Dennis Zimmer
Bertram Wöhrmann
Carsten Schäfer
Günter Baumgart
Urs Stephan Alder
Oliver Kügow
Marcel Brunner

VMware vSphere 5

Das umfassende Handbuch

Inkl. Umstieg von ESX nach ESXi

- Installation, Konfiguration, Administration
- Storage-Design und Storage-Konfiguration, NetApp, EMC²
- Netzwerk, Backup, Ausfallsicherheit, Cluster, Lizenzierung u.v.m.

Galileo Computing

Dennis Zimmer, Bertram Wöhrmann, Carsten Schäfer,
Günter Baumgart, Oliver Kügow, Urs Stephan Alder,
Marcel Brunner

VMware vSphere 5

Das umfassende Handbuch

Galileo Press

Liebe Leserin, lieber Leser,

Servervirtualisierung war gestern, heute ist »Cloud« das Modewort. Jede Cloud basiert jedoch auf der Technologie der Servervirtualisierung. VMware vSphere, das nun in der Version 5 vorliegt, ist das Flaggschiff unter den Servervirtualisierungs-Lösungen. Und stellt Ihnen wichtige Funktionen zur Verfügung: dynamische Provisionierung und Anpassung von Ressourcen, gute Messbarkeit, eine sehr hohe Ausfallsicherheit sowie die Abbildung von SLAs. Als VMware-Administrator verschwinden Ihre Tätigkeiten nicht in einer virtuellen Wolke. Im Gegenteil, Sie müssen sich mit neuen Funktionalitäten und Möglichkeiten auseinandersetzen und lernen diese im eigenen Betrieb umzusetzen. Effiziente Servervirtualisierung erfordert viel Know-how und Praxiserfahrung.

Aus diesem Grund hat Dennis Zimmer, erfolgreicher Unternehmer und bekannter Autor im Bereich der Virtualisierung und Rechenzentrumsverwaltung, ein ausgewähltes Autorenteam zur Servervirtualisierung mit VMware zusammengestellt. Neben ihm haben es sich Bertram Wöhrmann, Carsten Schäfer, Günter Baumgart, Oliver Kügow, Marcel Brunner und Urs Stephan Alder zur Aufgabe gemacht, Ihnen alles erforderliche Wissen rund um die Installation, die Konfiguration und die professionelle Administration klar und verständlich zu vermitteln. Die Autoren haben bereits viel produktive Erfahrung mit vSphere 5 gesammelt, die in diese Neuausgabe eingeflossen ist. Ihr enormes Fachwissen kommt Ihnen zu Gute.

Ob Sie Administrator oder Berater sind: Sie werden mit Sicherheit von den zahlreichen Tipps profitieren, die Ihnen diese Experten aus ihrer langjährigen Berufspraxis und ihrem Umgang mit den Virtualisierungslösungen von VMware geben. So nutzen Sie künftig die genannten Vorteile der Virtualisierung mit VMware vSphere 5 für sich!

Dieses Buch wurde mit großer Sorgfalt geschrieben, lektoriert und produziert. Sollte dennoch etwas nicht so funktionieren, wie Sie es erwarten, dann scheuen Sie sich nicht, sich mit uns in Verbindung zu setzen. Ihre Anregungen und Fragen sind jederzeit willkommen.

Wir wünschen Ihnen viel Erfolg bei Ihrer Arbeit mit diesem Buch und mit VMware vSphere 5.

Ihr Stephan Matteschеck
Lektorat Galileo Computing

stephan.matteschеck@galileo-press.de
www.galileocomputing.de
Galileo Press · Rheinwerkallee 4 · 53227 Bonn

Auf einen Blick

1	Einleitung	33
2	vSphere-Architektur	51
3	ESXi für Umsteiger	85
4	vMotion und Storage vMotion	97
5	Cluster	135
6	Installation	209
7	Verwaltungsmöglichkeiten	291
8	Netzwerk-Architektur	319
9	Storage-Architektur	393
10	Storage-Konfiguration unter VMware	487
11	Storage-Konfiguration des EMC-VNX-Speichersystems unter vSphere 5	569
12	Konfiguration von ESXi und vCenter	665
13	Konfiguration von vCenter-Add-ons	765
14	Ausfallsicherheit	847
15	Virtuelle Maschinen	885
16	Kapazitätsplanung mit dem VMware Capacity Planner	971
17	Sicherheit	1021
18	Die Lizenzierung von vSphere	1043
A	Automatisierung, Billing, Performance, vCenter Site Recovery Manager	1077
B	VMware-vShield-Zones-Produktfamilie	1099
C	Your Cloud	1129
D	vCenter Operations	1143
E	Die Virtualisierung des Desktops	1147

Der Name Galileo Press geht auf den italienischen Mathematiker und Philosophen Galileo Galilei (1564–1642) zurück. Er gilt als Gründungsfigur der neuzeitlichen Wissenschaft und wurde berühmt als Verfechter des modernen, heliozentrischen Weltbilds. Legendär ist sein Ausspruch *Eppur se muove* (Und sie bewegt sich doch). Das Emblem von Galileo Press ist der Jupiter, umkreist von den vier Galileischen Monden. Galilei entdeckte die nach ihm benannten Monde 1610.

Lektorat Stephan Mattescheck
Korrektorat Petra Biedermann, Reken
Einbandgestaltung Barbara Thoben
Coverfoto Oben: © Photomorphic Pte Ltd/istockimages, Links: © nynl – Fotolia.com; Rechts: © Vldislav Kochelaevs – Fotolia.com
Typografie und Layout Vera Brauner
Herstellung Steffi Ehrentraut
Satz SatzPro, Krefeld
Druck und Bindung Beltz Druckpartner, Hemsbach

Dieses Buch wurde gesetzt aus der Linotype Syntax Serif (9,25/13,25 pt) in FrameMaker.

Gerne stehen wir Ihnen mit Rat und Tat zur Seite:
stephan.mattescheck@galileo-press.de bei Fragen und Anmerkungen zum Inhalt des Buches
service@galileo-press.de für versandkostenfreie Bestellungen und Reklamationen
britta.behrens@galileo-press.de für Rezensions- und Schulungsexemplare

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über *http://dnb.d-nb.de* abrufbar.

ISBN 978-3-8362-1847-4

© Galileo Press, Bonn 2012
2., aktualisierte Auflage 2012

Das vorliegende Werk ist in all seinen Teilen urheberrechtlich geschützt. Alle Rechte vorbehalten, insbesondere das Recht der Übersetzung, des Vortrags, der Reproduktion, der Vervielfältigung auf fotomechanischem oder anderen Wegen und der Speicherung in elektronischen Medien. Ungeachtet der Sorgfalt, die auf die Erstellung von Text, Abbildungen und Programmen verwendet wurde, können weder Verlag noch Autor, Herausgeber oder Übersetzer für mögliche Fehler und deren Folgen eine juristische Verantwortung oder irgendeine Haftung übernehmen. Die in diesem Werk wiedergegebenen Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. können auch ohne besondere Kennzeichnung Marken sein und als solche den gesetzlichen Bestimmungen unterliegen.

Inhalt

Vorwort 23

1 Einleitung 33

1.1 Server-Virtualisierung 33
1.1.1 Was ist Server-Virtualisierung? 33
1.1.2 Was ist eine virtuelle Maschine? 34
1.1.3 Warum virtualisiert man? 34
1.1.4 Gibt es auch Nachteile? 36
1.1.5 Welche Arten der Virtualisierung gibt es? 37
1.1.6 Der Hypervisor genauer betrachtet 39
1.1.7 Die Entwicklungsgeschichte der Virtualisierung 39
1.2 Die VMware-Produktfamilie 40
1.3 Einführung in VMware vSphere 42
1.3.1 VMware ESXi 42
1.3.2 VMware vCenter Server 42
1.3.3 VMware vSphere-Client und VMware vSphere Web Client 42
1.3.4 VMware vSMP (Virtual Symmetric Multi Processing) 43
1.3.5 vSphere Virtual Machine File System (VMFS) 43
1.3.6 Thin Provisioning 43
1.3.7 vSphere Fault Tolerance 44
1.3.8 vSphere vMotion und Storage vMotion 44
1.3.9 vSphere High Availability (HA) 44
1.3.10 vSphere Distributed Resource Scheduling (DRS) 44
1.3.11 vSphere Distributed Power Management (DPM) 44
1.3.12 vSphere Storage DRS 45
1.3.13 vSphere Standard Switches, Distributed Switches (dvSwitch, vDS) und Port Groups 45
1.3.14 Storage I/O Control & Network I/O Control 45
1.3.15 Profile Driven Storage 46
1.3.16 Host-Profiles 46
1.3.17 VMware vShield Zones 46
1.3.18 vSphere Update Manager (VUM) 46
1.3.19 VMware vCenter Orchestrator 46
1.3.20 VMware Data Recovery 46
1.3.21 VMware vCenter Server Heartbeat 47
1.3.22 VMware Server Linked Mode 47

1.3.23 VMware vSphere SDKs 47
1.3.24 Die verfügbaren VMware-Editionen 48

2 vSphere-Architektur 51

2.1 Bestandteile der virtuellen Infrastruktur 51
2.2 vSphere-Host 52
2.2.1 Hardware 52
2.2.2 HCL 53
2.2.3 Maximale Ausstattung eines ESXi-Hosts 53
2.3 vCenter-Server 56
2.4 Architektur eines vSphere-Hosts 64
2.5 Grundlagen der CPU-Virtualisierung 66
2.5.1 CPU-Affinity 70
2.5.2 Hyperthreading 70
2.5.3 Virtual SMP (vSMP) 71
2.5.4 Best Practices 76
2.6 Grundlagen der Memory-Virtualisierung 77
2.6.1 Virtual Machine Memory 78
2.6.2 Memory-Overhead 78
2.6.3 Memory-Overcommitment 79
2.6.4 Memory-Compression 79
2.6.5 Content-based Page-Sharing 80
2.6.6 Memory-Ballooning 80
2.6.7 Memory-Swapping 81
2.6.8 Best Practices 82
2.7 Grundlagen der Hardwarevirtualisierung 82

3 ESXi für Umsteiger 85

3.1 Voraussetzungen 88
3.2 Migration vCenter Server 89
3.3 Migration ESX-Hosts 93

4 vMotion und Storage vMotion 97

4.1 vMotion 97
4.1.1 Funktionsweise 98
4.1.2 Voraussetzung 101
4.1.3 Neuerungen mit vSphere 5 107
4.1.4 Bedienung 114
4.1.5 Sicherheit 116

4.1.6 Problemfälle ... 116
4.1.7 Lizenzierung ... 122
4.1.8 Long Distance vMotion ... 122
4.2 Storage vMotion ... 123
4.2.1 Funktionsweise ... 123
4.2.2 Voraussetzung ... 126
4.2.3 Bedienung ... 129
4.2.4 Problemfälle ... 131
4.2.5 Lizenzierung ... 134

5 Cluster ... 135

5.1 Cluster-Objekt ... 135
5.1.1 Anlage des Clusters ... 135
5.1.2 EVC-(Enhanced vMotion Compatibility-)Mode ... 136
5.2 HA-Cluster ... 140
5.2.1 Technologie-Übersicht ... 140
5.2.2 Voraussetzungen für HA ... 143
5.2.3 HA-Komponenten ... 144
5.2.4 Lizenzierung von HA ... 145
5.2.5 Einrichtung von HA ... 145
5.2.6 ESX 4 und ESX 5 im Mix ... 149
5.2.7 HA Advanced Options ... 149
5.2.8 Virtual Machine Options ... 153
5.2.9 Der HA-Agent oder »Was passiert beim Hinzufügen eines ESX-Hosts zum HA-Cluster?« ... 155
5.2.10 Reconfigure for vSphere HA ... 156
5.2.11 Das Verhalten eines HA-Clusters ... 156
5.2.12 HA-Slot-Berechnung ... 158
5.2.13 HA-Master- und -Slave-Agents ... 159
5.2.14 HA Host Isolation ... 160
5.2.15 HA und getrennte (disconnected) ESX-Server ... 162
5.2.16 HA und DNS ... 162
5.2.17 HA im vSphere-Client (oder: Der Cluster treibt's bunt …) ... 163
5.2.18 HA-Limitierungen mit vSphere ... 163
5.2.19 HA Virtual Machine Monitoring ... 163
5.3 DRS-Cluster ... 167
5.3.1 Technologie-Übersicht ... 167
5.3.2 Lizenzierung von DRS ... 169
5.3.3 Anlage eines DRS-Clusters ... 169
5.3.4 Prioritäten-Ranking ... 170

5.3.5 DRS-Automation-Level ... 170
5.3.6 DRS Groups Manager ... 173
5.3.7 DRS-Affinity-Rules ... 176
5.3.8 DRS Virtual Machine Options ... 180
5.3.9 DRS und Resource-Pools ... 181
5.3.10 DRS und der Maintenance-Modus ... 182
5.3.11 DRS-Limitierungen mit vSphere ... 183
5.3.12 DPM (Distributed Power Management) ... 183
5.3.13 HA und DRS in Kombination ... 186
5.4 Storage DRS ... 186
5.4.1 Voraussetzungen und Limitierungen ... 187
5.4.2 Anlage des Datastore-Clusters ... 187
5.4.3 SDRS Initial Placement ... 192
5.4.4 SDRS-Regelwerk ... 194
5.4.5 SDRS-Zeitsteuerung ... 195
5.4.6 SDRS Maintenance Mode ... 197
5.4.7 SDRS und Speicherprofile ... 198
5.5 Fault Tolerance ... 198
5.5.1 Wie funktioniert Fault Tolerance? ... 199
5.5.2 Technische Voraussetzungen ... 200
5.5.3 Aktivieren von Fault Tolerance für eine virtuelle Maschine ... 204
5.5.4 Bedienung von Fault Tolerance für eine virtuelle Maschine ... 206
5.5.5 Snapshots mit FT ... 207
5.5.6 Was passiert im Fehlerfall? ... 208
5.5.7 Lizenzierung von FT ... 208

6 Installation ... 209

6.1 VMware vSphere 5.0 ... 209
6.1.1 VMware-vSphere-Systemvoraussetzungen ... 209
6.1.2 Download der Installationsmedien ... 212
6.1.3 Vor der Installation ... 214
6.1.4 Lokale Installation ... 214
6.1.5 Erststart vSphere 5i ... 220
6.1.6 vSphere CLI ... 221
6.1.7 PowerCLI ... 227
6.1.8 Installation über das Netzwerk ... 228
6.1.9 Installation im SAN ... 229
6.1.10 Installation in der virtuellen Maschine ... 231
6.2 Upgrade auf vSphere 5.x ... 231
6.2.1 Upgrade von der Version ESX 3.x/ESXi 3.x ... 231

6.2.2 Upgrade von der Version ESX 4.x/ESXi 4.x ... 231
6.3 VMware vCenter Server ... 235
6.3.1 vCenter-Systemvoraussetzungen ... 237
6.3.2 Download der Installationsmedien ... 239
6.3.3 Vorbereitung der Datenbank ... 239
6.3.4 Installation vCenter und Komponenten ... 249
6.3.5 vCenter-Protokolldateien ... 277
6.4 VMware vCenter Server-Appliance ... 278
6.5 VMware vCenter Converter Standalone ... 279
6.6 VMware Consolidated Backup ... 281
6.7 Hochverfügbarkeit vCenter Server ... 281
6.7.1 Manuelle Hochverfügbarkeit ... 281
6.7.2 Hochverfügbarkeit mit Microsoft Cluster ... 282
6.7.3 vCenter Server Heartbeat ... 282
6.7.4 Zusätzliche Software ... 282
6.8 Lizenzierung ... 282
6.8.1 Lizenzierung vSphere ... 283
6.8.2 Lizenzen prüfen – VI3.x ... 283
6.9 VMware Data Recovery ... 285
6.9.1 Installation des VMware Data Recovery Clients ... 287
6.10 VMware vSphere Storage Appliance (VSA) ... 287
6.10.1 Installation des VSA-Managers ... 288
6.10.2 Installation des VSA-Clusters ... 289

7 Verwaltungsmöglichkeiten ... 291

7.1 Weboberfläche ... 291
7.2 Lokale Host-Konsole ... 294
7.3 Host-Konsole per SSH ... 295
7.4 vSphere-Client ... 296
7.4.1 Download und Installation des vSphere-Clients ... 296
7.4.2 Verwenden des vSphere-Clients ... 296
7.5 Administration über mobile Geräte ... 302
7.6 vCenter-Server ... 305
7.6.1 Installation des vCenter-Servers ... 306
7.6.2 Starten des vCenter-Servers ... 307
7.6.3 Hinzufügen von ESXi-Hosts ins vCenter ... 307
7.6.4 Verwaltung von vSphere-Hosts ... 308
7.6.5 Weitere Funktionen durch vCenter-Server ... 309
7.6.6 Einbindung ins Active Directory ... 310
7.6.7 Troubleshooting vCenter-Server ... 312

7.7 Remote Command-Line Interface 313
7.7.1 Installation 313
7.7.2 Ausführen des vSphere CLI 315
7.8 VMware vSphere PowerCLI 317

8 Netzwerk-Architektur 319

8.1 Grundsätzliche Planungsaspekte 319
8.1.1 Gutes Netzwerk-Design 319
8.1.2 1- und 10-Gigabit-LAN, maximale Anzahl physischer NICs 320
8.1.3 1 und 10 Gigabit versus Load-Balancing und Verkehrsmuster-Kontrolle 321
8.1.4 Wie viel Bandbreite benötige ich in der Praxis wirklich? 321
8.1.5 VLANs oder keine VLANs? 321
8.1.6 Physische Switches können die Load-Balancing-Policy beeinflussen 322
8.1.7 Links zwischen den physischen Switches 323
8.2 Die physischen und virtuellen Netzwerkschichten 323
8.3 Die physischen Netzwerkkarten im Host 326
8.4 Gegenüberstellung vSS und vDS 327
8.4.1 Die Eigenschaften der vSwitch-Typen im Überblick 327
8.4.2 Die beiden vSwitch-Typen 328
8.4.3 Der Switch-Teil bei vSS und vDS 329
8.4.4 Portgruppen bei vSS und vDS 330
8.4.5 Ports bei vSS und vDS 330
8.4.6 Die Layer-2-Security-Policies 331
8.4.7 Traffic-Shaping 332
8.4.8 Die VLAN-Einstellungen der vSwitch-Typen 333
8.4.9 Die NIC-Teaming- und die Load-Balancing-Policies der vSwitch-Typen 336
8.4.10 Die Arbeitsweise der Load-Balancing-Policies 336
8.4.11 CDP – Cisco Discovery Protocol der vSwitch-Typen 342
8.4.12 Configuration Maximums für vSS und vDS 343
8.5 Arbeiten mit dem vNetwork-Standard-Switch – vSS 344
8.5.1 Der vSS ist hostbezogen 344
8.5.2 Die Konfigurationsmöglichkeiten zum vSS 345
8.5.3 Einstellungen auf dem Switch oder den Portgruppen 346
8.6 Arbeiten mit dem vNetwork Distributed Switch – vDS 348
8.6.1 Der vDS existiert im vCenter und im Host 348
8.6.2 Die Konfigurationsmöglichkeiten des vDS 349
8.6.3 Einstellmöglichkeiten auf dem Switch-Teil des vDS 351

8.6.4 Private VLAN 354
8.6.5 Einstellmöglichkeiten auf der Distributed Portgruppe 356
8.6.6 Network I/O Control 359
8.6.7 NetFlow 363
8.6.8 Port-Mirroring 366
8.7 Die Migration von vSS auf vDS 370
8.7.1 Was wäre, wenn etwas falsch migriert wurde? 378
8.7.2 Was wäre, wenn das Management-Netzwerk verlorenginge? 378
8.8 Wiederherstellung des Management-Netzwerks 378
8.9 Architekturbeispiele 381
8.9.1 Empfehlungen und Best Practice 381
8.9.2 Beispiel auf Basis verfügbarer Ports im Server 386
8.9.3 ESX-Hosts mit zwei Netzwerkports 386
8.9.4 ESX-Hosts mit vier Netzwerkports 388
8.9.5 ESX-Hosts mit sechs Netzwerkports 389

9 Storage-Architektur 393

9.1 Lokale Medien 393
9.1.1 SATA 393
9.1.2 SCSI und SAS 396
9.1.3 Fibre-Channel 396
9.1.4 IDE 397
9.1.5 SSD 397
9.1.6 USB 400
9.1.7 Cache 400
9.2 Die Wahl: Block oder File 401
9.3 Storage Area Network – Was ist eigentlich ein SAN? 402
9.4 Infiniband 404
9.5 Kommunikationsadapter 404
9.5.1 Initiator 404
9.5.2 Target 409
9.5.3 Logical Unit Number – LUN 410
9.5.4 Pfadmanagement (Active/Active, Active/Passive) 410
9.6 FC-Speichernetzwerk 414
9.6.1 Vorteile und Nachteile 415
9.6.2 Support Matrix 415
9.6.3 Switch vs. Loop 416
9.6.4 Fabric 416
9.6.5 Verkabelung 416
9.6.6 Zoning 417

9.6.7 Mapping ... 419
9.6.8 NPIV (N-Port ID Virtualization) ... 419
9.7 FCoE ... 420
9.8 iSCSI-Speichernetzwerk ... 421
9.8.1 Vorteile und Nachteile ... 422
9.8.2 Kommunikation ... 422
9.8.3 IP-SAN-Trennung ... 423
9.9 Network-attached Storage ... 425
9.10 Flash-basiert ... 428
9.10.1 VMFS-Datastore ... 429
9.10.2 VMDirectPath ... 430
9.10.3 Host-Cache ... 432
9.10.4 Fusion-io ioTurbine ... 433
9.11 VMware-Storage-Architektur ... 434
9.11.1 VMkernel-Storage-Stack ... 435
9.11.2 Festplattendateien ... 438
9.11.3 Auslagerungsdateien ... 446
9.11.4 VMFS im Detail ... 449
9.11.5 Virtuelle Maschinen ... 460
9.11.6 VMware-Snapshots ... 464
9.11.7 VM-Speicherprofile ... 467
9.12 VAAI ... 470
9.12.1 VAAI-Einschränkungen ... 471
9.13 VASA ... 472
9.14 Storage I/O Control ... 472
9.14.1 Voraussetzungen ... 473
9.14.2 Konfiguration ... 473
9.15 VMware vSphere Storage Appliance ... 475
9.15.1 Funktionsumfang ... 476
9.15.2 Komponenten ... 476
9.15.3 Voraussetzungen ... 476
9.15.4 Kapazität ... 477
9.15.5 Architektur ... 477
9.16 Best Practices Storage ... 480
9.16.1 RAID-Leistungsfähigkeit ... 481
9.16.2 RAID-Größe ... 482
9.16.3 Geschwindigkeit vs. Kapazität ... 483
9.16.4 LUN-Größe ... 485
9.16.5 RAID-Rebuild und HP-EVA-Levelling ... 486

10 Storage-Konfiguration unter VMware 487

10.1 Verwendungszwecke von Storage 488
10.2 Einrichtung und Konfiguration von Datastores 489
10.2.1 Fibre-Channel 489
10.2.2 iSCSI 505
10.2.3 NFS-Datastores 517
10.3 Umgang mit Datastores 524
10.3.1 Rescan SAN 524
10.3.2 Speicheransichten 524
10.3.3 Datastore-Browser 526
10.3.4 Storage-Alarme 527
10.3.5 Datastore-Erweiterung 529
10.4 NetApp-Spezialitäten 531
10.4.1 Cloning-Technologien 531
10.4.2 Tuning und Optimierung 537
10.4.3 Best Practices 551

11 Storage-Konfiguration des EMC-VNX-Speichersystems unter vSphere 5 569

11.1 Einführung 569
11.2 Planung und Konfiguration eines VNX-Systems 570
11.2.1 Einleitung zu VNX-blockbasierten Speicheroptionen 572
11.2.2 Konfiguration der VNX für blockbasierten Zugriff 576
11.2.3 Best Practices zu blockbasierten Speicheroptionen 592
11.2.4 Einleitung zu VNX-dateibasierten Speicheroptionen 609
11.2.5 Konfiguration der Volumes für Dateisysteme 610
11.2.6 Best Practices der dateibasierten Speicheroption 619
11.3 Effizientes Arbeiten mit vSphere ESXi und VNX 626
11.3.1 Erstellen eines VMFS-Datastores 626
11.3.2 Erstellen eines Raw Device Mappings 628
11.3.3 Erstellen eines NFS-Datastores 628
11.3.4 Erweitern von Datastores 629
11.3.5 Snaps und Clones 630
11.3.6 Komprimierung 632
11.3.7 Einstellungen von Multipathing ändern 633
11.3.8 VAAI und Speicherprofile 633
11.4 Fortgeschrittene Techniken und Anwendungen 634
11.4.1 Command-Line Interfaces (CLIs) 634
11.4.2 Installation von VASA 637

11.4.3 Einrichten VAAI for File 640
11.4.4 Installation EMC PowerPath/VE 642
11.4.5 Blockbasierte Snapshots und Clones 644
11.4.6 Dateibasierte Snapshots und Clones 647
11.4.7 VMFS Volumen erweitern mit VNX 649
11.4.8 Erweitern eines NFS-Datastores mit VNX 650
11.4.9 Alignment von Volumes 651
11.4.10 Installation VSI 652
11.4.11 Installation des EMC Replication Managers 655
11.4.12 Installation von vSphere ESXi 5.0 657
11.4.13 VNX Virtual Storage Appliance 658
11.5 Troubleshooting – Erste Hilfe 659
11.5.1 Der ESXi-Host sieht keine FC-LUN 659
11.5.2 Der ESXi-Host hat keinen Schreibzugriff-Zugriff auf den NFS-Datastore 660
11.5.3 Ein Snapshot lässt sich nicht in ESXi präsentieren 661
11.5.4 Sie haben Trespassed LUNs 662

12 Konfiguration von ESXi und vCenter 665

12.1 Hostprofile 665
12.1.1 Erstellen eines Hostprofils 667
12.1.2 Anpassen eines Hostprofils 667
12.1.3 Host/Cluster mit Profil assoziieren 668
12.1.4 Anwenden eines Hostprofils 669
12.1.5 Profile-Compliance 671
12.2 NTP 672
12.2.1 NTP unter ESXi 673
12.2.2 NTP in der virtuellen Maschine mittels VMware Tools 675
12.2.3 Zeitsynchronisationsprobleme 676
12.3 SNMP 678
12.3.1 SNMP unter VMware 678
12.3.2 SNMP unter ESXi 679
12.3.3 SNMP in Gastbetriebssystemen 679
12.4 DNS 680
12.5 Einrichtung von Resource-Pools 681
12.6 VMware vApp 685
12.6.1 Erstellen einer vApp 685
12.6.2 Verknüpfung einer vApp mit virtuellen Servern 687
12.6.3 vApp-Einstellungen 689
12.7 Automatisches Starten und Stoppen der VMs mit dem Host 693

12.8 vSphere-Security 694
12.8.1 Öffnen und Schließen eines Ports mit dem vSphere-Client 697
12.9 Lizenz-Server 699
12.9.1 Konfiguration des vCenter-Lizenz-Servers 700
12.9.2 Konfiguration des Lizenz-Servers für VI3.x-Systeme 703
12.9.3 DNS-Name für Lizenz-Server 706
12.9.4 Umzug eines Lizenz-Servers 706
12.10 Erweiterte Hardwarekonfiguration 706
12.11 Erweiterte Softwarekonfiguration 711
12.11.1 Ablage der VM-Swapfiles 711
12.11.2 Host-Systemressourcen 711
12.11.3 Erweiterte Einstellungen 713
12.12 vCenter-Berechtigungen 714
12.12.1 Rollen 715
12.12.2 Benutzer einrichten 718
12.12.3 Absicherung gegenüber dem Betriebssystem 721
12.13 Performancedaten des Hosts im vCenter 722
12.14 Weitere Funktionen des vCenters 730
12.14.1 IP-Pools 731
12.14.2 Storage Views 733
12.14.3 Maps 736
12.14.4 Events 737
12.14.5 Scheduled Tasks 738
12.14.6 System-Logs 739
12.14.7 Sessions 742
12.14.8 vCenter Server Settings 742
12.14.9 vCenter Solutions Manager 742
12.14.10 Storage-Providers 743
12.14.11 VM-Speicherprofile 744
12.14.12 Customization Specification Manager 747
12.14.13 Hardware-Status 748
12.14.14 Dienste anzeigen 749
12.15 vCenter-Konfigurationseinstellungen 750
12.16 Einrichten von Alarmen 756
12.17 VMware vCenter Server-Appliance 760

13 Konfiguration von vCenter-Add-ons 765

13.1 Einsatz des vCenter Update Managers 765
13.1.1 Installation 766
13.1.2 Konfiguration 767

13.1.3 Events ... 773
13.1.4 Notifications ... 773
13.1.5 Patch Repository ... 773
13.1.6 ESXi Images ... 774
13.1.7 VA Upgrades ... 775
13.1.8 Download von Updates ... 775
13.1.9 Download von Updates auf Offline-Update-Manager ... 776
13.1.10 Baselines ... 780
13.1.11 Weitere Konfigurationsmöglichkeiten ... 789
13.2 VMware vCenter Linked Mode ... 790
13.3 vSphere Management Assistant (vMA) ... 793
13.3.1 Kommandozeile ... 794
13.3.2 Webinterface ... 796
13.3.3 Basisbedienung ... 797
13.4 VMware ESXi Dump Collector ... 800
13.5 VMware vSphere Syslog Collector ... 801
13.6 VMware vSphere Authentication Proxy ... 803
13.7 VMware vSphere Image Builder ... 805
13.8 VMware Auto Deploy ... 811
13.8.1 VMware Auto Deploy mit der vCenter Server-Appliance ... 816
13.9 VMware Data Recovery ... 818
13.9.1 Data Recovery – Hinweise ... 825
13.10 Einsatz des VMware vCenter Converters Standalone ... 825
13.10.1 Installation der Sysprep-Tools zur Anpassung von Windows-Maschinen ... 827
13.10.2 VMware vCenter Converter Standalone ... 828
13.10.3 Nacharbeiten nach der Übernahme ... 837
13.11 Einsatz der vSphere Storage Appliance ... 838
13.11.1 Virtuelle Maschinen auf einem VSA-Cluster ... 845
13.11.2 Deinstallation eines VSA-Clusters ... 846

14 Ausfallsicherheit ... 847

14.1 Sicherung – Rücksicherung ... 847
14.1.1 Sicherung des ESX-Hosts ... 847
14.1.2 Sicherung der Komponenten ... 849
14.1.3 Sicherung der virtuellen Maschinen ... 852
14.1.4 Backup von vSphere-Umgebungen mit NetApp-Storage ... 855
14.1.5 VMware Data Recovery ... 866
14.2 Cluster-Konfiguration ... 868
14.2.1 Voraussetzungen für den Microsoft Cluster Service ... 869

14.2.2 Cluster-Konfiguration auf einem Host ... 870
14.2.3 Cluster-Konfiguration über mehrere Hosts ... 877
14.2.4 Cluster-Konfiguration zwischen physischem und virtuellem Knoten ... 879
14.3 Virtual Machine Monitoring ... 881
14.4 Fault Tolerance ... 884

15 Virtuelle Maschinen ... 885

15.1 Grundlagen ... 885
15.1.1 Was ist eine virtuelle Maschine? ... 885
15.1.2 Virtuelle Hardware ... 886
15.1.3 Bestandteile einer virtuellen Maschine ... 891
15.2 Erstellung von virtuellen Maschinen ... 893
15.2.1 Netzwerkkonfiguration ... 896
15.2.2 Festplattenkonfiguration ... 896
15.2.3 Aktualisieren der virtuellen Hardware ... 898
15.3 vSphere DirectPath I/O ... 900
15.4 Eigenschaften einer virtuellen Maschine – Optionen ... 902
15.4.1 Änderung des Namens der VM ... 903
15.4.2 Änderung des Gastbetriebssystems ... 903
15.4.3 Erweiterung der Power-Aktivitäten durch die VMware Tools ... 904
15.4.4 Automatische Ausführung der VMware-Tools-Skripte ... 904
15.4.5 Automatische Aktualisierung der VMware Tools ... 905
15.4.6 Zeitsynchronisation der VM mit dem ESX-Server ... 905
15.4.7 Power-Management des Gastbetriebssystems ... 906
15.4.8 Erweiterte Konfiguration: Logging, Debugging, Acceleration und erweiterte Konfigurationsparameter ... 906
15.4.9 Erweiterte Konfiguration: CPU Identification Mask ... 907
15.4.10 Erweiterte Konfiguration: Memory/CPU Hot Plug ... 908
15.4.11 Erweiterte Konfiguration: Boot Options ... 909
15.4.12 Erweiterte Konfiguration: Fibre Channel NPIV ... 910
15.4.13 Erweiterte Konfiguration: CPU/MMU Virtualization ... 910
15.4.14 Erweiterte Konfiguration: Swapfile Location ... 912
15.5 Ressourcenmanagement einer VM ... 912
15.5.1 CPU-Ressourcen ... 912
15.5.2 Memory-Ressourcen ... 915
15.5.3 Disk-Ressourcen ... 918
15.6 USB-Geräte an virtuellen Maschinen ... 919
15.6.1 USB-Passthrough ... 919

15.6.2 USB-Autoconnect ... 920
15.6.3 Kompatible vSphere-Funktionen ... 920
15.6.4 Das Verbinden von USB-Geräten ... 921
15.6.5 Das Entfernen von USB-Geräten ... 925
15.7 VM-Speicherprofile (VM Storage Profiles) ... 925
15.7.1 Festlegen der benutzerdefinierten Speicherfunktionen ... 926
15.7.2 Erstellen von VM-Speicherprofilen ... 927
15.7.3 Zuweisen von benutzerbedingten Speicherfunktionen ... 928
15.7.4 Verwenden von VM-Speicherprofilen ... 929
15.8 Starten, Stoppen und weitere Power-Aktivitäten ... 930
15.9 Installation des Gastbetriebssystems ... 931
15.10 Konfiguration und Anpassung von virtuellen Maschinen ... 933
15.10.1 Ändern der Hardware ... 933
15.10.2 Hinzufügen weiterer Hardware im laufenden Betrieb (Hot Add) ... 934
15.10.3 Statische MAC-Adresse über GUI ... 936
15.10.4 Umgang mit Wechselmedien ... 937
15.11 Optimierung einer virtuellen Maschine ... 938
15.12 VMware Tools ... 940
15.12.1 Zeitsynchronisation ... 941
15.12.2 Installation der VMware Tools ... 941
15.12.3 Manuelle Installation ... 942
15.12.4 Aktualisierung der VMware Tools ... 943
15.13 Migration von virtuellen Maschinen ... 945
15.13.1 Verschiedene Arten der Migration ... 945
15.13.2 Verwendung des Migration-Wizards zur Migration einer VM ... 946
15.14 Templates und Clones ... 946
15.14.1 Was sind Templates, und welchen Nutzen bringen sie? ... 946
15.14.2 Templates im vCenter ... 947
15.14.3 Templates erstellen, bearbeiten und löschen ... 947
15.14.4 Virtuelle Maschinen mit Hilfe von Templates erstellen ... 948
15.14.5 Was sind Clones, und wie erstellt man sie? ... 949
15.15 Anpassen der Gastbetriebssysteme ... 951
15.15.1 Voraussetzungen ... 951
15.15.2 Bearbeiten von Anpassungsspezifikationen ... 952
15.15.3 Anpassung des Gastbetriebssystems ... 955
15.16 Snapshots ... 956
15.16.1 Funktionsweise ... 956
15.16.2 Snapshot-Dateien auf dem Datastore ... 957
15.16.3 Hilfe bei Problemen ... 958

15.16.4 Die Snapshot-Hierarchie ... 958
15.16.5 Das Erstellen eines Snapshots (Take Snapshot) ... 960
15.16.6 Das Persistieren eines Snapshots (Delete Snapshot) ... 960
15.16.7 Das Verwerfen des aktuellen Zustands oder die Wiederherstellung eines Snapshots (Revert to Snapshot) ... 960
15.17 Die virtuelle Maschine im vSphere-Client ... 961
15.18 Erweitertes VM-Management ... 967
15.18.1 Killen einer hängenden VM ... 967
15.18.2 Überwachung der CPU-Performance von virtuellen Maschinen mit »esxtop« ... 968

16 Kapazitätsplanung mit dem VMware Capacity Planner ... 971

16.1 Erste Vorüberlegungen zu einem Migrationsprojekt ... 972
16.2 Arbeitsweise und Funktion des Capacity Planners ... 974
16.2.1 Data Collector und Information Warehouse ... 974
16.2.2 Collector-Modul ... 975
16.2.3 Data-Manager-Modul ... 976
16.2.4 Data Analyzer ... 977
16.2.5 Dashboard ... 977
16.3 Die Arbeit mit dem Capacity Planner ... 978
16.4 Die Arbeit mit dem Data Collector ... 978
16.4.1 Auffinden der Zielsysteme ... 978
16.4.2 Verbindungsaufbau zu den Zielsystemen ... 978
16.4.3 Manuelle Inventarisierung ... 979
16.4.4 Manuelle Leistungsdatenermittlung ... 980
16.4.5 Die Datensynchronisationsfunktion des Data Collectors ... 981
16.4.6 Automatisierte Ausführung von Jobs ... 982
16.4.7 Registrierung des Data Collectors im Information Warehouse ... 983
16.5 Das Dashboard im Detail ... 984
16.6 Ablauf eines Kapazitätsplanungsprojekts ... 1002
16.6.1 Company-ID-Request ... 1004
16.6.2 Vorbereitende Maßnahmen ... 1005
16.6.3 Überwachung der Messung ... 1008
16.6.4 Außerbetriebnahme des Data Collectors ... 1009
16.7 Auswertung ... 1009
16.7.1 Phantom-Server ... 1009
16.7.2 Konsolidierungsszenario ... 1010
16.7.3 Ergebnis ... 1013
16.7.4 Was bedeutet Verfügbarkeit? ... 1014

16.7.5 Berücksichtigung von Verfügbarkeit ... 1014
16.7.6 Betrachtung der Skalierbarkeit ... 1016
16.7.7 Ermittlung des Konsolidierungsverhältnisses bzw. der Grad der Konsolidierung bei der Virtualisierung ... 1017
16.7.8 Der Weg zum CP-Admin ... 1018

17 Sicherheit ... 1021

17.1 VMware ESXi ... 1021
17.1.1 Hardware-Management-Schnittstellen ... 1022
17.1.2 Security Profile ... 1022
17.2 »root«-Zugriff ... 1024
17.2.1 Troubleshooting-Modus über die Konsole ... 1025
17.3 Benutzerverwaltung ... 1025
17.3.1 Zurücksetzen des »root«-Passworts ... 1026
17.4 Firewall ... 1027
17.4.1 Firewall-Regeln anzeigen ... 1027
17.4.2 Firewall-Bedienung ... 1028
17.4.3 Custom Ports ... 1028
17.5 SSL-Zertifikat ... 1029
17.6 Überwachung ... 1030
17.7 Protokollierung ... 1030
17.8 Nützliche Zusatzsoftware ... 1033
17.8.1 HyTrust ... 1033
17.8.2 icomasoft Opvizor ... 1036
17.9 Virtuelle Maschinen in der DMZ ... 1038
17.9.1 Isolation ... 1038
17.9.2 Firewalls und VMs ... 1038
17.9.3 PVLAN ... 1039
17.9.4 Best Practices ... 1039
17.10 VMs und der Virenschutz ... 1039
17.10.1 Pattern-Updates ... 1039
17.10.2 CPU-Last im Host ... 1040
17.10.3 Antwortzeiten im Gast ... 1040
17.10.4 Fileserver mit Virenschutz ... 1040
17.11 VMware VMsafe-API ... 1041

18 Die Lizenzierung von vSphere ... 1043

18.1 Die unterschiedlichen Editionen und Pakete ... 1044
18.1.1 Grundlegende Informationen zur Lizenzierung ... 1044

18.1.2 vSphere 5 – for free ... 1046
18.1.3 vSphere 5 – Small Business ... 1047
18.1.4 vSphere 5 – Standard, Enterprise und Enterprise Plus ... 1049
18.1.5 vSphere 5 – Standard, Enterprise und Enterprise Plus als Pakete ... 1051
18.1.6 Erweiterung einer Umgebung durch Hinzufügen von Funktionalität ... 1052
18.1.7 SLES für vSphere-Lizenz-Besitzer ... 1052
18.2 Support und Subscription ... 1053
18.2.1 Die unterschiedlichen Schweregrade ... 1055
18.2.2 Wie stellen Sie eine Supportanfrage bei VMware? ... 1055
18.3 Die vSphere 5-Lizenzen ... 1062
18.4 Die VI3-Lizenzierung ... 1068

Anhang ... 1075

A Automatisierung, Billing, Performance, vCenter Site Recovery Manager ... 1077
A.1 Automatisierung ... 1077
A.2 Billing: VMware vCenter Chargeback ... 1084
A.3 Performance: VMware vCenter AppSpeed ... 1087
A.4 vCenter Site Recovery Manager ... 1091
B VMware-vShield-Zones-Produktfamilie ... 1099
B.1 Einleitung ... 1099
B.2 VMsafe-API ... 1101
B.3 Die einzelnen vShield-Komponenten ... 1104
B.4 vShield App ... 1111
B.5 vShield Edge ... 1124
B.6 vShield Endpoint ... 1127
B.7 Versionskompatibilität und Links ... 1127
C Your Cloud ... 1129
C.1 Cloud-Komponenten ... 1130
D vCenter Operations ... 1143
D.1 Lizenzierung ... 1146
E Die Virtualisierung des Desktops ... 1147
E.1 Desktop-Management mit VMware View ... 1148
E.2 Das Display-Protokoll – PCoIP ... 1160
E.3 Virtualisierung von Applikationen mit ThinApp ... 1161

Index ... 1163

Vorwort

Da wir im Buch die sehr gute Diagramm- und Icon-Library von VMware zur Erstellung der Grafiken genutzt haben, sind wir verpflichtet, folgendes Statement abzudrucken:

This document was created using the official VMware icon and diagram library. Copyright 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware does not endorse or make any representations about third party information included in this document, nor does the inclusion of any VMware icon or diagram in this document imply such an endorsement.

Vorwort Thomas Kühlewein

VMware hat die Komplexität von IT Infrastrukturen massiv reduziert und konnte seine Marktführerschaft in der Virtualisierung von X86 Systemen kontinuierlich ausbauen.

Die Autoren sind zu engen Wegbegleitern von VMware geworden. Durch ihre Bücher konnten zahlreiche Kunden und Partner von VMware das Potential der Virtualisierung schneller erschließen und Ihre IT verbessern. Im Namen von VMware möchte ich mich hierfür herzlich bedanken. Mit VMware vSphere 5 hat VMware seinen Kunden den Weg zu Cloud-Computing eröffnet. Das Buch erklärt auf sehr verständliche Weise, wie Sie Auslastung, Automatisierung und Sicherheit Ihrer IT-Infrastruktur weiter verbessern können. Ein Muss für alle, die den Weg in die Ära des Cloud-Computings erfolgreich beschreiten wollen.

Thomas Kühlewein
Vice President CEMEA bei VMware

Danksagung Urs Stephan Alder

Diese kurze Danksagung zu schreiben war fast schwieriger, als das Netzwerk-Kapitel in dieser neuen Auflage, da meine poetische Ader bei weitem nicht so ausgeprägt ist wie meine technische.

Es hat mich schon immer gereizt, ein Fachbuch zu schreiben. Doch ein Umstand, der sich immer massiv in den Weg stellte, war meine verfügbare Zeit. Dank dem Autorenteam dieser Auflage des Buches, das mich dankenswerterweise sehr freundlich aufgenommen hat, durfte ich mich nun als Fachbuchautor für ein Kapitel einbringen. Die Erfahrung war sehr intensiv und interessant. Wer weiß, vielleicht wird es nächstes Mal noch ein wenig mehr.

Bedanken möchte ich mich vor allem bei meiner Frau Sabine und meinem dreieinhalbjährigen Sohn Max: Danke, dass ihr es mir nicht übelgenommen habt, dass ich zwischen Weihnachten und Neujahr 2011/2012 »untergetaucht« bin, um mich voll auf das Buchkapitel zu konzentrieren!

Vorwort und Danksagung Günter Baumgart

Bis Anfang der 1990er Jahre studierte ich Elektrotechnik an der Fachhochschule Bochum und absolvierte ab 2003 ein weiterbildendes Studium »IT-Sicherheit – Administration und Sicherheit von IT-Systemen und -Netzwerken« an der Ruhruniversität Bochum. Seit 1990 bin ich im Bereich Softwareentwicklung, Engineering und Architektur von IT-Systemen tätig. 1999 setzte ich erstmalig ein Virtualisierungsprodukt aus dem Hause VMware ein und war augenblicklich ein Anhänger von Virtualisierungstechnologien.

Ich freue mich ganz besonders, auch in dieser Auflage des Buches wieder mit meinen Beiträgen dabei zu sein: Kapitel 16, »Kapazitätsplanung mit dem VMware Capacity Planner«, Kapitel 18, »Die Lizenzierung von vSphere«, und sogar mit einem neuen Beitrag in Anhang B, »Die Virtualisierung des Desktops«. Und auch dieses Mal war es wieder eine Herausforderung, die Themen so aufzuarbeiten und zu beschreiben, dass ein interessierter Leser voll auf seine Kosten kommt! Es hat wieder viele Wochenenden, Feiertage und Nächte gebraucht, um alle Kapitel fertigzustellen, und auch bei diesem Projekt hatte ich wieder die volle Unterstützung meiner ganzen Familie.

Meine Frau Annette war wie immer eine großartige Unterstützung und stand mir jederzeit mit Rat und Tat zur Seite, um mir zu ermöglichen, so zu schreiben, dass die Inhalte auch diesmal zum Weiterlesen bewegen. Sie hat mir auch, wie immer, den Rücken freigehalten, so dass ich die Möglichkeit hatte, die nötige Ruhe zu finden, um eine gute Arbeit abliefern zu können. Alle, die dieses Kapitel lesen und Kinder haben, werden wissen, wovon ich spreche. Und natürlich gilt mein Dank auch Maxi und Flori, die einmal mehr auf Papa verzichten mussten, und das gerade in der Zeit, in der viele Klausuren in der Schule anstanden.

Vorwort und Danksagung Marcel Brunner

Nach meinem Besuch an der Universität Zürich mit Studien in Wirtschaft und Psychologie entschloss ich mich, in die Informatik zu wechseln. Mein Ausflug in die operative Informatik dauerte weniger als ein Jahr. Ende der 1990er Jahre ergriff ich die Chance, bei dem amerikanischen Hersteller Sun Microsystems als Presales Consultant zu arbeiten. Fünf Jahre später begann ich meine Tätigkeit bei EMC. Ich war vier Jahre als Spezialist für NAS-Lösungen zuständig.

Im Jahr 2008 nahm ich eine neue Herausforderung bei EMC als Virtualisierungsspezialist an. Heute arbeite ich als vSpecialist und betreue die Großkunden von EMC im Raum Europa, Mittlerer Osten und Afrika. Nebenberuflich leite ich die Informatik des schweizerischen Kleinunternehmens wellwave.net AG.

Es freut mich sehr, dass in dieser Auflage des Buches auch EMC mit einem vollwertigen Kapitel vertreten ist. Ich konzentriere mich auf die Produktreihe VNX, die sich in der DACH-Region großer Beliebtheit erfreut. Einsteiger in die EMC-Technologie erfahren, wie sie nach Best Practices eine VNX für den Block- und NAS-Bereich konfigurieren und in vSphere 5 integrieren. Ich hoffe, dass ich auch Experten den einen oder anderen Tipp vermitteln kann. Besonderen Spaß bereitete mir die Aufbereitung der Themen VAAI und VASA!

Besonderer Dank gebührt meiner Freundin Valérie für Ihr Verständnis und Ihre Fürsorge. Bedanken möchte ich mich auch bei der Kybernetika AG, die keine Mühe scheute und mir die benötigte Infrastruktur zur Verfügung stellte.

Vorwort Oliver Kügow

An einem schönen Sommerabend im Jahre 2009 saß ich zusammen mit Dennis Zimmer in einem Weingut im Rheingau. Wir waren Sprecher auf einer Konferenz und saßen abends beide am gleichen Tisch. In einem schwachen Moment, als ich nicht schnell genug »nein« sagte, war ich plötzlich als Co-Autor für das Buch »vSphere 4« verpflichtet. Dieses Ereignis ist nun fast drei Jahre her. VMware hat uns mit einer weiteren Version der Plattform vSphere gesegnet. Auch NetApp als Speicherhersteller brachte in den letzten Jahre weitere neue Funktionen in seinem Betriebssystem auf den Markt. Ganz besonders interessant ist der Grad der Integration zwischen Virtualisierung und Storage geworden.

Es ist Zeit geworden, nach etwa zwei Jahren das Buch und somit mein Kapitel 10, »Storage-Konfiguration unter VMware«, auf den aktuellen Stand der Zeit und Technik zu bringen. Doch nun zu meinem Werdegang: Mein Name ist Oliver Kügow, ich bin aktuell 33 Jahre alt und arbeite seit mehr als 10 Jahren in der IT-Branche. Begonnen hat mein Bezug zur IT schon in der Jugend, als ich neben der Schule bei diversen Internet-Providern mit Linux und Netzen arbeitete und dort mein Wissen aufbauen konnte.

Anschließend studierte ich Wirtschaftsinformatik an der Technischen Fachhochschule in Berlin – als Werksstudent bei der Siemens AG in Form eines berufsbegleitenden Studiums. Bei Siemens arbeitete ich während meines Studiums in der Systemadministration, im Netzwerkbetrieb und in der Systemplanung.Während dieser Zeit lernte ich auch die Firma NetApp und deren beeindruckende Produkte kennen; damals wurde bei Siemens das Produkt »NetCache« als Proxy-Lösung eingesetzt, wenig später kam ich auch mit den NetApp-Storage-Produkten in Kontakt.

Neben meinem Studium hielt ich bereits Schulungen für Fujitsu Siemens in Nürnberg ab; dort traf ich auf Kurt-Jürgen Jacobs und Dirk Schmiedt – zwei immer noch sehr geschätzte Geschäftspartner. Noch vor dem Ende meines Studiums machte ich mich zusammen mit Richard Müller selbständig: Wir gründeten die teamix GmbH, ein Systemhaus mit starkem Dienstleistungs- und Know-how-Fokus. Die Firma teamix wurde 2011 10 Jahre alt – unser Geschäftsfeld konzentriert sich auf die IT-Infrastruktur: Virtualisierung, Speicherlösungen, Netzwerke und Betriebssysteme.

Cloud-Computing – mein Verständnis

Wer schon länger in der IT-Branche tätig ist, der weiß, dass dort gerne in »Wellen« gedacht wird; verschiedene Trends setzen sich durch und wiederholen sich – manchmal auch in gegenläufigen Zyklen. Wir schwanken von Zentralisierung zu Dezentralisierung, von Outsourcing zu Insourcing. Der aktuelle Trend heißt ganz klar »Cloud-Computing«. Ob alle Visionen, die aktuell kursieren, wahr werden, möchte ich bezweifeln, aber ein Wandel in der Branche vollzieht sich momentan ganz sicher.

Ich bin der Meinung, dass es sich hierbei um mehr als nur einen »Hype« handelt – es ist die Transformation der klassischen IT weg vom Silo-Denken hin zu einer dynamischen IT-Infrastruktur. Das muss nicht gleich »Outsourcing« bedeuten, sondern lediglich die Entwicklung von Rechenzentren hin zu Dienstleistungsfabriken, die es ermöglichen, agilere Geschäftsprozesse abzubilden und somit die Wettbewerbsfähigkeit von Unternehmen zu stärken. IT-Abteilungen werden sich künftig weniger um den Infrastrukturbetrieb kümmern, sondern mehr Zeit in Applikationen und Geschäftsprozesse investieren können.

Es ist wichtig zu verstehen, dass die interne IT nicht ausschließlich durch den Vorgang der Virtualisierung zu einer »Cloud« wird. Eine Cloud entsteht durch hochgradige Automatisierung und integriertes Management. In den nächsten Jahren wird es darum gehen, die verschiedenen Komponenten der Virtualisierung (Hypervisor, Storage, Netzwerk) durch Orchestrierung und Managementlösungen in eine automatisierte IT zu verwandeln.

Dennoch: Die Basis-Infrastruktur muss zuverlässig funktionieren, und Virtualisierung ist eine wichtige Komponente dafür. Wie Sie richtig virtualisieren und welche Hürden im Zusammenhang mit zentralen Speicherlösungen zu nehmen sind, können Sie in meinem Kapitel 10, »Storage-Konfiguration unter VMware«, nachlesen. Viel Spaß dabei!

Danksagung

An dieser Stelle möchte mich ganz herzlich bei Dennis Zimmer bedanken, der mich bat, an diesem Buch mitzuwirken. Das Buch »vSphere 4« war unser erstes gemeinsames Projekt, nun arbeiten wir zum zweiten Mal gemeinsam an einem Buch. Des Weiteren möchte ich meinem teamix-Team dafür danken, dass sie immer einen exzellenten Job bei unseren Kunden machen und dafür sorgen, dass die Kunden stets eine solide IT-Infrastruktur betreiben können!

Danke auch an Kurt-Jürgen Jacobs und seine Schulungsfirma qSkills aus Nürnberg; ohne dich wären wir, teamix, heute nicht so weit, wie wir es jetzt sind.

Last but not least: Danke auch an Steffi, meine Frau, und Alex, meinen Sohn, und Johanna, meine kleine Tochter, für die Geduld, die ihr aufgebracht habt, während ich an meinem Kapitel geschrieben habe, anstatt euch die Zeit zu widmen!

Vorwort Carsten Schäfer

Mein Name ist Carsten Schäfer, und ich bin seit 1990 beruflich in der IT-Welt unterwegs. Hier ist mein Aufgabengebiet breitgefächert und umfasst heute für meine selbständige Beratertätigkeit in der G-TAC IT-Beratung die Technologien Virtualisierung mit VMware vSphere, Hyper-V und Microsoft Active Directory Services, vornehmlich für den Einsatz in Server-Farmen und Enterprise-Umgebungen. Hierzu zähle ich auch die großen Themengebiete Server-Konsolidierung, Server-Migrationen und Rechenzentrumsplanungen. Darüber hinaus agiere ich in Projekten auch als GPM-zertifizierter Projektmanager.

Eine weitere große Leidenschaft ist die Softwareentwicklung im .NET-Umfeld, die ich zum einen in Projekten zur Betriebsautomatisierung von IT-Landschaften auslebe und zum anderen als geschäftsführender Gesellschafter der G-TAC Software Unternehmergesellschaft – hier mündet diese Leidenschaft in Produkte zur Automatisierung des IT-Betriebes, vornehmlich von Printing-Umgebungen, und weiteren Administrations-Tools sowie in ein plattformübergreifendes Produktivitätswerkzeug, das im Sommer 2012 das Licht der Software-Welt erblickt. Unsere Arbeit fußt auf dem Clean-Code-Developer-Wertesystem, und mein Team und ich halten diese Fahne fortwährend nach oben, um qualitativ hochwertige Produkte mit Spaß und Genuss herzustellen.

Danksagung

Zuerst möchte ich Dennis Zimmer und Bertram Wöhrmann für ihr Vertrauen danken und für die Chance, wieder an diesem Projekt mitzuarbeiten. Ging doch der ersten Auflage eine lange Zeit mit Vorbereitungen und Änderungen voraus, so dass wir heute mit der zweiten Auflage froh und stolz sein können, Ihnen wieder ein umfassendes Werk zur Verfügung zu stellen. Auch sei hier Dennis Zimmers erstklassiger Support während der letzten Jahre erwähnt, für den ich mich gerne zusätzlich bedanken möchte.

An unseren Sponsor richte ich nochmals ein großes Dankeschön. Er hat es uns ermöglicht, unsere Tests auf einer performanten Umgebung zu fahren!

Unserem Lektor Stephan Matteschеck gebührt ebenfalls mein Dank für seine Geduld und Unterstützung bei diesem Projekt.

Abschließend noch mein herzlichstes Dankeschön an meinen Sohn Tim, der mich nicht immer belagern konnte, wie er wollte, und sicherlich mehr als einmal gedacht hat: »Warum sitzt mein Papa immer wieder vor seinem Mac und schaut so ...?«

Vorwort Bertram Wöhrmann

Es war für mich Anfang 2009 ein großer Schritt, von Dennis in das Team für das vSphere 4-Buch aufgenommen zu werden. Bis heute folgten dem ein weiteres Buch und viele Fachartikel. Ende letzten Jahres kam dann ein Videotraining zum Thema vSphere 5 dazu. Dieser Einsatz für VMware und meine Tätigkeit als Co-Autor beim Blog *www.vmachine.de* haben mir im letzten Jahr erstmalig die Ernennung zum vExpert gebracht. Diese Auszeichnung vergibt VMware jedes Jahr an weltweit 300 Personen.

Doch nun zu meinem Werdegang: Nach meinem Informatikstudium begann ich als Programmierer und schrieb in Chile eine Teleskopsteuerungssoftware. Nachdem das Projekt abgeschlossen war, wechselte ich in den Bereich Windows-Administration und Netzwerke. Nach einem Arbeitgeberwechsel konzentrierte ich mich ganz auf die Administration von Windows-Servern. Im Jahr 2005 wurde ich auf das Thema VMware-Virtualisierung aufmerksam. Seitdem gilt diesem Bereich ein großer Teil meiner Aufmerksamkeit. Die Planung, der Aufbau und die Weiterentwicklung von virtuellen Landschaften sind dabei meine Hauptaufgaben.

Ich hoffe, dass ich Ihnen das Thema VMware vSphere näherbringen kann und Sie von dem Buch für Ihre Arbeit profitieren.

Danksagung

Zuallererst möchte ich mich beim Buchteam für die tolle Zusammenarbeit bedanken. Es ist schon fantastisch, mit so vielen Spezialisten an einem Projekt zusammenzuarbeiten. Der daraus resultierende Tiefgang kommt letztendlich dem Buch und Ihnen als Leser zugute. Das war wohl auch der Grund für den Erfolg der ersten Auflage. Den Dank von Dennis Zimmer kann ich nur zurückgeben. Er hat mich zum Schreiben gebracht, sein Vertrauen in mich gesetzt und mir die Chance zur Mitarbeit in den Buchprojekten gegeben.

Mein Dank gilt ebenfalls allen Kollegen des Verlags, die uns tatkräftig unterstützt haben und uns die Veröffentlichung des Buchs ermöglichen. Besonderer Dank gilt Stephan Matteschеck, der auf Seiten des Verlags die Fäden in der Hand gehalten hat. Auch unsere Korrektorin möchte ich an dieser Stelle erwähnen, die es geschafft hat, die Wahl von Begriffen und Namensgebungen abzugleichen, so dass Sie ein einheitlich verständliches Werk in der Hand

halten können. Viele Menschen haben mir mit Rat und Tat zur Seite gestanden und mich immer wieder motiviert. Den Kollegen, die uns unterstützt haben, die Qualität des Buches zu sichern, gilt ebenfalls mein ausdrücklicher Dank.

Danke auch an Urs Alder, der uns die Serverlandschaft zur Verfügung gestellt hat und uns somit das Schreiben des Buchs erst ermöglicht hat.

Meiner Familie gilt mein größter Dank; meine Frau Kornelia hat mich immer in meiner Arbeit bestärkt. Dieser Rückhalt und das Verständnis meiner Jungs Sven und Pit für das Schreiben haben mir erst ermöglicht, meine Buchprojekte durchzuführen.

Widmen möchte ich das Buch meinen Eltern. Leider hat mein Vater den Abschluss dieses Projekts nicht mehr erlebt. Durch die Unterstützung meiner Eltern während meiner Ausbildung haben sie einen wesentlichen Anteil an meinem beruflichen Werdegang gehabt und mir so die Basis für das gegeben, was ich bis jetzt erreicht habe.

Vorwort Dennis Zimmer

Ich arbeite seit mittlerweile über 15 Jahren in der IT-Branche und bin Gründer und CEO der opvizor GmbH sowie der icomasoft AG, welche die SaaS-Software opvizor entwickelt – zur Fehlerverhinderung und Optimierung von VMware-vSphere-Umgebungen. Außerdem wurde ich 2009 durch VMware zu einem von weltweit 300 vExperts ernannt und konnte diesen Status bis zur Drucklegung des Buches halten. Diese Auszeichnung wurde 2009 das erste Mal verliehen. Außerdem bin ich VCP seit der Version 2 und VCAP-DCA und VCAP-DCD in der Version 4.

Mit Erstaunen habe ich festgestellt, dass ich dank diesem Buch an sieben deutschsprachigen und zwei englischsprachigen Büchern beteiligt war, bzw. einige alleine geschrieben habe. Das tolle Feedback, das ich in den Jahren seit dem Erscheinen des ersten Buches 2006 von Lesern und der Community erhalten habe war sensationell und darüber bin ich sehr dankbar!

Doch zurück zu meiner Historie: Nach der Ausbildung zum Datenverarbeitungskaufmann war ich lange Jahre in der Systemadministration tätig. Meine Begeisterung für die virtuelle Infrastruktur lenkte meinen Weg in Richtung Beratung. Als Berater für Konsolidierungs- und Infrastrukturlösungen war ich bei einem der ersten deutschen VMware Consulting Partner (VAC), der Mightycare Solutions GmbH, tätig und beriet viele mittlere und große Unternehmen in Virtualisierungsfragen. Danach wollte ich einmal die Seite des Herstellers kennenlernen, und ich startete bei dem Storage-Hersteller Pillar Data Systems als Virtualisation Specialist und Systems Engineer. In dieser Funktion kamen zur Kundenberatung die Aspekte Produktweiterentwicklung und Marketing hinzu.

Ich hoffe sehr, Ihnen aufgrund meiner langjährigen Erfahrung auf diesem Gebiet hilfreiche Tipps und Leitfäden zu VMware vSphere geben zu können.

Danksagung

An dieser Stelle möchte mich ganz herzlich bei allen Personen bedanken, die mich bei der Planung und Durchführung unterstützt haben. Dazu zählen sämtliche Unterstützer bei Galileo Computing. Natürlich gilt auch besonderer Dank dem Team der Autoren, die fantastisch mitgearbeitet und dem Buch zu einem erstaunlichen Tiefgang verholfen haben: Urs Alder, Günter Baumgart, Stephan Bohnengel, Marcel Brunner, Daniel Köck, Oliver Kügow und Carsten Schäfer.

Nicht zuletzt möchte ich Bertram Wöhrmann für seine Unterstützung danken, der unentwegt am Buch arbeitete und zusätzlich die Koordination übernahm! Vielen Dank für die tolle Zusammenarbeit!

Des Weiteren möchte ich mich bei vielen Personen bedanken, die mich sowohl bei der Inhaltserstellung als auch bei der Überprüfung auf Richtigkeit und Lesbarkeit unterstützt haben. Die Reihenfolge sagt nichts über den Einsatz der einzelnen Personen aus: Axel Rosenberg, Bengt Lassen, Sven Kempf, Thomas Weyell.

Außerdem möchte ich nochmals gesondert allen Sponsoren dieses Buchs danken, die durch Teststellungen und Infrastruktur dieses Buch erst in dieser Tiefe möglich machten:

- teamix GmbH
- d-on-d.com
- Emulex Corporation
- NetApp Deutschland GmbH
- NetApp Schweiz GmbH
- EMC Computer Systems AG, Schweiz

Mein sehr guter Kollege Urs Alder, der dieses Mal auch als Autor des Netzwerkkapitels mitwirkte, hat auch bei dieser Auflage eine komplette VMware-Infrastruktur mit zahlreichen Servern zur Verfügung gestellt, wofür ich ihm nochmals gesondert im Namen aller Autoren danken möchte.

Das größte Dankeschön gilt jedoch wie seit dem ersten Buch 2006 meiner Freundin Andrea, ohne die ich bisher keines meiner Bücher fertiggestellt hätte (bzw. gar nicht erst angefangen hätte), und auch diese Auflage hat wieder Monate Freizeit gekostet.

Widmung

Nachdem ich bei der ersten Auflage einen traurigen Anlass zur Widmung hatte, möchte ich diese neue Auflage meinem Vater widmen, der in den letzten Jahren viel Kraft aufbringen musste, um die Schicksalsschläge zu überstehen! Ich freue mich, dass du diese Zeit überstanden hast, und wünsche dir alles Glück und vor allem Gesundheit für die Zukunft.

Vielen Dank an unsere Sponsoren

Virtualisierung ist nicht bloß ein Hype,
es ist fester Bestandteil vieler IT-Landschaften geworden.

1 Einleitung

Autor dieses Kapitels ist Carsten Schäfer, G-TAC IT-Beratung,
Carsten.Schaefer@G-TAC.de

1.1 Server-Virtualisierung

Zunächst sollten wir die wichtigsten Fragen klären, nach dem Was, Warum und Wie der Virtualisierung.

1.1.1 Was ist Server-Virtualisierung?

Die Virtualisierung abstrahiert die physische Hardware vom Betriebssystem. Die klassische 1:1-Verbindung von Hardware und Betriebssystem, die man vor allem in der PC-Welt kennt, wird aufgehoben; dazwischen wird eine neue Schicht gelegt, die diese Abstraktion vornimmt, die *Virtualisierungsschicht*. In unserem Falle übernimmt das VMware-Produkt vSphere 5 mit seinem ESXi Server 5.0 die Aufgabe des Virtualisierers.

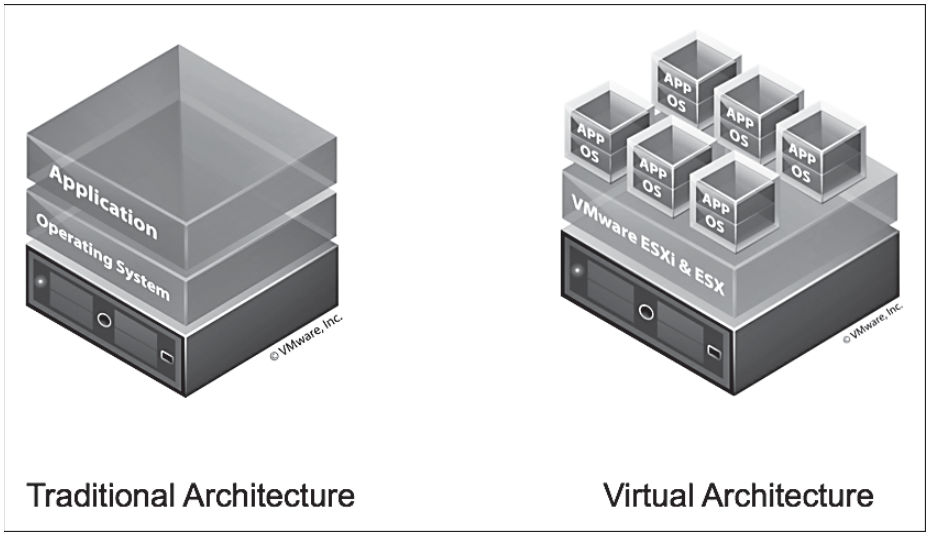


Abbildung 1.1 Ein Virtualisierer hebt die klassische Kopplung von Betriebssystem und Hardware auf.

1.1.2 Was ist eine virtuelle Maschine?

Da Sie den Begriff *virtuelle Maschine* ab jetzt mit schöner Regelmäßigkeit immer wieder lesen werden, möchten wir ihn kurz beschreiben. Eine virtuelle Maschine, oder auch VM abgekürzt, ist ein Synonym für virtuelle Systeme auf Basis der hier vorgestellten Technologien. Diese virtuelle Maschine besteht in erster Linie aus der virtuellen Hardware, nämlich Grafikkarte, CPUs, Speicher (RAM), Netzwerkkarten und Festplatten an SCSI- oder IDE-Controllern. Die vier zuletzt genannten Grundbestandteile einer virtuellen Maschine werden auch *Core Four* genannt. Zusätzlich kann die virtuelle Hardware um CD-/DVD-Laufwerke oder USB-Sticks erweitert werden. Wie für ein System üblich, wird auch eine virtuelle Maschine mit einem virtuellen BIOS versehen.

In einer virtuellen Maschine läuft ein vollständiges Betriebssystem, *Gastbetriebssystem* genannt, von verschiedenen Herstellern wie Microsoft (mit Windows 7, Windows Server 2008, Windows Server 2008 R2) oder verschiedene Linux-Distributionen (wie Suse oder Red Hat, Solaris), Apple OS X, Novell NetWare und teilweise auch Exoten wie OS/2. Das Gastbetriebssystem bedarf keinerlei Anpassungen, da es aus seiner Sicht auf einem vollständigen Server aufsetzt. Sogar die im Betriebssystem standardmäßig vorhandenen Treiber würden ausreichen, doch dies ist der erste Ansatzpunkt, um virtuelle Maschinen zu optimieren, indem auf ihnen speziell angepasste Treiber für die virtuelle Hardware installiert werden. Bei VMware befinden sich diese Treiber mitunter in den VMware Tools, die für die gängigen Betriebssysteme zur Verfügung stehen.

Eine virtuelle Maschine wird mit Hilfe von Dateien auf dem File-System des Virtualisierers abgebildet. Dies sind z. B. eine Konfigurationsdatei, die u. a. beschreibt, aus welchen virtuellen Bestandteilen diese virtuelle Maschine zusammengesetzt ist, oder auch die virtuelle Festplattendatei. Diese virtuelle Festplatte bildet die aus Sicht der virtuellen Maschine real existierende Festplatte ab und enthält alle Inhalte dieser Festplatte in einem spezifischen Format. Zusätzlich können weitere Dateien existieren. Die Bestandteile – also die Dateien – einer virtuellen Maschine unterscheiden sich zwischen den verschiedenen Virtualisierungslösungen der Hersteller.

1.1.3 Warum virtualisiert man?

Das Schlagwort in der IT ist *Consolidation* bzw. *Konsolidierung*. Dieser Begriff bezeichnet die Zusammenführung von vielen einzelnen Server-Systemen auf wenige physische Systeme. Diese wenigen physischen Systeme wiederum sind die Basis für darauf laufende virtuelle Maschinen. Genau genommen beschreibt die Konsolidierung die Zusammenführung der in den letzten Jahren rasant gewachsenen Anzahl von hardwarebasierten Servern.

Die Virtualisierung bietet uns folgende Vorteile:

- **Zusammenfassung von Servern**
  Das in der Windows-Welt sehr beliebte »One Service/One Server«-Denken verschlingt Unmengen von Platz und Strom. Es wird für einfache Windows-Server, die einen Dienst

bereitstellen, moderne Server-Hardware angeschafft, die mitunter für solche Aufgaben schlichtweg überdimensioniert ist. Mit virtualisierten Systemen partitionieren Sie leistungsstarke Hardware in kleinere Einheiten und betreiben in diesen Einheiten unterschiedliche Systeme für unterschiedlichste Anforderungen.

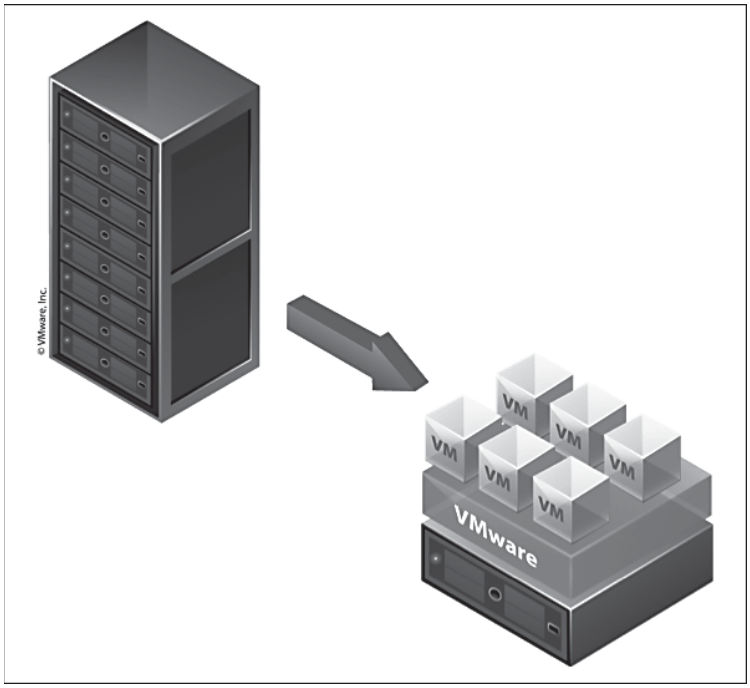


Abbildung 1.2 Viele physische Server werden auf einem physischen Server zusammengefasst (konsolidiert).

Auf einem physischen System können verschiedene Betriebssysteme in voneinander getrennten Einheiten parallel existieren.

Unterschiedliche Anforderungen verlangen nach unterschiedlicher (virtueller) Hardware. Auch eine nachträgliche Änderung einer Hardwareausstattung ist ohne langwierige Hardware-Beschaffungsprozesse mit Technikertermin und langer Downtime des Servers durch wenige Mausklicks durchführbar – bei entsprechender Unterstützung durch das Betriebssystem können z. B. Speicher oder CPUs hinzugefügt oder auch entfernt werden.

- **Server-Deployment**
  Die Deployment-Prozesse werden stark vereinfacht und um einiges schneller durchführbar. Nicht nur, dass Sie neue virtuelle Server in wenigen Minuten bereitstellen können, das Betriebssystem wird standardisiert und in ebenso kurzer Zeit installiert und muss lediglich noch vor dem Start angepasst werden.
- **Testumgebung**
  Eine virtuelle Testumgebung ist die ideale Spielwiese von IT-Administratoren, die gerne viele Systeme bereithalten, sich aber immer entsprechend aufwendig um diese kümmern

müssen. Nicht nur, dass Sie diese virtuelle Umgebung schnellstmöglich aufsetzen, abbauen und verändern können, durch Technologien wie Snapshots können Sie jeden beliebigen Stand Ihres Servers einfrieren, munter weitertesten und bei Bedarf in kürzester Zeit zum Ursprungszustand zurückspringen.

- **Backup und Disaster-Recovery**
  Ihre Strategie für Backup und Disaster-Recovery fußt auf komplett anderen Umgebungsvariablen als die einer physischen Umgebung und bringt höhere Flexibilität und erheblich bessere Laufzeiten mit sich. Stellen Sie sich nur vor, wie Sie mit einem Snapshot in Ihrer Storage-Umgebung Dutzende von Servern sichern können.
- **Vereinheitlichung von Hardware**
  Durch die einheitliche Hardware der virtuellen Systeme haben Sie immer einen Ansprechpartner für neue Hardwaretreiber. Das Wesentliche hierbei ist, dass es um *einen* Ansprechpartner geht und *alle* Ihre Systeme eben auf dieser Hardware basieren. Müssen Sie diese Systeme aktualisieren, so geschieht das über einfachste Wege ohne lästige BIOS-Updates von Server-Systemen oder ähnliche aufwendige Arbeit.

1.1.4 Gibt es auch Nachteile?

Wo Licht ist, ist auch Schatten. Gerne reden die namhaften Hersteller von Virtualisierungslösungen nicht über die Nachteile, da doch ihr Produkt alles kann. Über folgende Punkte sollten Sie genaue Überlegungen anstellen:

- **Know-how**
  Neben dem umfangreichen Wissen über die verschiedenen Betriebssysteme und die Anwendungen gesellt sich jetzt noch ein nicht minder komplexes Thema: Die virtuelle Infrastruktur will geplant, aufgebaut, betrieben und aktualisiert werden – als wenn die IT-Administratoren nicht genügend Themen zu betreuen haben ...
- **Single Point of Failure**
  Bis vor kurzem war gegen diesen Kritikpunkt noch kein Kraut gewachsen. Aber mit vSphere 5 kann auch ein Ausfall eines physischen Servers, des Virtualisierungs-Hosts, nicht mehr den Lebenswillen der darauf laufenden virtuellen Maschinen auslöschen. VMware Fault Tolerance ermöglicht eine Spiegelung von virtuellen Maschinen, was wir Ihnen in Kapitel 6, »Cluster«, beschreiben.
- **Server-Auslastung**
  Ein klarer Grund für die Entscheidung gegen eine Virtualisierung wäre eine hohe Auslastung eines physischen Servers. Auch die Art der Auslastung spielt eine Rolle: Ein physischer Server, der seine acht CPUs dauerhaft über 50 % Auslastung bringt und zudem einen hohen dauerhaften Speicherbedarf von z. B. 32 GByte oder mehr hat, ist sicherlich kein optimaler Virtualisierungskandidat. Möglich wäre die Virtualisierung, aber ob sie sinnvoll ist, sei dahingestellt.

Auch I/O-lastige Anwendungen, wie beispielsweise Webserver mit vielen statischen Seiten, generieren sehr viele I/Os, die durch das Nadelöhr der emulierten Festplatten und Netzwerkkarten des Virtualisierers geschickt werden müssen.

- **Server-Erweiterungen**
  Server mit Erweiterungskarten, wie z. B. zum Anschluss von Steuerungssystemen oder Fax- und ISDN-Karten, können nicht virtualisiert werden. Das Gleiche gilt für am Server angeschlossene Dongles oder sonstige Geräte, die über den seriellen Port mit einer Software auf dem Server kommunizieren. Vielleicht findet sich eine neue Version der Software oder Hardware beim Hersteller, um die starre Verbindung zwischen dem physischen Server und der Anwendung zu lösen.
- **Support und Lizenzen**
  Überprüfen Sie Ihre im Einsatz befindliche Software. Gibt es für alle Produkte Support vom jeweiligen Hersteller, wenn dessen Anwendungen auf virtueller Hardware laufen? Ein Beispiel für solche Fälle wäre Oracle, da dieses Unternehmen jeglichen Support für den Betrieb in einer Virtualisierungslösung, die nicht aus dem Hause Sun Microsystems stammt, verweigert.

  Oder ist die Lizenz einer Applikation mit z. B. der MAC-Adresse oder der CPU-ID des Servers verdrahtet? Ist der Support dieses Herstellers noch erreichbar oder bereits vom Markt verschwunden? Diese Lizenz wird nach der Umstellung des Servers auf eine virtuelle Hardware nicht mehr gültig sein, da sich die komplette Hardware ändert. Selbst wenn die Lizenz nur mit der MAC-Adresse verdrahtet ist, werden Sie nicht diese MAC-Adresse mit Ihrem virtuellen Server ins Netzwerk einbringen, da VMware zwar das manuelle Abändern der MAC-Adresse aller virtuellen Netzwerkkarten zulässt, die Hersteller-Signatur der MAC-Adresse ist und bleibt aber die von VMware.

1.1.5 Welche Arten der Virtualisierung gibt es?

Es existieren mehrere Wege der Virtualisierung, hier eine Übersicht:

- **Hypervisor-basierte Virtualisierung**
  Ein Hypervisor, auch *Virtual Machine Manager* (VMM) genannt, ist die Virtualisierungsschicht, die die Aufgabe hat, mehrere virtuelle Server-Systeme zu erzeugen, um darin dem laufenden Betriebssystem eine komplette, aber virtuelle Hardware vorzugaukeln. Sie kümmert sich um die Zuordnung der Hardwareressourcen zu den virtuellen Servern. Die hypervisor-basierte Virtualisierung unterteilt sich wiederum in zwei Varianten:
  - **Hypervisor Typ 1**
    Der Hypervisor vom Typ 1 wird auch *native* oder *Bare-Metal-Virtualisierung* genannt, läuft direkt auf der Hardware des Trägersystems und hat als Einziger die Kontrolle über die Hardware, um den darauf laufenden virtuellen Systemen die notwendigen Ressourcen zuzuteilen und diese zu kontrollieren.

Diese Form ist die schlankste und somit performantere Lösung der hypervisor-basierenden Virtualisierung. Die typischen Vertreter sind VMware vSphere, Citrix XenServer und Microsofts Hyper-V.

- **Hypervisor Typ 2**
  Der Hypervisor vom Typ 2 wird auch *Hosted Virtualisierung* genannt. Er setzt im Gegensatz zu Typ 1 auf einem Betriebssystem auf und ist aus Sicht des Träger-Betriebssystems lediglich eine Anwendung. Auch dieser Typ stellt den virtuellen Systemen Ressourcen zur Verfügung, und aus Sicht des Gastbetriebssystems im virtuellen System ist kein Unterschied zwischen Typ 1 oder Typ 2 erkennbar.

Diese Form der Virtualisierung stellt im Vergleich zu Typ 1 weniger Ressourcen zur Verteilung an die virtuellen Systeme zur Verfügung, da auch das Träger-Betriebssystem einen gewissen Ressourcenanteil beansprucht. Diese Form war es jedoch, die VMware damals den Siegeszug mit VMware Workstation ermöglichte, da damit jedermann auf seinem PC viele weitere Server- oder PC-Systeme zum Testen oder Entwickeln installieren konnte. Lediglich die Hardwareaustattung des PCs war und ist der limitierende Faktor.

VMware ist mit seinem Produkt VMware Workstation also ein Vertreter dieses Hypervisor-Typ-2-Virtualisierers. Ferner reiht sich der VMware Server 2.x in diese Riege ein oder auch VirtualBox von Sun.

- **Hardwarevirtualisierung**
  Die Hardware selbst bietet die Virtualisierungsfunktionen, z. B. die IBM-LPAR-Technik in Großrechnern.
- **Betriebssystem-Virtualisierung**
  Hier ist die Virtualisierungsschicht bereits im Betriebssystem eingebaut und kann so mehrere isoliert voneinander existierende Umgebungen erstellen. Aus Anwendungssicht werden komplette Betriebssysteme zur Verfügung gestellt.

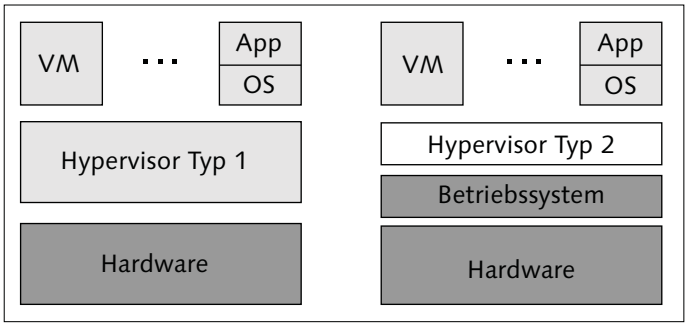


Abbildung 1.3 Ein Vergleich der Virtualisierungstypen: Bare-Metal- oder Typ-1-Hypervisor (links) und Hosted oder Typ-2-Hypervisor (rechts)

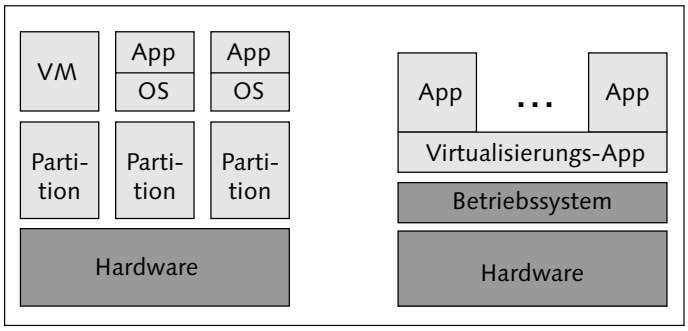


Abbildung 1.4 Fortsetzung des Vergleichs der Virtualisierungstypen: Hardware-Virtualisierung (links) und Betriebssystem (rechts)

1.1.6 Der Hypervisor genauer betrachtet

Der Hypervisor (Typ 1) ist das mittlerweile gängige Virtualisierungsmodell, und da auch vSphere von diesem Typ ist, werden wir ihn kurz vorstellen.

Der Hypervisor bringt ein eigenes schlankes Betriebssystem mit, das für den Einsatzzweck der Virtualisierung optimiert wurde. In diesem Betriebssystem werden die Hardwaretreiber eingebunden. VMware geht hier recht restriktiv vor und bietet ein vordefiniertes Paket an Treibern an, die im Betriebssystem installiert werden können. Microsoft hingegen geht einen anderen Weg, den Hypervisor zu implementieren, und im Zuge dessen werden alle Treiber, die für Windows Server 2008 R2 existieren, für den Einsatz in Microsofts Hypervisor, genannt *Hyper-V*, einsetzbar.

1.1.7 Die Entwicklungsgeschichte der Virtualisierung

Virtualisierung ist an sich nichts Neues, es ist im Unix- oder Großrechnerbereich schon seit Jahren Standard. In der PC-Welt sah es jedoch anders aus – wild wachsende PC- und Server-Umgebungen mit Verschwendung von Hardwareressourcen waren leider normal. In dieser Intel-Welt begann alles im Jahre 1999 mit einem einfachen Produkt, auf das jeder IT-Administrator und Softwareentwickler gewartet hatte: VMware Workstation wurde veröffentlicht. Ursprünglich waren virtualisierte Systeme eher für Test- und Entwicklungsumgebungen gedacht. Doch mit immer leistungsfähigerer Hardware und auch immer besser werdender Virtualisierungssoftware weitete sich das Feld auf Produktionsumgebungen aus.

Die VMware Workstation gehörte damals zur ersten Generation der Virtualisierer und stellte lediglich die virtuelle Hardware bereit. Hinzu gesellten sich im Jahre 2001 die ersten Versionen von VMware GSX (später in »VMware Server« umbenannt), ebenfalls ein Vertreter der Hypervisor-Typ-2-Virtualisierer, und VMware ESX Server (heute als »vSphere« bekannt) als Vertreter des Hypervisors vom Typ 1.

Im Jahre 2003 läutete VMware die zweite Generation ein: Features zur zentralen Administration von Virtualisierungsumgebungen hielten Einzug; das VMware Virtual Center wurde geboren, um immer größer werdende Virtualisierungslandschaften zentral zu verwalten. In diesem Jahr kaufte Microsoft den Virtualisierungspionier Connectix auf, der bereits zwei Jahre vor VMware ein Hypervisor-Typ-2-basiertes Produkt für Apple-Produkte auf den Markt gebracht hatte und erst später für die Intel-Welt einen Virtualisierer lieferte. Kurz darauf versuchte Microsoft, in diesem immer größer werdenden Markt mit dem Virtual Server 2005 mitzuspielen. Als direkte Konkurrenz zu VMwares Workstation brachte Microsoft die kleinere Variante Virtual PC ins Rennen.

Die dritte Generation der Virtualisierungsprodukte hat in den letzten drei Jahren den Anspruch erhoben, die komplette Infrastruktur zu virtualisieren, die Verfügbarkeit der Systeme zu erhöhen und die Automatisierung von Provisioning oder Betriebsprozessen zu ermöglichen. VMware Virtual Infrastructure 3.x war hier der Vorreiter, und Microsoft versuchte im Jahre 2008, mit dem komplett neu entwickelten Produkt Hyper-V – für Microsoft erstmals auch ein Typ-1-Hypervisor – auch in diesen Bereich vorzustoßen. Im Jahre 2009 legte VMware mit vSphere die aktuelle und fortschrittlichste Lösung vor. Microsoft zog zwar im Oktober 2009 mit dem Hyper-V R2 nach, doch vom Funktionsumfang her bewegt er sich auf dem Niveau von VMware VI3.5. Es bleibt abzuwarten, wie sich Microsoft mit seinem Hyper-V-Nachfolger und auch mit dem System Center Virtual Machine Manager 2012 gegenüber VMware vSphere positionieren wird.

1.2 Die VMware-Produktfamilie

Die Produktfamilie von VMware ist in den letzten Jahren stetig gewachsen. Da wir uns in diesem Buch auf vSphere beschränken, möchte ich nur kurz die Hypervisor-Produkte von VMware vorstellen.

VMware Workstation

VMwares erstes Produkt und Begründer des Siegeszugs von VMware ist VMware Workstation. Dieser Hypervisor vom Typ 2 wurde 1999 auf den Markt gebracht und setzt auf einem Träger-Betriebssystem auf. In der Regel findet sich dieses kostenpflichtige Produkt auf Desktop-PCs wieder; es ist für Windows und Linux verfügbar. Es ist die ideale Anwendung, um Software und Betriebssysteme zu testen. Auch Softwareentwickler setzen es gerne ein, um die Anwendungen auf unterschiedlichen Systemen oder auch nur auf einem Rechner ohne Entwicklungsumgebung zu testen. VMware Workstation ist zurzeit in der Version 8 erhältlich.

Mit VMware Workstation haben Sie einen Virtualisierer für 32- und 64-Bit-Gastbetriebssysteme von Microsoft inklusive Windows 2008 R2 und Windows 7 sowie für OS X, Linux, Solaris x86 oder auch NetWare.

Neben der Core-Four-Hardware haben Sie Unterstützung für USB-2.0-Geräte in der virtuellen Maschine. Ihre virtuellen Netzwerkkarten konfigurieren Sie so, dass sie entweder nur auf dem Host (z. B. Ihrem PC) verfügbar sind, als Netzwerkkarten zum physischen Netzwerkkabel durchgereicht werden (*bridged*) oder via NAT mit der physischen Hardware verbunden werden. Um kurzfristig Ressourcen auf Ihrem PC zu schaffen oder Ihre Arbeit für den Tag zu beenden, können Sie eine virtuelle Maschine anhalten, um diese später wieder innerhalb weniger Sekunden zu aktivieren.

Auch die Snapshot-Technologie unterstützt Sie dabei, zu verschiedenen Zeitpunkten den aktuellen Stand Ihres Gastbetriebssystems abzuspeichern, um nach Tests oder im Fehlerfalle im Gast wieder zu einem bestimmten Punkt zurückzuspringen. VMware Workstation erledigt das Erstellen der Snapshots auf Wunsch automatisch für Sie.

Für Softwareentwickler gibt es eine Integration in Microsofts Visual Studio, in die Eclipse-Entwicklungsumgebung und in die SpringSource Tools. Zum Datenaustausch können Sie über die Shared Folders Laufwerke vom Gast zum Host nutzen oder auch via Drag & Drop Dateien kopieren. Ebenso können Sie durch den integrierten Converter Ihren PC oder ein Betriebssystem-Image der Hersteller Symantec oder Acronis oder eine andere virtuelle Maschine von VMware oder Microsoft in Ihre VMware Workstation übertragen.

VMware Player

Der kostenfreie VMware Player ist, wie der Name schon sagt, eine reine Laufzeitumgebung für virtuelle Maschinen. Sie können damit virtuelle Maschinen erstellen und betreiben und das Gastbetriebssystem nutzen. Features wie Snapshots, Clones, Integration in Entwicklungsumgebungen u. a. sind nur in VMware Workstation enthalten.

VMware Fusion

VMware Fusion ist der kostenpflichtige Virtualisierer für Apples Mac-Rechner und zurzeit in der Version 4 auf dem Markt. Im Großen und Ganzen entsprechen die Features der Mac-Lösung dem Produkt VMware Workstation.

VMware vSphere Hypervisor (ESXi)

VMware vSphere Hypervisor ist der kostenfreie Virtualisierer auf Basis des ESXi-Servers und bietet Ihnen die Grundfunktionen von ESXi.

Sie verwalten den Server mit dem kostenfreien vSphere-Client, indem Sie sich damit direkt auf den ESXi-Host verbinden. Alternativ können Sie auch VMwares Kommandozeile, das vSphere Command Line Interface (vCLI), dazu verwenden. Dabei werden allerdings keine Konfigurationsänderungen beim freien ESXi unterstützt. Sollten Sie zur Verwaltung den vCenter Server einsetzen wollen, so müssen Sie auf eine kostenpflichtige Variante aktualisieren. Falls Sie sich zu einem späteren Zeitpunkt entschließen, Ihren Virtualisierer intensiver zu nutzen, können Sie ohne Neuinstallation den bestehenden ESXi-Server zu einer kostenpflichtigen vSphere Edition upgraden und Ihr virtuelles Rechenzentrum ausbauen.

VMware vSphere

VMware vSphere – das Flaggschiff in der Produktpalette von VMware und zurzeit am Markt die unangefochtene Nummer eins der Hypervisor-Typ-1-Virtualisierer – besteht aus einer Vielzahl von Komponenten und lässt sich für verschiedene Einsatzgebiete mit weiteren VMware-Produkten erweitern oder kombinieren, um dem Einsatz in Enterprise-Umgebungen gerecht zu werden.

1.3 Einführung in VMware vSphere

VMware vSphere setzt sich aus mehreren Features und Produkten zusammen, die je nach Edition im Paket enthalten sind. VMware unterteilt die Features und Produkte in verschiedene Bereiche, und daher möchten wir im Wesentlichen diese Gruppierung zur besseren Übersichtlichkeit hier ebenso verwenden.

Zu allen hier genannten Features finden Sie in nachfolgenden Kapiteln ausführliche Informationen.

1.3.1 VMware ESXi

Der VMware ESXi Server ist der zentrale Bestandteil der vSphere-Landschaft – nämlich der Hypervisor-Typ-1-basierte (Bare-Metal-) Virtualisierer. Der ESXi Server verwaltet die Hardwareressourcen und kümmert sich um deren Verteilung an die virtuellen Maschinen. Ausgereifte Techniken zur Speicherzuweisung mit der Möglichkeit, mehr Speicher an virtuelle Maschinen zu vergeben als physisch vorhanden (Memory-Overcommitment), und zur Zuteilung von CPU-Ressourcen (CPU Scheduler) bieten den virtuellen Maschinen höchstmögliche Performance.

1.3.2 VMware vCenter Server

Der vCenter Server ist das Werkzeug, um die virtuelle Infrastruktur von zentraler Stelle aus zu verwalten. Mit diesem Werkzeug arbeiten Sie an den virtuellen Maschinen, verwalten die ESXi-Server, überprüfen diese mit Host-Profilen, erstellen Rechtestrukturen, um die Verwaltung der Umgebung an weitere Administratoren zu vergeben, starten vMotion-Vorgänge, konfigurieren die Hochverfügbarkeit (HA), Ausfallsicherheit einzelner virtueller Maschinen (FT) und Last-Verteilung (DRS) und vieles mehr.

1.3.3 VMware vSphere-Client und VMware vSphere Web Client

Der vSphere-Client ist eine Windows-Anwendung, die Ihnen den Zugang entweder zum vCenter-Server oder zu einem ESXi-Server bietet. Er ist ihr tägliches Werkzeug zur Verwaltung der virtuellen Infrastruktur. Der Web Client bietet die gleiche Funktionalität über den Browser.

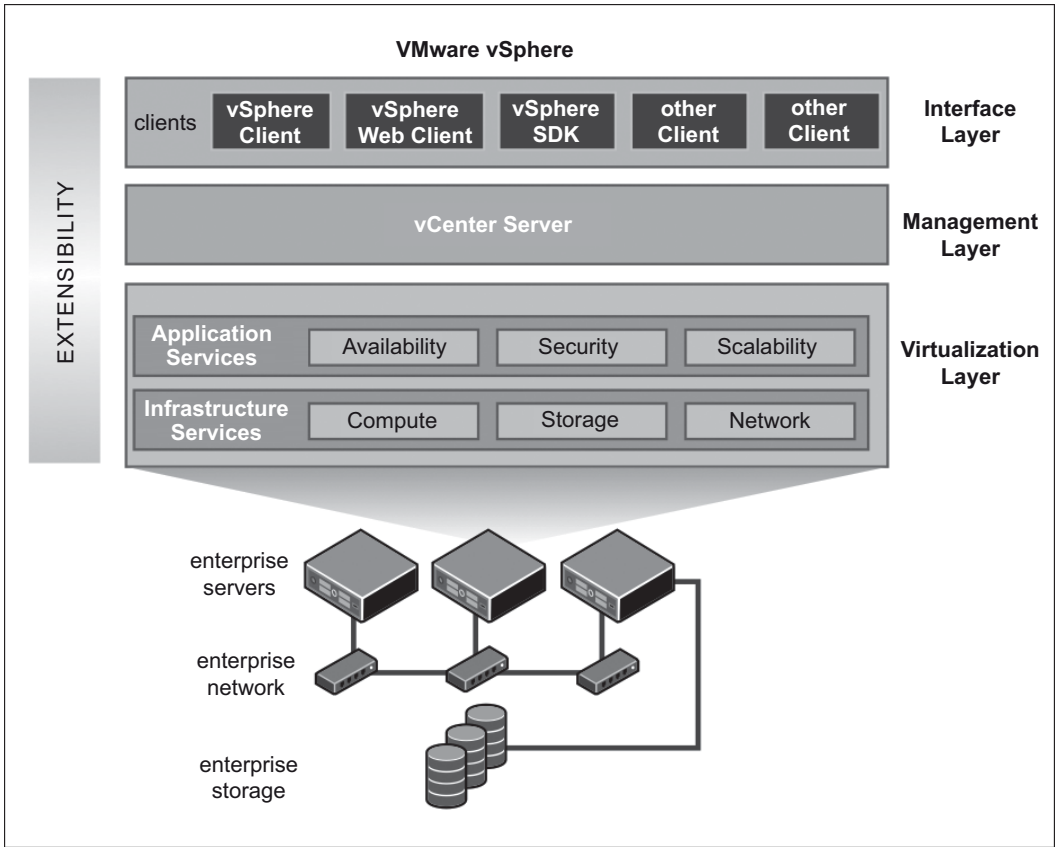


Abbildung 1.5 Die verschiedenen Ebenen in vSphere

1.3.4 VMware vSMP (Virtual Symmetric Multi Processing)

Dieses Feature erlaubt der virtuellen Maschine die Zuweisung von mehr als einer CPU.

1.3.5 vSphere Virtual Machine File System (VMFS)

Das von VMware entwickelte Festplattenformat ist speziell für den Betrieb in ESXi-Umgebungen ausgelegt und bietet bei einer Verzeichnisebene maximale Performance für sehr große Dateien zur Ablage der VM-Dateien.

1.3.6 Thin Provisioning

Durch Thin Provisioning können Sie virtuelle Maschinen erstellen, ohne dass diese von Anfang an den konfigurierten Speicherplatz für die virtuellen Festplatten in Anspruch nehmen.

1.3.7 vSphere Fault Tolerance

Hat der Ausfall eines ESXi-Servers auch mit vSphere HA durch den ungeplanten Ausfall von virtuellen Maschinen die Anwender samt ihren Applikationen verärgert, so können Sie mit dem Feature VMware FT Paroli bieten. Hierbei werden virtuelle Maschinen auf ESXi-Servern in einem HA-Cluster per Mausklick abgesichert, indem die komplette virtuelle Maschine inklusive des Speicherinhalts ständig auf einen anderen ESXi-Server repliziert wird. Fällt die primäre virtuelle Maschine aus, so steht das Gastbetriebssystem dennoch ununterbrochen zur Verfügung.

1.3.8 vSphere vMotion und Storage vMotion

Die VMware-vMotion-Technologie ermöglicht das Verschieben von aktiven virtuellen Maschinen von einem ESXi-Host auf einen anderen. Die Voraussetzung hierfür ist die Ablage der Dateien einer virtuellen Maschine auf einem Shared Storage (SAN, NAS, NFS), auf den beide ESXi-Hosts Zugriff haben. Somit können Sie ESX-Server im laufenden Betrieb aktualisieren und neu starten, indem Sie vorher alle aktiven virtuellen Maschinen auf andere ESXi-Hosts verschieben. Durch Storage vMotion können Sie aktive virtuelle Maschinen ohne Ausfall auch auf einen anderen Datastore, d. h. eine andere Speichereinheit in der vSphere-Umgebung, verschieben.

1.3.9 vSphere High Availability (HA)

Bei einem Ausfall eines ESXi-Servers kann vSphere HA die auf diesem ESXi-Server aktiv gewesenen virtuellen Maschinen auf anderen ESXi-Servern in einem VMware-HA-Cluster-Verbund automatisch neu starten. Die Applikationen innerhalb der virtuellen Maschinen werden ebenso neu gestartet, was Auswirkungen auf die Anwender haben kann.

1.3.10 vSphere Distributed Resource Scheduling (DRS)

DRS kann nur in Verbindung mit dem vCenter Server genutzt werden und bietet die Möglichkeit, die virtuellen Maschinen nach verschiedenen Kriterien auf den in einem DRS-Cluster zusammengefassten ESXi-Servern zu verteilen. Dies kann vollautomatisiert, halbautomatisiert oder rein administrator-induziert geschehen. VMware erreicht dadurch eine dynamische Lastverteilung auf den ESXi-Servern.

1.3.11 vSphere Distributed Power Management (DPM)

VMware DPM ist ein Bestandteil von VMware DRS und trägt der Green IT Rechnung, da je nach Auslastung der ESXi-Server im Cluster-Verbund die virtuellen Maschinen im laufenden Betrieb unterbrechungsfrei so verschoben werden, dass dadurch einzelne ESXi-Server komplett lastfrei werden, um diese dann in den Stromsparmodus zu schicken. Fordert die virtuelle

Infrastruktur wieder mehr Ressourcen, so können diese ESXi-Hosts wieder aus dem Schlaf erweckt und die virtuellen Maschinen vollautomatisiert wieder auf alle ESX-Server im Cluster verteilt werden.

1.3.12 vSphere Storage DRS

Was vSphere DRS für CPU- und Memory eines ESXi-Servers darstellt, ist vSphere Storage DRS für die Datastores. Mit Hilfe dieses Features wird die Speicherausnutzung und Speicherperformance innerhalb der Datastores eines Clusters balanciert. Dabei werden mit Hilfe von Storage vMotion die virtuellen Maschinen auf andere Datastores verschoben, um den Lastenausgleich zu erreichen.

1.3.13 vSphere Standard Switches, Distributed Switches (dvSwitch, vDS) und Port Groups

Der vSphere Standard Switch und der vSphere Distributed Switch sind rein auf Software basierende Netzwerk-Switches, um die virtuellen Maschinen mit Netzwerk zu versorgen. Dabei ist der Standard Switch auf jeweils einen ESXi-Host beschränkt und muss daher pro ESXi-Host einzeln verwaltet werden.

Ein vSphere Distributed Switch vDS verteilt die Netzwerkkonfiguration eines ESXi-Hosts auf mehrere ESXi-Hosts im VMware-Datacenter. Dadurch reduziert sich die Verwaltung der Netzwerkkonfiguration erheblich, da diese nur noch einmal erfolgen muss und nicht für jeden ESXi-Host einzeln.

Damit vMotion und Storage vMotion funktionieren, muss auf jedem ESXi-Host eine identische Netzwerkkonfiguration vorliegen, so dass sich die virtuellen Maschinen mit den gleichnamigen virtuellen Switches und Port Groups verbinden können, um über die gleichen physischen Netzwerke mit der Außenwelt zu kommunizieren.

Die Port Groups sind eine Untermenge der virtuellen Switches und bieten auf den Ports eine jeweils identische Netzwerkkonfiguration. Insbesondere richtet man die Port Groups ein, um benötigte Subnetze entweder nativ, also ohne vLAN-Tag, oder als vLAN an die virtuellen Maschinen zu bringen. Weitere Einstellungen wie Sicherheitseinstellungen (z. B. ob an den Ports der Promiscuous Mode erlaubt ist) oder auch Teaming- und Failover-Konfigurationen werden jedoch auf Ebene der Port Groups getroffen.

1.3.14 Storage I/O Control & Network I/O Control

Mit Hilfe von Storage I/O Control können Administratoren Prioritäten und Limitierungen bei I/O-Operationen von virtuellen Maschinen auf Datastores vergeben. Dadurch ist für VMs sichergestellt, dass der Zugriff auf den Speicher mit der benötigten Priorität stattfindet. Das Gleiche gilt für Network I/O Control, nur eben für die physische Netzwerkkarte.

1.3.15 Profile Driven Storage

Das seit vSphere 5 neue Feature Profile Driven Storage ermöglicht mittels der vom SAN-System kommenden Speicher-Systeminformationen und der vom Administrator konfigurierbaren VM-Speicherprofilen, einzelnen virtuellen Maschinen den Festplattenspeicher aus dem SAN zuzuweisen, der auch die benötigten Eigenschaften und Leistungsmöglichkeiten bietet, die diese VM zum performanten Betrieb benötigt.

1.3.16 Host-Profiles

Mit Hilfe von Host-Profiles standardisieren Sie Ihre ESXi-Server, indem Sie bei deren Konfiguration und Verwaltung eine Vorlage mit Ihren Systemen vergleichen und gegebenenfalls die ESXi-Server analog zur Vorlage konfigurieren lassen. Diese Vorlage, das Profil, erstellen Sie von einer Standard-ESXi-Konfiguration.

1.3.17 VMware vShield Zones

Die VMware vShield Zones integrieren sich in die vSphere-Netzwerke, um zusätzliche Sicherheit in Form von Firewall-Funktionalität in die virtuelle Infrastruktur zu bringen. Dadurch erhalten die vSphere-Administratoren Einblick und Verwaltungsmöglichkeiten für den Netzwerkverkehr der virtuellen Switches in der vSphere-Umgebung

1.3.18 vSphere Update Manager (VUM)

Der vSphere vCenter Update Manager ist VMwares Lösung, um die ESXi-Server einer vSphere-Umgebung automatisiert mit Patches zu versehen. Dabei überprüft der Update Manager, ob neue Patches verfügbar sind, lädt diese von der VMware-Internetseite und legt sie in einem konfigurierten Verzeichnis ab. Durch Scan-Vorgänge verschafft sich der Update Manager einen Überblick über den Softwarestand aller ESXi-Server und vergleicht diesen dann mit den verfügbaren Patches. Per Mausklick können Sie die ESXi-Server mit einem von Ihnen definierten Patch-Stand versehen, und der Update Manager instruiert VMware DRS, alle aktiven virtuellen Maschinen eines ESXi-Servers auf andere ESXi-Server zu verschieben, bevor die Patches auf dem ESXi-Server installiert werden.

1.3.19 VMware vCenter Orchestrator

Der VMware vCenter Orchestrator ist kostenlos bei VMware erhältlich und unterstützt die Automatisierung von Workflows, d. h. nahezu alle Vorgänge rund um virtuelle Maschinen.

1.3.20 VMware Data Recovery

VMware Data Recovery bietet Ihnen einen zentralen Ansatz zum Backup oder Restore Ihrer virtuellen Maschinen über den VMware vCenter Server. Durch die Integration in vCenter ist

der VMware-eigenen Backup-Lösung auch bekannt, auf welchem ESXi-Host sich die virtuellen Maschinen befinden.

1.3.21 VMware vCenter Server Heartbeat

Die Erweiterung zum vCenter Server, die auch diesen Teil der virtuellen Infrastruktur hochverfügbar gestaltet, nennt sich vCenter Server Heartbeat und repliziert einen aktiven vCenter-Server, um bei einem Ausfall des primären vCenter-Servers auf die Replik umzuschalten.

1.3.22 VMware Server Linked Mode

Der Linked Mode ist ein Zusatzprodukt und unterstützt die Skalierbarkeit Ihrer vSphere-Umgebung durch die Verbindung mehrerer vCenter-Server. Dabei werden die Benutzerrollen und Rechte sowie die Lizenzen zwischen den verbundenen vCenter-Servern repliziert, damit Sie in allen vCenter-Servern arbeiten können.

1.3.23 VMware vSphere SDKs

VMware bietet eine Reihe von Software Development Kits (SDKs), um eine vSphere-Umgebung per Skript oder Kommandozeile zu steuern.

- **vSphere PowerCLI**
  Das PowerCLI ist eine Sammlung von Commandlets für Microsofts PowerShell. Mit Hilfe dieser Erweiterungen können Sie über PowerShell-Skripte eine komplette vSphere-Umgebung in all ihren Aspekten automatisieren.
- **vSphere SDK for Perl**
  Das SDK für Perl bietet ein clientseitiges Scripting-Interface für die vSphere Web Services API.
- **vSphere CLI (vCLI)**
  Das vSphere CLI ist eine Sammlung von Kommandozeilen-Tools zur Verwaltung von vCenter- und ESXi-Servern. Speziell für die Administration von ESXi-Servern sind diese Tools sinnvoll, da der ESXi-Server keine Service Console zum Management des Hosts mitbringt.

vSphere SDK for .NET

Das vSphere SDK for .NET bietet für .NET-basierte Programmiersprachen wie z. B. C# den Zugang zur vSphere API und gehört zur vSphere PowerCLI. Damit lassen sich Anwendungen schreiben, um vSphere-Inventarobjekte zu verwalten.

- **VMware vSphere Web Services SDK**
  Dieses SDK bietet Ihnen über Web Services eine API, um mit Programmiersprachen wie C# oder Java Anwendungen zu schreiben, die Ihre vSphere-Umgebung um Funktionen erweitern, und so z. B. auch eigene Plugins für den vSphere-Client zu erstellen.

- **VMware vSphere Management Assistant**
  Der vSphere Management Assistant ist eine virtuelle Appliance auf Basis von Linux, die mit dem vSphere vCLI und einigen weiteren Modulen für Authentication und Logging versehen ist. Mit Hilfe dieser VM können Administratoren ihre vSphere-Umgebung mit Skripten verwalten.

1.3.24 Die verfügbaren VMware-Editionen

VMware bietet in der Reihe »VMware vSphere for Enterprises« verschiedenen Editionen an; diese unterscheiden sich in den enthaltenen Features und in der maximal unterstützten ESXi-Hardware – d. h. maximale Cores pro CPU und maximal adressierbarer Speicher im ESXi-Host. Des Weiteren unterscheiden sich die Editionen in den maximal den virtuellen Maschinen zur Verfügung stehenden virtuellen CPUs.

Standard Edition

- pro Lizenz maximal 32 GByte Speicher für virtuelle Maschinen adressierbar
- maximal 8 virtuelle CPUs pro virtueller Maschine
- Features:
  - Thin Provisioning
  - Update Manager
  - Data Recovery
  - HA (High Availability)
  - vMotion
  - vStorage-APIs for Data Protection

Enterprise Edition

- pro Lizenz maximal 64 GByte Speicher für virtuelle Maschinen adressierbar
- maximal 8 virtuelle CPUs pro virtueller Maschine
- Features:
  - Thin Provisioning
  - Update Manager
  - Data Recovery
  - HA (High Availability)
  - vMotion
  - vStorage-APIs for Data Protection
  - Virtual Serial Port Concentrator

- Hot Add
- FT (Fault Tolerance)
- vShield Zones
- Storage vMotion
- Storage-APIs for Multipathing
- Storage-APIs for Array Integration
- DRS & DPM (Distributed Resource Scheduling & Distributed Power Management)

Enterprise Plus Edition

- pro Lizenz maximal 96 GByte Speicher für virtuelle Maschinen adressierbar
- maximal 32 virtuelle CPUs pro virtueller Maschine
- Features:
  - Thin Provisioning
  - Update Manager
  - Data Recovery
  - HA (High Availability)
  - vMotion
  - vStorage-APIs for Data Protection
  - Virtual Serial Port Concentrator
  - Hot Add
  - FT (Fault Tolerance)
  - vShield Zones
  - Storage vMotion
  - Storage-APIs for Multipathing
  - Storage-APIs for Array Integration
  - DRS & DPM (Distributed Resource Scheduling & Distributed Power Management)
  - Storage I/O Control
  - Network I/O Control
  - Distributed Switch
  - Host-Profiles
  - Auto Deploy
  - Storage DRS
  - Profile Driven Storage

Zusätzlich hat VMware eine Reihe für kleinere Unternehmen geschaffen, »VMware vSphere for SMBs«, die sich in Essential Kits und Acceleration Kits unterscheidet. Die Idee hierbei ist, dass in einem Kit alles Notwendige an Software und Lizenzen enthalten ist, um kleine virtuelle Rechenzentralen aufzubauen. Hier unterscheiden sich die Versionen in der maximalen Hardwareaustattung eines ESXi-Servers und in den bereitgestellten Features. Das Einstiegspaket Essential Kit gilt z. B. für maximal drei ESXi-Server, die mit maximal zwei CPUs ausgestattet sind und in Summe nicht mehr als 192 GB vRAM anbieten. Für dieses Kit kann der Support auf Call-Basis eingekauft werden. Weitere Kits bieten mehr Hardwareausstattung, umfassen Support und bringen einige VMware-Produkte zur Verwaltung, Überwachung, Backup etc. der Umgebung bereits mit.

Das folgende Kapitel beschäftigt sich mit dem strukturellen Aufbau einer virtuellen Infrastruktur. Wir gehen den Fragen nach, welche Elemente dazugehören, wie sie ineinandergreifen und wie sie aufgebaut sind.

2 vSphere-Architektur

Autor dieses Kapitels ist Bertram Wöhrmann, Ligarion, bwoehrmann@ligarion.de

Mit der Einführung der VMware Virtual Infrastructure in der Version 3.x vollzog VMware einen Strategiewechsel. Zusätzlich zu der eigentlichen Virtualisierungsplattform, dem ESX Server, und dem dazugehörigen Management begann VMware, zusätzlich Produkte um die Virtualisierung zu entwickeln. Es fing an mit der Service-Console-losen Version ESXi und dem Update Manager, vSphere HA, VMware DRS und der Plugin-Schnittstelle. Alles integrierte sich nahtlos in das zentrale Management. Mit vSphere 4.0 wurde dieser Ansatz konsequent weiterverfolgt. Auch der Lizenz-Server ist, nach einer kurzen externen Stippvisite, wieder integraler Bestandteil des vCenter Servers. Mit der neuen Version ESXi 5.0 hat sich dieser Trend weiter fortgesetzt. Die offensichtlichste Änderung ist der Wegfall der Variante ESX mit der Service Console. Aber auch um den Hypervisor herum finden Sie viele neue Produkte, die Ihre Arbeit unterstützen und erleichtern sollen.

Viele Themen reißen wir in diesem Kapitel nur kurz an. Wir sind der Meinung, dass es sinnvoller ist, die ausführlichen Erklärungen direkt in dem entsprechenden Abschnitt zu geben, in dem wir auch die passende Komponente beschreiben.

2.1 Bestandteile der virtuellen Infrastruktur

Die vSphere-Infrastruktur bietet alle Komponenten zum Virtualisieren von Betriebssystemen. Sie umfasst die Verwaltung sowie das Management der Virtualisierungs-Server (vSphere-Server). Diese Grundfunktionen hat VMware noch weiter optimiert, um eine Ausfallsicherheit der Virtualisierungs-Server zu erreichen (HA) und eine bestmögliche Lastverteilung zwischen den Virtualisierungs-Servern (DRS) zu ermöglichen. Des Weiteren werden die virtualisierten Systeme optimal mit den Server-Ressourcen (CPU, RAM etc.) versorgt. Damit Sie einen grundlegenden Überblick über die Grundbestandteile der Infrastruktur erhalten, erläutern wir diese nachfolgend.

2.2 vSphere-Host

Der physische Server, der seine Ressourcen wie CPU, Hauptspeicher (RAM), Netzwerkkarten und Festplattenspeicher über eine Virtualisierungsschicht (Hypervisor) den virtuellen Maschinen zur Verfügung stellt, ist der *vSphere-Host*. Viele werden den Vorgängernamen des vSphere-Hosts noch im Kopf haben, nämlich die Bezeichnung »ESX-Host« (Abbildung 2.1). Trotz der Namensänderung mit der Version 4.x hält sich hartnäckig der alte Name.

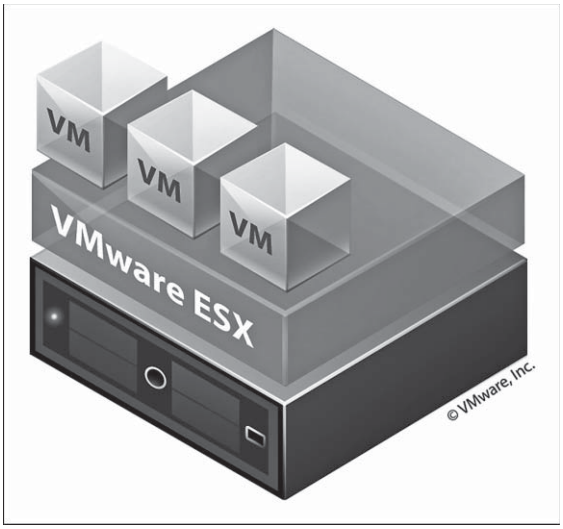


Abbildung 2.1 vSphere-Host

2.2.1 Hardware

Als Prozessorbasis für den Einsatz von VMware vSphere kommen nur 64-Bit-x86-Prozessoren zum Einsatz. Auf anderen CPUs ist das System nicht lauffähig, da der VMkernel einen 64-Bit-Kernel besitzt. Für die Installation benötigen Sie mindestens eine CPU und Minimum 2.048 MB Arbeitsspeicher. Des Weiteren ist ein unterstützter Storage-Controller nötig. Möglich sind SCSI, SAS, SATA und Fibre-Channel. Abschließend wird noch mindestens eine Netzwerkkarte benötigt, damit Sie auf das System zugreifen können. Im Normalfall werden aber wohl mehr Netzwerkports zum Einsatz kommen.

Intel VT-x/AMD-V

Alle Prozessoren, für die VMware Support anbietet, müssen eine Erweiterung zur Unterstützung von Virtualisierungstechnologien aufweisen. Durch diese Technologien wird im Wesentlichen der Virtual Machine Monitor (VMM) in seiner Arbeit unterstützt, dadurch wird der Overhead reduziert. Auch der Prozess der Migration einer aktiven virtuellen Maschine zwischen verschiedenen Prozessorgenerationen wird erleichtert.

Die unterstützten CPUs von beiden Herstellern bringen eine solche Technologie mit. Die folgenden Prozessoren erhalten Support von VMware:

- AMD Opteron (mindestens Barcelona für Fault Tolerance)
- Intel Xeon 3000/3200, 3100/3300, 5100/5300, 5200/5400, 7100/7300, 7200/7400, 7500

2.2.2 HCL

Wie andere Betriebssystemhersteller bzw. Hersteller von Hypervisoren pflegt die Firma VMware eine Hardware Compatibility List (HCL). Vergewissern Sie sich, dass Ihre Komponenten, die Sie einsetzen wollen, in dieser Liste aufgeführt sind. Sie müssen zwar keine Bedenken haben, dass ein nicht gelistetes System nicht funktionieren kann, aber Sie haben nur Support für Ihre Virtualisierungslandschaft, wenn Sie sich aus der Liste der unterstützten Hardware bedienen.

Die HCL finden Sie unter: *http://www.vmware.com/resources/compatibility/search.php*.

2.2.3 Maximale Ausstattung eines ESXi-Hosts

Auch wenn Sie sich an die HCL halten, so müssen Sie doch wissen, welche Ausstattung des Hosts mengenmäßig noch unterstützt wird. Diesen Punkt möchten wir in den folgenden Tabellen näher aufschlüsseln.

CPUs pro Host	Anzahl	Bemerkungen
logische Prozessoren	160	Die Anzahl berechnet sich aus: Sockel × Cores × Threads
virtuelle CPUs (vCPUs)	2.048	–
maximale Anzahl von virtuellen CPUs, pro Core	25	Die Anzahl ist abhängig von der Last, die die VMs verursachen. (Gilt ebenfalls für vSphere 4.0 Update 1, bei vSphere 4.0 sind es 20 vCPUs.)
maximale Anzahl von VMs pro Host	512	Die Anzahl ist abhängig von der Last, die die VMs verursachen.

Tabelle 2.1 Maximale CPU-Werte

Memory pro Host	Menge
Arbeitsspeicher	2 TB

Tabelle 2.2 Maximaler Memory-Wert

Anhand der Menge der Karten geben wir in den Tabellen für die Netzwerkkarten nur den Treiber und den Chiphersteller an.

Netzwerkkarte	Chiphersteller	Speed	Anzahl
e1000 tg3	Intel Broadcom	1 GBit	32
e1000e	Intel	1 GBit	24
igb bnx2	Intel Broadcom	1 GBit	16
forcedeth	Nvidia	1 GBit	2
be2net nx_nic	Emulex NetXen	10 GBit	8
ixgbe bnx2x	Intel Broadcom	10 GBit	8
Kombination 10GBit und 1 GBit	–	1 GBit 10 GBit	4 6

Tabelle 2.3 Maximale Anzahl physischer Netzwerkkarten

PCI VMDirectPath	Anzahl
PCI VMDirectPath Devices (pro Host)	8
PCI VMDirectPath Devices (pro VM)	4
vNetzwerk-Standard-Switch	**Anzahl**
virtuelle Switch-Ports pro vSwitch	4.088
Portgruppen pro vSwitch	256
Portgruppen pro vCenter	5.000
vNetzwerk Distributed Switch	**Anzahl**
virtuelle Switch-Ports gesamt	30.000
Hosts pro Switch	350
VDS pro vCenter	32
vNetzwerk	**Anzahl**
Maximal aktive Ports pro Host	1.016
virtuelle Switch-Ports gesamt	4.096

Tabelle 2.4 Maximale Anzahl virtueller Karten/Ports

Parallele vMotion Operationen pro Host	Anzahl
1-GBit-Netzwerk	4
10-GBit-Netzwerk	8

Tabelle 2.5 Maximale Anzahl von parallelen vMotion-Operatoren

Für den Storage gibt es ebenfalls Einschränkungen. Tabelle 2.6 trennt die verschiedenen Anbindungsmöglichkeiten voneinander und beschreibt außerdem das File-System VMFS.

VMFS allgemein	Maximalwert
Volume-Größe	64 TB
vDisk pro Host	2.048
Volumes per Hosts	256
Hosts pro Volume	64
VMFS-3	**Maximalwert**
Files pro Volume	~30.270
File-Größe	256 MB – 2TB – 512 Bytes
Blockgröße	1 MB / 2 MB / 4 MB / 8 MB
RDM-Größe (virtuelle Kompatibilität)	2 TB – 512 Bytes
RDM-Größe (physische Kompatibilität)	2 TB – 512 Bytes
VMFS-5	**Maximalwert**
Files pro Volume	~130.690
File-Größe	2 TB – 512 Bytes
Blockgröße	1 MB; bei einer Migration von VMFS-3 wird die alte Blockgröße übernommen
RDM-Größe (virtuelle Kompatibilität)	2 TB – 512 Bytes
RDM-Größe (physische Kompatibilität)	64 TB
Fibre-Channel	**Maximalwert**
LUNs pro Host	256
Anzahl Pfade pro LUN	32
maximale Anzahl pro Host	1.024
HBAs pro Host	8
maximale Anzahl von HBA-Ports	16
FCoE	**Maximalwert**
Maximale Anzahl SW-Adapter	4
NFS	**Maximalwert**
maximale Anzahl von NFS-Datastores	256
Hardware-iSCSI-Initiators	**Maximalwert**
LUNs pro Host	256
Pfade pro Host	1.024
Pfade pro LUN	8
QLogic dynamische Targets pro Port statische Targets pro Port	 64 128
Broadcom Targets pro Port (1 GBit) Targets pro Port (10 GBit)	 64 62
Software-iSCSI-Initiators	**Maximalwert**
Ziele pro Host	256

Tabelle 2.6 Maximalwerte im Storage-Umfeld

2.3 vCenter-Server

Der vCenter-Server ist Dreh- und Angelpunkt der VMware-Infrastruktur. Mit ihm verwalten Sie das komplette VMware-Datacenter von der Konfiguration der ESXi-Server über das Erstellen von virtuellen Maschinen bis zum Einrichten der VMware-Features HA (High Availability) und DRS (Distributed Ressource Scheduling) sowie viele andere Funktionen. Des Weiteren bietet das vCenter eine Zugriffskontrolle auf Basis von Benutzern und Gruppen. Performancedaten der vSphere-Server sowie der virtuellen Maschinen werden ebenfalls gesammelt und in der Datenbank abgelegt.

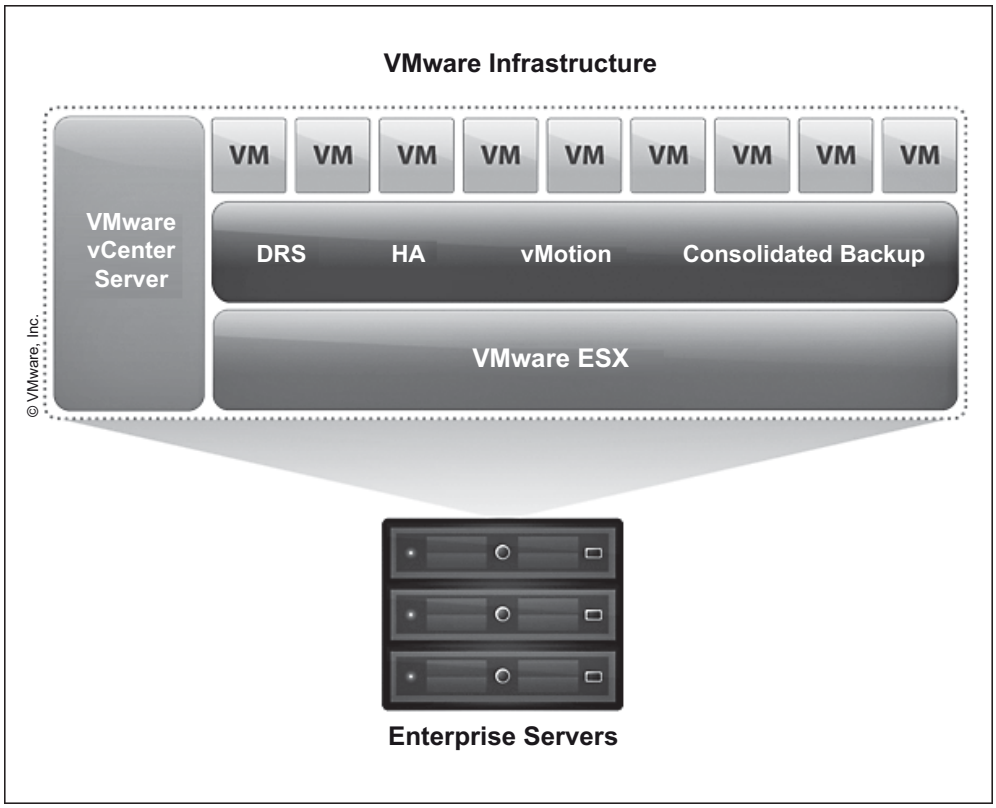


Abbildung 2.2 Struktur des vCenter-Servers

Der vCenter-Server ist nicht zwingend notwendig zum Betreiben von vSphere-ESXi-Hosts, damit diese die Dienste bereitstellen können, um virtuelle Maschinen zu erstellen. Sie können jeden Host einzeln und unabhängig voneinander verwalten. Einige Dienste aber, wie z. B. DRS, setzen zwingend einen vCenter-Server voraus.

Die Software bietet eine zentralisierte Verwaltung aller im VMware-Datacenter zusammengefassten Ressourcen, deren virtueller Maschinen sowie der Benutzer.

Die zentralen Dienste des vCenters sind:

- Provisionierung von virtuellen Maschinen
- Konfiguration von vSphere-Servern (Hosts) und virtuellen Maschinen (VMs)
- Konfiguration von Resource-Pools
- Inventarisierung von vSphere-Ressourcen und virtuellen Maschinen
- Konsolenzugang zu den virtuellen Maschinen
- Statistiken und Protokolle zur Ressourcenauslastung
- Alarm- und Event-Management, um VI-Administratoren über Events und erhöhte Auslastung zu informieren
- rollenbasiertes Rechtemodell, um Objektgruppen zu verwalten
- Task-Scheduler, um bestimmte Aktivitäten zu bestimmten Zeiten automatisiert auszuführen

Diese zentralen Dienste des vCenters können um bestimmte Features erweitert werden. Dabei dient das vCenter als zentrale Schnittstelle, in der Sie die zusätzlichen Dienste, *Distributed Services* genannt, verwalten. Die erweiterten Dienste sind:

- VMware DRS
- vSphere HA
- VMware Fault Tolerance
- VMware vMotion
- VMware Storage vMotion

Des Weiteren bieten der Management-Server sowie der vSphere-Client eine Schnittstelle für Plugins zur Erweiterung der Funktionalität:

- vCenter Configuration Manager
- vCenter Update Manager
- vCenter Orchestrator
- vCenter VASA
- Storage DRS
- Tools von Third-Party-Vendors oder auch Freewaretools

Editionen

Es gibt drei Versionen des vCenter Servers von VMware:

- vCenter Server for Essentials (maximal 3 Hosts mit zwei Sockeln und 192 GB vRAM)
- vCenter Server Foundation (maximal 3 Hosts)
- vCenter Server Standard

Wollen Sie ohne Einschränkungen arbeiten, dann müssen Sie mit der Standard-Version des vCenter Servers arbeiten. Bei kleineren Umgebungen können Sie auf die beiden anderen Versionen zurückgreifen. Ein späteres Upgrade von z. B. der Foundation- auf die Standard-Version ist nur eine Frage des Geldes.

Maximale Ausstattung

Auch das vCenter kann nicht unendlich viele Ressourcen verwalten; es gilt die eine oder andere Einschränkung. Die Angaben beziehen sich auf die Standard-Version des vCenter Servers.

vCenter Server Scalability – 64-Bit-OS-Server	Anzahl
Hosts	1.000
Powered-on VMs	10.000
Registered VMs	15.000
Concurrent vSphere-Client-Verbindungen	100

Tabelle 2.7 Verwaltbare Infrastruktur für das vCenter mit 64-Bit-OS-Server

vCenter Server Scalability – vCenter Linked Mode	Anzahl
Linked vCenter Server	10
Hosts im Linked Mode	3.000
Powered-on VMs	30.000
Registered VMs	50.000

Tabelle 2.8 Mögliche verwaltbare Infrastruktur für das vCenter im Linked Mode

vCenter Server Scalability – allgemein	Anzahl
Hosts pro Datacenter	500

Tabelle 2.9 vCenter – allgemeine Einschränkungen

Die Zahlen, die VMware hier ansetzt, sind an der einen oder anderen Stelle sicherlich sehr optimistisch gewählt. Sie sollen nur als Richtschnur dienen, damit Sie abschätzen können, wie viele Managementsysteme Sie benötigen.

Zugriff

Damit Sie die virtuelle Infrastruktur auch verwalten können, benötigen Sie ein Werkzeug, um auf die einzelnen Komponenten zuzugreifen. Hier haben Sie mehrere Möglichkeiten: Eine der Optionen ist die Nutzung eines Webbrowsers. Seien Sie sich dabei im Klaren darüber, dass Sie nicht alle Funktionen mit dem Webclient durchführen können. Außerdem ist der Webzugriff

von Haus aus deaktiviert. Die zweite Möglichkeit ist die Nutzung des vSphere-Clients. Mit diesem Client können Sie direkt einen Host administrieren oder sich damit am vCenter-Server anmelden. Eine weitere Option ist der Zugriff über das iPad. Auch hier gibt es Einschränkungen in der Funktionalität. Nicht alle Funktionen stehen über diesen Weg zur Verfügung.

Lizenzierung

Für die Verwaltung der VMware-Lizenzen in einer vSphere-Infrastruktur wird der im vCenter integrierte Lizenz-Server eingesetzt. In dieser Verwaltungskonsole tragen Sie alle VMware-Lizenzen ein und weisen sie den zugehörigen Hardwarekomponenten zu. Dieses gilt aber nicht für Hosts der Version 3.x, wie Sie im folgenden Absatz nachlesen können.

License Server 3.x

Soll ein vCenter-Server der aktuellen Version (5.x) auch ESXi 3.x-Hosts verwalten, so müssen Sie nach wie vor eine zusätzliche Komponente installieren. Es handelt sich um den alten Lizenz-Server, der schon in der Virtual Infrastructure 3 zum Einsatz kam. Dieser Lizenz-Server wird im Netzwerk bereitgestellt und in den vCenter-Eigenschaften konfiguriert.

VMware Infrastructure SDK

Es gibt die verschiedensten Möglichkeiten, in der virtuellen Infrastruktur Aufgaben zu automatisieren, auch außerhalb des vCenters und seiner Komponenten. Sie haben als Anwender verschiedene Optionen zur Verfügung, um eigene Anforderungen abzubilden. Dabei ist es egal, ob Sie mit der PowerShell skripten oder mit C programmieren möchten. Es gibt noch viele andere Möglichkeiten, das Management der Infrastruktur zu optimieren. Abbildung 2.3 zeigt nur eine Auswahl von Softwarepaketen, die VMware zur Verfügung stellt, damit Anwender das Management an ihre Bedürfnisse anpassen können.

Wenn Sie sich für alle Informationen interessieren, finden Sie auf der eigens dafür eingerichteten Webseite Näheres zu dem gewünschten Thema. Die Webseite erreichen Sie unter *http://www.vmware.com/support/pubs/sdk_pubs.html*, wo Sie auch die Applikationen herunterladen können.

Benötigte Netzwerkports – Implementierung

Das vCenter kommuniziert über das Netzwerk mit den zu verwaltenden Komponenten. Die Verbindungen werden über einen Windows-Dienst (*vpxd.exe*, gilt nur für die installierbare Version, nicht für die Appliance) hergestellt. Die folgenden Ports werden für die Kommunikation benötigt.

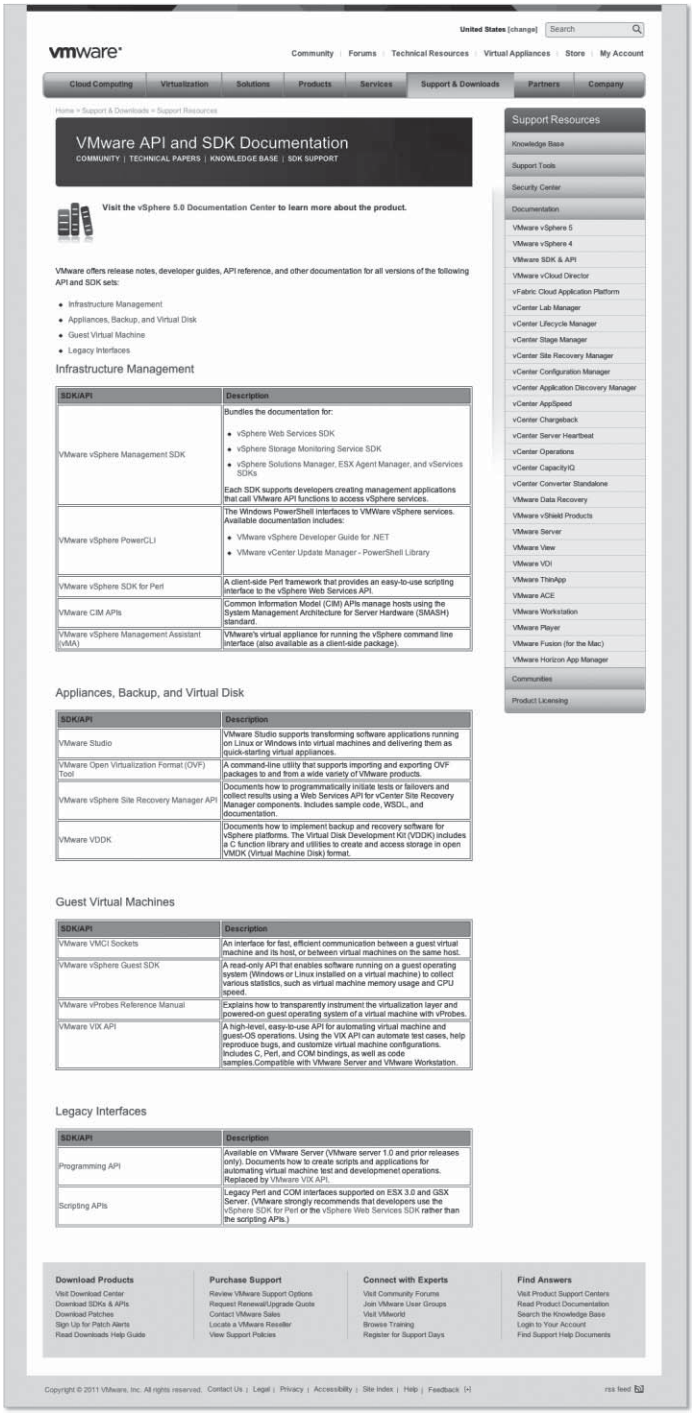


Abbildung 2.3 Webseite mit Informationen zu APIs und SDKs

Port	Protokoll	Kommunikation	Beschreibung
25	TCP	vCenter → SMTP-Server	E-Mail-Benachrichtigungen
53	UDP	vCenter → DNS-Server	DNS-Abfragen
80	HTTP	Client-PC → vCenter	Dieser Port wird für den direkten Webzugriff benötigt. Es erfolgt aber nur eine Umleitung auf Port 443. Es können Konflikte mit einem Installierten Microsoft IIS auftreten.
88	UDP	vCenter → AD-Server	Authentifizierung am Active Directory
88	TCP	vCenter → AD-Server	Authentifizierung am Active Directory
161	UDP	SNMP-Server → vCenter	SNMP-Polling
162	UDP	vCenter → SNMP-Server	Senden von SNMP-Traps
389	TCP	vCenter → Linked vCenter Server	Für die Kommunikation mit dem Active Directory wird dieser Port benötigt.
443	TCP	vSphere-Client → vCenter	Port für die initiale Anmeldung über den vSphere-Client
443	TCP	vCenter → ESX-Hosts	vCenter Agent, DPM-Kommunikation mit HP ILO
623	UDP	vCenter → ESX-Hosts	DPM-Kommunikation via IPMI
636	TCP	vCenter → Linked vCenter Server	SSL-Verbindung zwischen den vCenter-Servern beim Linked Mode
902	TCP	vCenter → ESX-Hosts	Kommunikation zwischen vCenter und vSphere-Hosts
902	UDP	vCenter → ESX-Hosts	Heartbeat-Kommunikation zwischen Hosts und vCenter
902	TCP/UDP	vSphere-Client → ESX-Hosts	Anzeige der Konsole von VMs
902	TCP/UDP	ESX-Host → ESX-Host	Interhost-Kommunikation bei Migration und Provisionierung
903	TCP	ESX-Host → vSphere-Client	Remote-Konsole-Kommunikation
1433	TCP	vCenter → MS SQL	Verbindung zum Datenbank-Server MS SQL
1521	TCP	vCenter → Oracle	Verbindung zum Datenbank-Server Oracle
5988	TCP	ESX-Host → vCenter	CIM-Transaktionen über HTTP
5989	TCP	vCenter → ESX-Host	CIM-XML-Transaktionen über HTTPS
5989	TCP	ESX-Host → vCenter	CIM-XML-Transaktionen über HTTPS
8000	TCP	vCenter → ESX-Host	vMotion-Anfragen
8005	TCP	vCenter → vCenter	interner Kommunikationsport
8006	TCP	vCenter → vCenter	interner Kommunikationsport
8080	HTTP	Client-PC → vCenter	Web Services HTTP
8083	TCP	vCenter → vCenter	Interne Dienstediagnose
8085	TCP	vCenter → vCenter	Interne Dienstediagnose
8086	TCP	vCenter → vCenter	Interner Kommunikationsport

Tabelle 2.10 vCenter-Server-Kommunikationsports

Port	Protokoll	Kommunikation	Beschreibung
8087	TCP	vCenter → vCenter	Interne Dienstediagnose
8443	HTTPS	Client-PC → vCenter	Webservices HTTPS
10109	TCP	vCenter → vCenter	Service Management vom vCenter Inventory Service
10111	TCP	vCenter → vCenter	Linked-Mode-Kommunikation des vCenter Inventory Services
10443	TCP	vCenter → vCenter	vCenter Inventory Server Service HTTPS
27000/ 27010	TCP	vCenter → Lizenz-Server	Lizenz-Server für VI3.x-Umgebungen
60999	TCP	vCenter → vCenter	Webservice Portchange

Tabelle 2.10 vCenter-Server-Kommunikationsports (Forts.)

Ports	Protokoll	Kommunikation	Beschreibung
80	TCP	Update Manager → Internet	Download von Patches aus dem Internet von den Websites: *www.vmware.com*, *www.shavlik.com*
80	TCP	ESX-Host → Update Manager	Kommunikation vom Host zum Update Manager
80	TCP	Update Manager → vCenter	Kommunikation zwischen Update Manager und vCenter Server
443	TCP	Update Manager → Internet	Download von Patches aus dem Internet von den Websites: *www.vmware.com*, *www.shavlik.com*
443	TCP	ESX-Host → Update Manager	Kommunikation vom Host zum Update Manager, Rückweg über 9084
443	TCP	vCenter → Update Manager	Kommunikation vom vCenter zum Update Manager, Rückweg über 8084
902	TCP	Update Manager → ESX-Host	Übermittlung von Patches vom Update Manager zum ESX-Host
1433	TCP	Update Manager → MS SQL	Verbindung zum Datenbank-Server MS SQL
1521	TCP	Update Manager → Oracle	Verbindung zum Datenbank-Server Oracle
8084	TCP	Update Manager → vCenter	SOAP-Server Update Manager
9084	TCP	ESX-Host → Update Manager	Webserver Update Manager
9087	TCP	Update Manager → vCenter	Port für das Uploaden von Host-Update-Files
9000 → 9100	TCP	ESX-Host → Update Manager	Ports für Hostscanning bzw. Bereich für Port-alternativen, wenn 80 und 443 schon anderweitig in Nutzung sind

Tabelle 2.11 Update-Manager-Kommunikationsports

Beim vCenter Converter werden unterschiedliche Ports genutzt. Dies hängt unter Umständen sogar davon ab, welches Betriebssystem importiert werden soll. In Tabelle 2.12 finden Sie die Ports, die für die Übernahme eines Servers benötigt werden.

Ports	Protokoll	Kommunikation	Bemerkungen
22	TCP	Helper VM → Source-Maschine	Für die Konvertierung von Linux-basierten Systemen
22	TCP	vCenter Converter → Source-Maschine	Für die Konvertierung von Linux-basierten Systemen
137	TCP	vCenter Converter → Source-Maschine	Für die Migration einer aktiven Maschine. Wird nicht benötigt, wenn die Quelle kein NetBIOS nutzt.
138	TCP	vCenter Converter → Source-Maschine	
139	TCP	vCenter Converter → Source-Maschine	
443	TCP	vCenter Converter Client → vCenter Converter Server	Wird benötigt, wenn der vCenter Converter Client nicht auf dem vCenter Converter Server installiert ist
443	TCP	Source-Maschine → ESX-Host	Dieser Port wird genutzt, wenn das Ziel ein ESX-Host ist.
443	TCP	Source-Maschine → vCenter	Dieser Port wird genutzt, wenn das Ziel ein vCenter ist.
443	TCP	vCenter Converter → vCenter	Dieser Port wird genutzt, wenn das Ziel ein vCenter ist.
443	TCP	vCenter Converter → ESX-Host	Port für die Systemkonvertierung
443	TCP	vCenter Converter → Helper VM	Für die Konvertierung von Linux-basierten Systemen
445	TCP	vCenter Converter → Source-Maschine	Nutzt die Quelle NetBIOS, dann wird dieser Port nicht benötigt.
902	TCP	Source-Maschine → ESX-Host	Datentransportport für das Cloning zum ESX-Host
9089/ 9090	TCP	vCenter Converter → Source-Maschine	Verteilung des Remote Agents

Tabelle 2.12 vCenter-Converter-Kommunikationsports

Kommt bei Ihnen das Data Recovery Tool von VMware zum Einsatz, dann müssen Sie die folgenden Ports in der Firewall freischalten.

Port	Protokoll	Kommunikation	Bemerkungen
443	TCP	Data Recovery → vCenter	Kommunikation zwischen Data Recovery und dem vCenter
902	TCP	Data Recovery → ESX-Host	Kommunikation zwischen Data Recovery und dem ESX-Host
22024	TCP	Data Recovery Plugin → Data Recovery	Data Recovery Management

Tabelle 2.13 Data-Recovery-Kommunikationsports

Der Orchestrator nutzt sehr viele Ports. Zur Gewährleistung einer einwandfreien Funktion sind diese Ports freizuschalten.

Port	Protokoll	Kommunikation	Bemerkungen
25	TCP	VCO-Server → SMTP-Server	E-Mail-Benachrichtigungen
389	TCP	VCO-Server → LDAP-Server	LDAP-Authentifizierung
443	TCP	VCO-Server → vCenter	Informationsaustausch über die virtuelle Infrastruktur
636	TCP	VCO-Server → LDAP-Server	SSL-LDAP-Kommunikation zur Abfrage von Gruppenmitgliedschaften
1433	TCP	VCO-Server → MS SQL	Kommunikation mit MS SQL
1521	TCP	VCO-Server → Oracle	Kommunikation mit Oracle-Datenbanken
3306	TCP	VCO-Server → MySQL	Kommunikation mit MySQL-Datenbanken
5432	TCP	VCO-Server → PostgreSQL	Kommunikation mit PostgresSQL-Datenbanken
8230	TCP	VCO-Client → VCO-Server	Lookup-Port – Kommunikation mit dem Konfigurations-Server
8240	TCP	VCO-Client → VCO-Server	Kommando-Port – Kommunikation für Remote-Aufrufe
8244	TCP	VCO-Client → VCO-Server	Daten-Port
8250	TCP	VCO-Client → VCO-Server	Messaging-Port – Weitergabe von Nachrichten im Java-Umfeld
8280	TCP	VCO-Server → VCO-Server	Kommunikation zwischen VCO-Server und Web-Frontend über HTTP
8281	TCP	VCO-Server → VCO-Server	Kommunikation zwischen VCO-Server und Web-Frontend über HTTPS
8281	TCP	vCenter → VCO-Server	Kommunikation zwischen VCO-Server und vCenter API
8282	TCP	VCO-Client-PC → VCO-Server	HTTP-Server-Port
8283	TCP	VCO-Client-PC → VCO-Server	HTTPS-Server-Port

Tabelle 2.14 Orchestrator-Kommunikationsports

Bei der Nutzung der vMA werden über das Netzwerk nur sehr wenige Ports verwendet.

Port	Protokoll	Kommunikation	Bemerkungen
443	TCP	vMA → vMA	SDK Traffic

Tabelle 2.15 vMA-Kommunikationsports

2.4 Architektur eines vSphere-Hosts

Die Architektur eines vSphere-Hosts definiert sich aus verschiedenen Kernkomponenten. Auf diese wollen wir im Folgenden eingehen.

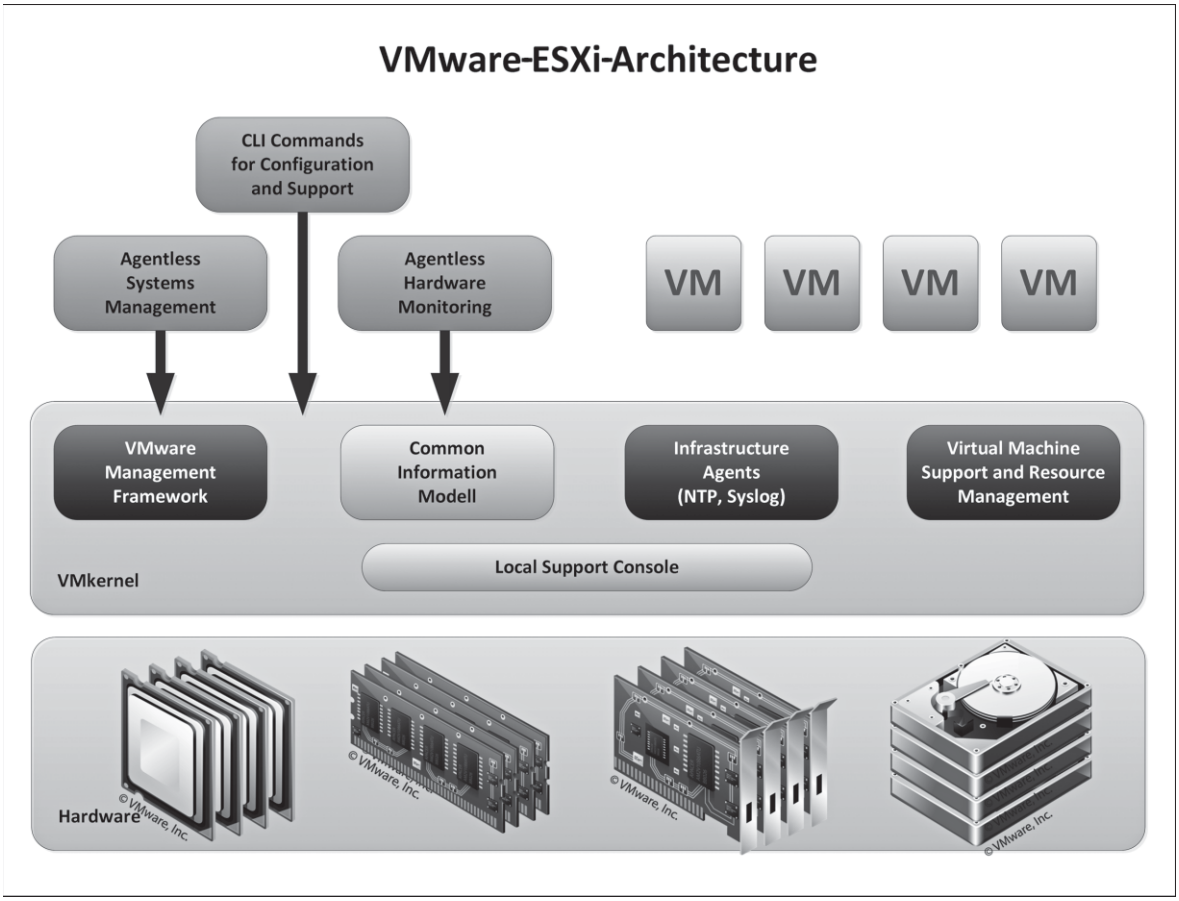


Abbildung 2.4 Struktur VMware vSphere ESXi

VMkernel

Der VMkernel ist eine sehr schlanke Implementierung des Hypervisors. Er kontrolliert und verwaltet die meisten Ressourcen eines vSphere-ESXi-Servers. Die Regelung des Zugriffs auf die Ressourcen CPU, Memory und Disk wird mit Hilfe eines Schedulers erreicht. Der Kernel hat neben einem TCP/IP-Stack zur Netzwerkkommunikation auch einen Storage-Stack für die Kommunikation mit Speichermedien. Der VMkernel ist eine Eigenentwicklung von VMware und nicht, wie viele meinen, ein Linux-Derivat.

VMware Management Framework

Sie können das System ohne zusätzlich zu installierende Agents verwalten. Ob Sie direkt auf den Host zugreifen oder den Host über einen vCenter Server managen, ist dabei vollkommen freigestellt.

Common Information Model (CIM)

Mit dem Common Interface Model gibt es eine offene Schnittstelle zum Management von Hardwareressourcen. Damit Ihre zum Einsatz kommende Hardware komplett unterstützt wird, müssen die passenden Treiber in dem ESXi-Image enthalten sein. Das Standard-Image von VMware bietet lediglich eine allgemeine Unterstützung. Arbeitet Ihr Hardwareanbieter nicht mit dieser freien Implementierung, müssen Sie bei ihm nach einem herstellerspezifischen Image fragen.

Infrastructure Agents

Die implementierten Infrastruktur-Agenten sind für das Syslogging, das SNMP-Handling und die Zeitsynchronisation zuständig. Zusätzlich werden hier die lokalen User verwaltet.

Resource Management

Der Resource Manager partitioniert die Hardware, um den virtuellen Maschinen mit Hilfe eines Share-Mechanismus die Ressourcen zur Verfügung zu stellen. Dabei werden die Einstellungen zur Reservierung und zur Limitierung der Ressourcen CPU und Memory beachtet sowie die Shares aller Core Four (CPU, Memory, Network und Disk) berücksichtigt. Der Resource Manager wird als Teilprozess des VMkernels gestartet.

Virtual Machine Support

Der Virtual Machine Support ist für die Virtualisierung der CPU zuständig. Er gibt die CPU-Befehle der virtuellen Maschine an die physische Hardware weiter. Außerdem kümmert er sich um die Verwaltung der virtuellen Maschine nach deren Start.

Hardware Interface Layer

Der Hardware Interface Layer setzt die Hardwareanfragen der VM in die physische Adressierung um und ermöglicht so eine Adressierung der Ressourcen. Außerdem koordiniert er die Bereitstellung des VMFS und der spezifischen Gerätetreiber. Er dient als Bindeglied zwischen dem VMkernel und der eigentlichen Server-Hardware.

2.5 Grundlagen der CPU-Virtualisierung

Bevor wir näher auf die CPU-Virtualisierung eingehen, möchten wir Ihnen zeigen, wie der logische Aufbau eines Prozessors aussieht. Als Beispiel haben wir das Schema einer Hexa-Core-CPU (6 Kerne) von AMD ausgewählt (Abbildung 2.5).

Unterhalb eines jeden Prozessor-Cores liegt der zugehörige Cache. Der Cache bildet das Bindeglied zwischen der CPU und dem Arbeitsspeicher. Der Arbeitsspeicher kann nicht so schnell getaktet werden wie der Cache. Damit aber der Zugriff auf den Speicher nicht das System ausbremst, werden im Cache Daten abgelegt, auf die das System öfter zugreifen muss.

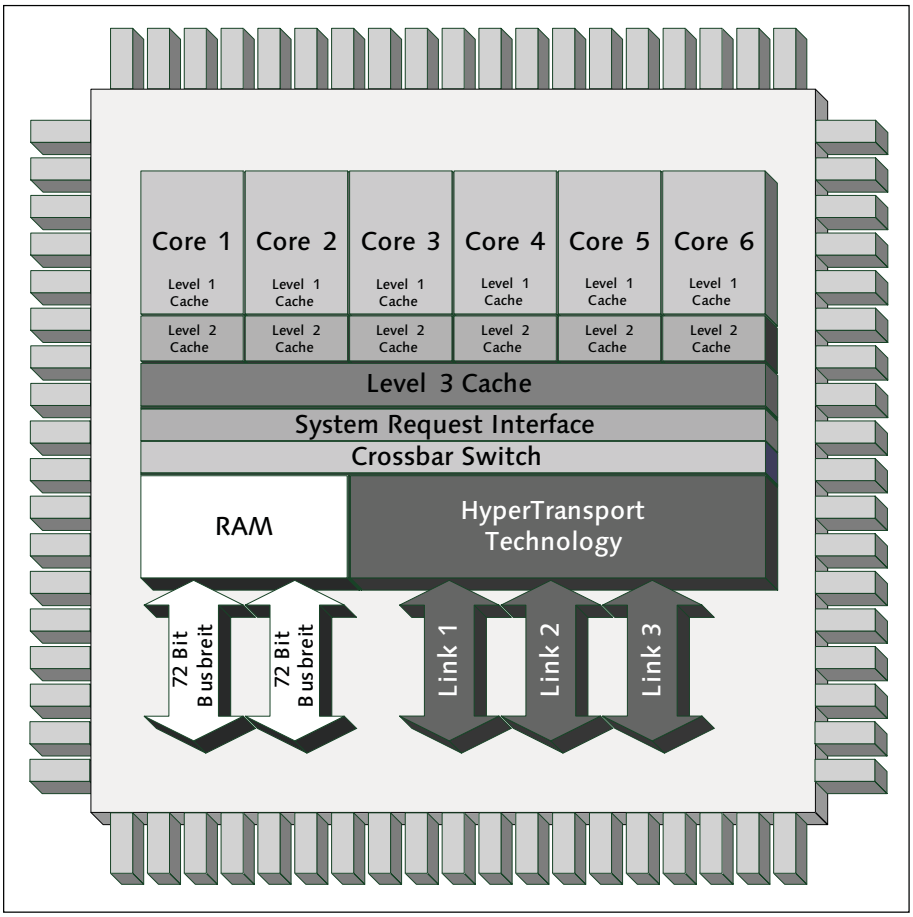


Abbildung 2.5 Logischer Aufbau einer AMD-CPU

Spezielle Mechanismen sorgen dafür, dass die Daten im Cache getauscht werden, wenn das System andere Informationen häufiger benötigt als die derzeit gespeicherten.

Der Cache gliedert sich in drei unterschiedliche Ebenen: Der Level-1-Cache ist direkt im Core integriert. Der Level-2-Cache ist ebenfalls dem einzelnen Core direkt zugeordnet. Erst der Level-3-Cache ist übergreifend allen Cores einer CPU zugänglich.

Über das *System Request Interface* (SRI) und den *Crossbar Switch* kommunizieren die einzelnen Cores untereinander und mit den weiteren Komponenten der CPU, wobei das SRI die CPU-Anfragen priorisiert.

Der Speicher-Controller ist direkt auf dem Prozessor integriert; somit kann die CPU direkt mit dem Speicher Daten austauschen, ohne über einen zusätzlichen externen Speicher-Controller die Informationen verschicken zu müssen. Das erhöht zum einen die Performance, zum anderen findet kein konkurrierender Zugriff der CPUs auf den Arbeitsspeicher statt.

Die HyperTransport Technology (HT) bildet das Bindeglied zwischen dem Prozessor und der Peripherie im Server. Sie hat aber auch die Aufgabe, sich um die Kommunikation der einzelnen Prozessoren untereinander zu kümmern. Soll ein Befehl ausgeführt werden, wird eine Broadcast-Meldung an alle Prozessoren geschickt, damit gewährleistet ist, dass wirklich die aktuellsten Daten verarbeitet werden.

Pro Core wurden früher mindestens zehn Nachrichten für den Abgleich benötigt. In einem Vier-Sockel-System (das heißt 48 Cores bei Hexa-Core-Systemen) bremsen die Nachrichten unter Umständen das System aus. An dieser Stelle greift die HT ein, koordiniert den Abgleich innerhalb der CPU und reduziert so die Anzahl der Nachrichten auf zwei bis drei für die Verbindung der CPUs untereinander.

Nach diesem kurzen, aber wichtigen Ausflug in die Hardware eines Systems kommen wir nun zu dem Unterschied zwischen einer Virtualisierung und einer Emulation.

Eine Emulation bildet Prozessoranfragen des Gasts über Software ab. Der Gast hat in diesem Fall keinen direkten Zugriff auf die CPU. Ein Virtualisierer leitet die Prozessoranfragen des Gasts direkt an die Hardware weiter.

VMware vSphere ist ein Virtualisierer. Unter vSphere wird die CPU einer virtuellen Maschine direkt vom Host-System abgeleitet und auch für bestimmte Arten von CPU-Instruktionen teilweise physisch verwendet. Aus diesem Grunde sieht eine VM dieselbe CPU, wie sie im Host vorhanden ist.

Die virtuelle CPU einer VM kann CPU-Instruktionen in zwei verschiedenen Modi abarbeiten: im Direct Execution Mode und im Virtualization Mode. In den meisten Fällen werden die CPU-Instruktionen im Direct Execution Mode ausgeführt, der nahe an der Geschwindigkeit der realen CPU liegt. Sollte der Befehl nicht in diesem Modus ausführbar sein, wird der Virtualization Mode verwendet. Eine virtualisierte CPU bedient sich so oft wie möglich der realen physischen CPU-Ressource, und die Virtualisierungsschicht greift nur bei der Ausführung von bestimmten CPU-Instruktionen ein.

Durch diese Umsetzung entsteht der oft erwähnte Virtualisierungs-Overhead. Den Virtualisierungs-Overhead beziffern wir näher in Abschnitt 2.6.2, »Memory-Overhead«, im Zusammenhang mit dem Arbeitsspeicher.

Dazu sei als Hintergrund erwähnt, dass eine CPU grundsätzlich vier Privilegierungsstufen hat, sogenannte *Ringe* oder auch *Domains* (Abbildung 2.7). Die höchste Priorität hat Ring 0. Hier liegt der sogenannte *Supervisor Mode*, der manipulativ auf Hauptspeicher und Interrupts zugreifen darf. In dieser Stufe läuft normalerweise der Kernel des Betriebssystems, im Falle von VMware vSphere also der Hypervisor-VMkernel. In den Ringen 1 bis 3 liegt der User-Mode, wobei normalerweise nur Ring 3 genutzt wird; es gibt nur wenige Applikationen, die direkt auf Ring 1 oder Ring 2 zugreifen.

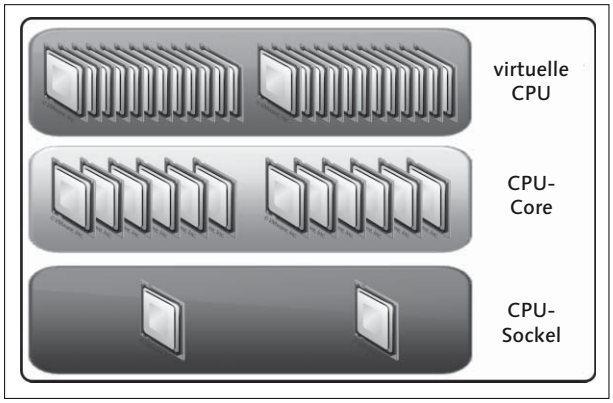


Abbildung 2.6 Zusammenhang zwischen physischen, logischen und virtuellen CPUs

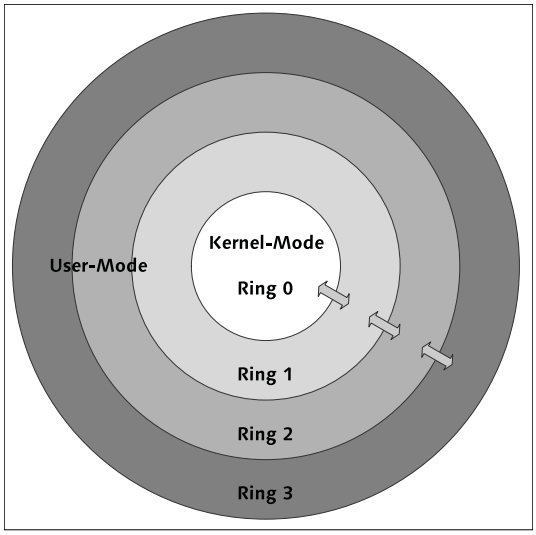


Abbildung 2.7 Ringstruktur der CPU

Bei einer virtuellen Maschine verhält sich das etwas anders: Die eigentlich an Ring 0 gestellten Anfragen des Betriebssystems werden an Ring 3 umgeleitet. Damit die Daten in Ring 1 bis 3 verarbeitet werden können, wird der physische Speicher in virtuelle Speicherseiten aufgeteilt. Der Memory-Controller (Memory Management Unit, MMU) übernimmt an dieser Stelle die Umsetzung von physischen Speicherinhalten in virtuelle. Damit der Programmcode auch richtig ausgeführt werden kann, enthält jede Speicherseite die Information, auf welchem Ring der Code ausgeführt werden muss. Um zu verhindern, dass ein solch komplexes System beeinflusst wird – z. B. durch Schadcode –, wurde das sogenannte *NX-Flag* kreiert (No Execution Flag). Diese Information hilft dem System, Daten von Programmcode zu unterscheiden. Dieser Mechanismus verhindert, dass Programmcode im Bereich der Daten ausgeführt werden kann.

Applikationen rufen in der Regel den unprivilegierten Ring einer CPU an, daher laufen diese Befehle im Direct Execution Mode. Wird hingegen eine Instruktion vom Betriebssystem ausgeführt, geschieht dies in der Regel modifizierend auf den privilegierten Ring der CPU. Diese Anfragen werden von der Virtualisierungsschicht, dem VMM, abgefangen.

Dieser Managementaufwand wird als der *Virtualisierungs-Overhead* bezeichnet. Er hängt ab von der Arbeitslast der virtuellen CPU und der Menge der Aufrufe an den privilegierten Ring. Die Auswirkungen zeigen sich in verlängerten Laufzeiten der einzelnen Befehle und durch eine erhöhte CPU-Last.

Die reale CPU wird an das Betriebssystem der VM durchgereicht. Aus diesem Grund sind dem Betriebssystem auch die Besonderheiten der eingesetzten CPU bekannt. Verschiedene Betriebssysteme nutzen diese CPU-spezifischen Befehle. Es kann auch während der Installation der Gast auf diese Besonderheiten hin optimiert worden sein. Ein Verschieben einer solchen speziellen VM auf andere vSphere-Server mit unterschiedlichen CPUs, insbesondere beim Wechsel zwischen Intel- und AMD-Prozessoren, beeinträchtigt unter Umständen die Funktionalität des Betriebssystems beziehungsweise der Applikation.

2.5.1 CPU-Affinity

Die *CPU-Affinität* bezeichnet eine Konfigurationsoption der virtuellen Maschine, und zwar die direkte Zuweisung einer physischen CPU bzw. eines Kerns. Diese Technik sollten Sie nur in Ausnahmefällen (z. B. Troubleshooting) verwenden, weil sie etliche Auswirkungen auf andere Bereiche der virtuellen Infrastruktur hat. Zum einen wird dadurch die CPU-Lastverteilung des ESXi-Servers außer Kraft gesetzt. Zum anderen kollidiert diese CPU-Zuordnung mit eventuell vorgenommenen Einstellungen von CPU-Shares und CPU-Reservierung. Durch das Umgehen der CPU-Lastverteilung kann der Hypervisor den Forderungen seitens der VM eventuell nicht mehr nachkommen. Die mögliche Virtualisierungsquote und die Flexibilität reduzieren sich. Die Nutzung von vMotion ist durch die CPU-Affinität eingeschränkt, und DRS verhindert diese sogar.

2.5.2 Hyperthreading

Der vSphere-Server unterstützt die Hyperthreading-Technologie von Intel. Diese bietet bei Nutzung von Ein-Sockel-Prozessoren der Pentium 4- und der Xeon-Reihe ein auf Hardwareebene realisiertes Multithreading zur Verbesserung der CPU-Performance. Lange Zeit war Pause mit hyperthreading-fähigen CPUs, bis Intel diese in den neuen 5500-Xeon-Prozessoren wieder integrierte. Dabei kann eine physische CPU – im Intel-Wortgebrauch wird sie als »Hyperthread« bezeichnet – gleichzeitig zwei Threads ausführen. Sie verhält sich mit aktiviertem Hyperthreading ähnlich wie zwei logische CPUs. Sofern ein Betriebssystem und die darauf laufenden Applikationen zwei CPUs nutzen können, sind hierdurch Geschwindigkeitsvorteile möglich. Dabei reicht die Performance nicht an eine Verdoppelung heran, wie sie durch einen Dual-Core-Prozessor erreicht würde, die Leistung einer CPU verbessert sich aber je nach

Anwendung auf dem Betriebssystem signifikant. Ungeeignete Applikationen werden durch die Hyperthreading-Technologie unter Umständen auch verlangsamt, wenn sie zu viel der gemeinsam genutzten Ressourcen eines Cores verwenden.

Auf der Hardwareebene muss das Hyperthreading im BIOS aktiviert sein. Im Host ist Hyperthreading per Default aktiv; bei Bedarf deaktivieren Sie es über den vSphere-Client im Tab CONFIGURATION eines vSphere-Hosts unter den Eigenschaften der CPU. Bedenken Sie bitte beim Einsatz von Hyperthreading, dass ein vSphere-Host nur eine bestimmte Anzahl von CPUs unterstützt.

Der vSphere-Server verteilt die Last zwischen den Cores, um eine ausgewogene Auslastung zu erreichen. Wenn für eine logische CPU keine Last gefordert wird, wird sie in einen speziellen *Halt State* geschaltet. Dabei kann eine andere VM auf dem Core von den zusätzlichen freien Ressourcen dieser CPU profitieren.

Um virtuelle Maschinen mit für Hyperthreading problematischen Anwendungen ohne dieses Feature zu betreiben, bietet vSphere auf Ebene der VM drei verschiedene Modi des Verhaltens an, siehe Tabelle 2.16.

Parameter	Funktion
ANY	Dies ist die Standardeinstellung und ermöglicht das Teilen der logischen CPUs eines Cores mit entweder einer weiteren virtuellen CPU derselben VM oder einer virtuellen CPU einer anderen VM. Diese Einstellung bietet, sofern die Anwendungen dafür ausgelegt sind, die optimale Performance.
NONE	Diese Einstellung schaltet das Hyperthreading pro virtueller Maschine aus. Eine virtuelle CPU wird einer logischen CPU eines Cores zugeordnet, die zweite logische CPU wird in den Halted State geschaltet. Da diese Einstellung eine virtuelle CPU vom restlichen System isoliert, wird diese Konfiguration für hyperthreading-problematische Applikationen verwendet und sollte nur nach Aufforderung durch den VMware-Support oder den Support des Anwendungsherstellers implementiert werden.
INTERNAL	Diese Einstellung beschränkt die Nutzung der zwei logischen CPUs auf eine VM und gilt daher nur für VMs mit aktiviertem vSMP. Eine VM teilt sich den Core nicht mit anderen VMs, sondern der Core wird nur für die virtuellen CPUs einer VM verwendet. Haben Sie diese Einstellung für eine Uniprozessor-VM ausgewählt, schaltet vSphere diese Einstellung automatisch auf NONE.

Tabelle 2.16 Hyperthreading-Parameter

Diese Einstellungen haben keinen Einfluss auf die Verteilung und Priorisierung von CPU-Ressourcen an die virtuelle Maschine.

2.5.3 Virtual SMP (vSMP)

Auch in virtuellen Umgebungen ist es möglich, virtuelle Maschinen mit mehr als einer vCPU zu erstellen. Die aktuelle Version von VMware vSphere unterstützt bis zu 32 virtuelle CPUs pro VM. VMware nennt diese Funktion *Virtual SMP* (Symmetric Multi Processing) oder auch

vSMP. Dabei ist einiges zu beachten: Grundsätzlich – das unterscheidet eine virtuelle Maschine nicht von einem physischen Server – ist nicht jede Applikation multiprozessorfähig. Vor der Erzeugung einer vSMP-Maschine sollten Sie dies abklären und dabei nicht nur das Betriebssystem (auf die HAL bzw. den Kernel achten), sondern auch die Anwendung beachten.

Schauen wir noch einmal zurück auf den Beginn von Abschnitt 2.5, »Grundlagen der CPU-Virtualisierung«, in dem wir den logischen Aufbau einer CPU erklärt haben. Da es allen CPUs einer VM möglich sein muss, auf identische Speicheradressen zuzugreifen, auch beim Cache, wird sofort klar, dass eine virtuelle Maschine mit mehreren CPUs am leistungsfähigsten arbeiten kann, wenn alle virtuellen Prozessoren auf einer logischen oder physischen CPU liegen. Liegen die Prozessoren auf unterschiedlichen Sockeln, dann können die virtuellen CPUs nicht in optimaler Geschwindigkeit miteinander kommunizieren. Die Ursache dafür ist, dass der Informationsaustausch der CPUs untereinander über den Frontside-Bus erfolgen muss.

Auch beim Betriebssystem müssen Sie auf einiges achten. Denken Sie bitte daran, dass Sie bei mehreren CPUs in einer VM einen Multiprozessor-Kernel installieren müssen. Einen Weg zurück, zumindest bei Windows-VMs, unterstützt Microsoft nicht.

Lassen Sie uns nun betrachten, wie VMware mit dem Thema vSMP und der Tatsache, dass freie Ressourcen anderen VMs zur Verfügung gestellt werden, umgeht. Während eine CPU im physischen Umfeld exklusiv einem Betriebssystem zur Verfügung steht, teilen sich die virtuellen Maschinen die CPU-Zyklen. Zur optimalen Abarbeitung der Prozesse werden diese in einem SMP- bzw. vSMP-System parallelisiert. Steht eine teilprozessabarbeitende Instanz nicht zur Verfügung, müssen alle anderen Teilprozesse so lange warten, bis auch dieser Prozess parallel zu den anderen abgearbeitet wurde. Diese Art der parallelen Abarbeitung wird auch *Co-Scheduling* genannt und dient grundsätzlich dazu, die Performance eines Systems zu erhöhen.

Es könnte vorkommen, dass ein Watchdog-Timer auf einen Schwesterprozess warten muss. Reagiert dieser Prozess aber nicht in einem passenden Zeitfenster, stirbt er. Zur Messung dieser Varianzen wird der sogenannte *Skew* herangezogen. Dieser Wert repräsentiert den zeitlichen Unterschied zwischen den Prozessteilen. Überschreitet der Skew einen definierten Schwellenwert, dann wird die CPU der VM mit angehalten (*co-stopped*). Sie wird erst wieder mitgenutzt (*co-started*), wenn genügend Ressourcen für die Abarbeitung auf der physischen CPU vorhanden sind. Der Co-Stop verhindert, dass der Skew-Wert sich erhöht; dieser kann nur sinken. Mit dem Relaxed Co-Scheduling wurde mit ESXi 3 nämlich eine Funktion eingeführt, dass angehaltene vCPUs keine Skew-Wert-Erhöhung mehr erfahren. Somit wird ein zu häufiges Co-Scheduling verhindert.

Der Skew-Wert hat aber noch eine weitere Funktion: Der VMkernel nutzt diesen Wert, um die Arbeitslast auf die physischen CPUs zu verteilen. Eine geskewte CPU hat Rechenzeit übrig, die andere VMs nutzen können.

vSphere bringt wesentliche Änderungen gegenüber ESXi 3 mit, da neben der deutlichen Minderung des Co-Stoppings nun auch die Nutzung aller Prozessorkerne ermöglicht wurde.

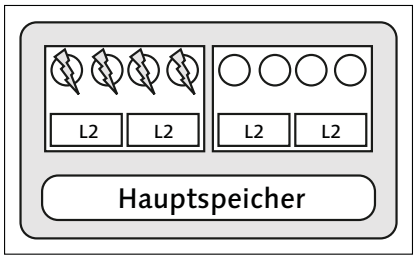


Abbildung 2.8 SMP-Handling unter ESXi 3

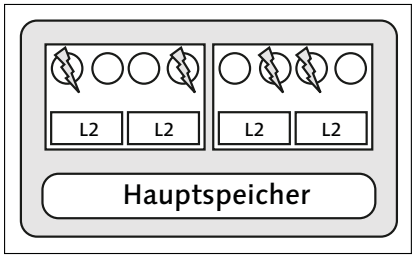


Abbildung 2.9 SMP-Handling unter ESXi 4

Dadurch wurde ein wesentliches Problem der ESXi 3-Welt gelöst, da CPU-Anfragen der VMs teilweise unnötig warten mussten, weil nicht genügend Kerne einer physischen CPU verfügbar waren. Somit hat der CPU-Scheduler ab ESXi 4 wesentlich mehr Möglichkeiten, CPU-Anfragen zu verteilen.

ESXi 3.x	ESXi 4
V0, V1, V2, V3	V0, V1, V2, V3
V0, V1, V2	V0, V1, V2
V0, V1, V3	V0, V1, V3
V0, V1	V0, V1
–	V0, V2
–	V1, V2
–	V0
–	V1
–	V2

Tabelle 2.17 SMP-Vergleich zwischen ESXi 3 und ESXi 4

Mit vSphere 5.x hat sich eine weitere Änderung an der Stelle ergeben, die die Performance noch einmal erheblich steigert: VMware bringt die NUMA-(Non-uniform Memory Access-)Architektur in die VM. Unterstützt wird diese Funktion sowohl von Intel- als auch von AMD-CPUs.

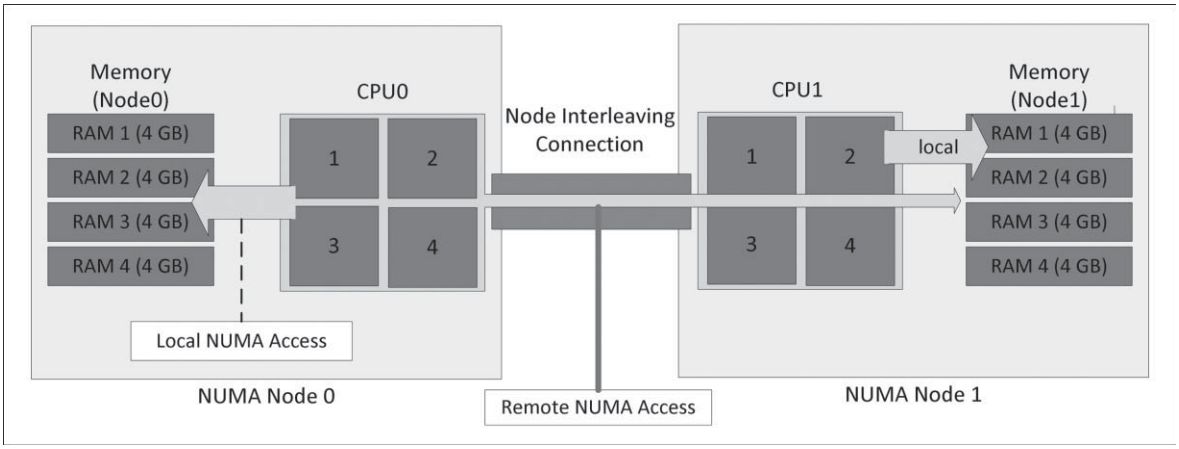


Abbildung 2.10 NUMA-Architektur

Lassen Sie uns zuerst darauf eingehen, was NUMA genau ist. NUMA ist interessant für Multiprozessorsysteme; hier hat jede CPU seinen lokalen Arbeitsspeicher, den sie aber auch anderen CPUs zur Verfügung stellen kann. Auf physischer Ebene erkennen Sie das daran, dass jede CPU ihre eigenen Speicherbänke besitzt. Im Sinne einer guten Performance sollten diese Bänke auch symmetrisch mit Memory bestückt werden. Eine solche Kombination von CPU plus zugehörigem Speicher nennt man *NUMA-Knoten*. In Abbildung 2.10 sehen Sie eine CPU mit zwei NUMA-Knoten, die wie empfohlen symmetrisch mit 16 GB Arbeitsspeicher ausgestattet sind.

Es wird so gewährleistet, dass überwiegend auf schnellen lokalen Speicher zugegriffen werden kann. Das macht sich positiv bei der Gesamtperformance bemerkbar, denn mehrere Prozessoren können nicht konkurrierend auf Speicherbereiche zugreifen. Mit der extremen Steigerung der Cores pro Prozessor ist das ein immer größer werdendes Problem. Gerade bei hochlastigen Anwendungen könnten sich die CPUs bzw. Cores untereinander ausbremsen.

Benötigt ein Kern nun mehr Arbeitsspeicher, als die eigene CPU direkt adressieren kann, so kann er diesen anfordern. Über einen Remote NUMA-Zugriff kann der Speicher einer anderen CPU angefordert und für die eigenen Belange genutzt werden. Dass dieser Zugriff langsamer ist als das Nutzen des eigenen Speichers, müssen wir wohl nicht extra erwähnen.

Welche Vorteile oder Nachteile hat das für eine virtuelle Maschine? Lassen Sie uns tiefer einsteigen und die möglichen Szenarien betrachten. Eine NUMA-VM bekommt einen sogenannten Home-Node, das bedeutet, sie bekommt damit einen Prozessor und Speicher zugewiesen. Braucht eine VM Speicher, so wird er optimalerweise vom Home-Node zugewiesen, so sind schnelle Zugriffszeiten garantiert. Ist der Workload in einem Home-Node zu hoch, kann bzw. wird die VM auf einen anderen Home-Node verschoben. Gewährleistet werden kann das aber nur, wenn die ESX-Optimierung aktiv ist. Ist das nicht der Fall, tritt nicht selten ein Fall auf, wie er in Abbildung 2.11 dargestellt ist.

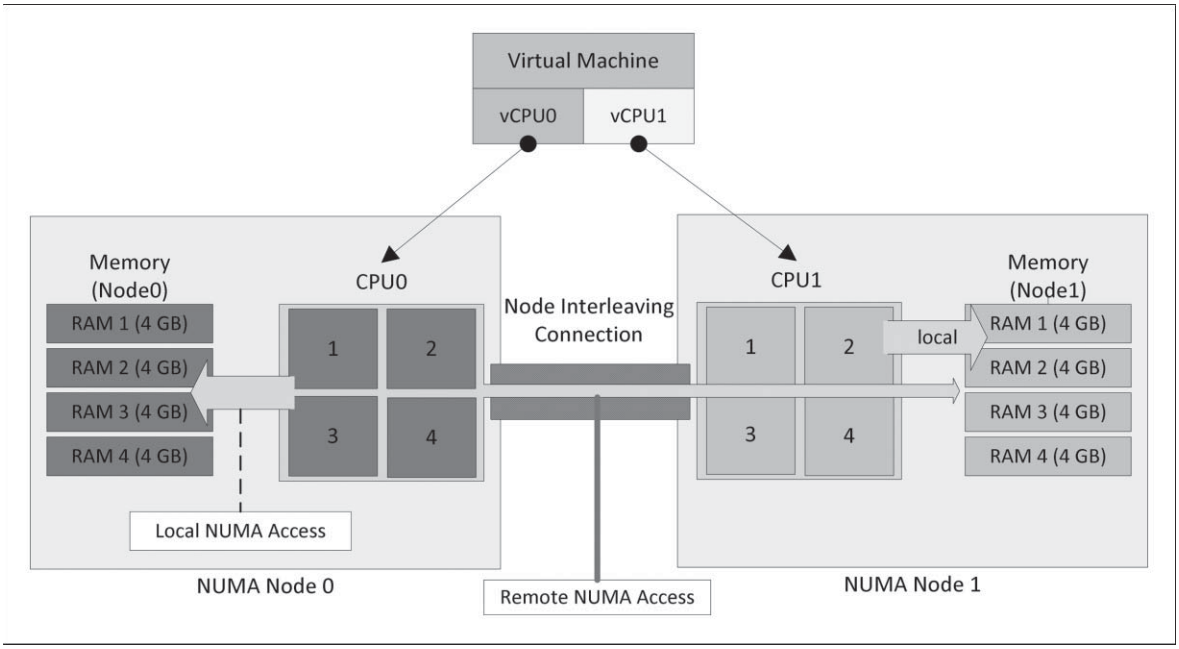


Abbildung 2.11 Verteilung der vCPUs bei deaktivierter ESX-Optimierung

Aufgrund der inaktiven Optimierung kann es bei Mehrprozessor VMs passieren, dass die vCPUs sich auf mehrere Prozessoren verteilen, was zur Folge hat, dass die virtuelle Maschine nicht optimal performen kann. In der Grundkonfiguration aktiviert sich NUMA automatisch in der virtuellen Maschine mit der virtuellen Hardwareversion 8. Da stellt sich sofort die Frage, wie Sie die ESX-Optimierung aktivieren können. Lassen Sie uns das Pferd an dieser Stelle von hinten aufzäumen, denn es ist einfacher, die Konfigurationen zu listen, die eine NUMA-Optimierung verhindern:

- NUMA ist in der BIOS-Konfiguration des Servers deaktiviert.
- CPU-Affinitätsregeln binden die virtuelle Maschine an Cores, die auf unterschiedlichen NUMA-Knoten liegen.
- Die VM nutzt mehr Arbeitsspeicher, als ein NUMA-Knoten direkt adressieren kann.
- Es werden in der VM mehr CPU-Kerne genutzt, als ein NUMA-Knoten bereitstellen kann.
- Es sind weniger als vier Cores insgesamt oder 2 Cores pro NUMA-Knoten nutzbar.

Bei den zuletzt genannten Werten handelt es sich um die Standardeinstellungen des ESXi-Hosts. Diese können Sie in den Advanced Settings unter dem Punkt NUMA an Ihre Bedürfnisse anpassen. Die Werte Numa.RebalanceCoresTotal und Numa.RebalanceCoresNode sind für diese Einstellungen verantwortlich.

Es handelt sich also um eine Funktion, die speziell auf die Performanceoptimierung von Mehrprozessor-VMs abzielt.

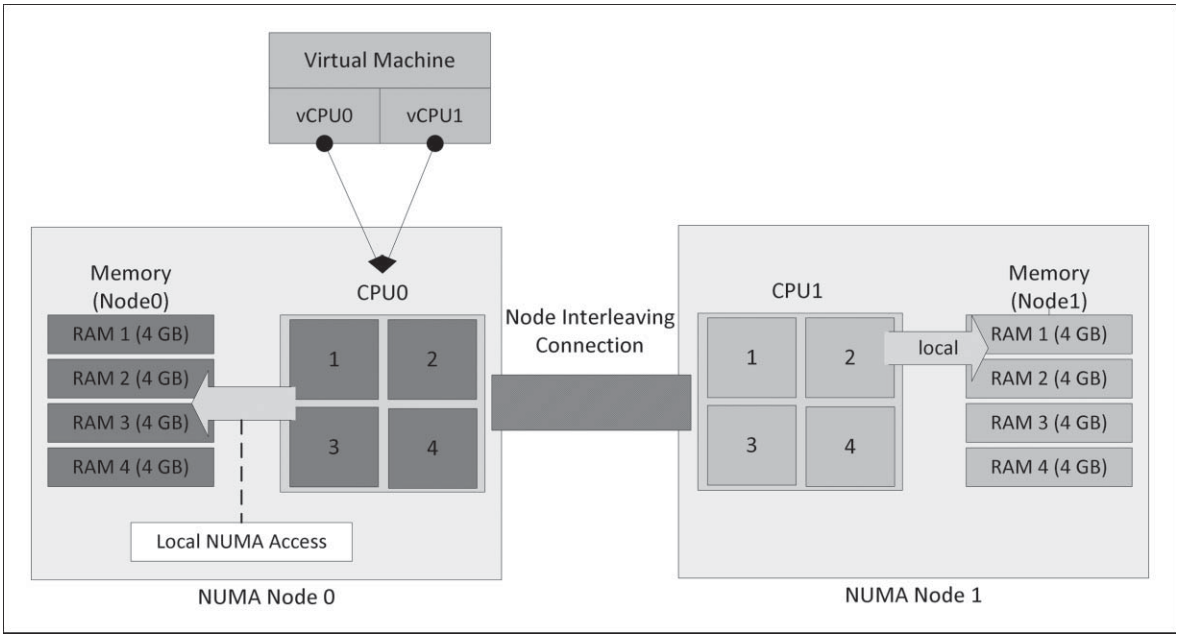


Abbildung 2.12 Aktivierte ESX-Optimierung – VM liegt auf einem NUMA-Knoten.

Es gilt zwar auch weiterhin unter vSphere vSMP, dass weniger mehr ist, allerdings ist es wesentlich entspannter geworden, Mehrprozessor-VMs zu verwenden. Das Hauptkriterium sollte immer noch die Anforderung der Anwendung und des Systems sein und nicht der Gedanke, dass mehr CPUs auch automatisch mehr Leistung bedeuten. Bedenken Sie aber bitte auch hier, dass es zwar möglich ist, VMs anzulegen, deren Anzahl von vCPUs der Anzahl der gesamten Cores der unterliegenden Hardware entspricht, aber in diesem Fall ist es nicht unwahrscheinlich, dass viele Remote NUMA-Zugriffe stattfinden. Das bedeutet, dass die Prozessoren untereinander auf ihre Speicherbereiche zugreifen. Für eine optimale Performance sollte somit eine virtuelle Maschine maximal so viele vCPUs besitzen, wie physische Cores auf einer CPU vorhanden sind. Diese Performanceeinschränkung greift auch, wenn Sie einer VM mehr Arbeitsspeicher zuweisen, als ein NUMA-Knoten, sprich eine physische CPU, direkt adressieren kann, ohne remote auf den Bereich einer anderen CPU zugreifen zu müssen.

2.5.4 Best Practices

Nachfolgend finden Sie einige Empfehlungen zum Umgang mit CPU-Reservation, -Limits und -Shares:

- Erfahrungsgemäß werden Prozessoren nicht zurückgerüstet, auch wenn sie eigentlich nicht benötigt werden. Bei Mehrprozessor-VMs fangen Sie einfach mit einer Zweiprozessor-Maschine an. Weitere Prozessoren lassen sich immer noch später hinzukonfigurieren. Vergeben Sie niemals mehr Prozessoren, als sich Cores auf der CPU befinden.

- Einer virtuellen Maschine sollten Sie zu Beginn grundsätzlich niedrige CPU-Ressourcen zuweisen, um im laufenden Betrieb die Ressourcenauslastung anhand der vCenter-Performancemessung zu analysieren.
- Es ist besser, mit CPU-Shares anstelle von CPU-Reservierungen zu arbeiten.
- Beim Einsatz von CPU-Reservierungen sollten Sie das aktuelle Minimum definieren, das eine VM benötigt, nicht aber die gewünschte absolute Menge an CPU in MHz. Wenn eine VM mehr Ressourcen benötigt, so weist der vSphere-Server diese, je nach definierten Shares, bis zu einem eventuell definierten CPU-Limit dynamisch zu. Des Weiteren ist zu beachten, dass der Einsatz von CPU-Reservierungen die auf einem Host zur Verfügung stehenden CPU-Ressourcen limitieren kann und dadurch weniger VMs gestartet werden können. Zu hohe Reservierungen behindern möglicherweise auch Funktionen wie DRS oder HA. Das Verschieben von virtuellen Maschinen kann durch die Ressourcenauslastung der vSphere verhindert werden.

2.6 Grundlagen der Memory-Virtualisierung

Der physische Speicher eines Hosts wird in zwei Segmente unterteilt: System und Virtual Machines. Der Speicherbereich für System wird vom VMkernel und von den Gerätetreibern verwendet und ist nicht konfigurierbar. Er wird mit einer Größe von mindestens 50 MByte beim Starten des vSphere-Hosts angelegt und variiert je nach Anzahl und Art der verwendeten PCI-Geräte und deren Treibern. Der Speicherbereich für Virtual Machines ist der Rest des physischen Speichers und wird komplett für die VMs genutzt.

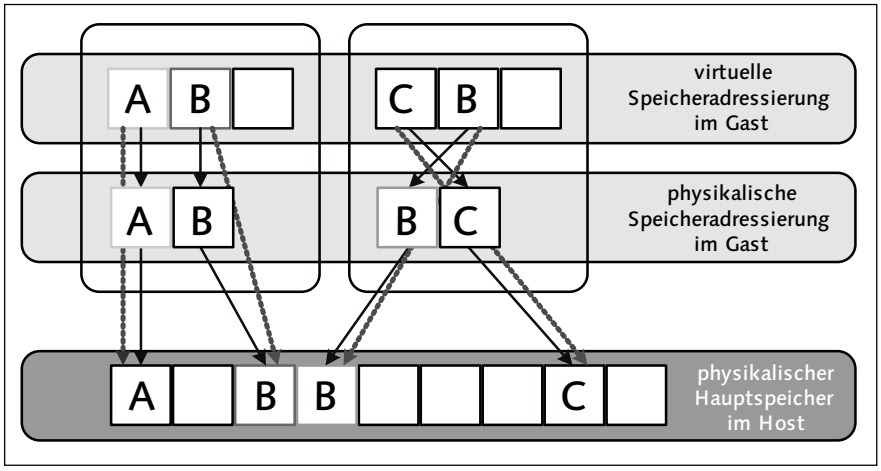


Abbildung 2.13 Speicheradressierung zwischen VM und Host

Zur Verdeutlichung hier zuerst eine Erklärung zur generellen Nutzung von Speicher innerhalb eines Betriebssystems. Speicher wird in einem Betriebssystem über virtuelle Speicheradressen

erreicht, die auf physische Adressen verweisen. Ein Zugriff von einer virtuellen Maschine auf den physischen Speicher eines vSphere-Hosts ist nicht erlaubt. Um den virtuellen Maschinen Speicher zur Verfügung zu stellen, bietet vSphere eine weitere, virtuelle Schicht. Diese gaukelt der VM die physischen Speicheradressen vor. Im VMware-Wortgebrauch heißt der physische Speicher im Host *Machine Memory Pages*, und die der VM virtualisiert vorgegaukelten physischen Speicherseiten nennen sich *Physical Memory Pages*. Die Physical Memory Pages für eine VM sind, so wie es ein Betriebssystem erwartet, mit durchgängigen Nullen gefüllt. Sie sind durch die Virtualisierungsschicht aus verschiedenen Bereichen, aber nicht zusammenhängend, zusammengefasst. Diese Bereiche sind z. B. normale, physische Speicherbereiche (Machine Memory Pages), von vSphere Shared Pages oder auch Swapped Pages. Das virtuelle Speichermanagement erfolgt durch den Host, unabhängig vom in der VM laufenden Betriebssystem, über den VMkernel. Dieser greift von der VM alle Befehle ab, die auf den Speicherbereich schreibend zugreifen möchten, und leitet diese auf die der VM vorgegaukelten Physical Memory Pages um.

Der Speicher wird normalerweise in 4-KB-Blöcke eingeteilt. Es werden aber auch Memory-Blöcke von 2 MB unterstützt. Diese Funktion können Sie nur pro VM konfigurieren. Dazu aktivieren Sie in dem Konfigurations-File die Funktion `Mem.AllocGuestLargePage=1`. Dies ist empfehlenswert, wenn die VM große Speicherseiten benötigt, wie z. B. ein Datenbank-Server.

2.6.1 Virtual Machine Memory

Der Speicherbereich, der für die VMs zur Verfügung steht, wird *Virtual Machine Memory* genannt und bietet allen VMs die Speicherressourcen des vSphere-Servers abzüglich eines Virtualisierungs-Overheads. Dem Betriebssystem wird vorgegaukelt, dass der Speicher, der in der Konfiguration festgelegt wurde, auch vorhanden ist. Der physisch zugewiesene Speicher kann aber variieren, bis zum konfigurierten Maximum. Auch hier setzen Sie über die Einstellung der Shares-Werte eine Priorität gegenüber den anderen VMs, die auf demselben Host arbeiten. Eine Reservierung weist den Speicher der virtuellen Maschine fest zu.

2.6.2 Memory-Overhead

Der Memory-Overhead hängt ab von der Anzahl der CPUs und natürlich von dem der VM zugewiesenen Speicher. Dieser Memory-Overhead stellt einen Speicherbereich zur Verfügung, um VM-Frame-Buffer sowie verschiedene Virtualisierungsdatenstrukturen abzulegen. Die Nutznießer dieses Speichers sind zum einen der VMkernel und zum anderen der VMM, die beide für die korrekte Arbeit der virtuellen Maschinen benötigt werden.

Der einzukalkulierende Overhead lässt sich nicht mehr in einer Tabelle zusammenfassen. Es bestehen verschiedene Abhängigkeiten, die einen Einfluss auf den Memory-Overhead haben. Das sind die Anzahl der vCPUs und die Größe des vRAMs. Wir haben uns einmal die Mühe gemacht, eine Formel zu aufzustellen, die Ihnen sehr genau die Größe des Overheads berech-

nen kann. Es war leider nicht ganz so einfach, weil sich die Werte an einigen Stellen sprunghaft erhöhen. Wir benötigen dazu eine kleine Hilfstabelle, in der die Anzahl der CPUs mit einem Faktor verbunden wird.

Anzahl CPUs	Wert für Faktor
1	0
2, 3, 4	1
5, 6, 7, 8, 9	3
10, 11, 12, 13, 14, 15,16, 17, 18, 19, 20	7
21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	15

Tabelle 2.18 Faktorberechnung für die Kalkulation des Overheads

Die Formel lautet:

[48 + (Speicher in GB × 19)]
\+ *[[23 + (Speicher in GB × 3)] × (Anzahl CPU 1)]*
\+ *[(Speicher in GB × 8) × Faktor]*

Sie ist verifiziert für virtuelle Maschinen bis 24 CPUs. Uns stand leider keine passende Hardware zur Verfügung, um VMs anzulegen, die mehr CPUs haben. Mit der Formel können Sie schon im Voraus genau berechnen, wie viel Arbeitsspeicher Sie zusätzlich benötigen abhängig von den virtuellen Systemen, die in der Virtuellen Infrastruktur aufgebaut werden sollen.

2.6.3 Memory-Overcommitment

vSphere bietet die Möglichkeit, mehr RAM an virtuelle Maschinen zu vergeben, als physisch im Host selbst vorhanden ist. Dieses Feature nennt sich *Memory-Overcommitment* und setzt sich zusammen aus mehreren verschiedenen Techniken: dem Memory-Compression, dem Page-Sharing, dem Memory-Ballooning und dem Memory-Swapping. Das Bestreben aller Techniken ist das Verteilen von ungenutzten Speicherbereichen von einer VM zu anderen Maschinen, die aktuell mehr Speicher benötigen. Die Priorisierung erfolgt auch in diesem Fall über die eingestellten Share-Werte.

2.6.4 Memory-Compression

Ist das Memory-Overcommitment aktiviert, wird auch automatisch die Memory-Compression eingeschaltet. Die Speicherseiten werden automatisch komprimiert und im Arbeitsspeicher vorgehalten. Die Performance ist dabei nur geringfügig eingeschränkt, denn der Zugriff auf den Arbeitsspeicher ist allemal schneller, als wenn das System auf geswappte Daten zugreifen muss. Zwei Einstellungen beeinflussen dabei das Verhalten der Funktion. In den Advanced Settings lässt sich die Funktion ganz Deaktivieren, indem Sie den Parameter Mem.MemZipEnable auf 0 setzen. Der Parameter Mem.MemZipMaxPct gibt prozentual an, wie viel Spei-

cher der VM maximal als Kompressions-Cache genutzt werden soll. Der Standardwert dieses Parameters liegt bei 10 %.

2.6.5 Content-based Page-Sharing

Die Page-Sharing-Technik wird beim Betrieb von mehreren VMs auf einem Host verwendet. Es wird versucht, identische Memory-Pages der VMs zusammenzufassen. Die dabei beobachtete Speicher-Blockgröße ist so klein, dass es vollkommen unerheblich ist, ob auf den virtuellen Servern identische Software installiert ist oder nicht.

Trotzdem gelingt dies umso besser, je homogener die verschiedenen Gastbetriebssysteme sind, also wenn mehr identische Server-Applikationen darauf laufen. Ein gutes Beispiel ist eine Server-Farm mit identischen Webservern, die aber alle unterschiedlichen Webcontent hosten. Es ist zu erwarten, dass diese Systeme eine große Anzahl von identischen Speicherblöcken haben, die vom VMM zusammengefasst werden können. So werden redundante Speicherinhalte eliminiert. Will nun eine der virtuellen Maschinen einen solchen Speicherbereich beschreiben, dann wird für diesen Server eine Kopie des Speicherblocks exklusiv für ihn angelegt, so dass er ihn frei nutzen kann. Bei dieser Technik sind bis zu 30 % Speicherersparnis erreichbar. Bei weniger homogenen Memory-Inhalten reduziert sich die Ersparnis auf ca. 5 %.

2.6.6 Memory-Ballooning

Das in Abschnitt 2.6.3, »Memory-Overcommitment«, beschriebene Memory-Overcommitment kann nur einwandfrei funktionieren, wenn dem Host ein Mechanismus zur Verfügung steht, der das Management des Arbeitsspeichers im virtuellen System übernimmt, und das natürlich im laufenden Betrieb. Dafür ist das sogenannte *Memory-Ballooning* zuständig.

Der Memory-Balloon-Treiber (*vmmemctl)* kommt ins Spiel, wenn der Speicher eines Hosts zu knapp wird oder wenn eine VM an ihre Speichergrenzen stößt. Braucht der Host Speicher, dann hat Ballooning immer Vorrang vor dem Swappen.

Wird Speicher benötigt, dann gibt der VMM dem Ballooning-Treiber das Kommando zur Anforderung von Speicher vom OS (Abbildung 2.14, ❶). Ist genug Speicher vorhanden, gibt die VM demjenigen Treiber Speicher, der in der Free-List steht. Ist kein freier Speicher vorhanden, wird dem Gast-OS überlassen, welcher Speicher freigegeben werden kann.

Der vSphere-Kernel gibt im Hintergrund die vom Ballooning-Treiber markierten Speicherseiten frei, bis genug Speicher für den Host akquiriert worden ist (❷). Anschließend beginnt der Ballooning-Treiber, den reservierten Speicher wieder freizugeben (❸).

Das Verhalten des Memory-Ballonings können Sie pro vSphere-Server durch den Parameter SCHED.MEM.MAXMEMCTL festlegen. Dieser Wert bestimmt die maximale durch diese Technik von einer virtuellen Maschine abziehbare Speichermenge und wird in Megabytes angegeben.

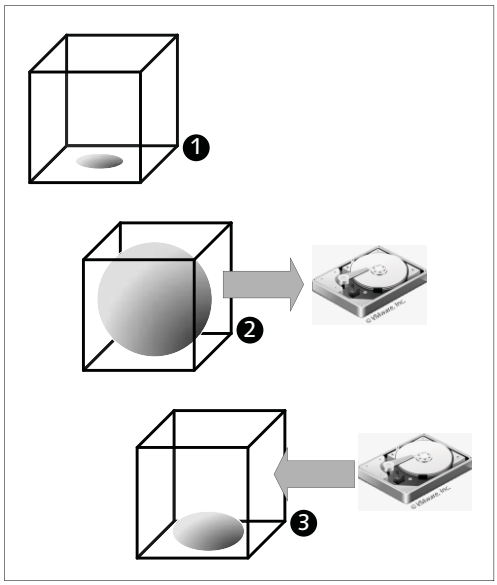


Abbildung 2.14 Darstellung des Memory-Balloonings

2.6.7 Memory-Swapping

Das Memory-Swapping dient ebenso wie das Ballooning zum Zuweisen von mehr Arbeitsspeicher an die VM. Diese Technik ist für den Host die letzte, aber auch langsamste Möglichkeit, Speicher für andere virtuelle Maschinen zur Verfügung zu stellen. Beim Start einer VM wird automatisch ein solches Swapfile angelegt. Swapping tritt zu dem Zeitpunkt in Aktion, wenn der Hypervisor nicht die Möglichkeit hat, über den Ballooning-Treiber festzustellen, welche Speicherseiten zurückgegeben werden können. Die Ursache dafür kann auch sein, dass keine VMware Tools installiert oder kein Ballooning-Treiber vorhanden ist. Bootet die VM (zu diesem Zeitpunkt sind noch keine VMware Tools aktiv), ist der Treiber auch nicht produktiv. Des Weiteren kommt diese Technik zum Zuge, wenn das Memory-Ballooning zu langsam ist, um den Speicherbedarf einer VM zu decken. Das Swapping ist generell langsamer als das Ballooning. Es wird eine Swap-Datei pro VM auf dem Volume abgelegt, und zwar im Verzeichnis der virtuellen Maschine. Das Swapping garantiert einer VM eine mindestens verfügbare Speichermenge, damit die VM starten kann.

Dieser Speicherbereich, die Swap-Datei, ist der der VM jetzt neu zugewiesene Speicher und wird beim Einschalten einer VM angelegt. Die Größe variiert je VM und ist die Differenz zwischen dem Reservierungswert und dem zugewiesenen Speicher einer VM.

Eine Besonderheit bei der Verwendung von Memory-Swapping sollten Sie beachten: Im Falle eines Ausfalls des ESXi-Servers werden diese Swap-Dateien nicht mehr automatisch gelöscht. Sie müssen sie dann manuell löschen, wozu das Stoppen und Starten einer VM notwendig wird.

Ein neues wichtiges Feature von vSphere 5 möchten wir hier nicht verschweigen: Es nennt sich *Swap to Host Cache*. Was soll damit erreicht werden? Voraussetzung zur Nutzung der Funktion ist das Vorhandensein einer lokalen SSD-Platte im vSphere-Host. Sie können diese Platte als lokale Swap-Disk für die virtuellen Maschinen einrichten. Der Vorteil liegt auf der Hand: Wenn schon geswappt werden muss, dann erfolgt das auf einer sehr schnellen lokalen Disk.

2.6.8 Best Practices

Nachfolgend finden Sie einige Empfehlungen zum Umgang mit Memory-Reservation, Memory-Limits und Memory-Shares:

- Grundsätzlich sollten Sie den Einsatz von Memory-Overcommitment vermeiden. Es bewirkt auf jeden Fall eine Verlangsamung. Sollte die Überbelegung des Speichers unvermeidbar sein, achten Sie darauf, dass nicht das Memory-Swapping genutzt wird, denn dies reduziert die Performance einer VM deutlich.
- Sie sollten Memory-Shares gegenüber von Memory-Reservierungen den Vorzug geben.
- Beim Einsatz von Memory-Reservierungen sollten Sie ein Minimum an RAM definieren, den eine VM benötigt. Falls eine VM mehr Ressourcen benötigt, so werden diese vom Host, je nach Shares, bis zum eventuell definierten Memory-Limit dynamisch zugewiesen. Beachten Sie außerdem, dass der Einsatz von Memory-Reservierungen die auf einem vSphere-Server zur Verfügung stehenden Speicherressourcen limitiert. Somit können weniger VMs gestartet werden, selbst dann, wenn andere VMs den reservierten Speicherbereich nicht nutzen. Auch kann DRS in seiner Funktion behindert werden, da hier die Ressourcenauslastung des Hosts ein Verschieben von virtuellen Maschinen verhindert.
- Ein Delegieren von Ressourcen-Management erreichen Sie idealerweise durch die Einführung von Resource-Pools. Dabei geben Sie die Grenzen des Resource-Pools an, also die Reservierung und das Limit, um die darin laufenden virtuellen Maschinen von den weiteren Ressourcen eines Hosts zu isolieren.

2.7 Grundlagen der Hardwarevirtualisierung

Wie wir bis jetzt gezeigt haben, wird bei der klassischen Virtualisierung dem Gast eine virtuelle Hardware zur Verfügung gestellt. Das sehen Sie sehr schön, wenn Sie eine virtuelle Maschine booten: Sofort ist der vom Computer bekannte BIOS-Schirm sichtbar. Gehen Sie in die Tiefen des BIOS, stellt sich die virtuelle Maschine wie ein ganz normaler Computer dar. Alle Elemente eines Computers werden in der VM emuliert, seien es der Festplatten-Controller, die Netzwerkkarte oder andere Hardwareelemente. Wie schon beschrieben, handelt es sich um einen »normalen« PC, nur eben virtuell. Der Vorteil besteht darin, dass Sie ein Betriebssystem – die passenden Treiber vorausgesetzt – einfach in die virtuelle Hülle bringen können. Anschließend installieren Sie die Applikation, und fertig ist der virtuelle Server.

Es gibt aber noch andere Varianten von virtuellen Maschinen, die sogenannten *paravirtualisierten VMs*.

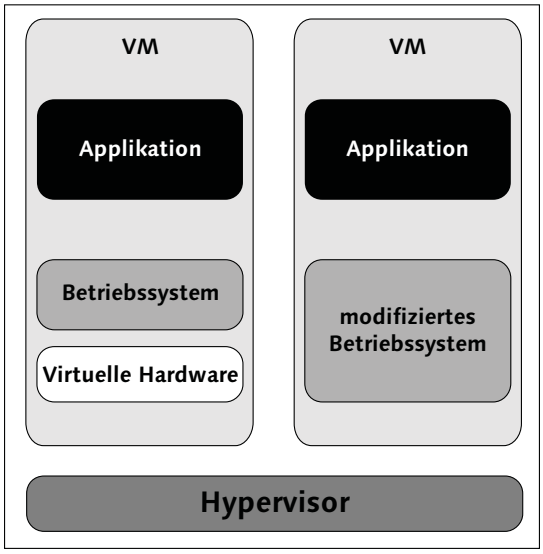


Abbildung 2.15 Unterschied zwischen klassischer und paravirtueller VM

Abbildung 2.15 stellt den Unterschied zwischen beiden Varianten dar. Sie veranschaulicht, dass bei der paravirtuellen Maschine der Layer der virtuellen Hardware fehlt. Dafür existiert eine definierte Schnittstelle. Sie steuert die Ressourcen und den direkten gemeinsamen Zugriff auf die physische Hardware. Ein solcher Mechanismus kann aber nur funktionieren, wenn dem Betriebssystem der Hypervisor »bekannt« ist. Als Ergebnis erhöht sich die Performance der virtuellen Maschine, denn es fehlt die Schicht der virtuellen Hardware. Die direkte Kommunikation zwischen dem Gastsystem und dem Hypervisor wird als *Paravirtualisierung* bezeichnet.

Es gibt aber nur wenige Betriebssysteme, die die Paravirtualisierung unterstützen. Ursache dafür sind die starken Eingriffe, die in dem Kernel erforderlich sind. Einzig einige freie Betriebssysteme unterstützen die Paravirtualisierung. Es handelt sich um verschiedene Linux-Derivate. Der Grund ist relativ logisch, denn der Kernel ist frei, und somit kann – das Wissen vorausgesetzt – der Kernel für die Paravirtualisierung angepasst werden.

Im Gegensatz zu dem kompletten Ansatz, dass der Layer der virtuellen Hardware vollständig entfällt, gibt es Teilansätze, auf die wir hier kurz eingehen wollen. Lassen Sie uns zuvor etwas ausholen: Warum geht VMware diesen Weg, und welche Vorteile bringen diese Technologien?

Der Layer der Hardwarevirtualisierung ist eine Softwarekomponente, die die Hülle für die VM simuliert. Das bedeutet aber im Gegenzug, dass alle Aktionen, die über diese Schicht laufen, Last in diesem Layer erzeugen, bevor die Daten an die eigentliche Hardwarekomponente

gelangen, wie z. B. die Netzwerkkarte. Das erzeugt Rechenzeit auf der CPU und bremst die Performance. Der Ansatz, dem nun gefolgt wird, ist, Teilkomponenten zu paravirtualisieren. Der Vorteil dabei ist, dass nicht der gesamte Kernel angepasst werden muss, sondern dass es reicht, passende »Hardwaretreiber« für das Gastbetriebssystem zur Verfügung zu stellen.

An zwei Stellen gibt es bereits entsprechende Ansätze: bei der Netzwerkkarte VMXNET 3 und bei dem paravirtualisierten SCSI-Adapter (PVSCSI). Auf die Funktionen der beiden Adapter gehen wir an entsprechender Stelle im Kapitel 15, »Virtuelle Maschinen«, im Buch ein.

Lassen Sie uns jetzt die allgemeinen Beschreibungen verlassen und direkt in die Materie vSphere 5 einsteigen.

Mit der aktuellen Version fällt die ESX-Variante weg und mit ihr die Service Console. Es wird nur noch die ESXi-Version geben. Lesen Sie hier nach, wie die Vorgehensweise für die Umstellung auf ESXi ist, wenn Sie diese Version noch nicht einsetzen.

3 ESXi für Umsteiger

Autor dieses Kapitels ist Bertram Wöhrmann, Ligarion, bwoehrmann@ligarion.de

In diesem Kapitel möchten wir auf die Schritte eingehen, die Sie gehen müssen, um den Umstieg zu schaffen, wenn bei Ihnen ESXi noch nicht im Einsatz ist. Strukturelle Unterschiede finden Sie in Kapitel 2, »vSphere-Architektur«.

Die ersten VMware-Versionen brachte der Hersteller nur in der ESX-Variante auf den Markt. Die Service Console war also von Anfang an Bestandteil des Hypervisors, und der Administrator musste sich mit der Console auseinandersetzen. Mit der Version ESX 3.5 stellte VMware zu der Version ESX mit Service Console erstmals auch ESXi vor. Bei dieser Version handelt es sich um ein ESX ohne Service Console. Die Version sollte sicherer werden, und der Patchaufwand sollte sich reduzieren. Bei einer Analyse der von VMware bereitgestellten Patches fällt auf, dass ein Großteil Sicherheitspatches für die Service Console sind. Hier wurde Handlungsbedarf erkannt.

Mit der September 2011 erschienenen Version vSphere 5 hat sich wieder eine signifikante Änderung ergeben: Ab dieser Version wird es nur noch die ESXi-Variante geben. Die Version mit Service Console ist eingestellt worden.

Bevor wir in die Details gehen, lassen Sie uns noch ein wenig auf die Unterschiede der beiden Versionen eingehen. In der Architektur der ersten ESX-Versionen diente die Service Console als Managementschnittstelle zum Virtualisierungskernel. In dieser zusätzlichen Partition hatte der Administrator die Möglichkeit, direkt am Host zu arbeiten und an dieser Stelle z. B. Agenten zu installieren, die weitere Aufgaben übernehmen sollten. Auch wurden an dieser Stelle Managementskripte ausgeführt. Die Analyse von Fehlern findet bei der ESX-Version meistens an dieser Stelle statt. In Abbildung 3.1 sehen Sie sehr gut, wie die einzelnen Komponenten ineinandergreifen. Mit dem Erscheinen des Releases 4.x hat VMware die Service Console in einer eigenen virtuellen Maschine isoliert.

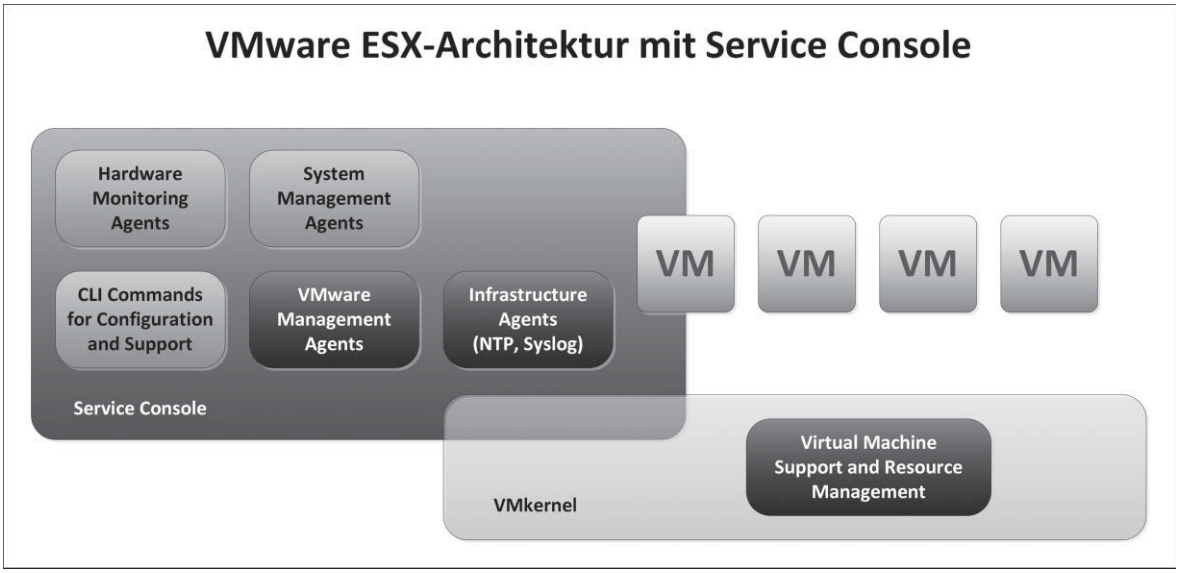


Abbildung 3.1 Architektur VMware ESX

Schauen Sie sich nun Abbildung 3.2 an, und Sie werden sehen, dass VMware dem VMkernel eine Reihe von weiteren Funktionen zugewiesen bzw. in ihn verlagert hat. Der große Vorteil liegt darin, dass in dem System nur die Komponenten verankert sind, die auch für die Virtualisierung notwendig sind. So können Hardwarehersteller ihre Agenten zertifizieren lassen, um sie so in einer speziellen Version dem Kunden zur Verfügung zu stellen. Die digitale Signatur, die VMware in diesen Paketen integriert, macht das Gesamtkonstrukt extrem sicher und sperrt es für willkürlich ausgeführten Code. Jetzt kommt natürlich die Frage auf, wie das System administriert werden soll, wenn keine lokale Konsole mehr vorhanden ist. Haben Sie sich schon länger mit dem Thema auseinandergesetzt, wissen Sie, dass VMware stetig unterschiedliche Remote-Tools etabliert hat. Diese Tools sind universal, soll heißen, sie sind sowohl für ESX als auch für ESXi nutzbar. Dabei stehen Ihnen die vSphere Management Assistance (vMA), die vSphere CLI (vCLI) und das PowerCLI zur Verfügung. Die vMA ist eine Appliance; sie stellt Befehle zur Verfügung, die denen der Service Console stark ähneln. Die beiden anderen Tools sind Komponenten, die auf dem Administrations-PC installiert werden müssen. Sie bieten Befehle, die die Administration einer virtuellen Landschaft ermöglichen. Das PowerCLI ist von allen drei Optionen das Interface mit dem größten Funktionsumfang.

Viele werden bedauern, dass sie keine Software auf dem Host installieren können. Aber vergleichen Sie einmal für die letzte Version die Anzahl der Patches zwischen ESX und ESXi, dann geht dieser Punkt eindeutig an die zweite Variante.

Jeder Administrator weiß, wie kompliziert die Koordination von Auszeiten ist. Sicher benötigen Sie die Auszeit nicht für die Hosts, aber jedes Mal, wenn auch die VMs betroffen sind, wird die Durchführung schon recht aufwendig.

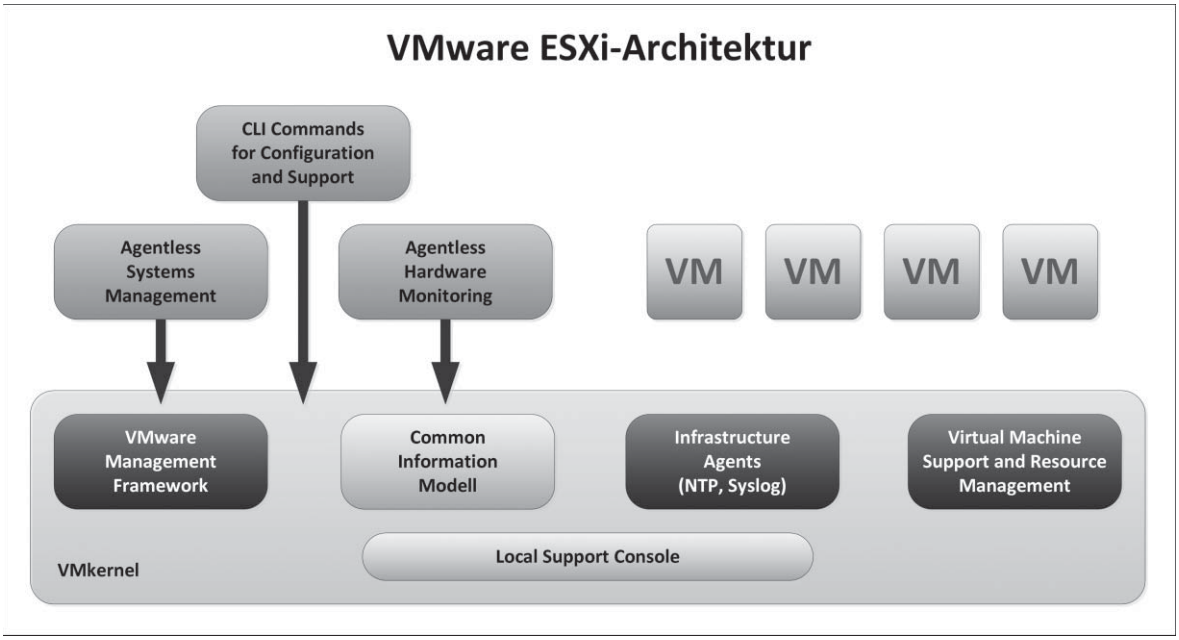


Abbildung 3.2 Architektur ESXi

Damit Sie eine Vorstellung davon entwickeln können, wie sich die beiden Versionen unterscheiden, haben wir eine Tabelle zusammengestellt, die Ihnen einen Überblick über die Unterschiede zwischen den beiden Versionen gibt.

Funktion	ESX	ESXi
Service Console	vorhanden	nicht vorhanden
CLI	Der Host kann über die lokale Konsole oder remote über das vCLI bzw. das PowerCLI administriert werden.	Die Administration erfolgt remote über das vCLI oder das PowerCLI.
geskriptete Installation	Das Skripten von Installationen ist möglich.	Das Skripten von Installationen ist möglich.
Boot vom SAN	Ist möglich mit einer dedizierten LUN pro Server.	Bei der Nutzung von Fibre-Channel, Fibre- Channel over Ethernet und iSCSI besteht Support, solange das in der HCL so vermerkt ist.
serielle Konsole	Mit Hilfe eines seriellen Kabels kann der Host gesteuert werden.	nicht implementiert
SNMP	Wird unterstützt.	Die Unterstützung erfolgt bei allen lizenzierten Versionen.

Tabelle 3.1 Unterschiede zwischen den ESX- und ESXi-Versionen

Funktion	ESX	ESXi
Hardwareinstrumentierung	Über die Service Console möglich.	In der von VMware bereitgestellten ESXi-Version sind Standard-CIM-Provider integriert. Verschiedene Hardwarehersteller liefern ESXi-Versionen mit eigens integrierten CIM-Providern aus.
Patches und Updates	Gepatcht wird über die Service Console oder über den vCenter Update Manager.	Verhält sich wie ein Firmware-upgrade und ist immer kumulativ. Die Arbeiten erfolgen über den vCenter Update Manager.
Webzugriff	Für den Webzugriff gibt es nur experimentellen Support.	Webzugriff ist nicht unterstützt.
Lizenzierung	Es gibt unterschiedliche Lizenzversionen, die verschiedene Funktionen freischalten.	Es gibt unterschiedliche Lizenzversionen, die verschiedene Funktionen freischalten.
Diagnose und Fehlerbehebung	Diese Arbeiten werden entweder über die Service Console oder über die Remote-Tools durchgeführt.	Diese Arbeiten werden über die genannten Remote-Tools durchgeführt. Über den Tech-Support-Mode können Low-Level-Befehle abgesetzt werden.
Jumbo-Frames	voll unterstützt	voll unterstützt
Active-Directory-Integration	Die AD-Integration wird nativ unterstützt.	Die AD-Integration wird nativ unterstützt.

Tabelle 3.1 Unterschiede zwischen den ESX- und ESXi-Versionen (Forts.)

Für die leichtere Analyse im Fehlerfall sollten Sie beim Einsatz von ESXi einen zentralen Server einsetzen, auf dem die Logdateien gesammelt werden.

3.1 Voraussetzungen

Damit der Umstieg auf die aktuelle Version von vSphere 5 nicht zu Problemen führt, sollten Sie sich die Zeit nehmen und die Vorbereitungen ganz genau planen. Lassen Sie uns alle Schritte darstellen, die notwendig sind für diesen Umstieg. Sollten Sie schon einige Schritte im Vorfeld durchgeführt haben, können Sie diese einfach überspringen und mit dem nächsten Abschnitt fortfahren.

Zuallererst ist der vCenter Server an der Reihe. Wie auch bei den vorhergehenden Versionen können Sie mit dem aktuellen vCenter zwar Hosts mit älteren Versionen als die des vCenters administrieren, aber der aktuellste Host gibt auch die Version des vCenters vor. Bei einer ESXi-Landschaft darf ein Add-on für den vCenter Server nicht fehlen, der vCenter Update Manager. Er sorgt dafür, dass Sie den ESX-Host immer auf dem aktuellen Patchlevel halten

können. Sicherlich können Sie ESX-/ESXi-Hosts auch manuell aktualisieren, aber je größer die Landschaft, desto sinnvoller ist der Einsatz dieses Tools.

Es folgt der Aufbau eines Log-Servers. Im Fehlerfall können Sie sich bei ESX-Systemen auf die Service Console einloggen und die Log-Dateien sichten und analysieren. Hier unterscheidet sich der ESXi von seinem Bruder: Die Logs werden nicht unbedingt bootresistent abgelegt; aus diesem Grund sollten Sie einen zentralen Log-Server einrichten, der die Log-Dateien zentral von allen System sammelt und so einen Einstiegspunkt für die zentrale Analyse der Dateien gibt. Auf der vCenter-DVD findet sich der VMware Syslog Collector; er kann sich um diese Aufgabe kümmern.

Last but not least müssen Sie sich um das Management für die ESXi-Systeme kümmern. Die Service Console gehört ja der Vergangenheit an, also müssen Sie auf andere Alternativen von VMware zurückgreifen. Passende Tools gibt es schon länger, aber in reinen ESX-Umgebungen sind sie selten zu finden.

Sie können sich aussuchen, mit welchem Tool Sie arbeiten. Da gibt es zum einen das vCLI. Die Software wird lokal auf einem PC installiert und stellt Service-Console-ähnliche Befehle zur Verfügung. Ähnliche Befehle werden durch die vSphere Management Assistant (vMA) zur Verfügung gestellt. Es handelt sich hierbei um eine zentrale Komponente, auf die per SSH-Client zugegriffen wird. Von der Konsole aus können Sie dann die Befehle zu den Hosts absetzen. Als letzte, sehr populäre Möglichkeit können Sie das PowerCLI nutzen. Sie hat zwar eine neue eigene Syntax, aber hat seit der Einführung einen Zuwachs an Befehlen erhalten, der zeigt, wohin der Weg geht. Nebenbei lässt sich das Tool auch zur Automatisierung nutzen. Das erste und letzte Tool sind reine Client-Komponenten, die auf dem Gerät des Administrators installiert werden müssen. Setzen Sie diese Softwarepakete ein, benötigen Sie Mechanismen, um die Softwarepakete aktuell zu halten, damit die Administratoren auch die aktuellsten Hosts allumfänglich betreiben können.

Bedenken Sie, dass der Betrieb mit den neuen Tools Erfahrungen sammeln muss, damit ein reibungsloser Ablauf gewährleistet ist. Sie können die Tools auch schon im Vorfeld einsetzen und damit die ESX-Hosts administrieren.

Mit vSphere 5 hat VMware noch ein Tool bereitgestellt, den VMware ESXi Dump Collector. Er ist dafür zuständig, Memory-/vmkernel-Dumps von Hosts zentral zu sammeln. Zu all diesen Themen finden Sie selbstverständlich ausführliche Abschnitte in diesem Buch. Lassen Sie uns nun den Exkurs verlassen und mit dem eigentlichen Migrationspfad fortfahren.

3.2 Migration vCenter Server

Vor dem Beginn der eigentlichen Migration sind unterschiedliche Arbeiten durchzuführen, damit die Migration auch erfolgreich abgeschlossen werden kann. Wie auch bei den Versionen zuvor beginnen die Arbeiten mit dem vCenter Server. Lassen Sie uns die einzelnen

Schritte hier näher betrachten. Zur Orientierung möchten wir Ihnen den folgenden Ablauf an die Hand geben.

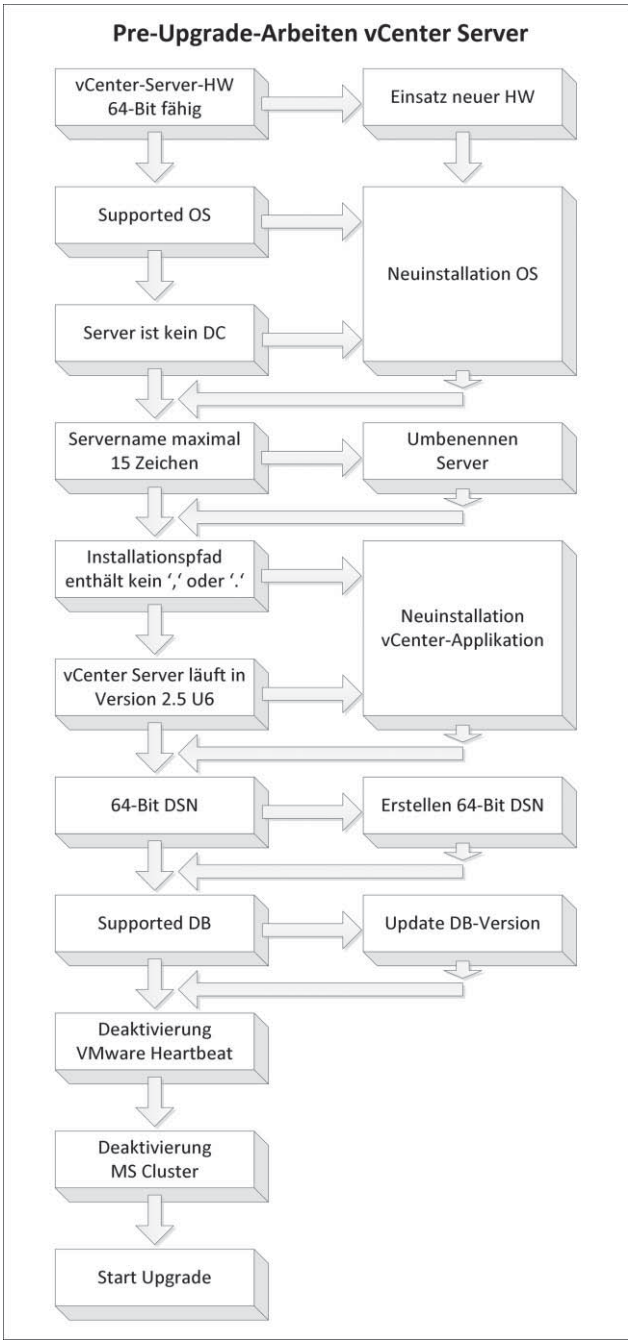


Abbildung 3.3 Upgradevorbereitung vCenter Server

Zu Beginn der Arbeiten steht die Überprüfung der eingesetzten Hardware an. Diese muss 64-bit-fähig sein. Empfehlenswert wären zwei CPUs und 16 GB Arbeitsspeicher. Ein aktuell unterstütztes Betriebssystem ist genauso selbstverständlich wie eine Funktionsrollentrennung. Die Datenbank für das vCenter können Sie selbstverständlich auch auf der Hardware installieren, aber z. B. ein AD hat auf dem vCenter-Server nichts zu suchen. Die Länge des Server-Namens ist ebenfalls zu berücksichtigen, sie darf 15 Zeichen nicht überschreiten. Die Anzahl der Upgradeschritte ergibt sich letztendlich aus dem Versionsstand des bei Ihnen eingesetzten Management-Servers. Erst ab der Version 2.5 Update 6 kann ein Upgrade erfolgen. Es kann darum notwendig sein, das Upgrade in mehreren Schritten durchzuführen. Beachten Sie dabei bitte die Upgrademöglichkeiten von den unterschiedlichen älteren Versionen. Ein weiterer Stolperstein ist der genutzte Installationspfad: Er darf die Zeichen ».« und »,« nicht enthalten.

Kommen wir zur eingesetzten Datenbank und zum Zugriffs-Client. Beides sollte in der Supportmatrix von VMware zu finden sein. Falls die bei Ihnen eingesetzte Version nicht unterstützt wird, sollten Sie im Vorfeld die Datenbankversion aktualisieren. Erfahrungsgemäß sollten solche Arbeiten entzerrt stattfinden, das heißt, dass Sie die Upgradearbeiten von vCenter und Datenbank zeitlich entzerren. Passt Ihre Version zum neuen Management-Server, ist nur noch der ODBC-Eintrag zu kontrollieren, er wird in der 64-Bit-Version benötigt. Als letzter Schritt vor dem Upgrade sind jetzt noch Applikationen zur Erlangung einer Hochverfügbarkeit des vCenter Servers zu deaktivieren.

Jetzt ist es endlich so weit – Sie haben alle Hürden genommen. Starten Sie nun mit der DVD den Upgradevorgang des vCenters. Sichern Sie zuerst die Datenbank(en), und starten Sie dann den Updateprozess. Der Ablauf ähnelt dem der Installation. Nähere Informationen finden Sie in Abschnitt 6.3.4. Ist der Prozess durchgelaufen, arbeiten Sie bereits mit der neuen VMware-vCenter-Version und haben den ersten Schritt bereits, hoffentlich erfolgreich, abgeschlossen. Nutzen Sie ruhig die beim Update bereitgestellte Trial-Lizenz von 60 Tagen. Sie gibt Ihnen die Möglichkeit, alle Features zu nutzen, die VMware zur Verfügung stellt. Sind alle Upgradearbeiten abgeschlossen, sollten Sie abschließend aber Ihren Lizenz-Key einspielen, damit Ihr System nicht nach 60 Tagen ausläuft. Bei der erstmaligen Verbindung mit dem neu installierten Server erhalten Sie automatisch, wie gehabt, den aktuellen vSphere-Client, der auch wieder abwärtskompatibel ist.

Es folgt die Bereitstellung der neuen Management-Interfaces, dabei ist die Wahl des Tools Ihnen überlassen. Nutzen Sie die Lösung, mit der Sie Ihre Arbeiten optimal durchführen können. Sie können auch dem Betrieb eine vMA geben und den Integratoren das PowerCLI zur Verfügung stellen. Bedenken Sie bei der Auswahl der Managementkomponenten, dass es wichtig ist, immer die aktuellen Versionen zu nutzen. Das kann Auswirkungen auf das Endgerät des Administrators haben. Kommt die vMA zum Einsatz, benötigen Sie nur einen SSH-Client, mehr Anpassungen sind auf dem Endgerät nicht vorzunehmen. Bei den anderen Bestandteilen wie vCLI bzw. PowerCLI sind Komponenten auf dem Endgerät zu installieren. Das erweist sich unter Umständen als Herausforderung. Letztendlich hängt das davon ab, wie

in Ihrem Unternehmen mit solchen Anforderungen umgegangen wird. Setzten Sie eine Softwareverteilung ein, dann sind bei jedem Update der Tools neue Applikationspakete zu schnüren.

Zu diesem Zeitpunkt haben Sie die eigentlichen Vorbereitungen abgeschlossen, nicht nur durch das bloße Lesen, sondern auch durch das Arbeiten an der Konsole. Auch wenn das vCenter in der aktuellen Version jetzt bereitsteht, sind Sie mit den Arbeiten noch nicht fertig. Auch für die Nacharbeiten möchten wir Ihnen eine kleine Grafik zur Übersicht zeigen.

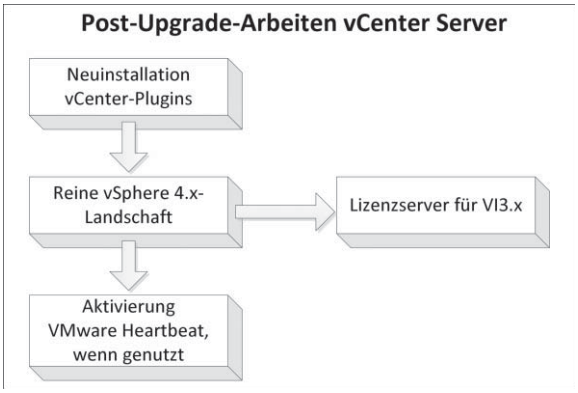


Abbildung 3.4 Nacharbeiten für das vCenter-Upgrade

Sollte Sie den Wunsch haben, die gesamte Funktionalität wie vor dem Upgrade zu nutzen, dann sollten Sie sich an die Nacharbeiten machen. Schon beim Einlegen der DVD haben Sie gesehen, dass der Datenträger zusätzlich Applikationen in der aktuellen Version enthält. Diese sollten Sie jetzt ebenfalls aktualisieren, um die volle Funktionalität wieder zur Verfügung zu stellen. Wählen Sie die Komponenten nacheinander aus, und bringen Sie sie so auf den neuesten Stand.

Hinweis

Auch wenn Sie andere Patch-Management-Tools einsetzen, für das Patchen der ESXi-Hosts können wir Ihnen den Update Manager nur ans Herz legen. Planen Sie eine Einführung, wenn er bei Ihnen nicht sowieso schon zum Einsatz kommt.

Nennen Sie auch noch ESX 3.x-Hosts Ihr Eigen, dann kommen Sie an der Bereitstellung von dem Lizenz-Server für diese Landschaft nicht vorbei. Optimalerweise installieren Sie den Server auf der Maschine, die das vCenter trägt, direkt mit. Die passenden Quellen finden Sie in der neuesten Version des Management-Servers 2.5 Update 6 oder später.

Zu guter Letzt sollten Sie eventuell zum Einsatz kommende Hochverfügbarkeitslösungen für das vCenter wieder in Betrieb nehmen. Auch hier ist darauf zu achten, dass das Release der Applikation mit den unterliegenden Komponenten harmoniert. Andernfalls könnte es im Falle eines Support-Calls ein böses Erwachen geben, wenn der Supporter Sie abweist.

Hinweis

Microsoft Clustering für den vCenter-Server wird nicht mehr supportet.

Ihre derzeit bestehende Landschaft ist jetzt so weit vorbereitet, dass Sie sie wieder in den Ihre Ihre derzeit bestehende Landschaft ist jetzt so weit vorbereitet, dass Sie sie wieder in den Regelbetrieb übergeben können. Die Host-Arbeiten können ab jetzt durchgeführt werden. Diese Arbeiten können Sie nach und nach in Angriff nehmen. Planen Sie auch hier akribisch, um eine ungeplante Unterbrechung des Betriebs zu verhindern.

3.3 Migration ESX-Hosts

Nun können Sie mit der Planung der Aktualisierung der Hosts beginnen. Auch hier möchten wir mit einem kleinen Schaubild die Abhängigkeiten der Schritte untereinander darstellen. Vergessen Sie auch hier nicht die Voraussetzungen für die Installation oder das Update der Hosts.

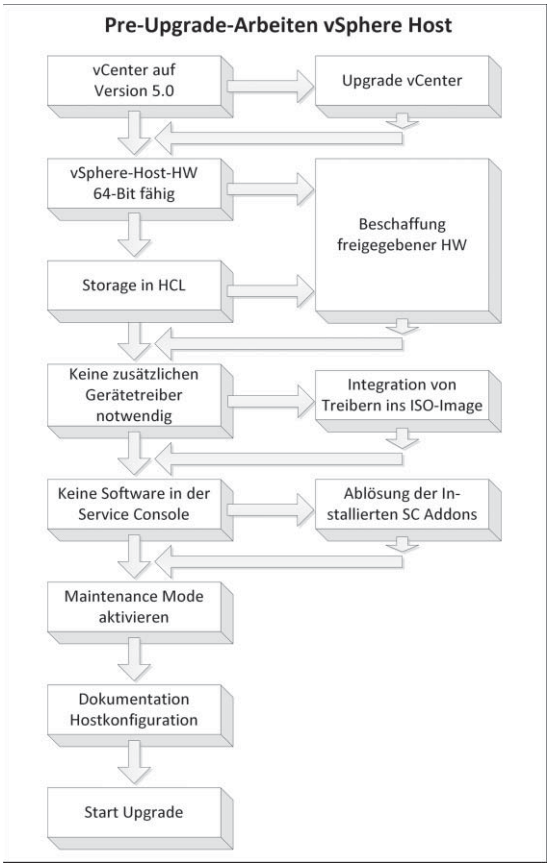


Abbildung 3.5 Upgradeablauf der Host-Migration

Wir wollen hier auf den Upgradepfad für die Virtualisierungs-Hosts eingehen. Wir gehen in diesem Fall davon aus, dass bei Ihnen ESX-Hosts zum Einsatz kommen. Die Aktualisierung von ESX nach ESXi kann mit dem vCenter Update Manager erfolgen.

Die erste Voraussetzung haben wir ja bereits im Abschnitt zuvor beschrieben, also sollte der erste Schritt für Sie schon erledigt sein. Bevor Sie nur daran denken, den Datenträger zu nutzen, sollten Sie Ihre zu aktualisierende Landschaft an der Hardware Compatibility List (HCL) spiegeln. Sind alle Ihre Komponenten dort gelistet, sind Sie schon einen großen Schritt weiter. Ein ganz wichtiger Punkt im Gegensatz zur ESX-Version ist, dass Sie während der Installation keine zusätzlichen Treiber einbinden können. Kommt sehr aktuelle Hardware zum Einsatz, ist es eventuell nicht möglich, ESXi zu installieren. Sie müssen dann warten, bis der Hardwarehersteller oder VMware ein aktualisiertes Installations-Image zur Verfügung stellt. Kritisch sind dabei Treiber für die Storage- und Netzwerkanbindung.

Installationstrick

Wird der Storage-Adapter sauber erkannt, so dass eine Installation grundsätzlich möglich wäre, können Sie sich mit einem Trick behelfen. Wird während der Installation die Netzwerkkarte nicht erkannt, dann bauen Sie kurzerhand eine ältere, unterstützte Karte in den Server ein, nehmen den Server über diese in Betrieb und patchen ihn anschließend. Sind die Treiber dann aktuell, können Sie die Karte wieder entfernen.

Haben Sie ein Augenmerk darauf, welche zusätzliche Software in der Service Console der bestehenden Server installiert ist, und schauen Sie, wie Sie das nach dem Umstieg abbilden können. Für jede zusätzlich installierte Software und für jedes bereitgestellte Skript müssen Sie nun eine Möglichkeit haben, die Funktionen über andere Wege wieder anzubieten. Diese Begutachtung sollten Sie frühzeitig angehen. Beschäftigen Sie sich nicht erst während des Upgrades mit dem Thema, es kann sich als ein sehr langwieriges herausstellen.

Sind diese Aufgabenstellungen gelöst, können Sie mit dem eigentlichen Updateprozess beginnen. Evakuieren Sie den Host, und aktivieren Sie danach den Maintenance-Modus. Entfernen Sie den Host dann aus dem Cluster, wenn er dort Mitglied ist. Vergessen Sie bitte nicht, die gesamte Konfiguration des Hosts fein säuberlich zu dokumentieren, damit Sie die Konfiguration später übernehmen und auf dem neu bereitgestellten Host einpflegen können.

Starten Sie nun die Neuinstallation des Hosts, vergeben Sie ein gültiges Passwort, und konfigurieren Sie die IP-Parameter. Abschließend sollten Sie den Lockdown-Modus aktivieren. Er sorgt dafür, dass nur der »root«-User sich an der Konsole anmelden kann und nur das vCenter mit dem Host kommuniziert. Alle weiteren möglichen Optionen sind deaktiviert.

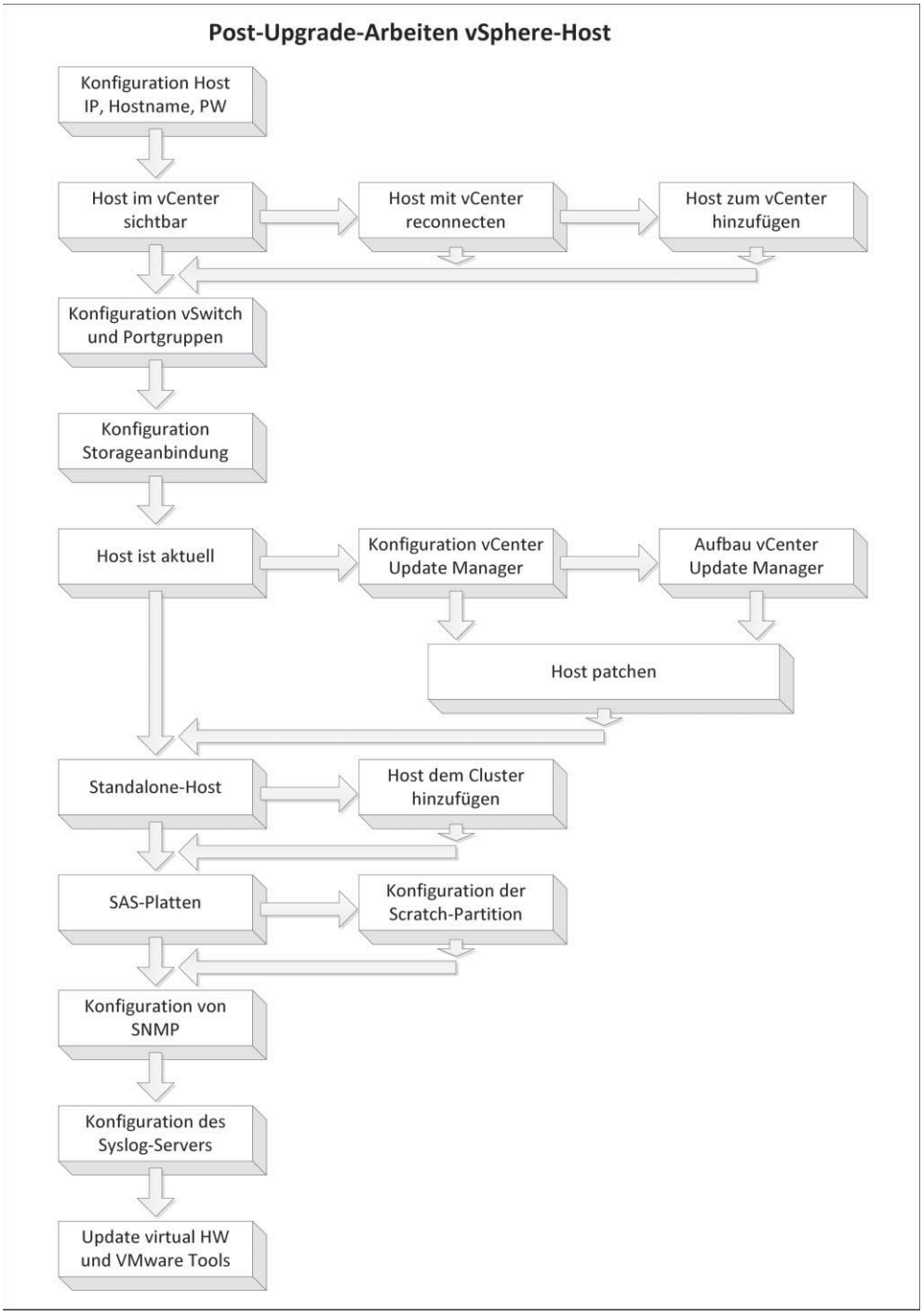


Abbildung 3.6 Nacharbeiten auf dem Host nach der Bereitstellung

Ist der Host fertig installiert, können Sie im vCenter einen Reconnect durchführen und die Konfigurationsnacharbeiten durchführen. Es gibt leider einen kleinen Wermutstropfen, denn trotz Enterprise-Plus- oder Evaluation-Lizenz und trotz der damit freigeschalteten Hostprofile können Sie nicht einfach die Konfigurationen der »alten« ESX-Hosts übernehmen. Sie müssen den ersten Host händisch konfigurieren und können anschließend das dann erstellte Hostprofil für alle weiteren Hosts nutzen. Aus diesem Grund sollten Sie auch vor dem Upgrade eines Hosts die Konfiguration peinlich genau dokumentieren.

Richten Sie das Netzwerk ein, und verbinden Sie den Host mit dem Storage. Vergessen Sie nicht, mit dem Update Manager die letzten ESXi-Patches einzuspielen, bevor Sie den Host wieder in den Cluster aufnehmen. Es fehlt noch die Anbindung an den zentralen Dump- und Logserver, damit auch im Fehlerfall eine einfache Analyse stattfinden kann.

Ein Großteil der Nacharbeiten nach dem Upgrade sollte Ihnen bekannt sein, wenn Sie schon ein Upgrade mitgemacht haben. Es sind die VMware Tools zu aktualisieren, und auch dieses Mal gibt es wieder eine neuere Version der virtuellen Hardware. Diese Aktionen sind ebenfalls wieder durchzuführen. Vergessen Sie nicht, nach der Beendigung der Konfigurationsarbeiten des Hosts diese Einstellungen zu sichern und an geeigneter Stelle abzulegen.

Ich hoffe, wir konnten Ihnen hier die einzelnen Schritte für einen Umstieg darlegen, und Sie haben nun alle Mittel an der Hand, um diesen Umstieg zu meistern. Wir sind nicht in voller Detailtiefe an dieser Stelle eingestiegen, aber wir gehen auf alle Themen im Verlaufe dieses Buches noch näher ein. Alle Informationen zur Installation des Hosts erhalten Sie in Abschnitt 6.1, die Angaben zum Update Manager finden sich in Abschnitt 12.1.1. Sollten Sie Näheres über die Arbeiten zu den virtuellen Maschinen nachlesen wollen, schauen Sie bitte in Kapitel 15 nach.

vMotion und das erst mit VI3.5 hinzugekommene Storage vMotion werden täglich über zehntausend Mal von VMware-Kunden weltweit genutzt und haben sich als zuverlässige und enorm nützliche Funktionen etabliert.

4 vMotion und Storage vMotion

Autor dieses Kapitels ist Dennis Zimmer, opvizor GmbH – opvizor.com, virtuellemaschinen@email.de

vMotion und Storage vMotion haben zwar eine unterschiedliche Funktion, allerdings sind Teile der Technologie überlappend, daher passen die beiden vSphere-Funktionen gut in ein Kapitel. Beide Technologien sind proaktiv, das heißt, vMotion wird zum Migrieren einer virtuellen Maschine zwischen funktionierenden ESX-Hosts verwendet, und Storage vMotion migriert die Daten der virtuellen Maschinen zwischen funktionstüchtigen Datastores. Beide vSphere-Features sind nicht mehr möglich, wenn eine Quelle oder ein Ziel ausgefallen ist.

Daher dienen vMotion und Storage vMotion der höheren Ausfallsicherheit, da sie Wartungsfenster an den Hosts und Datastores ohne Ausfall überbrücken können; es sind aber keine Funktionen zur Steigerung der Hochverfügbarkeit, was oft falsch verstanden wird.

4.1 vMotion

Von vMotion, der Live-Migrationsfunktion von VMware, hat mit Sicherheit bereits jeder Leser gehört, daher fasse ich mich kurz: vMotion ist die Funktion, aktive virtuelle Systeme von einem ESX-Host auf einen anderen zu verschieben, ohne dass die virtuelle Maschine oder deren Dienste ausfallen.

vMotion, oder auch Hot Migration, steht im Gegensatz zur Cold Migration, die nur bei ausgeschalteter VM möglich ist und eine gleichzeitige Migration zwischen Host-Systemen und Datastores zulässt. Außerdem entfällt bei der Cold Migration die sehr restriktive Notwendigkeit ähnlicher Host-Prozessoren. Zu guter Letzt unterstützt Cold Migration die Migration von VMs zwischen Datacenter-Objekten, während vMotion nur innerhalb eines Datacenters erlaubt ist. Dies ist mittlerweile sogar so ausgefeilt, dass es auch bei Tests auf Messen mit Hunderttausenden von vMotion-Migrationen nie zum Verlust einer VM oder von deren Diensten kam. Allerdings ist nicht jede virtuelle Maschine für vMotion geeignet, was ich im Laufe des Kapitels näher erläutern werde.

4.1.1 Funktionsweise

Denkt man genauer über vMotion nach, so muss man gestehen, dass der Vorgang simpel, aber genial ist, und er stellt die Lösung der Ausfallsicherheit von Systemen während eines regelmäßigen Problems dar – Wartungen am Host. Außerdem erkennen Sie durch vMotion sehr leicht, wie sinnvoll die Unabhängigkeit und Trennung der Hardware vom Betriebssystem und von der Applikation wirklich ist.

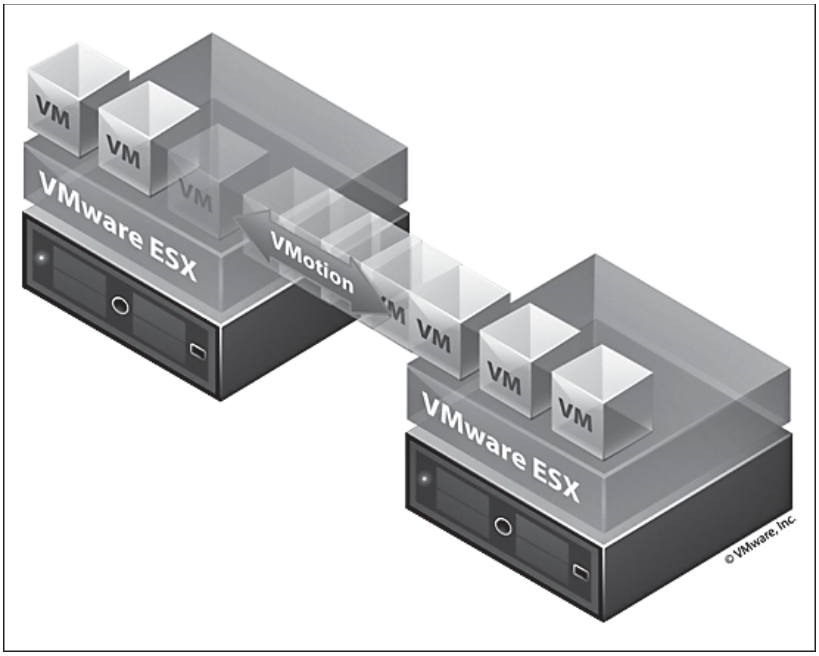


Abbildung 4.1 vMotion-Migration aktiver virtueller Maschinen zwischen ESX-Hosts

Doch schauen wir uns den vMotion-Prozess aus Sicht der virtuellen Maschine im Detail an:

1. Überprüfung, ob die Quell-VM auf dem gewünschten Ziel-Server betrieben werden kann
2. Erstellung einer zweiten VM als Prozess auf dem Zielsystem inklusive der Ressourcenreservierung
3. Anlage eines Hauptspeicher-Checkpoints, das heißt, alle Änderungen der Quell-VM werden in einen zusätzlichen Speicherbereich geschrieben
4. Übertragung des Hauptspeicherinhalts des Checkpoints zur Ziel-VM
5. Wiederholung des Checkpoint/Checkpoint-Restore-Vorgangs, bis nur noch kleinste Änderungsmengen im Hauptspeicher der Ziel-VM ausstehen
6. CPU-Stop der Quell-VM
7. Übertragung der letzten Hauptspeicheränderungen zur Ziel-VM innerhalb von Millisekunden

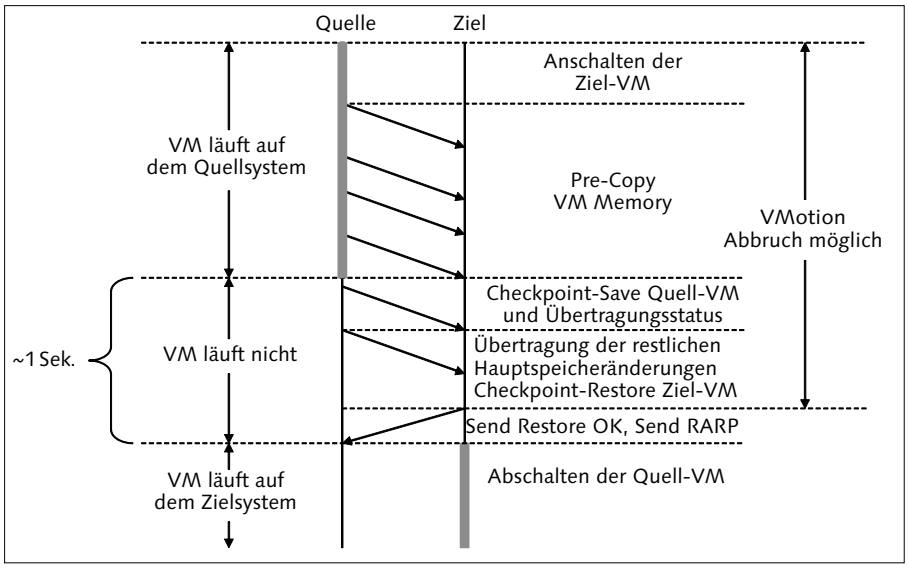


Abbildung 4.2 vMotion-Vorgang aus Sicht der virtuellen Maschine

8. Abschluss des vMotion-Vorgangs und Senden des Reverse-ARP-Pakets an die physischen Switches (wichtig: NOTIFY SWITCHES muss in den Eigenschaften der virtuellen Switches aktiviert sein); Übernahme des Festplattenzugriffs vom Ziel-ESX
9. Abschalten der Quell-VM – Löschung des VM-Prozesses auf dem Quell-ESX

   Noch eine kurze Anmerkung dazu, was die vMotion-Checkpoints überhaupt umfassen bzw. wofür sie stehen:

   - alle Geräte inklusive Status
   - CPU-Register
   - Hauptspeicherinhalt
   - Serialisierung des Status zur Übertragung über das Netzwerk

Wie Sie sehen, besteht vMotion hauptsächlich aus der Übertragung des Hauptspeichers von einem ESX-Server auf den anderen mit einer anschließenden Benachrichtigung des physischen Netzwerks über die neue Schnittstelle, über die die VM neuerdings erreichbar ist. Das Gastsystem bekommt davon natürlich nichts mit.

Folgend ein Berechnungsbeispiel für die Hauptspeicherübertragung:

Pre-Copy Iteration	zu übertragender Hauptspeicher	verbrauchte Zeit zur Übertragung	Hauptspeicheränderung während der Übertragung
1	2.048 MB	16 Sekunden	512 MB
2	512 MB	4 Sekunden	128 MB

Tabelle 4.1 Hauptspeicherkopie während vMotion

Pre-Copy Iteration	zu übertragender Hauptspeicher	verbrauchte Zeit zur Übertragung	Hauptspeicheränderung während der Übertragung
3	128 MB	1 Sekunde	32 MB
4	32 MB	0,25 Sekunden	8 MB
5	8 MB	vMotion-Abschluss, da die Restübertragung in ~0,06 Sekunden erfolgt	

Tabelle 4.1 Hauptspeicherkopie während vMotion (Forts.)

Wie Sie in Tabelle 4.1 sehen, erfolgt die Kopie des Hauptspeichers sukzessive in mehreren Schritten, bis ein CPU-Stopp möglich ist, der nicht zum Ausfall des Systems führt.

An vMotion sind mehrere Komponenten beteiligt, die jeweils Teile des Prozesses steuern. vCenter führt dabei die ersten Konfigurationsprüfungen durch und startet den Prozess über die vpxa- und hostd-Komponenten, indem eine Pseudo-VM als Container auf dem Ziel-Host erstellt wird. Das vMotion-Modul startet den eigentlichen vMotion-Vorgang und kontrolliert die Datenübertragung.

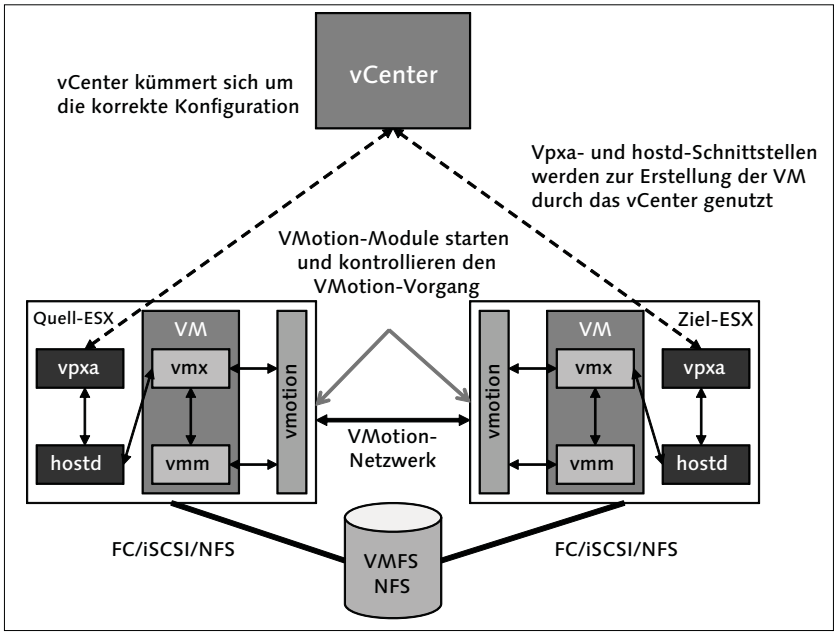


Abbildung 4.3 Beteiligte Komponenten bei vMotion

Da vCenter nur den Prozess validiert und startet, aber nicht in die Datenübertragung involviert ist, wird ein aktiver vMotion-Prozess zu Ende geführt, selbst wenn das vCenter abstürzen sollte. Es kann allerdings passieren, dass vCenter danach die Quell-VM weiterhin in der Datenbank hat und noch nichts vom neuen Ort der Ziel-VM weiß. In diesem Fall hilft ein Restart des Management Agents oder ein Disconnect/Connect des ESX-Hosts im vCenter.

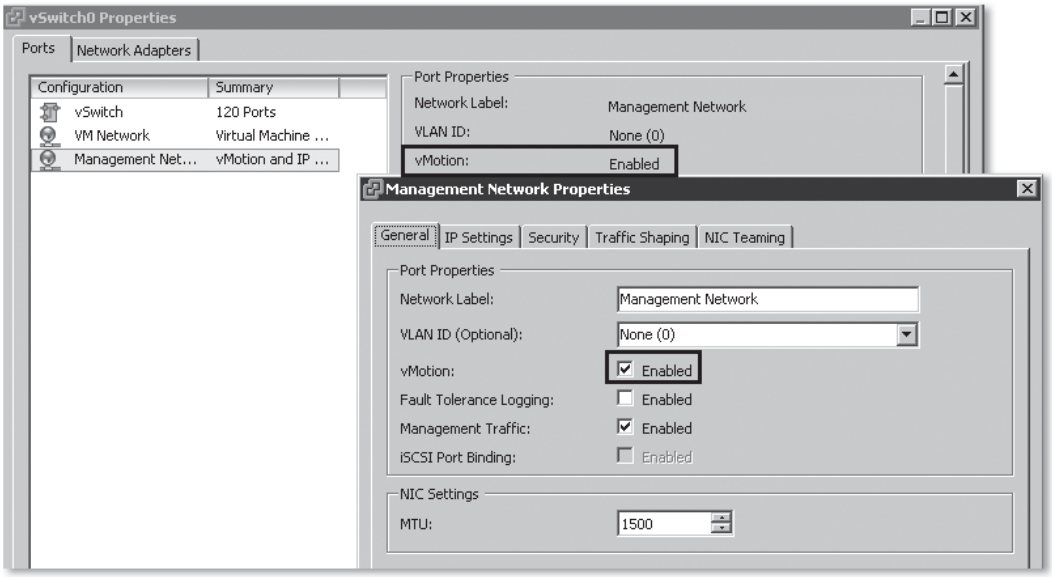


Abbildung 4.4 Ein VMkernel-Adapter muss für vMotion aktiviert werden, damit vMotion funktionieren kann.

Das zu nutzende vMotion-Interface muss vom Administrator angelegt werden und setzt auf dem VMkernel-Port auf, das heißt, in den Eigenschaften des VMkernel-Ports muss vMotion auf ENABLED gesetzt werden.

4.1.2 Voraussetzung

Da es sich bei vMotion um einen Eingriff in eine aktive virtuelle Maschine handelt, die ihrerseits davon keine Kenntnis hat, müssen verschiedene Gegebenheiten vorhanden sein, damit der Prozess ohne Ausfall und Probleme ablaufen kann:

- CPU-Kompatibilität
- vMotion-Interface (mindestens 1-GBit-Adapter)
- gemeinsamer, zentraler Massenspeicher
- gleich benannte virtuelle Portgruppen
- ausreichende Ressourcen auf dem Ziel-Host
- mindestens vSphere-Essentials-Plus-Lizenz auf den entsprechenden ESX-Hosts

Ein richtiges Problem stellt zumeist nur die CPU-Kompatibilität dar, da die Server-Infrastrukturen in vielen Unternehmen nach wie vor organisch wachsen und nicht jegliche Server-Hardware über gleiche Komponenten verfügt. Ob eine virtuelle Maschine zwischen zwei ESX-Servern migriert werden kann, ist leicht festgestellt, da das vCenter gegebenenfalls bereits vor der eigentlichen Migration den Prozess mit einer entsprechenden Fehlermeldung abbricht.

CPU-Kompatibilität

Das Problem der CPU-Kompatibilität ist ganz leicht zu erklären: Stellen Sie sich vor, eine virtuelle Maschine wird auf einem ESX-Host mit AMD-CPU und SSE3-Funktion gestartet. Da VMware ESX ein Virtualisierer ist, sieht das Gastbetriebssystem die CPU-Funktionen im Standard komplett, und das Betriebssystem kann sich den Gegebenheiten anpassen und durch Zusatztreiber die Multimediafunktion gut nutzen.

Würde diese virtuelle Maschine nun einfach auf einen Host übertragen, dessen CPU nur SSE2 unterstützt, so würde das Gastbetriebssystem trotzdem weiter die SSE3-Funktion nutzen wollen. Es käme zwangsweise zu Problemen bis hin zum Absturz. Während diese Schwierigkeit durch das sogenannte CPU-Masking in den Griff zu bekommen ist, wäre es bei größeren CPU-Unterschieden ein unlösbares Problem, z. B. der Wechsel von einer AMD- auf eine Intel-CPU oder der Wechsel von einer 64-Bit- auf eine 32-Bit-CPU.

Da der ESX-Server nicht voraussagen kann, welche CPU-Instruktion die virtuelle Maschine, oder besser das Gastbetriebssystem, nutzt und noch nutzen wird, muss der Anwender sich darum kümmern, entweder gleiche CPUs zu verwenden oder ein entsprechendes Masking einzurichten.

Welche Funktionen die eingebaute CPU hat, finden Sie mit dem VMware-eigenen *CPU Identification Utility* heraus, das die vMotion-Kompatibilität, EVC und den 64-Bit-Support anzeigt: *http://www.vmware.com/download/shared_utilities.html*.

Welche CPUs miteinander kompatibel sind, erfahren Sie übrigens in den VMware-Knowledge-Base-Artikeln 1991 (Intel) und 1992 (AMD):

- Intel: *http://kb.vmware.com/kb/1991*
- AMD: *http://kb.vmware.com/kb/1992*

Es existiert beim Upgrade von VI3.x auf vSphere leider noch ein sehr ernstes Problem bezüglich des CPU-Maskings, das unter VI3.x oft automatisch in der Konfiguration der virtuellen Maschinen gesetzt wird. Nach dem Upgrade lassen sich manche virtuelle Maschinen dann nicht mehr per vMotion migrieren, und Sie erhalten eine Fehlermeldung. Dieses Problem ist beim Upgrade von vSphere 4 auf vSphere 5 bisher nicht bekannt. Die Lösung ist recht einfach, da nur das CPU-Masking auf Default per Reset All to Default in den CPU Identification Mask-Eigenschaften der virtuellen Maschinen ausgewählt werden muss. Ärgerlich ist, dass die VM abgeschaltet werden muss, um diese Einstellung vorzunehmen. Den dazugehörigen Knowledge-Base-Artikel finden Sie hier:

http://kb.vmware.com/kb/1011294.

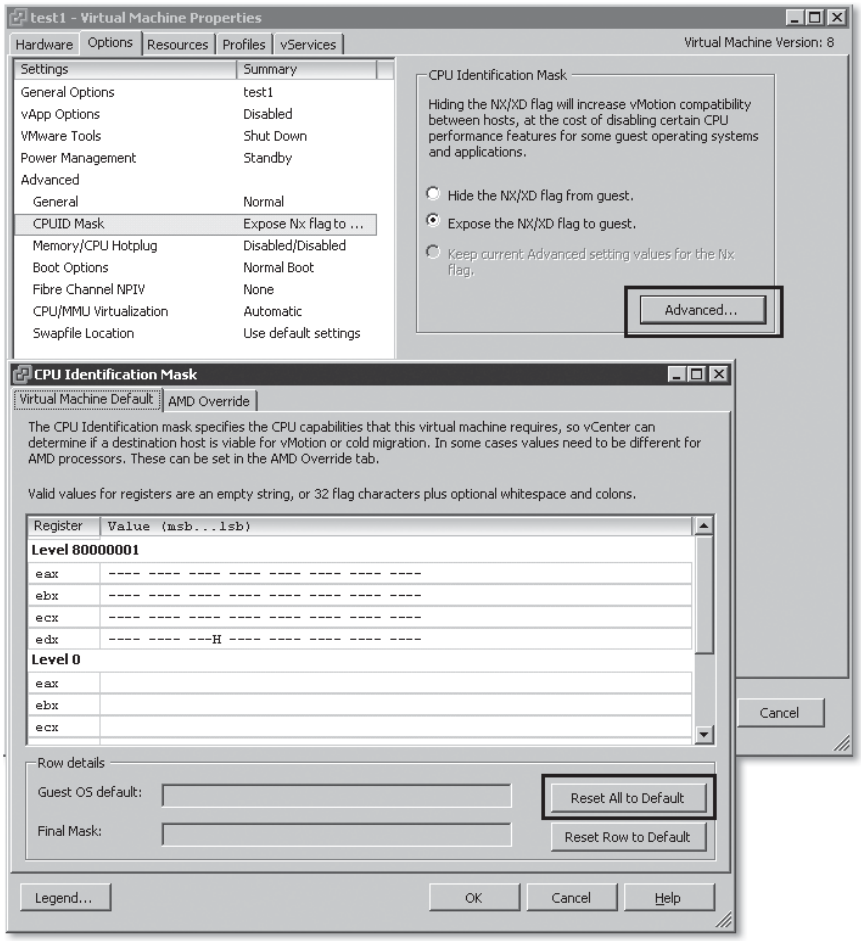


Abbildung 4.5 CPU-Masking zurücksetzen in den Eigenschaften der VM

CPU-Masking und EVC

In den Eigenschaften einer virtuellen Maschine finden Sie unter den Optionen den Punkt CPUID Mask, um eine *abgeschaltete* VM CPU-Funktion auszublenden. Durch diese Ausblendung von CPU-Features erhöhen Sie die vMotion-Kompatibilität zwischen ESX-Hosts mit unterschiedlichen CPU-Generationen (siehe Abbildung 4.6).

Die Standardmöglichkeit ist das Verstecken des Non-Execution-Bits, das nur von neueren CPUs unterstützt wird (Hide the NX/XD flag from guest). Wird dieses aktiviert, so kann eine virtuellen Maschine zwischen ESX-Servern migriert werden, wobei es egal ist, ob die Prozessoren über die NX-Funktion verfügen oder nicht, es sei denn, es sind noch weitere CPU-Instruktionen auf den CPUs unterschiedlich, die nicht ausgeblendet werden (siehe Abbildung 4.7).

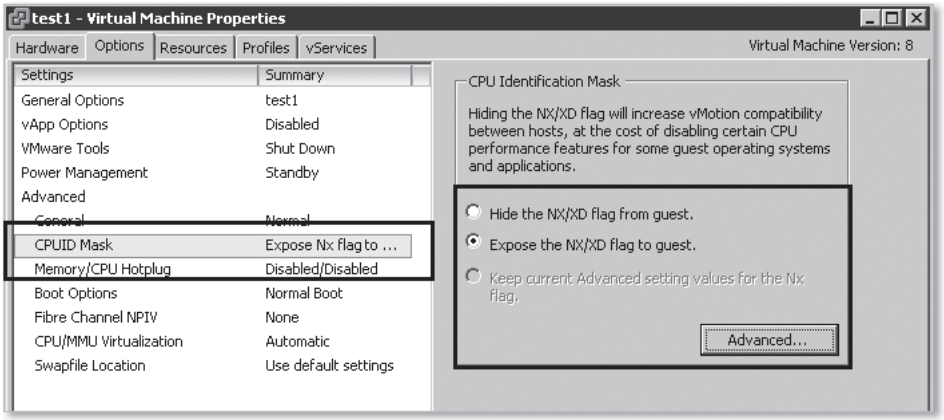


Abbildung 4.6 In den Eigenschaften der virtuellen Maschine beeinflussen Sie das CPU-Masking.

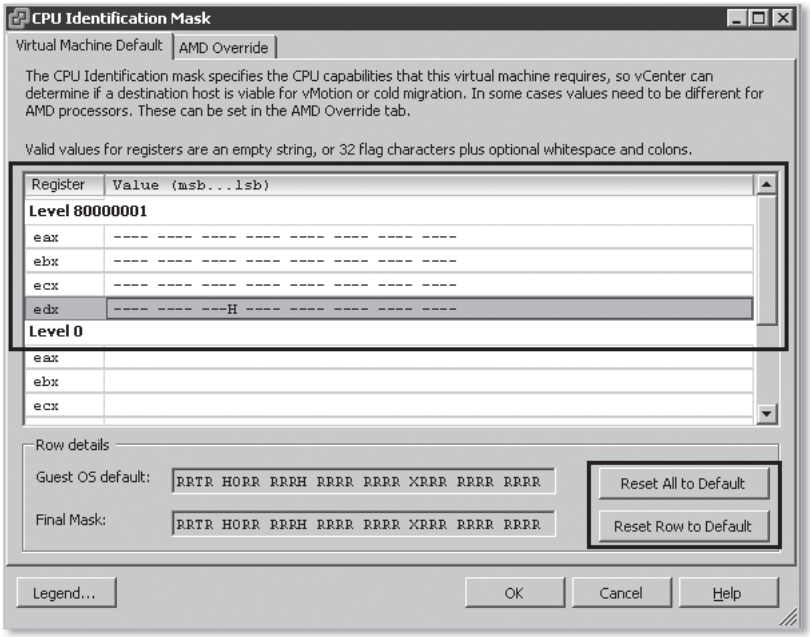


Abbildung 4.7 Eine direkte Ausblendung bestimmter Funktionen ist für Intel- und AMD-CPUs möglich.

Reicht das Non-Execution-Bit nicht aus, so ist es möglich, CPU-Hersteller-spezifisch Anpassungen zu machen, d. h. entweder allgemein, für AMD- oder für Intel-Prozessoren die Register anzupassen. Möchten Sie z. B. bei den genutzten AMD-Prozessoren die SSE3-Funktion verstecken, so sähe die Anpassung wie folgt aus:

Level 1 – Reihe **ecx** : `---- ---- ---- ---- ---- ---- ---0 -0-0`

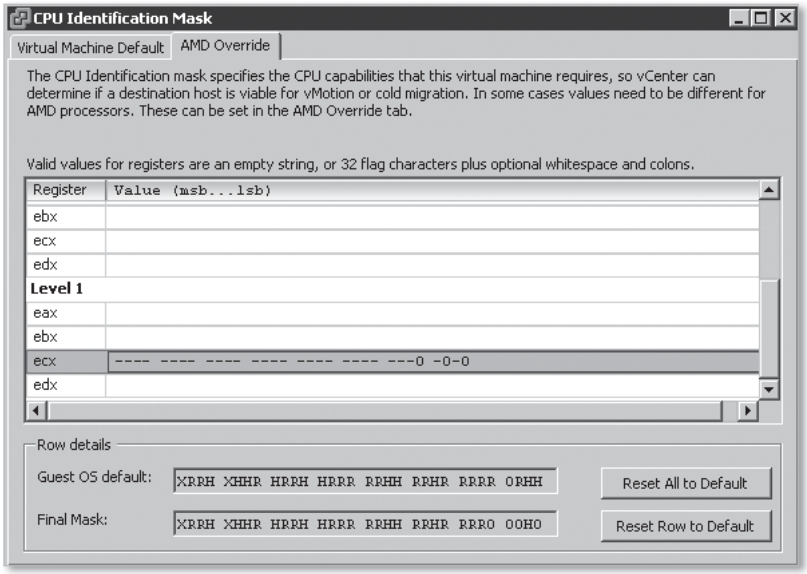


Abbildung 4.8 SSE3 wird durch diese Anpassung für die VM ausgeblendet.

Einen sehr guten VMware-Knowledge-Base-Artikel zu den verschiedenen Maskierungen mit den entsprechenden Prozessoren finden Sie hier:

http://kb.vmware.com/kb/1993.

Möchten Sie die Änderung rückgängig machen, so reicht entweder die Auswahl Reset Row to Default, wenn Sie gerade die angepasste Reihe ausgewählt haben, oder Sie setzen direkt alles zurück, indem Sie Reset All to Default auswählen.

Komfort der Geschwindigkeit

Sie müssen bei der Anpassung der CPU-Maskierung immer bedenken, dass ein Verstecken bestimmter Funktionen das Gastbetriebssystem ausbremsen kann, falls dieses mit diesen Funktionen schneller betrieben werden könnte. Im Endeffekt entscheiden Sie sich zwischen Komfort und Geschwindigkeit, abhängig vom Gastbetriebssystem.

EVC (Enhanced vMotion Compatibility)

Wollen Sie die CPU-Maskierung nicht für jede virtuelle Maschine definieren, bietet der EVC-Cluster (er wird in Kapitel 5, »Cluster«, näher beschrieben) die Möglichkeit, CPU-Funktionen global auszublenden, das heißt, in den Cluster-Eigenschaften wird definiert, welche CPU-Generation von den virtuellen Maschinen innerhalb des Clusters gesehen wird. Man kann hier von dem kleinsten gemeinsamen Nenner aller ESX-Host-CPUs im Cluster sprechen.

EVC ermöglicht es seit vSphere auch, die Prozessorgeneration während des Betriebs der virtuellen Maschinen zu erhöhen, z. B. von CPU-Generation 1 auf 2, allerdings nicht umgekehrt.

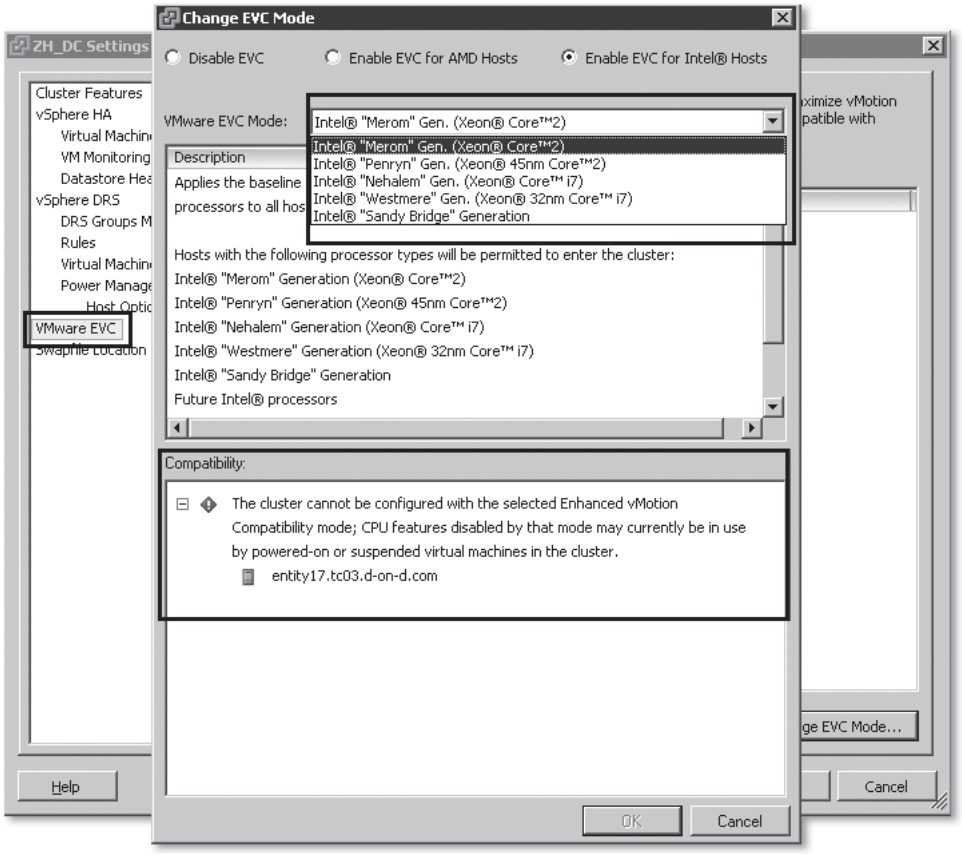


Abbildung 4.9 In den Cluster-Eigenschaften können Sie die CPU-Generation global für den gesamten Cluster einrichten.

Wird die CPU-Generation erhöht, so erhalten aktive virtuelle Maschinen erst nach einer Abschaltung oder einem Reset die neue Einstellung (Abbildung 4.10).

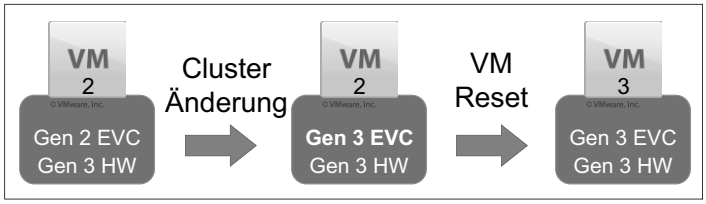


Abbildung 4.10 Änderung der EVC-Prozessorgeneration im Cluster während des laufenden Betriebs

Innerhalb des EVC-Clusters garantiert die EVC-Funktion, dass es zu keinen CPU-Inkompatibilitäten der CPU Generationen bei den vMotion-Vorgängen kommt. Andere Gründe zur Verhinderung von vMotion werden dadurch nicht ausgeschlossen, z. B. Nutzung von lokalen Festplatten.

4.1.3 Neuerungen mit vSphere 5

Ich möchte mit einer Neuerung beginnen, die bereits mit vSphere 4.1 eingeführt wurde, im Vorgängerbuch »vSphere 4« aber noch nicht betrachtet wurde: Quick Resume.

Quick Resume & Stun During Page Send

Da die Hauptspeichergröße von virtuellen Maschinen immer mehr gesteigert wird, musste VMware reagieren und vMotion von diesen VMs optimieren. Quick Resume verändert den vMotion-Vorgang minimal, da nicht zuerst der komplette Hauptspeicherinhalt auf dem Ziel-Host benötigt wird, bevor es zu einer kompletten Umschaltung kommt. Bei Quick Resume wird die Ziel-VM bereits aktiv geschaltet, bevor alle Hauptspeicherdaten migriert wurden, und die Quell-VM wird dabei angehalten (*Stun Mode*), aber die Ressourcen werden nicht gelöscht. Im Hintergrund kopiert VMware die restlichen Hauptspeicherinhalte weiter und ermöglicht den Zugriff auf Pages vom Ziel-ESX-Host auf dem Quell-ESX-Host.

So schön dieses Verfahren auf den ersten Blick erscheint, bringt es doch die Gefahr mit sich, dass Probleme auftreten, sollte ein Hardwareausfall in der Zeit des Quick Resumes passieren. Um dies abzufangen, nutzt VMware eine Datei auf dem zentralen Storage, die eine Art Datenpuffer bereitstellt, so dass bei einem Ausfall der Migrationsvorgang trotzdem abgeschlossen werden kann. Natürlich führt diese Form des Quick Resumes zu einem geringen Leistungsabgang, allerdings wäre ohne diese Funktion ein vMotion-Vorgang bei VMs mit viel vRAM nicht möglich.

Mit vSphere 5 wird diese Funktion durch »Stun During Page Send« oder »Slow Down During Page Send«, kurz SDPS, ersetzt. Der vMotion-Prozess beobachtet bei diesem Verfahren die Rate der veränderten Speicherseiten (*dirty pages*) während des vMotion-Vorgangs und vergleicht diese mit der aktuell möglichen Übertragungsrate zum Ziel-ESX. Basierend auf diesem Ergebnis wird die vCPU der Quell-VM etwas verlangsamt, indem Stopps (Sleep) im Millisekundenbereich künstlich eingebaut werden, um die Änderungsrate etwas zu verlangsamen. Damit wird dem vMotion-Vorgang die Chance gegeben, selbst sehr dynamische Systeme zu migrieren.

Auch hier kommt es zu Leistungseinbußen, allerdings müssen Sie bedenken, dass die langsame Datenübertragung bzw. die hohe Datenänderungsrate in früheren vMotion-Versionen normalerweise zum Fehlschlagen von vMotion geführt hätte.

Multi-NIC-vMotion-Unterstützung

Diese Funktion, die seit vSphere 5 verfügbar ist, bietet deutliche Vorteile, um die Bandbreite beim vMotion-Transfer zu erhöhen, da mehrere Netzwerkadapter gleichzeitig genutzt werden können. Allerdings müssen Sie für die Multi-NIC-Unterstützung auch das Design, also die Netzwerkinfrastruktur der vSphere-Umgebung, überdenken.

Es ist möglich, bis zu 16 mal 1-GbE- und 10 mal10-GbE-Netzwerkkarten für die vMotion-Übertragung miteinander zu koppeln.

Daher sollten Sie bei der Planung darauf achten, welche virtuellen Maschinen genutzt werden (vRAM-Konfiguration) und wie die Serversysteme (PCI-Bus-Nutzung) ausgelegt sind bzw. werden müssen, um erhöhtem Netzwerkverkehr (Peaks) gerecht zu werden.

Konfiguration Standard-vSwitch

Die Einrichtung des Multi-NIC-Supports für vMotion ist nicht ganz so intuitiv wie erhofft, aber immer noch gut verständlich und planbar. Sie legen so viele VMkernel-Ports an, wie Sie benötigen, und stellen anschließend jeweils die zu nutzenden vmnic-Adapter auf aktiv, während Sie alle übrigen Adapter auf »unused« schalten.

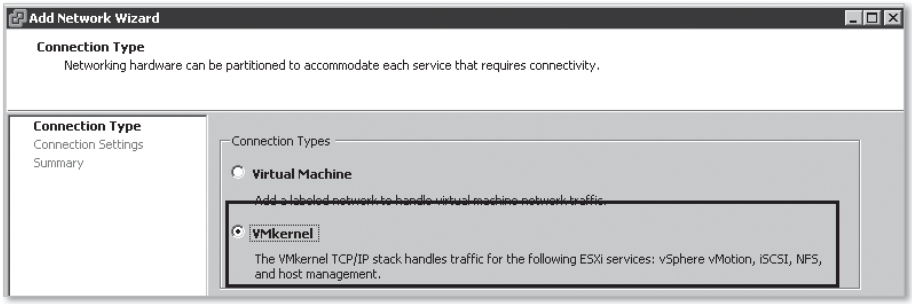


Abbildung 4.11 Anlage des ersten VMkernel-Adapters für vMotion

Dazu müssen Sie an dem gewünschten virtuellen Switch einen neuen VMkernel-Adapter anlegen (Abbildung 4.11).

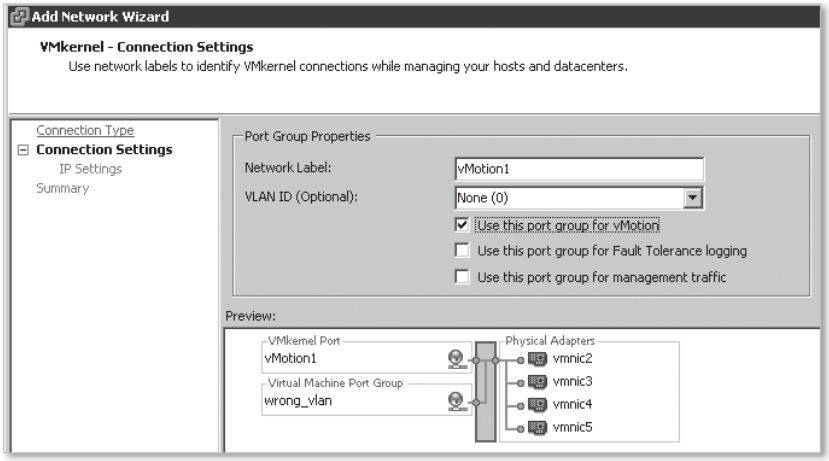


Abbildung 4.12 Aktivierung von vMotion

Diesen müssen Sie natürlich für vMotion aktivieren, und Sie sollten auch einen sprechenden Namen wie »vMotion1« oder »vMotion_1« oder »vMotion1_64« (bei VLAN-Nutzung) gewählt werden, damit die Zuordnung später leichter fällt (Abbildung 4.12).

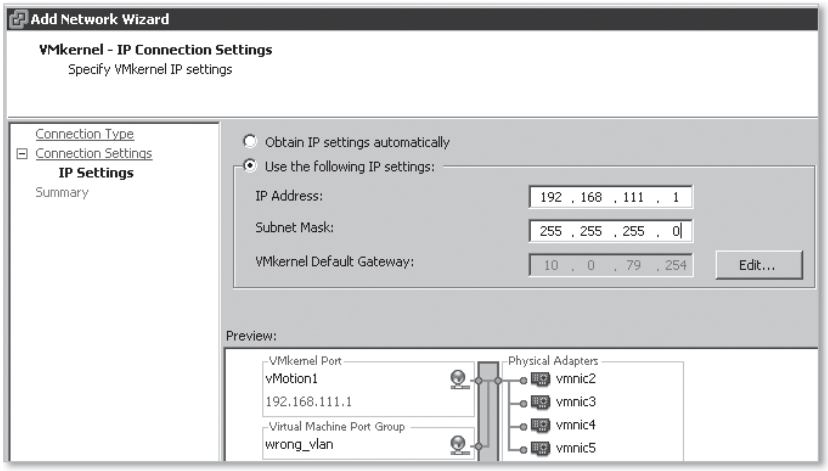


Abbildung 4.13 IP-Konfiguration des ersten vMotion-Adapters

In diesem Beispiel erhält der erste VMkernel-Adapter die IP-Adresse 192.168.111.1 – wichtig ist hierbei nur, dass sich zumindest alle vMotion-Adapterpärchen der beteiligten ESX-Hosts im gleichen Netzwerksegment befinden (Abbildung 4.13).

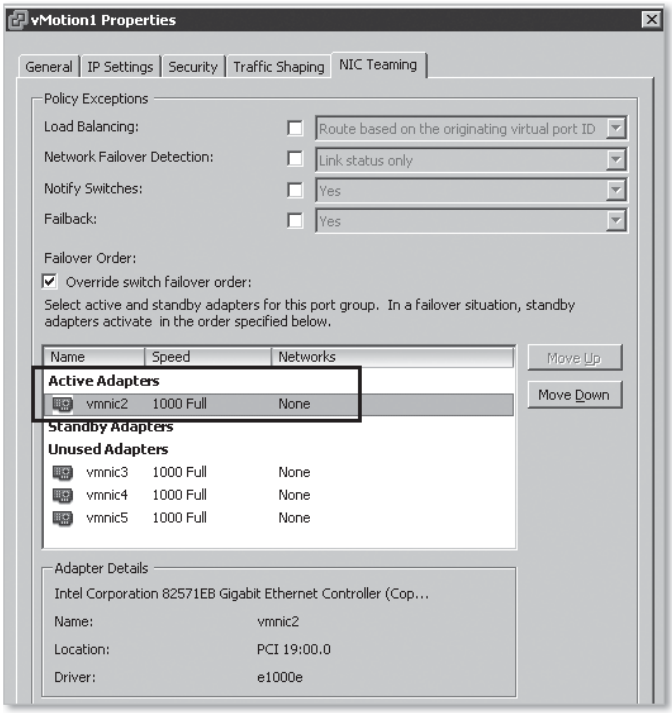


Abbildung 4.14 Beim ersten vMotion-Adapter wird nur der vmnic2-Adapter aktiv belassen, alle anderen Adapter werden als »unused« konfiguriert.

Nach der Erstellung des VMkernel-Adapters ist es wichtig, die zu nutzenden physischen Netzwerkkarten zu definieren. Genau gesagt, darf immer nur ein vmnic-Adapter aktiv sein, alle anderen Adapter müssen auf »unused« gesetzt werden (Abbildung 4.14).

Danach werden weitere Adapter nach dem gleichen Schema angelegt:

1. Label und VLAN (Abbildung 4.15)
2. IP-Konfiguration (Abbildung 4.16)
3. Active/Standby-Konfiguration der Portgruppe/des VMkernel-Adapters (Abbildung 4.17)

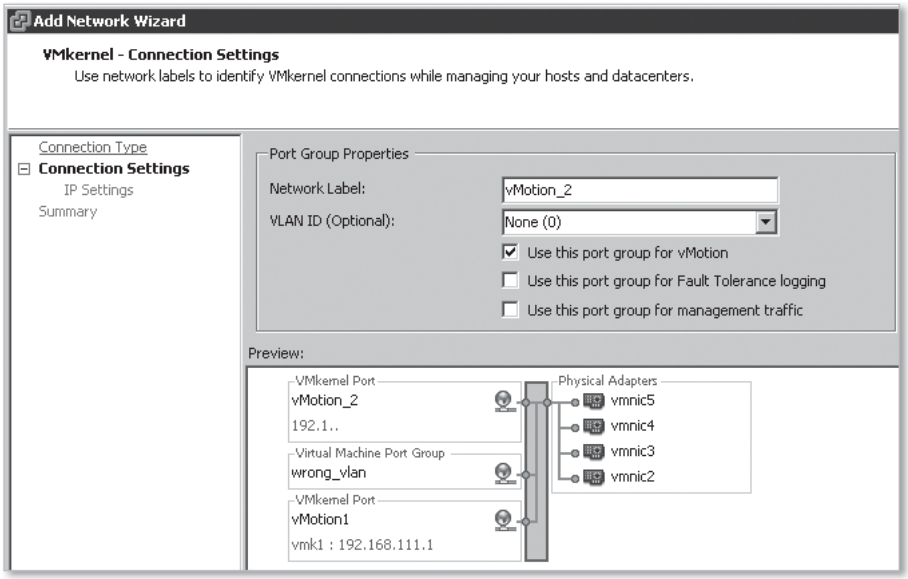


Abbildung 4.15 Anlage des zweiten VMkernel-Adapters für vMotion

Dieses Verfahren zur Erweiterung der Uplinks kann man annähernd beliebig fortführen, d. h. bis die maximale Anzahl der möglichen Multi-NIC Unterstützung erreicht ist.

Konfiguration distributed vSwitch

Die Konfiguration mittels Distributed vSwitch sieht auf ESX-Host-Seite identisch (VMkernel anlegen, IP-Adresse angeben) aus, allerdings muss man sich nicht um die »active«/»unused«-Konfiguration jedes einzelnen vMotion-Adapters kümmern, sondern kann dies einmalig zentral einrichten (Abbildung 4.18).

Die beiden (oder mehr) *distributed* Portgroups werden entsprechend angepasst, damit immer nur ein physischer Netzwerkadapter genutzt werden kann (1. Adapter: Abbildung 4.19, 2. Adapter: Abbildung 4.20).

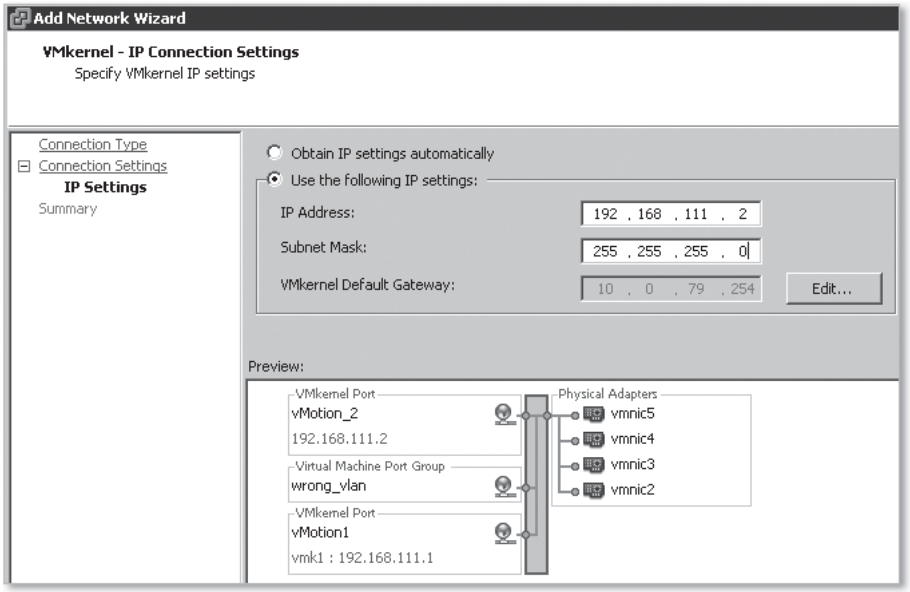


Abbildung 4.16 IP-Konfiguration des zweiten vMotion-Adapters

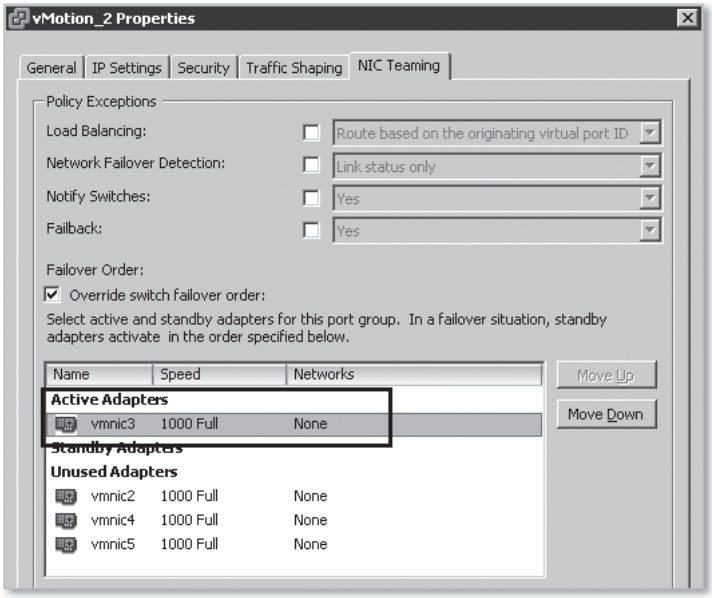


Abbildung 4.17 Beim zweiten vMotion-Adapter wird nur der vmnic3-Adapter aktiv belassen, alle anderen Adapter werden als »unused« konfiguriert.

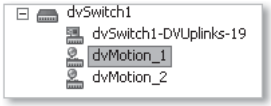


Abbildung 4.18 Anlage von zwei oder mehr vMotion-Portgruppen am dvSwitch

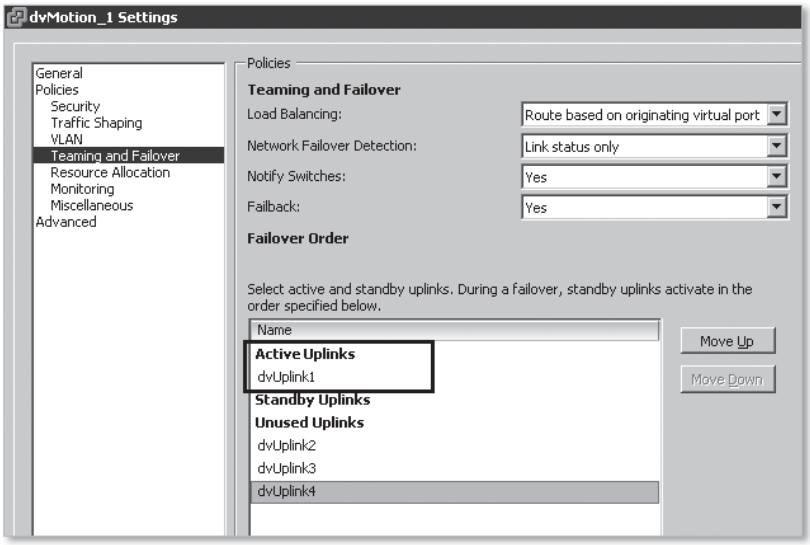


Abbildung 4.19 Die erste vMotion Portgruppe wird so konfiguriert, dass nur dvUplink1-Adapter aktiv ist, alle anderen Adapter sind »unused« konfiguriert.

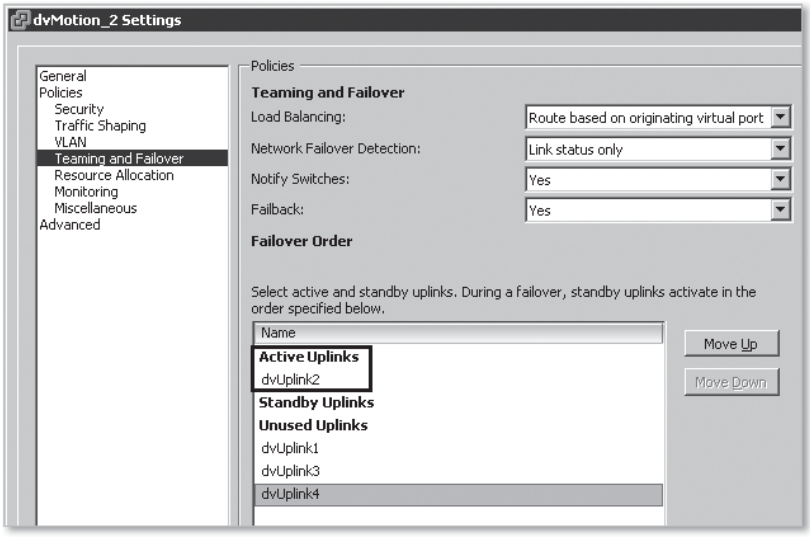


Abbildung 4.20 Die zweite vMotion Portgruppe wird so konfiguriert, dass nur dvUplink2-Adapter aktiv ist, alle anderen Adapter sind »unused« konfiguriert.

Sind die Portgruppen angelegt muss man auf den ESX-Hosts die VMkernel-Adapter anlegen und den Portgruppen zuweisen:

1. Verwaltung der virtuellen Adapter (Abbildung 4.21)
2. Erstellung des VMkernel-Adapters (Abbildung 4.22)
3. Zuordnung zu der gewünschten Portgruppe (Abbildung 4.23)
4. Vergabe der IP-Konfiguration (Abbildung 4.24)

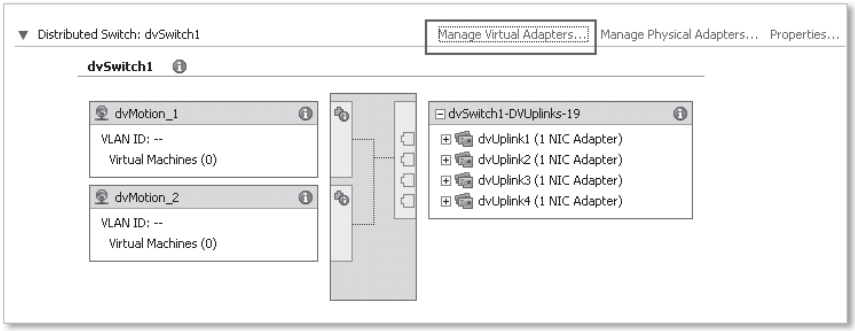


Abbildung 4.21 Verwaltung der VMkernel-Adapter auf dvSwitches auf dem ESX-Host

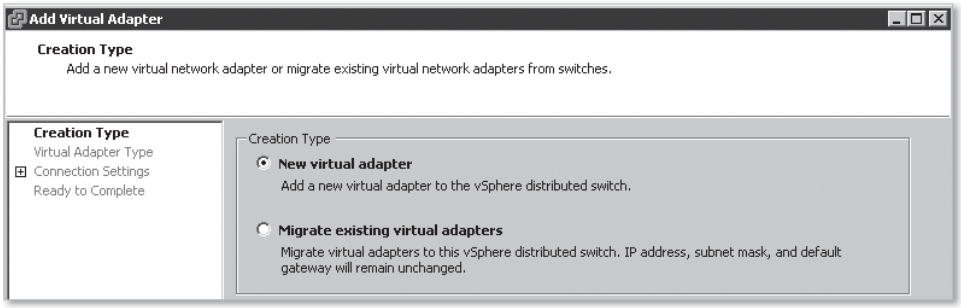


Abbildung 4.22 Neuen VMkernel-Adapter auf dem dvSwitch erstellen

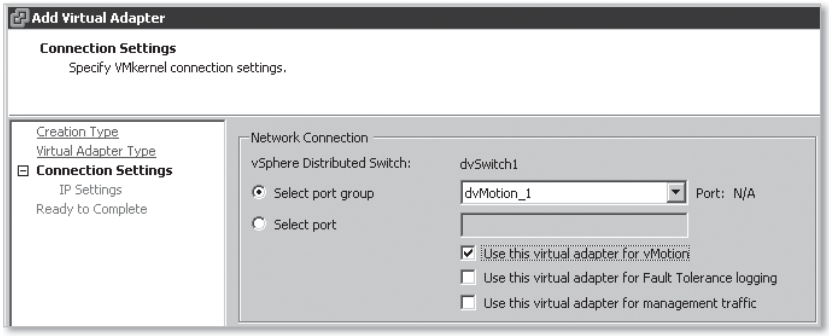


Abbildung 4.23 dvPortgroup auswählen und vMotion aktivieren

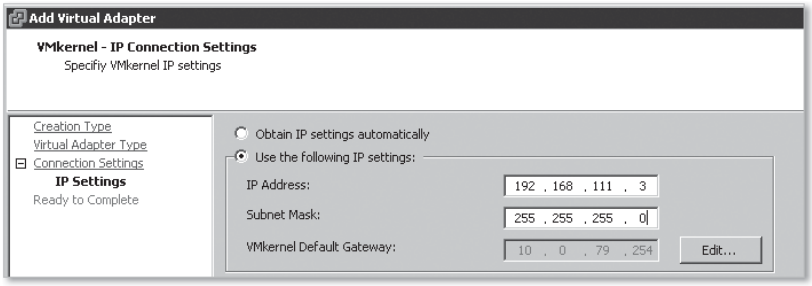


Abbildung 4.24 IP-Adresse für den vMotion-Adapter angeben

Nach Abschluss der Konfiguration sollten Sie zwei oder mehr Portgruppen mit VMkernel-Adapter vorfinden (Abbildung 4.25).

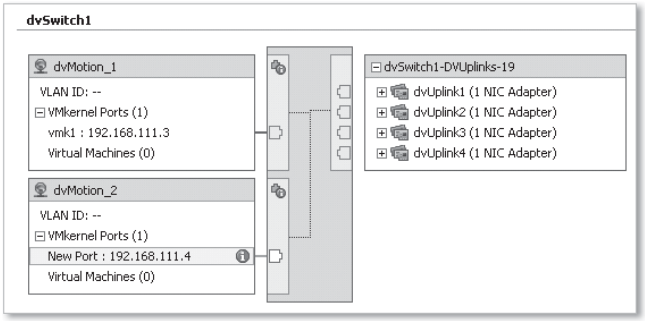


Abbildung 4.25 Nach Abschluss sollten zwei vMotion-Adapter an den unterschiedlichen vMotion-Portgruppen existieren.

Higher Latency Link Support

Vor vSphere 5 durfte die Latenzzeit 5 ms nicht überschreiten, obwohl dies bei vMotion über große Distanzen (Long Distance vMotion) keine Seltenheit war. Manche Implementation von Clustern über Rechenzentrumsgrenzen hinweg konnte aufgrund dieser Anforderung nicht oder nur eingeschränkt betrieben werden. Daher wurde die unterstütze Latenzzeit von 5 auf 10 ms verdoppelt, was allerdings eine Enterprise-Plus-Lizenz voraussetzt.

4.1.4 Bedienung

Die Bedienung von vMotion ist sehr intuitiv und trivial, da eine aktive virtuelle Maschine einfach per Drag & Drop auf einen anderen ESX-Host gezogen werden kann. Da die virtuelle Maschine angeschaltet ist, startet der vMotion-Prozess automatisch mit dem ersten Dialog.

Eine andere Variante ist die Auswahl MIGRATE im Kontextmenü einer virtuellen Maschine. Der Unterschied zwischen diesen beiden Möglichkeiten der Bedienung ist, dass letztere auch für Storage vMotion genutzt werden kann und natürlich eine weitere Abfrage bezüglich des Zielsystems und des Resource-Pools erscheint.

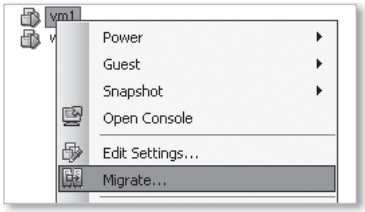


Abbildung 4.26 Start des vMotion-Vorgangs aus dem Kontextmenü der virtuellen Maschine

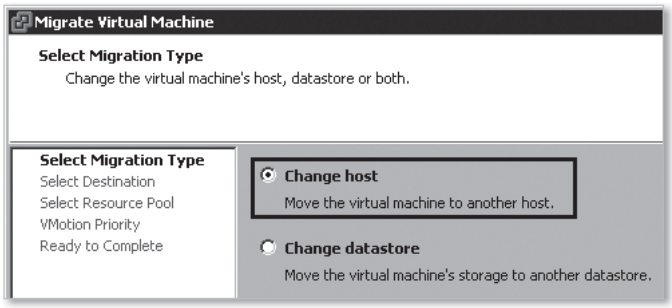


Abbildung 4.27 »Change host« steht für vMotion, »Change datastore« für Storage vMotion.

Haben Sie sich für die Drag-and-Drop-Variante entschieden, fällt der Dialog deutlich kürzer aus, und Sie haben nur die Wahl der vMotion-Priorität. Übrigens ist es auch möglich, mehrere virtuelle Maschinen gleichzeitig zu markieren und per Drag & Drop oder Kontextmenü zu migrieren.

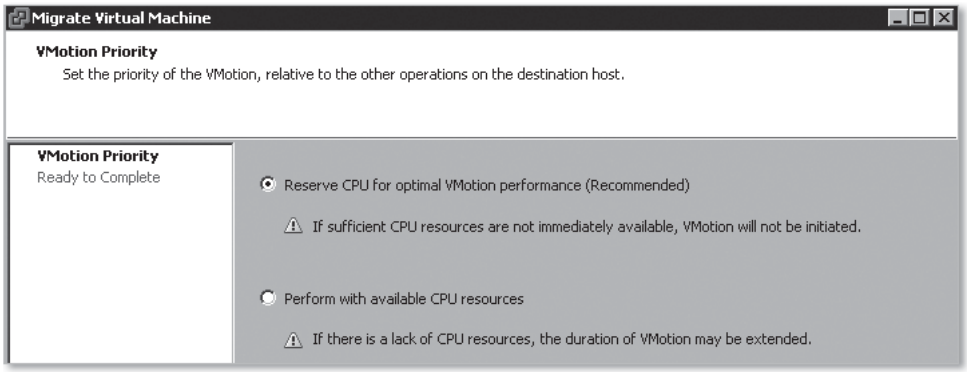


Abbildung 4.28 Abfrage der vMotion-Priorität

Bei der vMotion-Priorität sollten Sie möglichst immer Reserve CPU for optimal vMotion Performance auswählen, damit eine entsprechende Absicherung der Ressourcen auf dem Zielsystem gewährleistet ist und der vMotion-Prozess möglichst schnell ablaufen kann. Außerdem wird der vMotion-Prozess direkt abgebrochen, falls die Ressourcen auf dem Zielsystem nicht zur Verfügung stehen.

Die Auswahl Perform with available CPU Resources kann den vMotion-Vorgang zeitlich deutlich in die Länge ziehen, da auf die Ressourcen gewartet wird, anstatt sie direkt zu reservieren. Daher werden diese Migrationen auch immer ausgeführt, selbst bei Problemfällen mit zu hohem Hauptspeicherbedarf. Die virtuelle Maschine kann daher auch kurzzeitig nicht zur Verfügung stehen, falls die Ressourcen auf dem Zielsystem nicht rechtzeitig vorhanden sind.

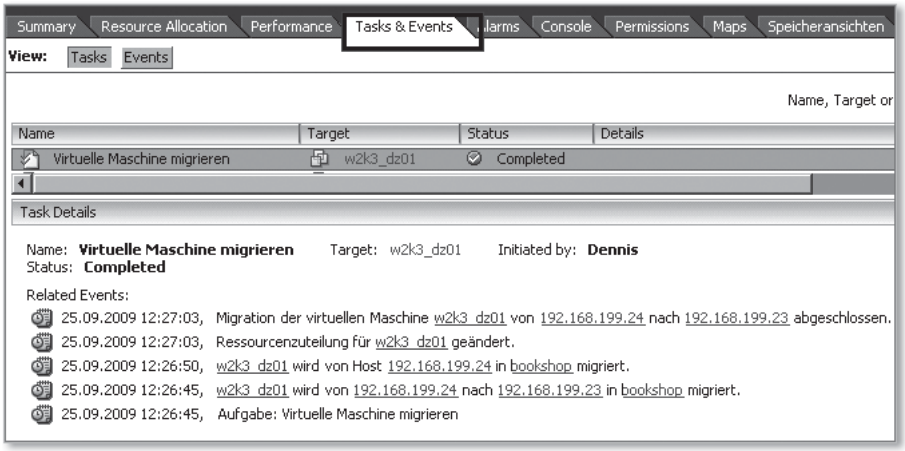


Abbildung 4.29 In der Ereignisanzeige der VM können Sie vMotion direkt nachvollziehen.

Sobald der vMotion-Prozess gestartet wurde, können Sie den gesamten Prozess in den Events der Host-Systeme und der virtuellen Maschine nachvollziehen. Damit können Sie auch die Dauer des gesamten Prozesses im Nachhinein prüfen. Während der Laufzeit lässt sich nicht nachvollziehen, wie lange der Prozess noch dauern wird.

In der Standardkonfiguration sind nur vier (GBit-Netzwerk) bzw. acht (10-GBit-Netzwerk) vMotion-Migrationen gleichzeitig pro Host und 128 vMotion-Migrationen pro VMFS-Datastore zugelassen.

4.1.5 Sicherheit

Die vMotion-Datenübertragung findet im Klartext statt. Daher ist es nicht nur aus Performance-, sondern auch aus Sicherheitsgründen zu empfehlen, ein dediziertes Netzwerk für den vMotion-Verkehr zu betreiben. In keinem Fall sollte der vMotion-Verkehr mit dem Netzwerkverkehr der virtuellen Maschinen vermischt werden, sprich über die gleichen Netzwerkadapter betrieben werden, ohne zumindest eine VLAN-Trennung durchzuführen.

4.1.6 Problemfälle

Neben den vielen möglichen Inkompatibilitäten, die eine Migration verhindern, existieren auch Problemfälle, die nicht einfach zu erkennen oder zu beheben sind.

Lokale Geräte

Viele lokale Geräte verhindern unter Umständen vMotion, und der Prozess bricht bereits bei der ersten Überprüfung mit einer Fehlermeldung ab.

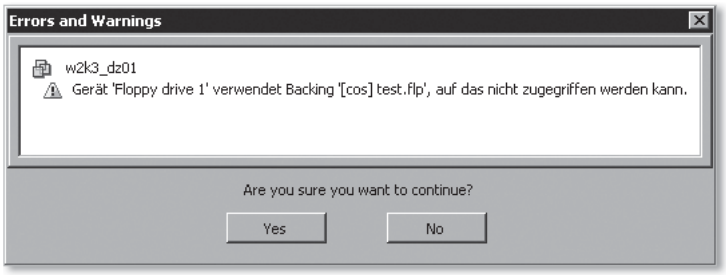


Abbildung 4.30 Problem beim Zugriff auf die Diskette durch den Ziel-ESX-Host, da ein lokales Medium verwendet wurde

Dies ist z. B. bei lokalen Festplatten der Fall. Bei für den VMkernel »weniger wichtiger« Geräten wie beispielsweise lokal verbundenen Wechselmedien erscheint eine Warnmeldung, dass das Gerät auf dem Zielsystem nicht verfügbar ist. Sind Sie damit einverstanden, wird der vMotion-Vorgang ohne den Anschluss der CD oder Diskette fortgesetzt. Dies gilt nicht bei bestehender Verbindung eines Client-Device, da dort eine direkte Verbindung vom Client zum ESX Server hergestellt ist. In diesem Fall ist vMotion verboten.

Datacenter

Es ist nicht möglich, virtuelle Maschinen mit vMotion über Datacenter-Grenzen zu migrieren. Dies ist nur in abgeschaltetem Zustand ausführbar. Allerdings kann zwischen allen anderen kompatiblen ESX-Hosts innerhalb des Datacenters migriert werden.

Allerdings sollten Sie den Grund dieser Limitierung immer im Auge behalten. Da Datacenter meist räumlich voneinander getrennt sind und über schmalbandige Kommunikationsverbindungen verfügen, ist es äußerst unwahrscheinlich, den gleichen Shared Storage von beiden Rechenzentren erreichen zu können. Aus diesem Grund sollten Sie auch bei der Offline-Migration daran denken, dass eine Datenübertragung einer 50-GB-VM möglicherweise die gesamte Leitungskapazität zwischen den Rechenzentren für eine lange Zeit komplett vereinnahmt, was einer Denial-of-Service-Attacke gleichkäme.

Gleiche Portgruppe = gleiches Netzwerk?

vMotion achtet bei der Prüfung der Netzwerke nur auf die Portgruppennamen, ohne die physische Verbindung prüfen zu können. Existieren zwei ESX-Hosts mit der Portgruppe LAN (der die virtuelle Maschine auch angehört), die aber auf unterschiedliche physische Netzwerke konfiguriert sind, kann der vMotion-Prozess zwar erfolgreich abgeschlossen werden, der VM allerdings steht kein funktionierendes Netzwerk mehr zur Verfügung. Sie ist in dem Fall zwar noch aktiv, aber die Netzwerkverbindung zur Außenwelt ist gekappt – Sie hätten die VM sozu-

sagen »totmigriert«. Daher müssen Sie auf die Gleichheit der Portgruppennamen auf den beteiligten ESX-Hosts achten (Distributed vSwitches bieten durch die zentrale Verwaltung der Portgruppen eine deutliche Vereinfachung) und auch darauf, ob die physischen Gegebenheiten der Uplinks hinter den Portgruppen ebenfalls identisch sind.

Hauptspeicheränderungen

Ein sehr typischer Problemfall sind virtuelle Maschinen, die enorm viele Änderungen im Hauptspeicher durchführen. Je größer die Hauptspeichermenge und je mehr Änderungen, desto schwieriger stellt sich die Möglichkeit einer reibungslosen vMotion-Migration dar. Kommt es stetig zu Abbrüchen bei einer VM, sollten Sie sich deren Hauptspeicheraktivitäten näher anschauen. Ein Beispielsystem hierzu wären Webserver, die viele dynamische Webseiten hosten und die Inhalte im Hauptspeicher vorhalten und stetig verändern.

Diese problematischen Vorgänge werden aber nach und nach auch durch Unterstützung der Prozessorhersteller behoben, da diese mit Funktionen wie AMDs Nested Page Tables und Tagged TLBs (die zusammen als »AMD Rapid Virtualization Index« benannt sind) eine deutliche Beschleunigung bringen und den Hypervisor selbst entlasten. Nähere Informationen zu den AMD-Technologien finden Sie unter folgender URL:

http://www.amd.com/us/products/technologies/virtualization/Pages/virtualization.aspx

Mit vSphere 5 hat VMware zwar nochmals die Verfahren von vMotion beim Transfer der Iterationskopien verbessert, die maximal zulässige Hauptspeichermenge einer VM aber auf 1 TB erhöht. Um Systeme mit mehr als 64 GB Hauptspeicher oder mehr als 120 MB/Änderungen pro Sekunde mit vMotion migrieren zu können, empfiehlt VMware 10-GBit-Verbindungen zwischen den ESX-Hosts. Die Migrationsfähigkeit bei VMs mit vielen Hauptspeicheränderungen wird durch 10 GBit natürlich ebenfalls gesteigert. Eine Dedizierung einer 10-GBit-Verbindung für vMotion ist aktuell noch nicht verpflichtend, kann aber mit der steigenden Menge an Migrationen und Datenmengen bei einzelnen Kunden heute bereits sinnvoll oder sogar notwendig sein.

SCSI-Reservation-Conflicts

Ein weiterer möglicher Grund sind zu hohe SCSI-Reservation-Conflicts, das heißt, die virtuelle Maschine kann nicht migriert werden, da das Zielsystem keinen rechtzeitigen Zugriff auf die SAN-Festplatten erhält. Dieses Problem tritt nur bei IP/FC SAN auf und kommt aufgrund von Treiberfehlern oder deutlich häufiger wegen Überlastung zum Tragen. Informationen über SCSI-Reservations finden Sie in den VMkernel-Protokollen der ESX-Server. Die Problematik SCSI-Reservation-Conflicts wurde mit vSphere 5 nochmals deutlich minimiert und kann bei Storage-Systemen mit VAAI-Unterstützung sogar eliminiert werden, da nicht mehr die komplette LUN, sondern nur die betroffenen Blöcke gesperrt werden.

Swapfile

Es existiert auf Host-Ebene die Möglichkeit, die Auslagerungsdateien der virtuellen Maschinen auf lokale Festplatten des ESX-Hosts zu legen, anstatt sie im zentralen Speicher vorzuhalten. Das spart auf der einen Seite zwar teuren SAN-/NAS-Plattenplatz, führt aber dazu, dass neben dem Hauptspeicher der virtuellen Maschine auch mit dem Swap-Speicher umgegangen werden muss. Liegen alle Daten im Shared Storage, so muss der Swap-Speicher nicht bewegt werden; liegt er jedoch auf dem lokalen ESX-Host, muss er zusätzlich übertragen werden, was einen vMotion-Vorgang deutlich verlängern kann.

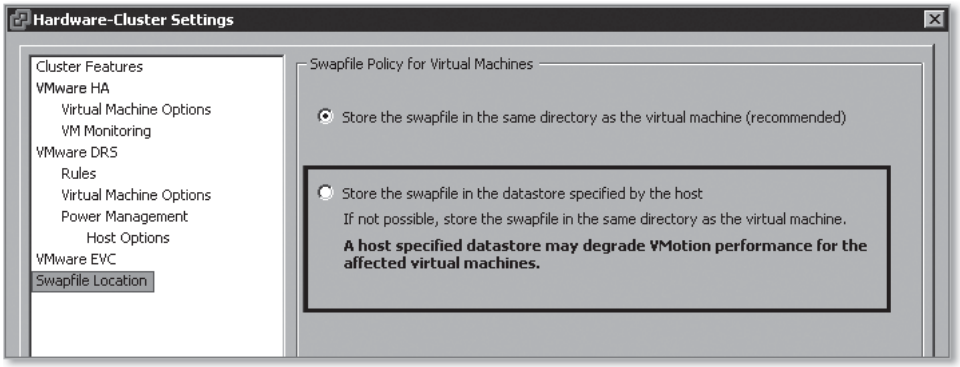


Abbildung 4.31 Anpassung des Swapfiles der virtuellen Maschinen im Cluster

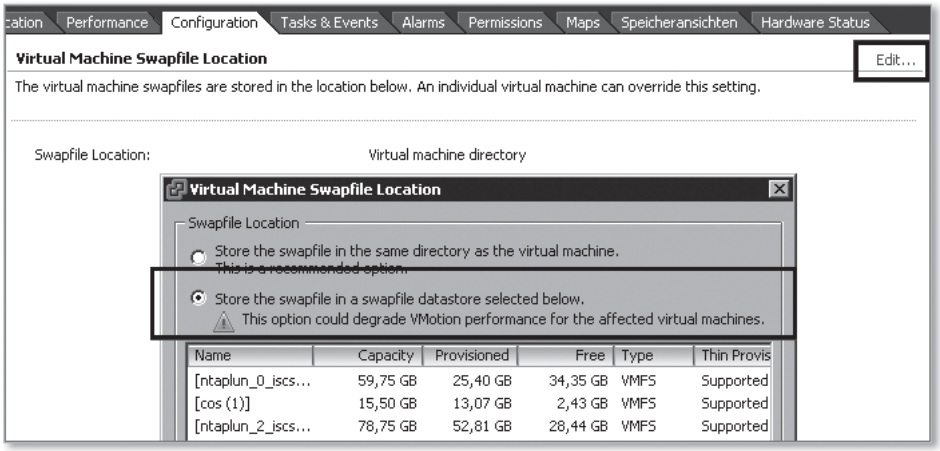


Abbildung 4.32 Anpassung des Swapfiles der virtuellen Maschinen in den Eigenschaften des ESX-Hosts

Timeouts und langsame Übertragung

Schlägt vMotion bei 10 % fehl, so handelt es sich um ein Problem mit der Verbindung zum Ziel-Host. Sie sollten in diesem Fall die vCenter-Meldung genau analysieren und das VMkernel-Protokoll (*/var/log/vmkernel.log*) auf dem Quell-ESX-Server anschauen.

Hier findet sich ein guter Blog-Eintrag zu diesem Thema:

http://www.vmwarewolf.com/vmotion-fails-at-10-percent/

Dauert vMotion sehr lange oder bricht ab, kann dies an einem sehr langsamen Netzwerk liegen, in dem keine rechtzeitige Rückmeldung durch den Ziel-ESX gesendet wird. Es existieren Fälle, bei denen das GBit-Netzwerk aufgrund einer Fehleinstellung auf den Ethernet-Switches auf 100 MBit Halbduplex heruntergestuft wurde, was zu diesem Problem führte. Hier sollten Sie sich auch die aktuelle Geschwindigkeit der Netzwerkkarten anschauen (`esxcfg-nics -l` auf der Management Console/vCLI) und das VMkernel-Protokoll des Ziel-Servers einsehen.

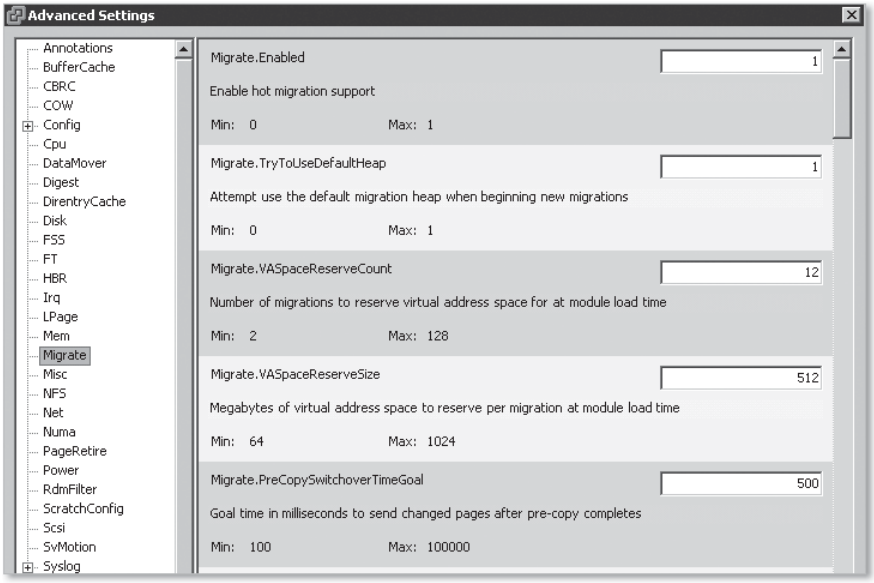


Abbildung 4.33 »Advanced Settings« für vMotion-Vorgänge in den Eigenschaften des ESX-Hosts

Ist das Netzwerk im Normalzustand sehr langsam, ist es möglich, die Switchover-Time zu erhöhen, beispielsweise in den Advanced Settings des ESX-Hosts: `PreCopySwitchoverTimeGoal` (Standard 500).

Anzahl gleichzeitiger vMotion-Vorgänge

Die Anzahl gleichzeitiger vMotion-Vorgänge ist bei Verwendung von 1 GbE auf 4 und bei 10 GbE auf 8 pro Host limitiert.

vMotion funktioniert nach VM-Hardware-Upgrade nicht mehr

Ein bekanntes Problem besteht übrigens bei virtuellen Maschinen, deren Hardware von Version 4 (ESX 3) auf Version 7 (vSphere) aktualisiert wurde und die entweder in einem EVC-Cluster waren oder deren CPU-Masking angepasst wurde. Bei diesen VMs bricht vMotion immer direkt mit einer Fehlermeldung ab, die auf eine nicht unterstützte VM-Konfiguration

hinweist. Die Lösung in diesem Fall ist das Zurücksetzen des CPU-Maskings in den Eigenschaften der virtuellen Maschine.

NFS-Storage

In den VMware-Foren existieren Beiträge zu vMotion-Abbrüchen bei 78 %, wenn NFS-Datastores genutzt wurden. Das ist definitiv kein allgemeiner Fehler, sondern kommt nur bei vereinzelten manchen Kunden vor. Hintergrund ist die unterschiedliche Einstellung bei der NFS-Freigabe an die verbundenen Host-Systeme. Dies stellen Sie sehr leicht fest, indem Sie die Datastore-UUIDs miteinander vergleichen. Sollten diese unterschiedlich sein, müssen Sie die Konfiguration auf dem Storage für die ESX-Hosts vereinheitlichen und die Datastores neu verbinden.

Die UUIDs der Datastores können Sie auf der Kommandozeile mit `df` auslesen:

```
/vmfs/volumes/18341836-debecbc6
             50.0G  100k  50.0G   0% /vmfs/volumes/nfs
```

Dieses Ergebnis muss auf allen ESX-Hosts gleich sein.

Ausfälle

Ausfälle in jeglicher Form können zu einem Fehlschlagen des vMotion-Vorgangs beitragen, z. B. Netzwerk-, Storage- oder Host-Ausfälle. vMotion ist allerdings so konzipiert, dass keiner dieser Ausfälle zum Totalverlust der virtuellen Maschine führen würde. Ein Ausfall auf dem Quellsystem, während die VM noch dort residiert, wirkt sich daher genau wie ein Ausfall ohne vMotion-Vorgang aus. Ein Ausfall des Zielsystems betrifft die virtuelle Maschine erst nach dem Senden des RARP-Paketes (Reverse ARP) und des vMotion-OK-Signals.

Protokolldateien

Sämtliche Informationen zu den vMotion-Vorgängen finden sich in den Protokolldateien der virtuellen Maschinen und der beteiligten ESX-Hosts. Dort können Sie nach den Begriffen »Migrate«, »migration id« oder »vMotion« suchen.

- **Home-Verzeichnis der virtuellen Maschine**

  vmware.log enthält die Informationen zu der Ziel-VM.

  vmware-<höchste Nummer>.log speichert die Informationen der Quell-VM.

- **Host-Protokolle befinden sich auf Quell- und Ziel-ESX-Host**

  /var/log/vmkernel.log

  /var/log/vmware/hostd.log*

Zeitunterschiede

Beachten Sie mögliche Zeitunterschiede der ESX-Hosts bei der Protokollanalyse.

Die VMkernel-Protokolle enthalten Netzwerk- und Storage-Fehler sowie vMotion-Timeouts. Außerdem ist es möglich, die Migrationsdatenmenge, die Änderungsrate und die VMotion-Dauer in den Logs einzusehen.

Hier ein kleines Beispiel mit einem Extrakt aus dem *vmkernel.log*:

1. `Another pre-copy iteration needed with 38769 modified pages (last = -1)`
2. `Another pre-copy iteration needed with 9616 modified pages (last = 38769)`
3. `Stopping pre-copy: only 3872 pages were modified`

Berechnung:

1. Iteration: 34,2 Sekunden, 38.769 Page-Änderungen (151,4 MB) = 4,43 MB/s
2. Iteration: 2,9 Sekunden, 9.616 Page-Änderungen (3776 MB) = 12,97 MB/s
3. Iteration: 0,87 Sekunden, 3.872 Page-Änderungen (15,1 MB) = 17,36 MB/s

Die dritte und letzte Iteration liegt unter 1 Sekunde und wird zum vMotion-Abschluss genutzt.

4.1.7 Lizenzierung

vMotion ist ab der Essentials Plus Edition und höher integriert und wird anhand der vSphere-Lizenzierung der Editionen pro CPU-Sockel und vRAM lizenziert.

4.1.8 Long Distance vMotion

Ein Trend zeichnet sich bei der vMotion-Funktion über große Distanzen ab, das heißt, Quell- und Ziel-ESX stehen Dutzende, Hunderte oder Tausende Kilometer voneinander entfernt. Hier kommen immer mehr Unternehmen auf den Markt, die an Systemen arbeiten, die die Latenz und die Datenübertragung über große Distanzen so optimieren, dass auch zwischen den USA und Europa eine vMotion-Funktion realisiert werden kann. VMware hat mit vSphere 5 bereits reagiert und die Akzeptanz der Latenzzeit bei vMotion-Vorgängen deutlich erhöht.

Diese Technologien für den als *Long Distance vMotion* bezeichneten Migrationsvorgang sind bereits zum großen Teil verfügbar und wurden auf Messen wie beispielsweise der VMworld bereits eindrucksvoll vorgeführt. Ein entsprechendes Whitepaper von EMC, Cisco und VMware ist hier zu finden:

http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/ns836/white_paper_c11-557822.pdf

4.2 Storage vMotion

Das Verschieben einer virtuellen Maschine von einem Datastore auf einen anderen war bis zu VI3.5 nur im abgeschalteten Zustand erlaubt. Einen Ausblick auf die Storage-vMotion-Funktion bot erstmals die Online-Migration einer VM von ESX 2.5 (VMFS-2) auf ESX 3 (VMFS-3). Mit VI3.5 wurde erstmals Storage vMotion als Funktion etabliert, war allerdings nur über das VMware SDK und das Remote CLI als Befehl verfügbar, eine grafische Implementierung fehlte gänzlich. Andrew Kutz, ein VMware-Community-Mitglied, entwickelte daher das erste inoffizielle Storage-vMotion-Plugin, das ein grafisches Frontend als vCenter 2.5-Plugin bereitstellte. vSphere bringt nun von Haus aus die grafische Integration von Storage vMotion mit.

Storage vMotion hat sich wie vMotion als sehr zuverlässig und sehr schnell herausgestellt und wird daher von VMware-Kunden sehr gerne verwendet, um

- virtuelle Maschinen besser auf den Datastores zu verteilen,
- Storage-Planungsfehler der Vergangenheit zu beheben,
- die Systeme auf neue Datastores (z. B. Wechsel des zentralen Speichersystems, Tiered-Storage-Modell) zu migrieren,
- die VMFS-Version zu aktualisieren und
- Storage-Wartungsfenster zu überbrücken.

Die wesentlichste Storage-vMotion-Neuerung unter vSphere 5 ist definitiv die Nutzung der VAAI-Storage-Kommunikation, um den Storage-vMotion-Vorgang komplett im Storage-Array abzubilden. Der große Vorteil daran ist, dass keine Datenübertragung der VMDK-Dateien zwischen ESX-Host und Storage-Array stattfindet. Natürlich ist diese Methode nur möglich, wenn eine VAAI-Unterstützung in der Infrastruktur besteht und die Migration nicht zwischen unterschiedlichen Storage-Arrays stattfindet.

4.2.1 Funktionsweise

Da von Storage vMotion gesprochen wird, kommt es zeitweise zu einem Missverständnis, dass durch Storage vMotion sowohl der ESX-Host als auch der Datastore gleichzeitig gewechselt werden könne. Dies ist nicht der Fall, allerdings führt Storage vMotion beim Wechsel der Konfiguration der virtuellen Maschine ein sogenanntes Self-vMotion durch, wodurch dieser Begriff wieder gerechtfertigt ist. Storage vMotion kann aus dem vSphere-Client, dem Remote CLI, dem PowerCLI oder dem VMware SDK gestartet werden.

Storage vMotion hat folgende Eigenschaften:

- VM verbleibt auf dem gleichen ESX-Host.
- VM-Festplatten sind individuell auf Datastores migrierbar.
- Es ist keine Abhängigkeit vom Massenspeicher (SAN/NAS) gegeben.

- Die Thick/Thin-Format-Unterstützung und -Konvertierung ist gegeben.
- Eine RDM-zu-VMDK-Konvertierung ist möglich.
- Keine Ausfallzeit ist notwendig.
- Storage vMotion ist komplett transparent für das Gastbetriebssystem.
- Es ist nur eine minimale Systembelastung gegeben.

Damit Sie die Migration der virtuellen Maschine von einem Datastore auf einen anderen besser verstehen, müssen Sie zuerst darüber nachdenken, aus welchen Dateien die VM normalerweise besteht:

- Konfigurationsdatei (*.vmx*)
- Protokolldateien (*.log*)
- Auslagerungsdatei (*.vswp*)
- Snapshots (*-delta*)
- andere Dateien (*.nvram* etc.)
- Festplattendateien

Bis auf die Festplattendateien liegen alle Dateien in der Standardkonfiguration im Home-Verzeichnis der virtuellen Maschine. Die Festplattendateien können entweder ebenfalls im Home-Verzeichnis liegen oder über mehrere Datastores verstreut sein.

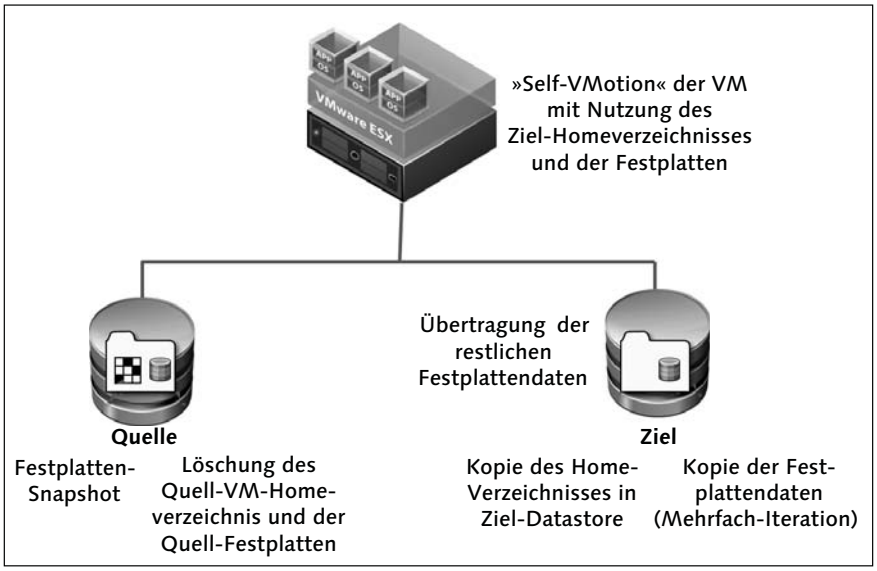


Abbildung 4.34 Storage vMotion vSphere 4 in Aktion

Schauen wir uns die einzelnen Schritte des Storage-vMotion-Prozesses unter vSphere 4 aus Sicht der virtuellen Maschine im Detail an (vergleiche Abbildung 4.34):

1. Überprüfung, ob die Quell-VM auf den/die gewünschten Ziel-Datastore(s) verschoben werden kann
2. Kopieren des Home-Verzeichnisses auf den Ziel-Datastore (Ausnahme Festplattendateien)
3. Anlage eines Snapshots auf die Festplattendateien
4. Übertragung der Festplattendateien zum Ziel-Datastore vor dem Snapshot
5. Übertragung der restlichen aufgelaufenen Snapshot-Dateien iterativ, bis nur noch wenige Restdaten vorhanden sind
6. Kopieren aller restlichen Daten mit gleichzeitigem Self-vMotion (Fast Suspend/Resume)
7. Löschen des Quell-Home-Verzeichnisses und der Quell-Festplatten

Für die unterschiedlichen Vorgänge sind zwei Komponenten zuständig, der NFC Copier und der Data Mover. Der NFC Copier ist für die »normalen« Dateien im Home-Verzeichnis verantwortlich, der Data Mover kümmert sich um die größeren Festplattendateien, die iterativ kopiert werden müssen.

Beide Komponenten arbeiten über dem Dateisystem, das heißt, sie sind unabhängig vom Speichersystem und können mit VMFS und mit NFS arbeiten. Außerdem kann der Aufbau der Festplattendatei durch den Data Mover verändert werden (thick/thin).

Zwischenzeitlich wurde mit vSphere 4.1 die Funktion Changed Block Tracking für Storage vMotion genutzt.

vSphere 5 Update

Durch die Verwendung von Snapshots hatte die vSphere 4-Version von Storage vMotion Probleme mit bestehenden Snapshots oder Linked Clones. Mit vSphere 5 verändert sich der komplette Prozess, so dass diese Probleme der Vergangenheit angehören.

1. Überprüfung, ob die Quell-VM auf den/die gewünschten Ziel-Datastore(s) verschoben werden kann
2. Kopieren des VM Home-Verzeichnis mittels vpxa auf den Ziel-Datastore
3. Starten einer »Shadow-VM« auf dem Ziel-Datastore mit den bereits kopierten Dateien. Danach wartet die Shadow-VM auf die noch fehlenden Daten.
4. Storage vMotion startet den Storage-vMotion-Mirror-Treiber, mit dem alle Schreibvorgänge auf bereits kopierte Blöcke automatisch auf den Ziel-Datastore repliziert werden.
5. Ähnlich vMotion werden die Festplatten komplett auf den Ziel-Datastore übertragen, wenn nur noch wenige Restdaten zu kopieren sind.
6. Auf Basis der neuen Daten wird ein Fast Suspend und Fast Resume auf der VM durchgeführt, was mit vMotion vergleichbar ist.
7. Nach dem erfolgreichen Fast Resume werden die Quelldaten gelöscht, und die VM ist auf dem Ziel-Datastore aktiv.

Die Shadow-VM wird übrigens nur gestartet, wenn das Home-Verzeichnis der VM migriert wurde. Werden nur einzelne Festplatten einer VM migriert, wird die VM (stun) nur kurz angehalten, was für das System und die Außenwelt nicht merkbar ist.

Das zwischenzeitlich verwendete Changed Block Tracking durch Storage vMotion wurde durch die neuen Techniken ersetzt.

Neben der Änderung auf den *Mirror Mode* (Storage-vMotion-Mirror-Treiber) werden neuerdings Snapshots und Linked Clones unterstützt, die Leistungsfähigkeit wird, verbessert und die Fehlermeldungen in den Protokolldateien werden ausgebaut.

Nach wie vor wird für Storage vMotion ein Data Mover verwendet, der in drei Typen vorkommt:

- **fsdm:** Basistreiber, der immer funktioniert, aber der langsamste aller Data Mover ist, da alle Daten den kompletten Stack (Storage Array – VMkernel Anwendungsebene) durchlaufen müssen. Dieser Treiber wird eingesetzt, wenn Quell- und Ziel-Datastore unterschiedliche Blockgrößen haben.
- **fs3dm:** Seit vSphere 4 steht der fs3dm-Modus zur Verfügung, der den Datenweg im Stack optimiert, d. h. auf ESX-VMkernel-Hardware-Ebene und nicht mehr bis auf Anwendungsebene. Dieser Treiber wird eingesetzt, wenn Quell- und Ziel-Datastore gleiche VMFS-Blockgrößen haben.
- **fs3dm Hardware Offload:** Mit vSphere 4.1 wurde auch ein Hardware-Modus auf Basis VAAI eingeführt, der den Host deutlich entlastet und die Daten auf Storage-Array-Ebene kopiert. Dieser Treiber wird eingesetzt, wenn Quell- und Ziel-Datastore gleiche VMFS-Blockgrößen haben und VAAI-Unterstützung durch die Storage Arrays zur Verfügung steht.

4.2.2 Voraussetzung

Genau wie für vMotion müssen auch für Storage vMotion bestimmte Voraussetzungen erfüllt werden, damit ein problemloser Ablauf gewährleistet ist:

- VMs mit bestehenden Snapshots können erst seit ESX 5 migriert werden.
- Virtuelle Festplatten müssen im persistenten Modus sein, damit Snapshots möglich sind.
- Werden Raw Device Mappings im Virtual Compatibility Mode genutzt, sind eine Migration der reinen Mapping-Datei und die Konvertierung des RDMs in eine Thin- oder Thick-Festplattendatei (außer bei NFS) möglich. Bei RDMs im Physical Mode kann die Mapping-Datei nur migriert, nicht aber in eine VMDK-Datei konvertiert werden.
- Migration während der Installation der VMware Tools ist nicht unterstützt.
- Der ESX-Host, auf dem die virtuelle Maschine betrieben wird, muss über eine Storage-vMotion-fähige Lizenz verfügen.

- ESX/ESXi 3.5-Systeme müssen für vMotion lizenziert und konfiguriert sein.
- Seit ESX/ESXi 4.0 ist keine vMotion-Konfiguration mehr notwendig.
- Der ESX-Host, auf dem die virtuelle Maschine betrieben wird, muss vollen Zugriff auf Quell- und Ziel-Datastore besitzen.
- In der Standardkonfiguration sind nur zwei Storage-vMotion-Migrationen gleichzeitig pro Host und acht Storage-vMotion-Migrationen pro VMFS-Datastore zugelassen.

Vorsicht

Vorsicht mit VMware-Backups während Storage-vMotion-Vorgängen unter vSphere 4. Da beide Prozesse mit Snapshots arbeiten, kann es zu sehr kritischen Storage-vMotion-Problemen kommen, wenn ein zusätzliches Programm auf die Snapshots zugreift. Dieses Problem wurde mit vSphere 5 behoben.

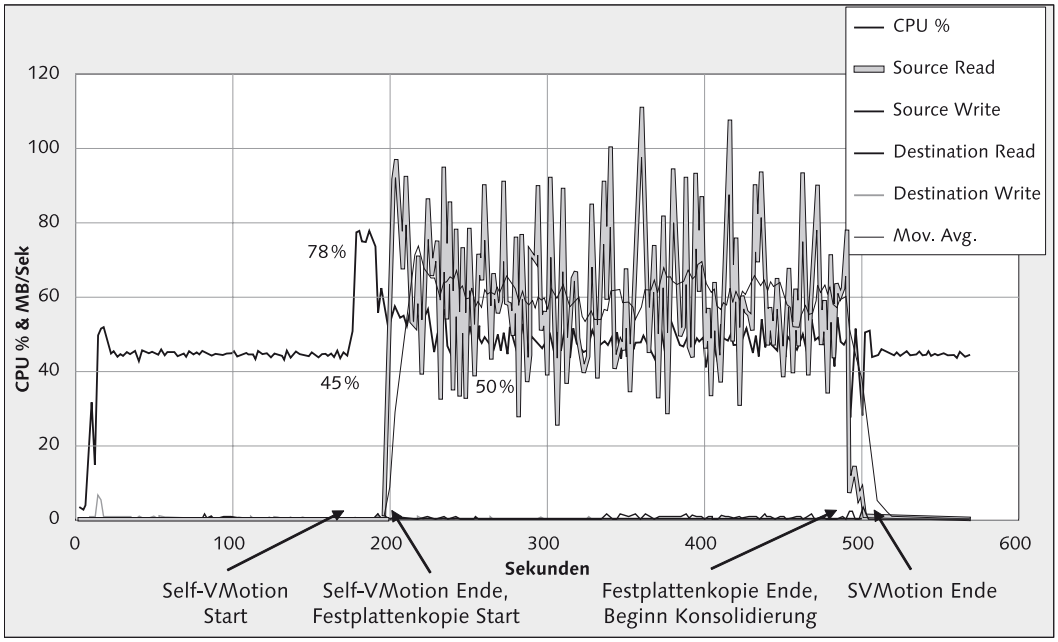


Abbildung 4.35 Belastung Storage-vMotion-Vorgang

Wie Sie in Abbildung 4.35 sehen, kommt es zu einem deutlichen Ressourcenanstieg während des gesamten Storage-vMotion-Vorgangs. Allerdings ist Storage vMotion als Prozess so ausgelegt, möglichst wenige von virtuellen Maschinen genutzte Ressourcen zu blockieren. Trotzdem ist eine gewisse Mehrbelastung des ESX-Hosts nicht von der Hand zu weisen, und die Dauer der Storage-vMotion-Übertragung verlängert sich natürlich, je weniger Ressourcen zur Verfügung stehen.

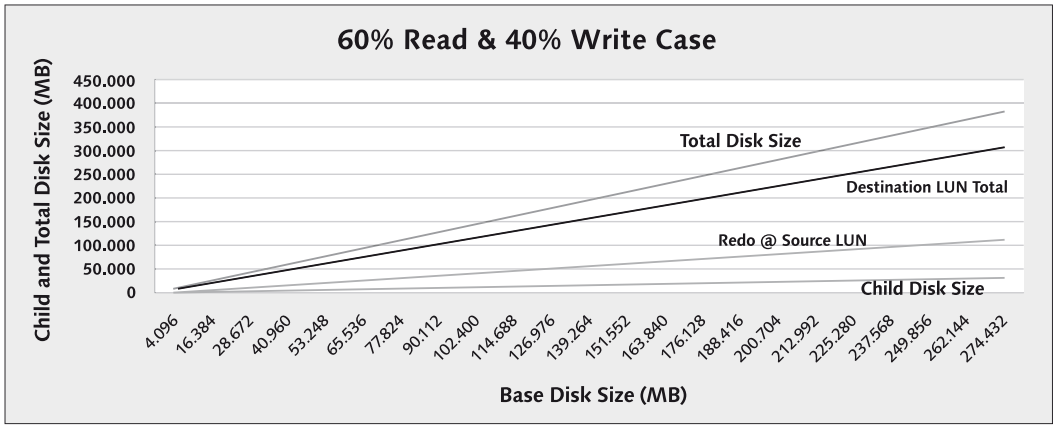


Abbildung 4.36 Festplattenbedarf während des Storage-vMotion-Vorgangs

Außerdem nicht vernachlässigen sollten Sie den benötigten Festplattenbedarf auf dem Quell- und dem Ziel-Datastore. Sie müssen bedenken, dass auf dem Quell-Datastore durch die Snapshots zusätzlich REDO-Logs vorgehalten werden müssen, die die Änderungsdaten während des gesamten Storage-vMotion-Prozesses aufnehmen. Diese Logs wachsen kontinuierlich.

Auf dem Ziel-Datastore werden erst die Quell-Festplatten mit den Daten vor der Anlage des Snapshots kopiert, und erst nach der vollständigen Übertragung werden die restlichen REDO-Logs kopiert. Daher benötigen Sie natürlich den gesamten Plattenplatz für die VM mit ihren Daten auf dem Ziel-Datastore und je nach Datenänderungen während der Übertragung noch einen gewissen Spielraum auf dem Quell-Datastore.

Je größer die Gesamtdatenmenge der virtuellen Maschine ist und je länger der Übertragungsprozess dauert, desto größer wird die benötigte Zusatzkapazität auf dem Quell-Datastore. Genaue Zahlen können wir nicht liefern, aber Sie sollten bei der Berechnung großzügig mit 20 % Zusatzkapazität der zu migrierenden VM auf dem Quell-Datastore kalkulieren.

Leistungseinbußen

Durch die Datenmenge, die übertragen werden muss, kommt es natürlich zu einer enormen Schreib-Lese-Belastung des Storage-Systems. Außerdem müssen Sie bedenken, dass Storage vMotion sequentiell mit sehr großen Blöcken arbeitet, während der normale Betrieb virtueller Maschinen eher von kleinen Blöcken und Random-Zugriff geprägt ist. Daher treffen auch zwei verschiedene Zugriffsarten auf den Storage, wobei sequentiell immer bevorzugt wird und daher der Random-Zugriff etwas benachteiligt ist. Gerade bei Einstiegs- und Mittelklasse-Storage-Modellen kann dies zu erheblichen Leistungseinbußen führen.

Mittels VAAI kann diese Belastung deutlich reduziert werden, da das Storage-System die Kopiervorgänge intern realisieren kann.

4.2.3 Bedienung

Da der gleiche Wizard für vMotion und Storage vMotion Verwendung findet, ist auch der Weg zum Aufruf des Wizards der gleiche: über das Kontextmenü der virtuellen Maschine.

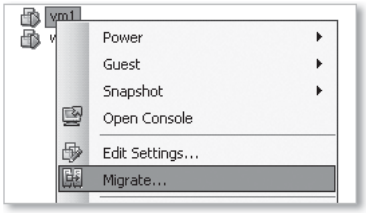


Abbildung 4.37 Wie bei vMotion öffnen Sie den Wizard über den Kontextmenüpunkt »Migrate« auf ein oder mehreren VMs.

Alternativ ist auch ein Drag & Drop möglich, allerdings müssen Sie dazu in die Datastore-Ansicht des vSphere-Clients wechseln und die virtuelle Maschine per Drag & Drop von dem aktuellen auf den Ziel-Datastore verschieben. In diesem Fall startet der Wizard bereits mit allen Angaben durch, und Sie müssen nur noch die Ziele des Home-Verzeichnisses und der virtuellen Festplatten angeben.

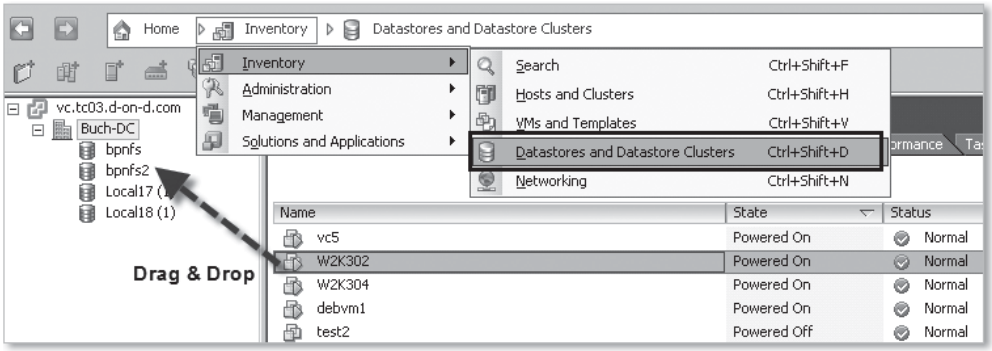


Abbildung 4.38 Storage vMotion per Drag & Drop im vSphere-Client

Der Wizard im vSphere-Client erlaubt:

- das Verschieben von Festplattendateien, ohne das VM-Home-Verzeichnis zu verschieben
- die Auswahl unterschiedlicher Datastores für die unterschiedlichen Komponenten (Home-Verzeichnis, einzelne Festplatten)
- die Konvertierung des Festplattenformats (thin/thick)
- das Kopieren von RDM-(Raw Device Mapping-)Festplatten zu virtuellen Festplatten (VMDK) im Thin- oder Thick-Format

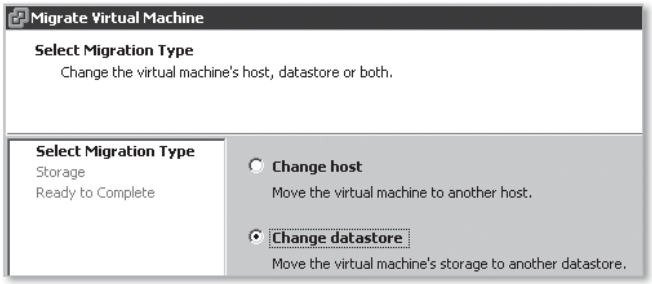


Abbildung 4.39 »Change Datastore« ist gleichbedeutend mit Storage vMotion.

Der einfachste Storage-vMotion-Vorgang besteht im Verschieben der kompletten virtuellen Maschine. In diesem Fall muss nur der Ziel-Datastore angegeben werden, und es wird direkt angezeigt, ob eine Migration möglich wäre.

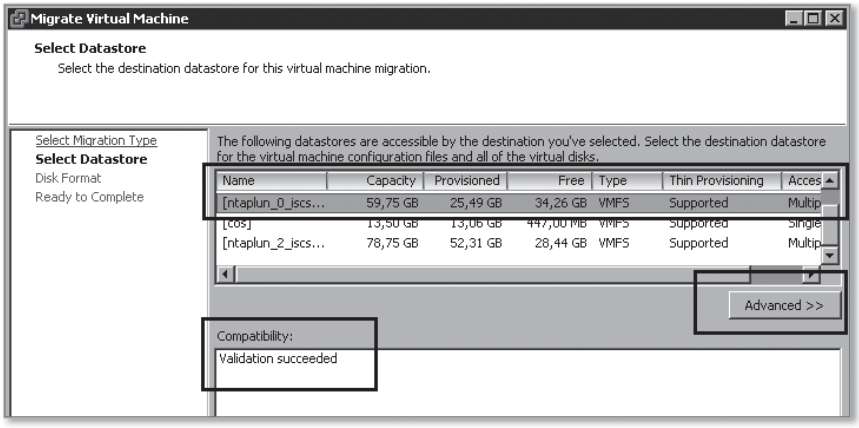


Abbildung 4.40 Auswahl des Ziel-Datastores bei Storage vMotion

Wählen Sie den Schalter ADVANCED, so schaltet die Ansicht direkt um, und Sie können unterschiedliche Datastores für das Home-Verzeichnis und die virtuellen Festplatten auswählen. Auch hier findet direkt eine Prüfung statt, ob die Ziel-Datastores kompatibel mit dem Storage-vMotion-Vorgang sind.

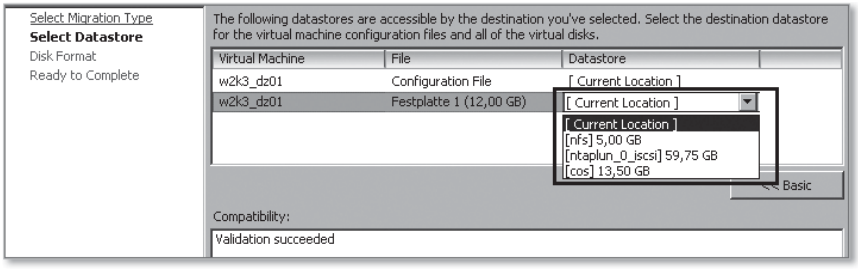


Abbildung 4.41 »Advanced«-Auswahl der Ziel-Datastores

Sobald die Ziele bestimmt sind, fragt der Wizard nach dem Typ der virtuellen Festplatte, und Sie haben drei Möglichkeiten zur Auswahl: Same, Thin und Thick.

Same Format as source ist einfach erklärt und bedeutet keine Änderung am Festplattentyp gegenüber dem derzeitigen Format der virtuellen Festplatten der zu migrierenden VM. Ist das Festplattenformat z. B. thin, dann bleibt es thin.

Thin Provisioned Format bedeutet, dass die Festplatte ins Thin-Format konvertiert wird, falls sie derzeit im Thick-Format vorliegt. Ansonsten würde keine Anpassung erfolgen. Das Thin-Format ist sehr plattenplatzeffizient, da nur wirklich geschriebene Daten Plattenplatz auf dem Datastore belegen. Existiert eine 20-GB-Festplatte mit 5 GB Belegung, dann schlagen auch nur 5 GB auf dem Datastore zu Buche.

Thick Format bedeutet, dass die Festplatte ins Thick-Format (eagerzeroedthick) konvertiert wird. Dabei ist zu bedenken, dass eine normale Anlage einer virtuellen Festplatte mit dem Wizard das zeroedthick-Format verwendet, daher findet meist eine Konvertierung von zeroedthick in eagerzeroedthick statt, was unter Umständen viel Zeit in Anspruch nimmt, da die Festplatte komplett mit Nullen überschrieben wird. Das Thick-Format ist performanter als das Thin-Format, allerdings wird die komplette Plattengröße im Datastore belegt, unabhängig von den wirklich geschriebenen Daten. Existiert eine 20-GB-Festplatte mit 5 GB Belegung, schlagen trotzdem 20 GB zu Buche.

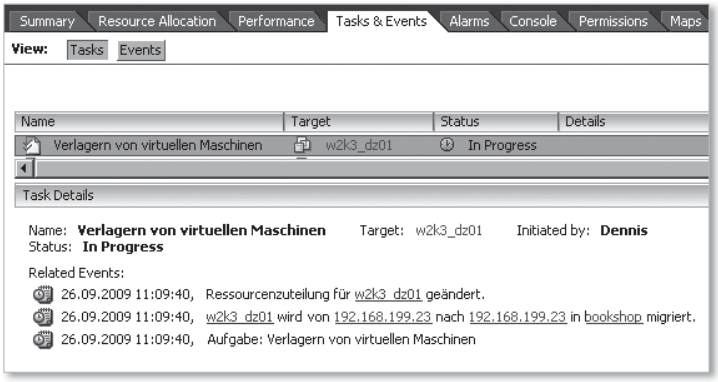


Abbildung 4.42 Storage-vMotion-Task in der »Tasks«-Ansicht der virtuellen Maschine

Zum Abschluss folgt eine Zusammenfassung des Vorgangs, und nach deren Bestätigung beginnt die Übertragung der Daten mittels Storage vMotion, was in den Tasks & Events des Host-Systems und der virtuellen Maschine einsehbar ist.

4.2.4 Problemfälle

Es sind derzeit wenige Problemfälle mit Storage vMotion bekannt, und die meisten rühren eher aus der Infrastruktur als aus der Software her. So werden natürlich leistungsfähige Storage-Systeme und -Anbindungen benötigt, damit Storage vMotion problemlos und schnell

durchgeführt werden kann. Zu hohe Latenzzeiten oder Paketverlust bis hin zum Ausfall von Infrastrukturkomponenten bergen eine gewisse Gefahr für den svMotion-Prozess, da dieser bei sehr großen virtuellen Maschinen mehrere Stunden andauern kann. Generell sollten Sie bei Systemen mit mehr als 20 GB (GBit-basierte Storage-Anbindung) bzw. 50 GB (FC-basiert) Daten die Storage-Migration eher in die Zeiten nach Büroschluss verschieben.

Große Raw Device Mappings

Ein sehr gerne übersehenes Problem ist die automatische Migration von RDMs in VMDK-Dateien. Wir müssen nicht lange nach einem Beispiel suchen – nehmen wir einfach einen Fileserver mit einer 1-TB-LUN, die über RDM angebunden ist. Wird diese auf einen Datastore per Storage vMotion verschoben, findet keine Prüfung statt, ob genügend Platz auf dem Datastore verfügbar ist; irgendwann ist der Datastore voll, da die wenigsten ein Terabyte Zusatzkapazität haben. Daher sollten Sie immer vorher kontrollieren, ob ein RDM angeschlossen ist und ob genügend Datastore-Kapazität zur Verfügung steht. Ansonsten besteht natürlich die Möglichkeit, nur die RDM-Mapping-Datei zu kopieren und nicht die Datastores selbst (Same Format as source auswählen).

Snapshots

Achten Sie unter vSphere 4 darauf, dass niemals Snapshots während des Storage-vMotion-Prozesses für die betroffene virtuelle Maschine angelegt werden. Besonders Aktionen, die direkt auf dem ESX-Server und nicht über das vCenter ausgeführt werden, sind gefährlich und führen im schlimmsten Fall zum Datenverlust. Achten Sie daher auf manuelle Snapshots, Snapshots durch VMware Consolidated Backup oder andere Backup-Skripte oder -programme. Informationen zu Problemen mit Snapshots und Storage vMotion finden Sie auch in der VMware Knowledge Base *http://kb.vmware.com/kb/1003114*. Dies ist mit vSphere 5 allerdings keine Problematik mehr.

Storage-vMotion-Timeout

Bei virtuellen Maschinen mit mehreren Festplatten können beim Storage-vMotion-Vorgang Abbrüche vorkommen, entweder bei 5, 10, 90 oder 95 %.

In den Protokolldateien des vCenters sind folgende Einträge zu finden:

```
[2008-07-17 12:29:57.283 02828 error 'App'] [MIGRATE]
(1216409209437375) vMotion failed: vmodl.fault.SystemError
[2008-07-17 12:29:57.454 02828 verbose 'App'] [VpxVmomi]
Throw vmodl.fault.SystemError with:
(vmodl.fault.SystemError) {
   dynamicType = <unset>,
   reason = "Source detected that destination failed to resume.",
   msg = "A general system error occurred: Source detected that
destination failed to resume."
```

Eine mögliche Lösung ist die Reduzierung gleichzeitiger Migrationsprozesse (Migration, Clonen, VM-Erstellung), eine weitere die Erhöhung der Übertragungs-Timeouts. Dies können Sie in den Eigenschaften (OPTIONS • ADVANCED; Abbildung 4.43) der virtuellen Maschinen oder direkt in der Konfigurationsdatei anpassen. Dazu müssen Sie den Eintrag `fsr.maxSwitchoverSeconds` als Timeout hinzufügen. Der Standardwert ist 100, daher sollten Sie den Wert entsprechend erhöhen.

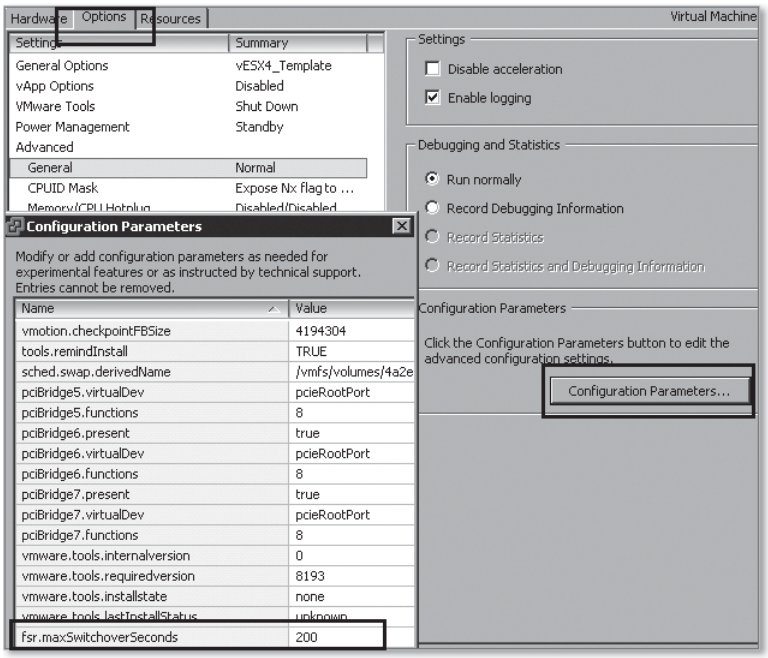


Abbildung 4.43 Erweiterte Konfiguration in den Eigenschaften einer VM

Den zugehörigen Knowledge-Base-Eintrag finden Sie hier: *http://kb.vmware.com/kb/1010045*. Dies ist mit vSphere 5 allerdings keine Problematik mehr.

Storage vMotion und vSphere HA

Solange Storage vMotion aktiv läuft, ist es für HA nicht möglich, die VM neu zu starten, bis Storage vMotion entweder beendet oder abgebrochen wurde. Storage vMotion passt den Fehlerzustand der VM automatisch beim Start des Vorgangs an. Sollte vCenter allerdings ausfallen, verfällt diese Anpassung nach 15 Minuten, damit die VM spätestens dann neu gestartet werden kann.

Große VMDK-Dateien

Nach einem Hinweis auf ein Phänomen, durch Christian Baldauf (Mightycare), dass Storage vMotion-Vorgänge von großen VMs –Festplatten von ca. 1 TB Größe, aber wenig geschriebenen Nutzdaten (Nettodaten) – enorm lange dauern, wollte ich dies genauer wissen.

Zur Drucklegung des Buches war noch keine Lösung oder Angabe von Gründen durch VMware bekannt. Daher habe ich eine VM angelegt und die Festplatte nur am Anfang, in der Mitte und am Ende formatiert und jeweils mit ca. 1 GB Daten beschrieben.

In meiner Testumgebung (NetApp FAS mit FC, iSCSI, NFS-Anbindung) wird normalerweise beim Storage vMotion nur die geringe Menge an geschriebenen Daten übertragen, d. h., die Migration (40-GB-Festplatte, 3 GB davon belegt) dauert etwas mehr als 120 Sekunden. Alle folgenden Tests wurden identisch festgelegt, egal ob NFS, iSCSI oder FC genutzt wurde. Dann wurde es jedoch spannend, und ich habe eine 1-TB-Platte angelegt und auch dort am Anfang, in der Mitte und am Ende jeweils eine 1 GB große Partitionen angelegt (`fdisk`) und Daten in die drei Partitionen kopiert (immer die gleiche ISO-Datei mit etwa 950 MB Datenvolumen). Die Nettodatenmenge habe ich absolut gleich gehalten, aber die Maximalgröße der VMDK-Datei habe ich von 40 GB auf 1 TB erhöht. Urplötzlich dauerte der Storage-vMotion-Vorgang statt der erwarteten 2 Minuten weit über vier Stunden. Daher liegt die Vermutung nahe, dass Storage vMotion bei großen VMDK-Dateien nicht mehr so effizient funktioniert wie bei kleinen VMDK-Dateien.

4.2.5 Lizenzierung

Storage vMotion ist ab der Enterprise Edition und höher integriert und wird anhand der vSphere-Lizenzierung der Editionen pro CPU-Sockel und vRAM lizenziert.

VMware führte bereits mit VI3.0 die ersten Cluster zur Ausfallsicherheit (HA) und zum Lastausgleich (DRS) ein. Deren Funktionsumfang wurde mit vSphere nochmals erhöht, und die Funktion Fault Tolerance (FT) basiert ebenfalls auf HA. Mit vSphere 5 folgte als nächster Meilenstein Storage DRS.

5 Cluster

Autor dieses Kapitels ist Dennis Zimmer, opvizor GmbH – opvizor.com, virtuellemaschinen@email.de – vmachine.de

VMware versteht unter »Cluster« in erster Linie eine Gruppe von zusammengehörenden Servern, die für Funktionen wie Ausfallsicherheit oder Lastenausgleich füreinander einstehen. Die Funktionen sind rudimentär und nicht mit Applikations-Clustern oder Clustern im Mid-Range- oder High-End-Bereich vergleichbar, aber trotzdem äußerst wirkungsvoll und dadurch auch sehr beliebt bei Kunden. Man kann das Cluster-Objekt grob in EVC-, HA- und DRS-Cluster aufteilen. Da Fault Tolerance ebenfalls einen HA-Cluster als Basis verwendet, behandeln wir in diesem Kapitel auch FT.

5.1 Cluster-Objekt

Sie müssen nicht zwingend HA und DRS nutzen, sondern können ein Cluster-Objekt einfach als organisatorischen Container für ESX-Hosts und virtuelle Maschinen verwenden, um beispielsweise Berechtigungen zu vergeben. Unabhängig von HA oder DRS kann ein ESX-Host zwar aktiv in einen Cluster verschoben werden, muss allerdings zum Entfernen aus dem Cluster in den Maintenance-Modus gesetzt werden. Durch Verwendung von vMotion bzw. DRS können die VMs manuell oder automatisch von dem zu entfernenden Host auf die übrigen ESX-Server verteilt werden. Damit ist es möglich, den ESX-Host auch ohne Abschalten von VMs aus einem Cluster zu entfernen. Danach kann der ESX-Host wieder problemlos für VMs genutzt werden.

5.1.1 Anlage des Clusters

Um einen Cluster zu erstellen, treffen Sie einfach im Kontextmenü des Datacenter-Objekts die Auswahl New Cluster.

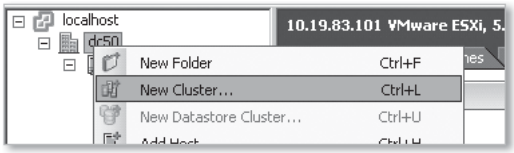


Abbildung 5.1 Anlage eines neuen Clusters

Nach Angabe des Cluster-Namens und gegebenenfalls der gewünschten Features ist der Cluster erstellt, und Sie können per Drag & Drop ESX-Hosts in den Cluster ziehen. Wählen Sie keine Features aus, so ist die Integration in den Cluster nur aus vCenter-Sicht eine Änderung; es werden keine Komponenten auf dem ESX-Host installiert.

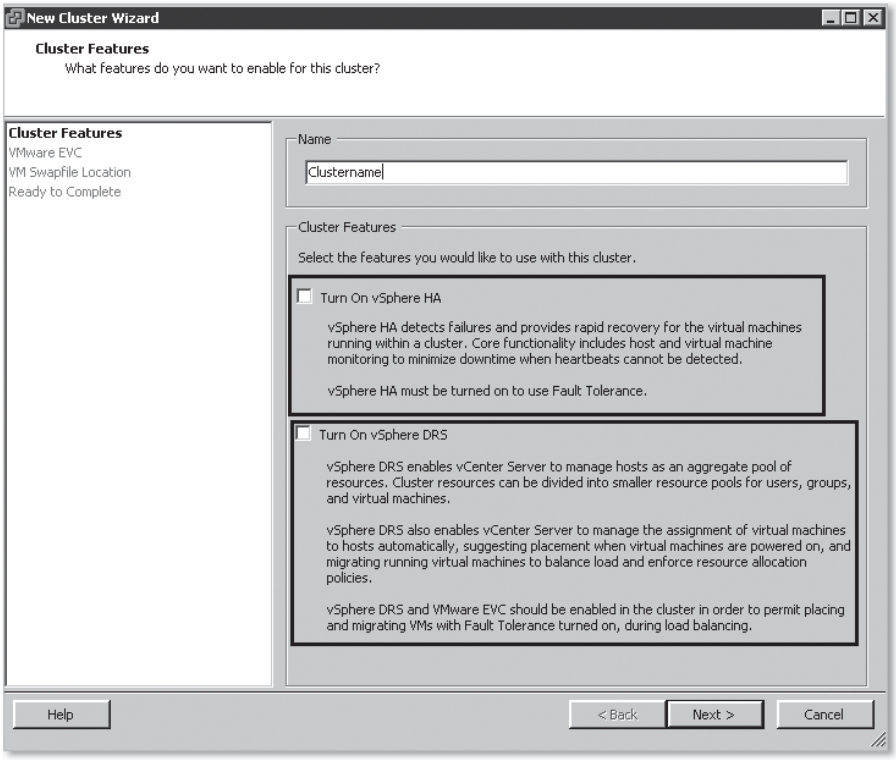


Abbildung 5.2 Name und Funktionsumfang des Clusters

5.1.2 EVC-(Enhanced vMotion Compatibility-)Mode

Eine Funktion, die nur im Cluster nutzbar ist, nennt sich EVC, was ausgeschrieben »Enhanced vMotion Compatibility« heißt. Die Bezeichnung deutet es bereits an: Es können ESX-Server mit unterschiedlichen CPU-Generationen in diesen Cluster integriert werden, und vMotion ist trotzdem möglich. Dies ist vergleichbar mit der Advanced-CPU-Funktion jeder virtuellen Maschine, CPU-Funktionen zu verstecken.

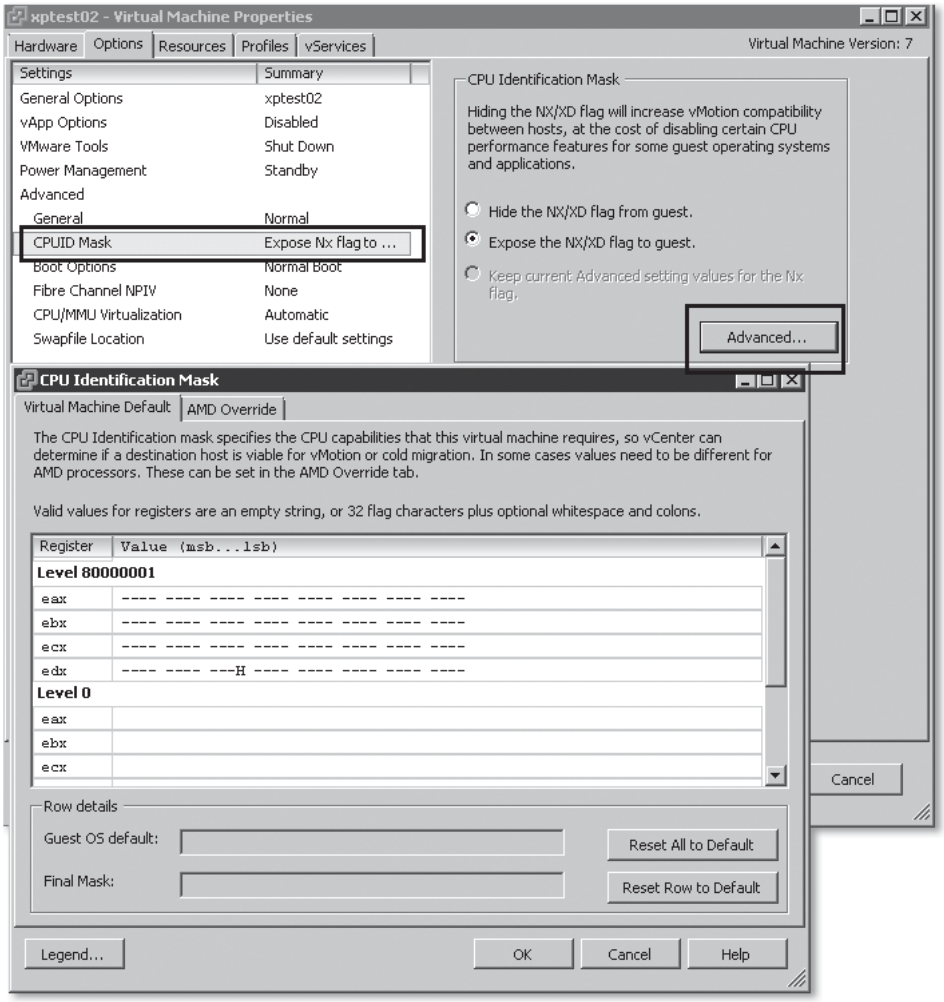


Abbildung 5.3 CPUID-Masking in den Eigenschaften einer VM

Allerdings bietet EVC im Cluster den klaren Vorteil, dass diese Einstellung nicht pro VM getroffen werden muss, sondern cluster-weit gilt, und dass jede VM automatisch konfiguriert wird. Trotzdem werden die Einstellungen einer VM durch den EVC-Cluster zugeordnet und erst beim Abschalten einer VM angepasst, selbst wenn diese die EVC-Cluster wechselt. Aus diesem Grund sollten Sie VMs bei Änderungen im EVC-Cluster bei Wartungsfenster VMs nicht neu starten, sondern komplett abschalten und wieder anschalten, damit ihre EVC-Konfiguration aktuell ist.

Dies bedeutet aber auch, dass VMs abgeschaltet sein müssen, bevor sie den ersten EVC-Cluster betreten dürfen, und damit betrifft dies natürlich auch die ESX-Hosts, die Sie integrieren möchten.

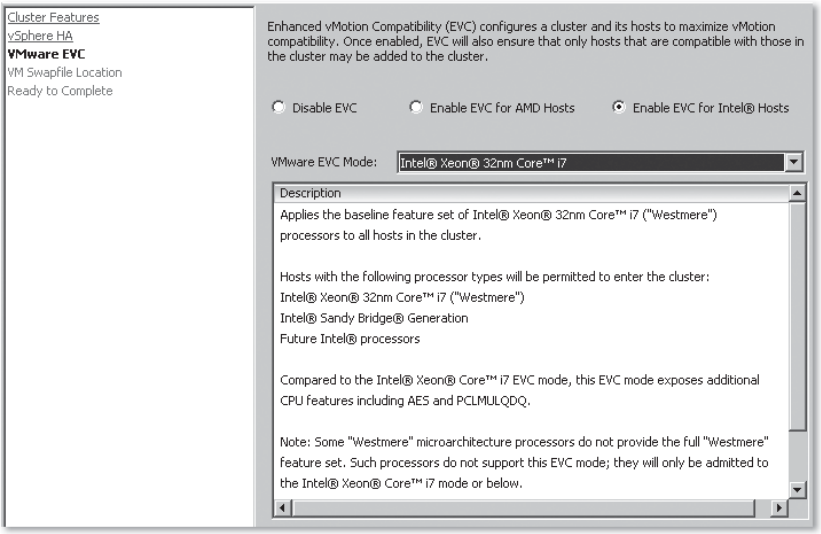


Abbildung 5.4 Ändern der EVC-Einstellungen eines bestehenden Clusters

Um die Funktion VMware EVC zu nutzen, können Sie dies entweder direkt bei der Anlage des Clusters angeben oder zu jedem Zeitpunkt nachträglich ändern. Aber auch hier gilt: Die VMs müssen abgeschaltet sein, wenn eine Generationsänderung nach unten (mehr CPU-Funktionen werden ausgeblendet) stattfindet!

Auch EVC kann keine Wunder bewirken, und es müssen zumindest gleiche CPU-Hersteller und ähnliche CPU-Familien in den ESX-Hosts eingebaut sein, damit ein gemeinsamer Nenner gefunden wird und die VMs entsprechend konfiguriert werden können.

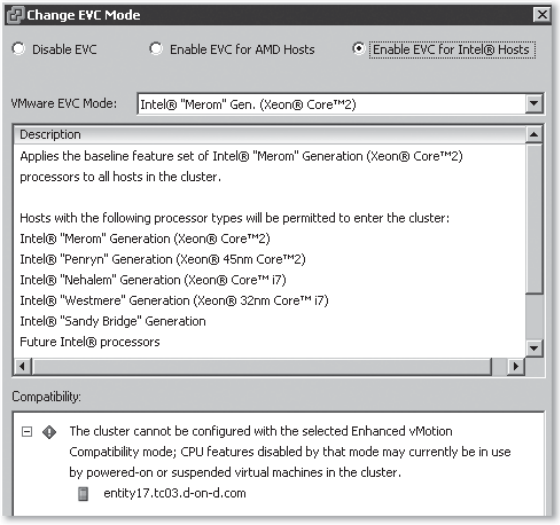


Abbildung 5.5 EVC bietet die Möglichkeit, zwischen verschiedenen CPU-Generationen zu wählen.

Man ist geneigt zu fragen: Hat EVC nur Vorteile? Wie immer ist die klare Antwort: Nein. Werden in einem Cluster zwei Server neuester AMD-Opteron-Generation (3) mit zwei Servern ältester AMD-Opteron-Generation (1) in einem EVC-Cluster kombiniert, so werden alle VMs auf Generation 1 zurückgestuft. Sind in Generation 3 CPU-Funktionen für einzelne Applikationen ideal zum Performancegewinn, so sind diese Funktionen für die VM nicht mehr sichtbar.

Das Gleiche gilt für virtuelle Maschinen, die auf einer aktuellen CPU gestartet und installiert wurden. Wenn die Applikation entsprechende Programmoptimierungen aufgrund der CPU-Funktionen mitinstalliert oder genau auf bestimmte CPU-Funktionen aufbaut, so kann ein Wechsel in einen EVC-Cluster mit älterer CPU-Generation Nachteile in Stabilität und Leistung bringen.

Obwohl es selten vorkommt, ist hierbei zu bedenken, dass VMware in der Standardkonfiguration die CPU mit allen Funktionen komplett sichtbar an die virtuelle Maschine durchreicht. Es findet eine Virtualisierung und keine Emulation statt. Sobald EVC genutzt wird, sieht die virtuelle Maschine zwar immer noch die reale CPU, allerdings werden bestimmte Register, die die Prozessorgenerationen ausmachen, weggeblendet. Die VM hat also unter Umständen nicht den vollen Funktionsumfang der aktuell genutzten physischen CPU im Zugriff.

Welche CPU-Funktionen genau zusätzlich eingeblendet werden, finden Sie in der Generationenbeschreibung (Abbildung 5.6).

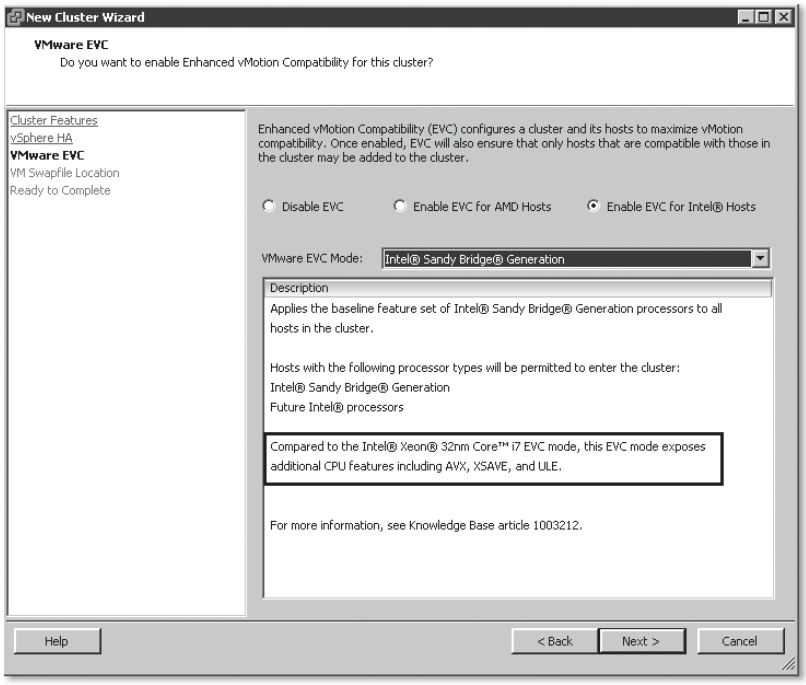


Abbildung 5.6 Die Beschreibung weist auf die zusätzlichen Funktionen der EVC Generationsauswahl hin.

Allerdings existieren im vSphere 5-EVC-Mode neue Funktionen, die es ermöglichen, flexibler mit den CPU-Generationen umzugehen. So ist es möglich, eine VM bereits in einen EVC-Cluster neuer Generation zu verschieben, ohne die VM auszuschalten. Sie behält einfach so lange die Einstellungen zum Betrieb unter der alten Generation, bis ein Power-Reset durchgeführt oder die VM ab- und wieder angeschaltet wird.

5.2 HA-Cluster

Ein vSphere-Cluster kann, wie bereits angekündigt, viel mehr, als nur virtuelle Maschinen zusammenzufassen und eine verbesserte vMotion-Kompatibilität herzustellen. Es ist durch Einsatz der HA möglich, virtuelle Maschinen automatisch neu zu starten, sowohl bei Ausfall des ESX-Servers als auch bei Ausfall des Gastbetriebssystems.

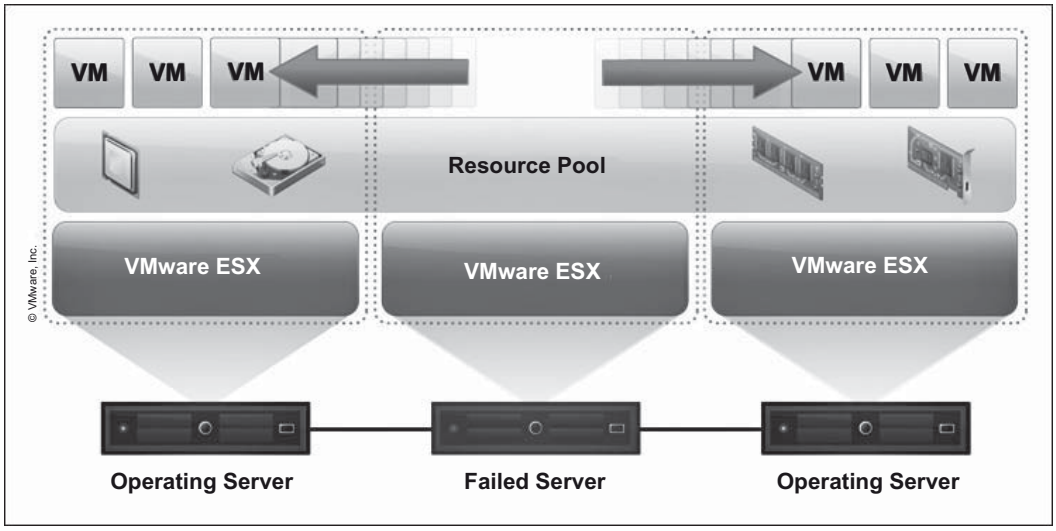


Abbildung 5.7 Übersicht der HA-Funktion von VMware

5.2.1 Technologie-Übersicht

Die Grundidee hinter VMware High Availability (HA) ist, den Ausfall eines ESX-Servers zu überwachen und ihn zu kompensieren. Dabei unterscheidet sich der Clustering-Gedanke von VMware komplett von zum Beispiel Microsofts Cluster-Lösung oder von HPs MC/ServiceGuard für HP Unix: Deren Cluster stellt eine virtuelle Einheit basierend auf mindestens zwei physischen Servern dar, und Anwendungen laufen auf der virtuellen Einheit, z. B. bei Microsoft auf einem SQL-Server oder einem DHCP-Server. Dabei ist immer ein physischer Server aktiv und verwaltet die virtuelle Einheit. Hier teilt sich der aktive Server mit den passiven Servern des Clusters über eine gemeinsam genutzte Festplatten-Ressource die Informationen über den aktuellen Zustand der virtuellen Einheit und der darauf laufenden Anwendungen.

Fällt bei solch einem Cluster-Verbund der aktive physische Server aus, so übernimmt ein passiver Server die Verwaltung der virtuellen Einheit, und die auf dem ausgefallenen Server laufenden Anwendungen können ohne Unterbrechung fortgeführt werden. Diese Anwendungen müssen cluster-aware sein, um diese Ausfallsicherheit mit der Cluster-Lösung zu nutzen. VMware realisiert mit HA eine andere Art des Clusterings, die besser in »VMware Fast Server Recovery« umbenannt werden sollte. Diese Lösung überwacht alle im HA-Verbund befindlichen ESX-Server, und bei Ausfall eines dieser Server wird versucht, die darauf aktiven virtuellen Maschinen auf einem anderen, freien ESX-Server wieder neu zu starten. In diesem Fall ist der Neustart der virtuellen Maschinen unumgänglich; ebenso ist die Grundlage hierfür die Verwendung von zentralem Storage für die Ablage der virtuellen Festplatten und der VM-Konfigurationsdateien sowie identische Virtual-Machine-Netzwerkverbindungen auf den ESX-Servern.

HA kann auch Ausfälle innerhalb der virtuellen Maschinen überwachen. Diese Funktion wird allerdings nicht durch den HA-Agent auf den ESX-Hosts, sondern durch das vCenter selbst realisiert. Mit vSphere 5 existiert mittels HA auch die Möglichkeit der Überwachung von Anwendungen im Gastbetriebssystem (Abbildung 5.8).

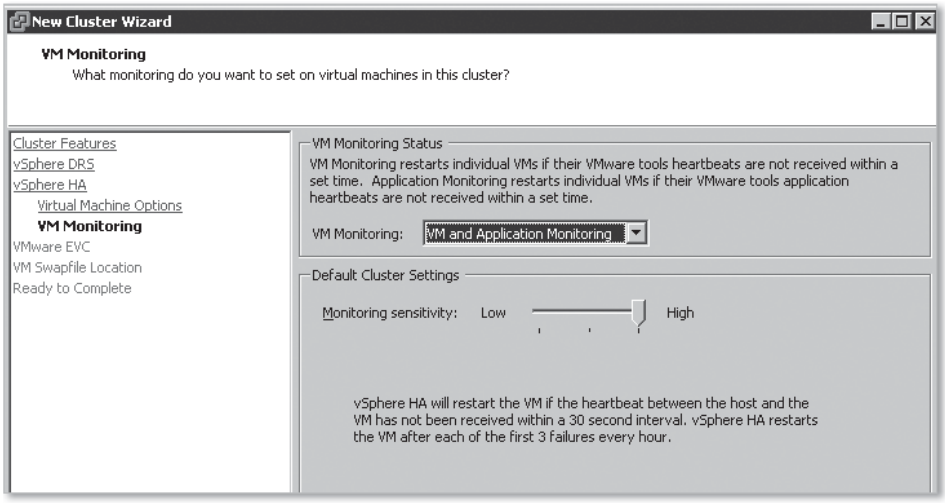


Abbildung 5.8 Applikationsüberwachung mittels HA

Ein Vorteil dieser Cluster-Lösung ist, dass keine redundante Hardware vorgehalten werden muss. Alle im HA-Verbund definierten ESX-Server sind aktive Server, die eine Anzahl von VMs hosten. Der größte Nachteil dieser Lösung ist jedoch der Ausfall und Neustart aller virtuellen Maschinen des ausgefallenen ESX-Servers. Durch die Strict Admission Control besteht beim Failover die Gefahr, dass VMs mangels Ressourcen auf den restlichen ESX-Servern nicht gestartet werden können. Durch eine Priorisierung in den HA-Eigenschaften einer VM können zumindest die wichtigen VMs zuerst gestartet werden und die weniger wichtigen VMs zuletzt, so dass eine eventuelle Ressourcenknappheit nur unwichtige VMs betrifft.

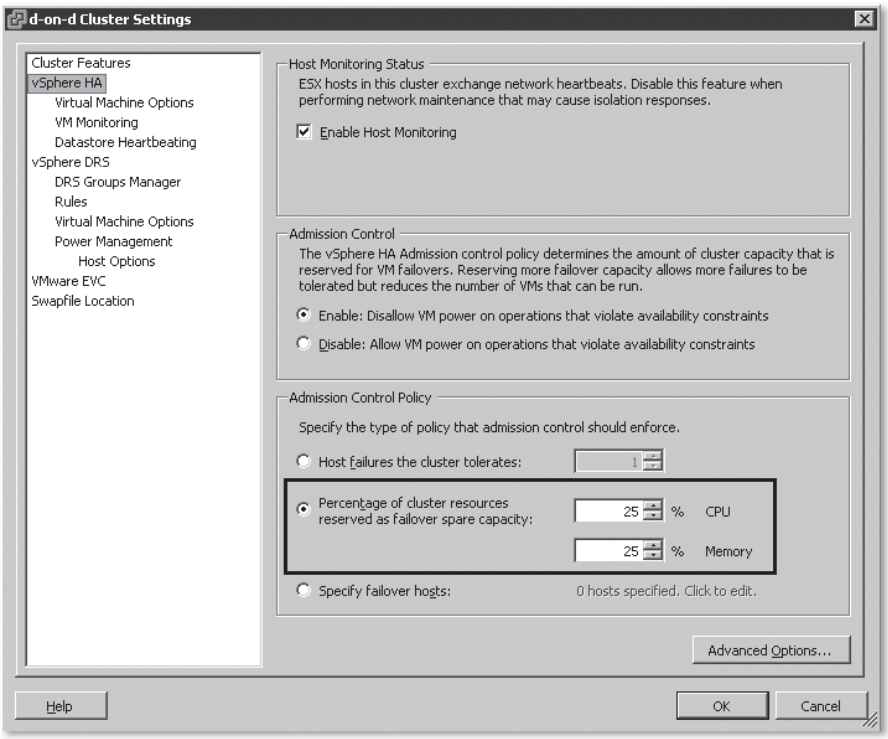


Abbildung 5.9 Admission Control mit Ressourceneinstellung

Sie sollten bei der Admission Control auf jeden Fall die prozentuale Einstellung der Ressourcen in Betracht ziehen, da in Umgebungen mit vielen ESX-Hosts im Cluster eine Host-Einstellung zu unscharf ist. Bei Scale-up-Clustern (wenige, hochperformante Server mit sehr vielen VMs pro Host) sollte der Failover-Host eine gute Alternative darstellen.

Auch ohne VC-Server

Ein HA-Cluster wird zwar über den vCenter-Server eingerichtet, bleibt aber auch ohne diesen lauffähig, da auf jedem ESX-Server lokale HA-Komponenten installiert sind, die unter anderen die komplette HA-Konfiguration vorhalten.

Es wird seit vSphere 5 nicht mehr zwischen primären und sekundären HA-Knoten unterschieden, was bei der Planung der Cluster-Umgebung deutliche Entspannung bringt. Das Konzept würde auf Master/Slave umgestellt, wobei nur noch ein Master existiert.

Des Weiteren ist ein HA-Cluster mit DRS kombinierbar: Beim Starten von virtuellen Maschinen wie auch im laufenden Betrieb wird immer die Auslastung der HA-Knoten im Cluster berücksichtigt, und je nach DRS-Konfiguration werden bestimmte VMs entweder automatisch auf freie ESX-Server verschoben, oder dies wird nur als Empfehlung ausgesprochen, um eine ausgewogene Lastverteilung zwischen den ESX-Servern zu erreichen.

5.2.2 Voraussetzungen für HA

Die Anforderungen für HA entsprechen zum größten Teil denen von vMotion, allerdings existiert keine zwingende Voraussetzung, gleiche Prozessoren in den ESX-Host-Systemen zu nutzen. Dies rührt daher, dass HA die virtuellen Maschinen nicht im aktiven Zustand migriert, sondern einschaltet, nachdem sie bereits durch den Ausfall gestoppt wurden. Daher gilt: »HA setzt voraus, dass jede VM auf jedem ESX-Host neu gestartet werden kann.«

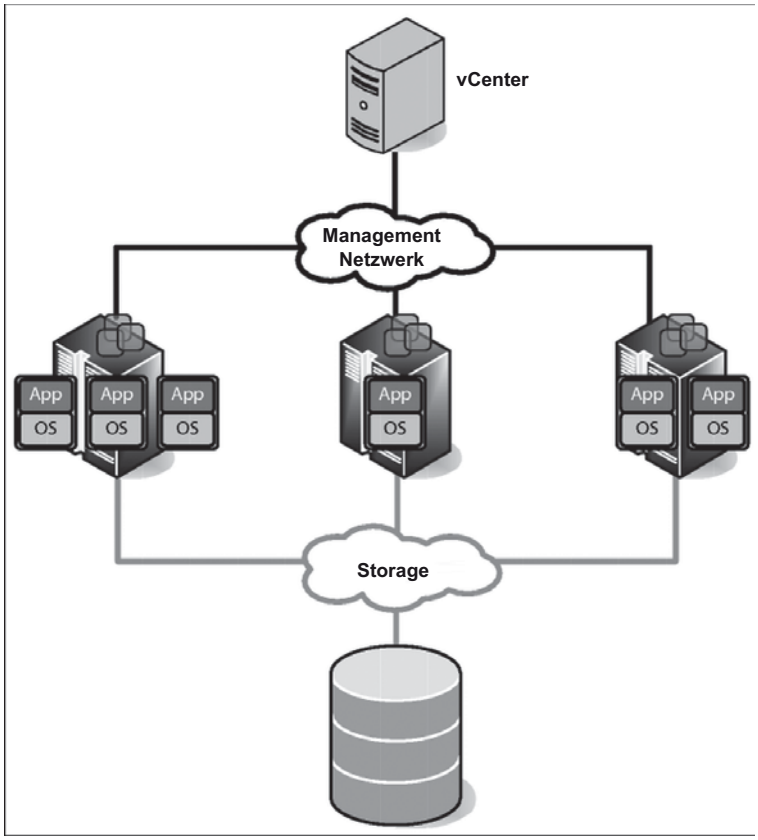


Abbildung 5.10 Grundstruktur Anforderungen vSphere HA – Service Console ist dabei das Management Interface

Die Empfehlungen zum Betrieb von vSphere HA lauten:

- vCenter-Integration
- zentraler SAN- oder NFS-Speicher, der von allen ESX-Systemen im Zugriff ist
- installierte und funktionstüchtige HA-Komponenten auf den ESX-Hosts (mindestens 3 GB RAM pro Host)
- DNS-Namensauflösung mit vSphere 5 kein kritisches Kriterium mehr, da der neue HA Agent mit IP Adressen arbeitet

- Managementnetzwerk-Verbindung zwischen allen ESX-Hosts im Cluster
- gleiche Netzwerkkonfiguration für die VMs auf allen ESX-Hosts im Cluster
- keine Managementnetzwerk-Verbindung zwischen ESX-Hosts über Router zulässig, die *gratuitous ARP* verwerfen

Tipp

Möchten Sie bei virtuellen Maschinen die Erfüllung der Anforderungen testen, so können Sie dafür vMotion Migration nutzen, da deren Voraussetzungen die von HA noch übertreffen. So ist es möglich, ohne Ausfall die HA-Fähigkeit einer VM zu überprüfen.

Aufgrund der Anforderungen an zentralen Shared Storage und direkte Netzwerkverbindungen zwischen den ESX-Hosts ist es manchmal schwierig, einen HA-Cluster zwischen mehreren Rechenzentren aufzubauen. Hier nutzt auch eine Replikation der Daten zwischen SAN-Systemen in den Rechenzentren nichts, sondern nur ein Zugriff auf die gleichen Daten. Schlagwörter sind Metro-Cluster und Stretched Cluster.

5.2.3 HA-Komponenten

Beim Einsatz von vSphere 5 HA kommen drei Komponenten ins Spiel: der vCenter Server, der ESX-Host-Prozess (hostd) und der FDM (Fault Domain Manager). Vor dem Sprung auf die Version 5 basierte HA auf den Komponenten des Legato Automated Availability Managers (AAM), der durch den Fault Domain Manager, eine Eigenentwicklung von VMware, ersetzt wurde.

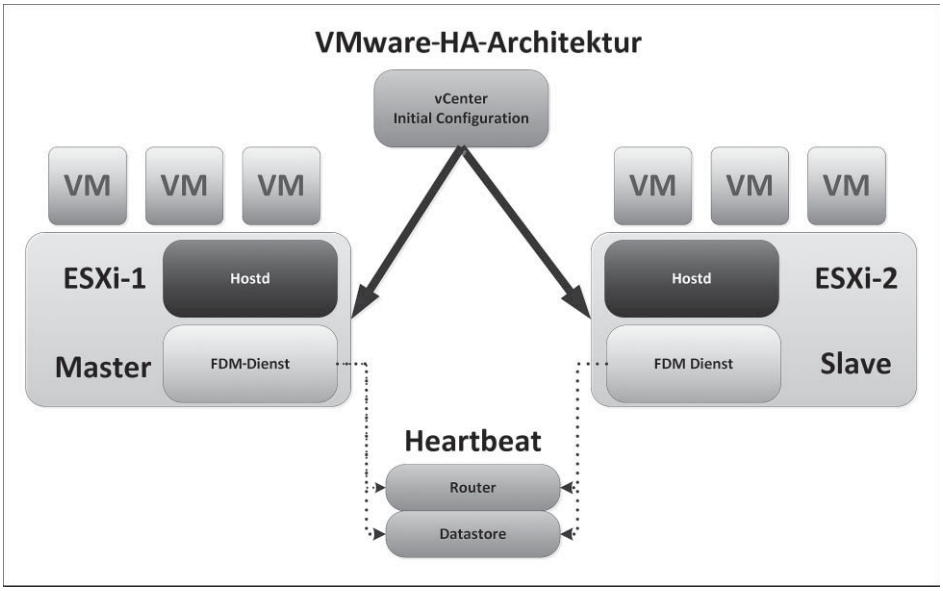


Abbildung 5.11 VMware-HA-Architektur

Die neue FDM-Komponente bringt deutliche Neuerungen gegenüber der früheren HA-Funktionalität mit sich, darunter:

- kein Primary/Secondary-Konzept mehr (ein Master, sonst Slaves)
- keine Agenteninstallation
- keine DNS-Abhängigkeit mehr (IP-basiert)
- Verbesserungen (Isolation Response, Admission Control)
- HA Protokollierung -> Syslog-fähig
- Netzwerk und Storage Heartbeat

5.2.4 Lizenzierung von HA

vSphere HA ist Bestandteil der vSphere Suite, die auf CPU-Sockel-vRAM-Basis lizenziert wird und ab der Edition Essentials Plus integriert ist.

5.2.5 Einrichtung von HA

HA kann schlicht durch Aktivierung des Features HA (Turn on vSphere HA) in den Eigenschaften eines Clusters oder bei der Neuerstellung eingerichtet werden. Damit werden die HA-Komponenten auf den ESX-Hosts aktiviert und kommunizieren miteinander.

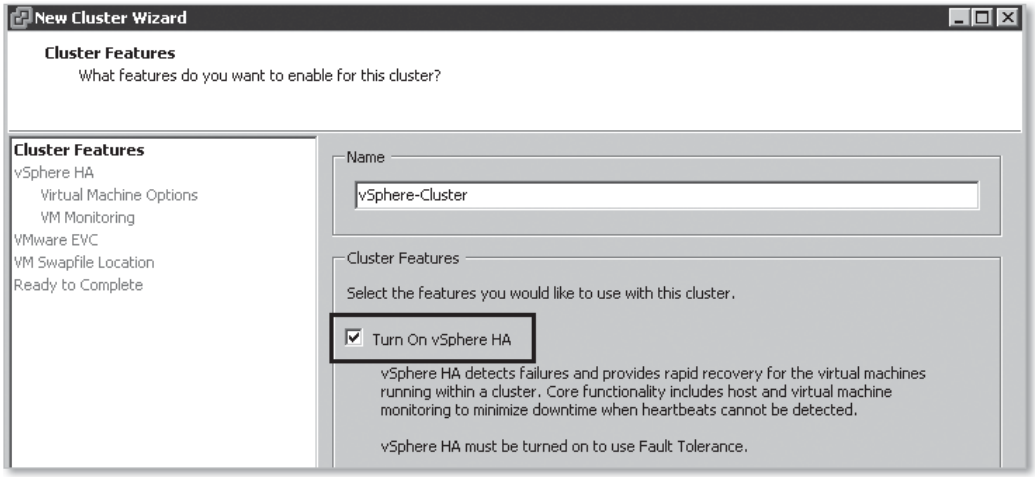


Abbildung 5.12 Aktivierung des VMware-HA-Features

Danach können Sie HA an die Bedürfnisse der Infrastruktur anpassen (siehe Abbildung 5.13).

Enable Host Monitoring

Die Option Enable Host Monitoring ❶ (siehe Abbildung 5.13) ist sinnvoll, wenn Sie Wartungsarbeiten an ESX-Hosts innerhalb eines Clusters ausführen, die zum Verlust der Heart-

beat-Pakete führen würden. Ein typischer Fall wäre ein Austausch oder ein Firmware-Upgrade von Ethernet-Switches. Der Schalter ist neu mit vSphere hinzugekommen und sollte vor der eigentlichen Wartung deaktiviert und nach Abschluss der Wartungsarbeiten wieder aktiviert werden.

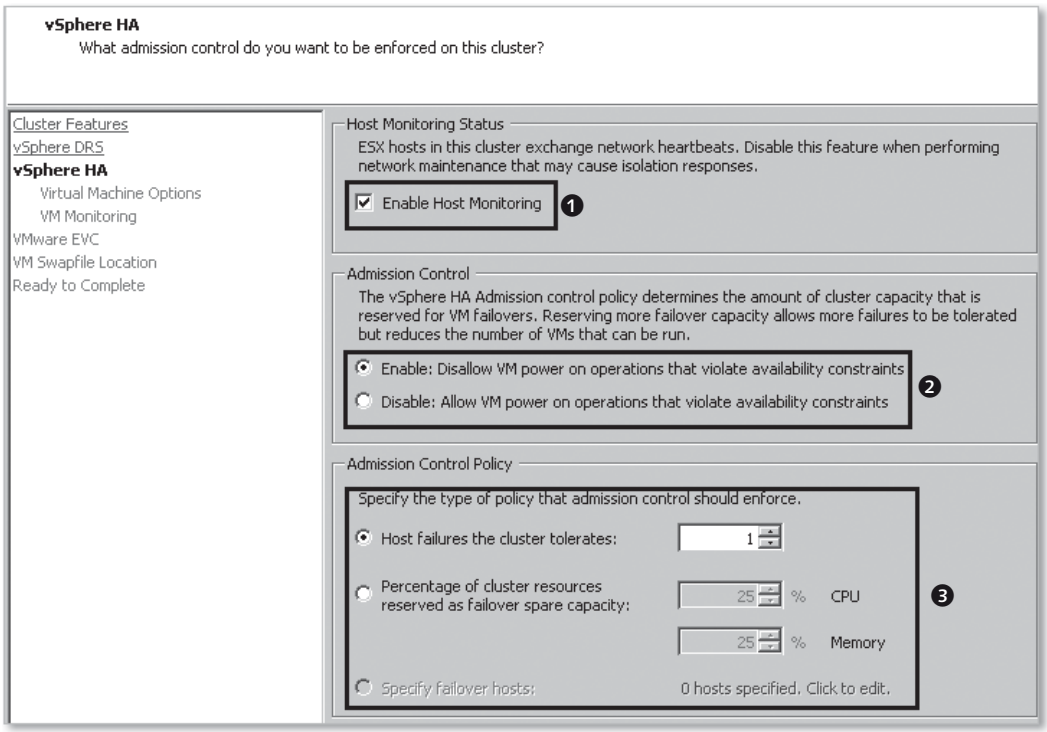


Abbildung 5.13 Konfigurationsübersicht der HA-Funktionen

HA-Failover-Capacity und Admission Control

Die HA-Failover-Capacity ❸ (siehe Abbildung 5.13) gibt die Anzahl von ausgefallenen ESX-Servern an, die ein HA-Cluster verkraften soll. Der vCenter-Server errechnet eigenständig, wie viel Ressourcen insgesamt im Cluster verfügbar sein müssen, um den Ausfall der angegebenen Anzahl von ESX-Servern abzufangen.

Als Grundlage hierfür dient der ESX-Server mit der stärksten Auslastung, wobei dieser Umstand eine sehr konservative Berechnung ergibt. Optimal wäre hier die Kombination von HA mit DRS, so dass alle ESX-Server im Cluster-Verbund mit einer ausgewogenen Lastverteilung aktiv sind. Der HA-Cluster überwacht dann die Gesamtmenge von startbaren virtuellen Maschinen, um die errechnete Kapazität nicht zu unterschreiten. Diese Funktion wird *Admission Control* genannt.

Die Admission Control ❷ (siehe Abbildung 5.13) überwacht die aktuelle Auslastung aller ESX-Server im HA-Cluster und stellt sicher, dass nicht so viele Ressourcen verbraucht werden, dass die HA-Failover-Capacity gefährdet ist. Das Sicherstellen der verfügbaren Ressourcen erfolgt mit der möglichen Sperre folgender Operationen:

- Start von virtuellen Maschinen
- Migration einer aktiven virtuellen Maschine in einen HA-Cluster
- zu einem Snapshot einer ausgeschalteten virtuellen Maschine zurückrollen und diesen aktivieren
- Erhöhen von CPU- oder Memory-Resource-Settings einer virtuellen Maschine

Diese Überwachung verringert die Flexibilität der ESX-Server im HA-Cluster und kann mit der Deaktivierung der Admission Control ausgeschaltet werden. Dadurch können mehr virtuelle Maschinen gestartet werden, als die Admission Control erlauben würde. Dabei signalisiert der vCenter-Client einen HA-Cluster mit niedriger Failover-Kapazität nicht mit einem roten Symbol, und virtuelle Maschinen können nach Belieben gestartet werden. Die Folge dieser Aufhebung ist eine reduzierte Kapazität, um die konfigurierte Anzahl von ESX-Server-Ausfällen abzufangen. Werden jetzt bei einem Ausfall die virtuellen Maschinen auf den übrigen ESX-Servern neu gestartet, entscheidet die HA Restart Priority einer VM, wann diese gestartet wird, um somit die letzten freien Ressourcen des HA-Clusters in Beschlag zu nehmen. VMs mit einer niedrigen Priorität laufen Gefahr, mangels Ressourcen nicht mehr gestartet werden zu können.

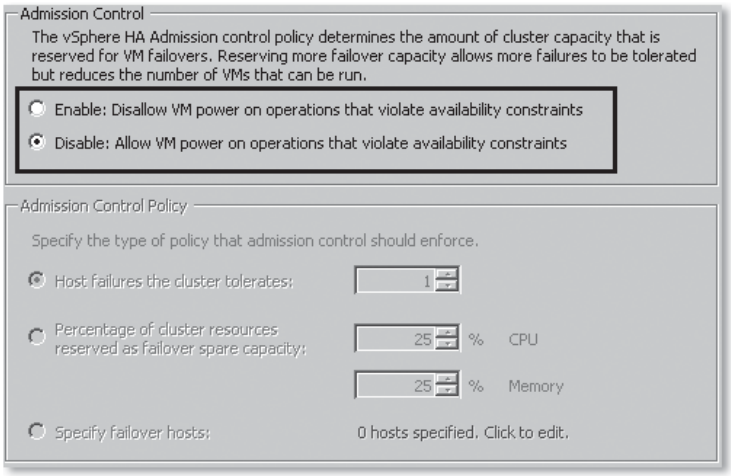


Abbildung 5.14 Deaktivierung der Ressourcenkontrolle der »Admission Control«

Dieses Standardverfahren der Admission Control können Sie jedoch in einem eingegrenzten Rahmen konfigurieren. So besteht auch die Möglichkeit, die Ressourcensperre der Admission Control komplett aufzuheben und auch bei erschöpften Ressourcen die VMs immer noch zu

starten. Die Auswahl treffen Sie mit dem Schalter Allow VM power on operations that violate availability constraints. In diesem Fall ist es auch nicht mehr möglich, die Admission Control Policy detaillierter zu konfigurieren, und der Bereich wird grau unterlegt.

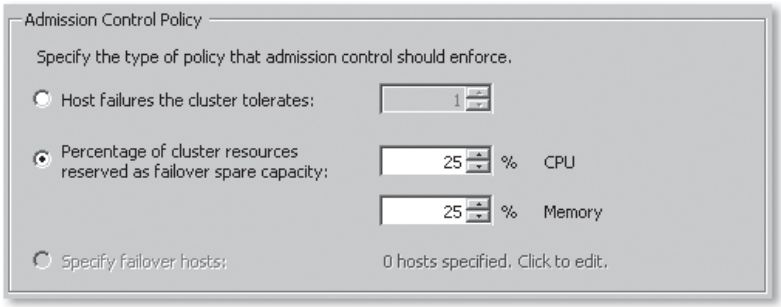


Abbildung 5.15 Admission Control Policy zur Detaileinstellung der HA-Regeln

Belassen Sie die Admission Control bei Disallow VM power on operations that violate availability constraints, so können Sie die zu nutzenden Regeln weiter konfigurieren, siehe Tabelle 5.1.

Option	Beschreibung
Host failures the cluster tolerates	Die Anzahl der Hosts, die ausfallen dürfen, bevor der Cluster nicht mehr aktiviert wird. Die Admission Control nimmt dies als Berechnungsgrundlage, um das Starten weiterer Systeme zu prüfen.
Percentage of cluster resources reserved as failover spare capacity	Prozentzahl der Ressourcen, die bei der Laufzeit aller Systeme noch ungenutzt bleiben müssen, um Ausfälle abfangen zu können. Wahrscheinlich die beste Einstellung.
Specify failover host	Angabe des ESX-Hosts, der bei Ausfall eines anderen ESX-Hosts die VMs übernimmt

Tabelle 5.1 Admission-Control-Policy-Optionen

Zuletzt ist es auch möglich, die Advanced Options direkt zu beeinflussen.

Datastore-Heartbeat

Neben dem Netzwerk-Heartbeat existiert unter vSphere 5 ein Datastore-Heartbeat, der zu dem Netzwerkausfall prüft, ob die Dateien der virtuellen Maschinen noch im Zugriff sind. Somit existiert ein weiterer Test, ob die VM wirklich ausgefallen sind oder nur die Managementschnittstelle des ESX-Hosts.

Bei Nutzung der Standardeinstellung werden (sofern verfügbar) zwei Datastores getestet, was Sie mit der Option das.heartbeatDsPerHost auf maximal fünf erhöhen können.

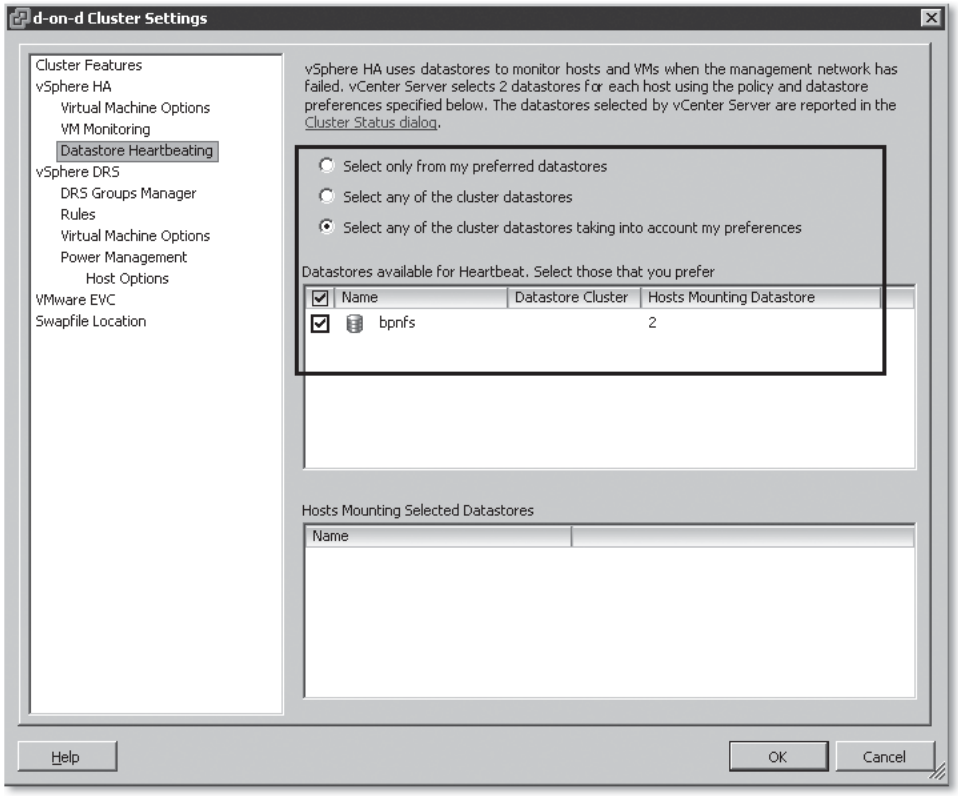


Abbildung 5.16 Einrichtung des Datastore-Heartbeats

5.2.6 ESX 4 und ESX 5 im Mix

VMware hat den neuen FDM HA Agent abwärtskompatibel entwickelt, d. h., bei ESX 4.x-Servern wird der gleiche FDM Agent auf die Server installiert wie der unter ESX 5 genutzte. Somit können ESX 4- und ESX 5- Systeme in einem HA-Cluster-Verbund gemeinsam existieren.

5.2.7 HA Advanced Options

Es existiert eine Vielzahl von erweiterten Optionen für den Einsatz des HA-Clusters, um diesen auf die vielfältigen Gegebenheiten der Kunden und der Infrastruktur einzustellen.

Eine komplette Liste aller Optionen finden Sie unter: *http://www.yellow-bricks.com/vmware-high-availability-deepdiv/#HA-advancedsettings*.

Die Advanced Options (siehe Tabelle 5.2) legen Sie in den Eigenschaften des Cluster-Objektes fest.

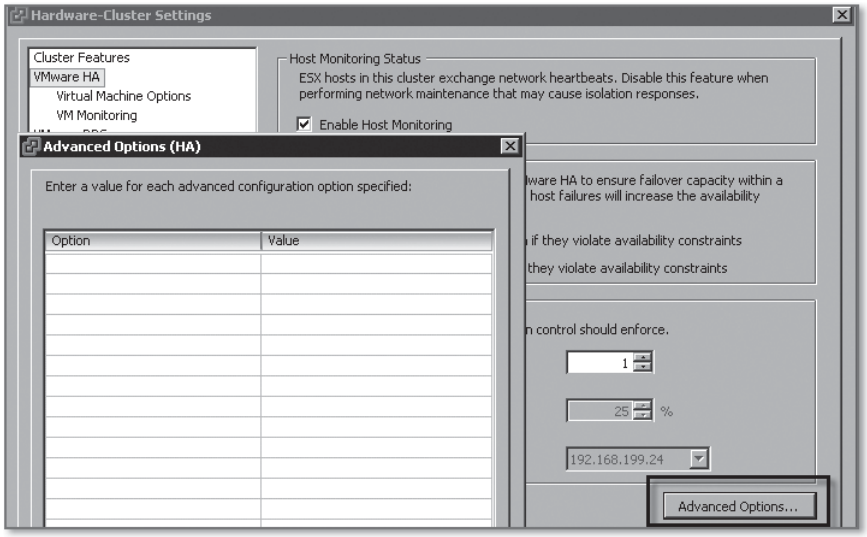


Abbildung 5.17 »Advanced Options« in den Cluster-Eigenschaften

Option	Beschreibung
`das.failuredetectiontime`	Anzahl Millisekunden des Timeouts für die Isolation Response (Standard 15.000 Millisekunden). Bei Anpassung der `das.isolationaddress` wurde der Wert früher erhöht. Mit vSphere 5 kann der Defaultwert beibehalten werden.
`das.isolationaddress[x]`	IP-Adressen der Service Console des ESX-Hosts, die für Heartbeat-Tests genutzt werden soll; `[x]` = `1–10`. Im Standard wird nur das Default-Gateway genutzt.
`das.usedefaultisolationaddress`	Wert kann `true` oder `false` annehmen und gibt an, ob das Default-Gateway als Heartbeat-Adresse genutzt werden soll.
`das.vmMemoryMinMB`	Hauptspeichermenge für die Slot-Berechnung – Admission Control
`das.vmCpuMinMHz`	CPU-MHz für die Slot-Berechnung – Admission Control
`das.allowNetwork[x]`	Dedizierte Eintragung, welche Netzwerke als Heartbeat-Netzwerke verwendet werden dürfen; `[x]` = 1–10. Als Wert muss der wirklich genutzte Portname angegeben werden, z. B. »Service Console 2«.
`das.ignoreRedundantNetWarning`	Entfernen der Warnung, falls keine redundanten Service-Console-Ports existieren. Standardwert ist `false`, und `true` verhindert die Warnung.

Tabelle 5.2 »Advanced Options« für vSphere HA

Mit vSphere 5 kamen neue Advanced Settings (siehe Tabelle 5.3) hinzu.

Die wichtigsten ADVANCED OPTIONS des HA-Clusters sind `das.isolationaddress[]`, `das.usedefaultisolationaddress`, `das.allowNetwork`, `das.ignoreRedundantNetWarning` und `das.failuredetectiontime`.

Option	Beschreibung
das.heartbeatDsPerHost	Anzahl der benötigten Heartbeat-Datastores, bevor ein Ausfall erkannt wird. (Default 2; Wert sollte zwischen 2 und 5 liegen)
das.config.log.maxFileNum	Anzahl der Rotationen der Protokolldateien
das.config.log.maxFileSize	Maximalgröße der Protokolldateien
das.config.log.directory	Pfad zu den Protokolldateiablagen
das.config.fdm.deadIcmpPingInterval	Anzahl der Ping-Versuche des Masters (Default 10), bevor ein Host als Problemfall gilt
das.config.fdm.icmpPingTimeout	Antwortzeit auf einen Ping-Request in Sekunden (Default 5)
das.config.fdm.hostTimeout	Zeitintervall in Sekunden (Default 10), bevor ein Slave-Host als ausgefallen markiert wird und der Prozess zum Filtern des Ereignisses (Ausfall, isoliert, Teilausfall) gestartet wird.
das.config.fdm.storageVmotionCleanupTimeout	Bei der Storage vMotion Migration von VMs unter vSphere kann es zu einer Zeitverzögerung beim Verschieben des Home-Verzeichnisses der VM kommen, die vom FDM-Master als Ausfall interpretiert werden könnte, so dass die VM neu gestartet würde. Der Default-Timeout von 900 Sekunden soll dies verhindern.
das.config.fdm.policy.unknownStateMonitorPeriod	Zeitintervall in Sekunden, bevor der Master eine als ausgefallene VM neu startet

Tabelle 5.3 Wichtige neue vSphere 5-HA-Optionen

das.isolationaddress

Ein Beispiel zur Nutzung dieser Option ist sehr einfach gefunden, da es aus Sicherheitsgründen oft sinnvoll ist, neben dem Default-Gateway weitere Systeme als Heartbeat-Ziel zu nutzen, um eine Isolation auszuschließen (siehe Abbildung 5.18).

Soll neben dem Default-Gateway, der z. B. ein HSRP-geschützter (Cisco Hot Standby Router Protocol – eine dynamische Adresse zeigt auf zwei Router) Router sein könnte, auch auf die beiden physischen Adressen der Router und des vCenter-Servers (192.168.199.22) gepingt werden, so sähen die Advanced Options wie folgt aus:

```
das.isolationaddress[1]    =    192.168.199.2
das.isolationaddress[2]    =    192.168.199.3
das.isolationaddress[3]    =    192.168.199.22
```

das.allowNetwork

Wann sollten Sie ein Heartbeat-Netzwerk definieren? Immer dann, wenn die Netze untereinander nicht direkt verbunden sind, sondern z. B. ein Router dazwischen eingesetzt werden muss. Dies kann bei physischer Trennung oder bei Nutzung unterschiedlicher IP-Adressen sinnvoll sein (siehe Abbildung 5.19).

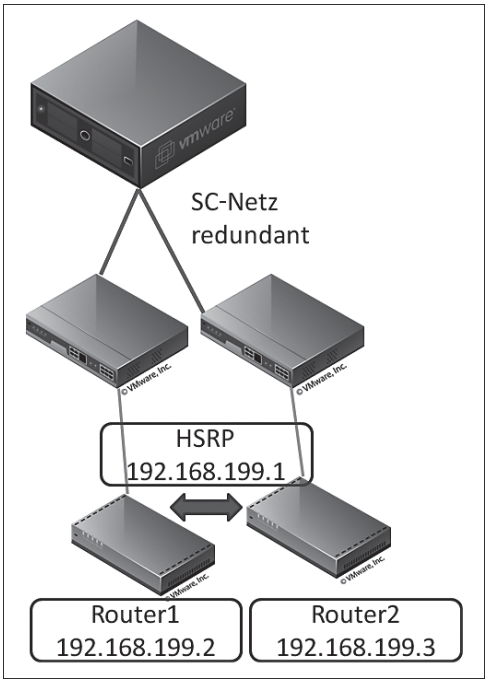


Abbildung 5.18 HSRP-ausfallsichere Konfiguration der beiden physischen Router

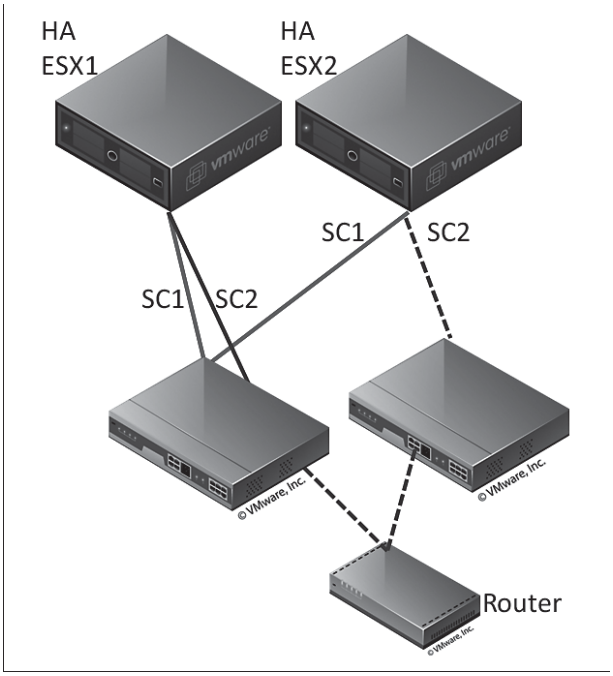


Abbildung 5.19 HA-Heartbeat-Pakete können nicht über Router weitergeleitet werden.

In unserem Beispiel ist es daher notwendig, das SC2-Netzwerk auszuklammern und nur das SC1-Netzwerk zu nutzen.

```
das.allowNetwork[1] = "SC1"
```

Zusätzlich entsteht das Problem, dass ESX2 keine Redundanz mehr besitzt. Daher wäre auch die Einstellung `das.ignoreRedundantNetWarning` interessant, zu der wir folgend kommen. Idealer wäre natürlich die Nutzung einer weiteren Netzwerkkarte.

das.ignoreRedundantNetWarning

Zu `das.ignoreRedundantNetWarning` müssen wir kein ausführliches Beispiel beschreiben. Haben Sie ein Testsystem konfiguriert und verfügen Sie dort nicht über genügend Netzwerkadapter, so werden Sie zwangsweise über Meldungen betreffend mangelnder Redundanz stolpern. Sind Sie davon genervt, ändern Sie `das.ignoreRedundantNetWarning` einfach auf `True`.

5.2.8 Virtual Machine Options

Da vSphere HA in erster Linie die VMs schützen soll und nicht die Host-Systeme, können Sie Regeln für einzelne virtuelle Maschinen aufstellen und auch das allgemeine Verhalten beim Neustart der VMs sowie das Verhalten bei erkannter Isolation konfigurieren.

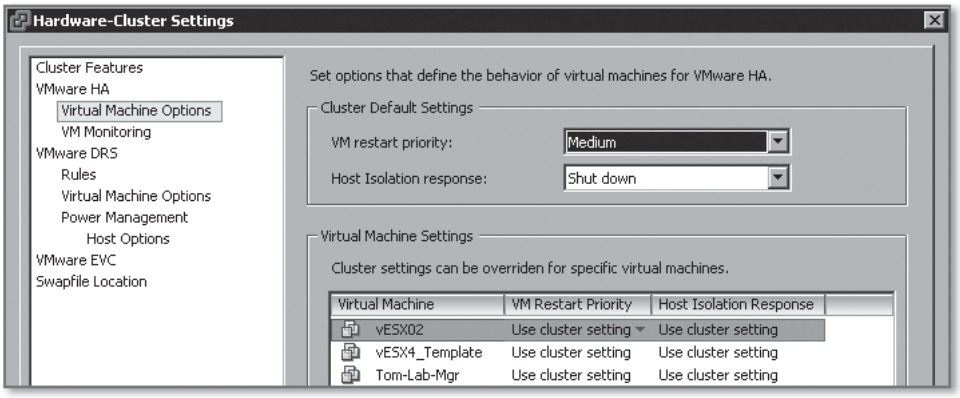


Abbildung 5.20 Mit den »Virtual Machine Options« können Sie unter anderem die Host Isolation Response konfigurieren.

Schauen Sie sich die Cluster Default Settings, also die Standardeinstellungen für alle virtuellen Maschinen innerhalb des Clusters, an, so stellen Sie fest, dass Sie die Priorität des Neustarts global setzen können. Eine Anpassung des Standards Medium ist allerdings nur sinnvoll, wenn Sie einzelnen virtuellen Maschinen andere Werte zuweisen möchten, z. B. High. Ansonsten spielt diese Einstellung keine Rolle, da ja jede VM die gleiche Priorität hat, unabhängig von High, Medium oder Low.

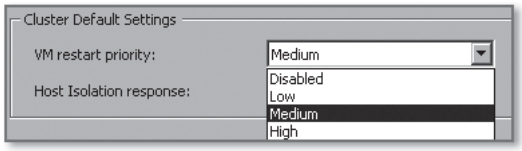


Abbildung 5.21 VM Restart Priority

Die Host Isolation response ist mit die wichtigste Einstellung des HA-Clusters, da sie die Reaktion des isolierten ESX-Hosts bestimmt. Ist dieser wirklich ausgefallen, sind sowieso alle virtuellen Maschinen offline, und die restlichen Cluster-Mitglieder können die VMs neu starten. Ein Problem tritt auf, wenn der Host samt virtuellen Maschinen noch läuft, aber das Heartbeat-Netzwerk der Service Console aussetzt.

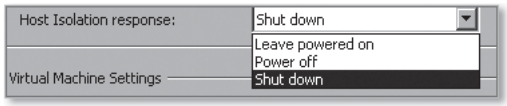


Abbildung 5.22 Host Isolation Response

Hier müssen Sie sich Gedanken machen, ob die virtuellen Maschinen dann wirklich automatisch vom ESX-Host gestoppt werden sollen (und wenn, in welcher Form) oder ob sie aktiv bleiben sollen. Entscheiden Sie sich für eine Abschaltung, bedeutet Power off das harte Abschalten der VM, während Shut down die virtuelle Maschine über die VMware Tools aus dem Gast heraus herunterfährt.

Die Entscheidung fällt leicht, wenn die physischen Switches, auf denen das Management Netz liegt, unabhängig von den physischen Switches der virtuellen Maschinen betrieben werden. In diesem Fall kann es zu einer Störung des Managementnetzwerks kommen, während die VMs aber normal weiterlaufen. Daher sollten Sie die Host Isolation Response auf Leave powered on einstellen. Dies gilt generell, wenn Probleme im Netzwerk einer Infrastruktur nicht selten sind.

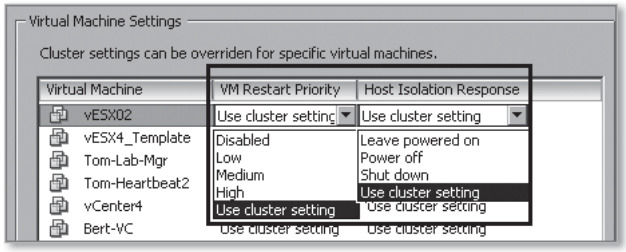


Abbildung 5.23 Einstellungen pro virtueller Maschine

Hinweis

Alle übrigen ESX-Hosts, die den isolierten Host als ausgefallen erkennen, können ihrerseits die VMs nicht neu starten, da die Festplattendateien der virtuellen Maschinen während der Laufzeit gesperrt sind.

Die Einstellungen zur Restart-Priorität und zur Isolation Response können Sie auch für jede einzelne VM getrennt unter Virtual Machine Settings einrichten, wenn diese Anforderung besteht. Hier ist es beispielsweise sinnvoll, die wichtigsten VMs mit einer hohen Priorität zu versehen, während alle anderen VMs im Standard auf Normal bleiben.

5.2.9 Der HA-Agent oder »Was passiert beim Hinzufügen eines ESX-Hosts zum HA-Cluster?«

Diese Frage ist zurzeit im Gegensatz zu früheren HA-Versionen leicht zu beantworten: Wenn der erste ESX-Server einem Cluster hinzugefügt wird, wird er automatisch Master, jeder nachfolgende Server wird ein Slave.

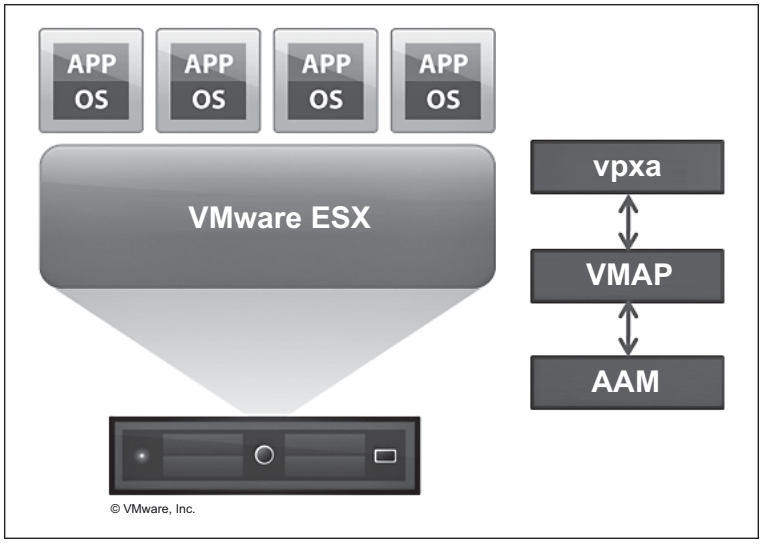
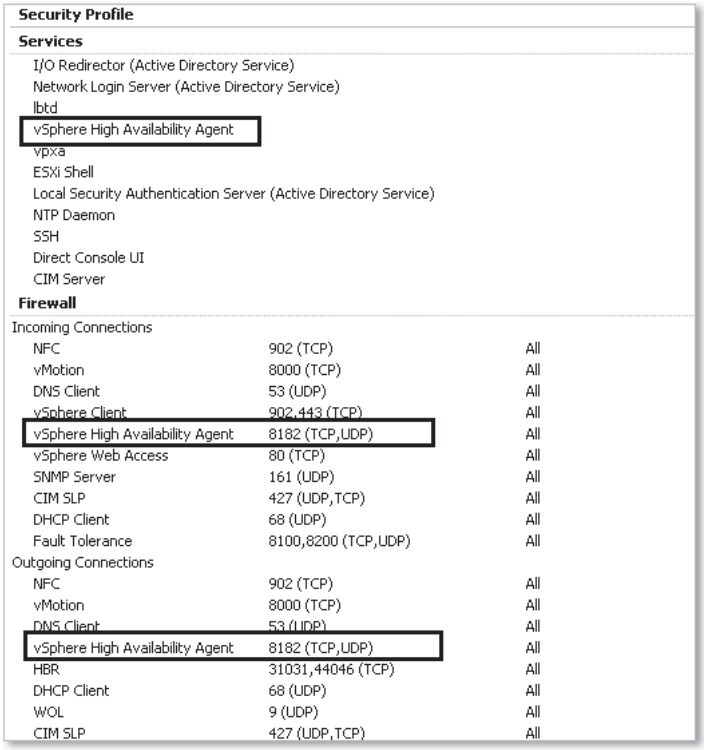


Abbildung 5.24 HA-Cluster-Prozesse pro ESX-Server

Die HA-Agents überwachen sich im Verbund gegenseitig durch einen HA-Heartbeat über das Netzwerk-Interface des Managementnetzwerks. Die Datenbank mit den vCenter-Informationen hält der Agent im RAM vor.

Außerdem wird automatisch in der Firewall des ESX-Hosts der vSphere High Availability Agent erlaubt, der u. a. für die Heartbeat-Kommunikation zuständig ist.



Security Profile		
Services		
I/O Redirector (Active Directory Service)		
Network Login Server (Active Directory Service)		
lbtd		
vSphere High Availability Agent		
vpxa		
ESXi Shell		
Local Security Authentication Server (Active Directory Service)		
NTP Daemon		
SSH		
Direct Console UI		
CIM Server		
Firewall		
Incoming Connections		
NFC	902 (TCP)	All
vMotion	8000 (TCP)	All
DNS Client	53 (UDP)	All
vSphere Client	902,443 (TCP)	All
vSphere High Availability Agent	8182 (TCP,UDP)	All
vSphere Web Access	80 (TCP)	All
SNMP Server	161 (UDP)	All
CIM SLP	427 (UDP,TCP)	All
DHCP Client	68 (UDP)	All
Fault Tolerance	8100,8200 (TCP,UDP)	All
Outgoing Connections		
NFC	902 (TCP)	All
vMotion	8000 (TCP)	All
DNS Client	53 (UDP)	All
vSphere High Availability Agent	8182 (TCP,UDP)	All
HBR	31031,44046 (TCP)	All
DHCP Client	68 (UDP)	All
WOL	9 (UDP)	All
CIM SLP	427 (UDP,TCP)	All

Abbildung 5.25 Firewall-Einträge für den HA-Agent

5.2.10 Reconfigure for vSphere HA

Der laufende FDM-Prozess von vSphere HA auf dem ESX-Host wird durch einen zusätzlichen Monitoring-Prozess überwacht, der diesen Prozess bei Ausfall automatisch neu startet. Dies hilft bei versehentlichem Stoppen des FDM oder bei kleineren Problemen. Sollte ein Konfigurationsfehler vorliegen, schafft oft ein Reconfigure for HA im Kontextmenü des ESX-Hosts Abhilfe. Dieser Aufruf rekonfiguriert den HA-Agent komplett und startet ihn neu (siehe Abbildung 5.26).

5.2.11 Das Verhalten eines HA-Clusters

Der Master-Agent in einem Cluster überwacht die Verfügbarkeit der ESX-Server und startet die virtuellen Maschinen des ausgefallenen HA-Knotens auf den verbleibenden ESX-Servern mit genügend freier Kapazität neu. Die Heartbeat-Pakete, die zur Funktionsüberprüfung der einzelnen Systeme genutzt werden, werden sekündlich über alle Management-Verbindungen verschickt, und falls konfiguriert werden zusätzlich die Datastores bzw. deren Verfügbarkeit getestet.

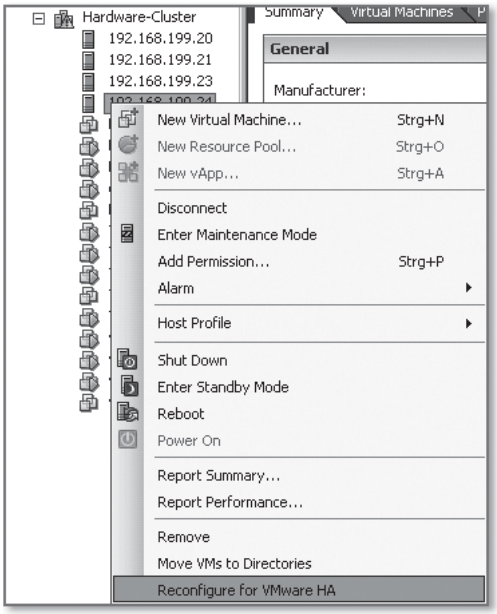


Abbildung 5.26 »Reconfigure for vSphere HA« kann bei Konfigurationsproblemen des Clusters Wunder bewirken.

Ist die aktuelle Failover-Kapazität des HA-Clusters unter dessen konfigurierte Failover-Kapazität gefallen, zeigt sich das Cluster-Symbol im vCenter-Client bei aktiver Admission Control rot. Das rote Symbol kann zum einen durch Ausfall zu vieler ESX-Server bedingt sein oder zum anderen durch zu hohe Belegung der ESX-Server mit virtuellen Maschinen. Haben Sie bei den virtuellen Maschinen keine HA-Restart-Priorisierung vergeben, werden die ausgefallenen virtuellen Maschinen nacheinander auf den verbleibenden ESX-Servern gestartet, bis die Kapazität der ESX-Server erschöpft ist. Dies kann zur Folge haben, dass wichtige VMs nicht mehr gestartet werden können. Das Vergeben einer HA-Priorität hilft, diese Problematik etwas zu entschärfen, indem ein ESX-Administrator den wichtigeren VMs eine höhere Priorität verleiht, damit diese frühestmöglich gestartet werden, um die freien Ressourcen garantiert zu erhalten. Virtuelle Maschinen mit einer niedrigeren Priorität fallen dann gegebenenfalls der Ressourcenknappheit zum Opfer.

Ein Sonderfall stellt der Ausfall eines ESX-Servers während einer vMotion-Operation dar: Fällt der ursprüngliche ESX-Server aus, so versucht HA, die betreffende virtuelle Maschine auf dem vom Administrator vorgesehenen Ziel-Server der vMotion-Operation zu starten. Fällt hingegen der Ziel-Server aus, wird HA versuchen, diese VM auf dem ursprünglichen ESX-Server wieder zu starten. Fallen im Extremfall beide an der vMotion-Operation beteiligten ESX-Server aus, wird HA versuchen, einen dritten ESX-Server mit ausreichend verfügbarer Kapazität zu finden, um die betroffene virtuelle Maschine darauf erneut zu starten.

Bei einem HA-Failover werden die virtuellen Maschinen mit der höchsten Priorität zuerst gestartet. Dabei wählt HA, je nach Version des vCenter-Servers, über zwei verschiedene Wege die ESX-Server aus, auf denen die VMs neu gestartet werden: Die Version 2.0 des vCenter-Servers bedient sich der ESX-Hosts anhand der alphabetischen Auflistung der ESX-Knoten mit ausreichenden Ressourcen; ab der Version 2.1 wird der ESX-Knoten mit den meisten nicht reservierten Ressourcen als erster herangezogen.

5.2.12 HA-Slot-Berechnung

Nahezu 100 % aller VMware-Kunden, die auf Memory-Reservierungen in virtuellen Maschinen setzen und diese VMs innerhalb eines HA-Clusters betreiben, schalten unbewusst die Cluster-Übernahme ab (`Current Failover Capacity = 0`). Hintergrund ist die doch etwas eigensinnige Interpretation der Slot-Berechnung, die vSphere HA vornimmt. Ein Standard-Slot bewegt sich in folgenden Grenzen: 256 MHz, 256 MB oder maximale Arbeitsspeicherreservierung einer VM im Cluster + Overhead.

Dies führte bereits bei vielen Kunden zu Verständnisproblemen und Verstimmung, wenn die `Current Failover Capacity` automatisch auf `0` ging, obwohl nur eine virtuelle Maschine über eine CPU oder Memory-Reservierung verfügte. Kann der Cluster beispielsweise insgesamt 128 GB RAM bereitstellen, so kann bei einer Gesamtanzahl von 40 VMs bereits eine VM mit 4-GB-RAM-Reservierung die `Current Failover Capacity` auf `0` herunterbringen. Hier würde man sich wünschen, dass stets mit dem Standard-Slot von 256 MB gerechnet würde und die reservierten Memory-Mengen einfach einzeln summiert würden. Glücklicherweise ist der Cluster immer noch betriebsbereit, auch wenn die `Current Failover Capacity` auf `0` steht.

Abbildung 5.27 Ressourcenwarnung aufgrund einer Verletzung der HA Admission Control

Trotzdem ist ab diesem Zeitpunkt ein gewisses Unbehagen beim Administrator vorhanden, und mögliche Fehler oder Probleme werden vielleicht übersehen, da die Admission Control aufgrund dieser seltsamen Berechnung zumeist abgeschaltet wird. Bleibt die Admission Control aktiv, so erhalten Sie direkt beim Starten einer VM eine Fehlermeldung, und der Start wird verhindert. Die aktuellen Slot-Größen lassen sich unter dem Menüpunkt HA Advanced Runtime Info im Summary des Clusters einsehen.

Dieses Problem können Sie umgehen, indem Sie die Admission Control auf einen Prozentteil des gesamten Clusters setzen (Abbildung 5.29). Damit ändern Sie die fixe Regel in eine relative Bewertung. Diese relative Bewertung ist auch bei Clustern mit vielen ESX-Hosts (6 und mehr) interessant, um die Slot-Berechnung zu optimieren.

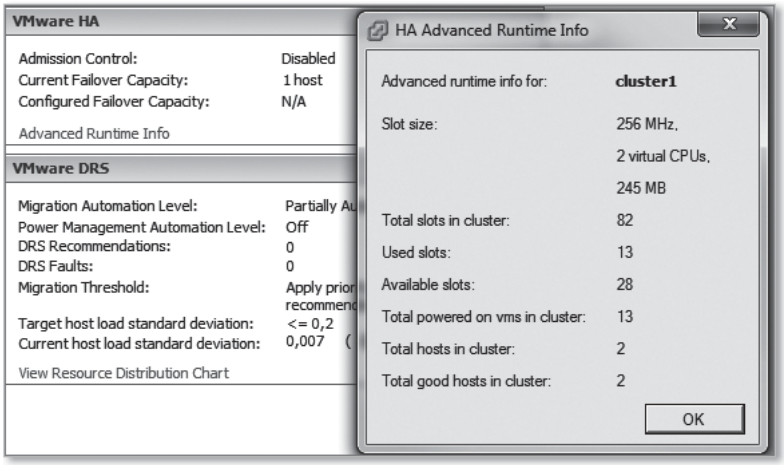


Abbildung 5.28 »Advanced Runtime Info« eines HA-Clusters

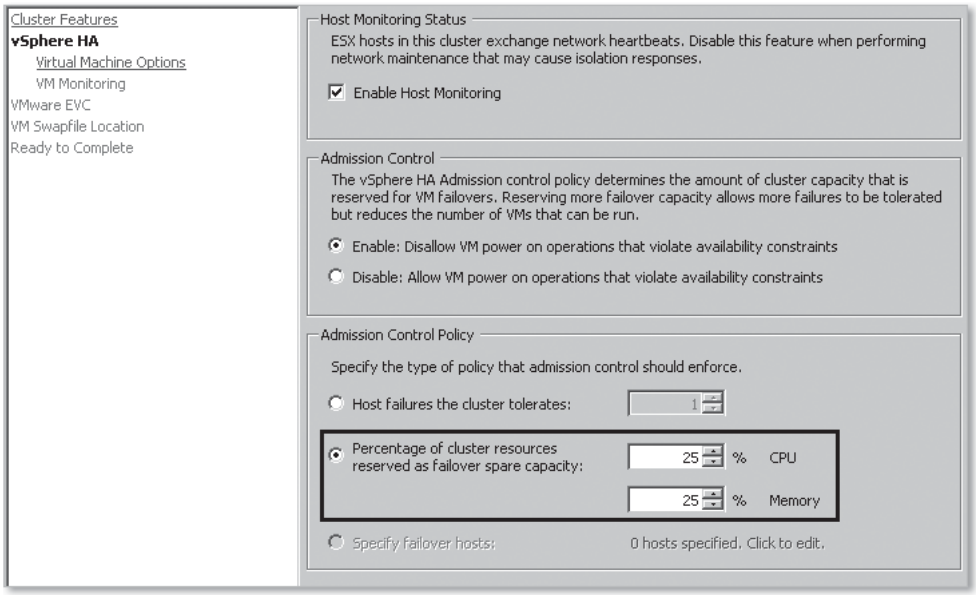


Abbildung 5.29 Cluster-Ressourcen nicht fix, sondern relativ angeben

5.2.13 HA-Master- und -Slave-Agents

Vor vSphere 5 war die Aufteilung der HA-Agents auf Primary und Secondary und die Limitierung der Primarys auf 5 ein großes Thema beim Design von Cluster. Zum Problem konnte es sogar werden, wenn der Cluster über unterschiedlichen Rechenzentren hinweg konfiguriert wurde. Dies hat sich mit vSphere 5 erledigt, da das Verfahren und die beteiligten Agents komplett neu geschrieben wurden.

Ganz abgelegt wurde das Konzept aber nicht, und so gibt es nach wie vor zwei Typen von Agents: Master und Slave. Es existiert im neuen HA-Modell immer nur ein Master; er nimmt die folgenden Aufgaben wahr:

- Neustart ausgefallener VMs
- Kommunikation mit dem vCenter
- Überwachung der Slaves

Welcher Host Master ist, können Sie im Summary des ESX-Hosts einsehen (Abbildung 5.30).

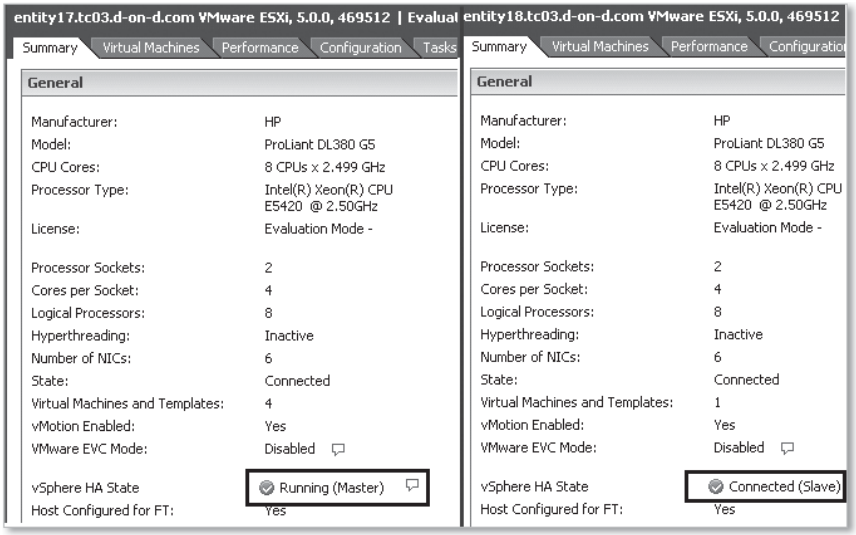


Abbildung 5.30 Status der HA-Agents

5.2.14 HA Host Isolation

Wie bereits erwähnt, werden die Heartbeat-Pakete im Standard sekündlich verschickt und auch erwartet. Verliert das Managementnetzwerk eines aktiven ESX-Knotens im HA-Cluster die Netzwerkverbindung, ohne aber komplett auszufallen, nennt man diesen ESX-Server *isoliert*. Der Master-Server würde diesen Zustand erkennen und den Neustart der vermeintlich ausgefallenen VMs beginnen. Fällt der Master aus, ernennen die übrigen HA-Slaves einen neuen Master untereinander. Der sich selbst ebenfalls als isoliert erkennende Master stuft sich automatisch herab. Da der ESX-Server aber nur die Netzwerkverbindung verloren hat, die notwendigen Prozesse der virtuellen Maschinen jedoch weiterhin laufen, sind auch diese noch aktiv und können nicht auf anderen ESX-Servern neu gestartet werden – die VMDK-Dateien auf dem VMFS-Volume sind gelockt, und ein versuchter Neustart dieser VMs würde auf einem anderen ESX-Server mit einer Fehlermeldung quittiert.

Aber halt! So war dies mit vSphere 4.x – dank dem Datastore-Heartbeat erkennt der Master zusätzlich, ob die VMs noch im Zugriff sind, und verzichtet automatisch auf einen Neustart.

Diese Verbesserung trägt deutlich zur Entspannung bei »halb ausgefallenen« Infrastrukturen bei. Sind die VMs nicht mehr im Zugriff und ist der Host isoliert, dann wird ein Neustart ausgeführt – also das gleiche Verhalten wie bei einem ausgefallen Host.

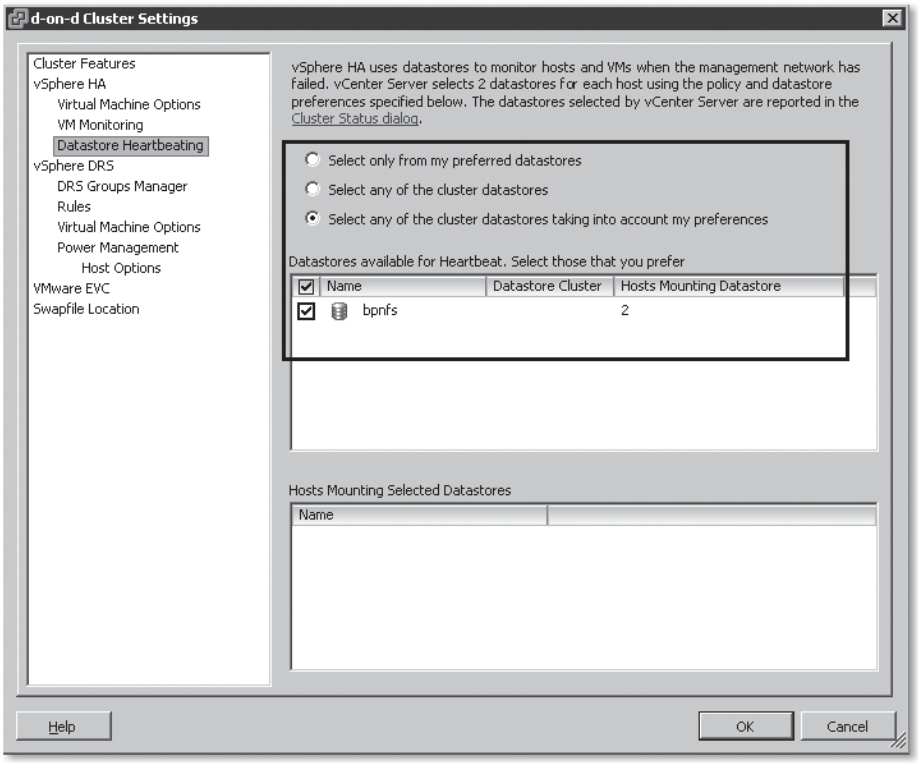


Abbildung 5.31 Datastore-Heartbeat

Isolationsvorgang

Slave isoliert:

1. 0 Sekunden – Slave-Host wird isoliert.
2. 10 Sekunden – Slave wechselt in »election state«.
3. 25 Sekunden – Slave ernennt sich selbst zum Master.
4. 25 Sekunden – Slave pingt die Isolation-Adressen an.
5. 30 Sekunden – Slave erkennt sich selbst als isoliert und startet den Isolationsprozess.

Master isoliert:

1. 0 Sekunden – Master Host wird isoliert.
2. 0 Sekunden – Master pingt die Isolation-Adressen an.
3. 5 Sekunden – Master erkennt sich selbst als isoliert und startet den Isolationsprozess.

Split-Brain oder Partitioned

Es existiert jedoch noch eine weitere Form der Host Isolation, namens partitioned. Partitioned bedeutet, dass kein Ping mehr vom ESX-Host beantwortet wird, dieser allerdings noch am Elektionsprozess der Hosts untereinander teilnimmt. Dieser Zustand kann eintreten, wenn beispielsweise bei einem verteilten Cluster die Netzwerkverbindung zwischen den Rechenzentren gekappt wird, was einer Split-Brain Situation entsprechen würde. In diesem Fall können die Hosts innerhalb des jeweiligen Rechenzentrums noch miteinander kommunizieren, aber die Verbindung zum Master ist nur noch aus dem Rechenzentrum möglich, in dem der ursprüngliche Master aktiv ist. Dies war in vSphere 4.x-Umgebungen ein sehr großes Problem, und aufgrund der Limitierung auf 5 Primary-Knoten war es in der Planung nur sinnvoll, maximal 4 ESX-Hosts pro Rechenzentrum aufzustellen.

Mit vSphere 5 wird dies nun sehr clever gelöst: Stellen Sie sich zwei Rechenzentren mit jeweils 8 ESX-Hosts in einem übergreifenden Cluster von insgesamt 16 Hosts vor. Nun fällt die Verbindung zwischen den beiden Rechenzentren aus. In RZ1 existiert noch der HA-Master, und die sich im RZ1 befindlichen 7 ESX-Server (Slaves) können das Netzwerk und den HA-Master erreichen. In RZ2 existiert kein HA-Master mehr, und 8 Slaves können keinen Master erreichen. Allerdings erkennen die 8 ESX-Hosts sich untereinander. In diesem Fall wird ein Elektionsverfahren gestartet, und einer der 8 Hosts wird zum Master. In jedem der beiden RZ existiert nun ein Master, und HA läuft nach wie vor korrekt. Sobald die Netzwerkverbindungen wiederhergestellt werden, wird erneut ein Elektionsprozess angestoßen, um einen der beiden HA-Master zum Slave zu stufen.

5.2.15 HA und getrennte (disconnected) ESX-Server

Ist ein ESX-Server eines HA-Clusters im vCenter als `disconnected` markiert, schließt die HA-Logik diesen Server aus ihren Failover-Berechnungen und Failover-Aktivitäten aus. War dieser Server ein Master-Knoten, so übernimmt einer der übrigen Slave ESX-Hosts als neuer Master den HA Cluster. Ein ESX-Server wird durch das explizite Trennen seitens des Administrators vom Cluster getrennt.

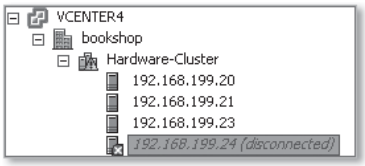


Abbildung 5.32 Werden Hosts getrennt, schaltet der HA-Agent ab.

5.2.16 HA und DNS

DNS ist keine Voraussetzung mehr für einen funktionierenden HA-Cluster, da alle Komponenten über IP kommunizieren. Für vSphere 4.1 gilt nach wie vor eine ausfallsichere und stabile DNS-Konfiguration als Notwendigkeit, um HA korrekt zu betreiben.

5.2.17 HA im vSphere-Client (oder: Der Cluster treibt's bunt …)

Der HA-Cluster zeigt sich im vCenter genauso wie ein DRS-Cluster, da beide VMware-Funktionen gleichzeitig in einem Cluster aktiviert werden können. Das Symbol kann bei der Kombination von HA und DRS insgesamt drei verschiedene Status anzeigen und zwei verschiedene Status, wenn HA allein betrieben wird: Ein normales Symbol informiert darüber, dass der HA-Cluster ohne Einschränkungen lauffähig ist; ein gelbes Symbol bei einem mit DRS kombinierten Cluster signalisiert, dass DRS überbucht (*overcommitted*) ist (das heißt, es stehen nicht genügend Ressourcen zur Verfügung); ein rotes Symbol signalisiert einen ungültigen HA- oder DRS-Cluster (zum Beispiel im HA-Bereich durch nicht ausreichende Ressourcen zum Erreichen der Failover-Kapazität).

Yellow Cluster – overcommitted

- Ein DRS-Cluster ist *overcommitted*, wenn ein ESX-Host ausfällt und somit nicht ausreichend Ressourcen mehr zur Verfügung stehen.
- Ein DRS-Cluster hat für einen Child-Resource-Pool oder dessen VMs nicht ausreichend Ressourcen, um dessen Anforderungen zu erfüllen.

Red Cluster – invalid

- Ein HA-Cluster hat keine ausreichende Kapazitäten (aktuelle Failover-Kapazität), um die konfigurierte Failover-Capacity abzudecken.

5.2.18 HA-Limitierungen mit vSphere

Mit vSphere 5 sind folgende Limitierungen in Bezug auf vSphere HA bekannt:

Beschreibung	Limitierung
ESX-Hosts pro HA-Cluster	32
aktive VMs per Cluster	3.000
aktive VMs pro ESX	512
maximale Failover-Hosts pro HA-Cluster	31
maximale Failover-Ressourcen (%) pro HA-Cluster	100

Tabelle 5.4 HA-Cluster-Limitierung

5.2.19 HA Virtual Machine Monitoring

Virtual Machine Monitoring, oft nur VMHA genannt, ist eine seit VI3.5 U3 bekannte Funktion zur Überwachung von virtuellen Maschinen auf Aktivität. Diese Aktivität wird in Form des Heartbeats gemessen, der über die VMware Tools erzeugt wird. Sobald kein Heartbeat über einen gewissen Zeitraum empfangen wird, führt vCenter einen harten Reset durch. Dieses Vorgehen soll z. B. Kernel-Panics unter Linux und Bluescreens unter Windows erkennen.

Allerdings wurde diese Funktion erweitert, so dass mittels VMware Tools auf Ausfälle von Anwendungen in den virtuellen Maschinen reagiert werden kann.

Bei der Aktivierung von VM Monitoring kann daher unterschieden werden zwischen reiner VM- oder VM-und-Anwendungs-Überwachung (Abbildung 5.33).

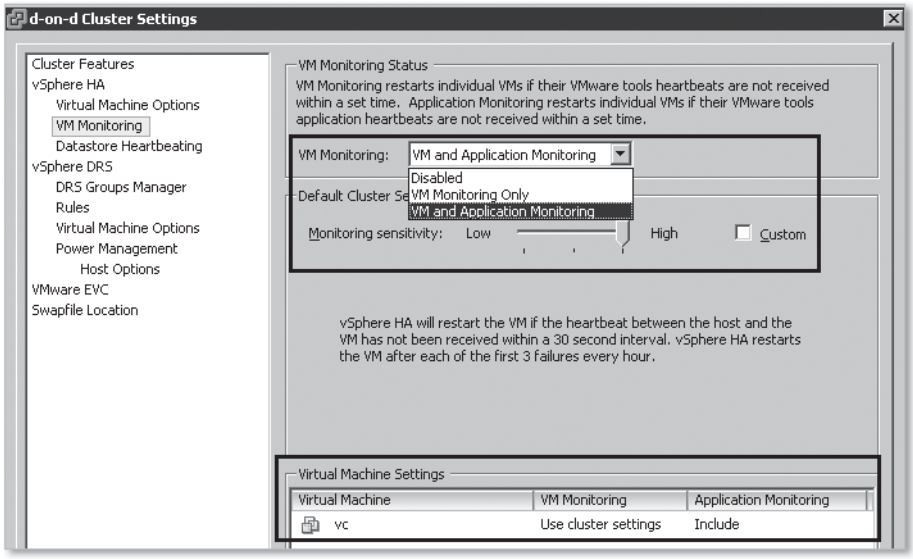


Abbildung 5.33 VM-Monitoring-Funktion von vSphere HA

In der ersten Version gab es noch einen sehr derben Fehler, der VMHA nach einem vMotion-Vorgang auslöste, da der Heartbeat in diesem Fall für mehr als 30 Sekunden ausfiel. Das Ergebnis war ein harter Reset der virtuellen Maschine nach jedem erfolgreichen vMotion.

Aus diesem Grund war die einfachste Lösung, die 30 Sekunden zu erhöhen, und zwar mittels der Monitoring sensitivity, die Sie unter der Sektion Default Cluster Settings finden.

Die Defaultwerte der Standardeinstellungen Low, Medium und High listet Tabelle 5.5 auf.

Level	Failure Interval	Minimum Uptime	Maximum per-VM Resets	Maximum Resets Time Window
Low	120 Sekunden	480 Sekunden	3	168 Stunden
Medium	60 Sekunden	240 Sekunden	3	24 Stunden
High	30 Sekunden	120 Sekunden	3	1 Stunde

Tabelle 5.5 Standard-Monitoring-Sensitivity

Vier Werte sind für die Sensitivity interessant:

- Failure Interval: Dieser Wert steht für das Prüfintervall auf Ausfall einer VM, d. h. wie lange kein Heartbeat erkannt wurde.

- Minimum uptime: Bestimmt die Mindestlaufzeit zwischen einem Fehler mit Neustart und einer erneuten Heartbeat-Überwachung.
- Maximum per-VM resets: maximale Anzahl an Neustarts aufgrund von erkannten VMHA-Fehlern. Danach findet kein weiterer Neustart statt, und die VMHA-Erkennung wird für die VM vorübergehend abgeschaltet.
- Maximum resets time window: Zeitfenster, in dem die maximale Anzahl der VM-Resets gezählt wird. Ist das Zeitfenster seit dem ersten Ausfall überschritten, startet das Reset-Time-Window von vorn.

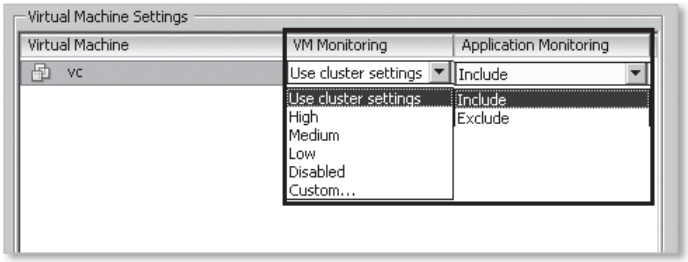


Abbildung 5.34 Pro-VM-Einstellungen für das VM Monitoring

Diese Einstellungen können nicht nur allgemein, sondern auch pro virtueller Maschine getroffen werden. Hier ist es möglich, beim Standard (Use Cluster Settings) zu bleiben oder ebenfalls zwischen High, Medium und Low zu wählen. Das Application Monitoring kann zu- oder abgeschaltet (Include/Exclude) werden. Reicht dies nicht aus, ist auch pro virtueller Maschine eine Custom-Einstellung möglich.

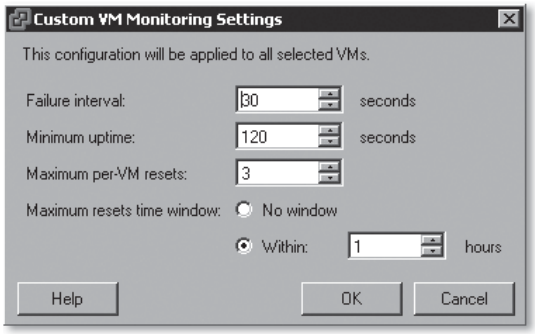


Abbildung 5.35 »Custom«-Einstellungen VM Monitoring pro virtueller Maschine

vSphere HA geschützt

vSphere 5 bietet übrigens eine einfache Möglichkeit, den aktuellen HA-Schutz einer virtuellen Maschine einzusehen, indem Sie im Summary der VM auf die vSphere HA Protection achten (siehe Abbildungen 5.36 und 5.37).

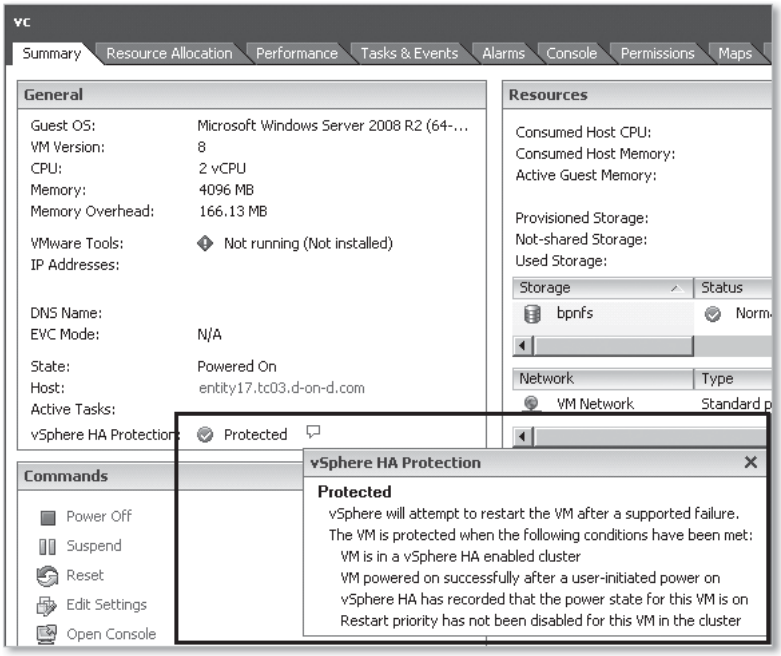


Abbildung 5.36 VM ist durch vSphere HA geschützt.

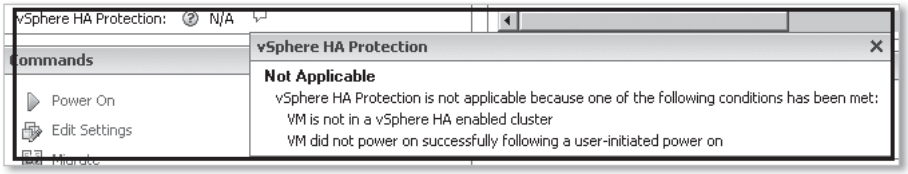


Abbildung 5.37 VM ist ungeschützt.

vSphere HA VM Application Monitoring

Die VM-Application-Monitoring-Funktion wurde bereits unter vSphere 4.1 als versteckte Programmierschnittstelle namens *Guest SDK* implementiert und zur Überwachung von Gastanwendungen über die VMware Tools genutzt. Mit vSphere 5 wurde das Guest SDK öffentlich zugänglich, d. h., jeder Entwicklungspartner kann diese Funktionalität nutzen, beispielsweise Symantec.

Virtual Machine Monitoring: Advanced Options

Neben den Advanced Options für die ESX-HA-Funktion existieren auch Optionen für die Überwachung der virtuellen Maschinen. Allerdings sind diese identisch mit den über die grafische Oberfläche verfügbaren Einstellungen.

Option	Beschreibung
das.failureInterval	Prüfintervall auf Ausfall der VM. Standard ist 30.
das.maxFailureWindows	Mindestlaufzeit zwischen den Fehlern und der Neustarts. Standard sind 3600 Sekunden. Fällt die Maschine innerhalb von 3.600 Sekunden zweimal aus, wird sie nur beim ersten Mal neu gestartet.
das.maxFailures	Maximalanzahl an Fehlern (Neustarts). Sobald der angegebene Wert erreicht ist, wird die VM nicht mehr automatisch neu gestartet. Standardwert ist 3.
das.minUptime	Angabe der Mindestlaufzeit der virtuellen Maschine, bevor VMHA wieder die Prüfung beginnt. Standard sind 120 Sekunden. Hiermit wird verhindert, das VMs stetig neu gestartet werden, ohne jemals aktiv zu werden.

Tabelle 5.6 vSphere HA Virtual Machine Monitoring Advanced Settings

5.3 DRS-Cluster

In den meisten Fällen unterstützen Cluster-Produkte sowohl Ausfallsicherheit als auch Lastverteilung. Dies ist bei VMware vSphere nicht anders, daher ist eine Lastverteilungsfunktion bei den Cluster-Objekten mit an Bord.

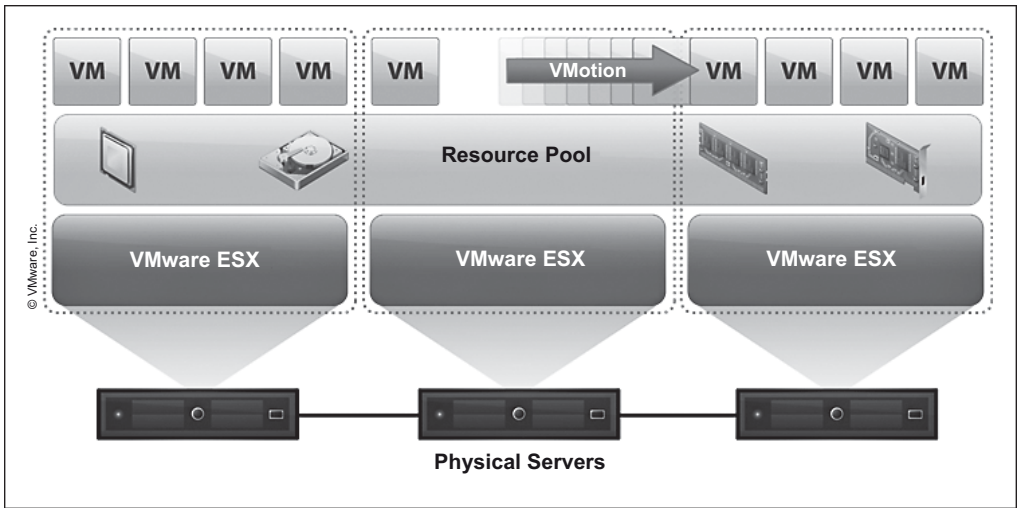


Abbildung 5.38 Funktionsübersicht DRS (Distributed Resource Scheduling)

5.3.1 Technologie-Übersicht

Um in einer VMware-Umgebung eine Lastverteilung zwischen den verschiedenen ESX-Hosts zu erreichen, fasst man bestimmte ESX-Hosts zu einem DRS-Cluster zusammen. DRS ist die Abkürzung für »Distributed Resource Scheduling« und kann kurzerhand als ein Load-Balancing-Tool für virtuelle Maschinen gesehen werden. Zwischen diesen ESX-Hosts innerhalb des Clusters werden die virtuellen Maschinen verschoben, um unter Betrachtung der CPU- und

Speicherauslastung der ESX-Hosts eine ausgeglichene Verteilung der Last zu erhalten. Dabei wird die Netzwerk- und Festplattenauslastung der ESX-Hosts nicht beachtet. Das Verschieben der VMs erfolgt mit Hilfe von vMotion, daher ist die Ablage der VM-Dateien auf einem zentralen Speichermedium die Grundvoraussetzung für DRS. Darum ist zu beachten, dass die verschiedenen ESX-Hosts eines DRS-Clusters auch CPU-kompatibel für vMotion-Aktivitäten sein müssen.

Das Ziel von DRS kann man also in einen Satz fassen: Durch das Verschieben von virtuellen Maschinen von stark ausgelasteten Servern hin zu weniger ausgelasteten Servern wird versucht, eine ausgewogene Verteilung von virtuellen Maschinen auf der vSphere-Umgebung zu erreichen.

DRS kann in verschiedenen Automatisierungsstufen betrieben werden. Diese reichen von reinen Empfehlungen, welche virtuelle Maschinen zu verschieben seien, bis hin zum voll automatisierten DRS-Betrieb, in dem jegliche Empfehlung sofort umgesetzt wird. Des Weiteren können Regeln aufgestellt werden, wie virtuelle Maschinen im gesamten DRS-Regelwerk zu behandeln sind. Diese Regeln bestimmen, dass z. B. virtuelle Maschinen immer gemeinsam auf einem ESX-Host betrieben werden sollen, oder das Gegenstück dazu, dass virtuelle Maschinen niemals gemeinsam auf einem einzigen ESX-Host platziert werden dürfen. Natürlich können bestimmte virtuelle Maschinen aus dem DRS-Cluster ausgeschlossen werden; diese werden bei allen DRS-Aktivitäten nicht berücksichtigt, wohl aber bei der Berechnung der Ressourcenauslastung.

Die Architektur von DRS basiert auf dem vCenter und benötigt auf den ESX-Hosts im Gegensatz zu vSphere HA keine lokalen Agents. Das vCenter ist für DRS der Dreh- und Angelpunkt, um die DRS-Konfiguration vorzunehmen und die DRS-Empfehlungen auszuführen. Ein DRS-Cluster kann maximal 32 Knoten umfassen. Das vCenter überprüft in Abständen von fünf Minuten (Standardeinstellung) die CPU- und Speicherauslastung der im DRS-Cluster befindlichen ESX-Hosts. Allerdings können Sie in den Eigenschaften des DRS-Clusters jederzeit auch einen manuellen Scan auslösen.

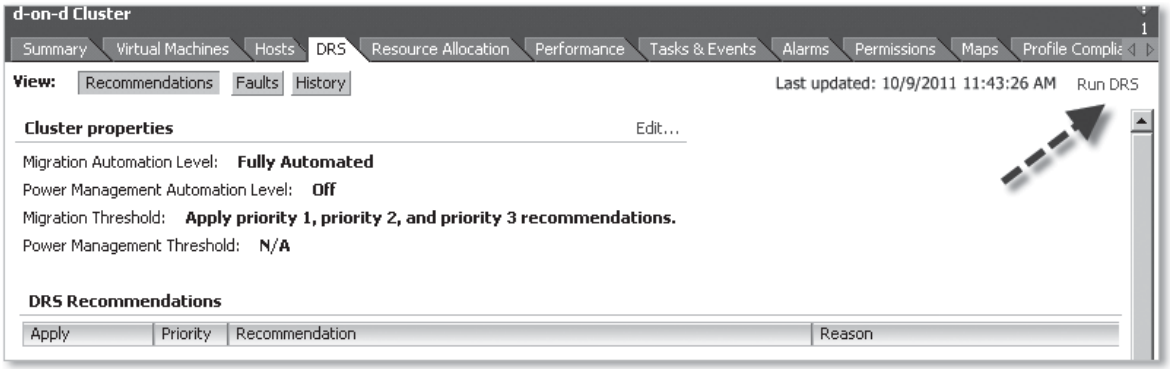


Abbildung 5.39 Manueller Start der DRS-Überprüfung

Bei der Berechnung der Ressourcenauslastung bezieht das vCenter alle virtuellen Maschinen der ESX-Hosts im DRS-Cluster ein, auch die aus der DRS-Funktion ausgegliederten virtuellen Maschinen. Dieser Berechnungsprozess wird auch durch das Hinzufügen oder das Entfernen eines ESX-Hosts aus dem DRS-Cluster gestartet, um schnellstmöglich eine optimale Auslastung von CPU und Speicher der ESX-Hosts zu erlangen.

5.3.2 Lizenzierung von DRS

VMware DRS ist Bestandteil der vSphere Enterprise Edition, die auf CPU-Sockel-Basis und vRAM lizenziert.

5.3.3 Anlage eines DRS-Clusters

Prinzipiell wird der DRS-Cluster genau gleich dem HA-Cluster angelegt, da DRS auch nur eine Funktion des Cluster-Objekts ist. Daher können Sie DRS direkt bei der Anlage eines Clusters aktivieren oder auch nachträglich.

Deaktivierung

Ebenso ist es jederzeit möglich, die DRS-Funktion zu deaktivieren, was allerdings direkte Auswirkungen auf die Systeme hat, da alle Resource-Pools entfernt werden!

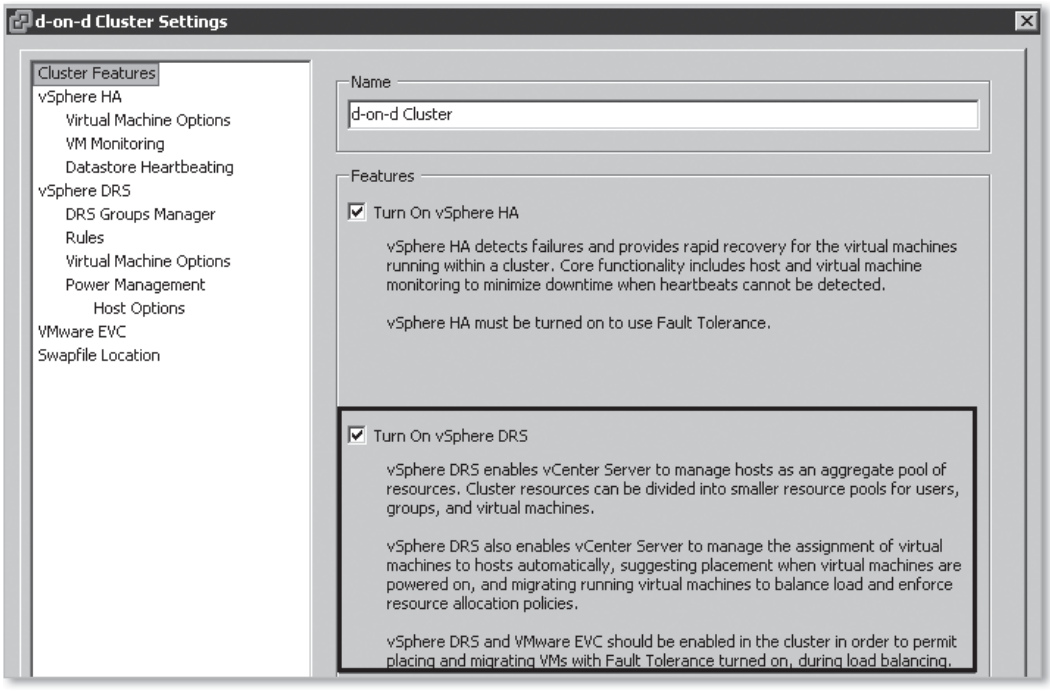


Abbildung 5.40 Aktivierung der DRS-Funktion im Cluster

Sobald ein DRS-Cluster existiert, können Sie ESX-Hosts inklusive Resource-Pools per Drag & Drop integrieren. Sie müssen lediglich entscheiden, wie die Resource-Pools übernommen werden sollen. Möglich ist eine Übernahme der Resource-Pools mit gleichem Namen in den Root-Resource-Pool des Clusters (der Cluster selbst ist der Root-Resource-Pool), oder Sie legen neue Resource-Pools an für alle VMs dieses Hosts mit dem zu wählenden Namen-Präfix (Vorgabe GRAFTED FROM ESX HOST).

Ist DRS nicht aktiviert, wird automatisch eine Warnmeldung ausgegeben, da alle Resource-Pools verlorengehen.

Abbildung 5.41 Ist im Cluster DRS nicht aktiviert, wird vor der Integration eines Hosts mit bestehenden Resource-Pools gewarnt.

5.3.4 Prioritäten-Ranking

Die DRS-Prioritäten werden in Werten von 1 bis 5 Sternen angegeben, die Auswirkungen auf eine Migration einer virtuellen Maschine von einem Host auf einen anderen haben sowie auf den Ziel-Host beim Neustart einer VM. Eine Empfehlung mit Priorität 5 hat die größte Auswirkung auf die Performanceauslastung eines ESX-Hosts und im Gegensatz dazu eine Empfehlung mit einem Stern die geringste. Die Empfehlungen mit Priorität 5 umfasst außerdem die Migrationen, die von den DRS-Affinity-Rules herrühren oder vom Einschalten des Maintenance-Modus auf einem ESX-Host, was eine automatische Evakuierung der Gastsysteme durch DRS auslöst. Des Weiteren versprechen Operationen mit Priorität 5 eine Auflösung von sehr großen Auslastungs-Ungleichgewichten. Die Empfehlungen mit weniger Priorität haben absteigend auch immer einen kleiner werdenden Einfluss auf den Ausgleich von Ungleichgewichten im DRS-Cluster.

5.3.5 DRS-Automation-Level

Der Automatisierungsgrad eines DRS-Clusters ist eine für alle ESX-Hosts des DRS-Clusters übergreifende Einstellung und umfasst die drei Stufen MANUAL, PARTIALLY AUTOMATED und FULLY AUTOMATED.

Das Automation-Level MANUAL gibt lediglich Empfehlungen über den vCenter-Client an den VMware-Administrator, welche virtuelle Maschine auf welchem ESX-Host zu starten ist, um eine ausgewogene Lastverteilung zu erreichen. Die aktuellen Empfehlungen werden im vCenter-Client nach Auswahl des DRS-Clusters aufgelistet.

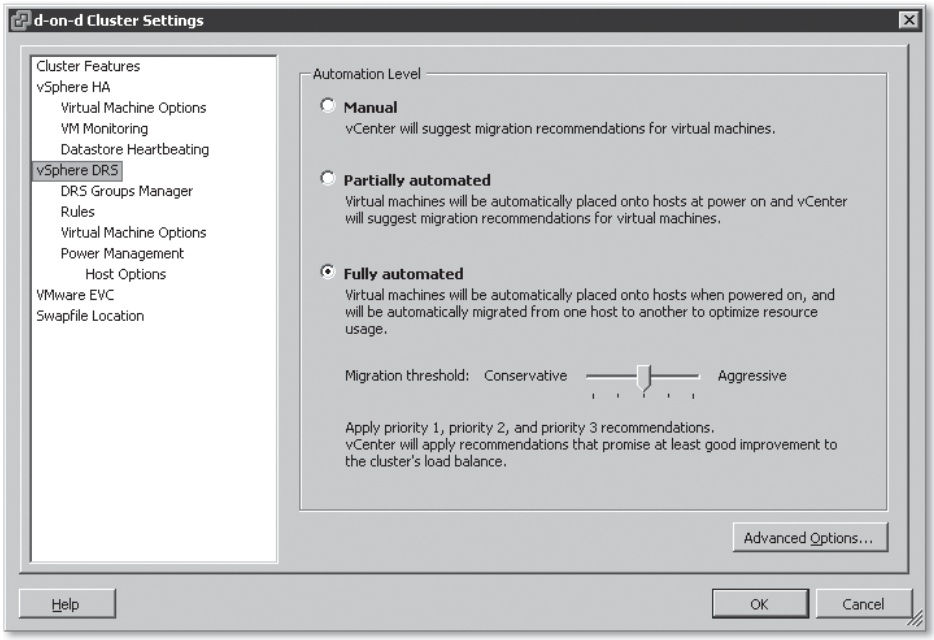


Abbildung 5.42 Eigenschaften des DRS-Clusters

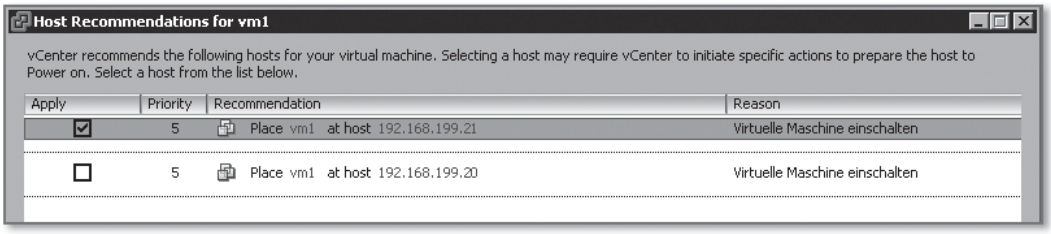


Abbildung 5.43 Prioritätenanzeige beim Start einer VM beim Automation-Level »Manual«

Dieses *Priority-Ranking* wird vom Automation-Level in der DRS-Automatisierungsstufe FULLY AUTOMATED immer verwendet, bei PARTIALLY AUTOMATED nur beim Einschalten einer VM. Die Empfehlungen enthalten unter anderem den Namen der virtuellen Maschine und das jeweilige Priority-Ranking. Diese können dann zu einem beliebigen Zeitpunkt durch Klick des Administrators durchgeführt werden. Hierbei ist eine Auswahl zu treffen, damit die virtuelle Maschine in Betrieb genommen werden kann. Natürlich werden auch hier nur jene ESX-Hosts als Ziel betrachtet, die alle Bedingungen zum Start der VM erfüllen.

Das Automation-Level FULLY AUTOMATED ist das Gegenteil der manuellen Methode. Sämtliche Empfehlungen werden vom vCenter automatisch durchgeführt, beim Starten von virtuellen Maschinen (Initial Placement) und im laufenden Betrieb (Virtual Machine Migration). In dieser Stufe kann die Migration von virtuellen Maschinen nochmals in fünf Level unterteilt werden:

- Dabei ist Level 1 das konservativste und Level 5 das aggressivste. Level 1, Conservative, bedeutet, dass nur Empfehlungen mit Priorität 5 automatisiert durchgeführt werden. Alle anderen Empfehlungen, also mit Priorität 1–4, werden Ihnen als Empfehlung angeboten.
- Level 2 führt alle Empfehlungen mit Priorität vier und fünf durch.
- Level 3 führt alle Empfehlungen mit Priorität drei oder mehr durch.
- Level 4 führt alle Empfehlungen mit Priorität zwei oder mehr durch.
- Die am höchsten automatisierte Form des DRS erreichen Sie mit Level 5, Aggressive. Hierbei werden grundsätzlich alle Empfehlungen, egal welche Priorität, vom System automatisch durchgeführt.

Im Summary-Tab des DRS-Clusters können Sie alle Empfehlungen und eine Kurzübersicht schnell einsehen.

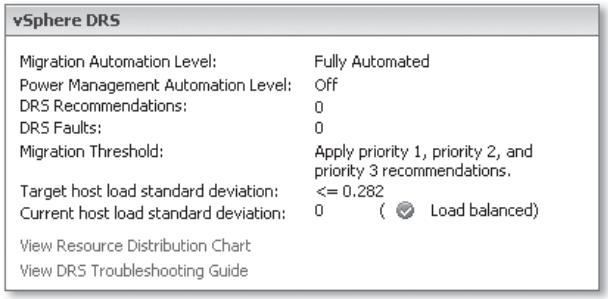


Abbildung 5.44 VMware-DRS-Kurzübersicht im »Summary«-Tab des DRS-Clusters

Das Automation-Level Partially automated ist eine Mischung aus den beiden Stufen Manual und Fully automated. Beim Starten von virtuellen Maschinen erfolgt deren Initial Placement komplett automatisiert. Je nach Ressourcenauslastung der ESX-Hosts wird die zu startende virtuelle Maschine auf einen freien ESX-Host verschoben und dann gestartet. Dies ist die einzige voll automatisierte Aktion in dieser Stufe. Die regelmäßige Überprüfung der ESX-Auslastung resultiert dann, wie unter der Stufe Manual, lediglich in Empfehlungen zur Migration von VMs. Diese können Sie dann bei Bedarf durchführen. Möchten Sie sich die derzeitige Auslastung genauer anschauen, so bieten sich die Resource-Distribution-Charts im Summary des DRS-Clusters an, die die Auslastung der einzelnen Hosts und eventuelle Ungleichgewichte anzeigen.

Vorsicht

Sie sollten immer Vorsicht walten lassen und Fully automated nicht zu aggressiv einstellen, da es sonst zu enorm vielen vMotion-Aktivitäten kommen kann, die den Cluster massiv negativ beeinflussen.

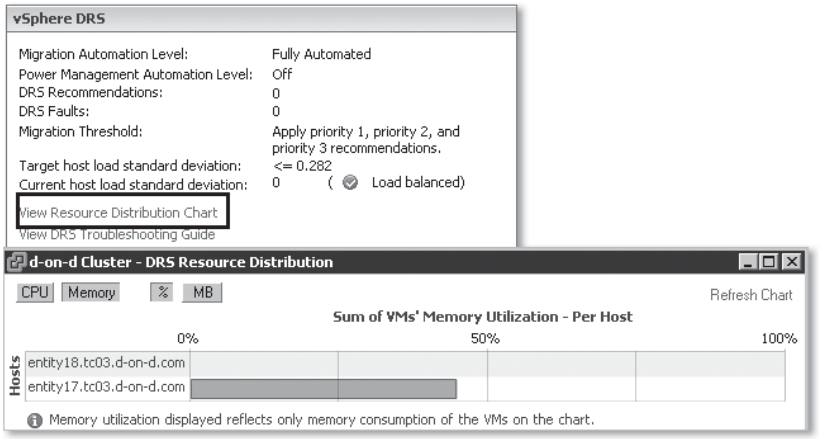


Abbildung 5.45 DRS-Distribution-Chart

5.3.6 DRS Groups Manager

Da vSphere-Umgebungen immer komplexer werden und man nicht immer mit einem Rechenzentrum, sondern mit übergreifenden Clustern (*Stretched Cluster*) ausfallsichere Szenarien realisiert, will man diese in DRS ebenso abbilden.

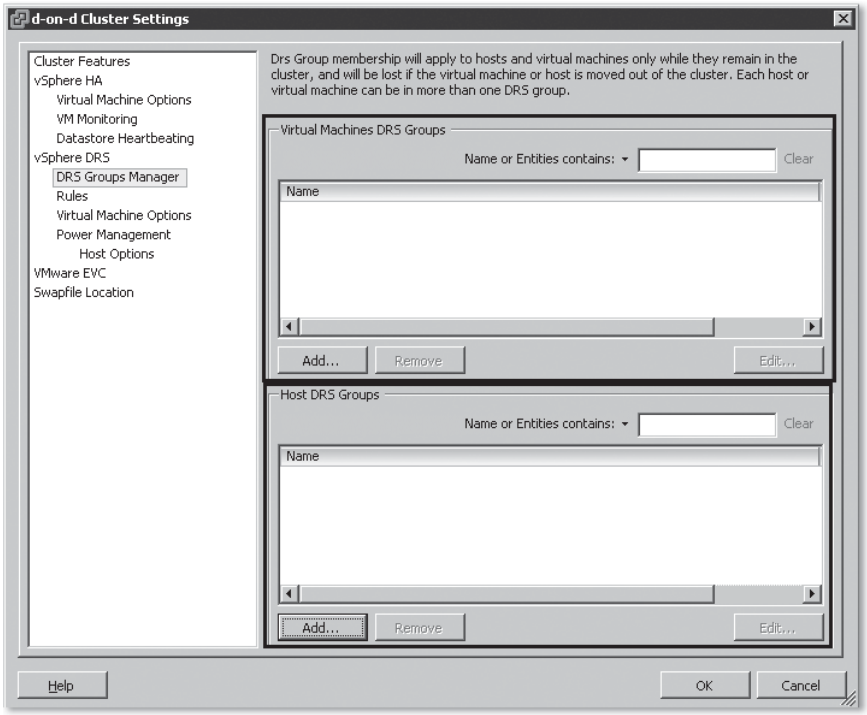


Abbildung 5.46 Einrichtung der DRS-Gruppen

An einem kleinen Beispiel will ich ein solches Szenario erklären:

1. Entity17 ist ein ESX-Server in RZ1.
2. Entity18 ist ein ESX-Server in RZ2.
3. Test1 liegt auf einem Datastore in RZ1, der von Entity17 in optimalem Zugriff ist; Entity18 hingegen sollte nur in Notfällen auf diesen Datastore zugreifen.
4. Test2 liegt auf einem Datastore in RZ2, der von Entity18 in optimalem Zugriff ist; Entity17 hingegen sollte nur in Notfällen auf diesen Datastore zugreifen.

Die DRS-Gruppen sollen daher die beiden Standorte mit ESX und VMs abbilden. Dies geschieht mittels DRS Groups Manager. Erstellen Sie eine VM-Gruppe, in der jeweils nur eine VM enthalten ist. Dieses Szenario können Sie natürlich um eine beliebige Anzahl Hosts und VMs erweitern.

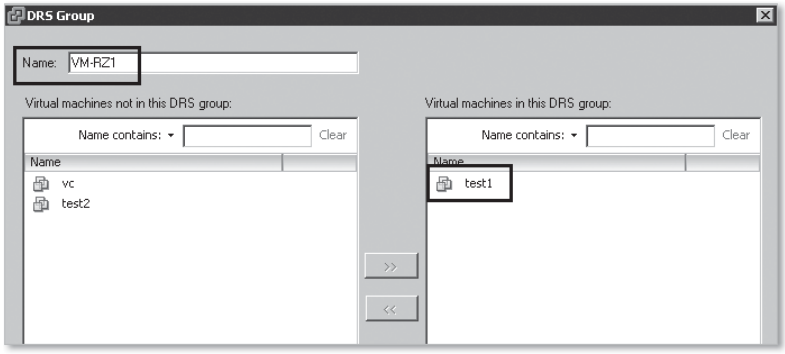


Abbildung 5.47 Anlage DRS-VM-Gruppe erstes RZ

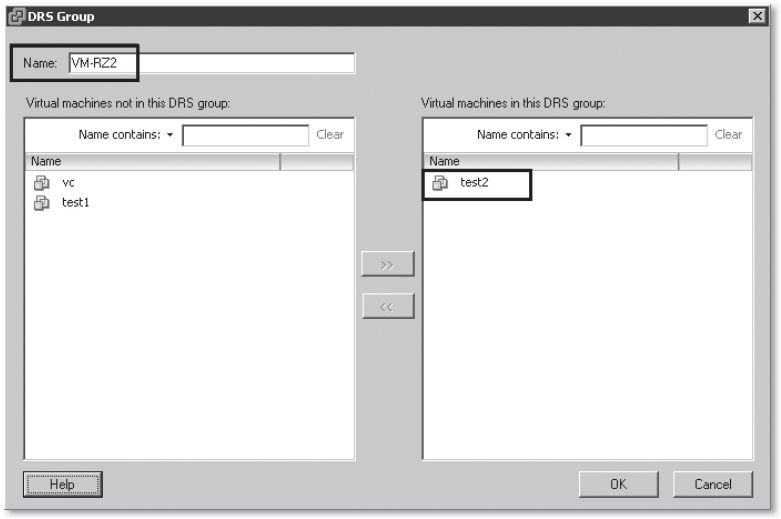


Abbildung 5.48 Anlage DRS-VM-Gruppe zweites RZ

Dazu werden zwei DRS-VM-Gruppen angelegt, die jeweils den Namen des Rechenzentrums tragen und die jeweiligen virtuellen Maschinen enthalten (Abbildung 5.47 und Abbildung 5.48). Nach Abschluss der Konfiguration erhalten Sie die Übersicht über alle DRS-VM-Gruppen (Abbildung 5.49).

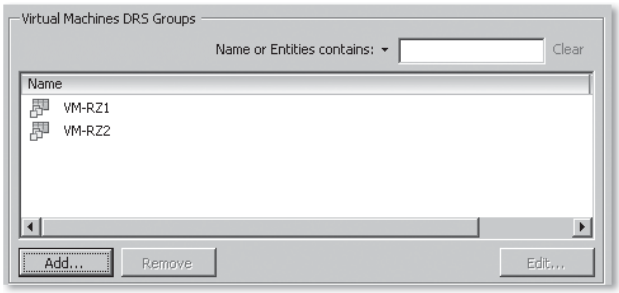


Abbildung 5.49 DRS-VM-Gruppen beider Rechenzentren

Danach erstellen Sie die DRS-Host-Gruppen nach dem gleichen Verfahren (siehe Abbildungen 5.50 und 5.51).

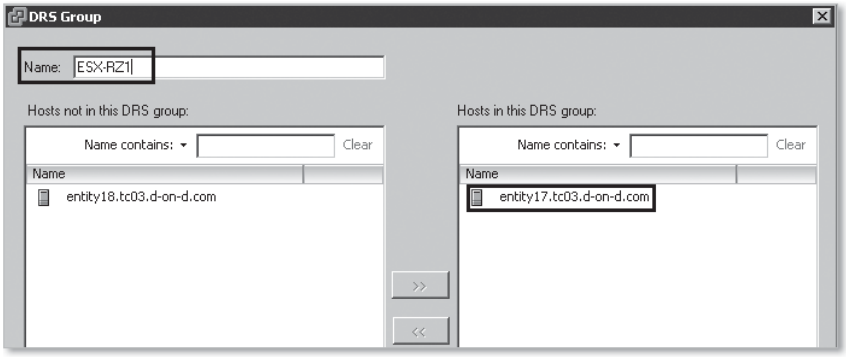


Abbildung 5.50 Anlage DRS-Host-Gruppe erstes RZ

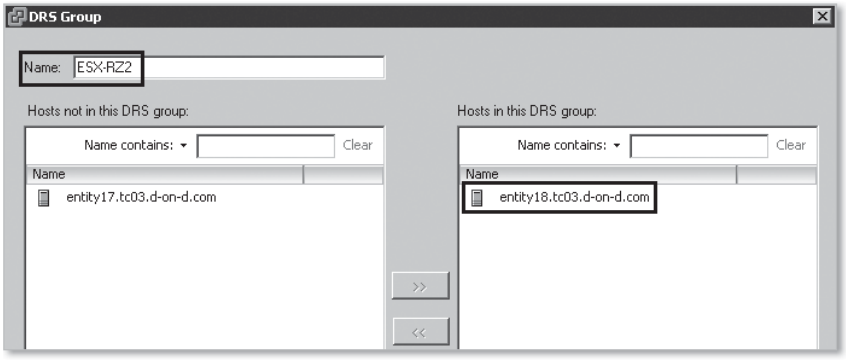


Abbildung 5.51 Anlage DRS-Host-Gruppe zweites RZ

Nach Abschluss der Konfiguration haben Sie alle notwendigen Gruppen (Abbildung 5.52) angelegt und können diese mittels DRS-Affinity-Rules steuern. Das Beispiel führen wir im nächsten Abschnitt weiter.

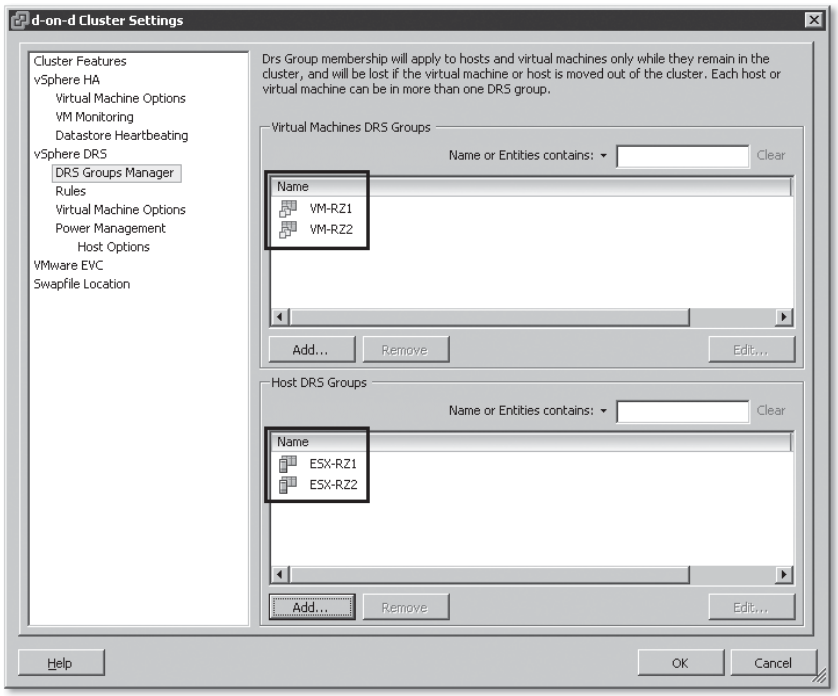


Abbildung 5.52 DRS-Host- und -VM-Gruppen beider Rechenzentren

5.3.7 DRS-Affinity-Rules

Die DRS-Affinity-Rules legen fest, ob und welche virtuelle Maschinen bei DRS-Migrationen immer gemeinsam oder niemals gemeinsam verschoben werden dürfen. Folgende zwei Regeln stehen zur Verfügung: Keep Virtual Machines Together und Separate Virtual Machines.

Die Regel Keep Virtual Machines Together stellt sicher, dass bei von DRS empfohlenen oder auch durchgeführten Migrationsvorgängen immer die in dieser Regel definierten virtuellen Maschinen zusammen verschoben werden, das heißt, diese VMs befinden sich immer zusammen auf einem ESX-Host. Um dies sicherzustellen, werden diese Regeln auch in die Berechnungen eingeschlossen, so dass die Empfehlung immer den Gesamtzustand berücksichtigt, die aktuelle Auslastung der ESX-Hosts sowie die Möglichkeiten, wenn alle VMs dieser Regel verschoben würden. Ein typischer Fall hierfür wären voneinander abhängige Systeme wie beispielsweise Datenbanksystem und dazugehöriges Applikationssystem. Können beide nicht unabhängig voneinander betrieben werden, ist es sinnvoll, sie immer auf dem gleichen ESX-Host zu betreiben.

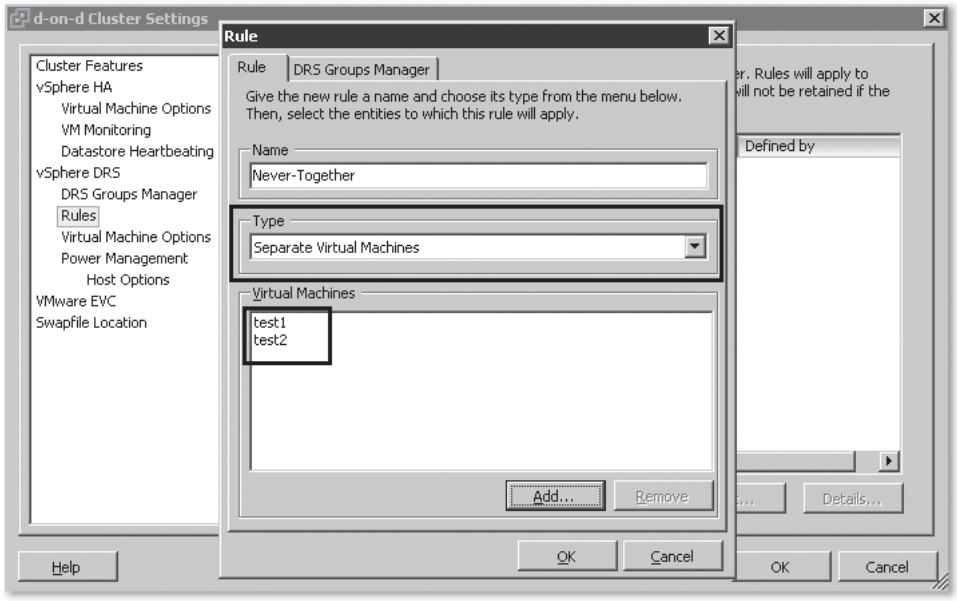


Abbildung 5.53 Affinity-Rules = Regelwerk für DRS

Das Gegenteil dazu stellt die Regel SEPARATE VIRTUAL MACHINES dar. Sie stellt sicher, dass die in dieser Regel definierten virtuellen Maschinen niemals auf einem ESX-Host gemeinsam laufen dürfen. Dies ist zum Beispiel für Cluster-Lösungen innerhalb der virtuellen Welt sinnvoll; ein Ausfall eines ESX-Hosts mit beiden Knoten eines Microsoft-Clusters oder eines NLB-Verbundes umginge die auf der virtuellen Ebene getroffenen Vorsichtsmaßnahmen wieder, und das komplette Cluster-System stünde still. Auch diese Regeln werden bei den Berechnungen der Performanceauslastung immer berücksichtigt.

Nach der Erstellung von neuen Regeln werden diese sofort gegen die aktuelle Verteilung der VMs überprüft, und bei den Modi MANUAL und PARTIALLY AUTOMATED werden neue Migrationen empfohlen. Diese müssen nicht zwingend durchgeführt werden, aber sie bleiben als Empfehlung bestehen, bis keine Regel mehr verletzt wird.

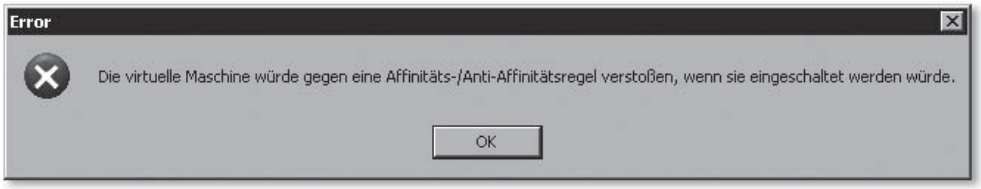


Abbildung 5.54 Verstoß gegen eine DRS-Affinitätsregel

Wird eine Regel z. B. beim Start einer virtuellen Maschine verletzt, so erscheint eine Fehlermeldung, und der Startvorgang wird gestoppt.

Kombination mit den DRS-Gruppen

In Abschnitt 5.3.6, »DRS Groups Manager«, bin ich bereits auf die Erstellung der DRS-Gruppen eingegangen. Allerdings haben diese Gruppen keinerlei Relevanz, wenn sie nicht mit Affinity-Rules kombiniert werden.

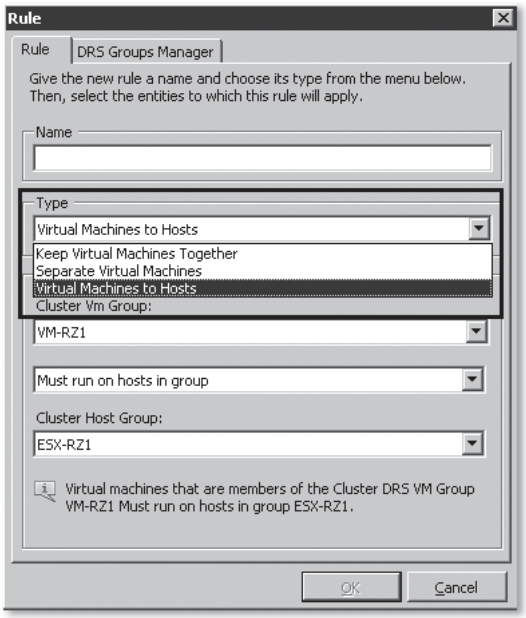


Abbildung 5.55 DRS-Group-Regeln

Dies wird automatisch möglich, sobald Sie bei den DRS-Regeln Virtual Machines to Hosts auswählt (Abbildung 5.55). Danach werden Sie nach den zur Auswahl stehenden VM- und Host-Gruppen gefragt und wie diese zueinander stehen sollen. Zur Auswahl stehen:

- Must run on hosts in group: Die VMs der VM-Gruppe müssen zwingend auf den ESX-Hosts der gewählten Host-Gruppe betrieben werden.
- Should run on hosts in group: Die VMs der VM-Gruppe sollen, falls möglich, auf den ESX-Hosts der gewählten Host-Gruppe betrieben werden.
- Must Not run on hosts in group: Die VMs der VM-Gruppe dürfen nicht auf den ESX-Hosts der gewählten Host-Gruppe betrieben werden.
- Should not run on hosts in group: Die VMs der VM-Gruppe sollen, falls möglich, nicht auf den ESX-Hosts der gewählten Host-Gruppe betrieben werden.

Wenn wir den begonnenen Mini-Workshop mit Affinity-Rules ergänzen, um eine wirkliche Trennung der beiden Rechenzentren zu erreichen, müssen wir folgende Schritte durchführen.

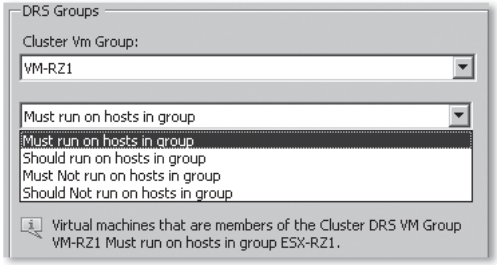


Abbildung 5.56 Wie stehen die VM- und Host-Gruppen zueinander?

Wir erinnern uns:

1. Entity17 ist ein ESX-Server in RZ1.
2. Entity18 ist ein ESX-Server in RZ2.
3. Test1 liegt auf einem Datastore in RZ1, der von Entity17 in optimalem Zugriff ist; Entity18 hingegen sollte nur in Notfällen auf diesen Datastore zugreifen.
4. Test2 liegt auf einem Datastore in RZ2, der von Entity18 in optimalem Zugriff ist; Entity17 hingegen sollte nur in Notfällen auf diesen Datastore zugreifen.

Ganz wesentlich in unserem Beispiel ist, dass es die Möglichkeit gibt, die VMs in RZ1 auch in RZ2 zu betreiben, es ist nur langsamer. Daher ist für unsere Regeln nicht MUST RUN, sondern SHOULD RUN auszuwählen, damit im Fehlerfall oder besser im Problemfall eine Zuordnung nicht-optimaler Ressourcen noch durchgeführt wird.

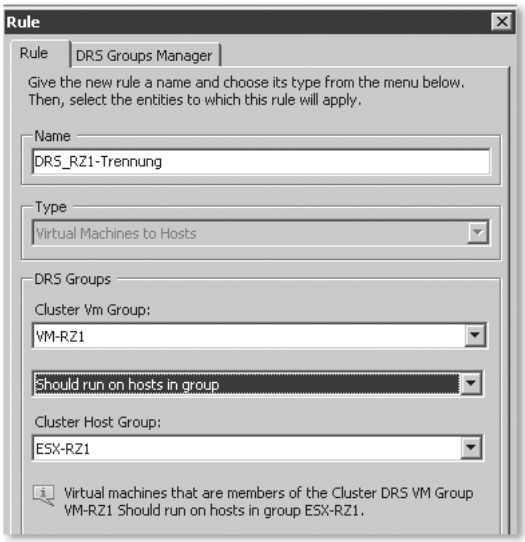


Abbildung 5.57 VMs in RZ1 sollen nur auf ESX-Hosts in RZ1 betrieben werden.

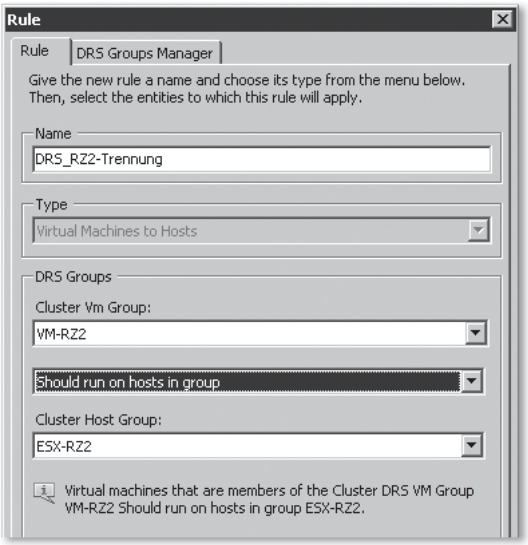


Abbildung 5.58 VMs in RZ2 sollen nur auf ESX-Hosts in RZ2 betrieben werden.

Somit ist die Zuordnung abgeschlossen, und DRS verschiebt die virtuellen Maschinen nach Möglichkeit nur innerhalb der Standorte. Im Problemfall oder bei einem Ressourcenengpass werden jedoch die Regeln aufgeweicht. Diese Regeln können Sie natürlich auch für andere Aspekte verwenden, wie Lizenzprobleme, oder wenn nur bestimmte ESX-Hosts mit sehr vielen Ressourcen ausgestattet sind und ressourcenfressende VMs auch nur dort betrieben werden sollen.

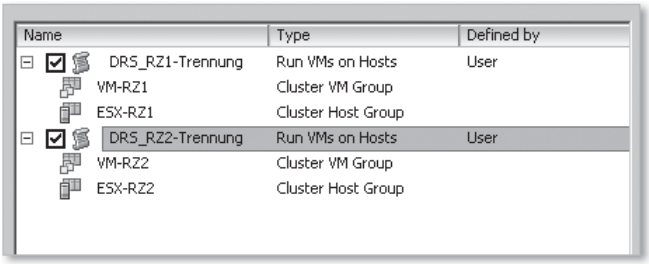


Abbildung 5.59 Komplette Regelwerke für die RZ-Trennung

Natürlich war dieses Beispiel mit nur jeweils einem ESX-Host pro Rechenzentrum ein Minimalbeispiel, allerdings können Sie die Anzahl der ESX-Hosts und der VMs einfach erhöhen, das Prinzip bleibt das gleiche.

5.3.8 DRS Virtual Machine Options

Die DRS-Regeln betreffen standardmäßig immer alle virtuellen Maschinen aller zum DRS-Cluster hinzugefügten ESX-Hosts. Zeitweise ist es aber möglicherweise notwendig, verschie-

dene virtuelle Maschinen innerhalb eines DRS-Clusters gesondert zu behandeln. Zum Beispiel sollten bestimmte VMs niemals via vMotion verschoben und somit von der DRS-Automatisierung ausgeschlossen werden. Andere wiederum sollten trotz Teil- oder Vollautomatisierung der DRS-Migration nur nach Zustimmung des Administrators verschoben werden – also entgegen der Cluster-Konfiguration auf MANUAL konfiguriert werden.

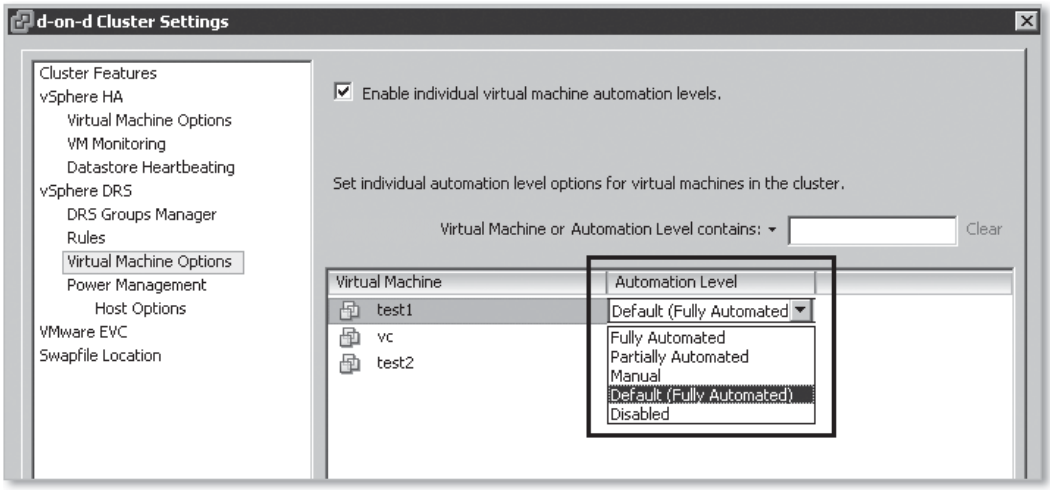


Abbildung 5.60 DRS-Automation kann auch pro VM gesondert definiert werden.

Diese Einstellungen definieren Sie in den DRS-Eigenschaften im Menü unter DRS VIRTUAL MACHINE OPTIONS. Hier existieren die Einstellungen DISABLED, MANUAL, FULLY AUTOMATED, PARTIALLY AUTOMATED und DEFAULT; Letzteres gibt die globale DRS-Cluster-Einstellung wieder und ist auch der Standardwert jeder VM. Durch die Einstellung DISABLED wird zwar die virtuelle Maschine von DRS-Migrationen ausgenommen und es werden dafür auch keine Empfehlungen ausgesprochen, aber die Performanceauslastung durch diese VM wird bei den DRS-Berechnungen dennoch berücksichtigt.

Zum Abschluss sei zu diesen Möglichkeiten erwähnt, dass zu viele Ausnahmeregelungen die Möglichkeiten und auch den Sinn von DRS unterwandern. Diese DRS-Optionen sollten Sie nur in Maßen einsetzen!

5.3.9 DRS und Resource-Pools

Die Ressourcen eines jeden ESX-Hosts im DRS-Cluster werden logisch zu einem Resource-Pool zusammengefasst. Wie auch bei Resource-Pools für alleinstehende ESX-Hosts können Resource-Pools einen DRS-Cluster weiter in logische Ressourcengruppen unterteilen. Dabei sind die Grenzen der Pools nicht mehr an einen ESX-Host gebunden, sondern umfassen die gesamten Ressourcen eines DRS-Clusters.

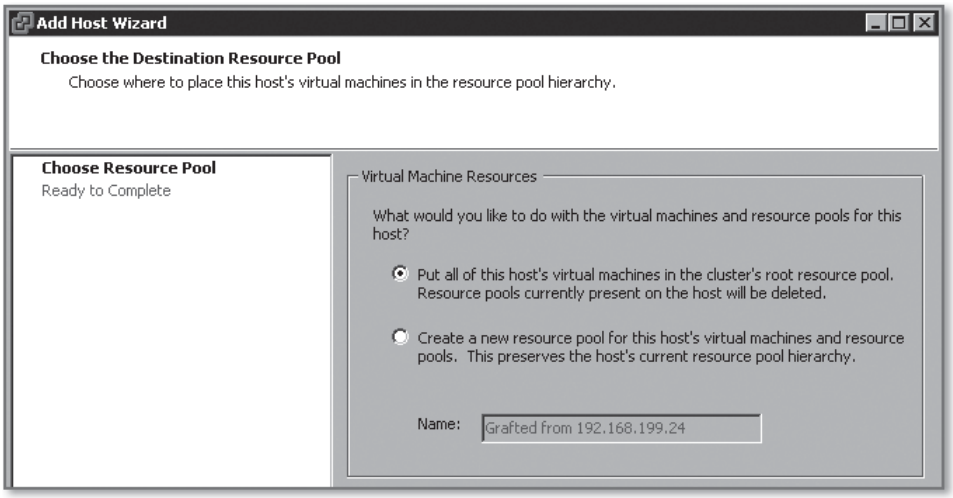


Abbildung 5.61 Wie soll mit bestehenden Resource-Pools bei der Cluster-Integration umgegangen werden?

Beim Hinzufügen eines neuen ESX-Hosts stehen zwei Möglichkeiten zur Verfügung, wie die neu hinzukommenden Ressourcen eines ESX-Hosts logisch verwaltet werden sollen: Die Option Put this host's virtual machines in the cluster's root resource pool fügt den ESX-Host mitsamt seinen virtuellen Maschinen zum Resource-Pool des DRS-Clusters hinzu. Sollten auf dem ESX-Host bereits Resource-Pools existieren, so werden diese ignoriert.

Die Option Create a new resource pool for this host's virtual machines and resource pools fügt den neuen ESX-Host in einem neu erstellten Resource-Pool dem DRS-Cluster hinzu. Der neu erstellte Resource-Pool existiert in der Hierarchie auf der obersten Ebene, und alle VMs des ESX-Hosts werden diesem neuen Pool zugeordnet. Dieser neue Pool erhält standardmäßig den Namen »Grafted from servername«, den Sie aber ändern können.

5.3.10 DRS und der Maintenance-Modus

Zum Patchen, Ausschalten oder für andere Administrationsaufgaben auf einem ESX-Host ist es notwendig, alle darauf laufenden VMs zu stoppen. In größeren Umgebungen mit DRS kann dies sehr problematisch werden, denn bei mehreren Administratoren führen Migrationen oder andere Aktivitäten auf dem gewünschten ESX-Host, das Herunterfahren oder das Patchen schnell zu größeren Problemen. Um diese Schwierigkeiten zu umgehen, wurde der Maintenance-Modus von VMware entworfen. Vor diesen Administrationstätigkeiten wird der Maintenance-Modus für einen ESX-Host entweder per vCenter-Client oder über die Kommandozeile aktiviert. In der Zeit, bis ein ESX-Host den Maintenance-Status erreicht hat (zuerst müssen alle darauf laufenden VMs verschoben oder gestoppt werden), und während des Maintenance-Modus werden auf diesem ESX-Server keine Aktionen mit den darauf abgelegten virtuellen Maschinen zugelassen. Dies betrifft auch das Verschieben von VMs mittels vMotion auf diesen Host.

Wird der Maintenance-Modus auf einem ESX-Host im DRS-Cluster gestartet, werden im vollautomatischen Betrieb alle VMs auf freie Ressourcen innerhalb des Clusters verschoben. Erst danach ist der Maintenance-Modus aktiv.

Manuell eingreifen

Bedenken Sie, dass der Maintenance-Modus erst aktiviert wird, wenn die VMs entweder auf andere Hosts migriert, abgeschaltet oder suspendiert wurden. Sind die vMotion-Kriterien nicht erfüllt, kann der Maintenance-Modus nicht automatisch aktiviert werden, und Sie müssen manuell eingreifen.

5.3.11 DRS-Limitierungen mit vSphere

Mit vSphere 5 sind folgende Limitierungen in Bezug auf VMware DRS bekannt:

Beschreibung	Limitierung
ESX-Hosts pro DRS-Cluster	32
aktive VMs in einem DRS-Cluster	3.000
aktive VMs pro ESX-Host in einem DRS-Cluster	512

Tabelle 5.7 DRS-Cluster-Limitierung

5.3.12 DPM (Distributed Power Management)

DPM alias »Distributed Power Management« war lange Zeit nur experimentell verfügbar, hat aber nun die volle VMware-Unterstützung. Dies ist eine der Funktionen, die am meisten kontrovers diskutiert werden, da DRS aufgrund der Auslastung versucht, viele VMs auf möglichst wenige ESX-Hosts zu verteilen, um die frei werdenden Hosts energiesparend in den Standby-Modus zu stellen.

Kritiker möchten natürlich nicht, dass Ressourcen künstlich konsolidiert und vorhandene Systeme abgeschaltet werden. Außerdem bestehen Bedenken, dass die abgeschalteten Systeme vielleicht nicht oder zu langsam bei steigenden Anforderungen wieder aktiv werden.

Allerdings gibt es genügend Gründe, dieses Risiko einzugehen, wenn es um Energieeffizienz und Kosteneinsparungen geht. Vor allem Provider und große IT-Unternehmen, die Ihre Hardware nicht im Detail planen können, sondern zwangsweise mehr Hardware vorhalten müssen als wirklich nötig, um die Spitzen abzufangen, ziehen großen Nutzen aus DPM.

DPM erfordert allerdings, dass die ESX-Server-Hardware den Standby-Modus unterstützt und auch wieder »aufgeweckt« werden kann. An Möglichkeiten stehen HP iLO, sämtliche IPMI-Schnittstellen und Wake on LAN auf der ESXi Management-Schnittstelle als Optionen bereit. Diese Konfiguration müssen Sie manuell in der Configuration des ESX-Hosts unter Power Management durchführen.

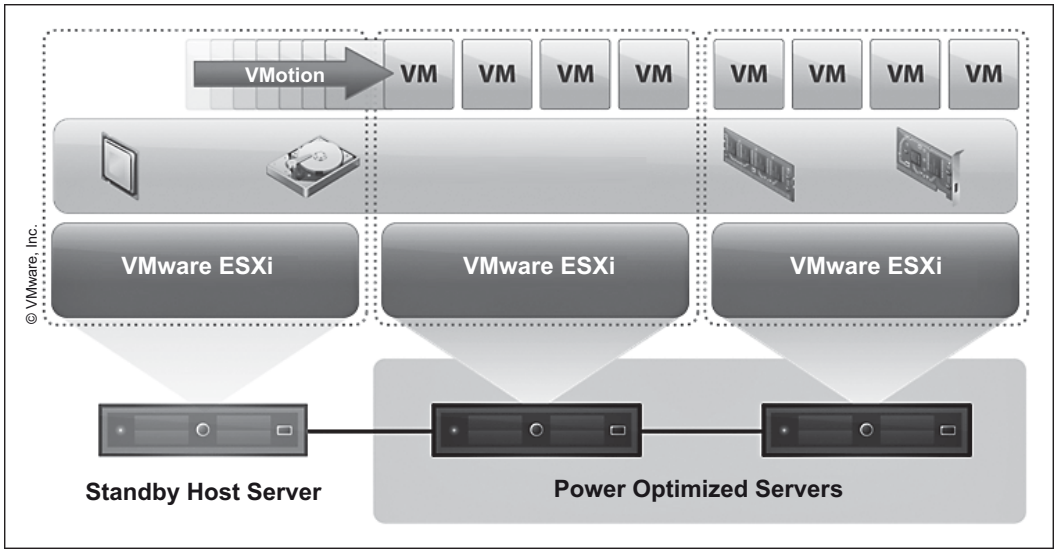


Abbildung 5.62 DPM schaltet nicht benötigte Hosts in einen Standby-Modus, um Energie einzusparen.

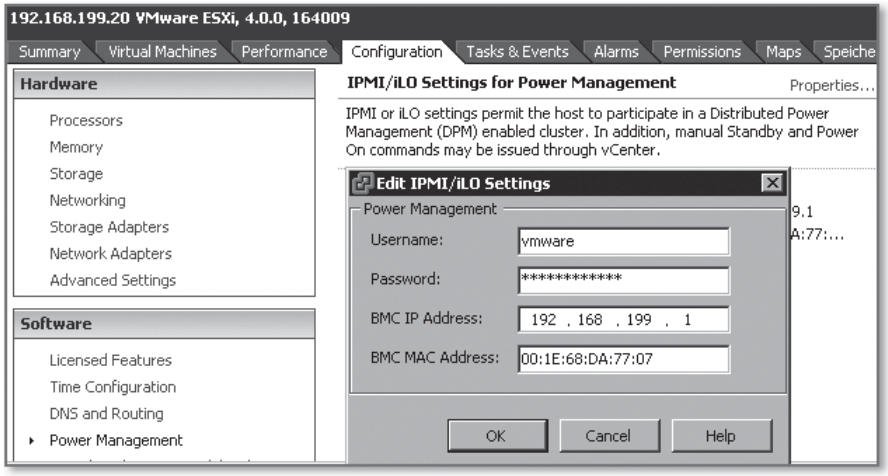


Abbildung 5.63 IPMI/iLO-Einstellung für DRS

Nachdem Sie sichergestellt haben, dass die Power-Management-Funktion des ESX-Servers korrekt eingetragen ist, können Sie DPM unter dem Punkt Power Management in den Eigenschaften des DRS-Clusters einrichten. Schalten Sie DPM ein, so können Sie entweder den ESX-Host manuell evakuieren, und DRS stellt entsprechende Empfehlungen bereit, oder Sie lassen DPM ähnlich der Fully automated-Einstellung selbständig agieren und bestimmen nur, anhand welcher Priorität die VMs migriert und die freien Systeme abgeschaltet werden.

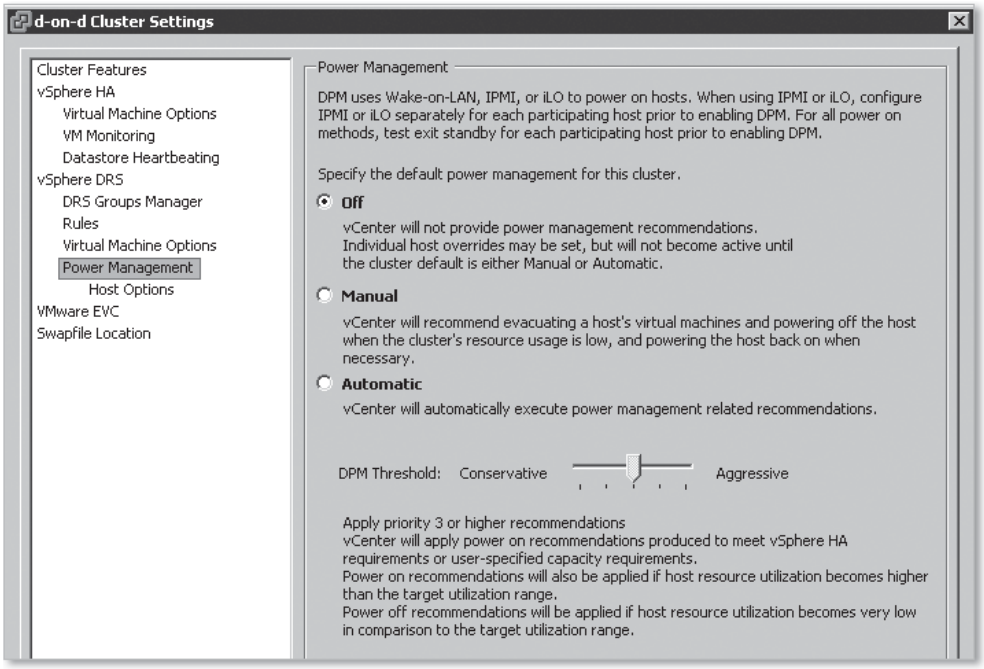


Abbildung 5.64 DPM-Konfiguration innerhalb des DRS-Clusters

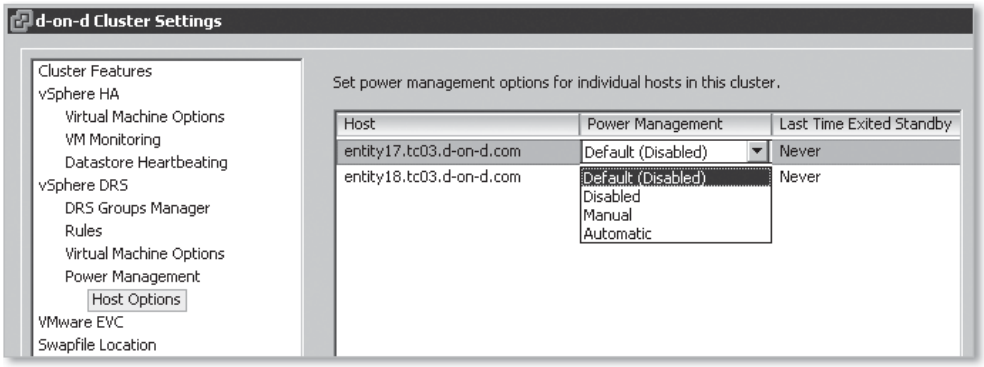


Abbildung 5.65 DPM-Einstellungen pro ESX-Host

Selbstverständlich ist es möglich, einzelne Hosts mit anderen Einstellungen zu versehen und komplett aus DPM zu entfernen. Außerdem können Sie unter Power Management • Host Options den Zeitpunkt des letzten erfolgreichen Standby-Vorgangs einsehen. Derzeit leider nur über eigene Erweiterungen durch Skripte möglich ist eine Zeitsteuerung. Es wäre für viele Unternehmen interessant, zu einer gewissen Abendstunde DPM zu aktivieren, morgens vor den Stoßzeiten wieder zu deaktivieren und alle ESX-Hosts verfügbar zu halten. An dieser Stelle können wir daher nur auf die PowerShell oder Perl verweisen.

5.3.13 HA und DRS in Kombination

HA und DRS werden sehr häufig gleichzeitig in einem Cluster aktiviert, um sämtliche Funktionen nutzen zu können. Die beiden Produkte ergänzen sich auch sehr gut; so kann DRS beispielsweise die virtuellen Maschinen anhand ihrer Last optimal verteilen, nachdem ein ESX-Host ausfiel und die VMs »wahllos« auf den übrigen ESX-Servern neu gestartet wurden.

Außerdem bietet DRS einen großen Vorteil bezüglich des Wartungsmodus (Maintenance-Modus), da die virtuellen Maschinen automatisch von dem zu wartenden System evakuiert werden, vorausgesetzt, die virtuellen Maschinen sind korrekt konfiguriert (keine verbundenen Wechselmedien, gleiche Netzwerke, keine lokalen Festplatten). Allerdings sollten Sie beachten, dass eine HA-DRS-Kombination realistisch erst ab drei ESX-Hosts im Cluster sinnvoll genutzt werden kann.

5.4 Storage DRS

Mit der Einführung von DRS vor einigen Jahren, das die CPU- und Memory-Last überwachte und auf deren Basis eine Lastverteilung durchführte, kam bei vielen Kunden der Gedanken auf, warum dies nicht auch mit Storage machbar sei. VMware hat mit vSphere 5 genau dieses Feature mit Storage DRS in einer äußerst umfangreichen Art implementiert, die weit über die rudimentäre Überwachung von DRS hinausgeht. Storage DRS (SDRS) überwacht nicht nur die I/O-Last der Datastores, sondern auch die Plattenplatznutzung, und verschiebt VMDK-Dateien. Außerdem ist SDRS in der Lage, die Informationen der Storage-Awareness (VASA) zu nutzen.

Bei Storage DRS stechen fünf Funktionen besonders heraus:

- **Datastore-Cluster**
  Fasst mehrere Datastores zu einem flexiblen Ressourcenpool zusammen, der mit Eigenschaften versehen werden kann, um das Initial Placement und die Lastverteilung zu optimieren.
- **Datastore Maintenance Mode**
  Wann immer ein Datastore geleert werden muss, hilft der Datastore-Maintenance-Modus, der ähnlich wie DRS bei der Wartung von Hosts die virtuellen Maschinen samt Festplatten und allen Dateien per Storage vMotion auf andere Datastores migriert. Diese Funktion ist beispielsweise auch sehr nützlich, wenn ein Neu-Design des Storage stattfinden soll und alte Datastores durch neue ersetzt werden sollen.
- **Affinity-Rules**
  Auch Storage DRS muss die Funktion der virtuellen Maschinen beachten und kann nicht wahllos VMs und Festplatten per Storage vMotion verschieben. Dazu dienen die Affinity-Rules, mit denen VMs separiert und VMDK-Dateien zusammengehalten werden können.

- **Initial Placement**
  Bei der Anlage virtueller Maschinen können Sie den Datastore-Cluster angeben, dann sucht Storage DRS automatisch nach dem bestgeeigneten Datastore und gibt Empfehlungen aus.
- **Load-Balancing**
  Anhand von I/O- und Festplattenplatz-Eigenschaften kann Storage DRS eine manuelle (per Empfehlung) oder automatische Lastverteilung durchführen, um Hot-Spots im Storage zu vermeiden (Datastores mit besonders viel Last, während andere Datastores keinerlei Last oder Belegung verspüren).

5.4.1 Voraussetzungen und Limitierungen

Folgende Punkte sollten Sie bei Storage DRS beachten:

- SDRS benötigt eine Enterprise-Plus-Lizenz.
- SDRS und SRM funktionieren nicht zusammen.
- SDRS setzt einen ESXi 5-Hosts voraus.
- SDRS-Datastore-Cluster können VMFS und NFS nicht mischen.
- SSD kann nicht mit anderen Datenträgern (SAS/FC/SATA) gemischt werden.
- Maximal werden 32 Datastores per Cluster unterstützt.
- Maximal warden 256 Datastore-Cluster per vCenter Server unterstützt.
- Maximal werden 9.000 VMDK-Dateien per Datastore-Cluster unterstützt.
- Replizierte Datastores sollten mit nichtreplizierten nicht gemeinsam in einem Datastore-Cluster angelegt werden.
- SDRS-Datastore-Cluster dürfen nicht über mehrere Rechenzentren gespannt sein (zumindest kein offizieller Support).
- Rebalance der VMDK-Dateien erfolgt alle 8 Stunden.
- SDRS hat keine Kenntnis von Templates und VMs, die nicht im vCenter registriert sind.

5.4.2 Anlage des Datastore-Clusters

Obwohl man aufgrund des »DRS« im Namen auch Storage DRS im Host-Cluster suchen würde, finden Sie die einzig mögliche Einstiegsstelle in der Datastore-Ansicht des vCenters.

Dort beginnen Sie mit der Anlage der Hauptkomponente, dem Datastore-Cluster, indem Sie im gewünschten Datacenter mittels Auswahl von New Datastore Cluster den Dialog starten (Abbildung 5.66).

Danach wird der Datastore-Cluster-Name verlangt, und Sie können Storage DRS direkt aktivieren (Abbildung 5.67).

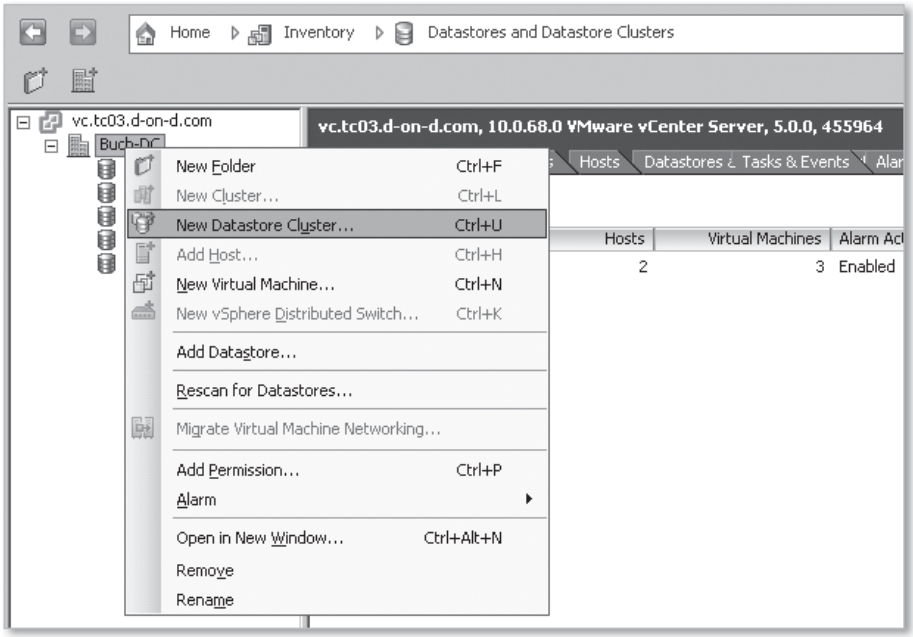


Abbildung 5.66 Anlage des Datastore-Clusters

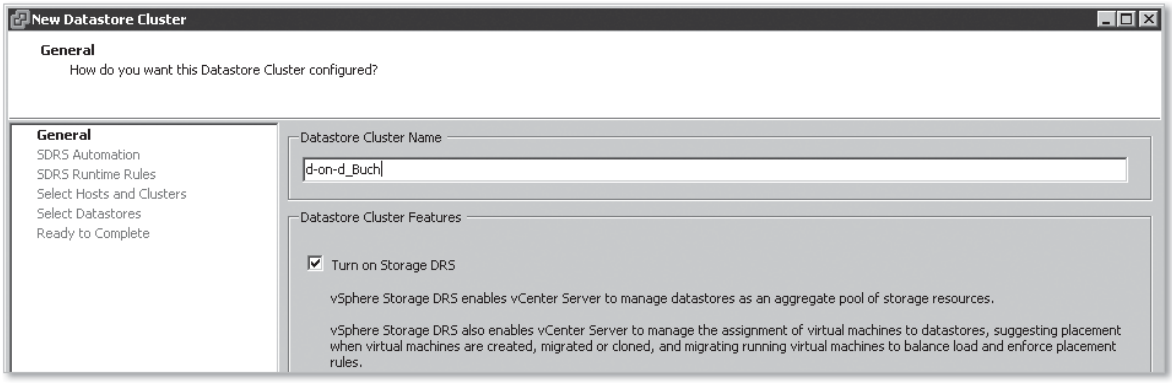


Abbildung 5.67 Vergabe des Datastore-Cluster-Namens und Aktivierung von Storage DRS

Im nächsten Dialogfenster geht es um die Form der Migration und des Platzierens neuer virtueller Maschinen. Wählen Sie No Automation (Manual Mode) aus, so werden Sie beim Anlegen der VMs gefragt, ob Sie mit der Empfehlung einverstanden sind, und es findet keine automatischen Migration mittels Storage vMotion (nur durch Annahme der Empfehlungen, ähnlich DRS) statt.

Fully Automated wiederum nimmt Ihnen einen großen Teil der Entscheidungen ab und funktioniert automatisiert anhand der vergebenen Regeln.

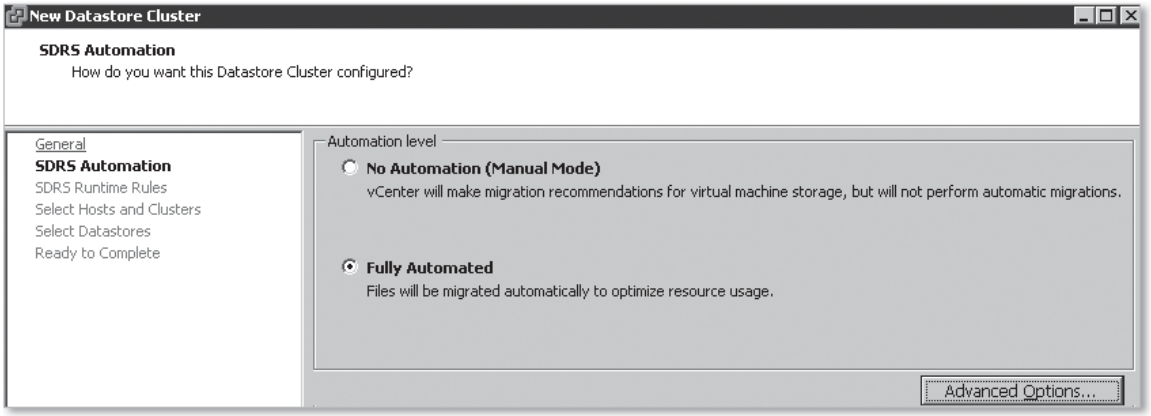


Abbildung 5.68 Automation-Level-Einstellung

Wichtig: Sie sollten niemals ohne vorherige Absprache mit Ihrem Storage-Administrator Storage DRS aktivieren geschweige denn auf automatisch stellen. Bedenken Sie immer, dass Funktionen im Storage-System wie Deduplizierung, Replikation und Thin Provisioning mit zu häufigen Storage-vMotion-Vorgängen und damit Datenveränderungen Probleme haben können. Dies reicht von erhöhtem Plattenplatzbedarf bis hin zum Aussteigen der Replikation (zu hohe Änderungsrate)!

Das Regelwerk kann entweder einfach (siehe Abbildung 5.69) oder komplex (siehe Abbildung 5.70) gehalten werden, einfach durch das Ein- oder Ausklappen mittels Show/Hide Advanced Options.

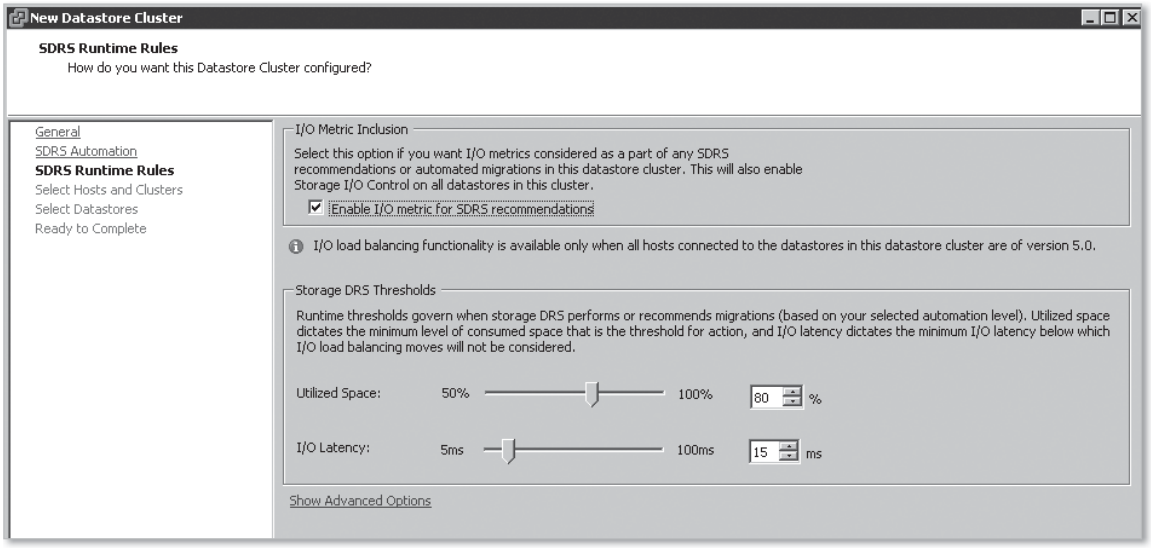


Abbildung 5.69 Einfache Storage-DRS-Regeln

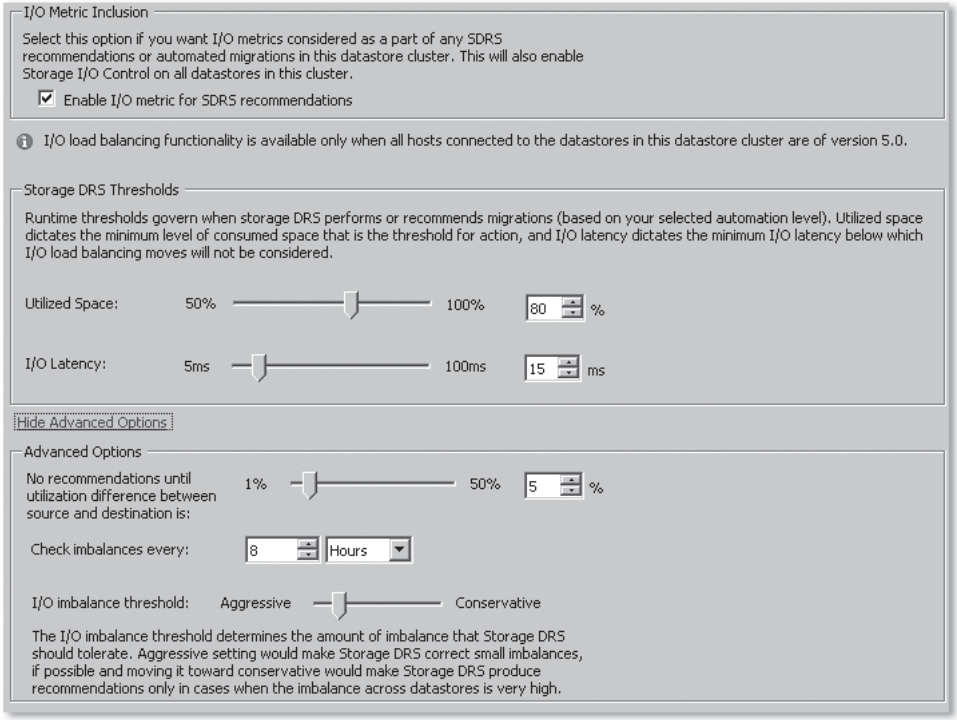


Abbildung 5.70 Erweitertes SDRS-Regelwerk

- Enable I/O metric for SDRS recommendations: Sobald diese Option ausgewählt wird, werden I/O-Patterns als Lastverteilungsgrundlage in die SDRS-Berechnung einbezogen. Dadurch wird automatisch Storage I/O Control auf allen Datastores aktiviert, das in Idle-Zeiten, wenn der Storage im Leerlauf ist, Performancetests seitens VMware durchführt.
- Utilized Space: Diese Einstellung ist selbsterklärend – so findet die Lastverteilung aufgrund des belegten Festplattenplatzes in % statt.
- I/O Latency: die Antwortzeiten des Storage-Systems, *I/O Latency* oder deutsch *Latenzzeiten* genannt, sind ein wichtiger Aspekt bei der Zuordnung der virtuellen Maschinen. Systeme mit hoher Latenz sind von einem Leistungsverlust während des I/O-Transportwegs betroffen. Diese Einstellung lässt SDRS erst einsetzen, wenn Storage-Systeme mit höheren Latenzwerten als die Angabe erkannt werden.
- No recommendations until utilization difference between source and destination is: Auch diese Einstellung ist aufgrund des langen Textes selbsterklärend. Wenn die Plattenbelegung nicht mehr als der angegebene Wert (im Beispiel 5 %) differiert, wird SDRS nicht eingreifen.
- Check imbalance every: Im Standard werden die Eigenschaften der Datastores alle 8 Stunden geprüft. Diese Einstellung sollten Sie auch nicht zu euphorisch nach unten anpassen, um Leistungsprobleme im Storage-Netz zu vermeiden.

- I/O IMBALANCE THRESHOLD: Vergleichbar mit dem DRS Star Rating existiert auch bei SDRS eine Bewertung der Datastores anhand der Ungleichmäßigkeiten. Diese Einstellung dient dazu, die Aggressivität von Storage DRS festzulegen.

Im nächsten Dialog (Abbildung 5.71) stehen die einzubeziehenden Cluster oder ESX-Hosts zur Auswahl.

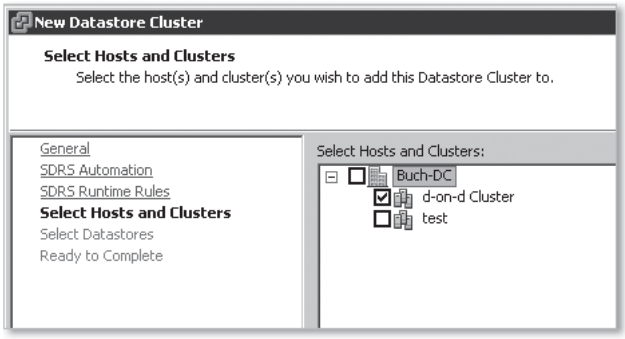


Abbildung 5.71 Auswahl der betroffenen Hosts und Cluster

Bei der Auswahl der zu integrierenden Datastores (Abbildung 5.72) sollten Sie darauf achten, möglichst gleiche oder zumindest ähnliche Storage-Konfigurationen (RAID-Level, Datenträgertyp, Anbindung) zu verwenden und NFS nicht mit VMFS zu mischen. Außerdem sollten Sie nach Möglichkeit mit VASA (vStorage API for Storage Awareness) bei entsprechender Unterstützung durch das genutzte Storage-System arbeiten.

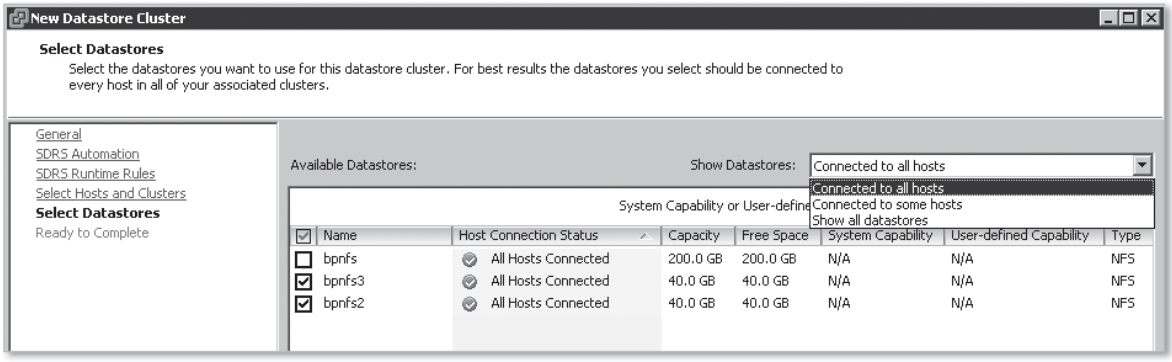


Abbildung 5.72 Auswahl der betroffenen Datastores

Zur Sicherheit erhalten Sie kurz vor Abschluss nochmals eine Zusammenfassung aller wesentlichen Einstellungen (Abbildung 5.73).

Schauen Sie sich nach der Anlage die Datastore-Anzeige nochmals an, erkennen Sie, dass ein neuer Cluster erstellt wurde, unter dem die beiden Datastores zu sehen sind (Abbildung 5.74).

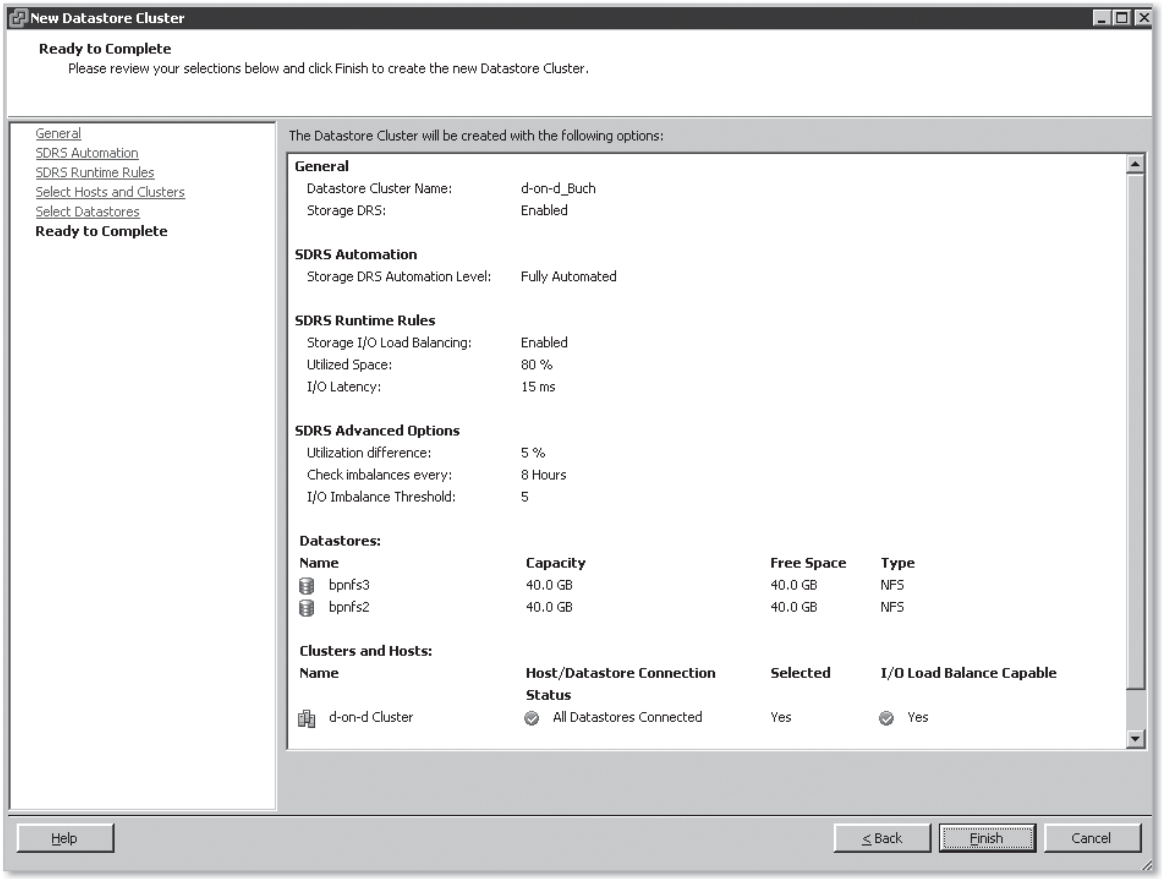


Abbildung 5.73 Zusammenfassung des Datastore-Clusters

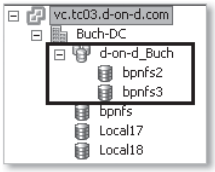


Abbildung 5.74 Datastore-Cluster in der Datastore-Ansicht

5.4.3 SDRS Initial Placement

Das Initial Placement kommt bei der Anlage neuer VMs zum Tragen, wenn nach dem Ablageort gefragt wird. Möchten Sie mit Storage DRS arbeiten, wählen Sie statt des einzelnen Datastores den Datastore-Cluster aus (Abbildung 5.75).

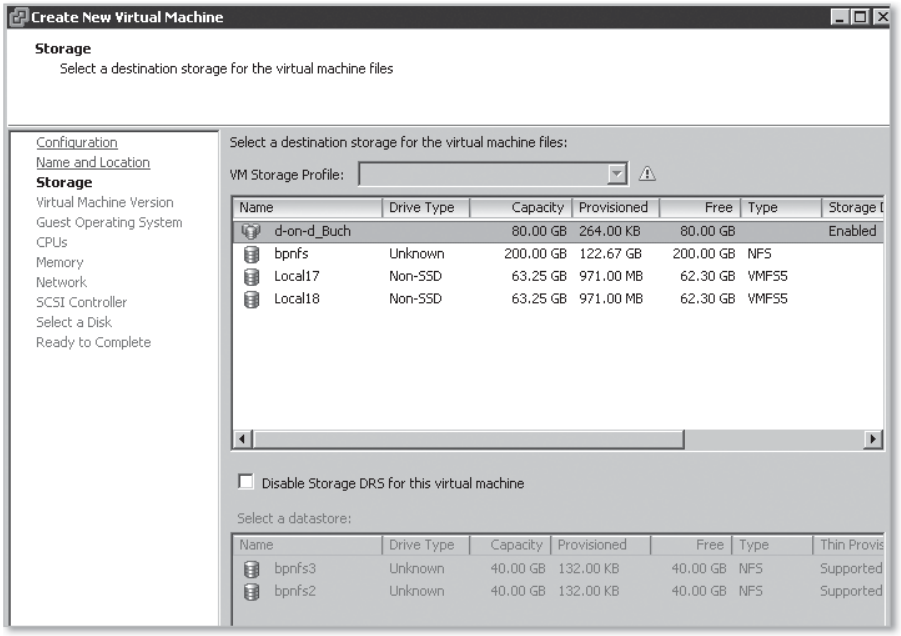


Abbildung 5.75 Auswahl des Datastore-Clusters bei Anlage der VM

Nach der Auswahl erscheint abhängig von der Automatisierungsoption des Datastore-Clusters die Empfehlung seitens SDRS, die Sie annehmen oder verändern können (Abbildung 5.76).

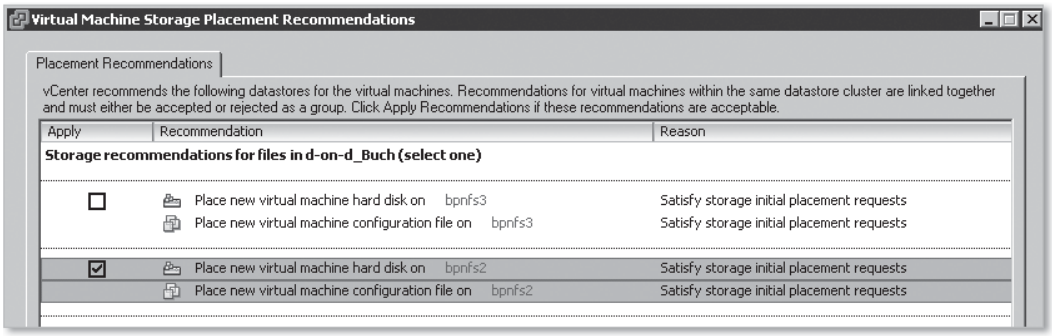


Abbildung 5.76 Datastore-Empfehlungen

Wird keine Möglichkeit der Platzierung gefunden, erscheint statt einer Empfehlung ein Fehler, den Sie behoben müssen. In unserem Beispiel ist die anzulegende Festplatte der virtuellen Maschine schlichtweg zu groß, um auf einen SDRS-Cluster-Datastore zu passen (Abbildung 5.77).

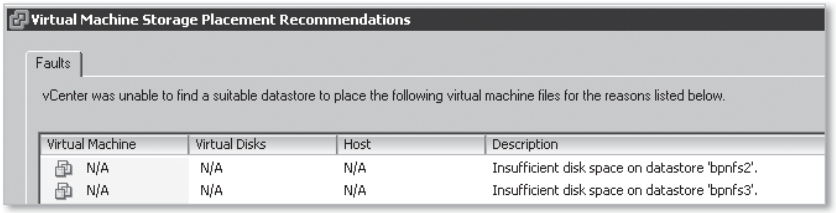


Abbildung 5.77 Fehler beim automatischen Platzieren der VM

5.4.4 SDRS-Regelwerk

Wie DRS können Sie auch SDRS unter Umständen nicht einfach gewähren und beliebig VMDK-Dateien verschieben lassen, sondern Sie möchten Systeme zusammenhalten oder auf unterschiedlichen Datastores betreiben.

Vielleicht sollen die beiden Applikations-Cluster nicht auf dem gleichen Datastore laufen, also separiert werden. Oder Sie möchten die VMDK-Dateien der VMs aufteilen, da aufgrund besserer Deduplizierungsraten verschiedene Datastores für System, Daten- und Swap-VMDK-Datei genutzt werden sollen.

Dies ist mit den SDRS-Regeln möglich, die Sie auf VM-Ebene oder VMDK-Ebene einrichten können (Abbildung 5.78 und Abbildung 5.79).

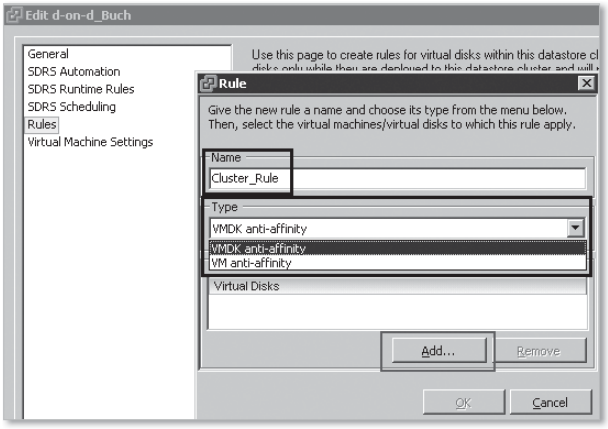


Abbildung 5.78 SDRS-Regeln

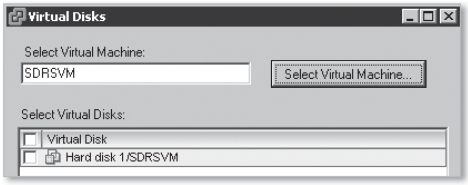


Abbildung 5.79 Auswahl der VMDK-Dateien für die SDRS-Regel

Pro virtueller Maschine bzw. VMDK-Datei können Sie das Automationslevel einzeln anpassen, oder Sie bestimmen per Checkbox das Zusammenführen der VMDK-Dateien auf einem Datastore (Abbildung 5.80).

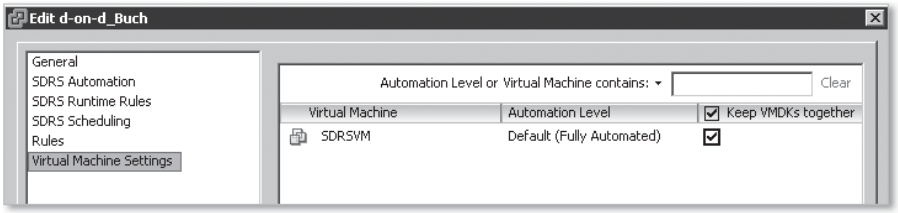


Abbildung 5.80 SDRS-VM-Regeln

Es gilt aber der gleiche Leitsatz wie bei der Verwendung der DRS-Regeln: Jede Regel benötigt bei der Auswertung Ressourcen und verlängert die Rechenzyklen bei der SDRS-Entscheidungsfindung.

5.4.5 SDRS-Zeitsteuerung

Storage DRS hat noch eine enorm nützliche Funktion zu bieten, falls Sie Tages- oder Wochenzeiten haben, an denen bestimmte virtuelle Maschinen oder Datastores, die sonst sehr genügsam sind, sehr viele I/O-Ressourcen benötigen. Um dem Rechnung zu tragen, können Sie die Lastverteilung anpassen, damit beispielsweise keinerlei Storage-vMotion-Aktivitäten stattfinden. In diesem Szenario kommt der SDRS Scheduler mit der Zeitsteuerung ins Spiel.

Mit ihm legen Sie einen generellen Zeitplan für den Scheduler an, nach dem die Änderungen stattfinden sollen (Abbildung 5.81).

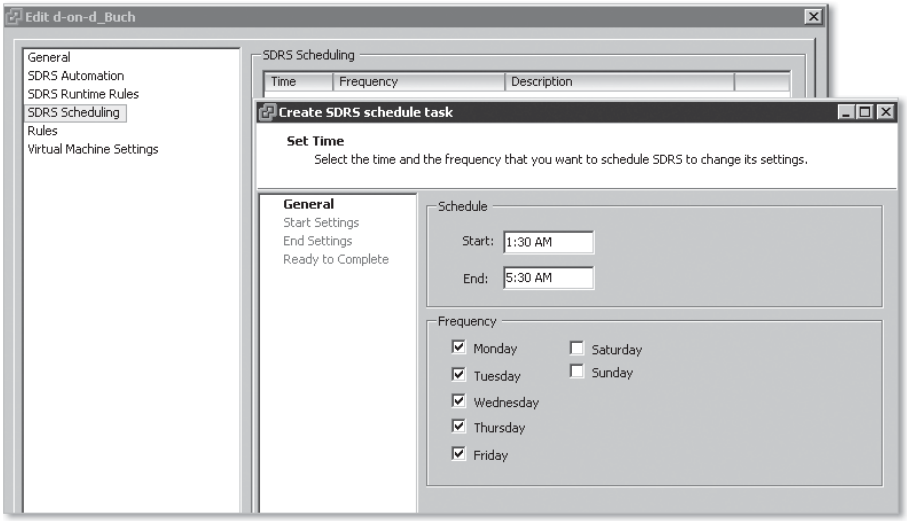


Abbildung 5.81 Einrichtung eines SDRS-Zeitplans

Im den beiden Nachfolgedialogen passen Sie die SDRS-Regel zur Startzeit des Zeitfensters entsprechend an (Abbildung 5.82) und setzen diese zum Ende des Zeitfensters wieder auf die Startkonfiguration zurück (Abbildung 5.83).

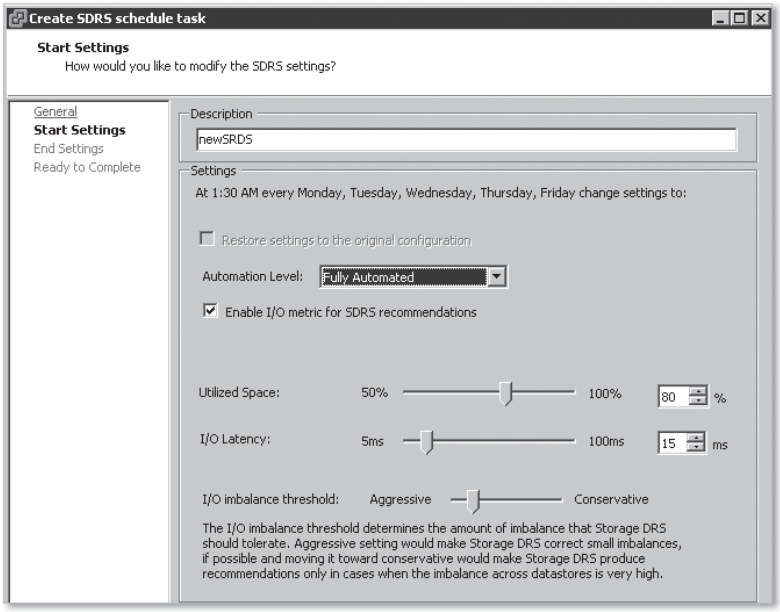


Abbildung 5.82 Starteinstellungen des SDRS Scheduled Tasks

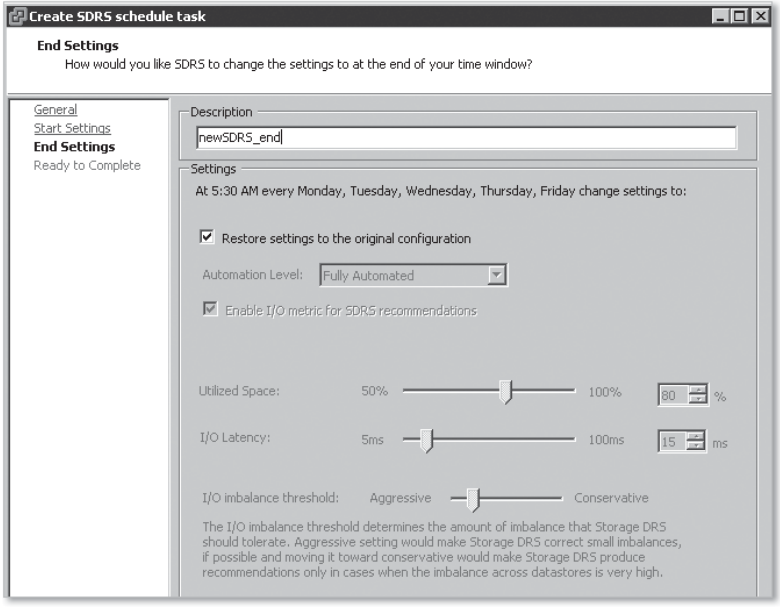


Abbildung 5.83 Stoppeinstellungen des SDRS Scheduled Tasks

Alle verfügbaren Regeln werden anschließend in der SDRS SCHEDULING-Ansicht angezeigt und können gelöscht oder editiert werden (Abbildung 5.84).

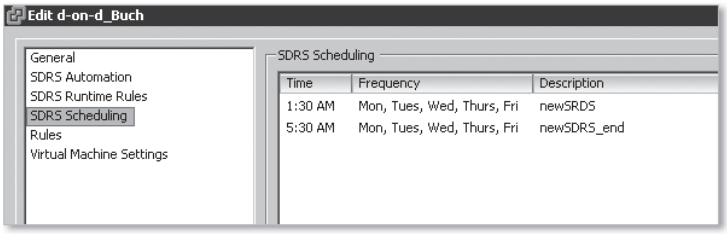


Abbildung 5.84 Übersicht des Zeitplans

5.4.6 SDRS Maintenance Mode

Wie bereits erwähnt besteht durch SDRS die Möglichkeit, alle virtuellen Maschinen samt Festplatten ohne Ausfall automatisch von einem Datastore auf andere Datastores des Datastore-Clusters zu migrieren, wenn Sie eine Wartung an dem Datastore ausführen müssen oder einen Datastore entfernen möchten.

Dazu wechseln Sie in die Datastore-Ansicht des vCenters, wählen den gewünschten Datastore innerhalb des Datastore-Clusters aus und rufen im Kontextmenü ENTER SDRS MAINTENANCE MODE aus (Abbildung 5.85).

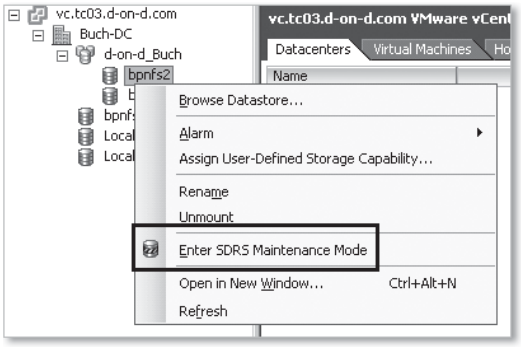


Abbildung 5.85 SDRS Maintenance Mode aktivieren

Anschließend startet direkt der Migrationsvorgang, und Sie können die Fortschritte in der RECENT TASK-Ansicht verfolgen (Abbildung 5.86).

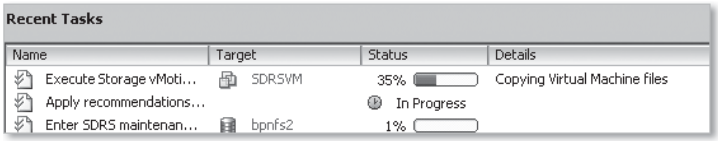


Abbildung 5.86 SDRS beginnt mit der Migration der VMs, sobald der Wartungsmodus aktiviert wurde.

5.4.7 SDRS und Speicherprofile

Man könnte definitiv »last but not least« zur letzten beschriebenen Funktion von SDRS in diesem Abschnitt sagen, da diese die VM-Speicherprofile mit den SDRS-Regeln zusammenführt.

VM-Speicherprofile wird in in Kapitel 9, »Storage-Architektur«, besprochen; sie dienen dazu, Datastores Eigenschaften zuzuweisen, die den virtuellen Maschinen als Profil zugeordnet werden können. So ist es möglich, die Datastores eines Metro-Clusters mit der höchsten Verfügbarkeit SLA1 zu kennzeichnen und den Datastore eines einzelnen RAID-5-Arrays mit deutlich weniger Verfügbarkeit mit SLA2 zu kennzeichnen.

Während der Anlage virtueller Maschinen sind Sie dank den VM-Speicherprofilen und den Datastore-Clustern in der Lage, Storage DRS automatisch den korrekten Ablageort auswählen zu lassen (Abbildung 5.87).

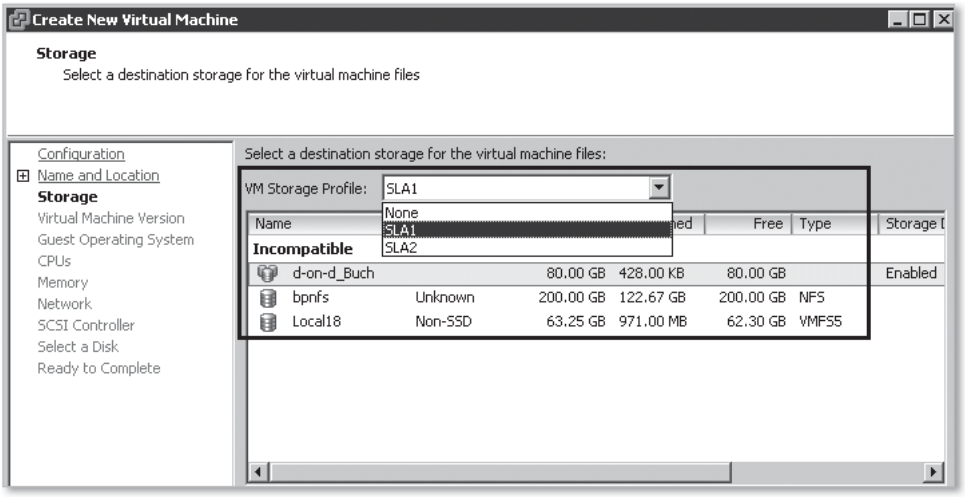


Abbildung 5.87 Kombination VM-Speicherprofil – SDRS

5.5 Fault Tolerance

Fault Tolerance (FT) ist eine neue Technologie von VMware und wurde mit VMware vSphere 4 eingeführt. Im Gegensatz zu VMware High Availability (vSphere HA), bei dem die virtuellen Maschinen auf einem anderen Host neu gestartet werden, sobald ein Cluster-Knoten ausfällt, läuft die virtuelle Maschine bei FT nahtlos weiter.

Das bedeutet: keine Ausfallzeit beim Absturz einer der durch FT geschützten virtuellen Maschinen. Dabei spielt es keine Rolle, ob nur die primäre VM ausgefallen ist oder das komplette Host-System, auf dem primäre VM lief. Es handelt sich also um eine erweiterte Hochverfügbarkeit, die vor Einführung auch als »Continuous High Availability« bezeichnet wurde. Ein Eingriff in den Gast ist nicht notwendig, allerdings müssen für FT viele Randbedingungen

erfüllt sein. Damit ist FT sogar weit mächtiger als die bekannten Cluster-Produkte und bietet den höchsten Grad an Ausfallsicherheit.

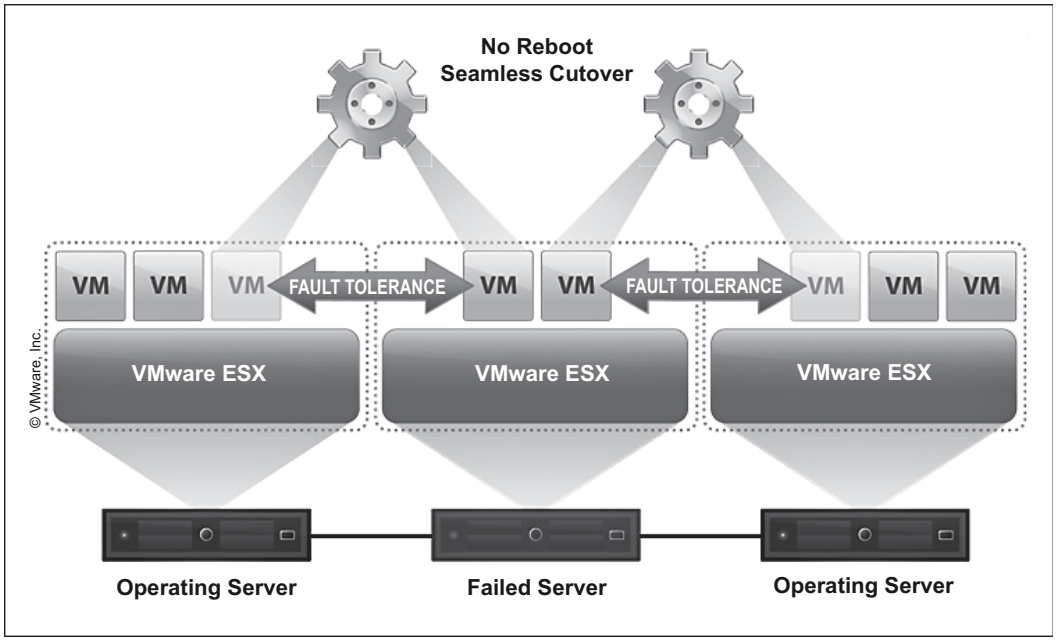


Abbildung 5.88 Fault Tolerance ermöglicht einen unterbrechungsfreien Betrieb virtueller Maschinen, sogar bei Ausfall des physischen ESX-Servers.

5.5.1 Wie funktioniert Fault Tolerance?

FT funktioniert mit bekannten Methoden. Mittels angepasstem vMotion wird eine sekundäre Maschine auf einem anderen Host des HA-Clusters erstellt und betrieben. Auf den ESX-Hosts läuft ein `vmklogger`-Prozess, der für die asynchrone Übertragung der Logs zuständig ist. Diese beiden Maschinen, primäre und sekundäre, greifen beide auf dieselben Dateien des Shared Storage zu. Doppelt werden nur die CPU-Befehle und der Inhalt des RAM gehalten, was über die vLockstep-Technologie geschieht.

Ändert sich zum Beispiel etwas im RAM der virtuellen Maschine, wird diese Änderung in beiden physischen Maschinen durchgeführt, bevor ein `commit` an die virtuelle Maschine gesendet wird. Die Befehle der CPU werden über die Record- und Replay-Funktion der VMware-Workstation übertragen.

Wichtig

Fällt die primäre virtuelle Maschine aufgrund eines Bluescreens aus, wird dieses Schicksal mit sehr hoher Wahrscheinlichkeit auch die sekundäre VM ereilen. Diese könnte allerdings durch HA Virtual Machine Monitoring neu gestartet werden.

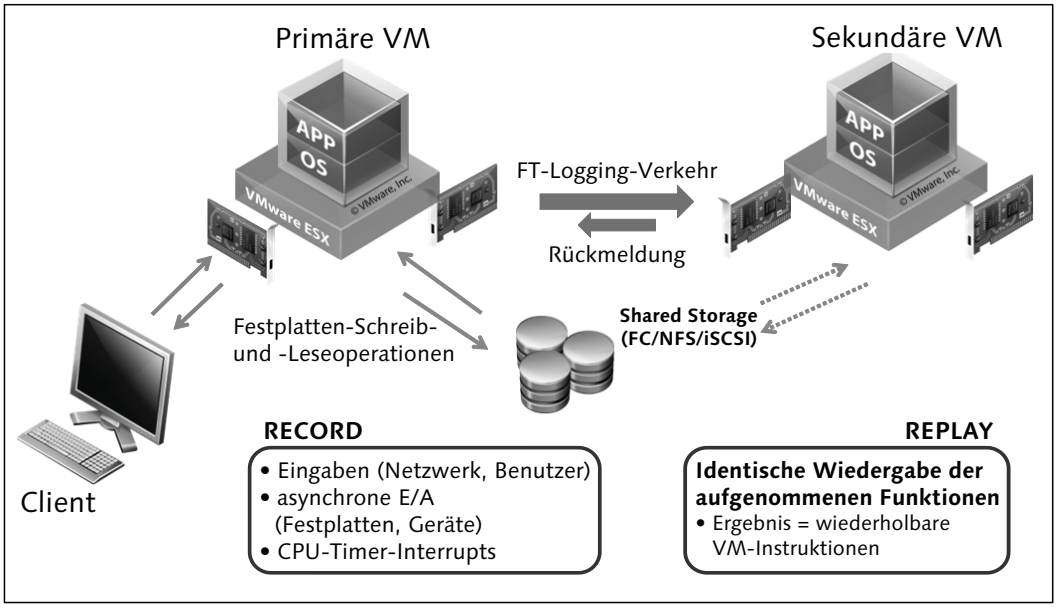


Abbildung 5.89 Funktionsübersicht von VMware Fault Tolerance

Wird die primäre VM gestartet, startet die sekundäre automatisch mit und wird, falls DRS aktiviert ist, anhand der DRS-Empfehlungen auf den entsprechenden Hosts verteilt. Wird die primäre VM heruntergefahren, wird auch die sekundäre VM heruntergefahren.

Sowohl primäre als auch sekundäre VM können mittels vMotion migriert werden, dürfen jedoch nie auf dem gleichen Host-System betrieben werden. Die beiden Primary- und Secondary-VMs unterhalten sich mittels Heartbeat miteinander, und ein Split-Brain wird durch Renaming (Umbenennung einer Datei im Shared Storage) verhindert.

5.5.2 Technische Voraussetzungen

Damit FT funktioniert, werden CPUs in den ESX-Hosts vorausgesetzt, die eine Hardwarevirtualisierung unterstützen. Das bedeutet, dass AMD-CPUs AMD-V und Intel-CPUs Intel VT unterstützen müssen. Abhängig von der CPU existiert übrigens noch eine Liste im Knowledge-Base-Eintrag 1008027 (*http://kb.vmware.com/kb/1008027*), welche Prozessoren ein Anschalten von FT bei aktiver oder nur bei abgeschalteter VM ermöglichen. Derzeit wird nur Intel Xeon mit 45-nm-Core-2-Architektur unterstützt, um laufende VMs mit FT zu konfigurieren, bei allen anderen CPUs muss die VM vorher abgeschaltet werden.

Neben der CPU-Kompatibilität müssen folgende Anforderungen erfüllt sein:

- Alle Hosts müssen mit derselben VMware ESX-Version installiert sein.
- Alle Hosts müssen im gleichen HA-Cluster konfiguriert sein.

- Shared Storage, da die Festplatten nicht repliziert, sondern gemeinsam genutzt werden
- Mindestens zwei Gigabit-Netzwerkkarten werden benötigt: eine dedizierte Karte für vMotion und eine dedizierte FT-Logging-Karte.
- Limitierung auf nur eine virtuelle CPU
- Festplatten müssen im Thick-Format sein, ansonsten werden sie konvertiert.
- DRS wird für die VM auf automatisch auf manuell umgestellt.
- Storage vMotion ist nicht erlaubt.
- Snapshots sind nicht erlaubt, und eine Anlage ist auch nicht möglich.
- Wechselmedien mit physischer Verbindung (nur ISO oder Client Device) sind nicht erlaubt.
- Paravirtualisierung im Gast ist nicht unterstützt.
- Keine USB- oder Soundgeräte werden unterstützt.
- Keine PCI-Passthrough-Unterstützung vorhanden.
- Keine Unterstützung für Device-Hot-Plugging vorhanden.
- Keine vlance-(AMD PCNet-)Netzwerkunterstützung vorhanden.
- RDM im Virtual Mode unterstützt, RDM im Physical Mode nicht

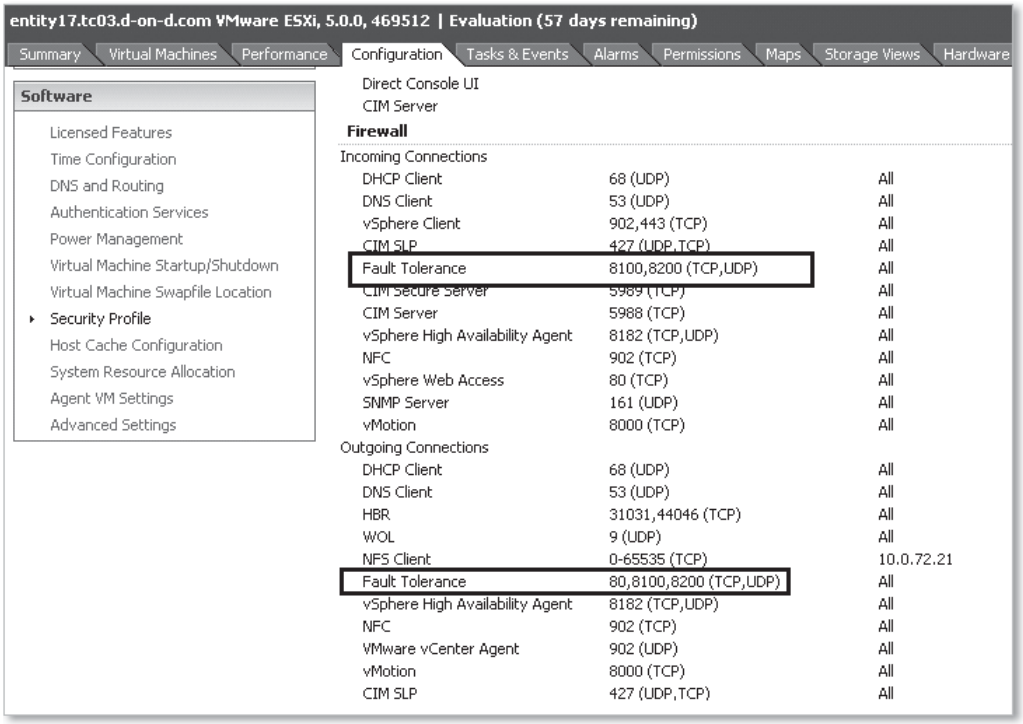


Abbildung 5.90 Fault-Tolerance-Firewall-Regel

Sobald ein FT-fähiger Management-Port eingerichtet ist und die CPU passt, wird automatisch eine Firewall-Regel für Fault Tolerance auf den ESX-Servern aktiviert. Diese sollten Sie auch nicht abschalten. Beim Management-Port sollten Sie beachten, dass das Fault-Tolerance-Netzwerk auf guten Durchsatz beim Datenverkehr angewiesen ist und daher ein von sonstigem Netzwerkverkehr getrenntes Netzwerk empfohlen wird.

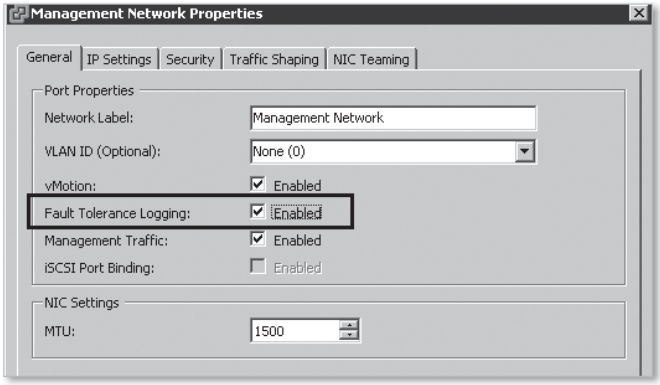


Abbildung 5.91 Aktivierung des FT-Loggings auf einem VMkernel-Port

Neben diesen Voraussetzungen müssen Sie eine weitere Einstellung setzen, die im vCenter konfiguriert wird. Es gibt die Möglichkeit, die ESX-Hosts auf SSL-Zertifikate überprüfen zu lassen. Diese Einstellung müssen Sie unter der VirtualCenter Management Server Configuration einschalten.

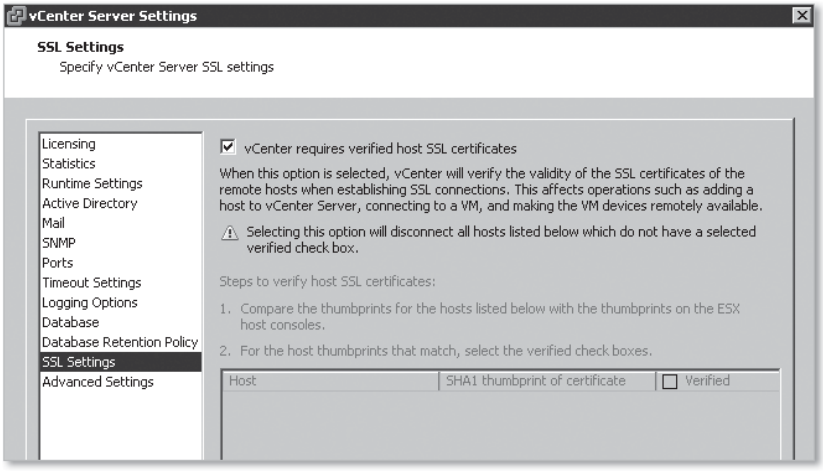


Abbildung 5.92 Die Überprüfung des SSL-Zertifikates muss für FT aktiviert sein.

Eine recht gute Möglichkeit, die FT-Funktionalität zu prüfen, liefert VMware direkt selbst mit dem Site Survey Tool, das auch ohne FT-Lizenz auf der VMware-Website zum Download bereitsteht: *http://www.vmware.com/download/shared_utilities.html*.

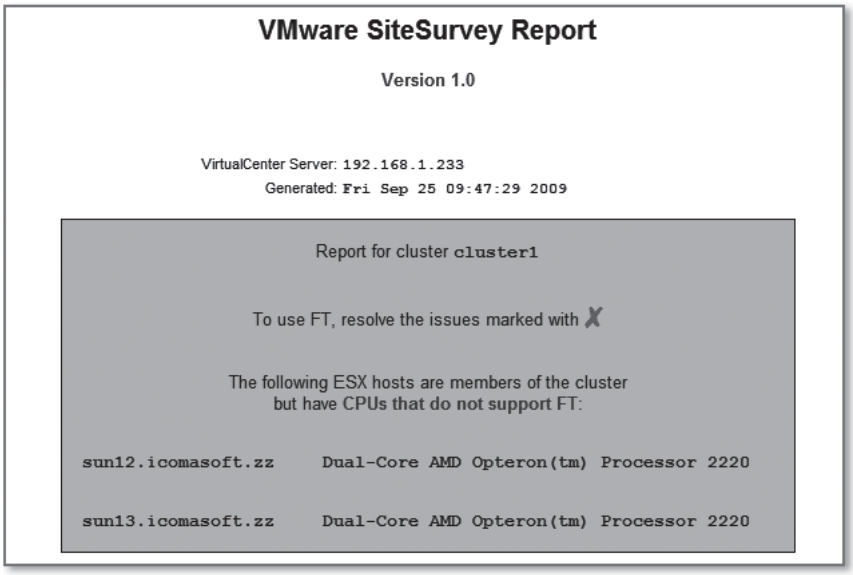


Abbildung 5.93 Eine sehr ärgerliche Meldung – die CPUs sind nicht FT-kompatibel.

Außerdem ist es mittels der VMware-Maps-Funktion möglich, sich Anhaltspunkte für den FT-Aufbau und mögliche Probleme anzuschauen.

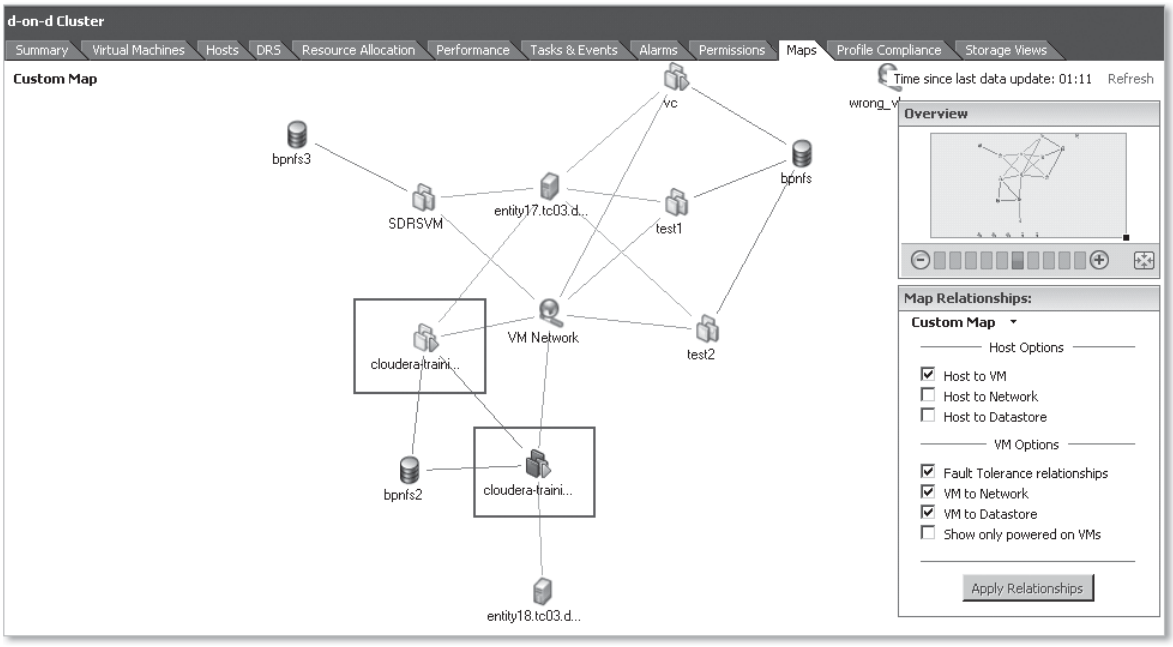


Abbildung 5.94 VMware Maps zur Anzeige des FT-Aufbaus

Berechnung des Fault-Tolerance-Logging-Datenverkehrs

Wer an der Berechnung des Fault-Tolerance-Logging-Datenverkehrs interessiert ist, sollte sich die Formel merken, mit der VMware die Datenmenge ermittelt:

VMware-FT-Logging-Bandbreite ~= (durchschnittliche Festplattenzugriffe (lesend) (MB/s) × 8 + durchschnittlicher Netzwerkverkehr (eingehend) (MBps)) × 1,2 [20 % Puffer]

5.5.3 Aktivieren von Fault Tolerance für eine virtuelle Maschine

Sind alle technischen Vorraussetzungen erfüllt, ist das Aktivieren von FT kein großes Problem mehr. Sie müssen nur abhängig von der genutzten CPU die VM gegebenenfalls vorher abschalten.

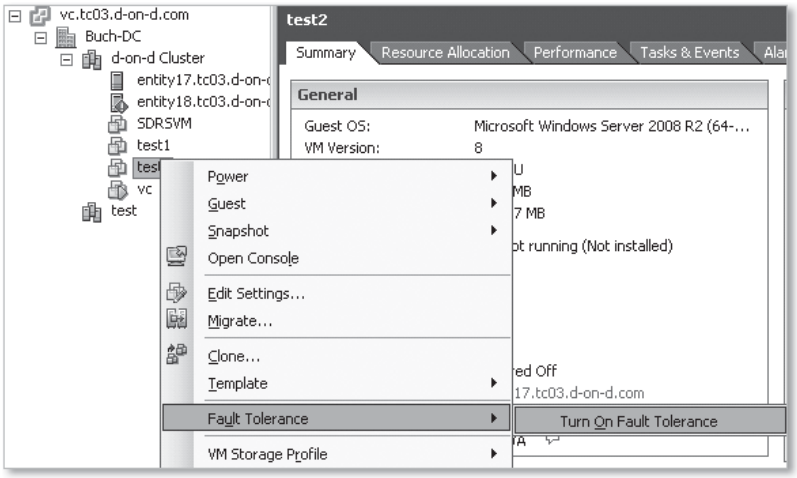


Abbildung 5.95 Aktivierung von FT über das Kontextmenü

Über das Menü im vCenter wählen Sie eine virtuelle Maschine aus. Nach einem Klick mit der rechten Maustaste öffnet sich das Menü mit den verschiedenen Einstellungen, in dem ein Punkt FAULT TOLERANCE heißt. Über diesen Punkt im Menü aktivieren Sie FT (TURN ON FAULT TOLERANCE).

Sollte der Menüpunkt ausgegraut sein, dann liegt dies mit hoher Wahrscheinlichkeit an einem der folgenden Punkte:

- Die VM wird auf einem Host betrieben, der über keine FT-Lizenz verfügt.
- Die VM wird auf einem Host im Maintenance- oder Standby-Zustand betrieben.
- Die VM ist vom vCenter getrennt oder verwaist (*orphaned*; *.vmx*-Datei ist nicht im Zugriff).
- Der Anwender hat keine Berechtigung, FT zu nutzen.

Danach findet direkt eine Überprüfung der VM auf Kompatibilität statt, und Thin-provisioned Disks können automatisch konvertiert und DRS kann automatisch abgeschaltet werden.

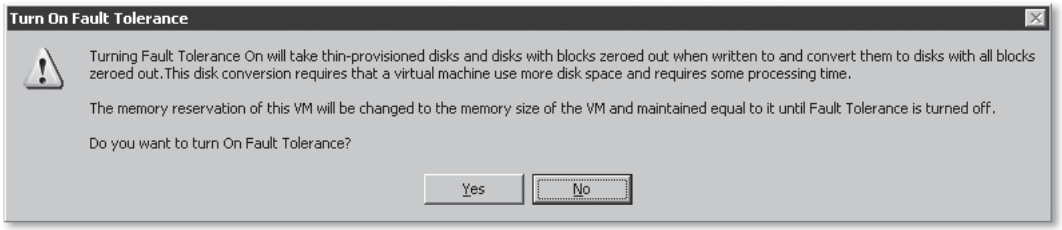


Abbildung 5.96 Automatische Anpassung der VM an die FT-Anforderungen

Nachdem Sie die Aktivierung bestätigt haben, erscheint im Recent Tasks-Fenster ein Task für die ausgewählte virtuelle Maschine, der Turn Fault Tolerance On heißt. Ist dieser Task abgeschlossen, wird ein weiterer Task aufgerufen, der FT startet.

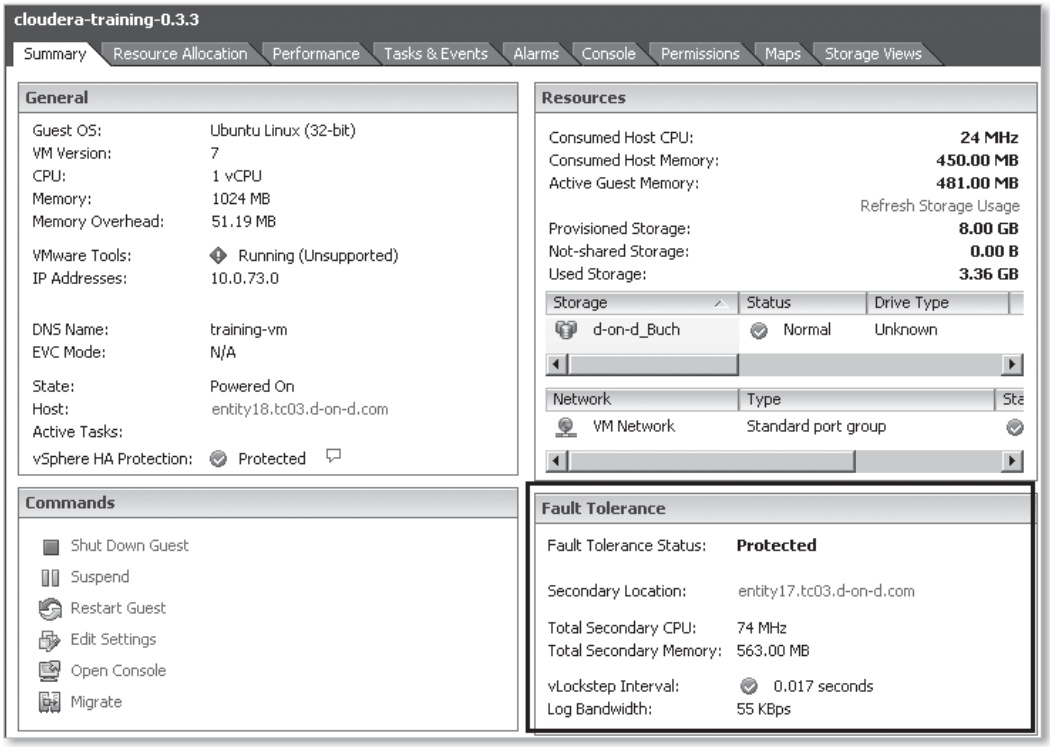


Abbildung 5.97 Anzeige des FT-Status in der »Summary«-Page der VM

Im selben Zug wird das Summary-Fenster der virtuellen Maschine um ein Fault Tolerance-Fenster erweitert. Dort finden Sie verschiedene Informationen zum FT-Status dieser virtuellen Maschine, zum Beispiel, auf welchem Host die sekundäre VM läuft und welche Latenzzeit bei

der Log-Übertragung herrscht. Das bekannte Icon der primären virtuellen Maschine im Inventar des vCenters wird außerdem in Blau geändert, so dass eine FT-geschützte VM direkt erkennbar ist.

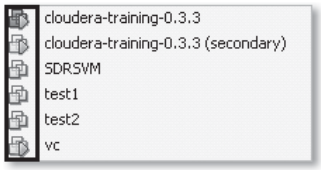


Abbildung 5.98 Anpassung des VM-Symbols nach erfolgreicher FT-Aktivierung

Schauen Sie sich die virtuellen Maschinen im Cluster an, werden Sie erkennen, dass ein weiterer Eintrag hinzugefügt wurde: Die durch FT geschützte virtuelle Maschine hat nun einen zweiten Eintrag, der durch (SECONDARY) erweitert wird. Dies ist die sekundäre Maschine, die verwendet wird, wenn die primäre Maschine ausfällt. Die sekundäre VM ist nur in der VIRTUAL MACHINES-Ansicht des Clusters oder des ESX-Hosts oder in der Ansicht VMS & TEMPLATES sichtbar.

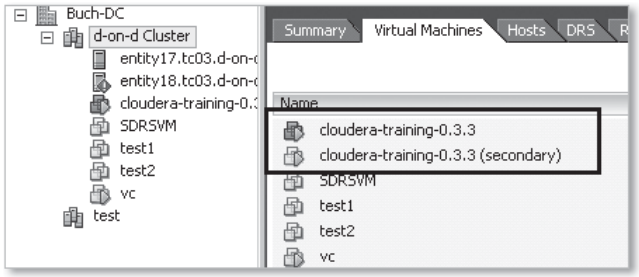


Abbildung 5.99 Anzeige der primären und sekundären VM

Ein schöner Test, um zu sehen, ob alles funktioniert, ist das Öffnen der Konsolen der primären und der sekundären virtuellen Maschine. Alles, was auf der Konsole der primären virtuellen Maschine ausgeführt wird, muss genauso auch auf der Konsole der sekundären virtuellen Maschine angezeigt werden. Wird zum Beispiel ein Video abgespielt, ist dies auf beiden Konsolen zu sehen. Sobald FT einwandfrei läuft, kann die primäre VM aus beliebigem Grund (mit Ausnahme des Ausfalls des Shared Storage) ausfallen, und die sekundäre VM springt in der gleichen Sekunde an und übernimmt die Funktionen der primären. Dies geschieht ohne Ausfall und ohne Datenverlust.

5.5.4 Bedienung von Fault Tolerance für eine virtuelle Maschine

Sobald Fault Tolerance für eine oder mehrere VMs aktiviert ist, existiert ein neues Kontextmenü mit deutlich mehr Menüpunkten zur Verwaltung von Fault Tolerance.

Option	Beschreibung
Turn Off Fault Tolerance	Abschalten von FT mit Löschung aller FT-Statistikdaten
Disable Fault Tolerance	vorübergehendes Abschalten von FT mit Beibehaltung aller FT-Statistikdaten
Migrate Secondary	Migration des sekundären Knotens auf einen anderen ESX-Host
Test Failover	FT-Umschaltung vom primären auf den sekundären Knoten testen
Test Restart Secondary	Neustart des sekundären Knotens

Tabelle 5.8 Optionen zur Verwaltung von Fault Tolerance

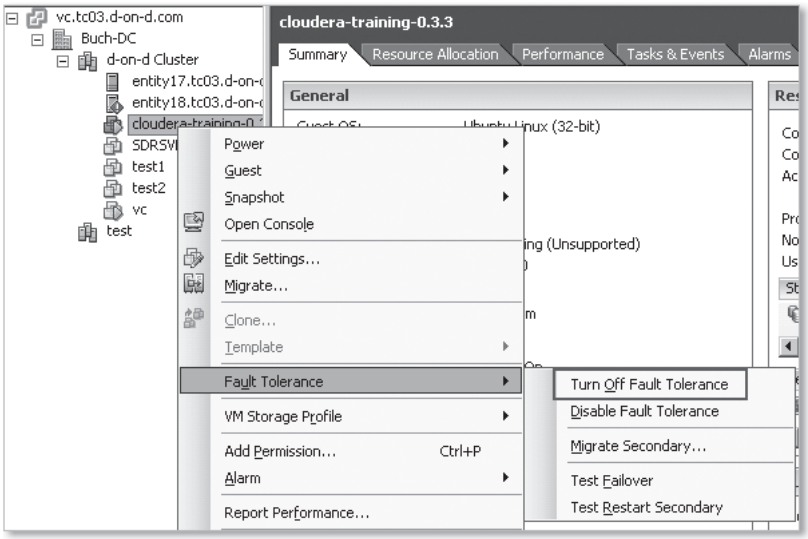


Abbildung 5.100 Kontextmenü bei aktivierter Fault Tolerance

5.5.5 Snapshots mit FT

Da mit FT geschützte VMs nicht gleichzeitig über Snapshots verfügen dürfen, ist eine Sicherung mit VCB (Consolidated Backup) oder anderen Sicherungsprogrammen außerhalb des Gastes nicht möglich. Um dies doch zu ermöglichen, ist es notwendig, FT temporär während der Aktivitäten mit Snapshot abzuschalten. Dies führen Sie idealerweise mit dem Menüeintrag Disable Fault Tolerance durch und aktivieren FT wieder, nachdem alle Snapshots gelöscht wurden.

Ein PowerShell-Beispiel zur Aktivierung und Deaktivierung von FT:

Aktivierung:

```
Get-VM VM1 | Get-View | % { $_.CreateSecondaryVM($null) }
```

Turn off:

```
Get-VM VM1 | Select -First 1 | Get-View | % { $_.TurnOffFault-ToleranceForVM() }
```

Disable FT:

```
Get-VM VM1 | Select -First 1 | Get-View | % { $_.DisableSecondary-VM(get-vm
  "secondary VM") }
```

Enable FT:

```
Get-VM VM1 | Select -First 1 | Get-View | % { $_.EnableSecondary-VM(get-vm
  "secondary VM") }
```

5.5.6 Was passiert im Fehlerfall?

Ausfall	Aktion
Teilausfall (z. B. Fibre-Channel-Ausfall – kein Zugriff auf den Storage) des primären Hosts	Fault Tolerance schaltet auf sekundäre VM um.
Komplettausfall primärer Host	Fault Tolerance schaltet auf sekundäre VM um.
Ausfall der Hosts, auf denen primärer und sekundärer Knoten laufen	vSphere HA startet den primären Knoten, und der sekundäre wird durch VMware FT gestartet.
Softwarefehler (Kernel-Panic, Bluescreen) auf primärem Knoten	VM Monitoring (VMHA) erkennt den Ausfall aufgrund des fehlenden VMware Tools Heartbeat und startet den primären Knoten neu. Der sekundäre Knoten wird mit dem primären durch FT neu gestartet.
Split-Brain-Situation, da primärer und sekundärer Knoten sich nicht mehr sehen (Netzwerkfehler)	Renaming (Umbenennen einer Datei im Shared Storage) wird von einer VM »gewonnen«, die andere schaltet sich selbst ab.
Primäre VM wird suspendiert	Sekundäre VM wird ausgeschaltet.
Reset der primären VM (*hard*)	Sekundäre VM wird beim Reset ausgeschaltet und beim Neustart des primären Knotens durch einen angepassten vMotion-Prozess erstellt.
Restart Guest der primären VM (*soft*)	Primäre und sekundäre VM führen einen Neustart ohne Abschaltung durch.

Tabelle 5.9 Was passiert im FT-Fehlerfall?

5.5.7 Lizenzierung von FT

VMwares Fault Tolerance ist Bestandteil der vSphere Suite, die auf CPU-Sockel-Basis lizenziert wird und ab der Edition Enterprise integriert ist.

Das folgende Kapitel beschäftigt sich mit der Installation der verschiedenen Softwarekomponenten von VMware vSphere 5.0. Hier erklären wir nicht nur die Standardinstallation, sondern auch Installationen in DAS- und SAN-Umgebungen.

6 Installation

Autor dieses Kapitels ist Bertram Wöhrmann, Ligarion, bwoehrmann@ligarion.de

Auch wenn die Installation der einzelnen VMware-Komponenten an sich nicht kompliziert und aufwendig ist, möchten wir doch auf die einzelnen Schritte genauer eingehen, damit Sie wissen, worauf Sie besonders achten müssen. Dabei beginnen wir mit der Version ESXi zunächst auf DAS-Systemen, und im Anschluss daran beschäftigen wir uns mit Installationen im SAN. Abschließend widmen wir uns dem vCenter-Server und seiner Komponenten.

6.1 VMware vSphere 5.0

Die Version VMware vSphere 5.0 ist der Vorgängerversion 4.x immer noch sehr ähnlich, die Service Console gehört der Vergangenheit an. Für alle Funktionen, die Sie dort abgebildet haben, müssen Sie nach Alternativen suchen.

6.1.1 VMware-vSphere-Systemvoraussetzungen

Die genauen Systemvoraussetzungen finden Sie in den Hardware Compatibility Guides auf der VMware-Website. Die Kompatibilitätslisten, d. h. die Auflistungen der von VMware unterstützten Hardware und Software, sind in mehrere Gruppen untergliedert: Systeme/Server, I/O-Komponenten, VMware View, Storage/SAN, Guest/Host OS, vSphere APIs for Storage Awareness, Site Recovery Manager, vCenter Orchestrator, CIM Provider und Hostprofile (Abbildung 6.1). Rufen Sie einfach die Seite *http://www.vmware.com/resources/compatibility/search.php* auf, und schon können Sie die Kompatibilität prüfen. Als Einstiegspunkt können Sie auch die VMware-Seite *http://www.vmware.com/resources/guides.html* nehmen.

Sollten Sie noch genug Papier im Drucker haben, können Sie auch die PDF-Variante der HCL ausdrucken. Diese beläuft sich auf 435 Seiten und ist unter folgender URL zu finden: *http://partnerweb.vmware.com/comp_guide/pdf/vi_systems_guide.pdf*. Alternativ speichern Sie die Datei ab, damit Sie sie jederzeit als Referenz Zugriff darauf haben.

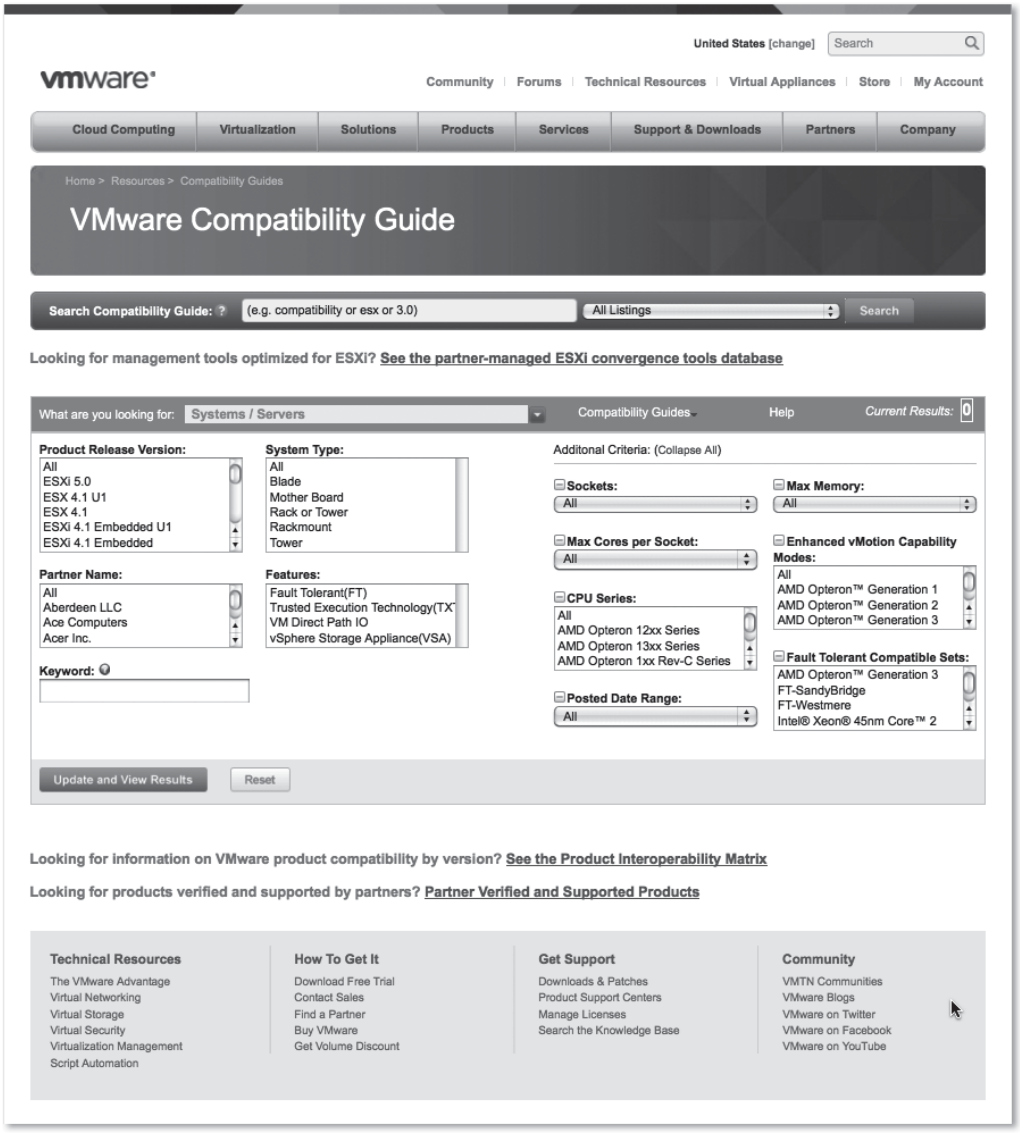


Abbildung 6.1 VMware-VI-Kompatibilitätsguides

VMware hat eine separate Website aufgebaut, um die Überprüfung der Kompatibilität von Komponenten zu ermöglichen. Hier können Sie nach einzelnen Systemen oder Systemkomponenten suchen. Wer länger nicht auf der Website gewesen ist, wird feststellen, dass VMware die Website angepasst hat. Aus unserer Sicht ist sie ein Stück übersichtlicher geworden. Dabei sind dort nicht nur die Hardware-, sondern auch die Softwarekompatibilitäten abgebildet.

Zu der offiziellen VMware-Kompatibilität gibt es auch eine Liste von Partner-Tools. Diese findet sich unter dieser URL: *http://www.vmware.com/resources/compatibility/vcl/esxi.php*.

Partner	Brocade				
Tools	**Tool**	**Version**	**Description**	**Compatible ESXi**	**Footnote**
	bcu	Version 3.0.0	CLI management tool for Brocade's storage adapters	ESX 4.x, ESXi 5.0	On ESXi 5.0 systems, BCU runs as an ESXCLI plug-in in the ESXi userworld environment.
KB article	http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2001842				

Partner	Hitachi				
Tools	**Tool**	**Version**	**Description**	**Compatible ESXi**	**Footnote**
	hfcmcup	--	Update or restore FLASH-ROM	ESX 4.x	Replaced by Hitachi CIM provider on ESXi 5.0.
	hfcmcup	--	Transfer FLASH-ROM data into hardware without OS reboot	ESX 4.x	Replaced by Hitachi CIM provider on ESXi 5.0.
	Hitachi CIM Provider	--	CIM provider with support for many standard CIM profiles	ESXi 5.0	See See Downloading CIM provider for Hitachi FC-HBA (KB 2001547).
KB article	http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2004169				

Partner	HP				
Tools	**Tool**	**Version**	**Description**	**Compatible ESXi**	**Footnote**
	HP CIM Providers	--	WBEM Providers for ProLiant Monitoring, Management and FW updating	ESXi 4.0, ESXi 4.1, ESXi 5.0*	* - HP provides versions of these components that are tested and compatible with the version of ESXi listed. A single version of these components does not support all of the listed versions of ESXi.
	HP NMI Driver	--	Driver to enable proper reporting of NMI events	ESXi 4.1, ESXi 5.0*	* - HP provides versions of these components that are tested and compatible with the version of ESXi listed. A single version of these components does not support all of the listed versions of ESXi.
	HP Utility Offline Bundle	--	Delivers the HP Boot Configuration utility and HP iLO Configuration utility for online configuration	ESXi 5.0	
	HP Insight Control for VMware vCenter	--	VMware vCenter plug-in that provides a high level of monitoring and management of HP ProLiant servers inside VMware vCenter	ESXi 4.0, ESXi 4.1, ESXi 5.0*	* - HP provides versions of these components that are tested and compatible with the version of ESXi listed. A single version of these components does not support all of the listed versions of ESXi.
	HP Custom ESXi Image	--	ESXi custom image with HP management tools and required drivers integrated with VMware's standard ESXi ISO	ESXi 5.0	* - HP provides versions of these components that are tested and compatible with the version of ESXi listed. A single version of these components does not support all of the listed versions of ESXi.
	HP ESXi 5.0 ImageProfile	--	ESXi 5.0 ImageProfile defining the components that HP includes in the custom image. It can be used by customers to create their own image or as a starting point for AutoDeploy support.	ESXi 5.0	
KB article	http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2004171				

Partner	LSI				
Tools	**Tool**	**Version**	**Description**	**Compatible ESXi**	**Footnote**
	MegaCLI	--	CLI for managing MR controllers	ESXi 5.0	
	MegaRAID Storage Manager	--	GUI application for managing MR controllers	ESXi 5.0	
	LSI SMI-S Provider	--	CIM provider for LSI MegaRAID, LSI SAS IR, LSI SAS IR2 and MegaSR	ESXi 4.x, ESXi 5.0	See LSI SMI-S CIM Provider Overview for ESXi 5.0 (KB 2001549).
KB article	http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2004166				

Partner	Network Appliance				
Tools	**Tool**	**Version**	**Description**	**Compatible ESXi**	**Footnote**
	mbralign	Available in the 'Tools' section of the OnCommand Plug-in for VMware 3.0 (formerly known as the Virtual Storage Console).	Guest partition block alignment	ESXi 4.x, ESXi 5.0	For ESX systems, customers should either download the ESX Host Utilities 5.2.1 (EHU 5.2.1) from NetApp's NOW site and use the mbralign provided in that bundle, or access the mbralign tool from the Virtual Storage Console 2.1 if deployed.
KB article	http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2004087				

Abbildung 6.2 Liste von Partner-Tools

6.1.2 Download der Installationsmedien

Die Installationsdateien von VMware vSphere 5.0 finden Sie auf der Website *www.vmware.com* unter dem Link »Support & Downloads • Product Downloads«. In dieser Sektion befinden sich die unterschiedlichen VMware-Produkte inklusive Versionsstände. Hier ist »Support & VMware vSphere • Download Licensed Copy« auszuwählen und danach die Version 5.0. Sollten Sie eine ältere Version suchen, finden Sie den passenden Link auf dieser Seite direkt über der Reitern des Produkt-Downloads der aktuellen Version.

Nach erfolgreicher Anmeldung befinden Sie sich auf der eigentlichen Download-Seite mit den Einzelkomponenten inklusive Download-Link (Abbildung 6.3).

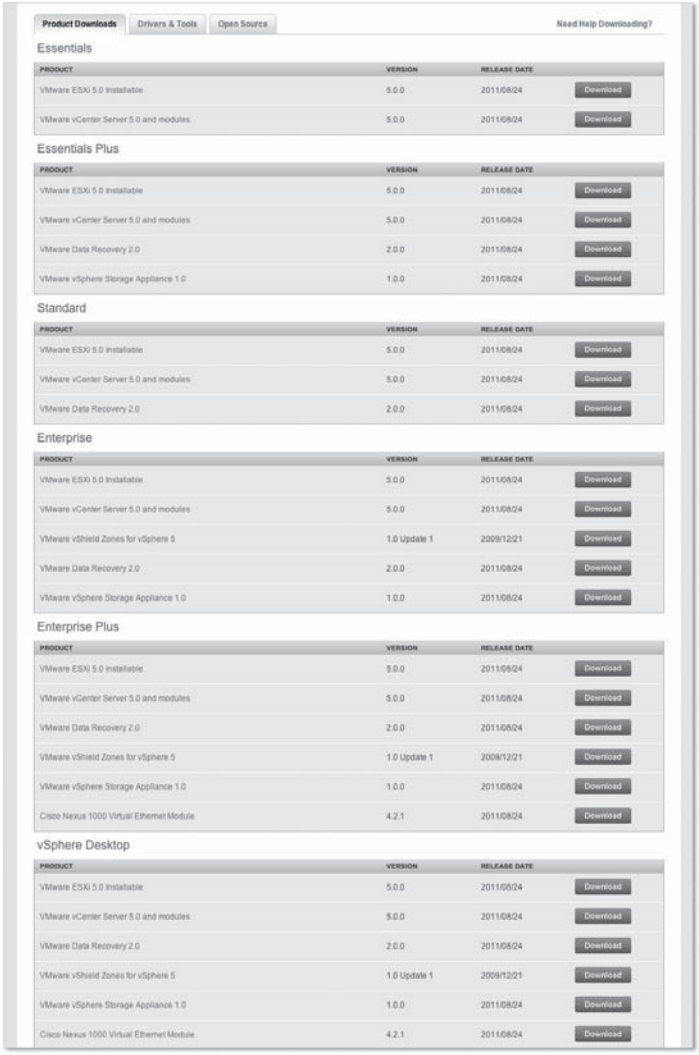


Abbildung 6.3 Download-Sektion Komponenten VMware vSphere 5.0

Auf der Webseite wählen Sie nun die Version aus, die Sie installieren wollen. Klicken Sie einfach auf den passenden Download-Link, und nach einer Anmeldung können Sie die Versionen herunterladen.

ESXi Version 5 ist in zwei verschiedenen Versionen erhältlich, zum einen als ISO-Image zur direkten Installation eines Servers oder alternativ als ZIP-Datei. Diese ZIP-Datei können Sie mit dem Update Manager nutzen, um vorhandene Hosts zu aktualisieren. Diese Version benötigen Sie auch, wenn Sie Auto-Deploy-Umgebungen für vSphere aufbauen wollen.

Generell sollten Sie jede heruntergeladene Datei auf die MD5-Checksumme hin prüfen (Abbildung 6.4), da es immer wieder zu Übertragungsfehlern kommt, die zu sehr unschönen Effekten wie einer fehlerhaften Installation führen. Unter jedem Download-Link finden Sie die Checksummen zum Überprüfen der Datei. Seit der neuen Version sehen Sie an dieser Stelle nicht nur eine MD5-, sondern auch eine SHA1-Checksumme.

Kostenfreie Programme zum MD5- oder SHA1-Checksummen-Test finden Sie mit Google wie Sand am Meer. Zwei recht empfehlenswerte MD5-Programme, die gerne genutzt werden, sind:

- Windows MD5 Checksum Tool
  http://ferruh.mavituna.com/md5-checksum/md5checksum-setup.exe
- winMD5Sum
  http://www.nullriver.com/index/products/winmd5sum

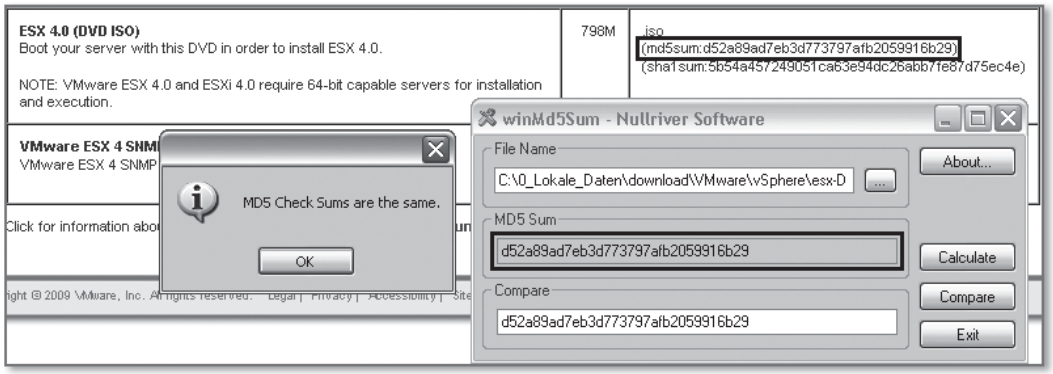


Abbildung 6.4 MD5-Checksummen-Vergleich mit winMD5Sum

Nach dem Test auf Integrität des Installationsmediums nutzen Sie das ISO-DVD-Image entweder auf eine DVD gebrannt oder über Softwareverteilungstools. DVD-Emulationsprogramme auf Server-Seite (z. B. HP iLO) können zur Anwendung kommen, um die Medien direkt zu nutzen. Alternativ besitzen Sie bereits eine Original-DVD von VMware, die auf dem aktuellsten Stand ist.

6.1.3 Vor der Installation

Vor der Installation sollten Sie unbedingt folgende Hinweise beachten.

Einrichten der Hardware

Bevor Sie beginnen, die Server aufzusetzen, müssen Sie die Hardware dafür konfigurieren. Die Hardwarehersteller haben Vorgaben, damit der vSphere-Server auch die volle Leistungsfähigkeit ausspielen kann. Dazu sind im BIOS einige Einstellungen vorzunehmen. Auf jeden Fall ist die Prozessorvirtualisierung zu aktivieren. Je nach CPU-Typ sehen die Empfehlungen von HP für ihre Server wie folgt aus:

AMD-CPU:

- Server Availability • ASR Status deaktivieren
- Advanced Options • Processor Options • AMD Virtualisation aktivieren
- Advanced Options • MPS table mode auf Full table APIC setzen
- Advanced Options • Processor Options • no-Execute Page-Protection aktivieren

Intel-CPU:

- Server Availability • ASR Status deaktivieren
- System Options • Processor Options • Intel® Virtualization Technology aktivieren
- Advanced Options • MPS table mode auf Full table APIC setzen
- System Options • Processor Options • no-execute memory protection aktivieren

Keine SAN-Verbindung

Außer bei Boot-from-SAN sollte der vSphere-Server während der Installation keine Verbindung zum SAN und zum zentralen Speicher haben. Dies ist empfohlene Praxis und dient zur eigenen Sicherheit, damit nicht ungewollt Formatierungen erfolgen.

Während der Installationsroutine werden bei der Partitionierung ausgewählte LUNs formatiert, unabhängig von den Daten! Die Auswahl einer falschen LUN ist leider viel zu schnell passiert!

Sie müssen allerdings nicht zwingend die FC- oder Ethernet-Kabel ziehen, ein Abschalten der Ports oder Aufheben der Zuordnung am Speichersystem genügt in den meisten Fällen.

6.1.4 Lokale Installation

Zur lokalen Installation müssen Sie entweder die VMware-vSphere-5.0-Installations-DVD im Server-System einlegen oder mittels Emulation (Virtual Media – HP iLO, Dell DRAC …) dem Server bekannt machen. Sehr wichtig ist hier die passende Kombination aus Firmware-, Java- und ActiveX-Version. Die entsprechenden Informationen sind Tabelle 6.1 zu entnehmen.

Remote-Controller	Firmware	Java-Version
DRAC 6	1.54 (Build 15), 1.70 (Build 21)	1.6.0_24
DRAC 5	1.0, 1.45, 1.51	1.6.0_20, 1.6.0_203
DRAC 4	1.75	1.6.0_23
ILO	1.81, 1.92	1.6.0_22, 1.6.0_23
ILO2	1.8, 1.81	1.6.0_20, 1.6.0_23
IBM RSA 2	1.03, 1.2	1.6.0_22

Tabelle 6.1 Remote-Controller-Firmware-Versionen

Alternativ ist es auch möglich, den Host über ein USB-Medium bereitzustellen. Während der Installation erfolgen fast keine Angaben; die eigentliche Konfiguration erfolgt nach dem Abschluss der Installation in der Managementkonsole des ESXi. An dieser Stelle können Sie auch den zu nutzenden Netzwerkadapter anpassen.

Als zusätzliche Voraussetzung muss die Uhr im BIOS auf UTC-Zeit gesetzt werden. Die Anpassung an die entsprechende Zeitzone erfolgt nach der Installationsprozedur mit dem vSphere-Client.

PCI-ID-Plan

Sollte der Server über sehr viele Netzwerkkarten verfügen, ist ein PCI-ID-Plan des Server-Systems (PCI-ID = PCI-Nummer von Geräten in PCI-Slots) sehr hilfreich. Es wird nach einer Netzwerkkarte als Uplink für den virtuellen Switch gefragt, der zur Nutzung durch die Service-Console-Portgruppe dient.

Vorbereitung USB-Medium

Soll die Installation über ein USB-Medium z. B. einem USB-Stick erfolgen, dann sind einige vorbereitende Arbeiten notwendig. Als Erstes benötigen Sie ein Tool, mit dem Sie einen USB-Stick bootfähig machen können. Sie können sich für diesen Zweck des Tools UNetbootin bedienen. Diese Software gibt es für alle gängigen Plattformen. Somit sind Sie vom Betriebssystem selbst unabhängig. Jetzt müssen Sie entweder in der oberen Auswahl eine DISTRIBUTION wählen, um den passenden USB-Stick zu erstellen, oder Sie wählen den unteren Auswahlpunkt aus und binden direkt das ISO ein.

Es folgt die Auswahl des USB-Mediums, auf das die vSphere-CD kopiert werden soll. Ist der Prozess abgeschlossen, dann können Sie mit USB-Stick einen Server booten und dann installieren.

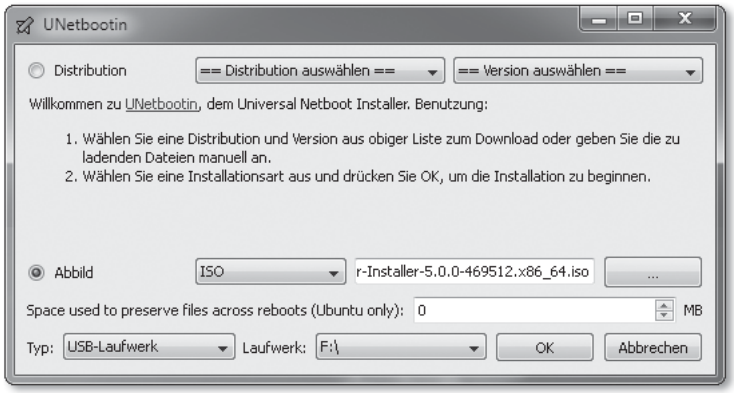


Abbildung 6.5 Erstellen eines bootfähigen USB-Mediums

Installation

Die Installation von vSphere 5i ist absolut simpel und erfordert keinerlei Linux-Kenntnisse. Sie benötigen lediglich zertifizierte und von VMware freigegebene Hardware. Für Testumgebungen können Sie sich auch in der Community umschauen, auf welchen Systemen die Software noch erfolgreich installiert werden konnte.

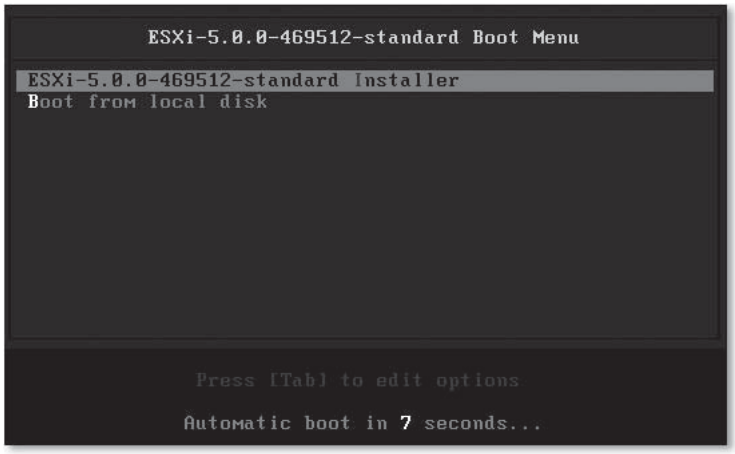


Abbildung 6.6 vSphere5i Installer

Nach Starten des ISO-Images oder der DVD wird direkt das Bootmenü mit dem Installer angezeigt (Abbildung 6.6). Mit der F2-Taste könnten Sie die Bootparameter ändern, zur Drucklegung des Buches war uns jedoch noch keine sinnvolle Nutzungsmöglichkeit bekannt. Wie der zweite Menüpunkt schon besagt, können Sie die Installation umgehen, und das System bootet von der Festplatte. Zu Beginn lädt das System nun verschiedene Treiber. Anschließend zeigt sich der Screen aus Abbildung 6.7.

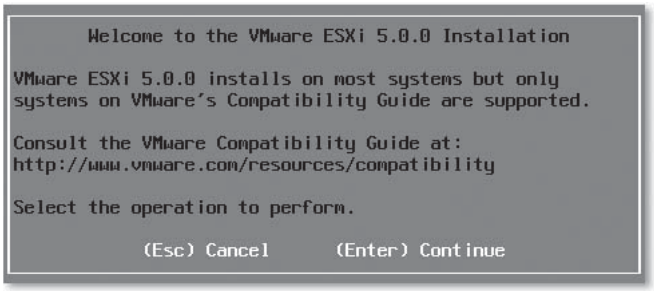


Abbildung 6.7 Abbildung 6.7:Hinweis auf die HCL von VMware

Nachdem Sie mit der Installationsroutine fortgefahren sind, kommt das EULA (Enduser License Agreement). Dieses ist zu bestätigen, und es folgt die Auswahl der Installationspartition.

Die Installationsroutine des vSphere 5i-Servers stellt keine Partitionierungsmöglichkeiten zur Verfügung, stattdessen wird die angegebene Festplatte komplett genutzt (Abbildung 6.8). Mit der Auswahl von F1 können Sie sich aber noch die Eigenschaften der markierten Festplatte anzeigen lassen.

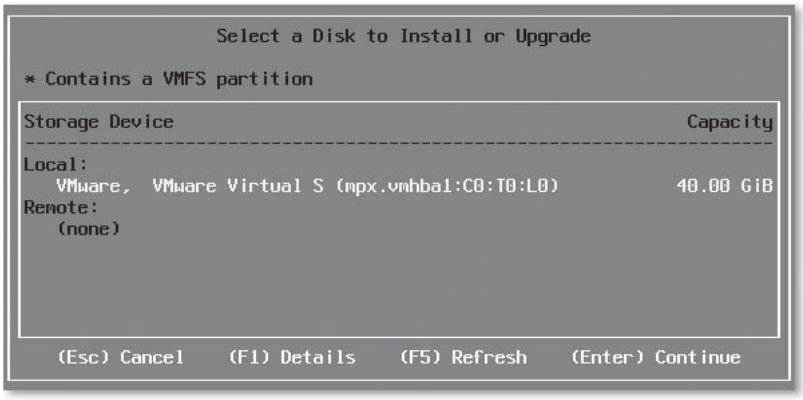


Abbildung 6.8 Auswahl der Zielfestplatte

An dieser Stelle finden Sie alle Angaben, die Sie für die Beurteilung der Festplatte benötigen. Zusätzlich erhalten Sie den Hinweis, ob die Installationsroutine eine vorhandene ESX(i)-Installation gefunden hat.

Tipp

Möchten Sie eine universale Installation auf einem USB-Stick haben, dann können Sie ein USB-Medium einsetzen. Nach dem Drücken von F5 wird der Stick angezeigt, und Sie können eine Installation direkt auf dem USB-Gerät vornehmen. Mit diesem Stick können Sie dann jeden unterstützten Host starten.

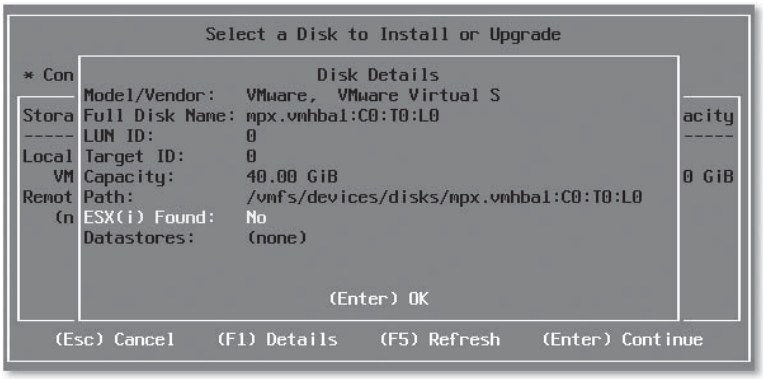


Abbildung 6.9 Eigenschaften der ausgewählten Festplatte

Nach der Auswahl und der Bestätigung der Festplatte wird Ihnen, falls bereits ein VMware-System auf der Festplatte installiert war, die Abfrage aus Abbildung 6.10 gezeigt.

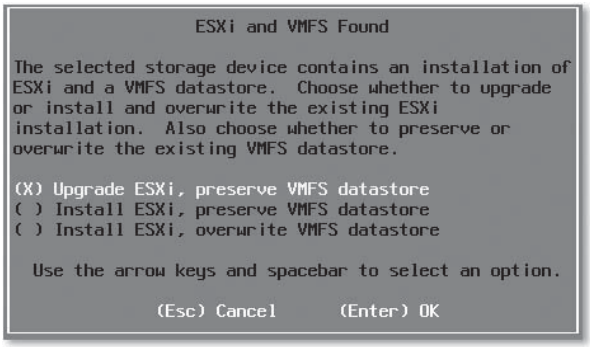


Abbildung 6.10 Upgradeoptionsauswahl bei gefundener Installation

Eine Reparatur wie in früheren Versionen gibt es an dieser Stelle nicht mehr. Wählen Sie einfach ihre gewünschte Aktion, und Sie können die Arbeiten entsprechend fortsetzen. Hier wird auch auf diejenigen Rücksicht genommen, die Single-Host-Umgebungen haben. Die VMFS-Datastores können behalten werden, ohne dass die darauf liegenden VMFS-Partitionen beeinträchtigt werden. Wählen Sie nun Ihr bevorzugtes Tastaturlayout aus, und fahren Sie mit der Installation fort.

Im Gegensatz zu den Vorgängerversionen wird im folgenden Dialog bereits das Passwort für den »root«-User vergeben. Es ist in der Version also nicht möglich, die Installation ohne die Vergabe eines Passworts durchzuführen.

Eine kurze Zusammenfassung bestätigt, dass eine Installation erfolgt und auf welcher Festplatte diese erfolgt. Nun kommt die Pause für ein Heißgetränk, während der Balken den Fortschritt der Installation anzeigt. Nach ca. 5 Minuten sind alle Arbeiten abgeschlossen. Ist die Installation erfolgreich durchgelaufen, dann weist die Installationsroutine Sie darauf hin.

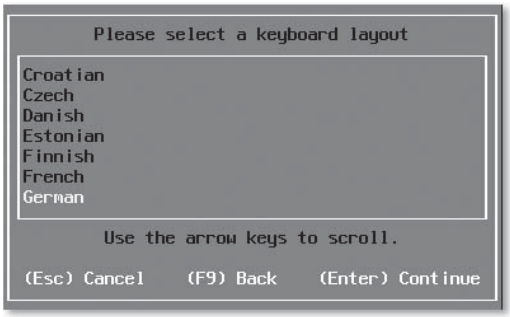


Abbildung 6.11 Auswahl des Tastaturlayouts

Abbildung 6.12 Festlegen des Passworts

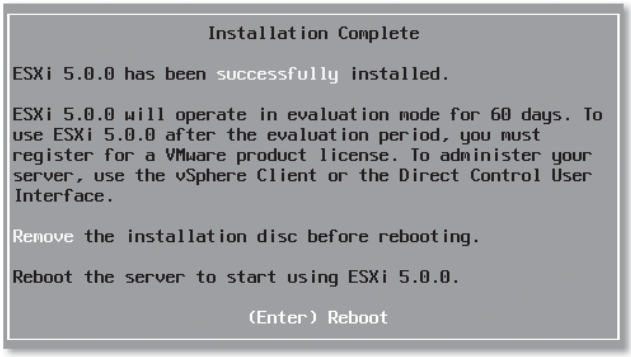


Abbildung 6.13 Installationsabschluss

Nach dem Entnehmen des Installationsmediums und dem erfolgreichen Reboot des Systems heißt Sie der neu bereitgestellte Server willkommen, und Sie können mit den weitergehenden Konfigurationsarbeiten beginnen.

Sie können selbstverständlich die Installation auch auf einem USB-Stick oder einer SD-Karte vornehmen. Es gibt Server, die passende Steckplätze im Gerät zur Verfügung stellen; denken Sie aber daran, dass Sie dann einen Single Point of Failure haben. Über solche Geräte lässt sich kein RAID spannen, und somit sollten Sie genau überlegen, ob Sie mit dieser Technologie arbeiten oder doch besser bei der klassischen Festplattenvariante im RAID-Verbund bleiben.

6.1.5 Erststart vSphere 5i

Sobald der vSphere 5i-Server komplett gestartet ist, befinden Sie sich in einem rudimentären Startmenü, das über die Tastatur zu bedienen ist (Abbildung 6.14). Da der vSphere 5i-Server laut Standardeinstellungen eine IP-Adresse per DHCP bezieht, kann bei vorhandenem DHCP-Server im Netzwerk auch direkt über den Virtual Infrastructure Client auf den neu installierten Host zugegriffen werden.

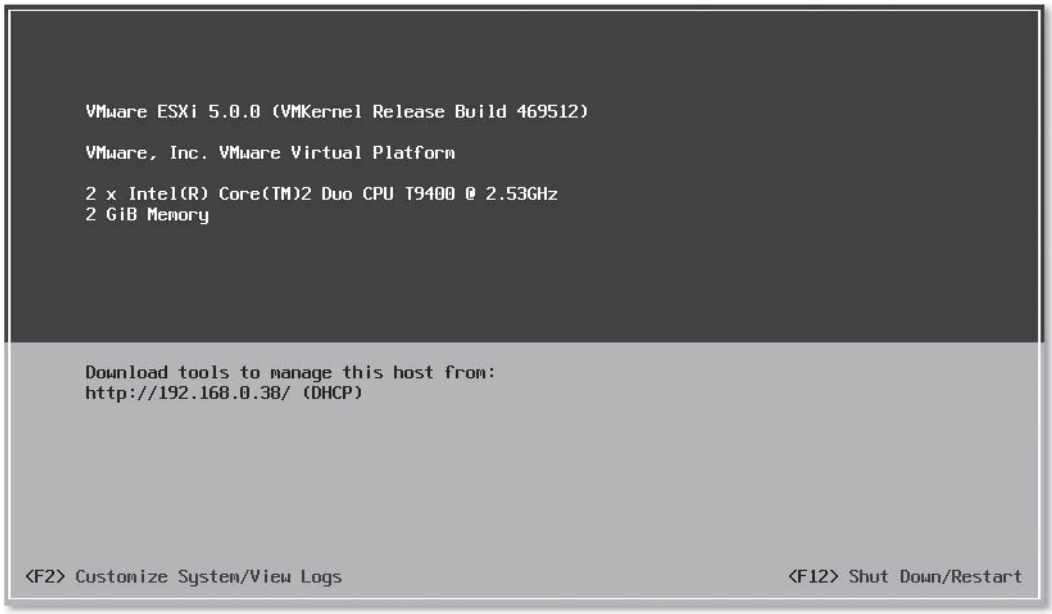


Abbildung 6.14 Erststart des vSphere 5i-Systems

Daher bietet sich die Taste F2 an, mit der Sie das Netzwerk konfigurieren können. Zuvor müssen Sie sich aber an dem System authentifizieren, im Gegensatz zu zu der Vorversion, wo das Passwort erst bei der erstmaligen Einrichtung konfiguriert wurde. Sehr gut ist die zusätzliche Anzeige im Anmeldedialog, die das eingestellte Tastaturlayout angibt. Damit entfallen Anmeldefehlversuche, weil das Layout nicht bekannt ist.

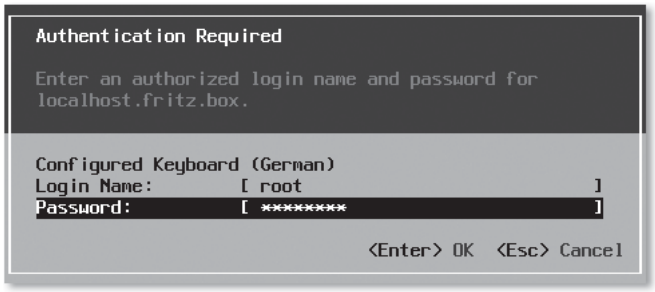


Abbildung 6.15 Server-Anmeldung mit der Anzeige des Tastaturlayouts

Nach der Anmeldung gelangen Sie in ein rudimentäres Konfigurationsmenü. Hier können Sie die Basiseinstellungen des ESXi-Hosts vorgeben. Auf nähere Details zur Konfiguration gehen wir in Kapitel 13 ein.

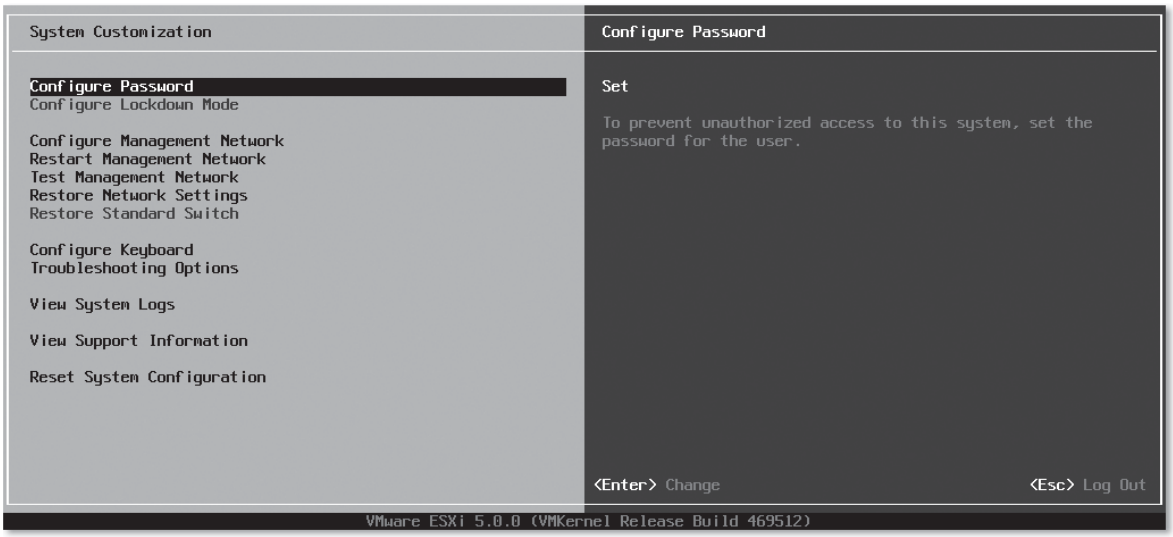


Abbildung 6.16 Konfigurationsseite des vSphere 5i-Systems

6.1.6 vSphere CLI

Mit dem Weggang von der Service Console musste sich die VMware-Entwicklungsabteilung Gedanken um einen entsprechenden Ersatz machen, da viele Hersteller und Anwender diese Console häufig für Skripte und Konfigurationen nutzten. Aus diesem Grund entstand das vSphere CLI (Command-Line Interface), das im Endeffekt eine Kombination aus Perl-Wrapper und Perl-Skripten ist. Diese Skripte nutzen die VI-API auf einfachem Weg über das Netzwerk und kommunizieren so mit vSphere-Server und vCenter-API.

Möchten Sie diese Funktionen verwenden, dann haben Sie grundsätzlich zwei Möglichkeiten, die Software herunterzuladen. Die Download-Sektion bei VMware stellt die entsprechenden Dateien zur Verfügung, und zwar unter: *http://communities.vmware.com/community/developer/vsphere_cli.*

Zumindest den vSphere-Client können Sie direkt vom ESXi 5i-Host herunterladen (Abbildung 6.17). Über den Webbrowser verbinden Sie sich mit der URL des ESXi 5i-Servers: *http://<IP-Adresse ESXi5i>.* Alle anderen Links, bis auf Browse Datastore of this host, leiten Sie direkt auf die VMware-Website.

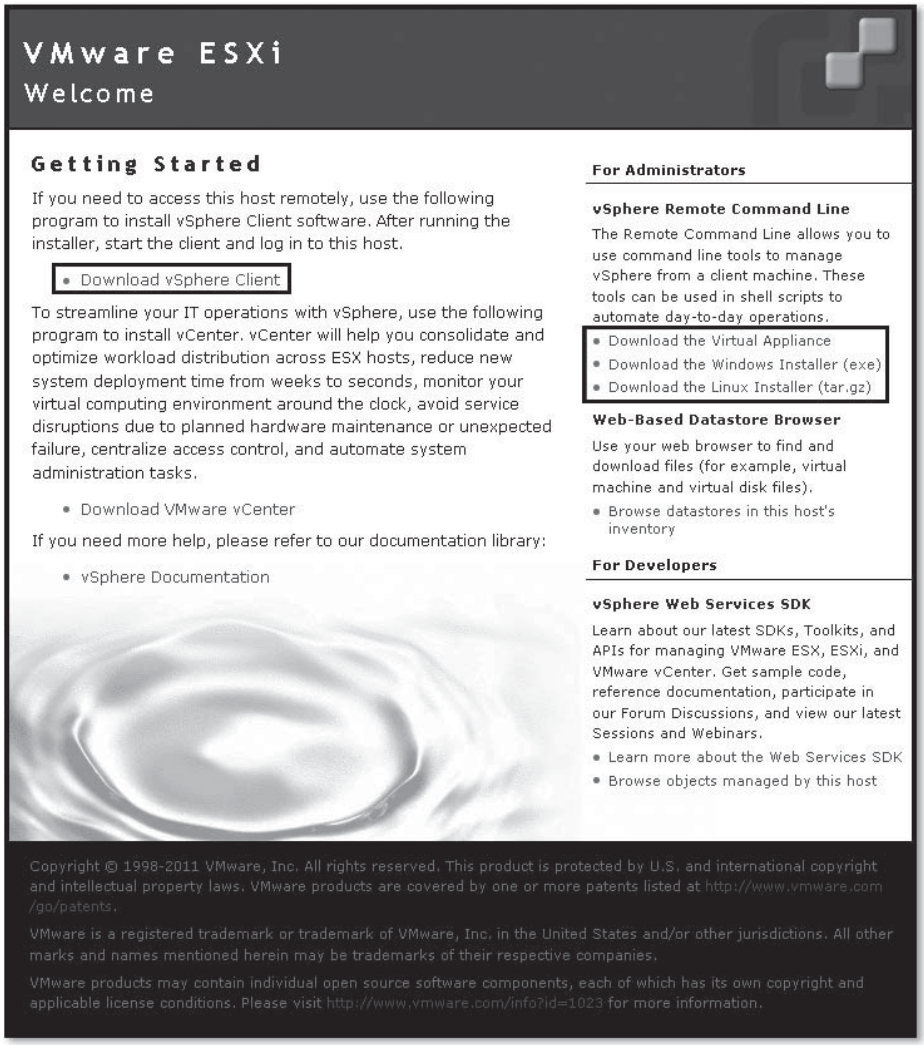


Abbildung 6.17 Zugriff auf ESXi via Webbrowser

Installation unter Linux

Kopieren Sie zuerst die Datei *VMware-vSphere-CLI-5.0.0-xxxxx.xxxx.tar.gz* auf das gewünschte Linux-System, und führen Sie sie mit `tar xzvf VMware-vSphere-CLI-5.0.0-xxxxx.xxxx.tar.gz` aus.

Es wird dadurch ein Verzeichnis *vmware-vsphere-cli-distrib* erstellt, in das alle Dateien entpackt werden. Die Installation starten Sie z. B. mit */tmp/vmware-vsphere-cli-distrib/vmware-install.pl*, wodurch alle Dateien laut Standardeinstellungen in */usr/bin* kopiert werden. Eine Deinstallation führen Sie mit */usr/bin/vmware-uninstall-vSphere-CLI* durch. Jetzt finden Sie einen Großteil der Befehle, die Sie von der ehemaligen Service Console her kennen.

Installation unter Windows

Das vSphere CLI kommt als normale Setup-Routine für Windows daher (*VMware-vSphere-CLI-5.0.0-xxxxxx.exe*) und läuft nach dem Start komplett selbständig durch; sollte bereits eine ältere Version installiert sein, wird diese vorher deinstalliert. Nach der Fertigstellung befindet sich eine ActivePerl-Installation im Verzeichnis *C:\Programme\VMware\VMware vSphere CLI* (oder *C:\Program files\VMware\VMware vSphere CLI*). Die Perl-Skripte finden Sie ebenfalls hier.

Virtual Appliance

Eine weitere Alternative ist der Import der Management-Appliance von VMware, die alle benötigten Remote-CLI-Komponenten samt Gastbetriebssystem enthält (Abbildung 6.18). Die Virtual Appliance laden Sie entweder manuell als OVF (Open Virtual Machine Format) herunter, oder Sie importieren sie mit dem OVF-Tool.

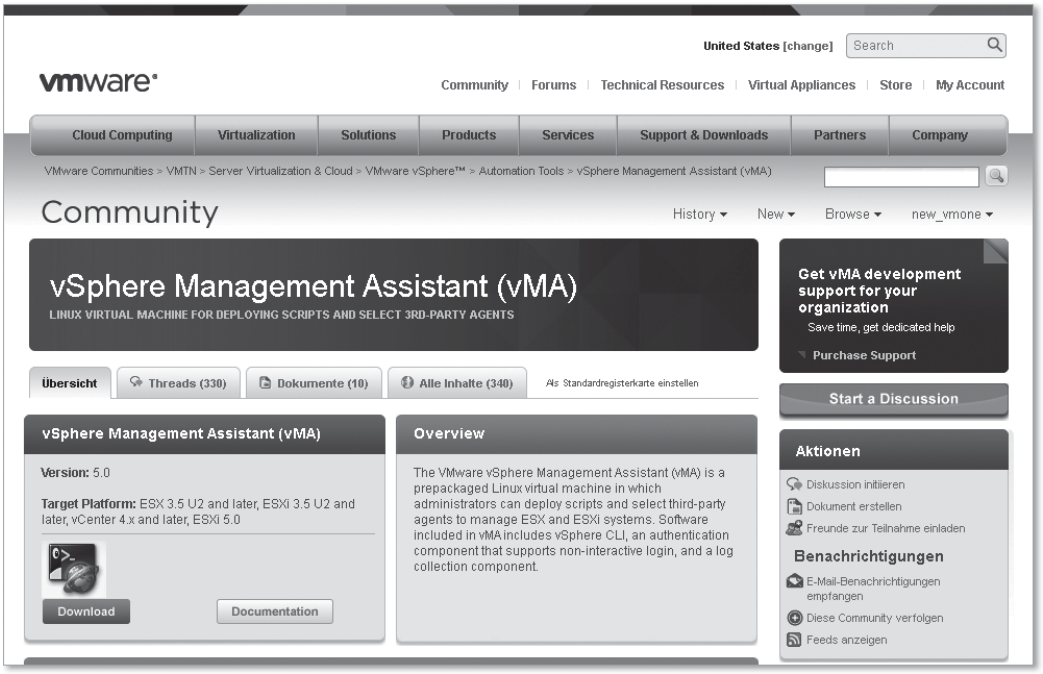


Abbildung 6.18 Download der vSphere-CLI-Appliance

Auf der Webseite von VMware unter *http://communities.vmware.com/community/vmtn/server/vsphere/automationtools/vima* lässt sich die Appliance herunterladen und anschließend im vSphere-Client importieren.

Wird die Appliance zum ersten Mal gestartet, sind einige Eingaben zu tätigen, um das System zu nutzen. Es werden der Name der Maschine abgefragt, die Netzwerkparameter und das Passwort des administrativen Users »vi-admin«. Mit dem »root«-User können Sie sich nicht

direkt an der Konsole anmelden. Sie müssen mit dem Kommando `sudo` arbeiten, um im »root«-Kontext Befehle abzusetzen. Zusätzlich wird automatisch ein Read-only-Account eingerichtet. Dieser Account »vi-user« hat standardmäßig kein Passwort. Vor der Vergabe eines Kennworts ist dieser Account nicht nutzbar.

Ist die Datei heruntergeladen, entpacken Sie sie. Den Import der Appliance stoßen Sie über den vSphere-Client an (Abbildung 6.19).

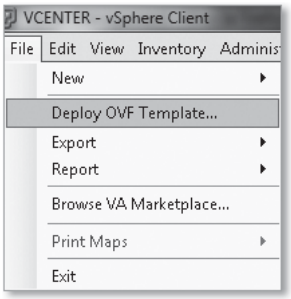


Abbildung 6.19 Importmenü Virtual Appliance

Über den folgenden Dialog importieren Sie über das File-System die Appliance (Abbildung 6.20).

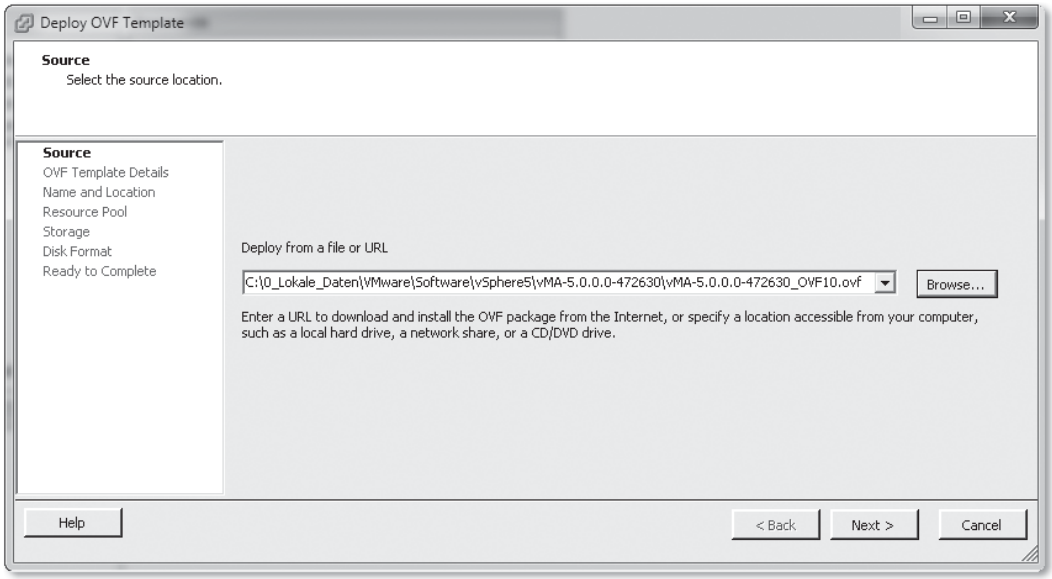


Abbildung 6.20 Appliance-Import

Bevor der Import anläuft, werden Ihnen noch alle Parameter angezeigt, und Sie müssen noch den einen oder anderen Parameter angeben.

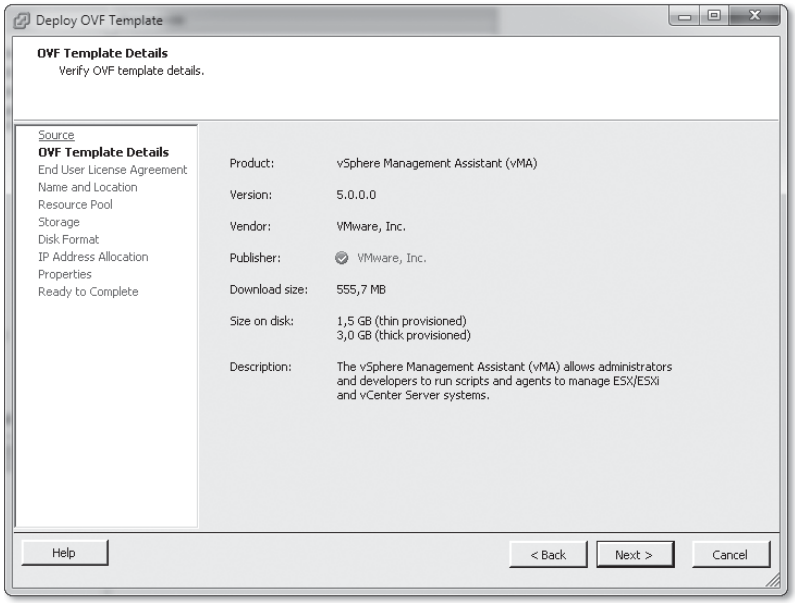


Abbildung 6.21 vSphere Management Assistant-Parameter

Achten Sie bitte auf die Anzeige im Konfigurationsfenster der IP-Adress-Allokation. Hier legen Sie das Verhalten der VM fest, was die Versorgung mit IP-Adressen angeht. Bei Auswahl des ersten Punktes müssen Sie die IP-Adresse per Hand konfigurieren. Der mittlere Punkt versorgt den vMA mit einer Adresse aus einem IP-Pool.

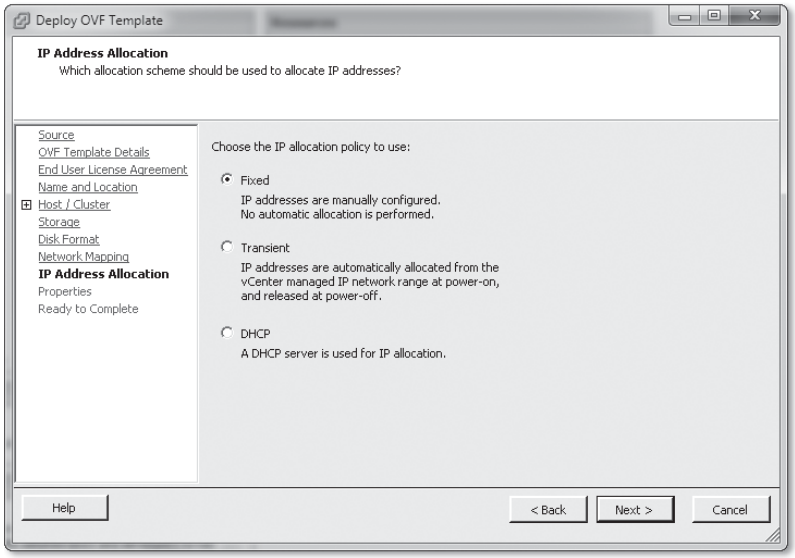


Abbildung 6.22 Festlegung der IP-Adress-Versorgung

Die letzte Auswahl versorgt den vMA automatisch mit einer IP über einen vorhandenen DHCP-Server. Sollten Sie keine IP-Pools im Datacenter eingerichtet haben, dann erscheint eine Fehlermeldung. Existiert der Pool, nimmt sich die Appliance die konfigurierte IP-Adresse aus dem angegebenen Pool.

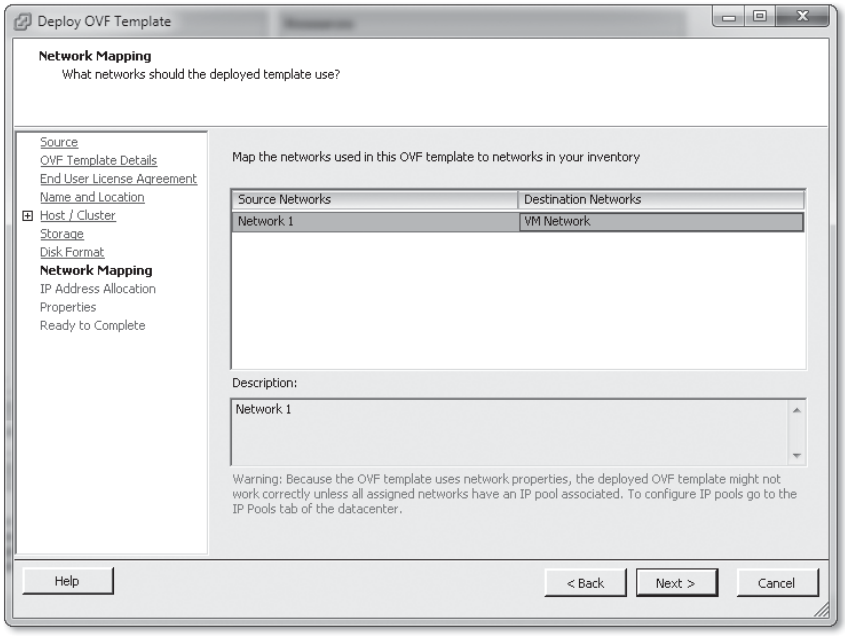


Abbildung 6.23 Fehlermeldung bei fehlendem IP-Pool

Die Appliance kann trotz alledem importiert werden, aber sie wird nicht starten, wenn Sie den Befehl dazu geben und die angegebene IP-Adresse nicht eingepflegt haben. Diese Konfiguration muss dann händisch durchgeführt werden, wenn die Appliance gestartet worden ist. Auch hier erscheint wieder eine Fehlermeldung.

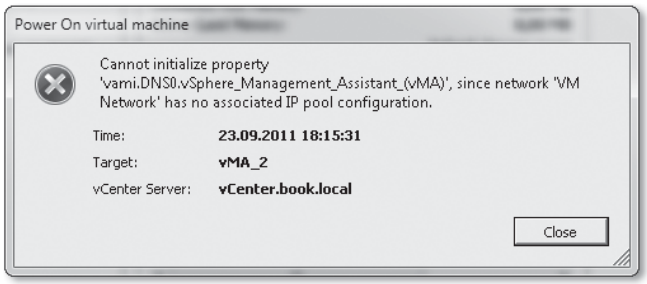


Abbildung 6.24 Fehler beim Starten des vMA

Sie haben jetzt zwei Möglichkeiten: Entweder legen Sie im IP-Pool Adressen an, oder Sie passen die Konfiguration des vMA an. Schauen Sie einfach in Abschnitt 13.6 vorbei, dort beschrei-

ben wir die Konfigurationsarbeiten. Ist der Import erfolgreich abgeschlossen, können Sie die virtuelle Maschine zur Administration von einzelnen ESXi-Hosts oder auch größeren Landschaften nutzen.

6.1.7 PowerCLI

Das PowerCLI ist eine nicht mehr so ganz neue Schnittstelle von VMware, die aber einen enormen Umfang hat und die mit jedem neuen Release immer weiter ausgebaut und immer wichtiger wird. Diese Softwarekomponente ist auf dem System zu installieren, von dem aus sie genutzt werden soll. Es ist also keine Komponenten ähnlich dem Update Manager, wo die Client-Komponente über den vSphere-Client heruntergeladen wird. Dieses Softwaretool läuft nur unter Windows! Die Installation setzt diverse Softwarekomponenten voraus.

Voraussetzungen

Die folgenden Softwarepakete müssen bereits installiert sein, damit die Installation funktioniert:

- .NET 2.0 SP1
- PowerShell 1.0 / 2.0
- Betriebssystemsupport für 32 Bit und 64 Bit ab Windows XP SP2
- VMware-Umgebungen ab ESX 3.0.3 Update 1 und ab vCenter 2.5 Update 6

Für die Installation laden Sie zuerst das Softwarepaket von der VMware-Website. Sie finden es unter der URL:

http://communities.vmware.com/community/vmtn/server/vsphere/automationtools/powercli

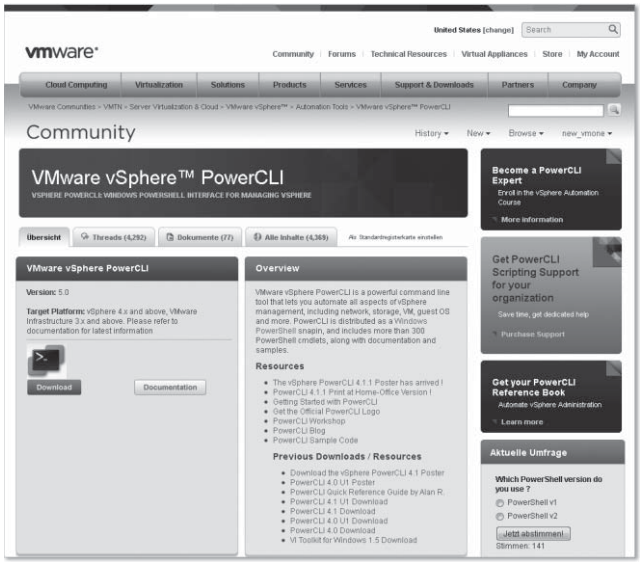


Abbildung 6.25 Download des PowerCLI

Hier finden Sie neben dem Download auch Beispiele und natürlich die notwendige Dokumentation zum PowerCLI. Nach dem Aufruf der EXE-Datei findet eine Überprüfung statt; sollten Sie eine Vorgängerversion installiert haben, werden Sie mit einer Meldung begrüßt.

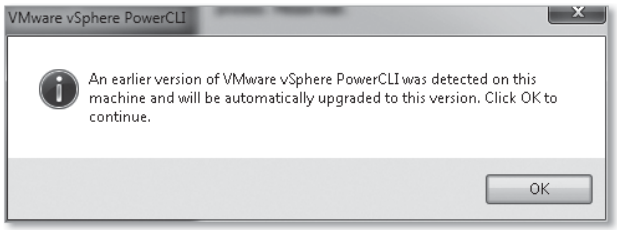


Abbildung 6.26 Installationshinweis PowerCLI

Besondere Einstellungen können Sie während der Installation nicht vornehmen. Sie müssen nur das EULA bestätigen und können bei Bedarf den Installationspfad ändern.

Damit Sie Skripte remote ausführen können, ist es erforderlich, eine Umgebungsvariable in der Shell zu setzen. Der Befehl `Set-ExecutionPolicy RemoteSigned` bringt den gewünschten Erfolg.

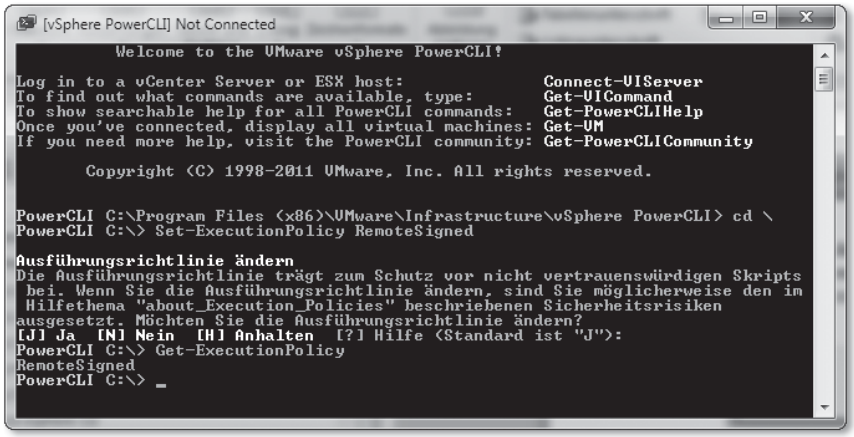


Abbildung 6.27 Setzten der Ausführungsrichtlinie

Nun können Sie in die Weiten des PowerCLI eintauchen und Ihre Infrastruktur damit administrieren.

6.1.8 Installation über das Netzwerk

Sie können den vSphere-Server auch über das Netzwerk installieren. Um diese Möglichkeit zu nutzen, benötigen Sie ein Preboot Execution Environment (PXE). Diese Umgebung besteht aus einem DHCP-(Dynamic Host Configuration Protocol-)Server, einem TFTP-(Trivial File Transfer Protocol-)Server und einem Boot-Environment.

Bootet ein Server via PXE, wird ihm eine gültige IP-Adresse zugewiesen; über den TFTP wird das Bootmenü auf den Host transferiert. Ist der Transfervorgang abgeschlossen, wird der Kernel geladen und eine RAM-Disk angelegt. Wählen Sie das Installationsskript, und sprechen Sie das Installationsmedium über das Netzwerk an. Ja, das ist neu, mit der Einführung der Version 5 des VMware ESX-Servers können Sie auch den ESXi Server geskriptet installiert werden. Die Installation kann, wie beschrieben, automatisch mit einem Skript laufen, oder Sie führen sie manuell durch. Die Vorgehensweise ist weitestgehend so, wie wir es bereits im vorhergehenden Abschnitt beschrieben haben.

Es gibt auch verschiedene Installationstools, die Ihnen ermöglichen, eine Konfiguration individuell einzurichten und automatisiert zu starten, so z. B. das Rapid Deployment Pack von HP, der Softservice Installer der Firma Softservice, die ESXi Deployment Appliance (EDA) oder, Sie haben es ja unter Umständen mitgekauft, das VMware Auto Deploy.

6.1.9 Installation im SAN

Ein sehr wichtiger Arbeitsschritt vor jeglicher Nutzung von Server-Systemen im SAN ist die Überprüfung des HBA-Controllers auf Firmware- und gegebenenfalls BIOS-Aktualität hin.

Bei der Vorgängerversion war das ganze Prozedere noch recht einfach: Die nötige Software konnte man in der Service Console installieren, und schon hatte man die nötigen Funktionalitäten. Bei vSphere 5 ist das nicht mehr möglich. Für ein Firmwareupdate des Adapters müssen Sie mit einem bootfähigen Medium den Server starten und über diesen Weg die Firmware aktualisieren.

Einschränkungen

Leider bietet eine Systeminstallation im Speichernetzwerk nicht nur Vorteile, sondern auch Einschränkungen. Allerdings werden die Einschränkungen mit jeder VMware ESXi-Version immer geringer.

Konnte man unter VMware ESXi 2.x keine Raw Device Mappings (RDM), also »Direktverbindungen« der VM zu einer LUN, in Verbindung mit SAN-Boot nutzen, ist dies seit der Version 3 kein Problem mehr. Das Gleiche gilt für die LUN-Nummerierung. Mittlerweile kann von jeder LUN-Nummer unterhalb 128 gebootet werden.

Auch die Einschränkung, dass immer nur von der niedrigsten LUN-ID gestartet werden kann, ist entfallen (bei LUNs 5, 6, 7 konnte nur von 5 gebootet werden). Allerdings sollten Sie im Interesse der Übersichtlichkeit und Verwaltung darauf verzichten, Boot-on-SAN-LUNs bunt zu nummerieren.

Soll aus dem SAN gebootet werden, müssen Sie weiterhin darauf achten, dass der vSphere-Server während der Installationsphase nur die ersten 128 LUNs erkennen kann (nach der Installation sind es insgesamt 256 LUNs).

Aus Hardwaresicht bestehen derzeit noch Probleme bei manchen Systemen mit internen IDE-Festplatten (z. B. IBM-Blades), die im BIOS deaktiviert werden müssen. Aus Performancegründen bietet es sich außerdem an, den HBA, von dem gebootet wird, möglichst hoch am PCI-Bus (PCI-ID) anzusiedeln.

Boot-on-SAN

Die Möglichkeit der Installation und des Starts des vSphere-Servers im bzw. aus dem SAN wurde hauptsächlich durch die Verbreitung von Blade-Servern forciert, da diese oft über keine lokalen Festplatten verfügen. Neben der Nutzung plattenloser Systeme bietet die Boot-on-SAN-Alternative einen weiteren Vorteil in Bezug auf Ausfallsicherheit: Blade-Server sind in vielen Fällen modellgleich, das heißt, es ist die gleiche Hardwaregrundlage vorhanden. Fällt ein Blade aus, können Sie durch einfaches Umsetzen der Boot-LUN im SAN ein anderes Blade mit identischer Konfiguration neu starten. Dadurch wird die Neuinstallation und Konfiguration bei Hardwareausfällen nichtig. Auch Replikationen oder Spiegelung und Sicherung der Systempartition sind somit sehr einfach, da alles im SAN passieren kann.

Eine Installation bzw. der Start des vSphere-Servers von zentralem (oder nicht-lokalem) Speicherplatz setzt einen bootfähigen und zertifizierten Fibre-Channel- oder iSCSI-HBA (Host-Bus-Adapter) voraus.

Allerdings sollten Sie im Idealfall die LUN-ID 0 für die Bootfestplattenzuordnung wählen. Wählen Sie eine andere Boot-LUN-ID, sollten Sie sich diesen Bereich gut merken, um später keine versehentlichen Formatierungen durchzuführen.

Zugriff beim Mapping der LUN

Beim Mapping der LUN (Zuordnung Host WWN/iSCSI Name <-> Storage LUN in der Speicherverwaltung) sollten Sie nur dem einen Host den Zugriff gestatten, der auch von der LUN bootet!

Nach entsprechender LUN-Anlage und dem Mapping können Sie den vSphere-Server mit der VMware-vSphere-Installations-DVD starten. Bei der Auswahl von Bootloader und zu partitionierender Festplatte müssen Sie die entsprechende LUN auswählen (im Idealfall LUN 0).

Fibre-Channel-HBAs und Boot-on-SAN

Bereits vor der Anpassung der Fibre-Channel-HBAs (Firmware-Update, Bootkonfiguration) kann die Installation stattfinden. Allerdings ist dies Geschmackssache. Der große Unterschied zwischen dem lokalen Boot und dem SAN-Boot besteht aus Sicht der Installationsroutine nur in der zugeordneten System- und Installationspartition. Daher muss der HBA die LUNs bereits vor dem Boot der vSphere-DVD sehen. Bei der Plattenauswahl wird die LUN dann angewählt.

Nach erfolgter Installation müssen Sie den Server allerdings vom lokalen Boot auf den Boot mittels HBA umkonfigurieren, was wir in den folgenden Zeilen beschreiben. Bevor Sie über die Einrichtung von Boot-on-SAN nachdenken, sollten Sie auf jeden Fall kontrollieren, ob die

aktuelle Firmware auf dem Host-Bus-Adapter eingespielt ist. Falls nicht, sollten Sie dies zuerst nachholen. Außerdem bieten die Hersteller Anleitungen an, wie der HBA als Boot eingerichtet wird.

6.1.10 Installation in der virtuellen Maschine

Mit Version 7 der VMware Workstation und einem VT-fähigen (Virtualization Technology) Prozessor wird kein manueller Eingriff in der Konfigurationsdatei mehr benötigt, um einen VMware-vSphere-Server in der virtuellen Maschine zu betreiben. Dies ist nicht besonders schnell, bietet jedoch viele Vorteile in Test- und Entwicklungsszenarien. Außerdem half diese Möglichkeit sehr, dieses Buch zu erstellen, da viele Tests und Versuche ansonsten viel zu aufwendig geworden wären. Auch wenn es als Betriebssystemkonfiguration der VMware Workstation den Punkt ESX Server 5 noch nicht gibt, so können Sie die Version vSphere 5 ohne Probleme mit dem Punkt ESX Server 4 installieren.

6.2 Upgrade auf vSphere 5.x

Möchten Sie eine bereits bestehende Landschaft auf die neue VMware-Version updaten, müssen Sie grundsätzlich zuerst einen vorhandenen vCenter-Server auf die Version 5.0 aktualisieren. Alle Vorgängerversionen des vCenter Servers 5.0 können die neuen vSphere-Hosts nicht managen.

Ist die Managementumgebung in der passenden Version vorhanden und betriebsbereit, bleiben mehrere Möglichkeiten, das Update der Hosts durchzuführen. Bei den kurzen Bereitstellungszeiten sollten Sie sich aber überlegen, ob es nicht grundsätzlich sinnvoller ist, direkt eine Neuinstallation vorzunehmen. Über diesen Weg werden Sie auch die gesamten Altlasten los und haben ein frisches neues System.

6.2.1 Upgrade von der Version ESX 3.x/ESXi 3.x

Das Upgradeszenario von der Version ESX 3.x/ESXi 3.x ist relativ einfach beschrieben. Es gibt keinen direkten Weg von diesen Versionen zu der Version ESXi 5.x, es ist auch nicht supportet. Die einzige Option, die Sie haben, wenn Sie diesen Weg gehen wollen, ist über ein Upgrade auf die Version 4.x mit dem anschließenden Upgrade zur Version 5.x. Denken Sie darüber nach, ob das arbeitstechnisch sinnvoll ist oder ob eine Neuinstallation nicht schneller geht oder ratsamer ist.

6.2.2 Upgrade von der Version ESX 4.x/ESXi 4.x

Ein Upgrade von der Version 4.x auf die aktuelle Version ist recht simpel und wird auch unterstützt. Legen Sie die CD mit der aktuellen Version ein, und gehen Sie den Installations-

weg durch. Nach der Auswahl der Festplatte stellt das System fest, dass bereits eine VMware-Installation auf der Festplatte ist, und Ihnen wird angeboten, das System zu aktualisieren.

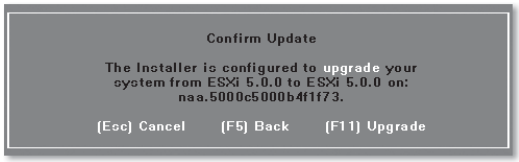


Abbildung 6.28 Upgrade ESX-Version 4.x auf 5.x

Wichtig!

Alle virtuellen Maschinen müssen auf dem zu aktualisierenden System gestoppt oder mit vMotion auf andere ESX(i)-Server verschoben werden.

Das mit der Version 4.0 vorgestellte vSphere Host Update Utility ist wieder von der Bildfläche verschwunden. Diese Option für ein Update von vSphere Hosts können Sie getrost vergessen. Insgesamt gibt es also zwei Möglichkeiten, einen vSphere-Host zu erhalten: die Neuinstallation oder ein Update über den Update Manager.

Neuinstallation

Aufgrund der schnellen Installation von VMware vSphere ist eine mögliche Wahl, alle Hosts neu zu installieren. Dazu fahren Sie einen Host eines eventuell bestehenden Clusters in den Maintenance-Modus. Dadurch werden alle virtuellen Maschinen vom Server evakuiert. Trennen Sie den Host im vCenter, und installieren Sie ihn neu. Nach erfolgreicher Installation und Aufnahme in den Cluster geben Sie den Host wieder für VMs frei. So können Sie einige der VMs wieder auf den neuen Host migrieren. Wiederholen Sie die Vorgehensweise für alle betroffenen Server, bis alle Systeme aktualisiert worden sind. Der Vorteil dieser Vorgehensweise liegt darin, dass die Möglichkeit besteht, die Systemkonfiguration anzupassen. Dieser Weg sollte die erste Wahl sein, wenn die Hostsysteme schon vorher von der Version ESX/ESXi 3.x aktualisiert wurden. Alternativ können Sie auch die Installation weglassen und die Systeme direkt vom Netzwerk starten. Dazu aber später mehr in Abschnitt 12.8.

vCenter-Server

Damit der vCenter-Server die Option für das Updaten von ESXi 4.x-Hosts anbietet, muss der vSphere Update Manager installiert sein. Dies kann sowohl auf dem vCenter selbst als auch auf einem anderen, im Netzwerk stehenden System erfolgen. Selbstverständlich müssen Sie den passenden Client installieren. Dieser Client integriert sich in den vSphere-Client und ist auf dem System einzurichten, von dem Sie die Arbeiten durchführen wollen.

Detaillierte und weitergehende Informationen zur Konfiguration des Update Managers finden Sie in Abschnitt 12.1, »Einsatz des vCenter Update Managers«. Jetzt soll nur darauf eingegangen werden, wie Sie vorhandene Hosts aktualisieren.

Setzen Sie den Update Manager zuerst nur für das Update von ESXi-Servern ein, ist initial kein Patch-Repository zu hinterlegen. Über den Button Hosts treffen Sie die Auswahl, alle hostbasierten Baselines anzuzeigen.

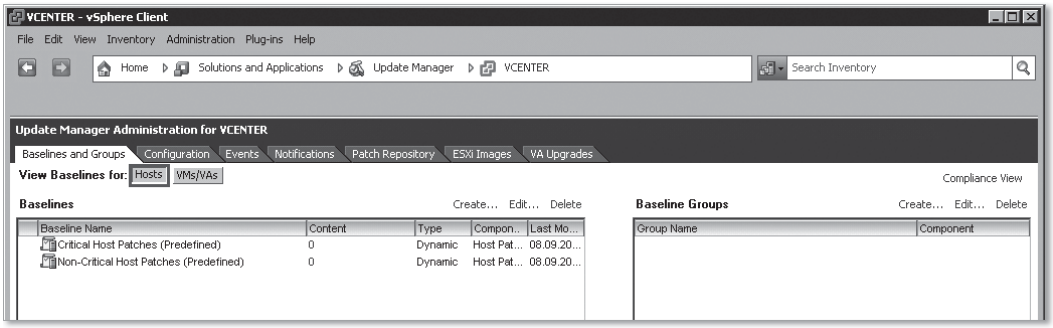


Abbildung 6.29 vSphere Update Manager

Es folgt der Import eines ESXi-Images über den Reiter ESXi Images. Nach dem Abschluss des Imports wird die Auswahl geboten, direkt eine Baseline zu erstellen. Das lehnen wir an dieser Stelle ab und erstellen sie in der Hauptoberfläche über das Kontextmenü. Über diesen Weg folgt die initiale Anlage einer Upgrade-Baseline. Über den entsprechenden Auswahlpunkt im Kontextmenü starten Sie einen Wizard, der die passenden Abfragen stellt, um eine zugehörige Baseline zu erstellen.

Das erste Fenster ist an sich selbsterklärend. Wir wünschen eine Baseline, mit der sich existierende Hosts updaten lassen (Abbildung 6.30).

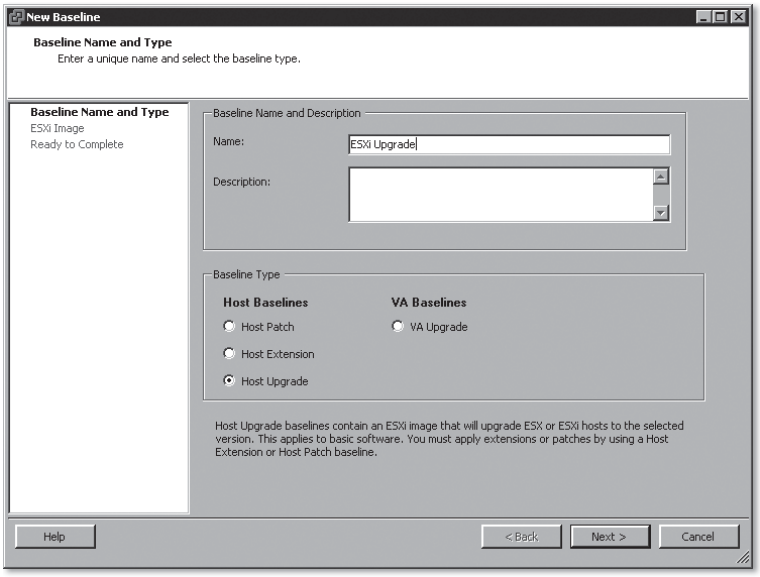


Abbildung 6.30 Erstellen einer Upgrade-Baseline

Damit die Arbeiten durchgeführt werden können, benötigt der Update-Server das ISO-File mit den vSphere-Installationsdateien (Abbildung 6.31).

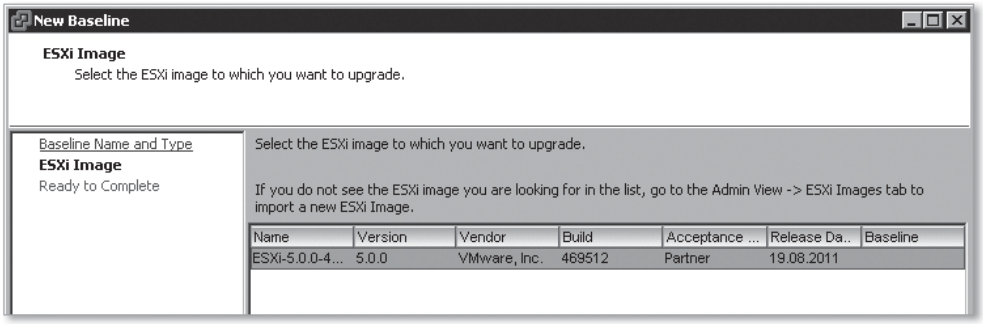


Abbildung 6.31 Einbinden der benötigten Medien

Die Baseline ist erstellt und nun nutzbar. Jetzt ist eine Baseline-Gruppe zu generieren. Über das Kontextmenü im Fenster Baseline Groups (Abbildung 6.32) kreieren Sie nun dieses Konfigurationselement. Es öffnet sich ein Dialog, in dem Sie einen Namen vergeben müssen. Selbstverständlich handelt es sich hier um eine Baseline für Hostsysteme. Es folgt die Verbindung der jetzt erstellten Host-Baseline mit der vorher erstellen Patch-Baseline (Abbildung 6.32).

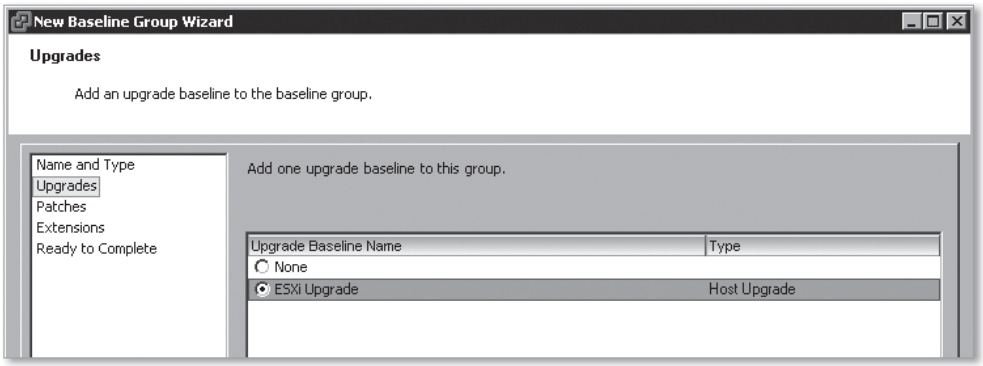


Abbildung 6.32 Verknüpfung von Patch- und Host-Baseline

Schließen Sie den Dialog mit Beenden ab. Wenn Sie jetzt auf die Hosts und dann auf den Reiter Update Manager gehen, befinden Sie sich an der Stelle, wo Sie die Update-Policy mit dem Host verbinden können.

Der ausgewählte Host ist zu standardisieren. Dies geschieht über den entsprechenden Button (Abbildung 6.33). Der folgende Dialog erwartet die Auswahl der passenden Baseline und Baseline-Gruppe. Es folgen die Lizenzvereinbarung und eine Zusammenfassung der eingestellten Konfiguration. Abschließend legen Sie die Startzeit des Auftrages fest und geben dem Auftrag einen eindeutigen Namen.

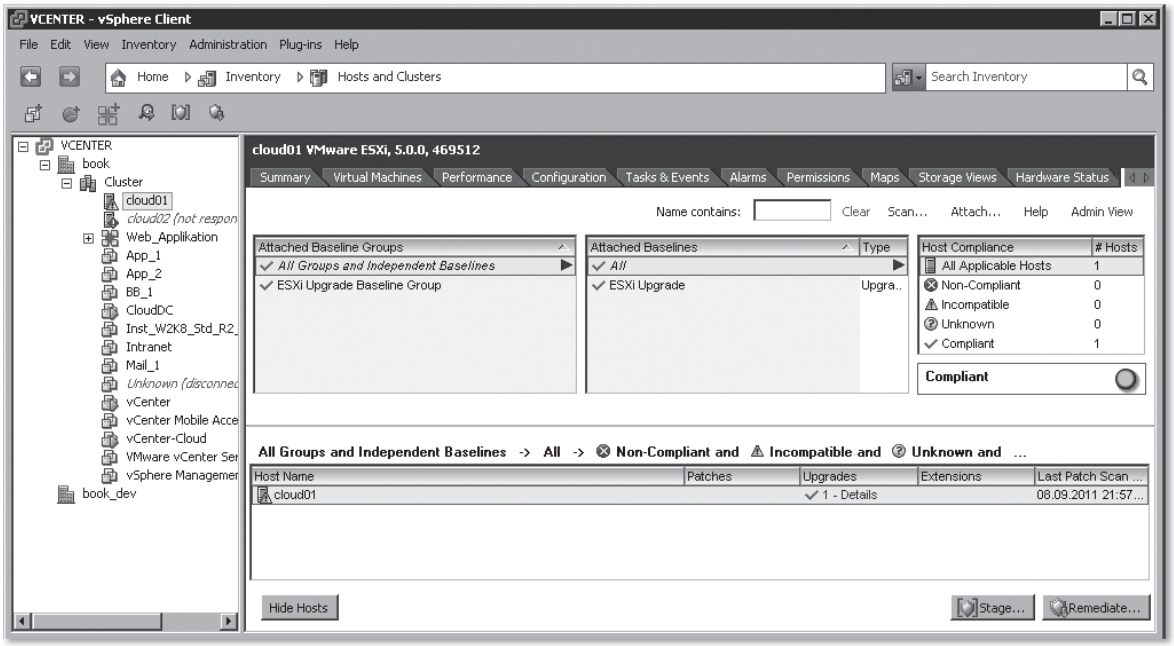


Abbildung 6.33 Update Manager für ein Host-Objekt

Stoßen Sie jetzt über den Link STAGE den Updatevorgang an. Dieser läuft dann vollkommen automatisch ab; es sind keine manuellen Eingriffe nötig. Zuerst wird der Server automatisch in den Maintenance-Modus gefahren. Anschließend führt der Patch-Manager die Updatearbeiten durch. Nach dem Abschluss der Arbeiten wird der Host automatisch neu gestartet. Das System ist wieder unter der alten Netzwerkkonfiguration erreichbar und ist nun wieder aus dem Maintenance-Modus zu nehmen.

6.3 VMware vCenter Server

Wenn es um erweiterte Funktionen wie vMotion, HA, DRS etc. oder zentrale Verwaltung geht, hilft die reine vSphere-Installation wenig weiter, da jeder vSphere-Server nur ein System darstellt, dessen Ressourcen partitioniert werden können, um virtuelle Maschinen zu betreiben. Mit der Version 2.x des VMware ESX-Servers wurde das Verwaltungswerkzeug vCenter in Version 1 eingeführt und stellt seitdem einen immer wichtigeren Bestandteil der VMware-Infrastruktur dar. In der aktuellen Version des vCenter-Servers haben Sie die Möglichkeit, über 1.000 vSphere-Server und über 10.000 eingeschaltete/15.000 registrierte virtuelle Maschinen zentral zu verwalten und durch Cluster, Resource-Pools und vMotion zu einer virtuellen Gesamtheit zu verschmelzen. Nutzen Sie die Verlinkung von vCenter-Servern, dann sind bis zu 3 .000 vSphere-Server und maximal 30 .000 eingeschaltete/50.000 registrierte virtuelle Maschinen adressierbar.

Das vCenter ist sogar der wichtigste Grund, um von einer virtuellen Infrastruktur sprechen zu können. Das vCenter, vormals Virtual Center-Server, hat im Laufe der Zeit, wie fast jede Software, viele Entwicklungsstufen durchgemacht und integriert zur Drucklegung des Buches nun folgende Komponenten: Hostprofile, VMware vCenter Server, vCenter Server License Manager, vCenter WebAccess, vCenter Update Manager, vCenter Server Heartbeat, vCenter Server Orchestrator.

In den meisten Fällen empfiehlt es sich, alle benötigten (bzw. lizenzierten) Komponenten auf einem einzelnen System zu installieren und zu betreiben. Für Test- und Entwicklungsumgebungen können Sie auch direkt eine MS SQL-Express-Datenbank-Engine mitinstallieren, ansonsten sollten Sie auf einen MS SQL-, IBM DB2- oder einen Oracle-Datenbank-Server zurückgreifen. In der aktuellen Version wird zwar die Express-Version des MS SQL Servers mitgeliefert, sie ist aber für produktive Umgebungen nicht zu empfehlen.

Handelt es sich um eine recht kleine Installation von 10 und weniger vSphere-Servern mit 100 und weniger virtuellen Maschinen, kann der Datenbank-Server auch auf der gleichen Maschine wie das vCenter mitlaufen. Ansonsten sollten Sie den Datenbank-Server auf einer getrennten Maschine betreiben, weil die Last und das Datenaufkommen entsprechend der Infrastrukturgröße steigen.

Für die Planung des Datenbankwachstums existiert ein VMware-Excel-Dokument, das Ihnen eine ungefähre Größenberechnung für Microsoft SQL ermöglicht: *http://www.vmware.com/support/vsphere4/doc/vsp_4x_db_calculator.xls*

Die Größenberechnung für Oracle findet sich unter: *http://www.vmware.com/support/vsphere4/doc/vsp_4x_db_calculator_oracle.xls*. Beide Versionen sind nur für vSphere 4.x; eine neuere Version lag zur Drucklegung noch nicht vor.

Abbildung 6.34 zeigt eine solche Berechnung mit 20 Hosts und 200 VMs, deren Größe bei ca. 3,4 GB liegt, wenn Sie das 2. Protokolllevel einschalten würden. Auch wenn im Kopf der Tabelle noch die alte Bezeichnung des Produktes steht, so gilt der errechnete Wert auch für die aktuelle Version des Management Tools.

Der Update Manager benötigt ebenfalls eine eigene Datenbank. Auch hier gibt es ein Excel-Sheet, das Sie bei der Berechnung der benötigten Datenbankgröße unterstützt. Sie finden dieses Dokument (Abbildung 6.35) unter der URL: *http://www.vmware.com/support/vsphere4/doc/vsp_vum_41_sizing_estimator.xls*

Dieses Dokument berechnet Datenbank- und Festplattenbelegung in einem. Während beim Update Manager nicht viel in der Datenbank passiert, ist die Festplattenbelegung nicht nennenswert und wächst, abhängig von der Anzahl verschiedener Betriebssysteme und -stände, schnell jährlich im zweistelligen GByte-Bereich. Auch in diesem Sheet werden analog die Daten der ersten Berechnung zugrunde gelegt. Microsoft Updates werden von dem aktuellen Update Manager aber nicht mehr unterstützt.

vmware

vCenter Server Database Sizing Calculator for Microsoft SQL Server
Valid for vCenter Server 4.0

Number of hosts	20
Number of virtual machines	200
Number of clusters	1
Number of resource pools	0
Number of datastores	50
Number of datacenters	1
Number of root folders	1
Average number of network devices per host	2
Average number of network devices per virtual machine	1
Average number of disk devices per host	10
Average number of disk devices per virtual machine	4
Average number of CPUs per host	4
Average number of virtual CPUs (vCPUs) per virtual machine	2
Number of device types per virtual machine for datastore statistics	4
Average number of debugging statistics or devices	1000

	Number of Samples Collected Every 5 Minutes	Potential DB Size in Gigabytes at the End of 1 Year	+15%	-15%	Space Required for Temporary DB
Statistics Collection Level 1	5968	1,7	1,9	1,4	1,7
Statistics Collection Level 2	12156	3,4	4,0	2,9	3,4
Statistics Collection Level 3	27636	7,8	9,0	6,7	7,8
Statistics Collection Level 4	43957	12,5	14,3	10,6	12,5

Abbildung 6.34 VMware-vCenter-Datenbank-Kalkulation

Fazit

Um vCenter und den vCenter Update Manager zu nutzen, benötigen Sie zwei unabhängige Datenbanken. Das voraussichtliche Wachstum können Sie mit den vorgestellten Excel-Dokumenten anhand der Infrastrukturdaten selbst berechnen.

6.3.1 vCenter-Systemvoraussetzungen

VMware vCenter Server gibt es mittlerweile in zwei unterschiedlichen Versionen: als Linux-Appliance und als Microsoft-Windows-Anwendung. Auf die Appliance gehen wir in Abschnitt 6.4 ein.

Für die Windows-Version wird als Basisbetriebssystem logischerweise nur ein Microsoft-Betriebssystem unterstützt. In der Kompatibilitätsliste (Abbildung 6.36) finden sich nur Windows-Server-Betriebssysteme ab der 2003er-Version in 64 Bit. Workstation-Betriebssysteme werden nicht mehr unterstützt. Auch wenn in der Abbildung nur das vCenter als abgefragte Einheit steht, so unterstützt der Update Manager genau dieselben Betriebssystemversionen wie das vCenter.

Als Datenbank können verschiedene Programmversionen des Microsoft SQL Servers, der IBM DB2 und des Oracle-Datenbank-Servers dienen. Die aus vorherigen vCenter-Server-Zeiten bekannte MSDE-Installationen für Test- und Entwicklungsumgebungen sind der Microsoft SQL Server 2008 Express Edition gewichen.

Answer these questions about the VMware vSphere 4.1 deployment in your organization:

Do you upgrade from 4.0 and continue using old ESXi upgrade bundles?	No
Do you perform patch remediation of virtual machines?	No
Do you have ESX 3.0.3+ hosts?	No
Do you have ESX 3.5+ hosts?	No
Do you have ESX 4.0 hosts?	No
Do you have ESX 4.0 U1+ hosts?	Yes
Do you have ESX 4.1 hosts?	Yes
Do you have ESXi 3.5+ hosts?	No
Do you have ESXi 4.0 hosts?	Yes
Do you have ESXi 4.0 U1+ hosts?	Yes
Do you have ESXi 4.1 hosts	Yes
How many concurrent ESXi host upgrades do you plan to do?	1
Number of hosts, including those in clusters	50
Number of virtual machines	1000
Number of Windows distributions (2k/XP/2k3/Vista) in the inventory	1
Average number of locales for Windows distribution	1
Average number of different Service Pack levels for Windows distribution	1
Patch scan frequency for virtual machines per month	1
VMware Tools upgrade scan frequency for virtual machines per month	1
Virtual machine hardware upgrade scan frequency per month	1
Patch scan frequency for hosts per month	2
Upgrade scan frequency for hosts per month	1
VMware vCenter Update Manager database deployment model recommendation:	Use a separate DB from the vCenter Server DB
VMware vCenter Update Manager server deployment model recommendation:	Install VUM on the same host as the vCenter Server host

Resource	Initial Utilization MB	Estimated Monthly Utilization MB		
		Median	+20%	-20%
Database Space Usage	150	79	94	63
Disk Utilization — Patch Content	12.938	2.700	3.240	2.160
Disk Utilization — Temporary Space	3.072	Not Applicable	Not Applicable	Not Applicable

Abbildung 6.35 VMware Update Manager – Berechnung Platten- und Datenbankbelegung

Search Results: Your search for "Guest/Host OS" returned **6 results**. Display: 10

Partner Name	OS Release	Bits	OS Use	Supported Releases
Microsoft	Windows Server 2003 R2	64	Host OS	**vCenter Server** 5.0
Microsoft	Windows Server 2003 Service Pack 2	64	Host OS	**vCenter Server** 5.0
Microsoft	Windows Server 2008 R2	64	Host OS	**vCenter Server** 5.0
Microsoft	Windows Server 2008 R2 Service Pack 1	64	Host OS	**vCenter Server** 5.0
Microsoft	Windows Server 2008 Service Pack 1	64	Host OS	**vCenter Server** 5.0
Microsoft	Windows Server 2008 Service Pack 2	64	Host OS	**vCenter Server** 5.0

Abbildung 6.36 Auszug VMware Compatibility Guide – unterstützte Betriebssysteme

Tabelle 6.2 zeigt die derzeitige Kompatibilität zwischen der vCenter-Applikation und den Datenbanken von Microsoft, IBM und Oracle.

Datenbank	Bemerkung	vCenter	vCVA	Update Manager
IBM DB2 9.5	Das FixPack 5 ist erforderlich, empfohlen wird jedoch das FixPack 7.	X	–	–
IBM DB2 9.7	Das FixPack 2 ist erforderlich, empfohlen wird jedoch das FixPack 3a.	X	–	–
MS SQL 2008 R2 Express	Die mitgelieferte Datenbank ist nur für kleine Umgebungen geeignet: maximal 5 Hosts und 50 VMs.	X	–	X
MS SQL 2005	32-Bit- und 64-Bit-Version; SP3 ist erforderlich, SP4 wird empfohlen. MSXML Core Services 6.0 müssen vor der Installation entfernt werden.	X	–	X
MS SQL 2008	32-Bit- und 64-Bit-Version, SP1 ist erforderlich, SP2 wird empfohlen.	X	–	X
MS SQL 2008 R2	64-Bit-Version	X	–	X
Oracle 10g R2	Zuerst sollte der Patch 10.2.0.4 oder neuer installiert werden. Anschließend kann der Patch 5699495 auf dem Client installiert werden.	X	X	X
Oracle 11g	Oracle 11g R1 11.1.0.7, Oracle 11g R2 11.2.0.1 Patch 5	X	X	X

Tabelle 6.2 Datenbankkompatibilität vCenter und Update Manager

6.3.2 Download der Installationsmedien

Auf der VMware-vCenter-Download-Seite ist die Companion-DVD zu finden (siehe Abbildung 6.3), die alle notwendigen Komponenten enthält. Haben Sie eine Mischumgebung im Einsatz, benötigen Sie noch den alten Lizenz-Server aus dem vCenter 2.5 Ux. Diese Version können Sie ebenfalls auf der VMware-Webseite herunterladen und in das neue vCenter einbinden.

6.3.3 Vorbereitung der Datenbank

Als Datenbanken werden im produktiven Umfeld verschiedene Versionen von IBM DB2, Microsoft SQL Server und Oracles Datenbank-Server unterstützt. In Test- und Entwicklungsumgebungen können Sie die mitgelieferte Version Microsoft SQL Server 2008 Express nutzen.

Für den Zugriff auf die Datenbanken benötigt das vCenter eine ODBC-Verbindung zu dem Datenbank-Server. Beachten Sie bitte, dass der vCenter Server selbst eine 64-Bit-ODBC-Verbindung benötigt, der vCenter Update Manager aber eine 32-Bit-Verbindung!

IBM DB2

Die Datenbank von IBM kommt nach unseren Erfahrungen so selten zum Einsatz, dass wir aus Platzgründen an dieser Stelle auf eine Beschreibung der Installation verzichten wollen. Es sei nur so viel gesagt, dass Sie für die Erstellung der ODBC-Verbindung den Treiber *IBM DB2 ODBC Driver – VCDB2_remote* nutzen müssen.

Microsoft SQL 2008 Express

Diese Datenbanksoftware wird auf der Companion-DVD direkt mitgeliefert und durch die Installationsroutine bei Nichtangabe einer externen Datenbank automatisch installiert. Diese empfiehlt sich jedoch nur für kleine Umgebungen. Es sind in diesem Fall keine Vorbereitungen nötig.

Microsoft SQL 2005/8

Haben Sie selbst oder der Datenbankadministrator eine vCenter-Datenbank (und zusätzlich eine VMware-Update-Manager-Datenbank) im Microsoft SQL Server eingerichtet, benötigt die vCenter-Installation einen vorbereiteten ODBC-Zugriffsweg. Diesen erstellen Sie in den Administrative Tools • Verwaltung • Data Sources, die innerhalb der Systemsteuerung (Abbildung 6.37) zu finden sind.

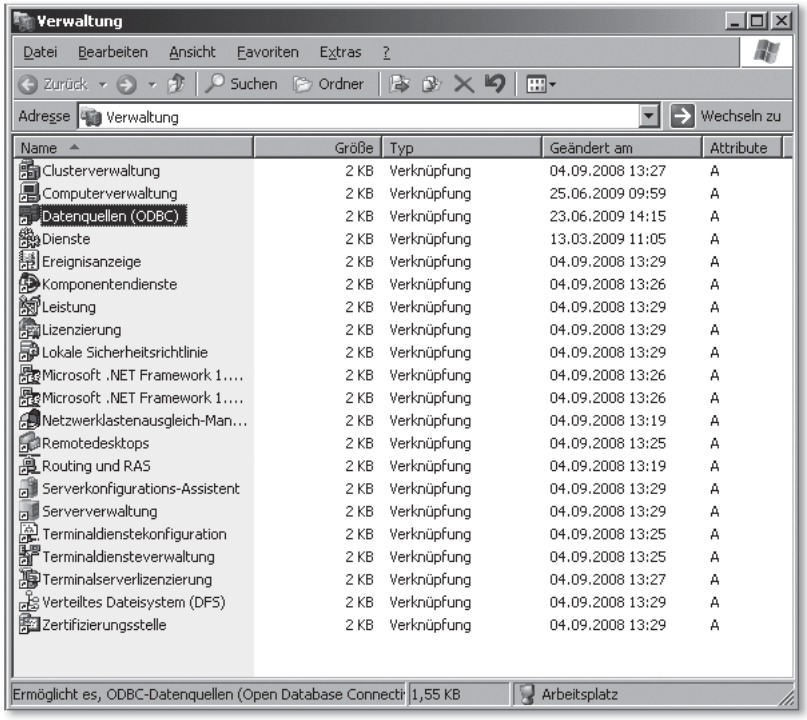


Abbildung 6.37 Anlage ODBC-Datenquelle

Wichtig!

Diese Vorgehensweise trifft nur bei der Benutzung eines 32-Bit-Betriebssystems zu. Kommt ein 64-Bit-System zum Einsatz, ist die Arbeitsweise wie im folgenden Abschnitt beschrieben.

ODBC auf 64-Bit-Systemen

Auch auf 64-Bit-Systemen müssen Sie für den Einsatz des Update Managers mit einer 32-Bit-ODBC-Verbindung arbeiten. Dabei ist es unerheblich, welche Datenbank Sie im Hintergrund verwenden. Die Vorgehensweise ist dabei wie oben beschrieben.

Kommt der Microsoft SQL Server zum Einsatz, müssen Sie die 64-Bit-ODBC-Treiber installieren. Während der Installation werden auch automatisch die 32-Bit-Treiber installiert. Die Konfiguration der 32-Bit-Verbindung erfolgt dann über das Tool *[Windows-Verzeichnis]\SysWOW64\odbcad32.exe*.

System-DSN (Data Source Name) anlegen!

Damit alles reibungslos funktioniert, müssen Sie eine System-DSN und keine User-DSN anlegen!

Für den Zugriff auf den SQL 2005/8 Server wird der Native Client benötigt. Bei der Anlage der ODBC-Verbindung sehen Sie sofort, ob der Client schon installiert ist. Ist er nicht vorhanden, dann müssen Sie ihn erst installieren, bevor Sie fortfahren können.

Den SQL Native Client finden Sie z. B. auf der SQL-Server-2005/8-DVD, und er wird auch direkt bei den Pre-Installation-Tasks (Abbildung 6.38) über das AUTOSTART-Menü mitinstalliert. Ist schon ein älterer Native Client vorhanden, kann dieser bei einer Aktualisierung zu Problemen führen: Deinstallieren Sie ihn daher sicherheitshalber vorher. Alternativ finden Sie den Client hier: *http://www.microsoft.com/download/en/details.aspx?id=26728*

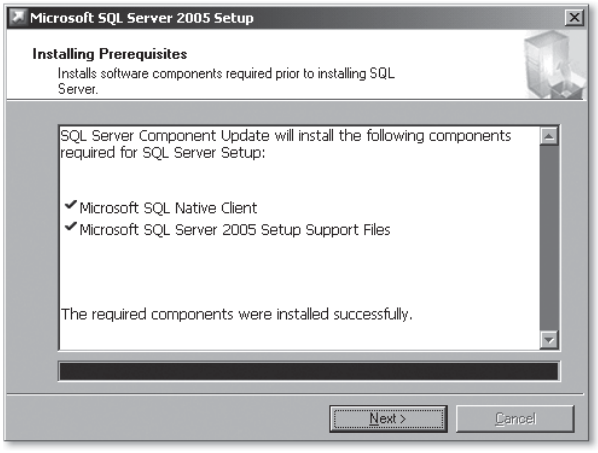


Abbildung 6.38 Installation des Microsoft SQL Native Clients

Nach der Installation des SQL Native Clients steht ein neuer ODBC-Treiber zur Verfügung, der zur Anlage der Datenquelle für vCenter genutzt werden muss (Abbildung 6.39). Das weitere Vorgehen läuft exakt so ab wie im folgenden Abschnitt beschrieben.

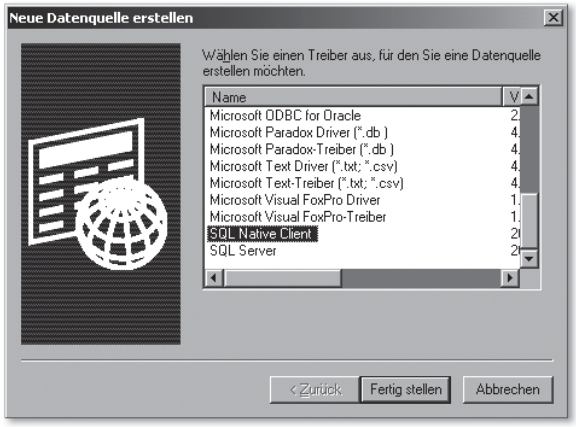


Abbildung 6.39 SQL Native Client für die Verbindung mit MS SQL 2005/8

Der zu vergebende Datenquellenname (Abbildung 6.40) wird später vom vCenter-Server referenziert und genutzt. Außerdem werden Sie nach dem SQL-Server-Namen gefragt. Idealerweise geben Sie hier den DSN an. Sind Datenbank und vCenter-Server gleich, genügt die Angabe »localhost«.

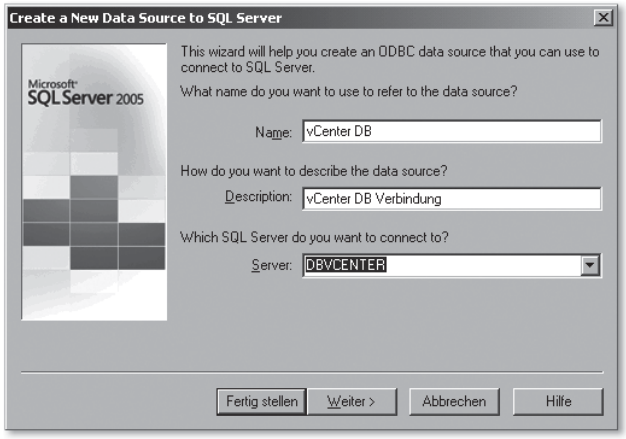


Abbildung 6.40 Konfiguration ODBC-Datenquelle – SQL-Server- und Quellenname

Der in Abbildung 6.41 vergebene Benutzername wird nur für den Windows-Test der Datenquelle und nicht vom vCenter-Server genutzt. Während der vCenter-Installation werden Sie ebenfalls nach einem Benutzerprofil, das in der Registry abgelegt wird, gefragt. Daher nutzt im Falle einer SQL-Benutzer-Kennwortänderung auch keine Anpassung der ODBC-Daten-

quelle. In den meisten Fällen wird die SQL-Benutzerauthentifizierung genutzt, wenn über das Netzwerk auf die Datenbank zugegriffen wird. Handelt es sich bei vCenter und SQL Server um das gleiche System, ist meist die Windows-Anmeldung erste Wahl. Die Registry-Angaben finden Sie in folgendem Zweig:

```
HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VCenter\DB
```

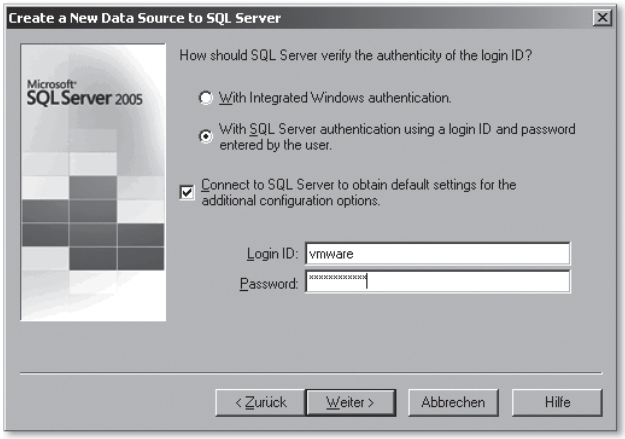


Abbildung 6.41 Verbindungsprofil – im Beispiel wird die SQL-Server-Authentifizierung genutzt.

Bei der Einrichtung des Benutzers und der vCenter-Datenbank auf dem Datenbank-Server ist die klare Empfehlung, einen exklusiven Benutzer für die Datenbank anzulegen. Ist dieses nicht gewollt oder möglich, müssen Sie darauf achten, die vCenter-Datenbank dediziert als Default-Database anzugeben (Abbildung 6.42).

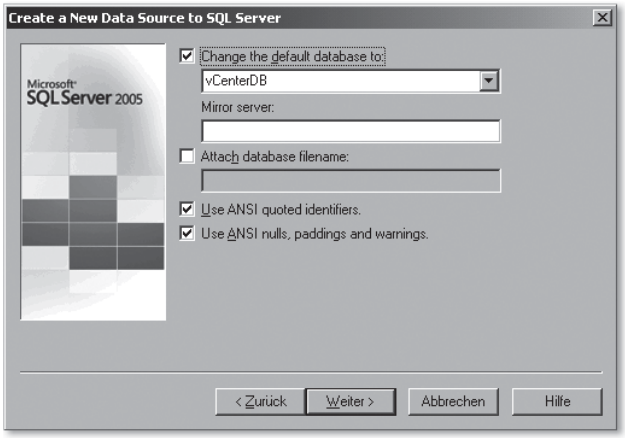


Abbildung 6.42 Die Standarddatenbank wird auf die vCenter-Datenbank umkonfiguriert.

Die weiteren Angaben im folgenden Fenster übernehmen Sie als Default. Ein abschließender Test (Abbildung 6.43) zeigt, ob die ODBC-Datenbankverbindung funktioniert oder noch Fehler auszubügeln sind. Diesen Test sollten Sie immer durchführen, um Fehler bereits frühzeitig zu erkennen.

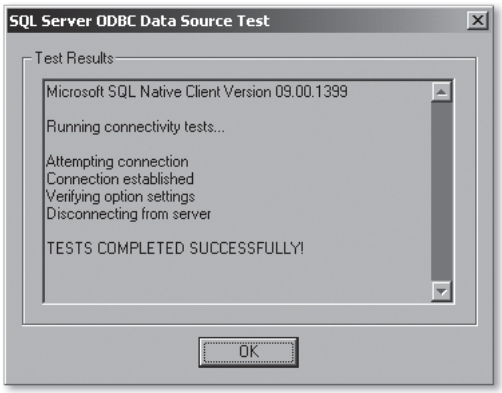


Abbildung 6.43 Sind alle Angaben korrekt, dann sollte der Test erfolgreich ausfallen.

Bekannte Probleme Microsoft SQL Server

Datenbankberechtigung

Bei der Anlage der vCenter-Datenbank muss natürlich eine entsprechende Berechtigung vorhanden sein. vCenter erwartet hier nahezu volle Berechtigung an der Datenbank, da außer Löschung der Datenbank und Änderung des Owners fast alles verändert wird. Glücklicherweise kontrolliert die vCenter-Installationsroutine bereits die Berechtigungsstruktur und zeigt eine Warnmeldung (Abbildung 6.44), was Ihnen die spätere Fehlersuche erspart.

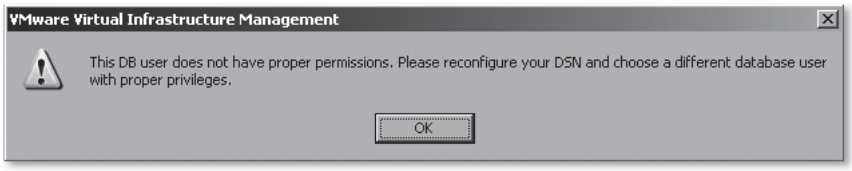


Abbildung 6.44 Falsche Berechtigungen auf der vCenter-Datenbank

Recovery-Modell

Bei der Anlage der beiden Datenbanken für vCenter und VMware Update Manager sollten Sie außerdem die Einstellung des Recovery-Modells überdenken, da die Full-Recovery-Einstellung schnell die Festplattenpartition des Datenbank-Servers bis an die Kapazitätsgrenze füllt (Abbildung 6.45, Abbildung 6.46). Zumeist reicht die Einstellung SIMPLE für das Recovery-Modell.

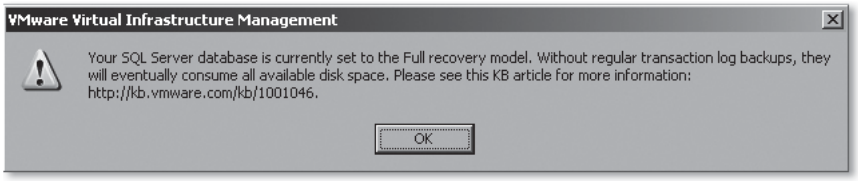


Abbildung 6.45 Das Recovery-Modell »Full« bei SQL Server kann zu vollem Dateisystem führen.

VMware hat zu diesem doch recht häufigen Support-Call einen eigenen Knowledge-Base-Artikel mit der Nummer 1001046 verfasst, den Sie unter *http://kb.vmware.com* finden.

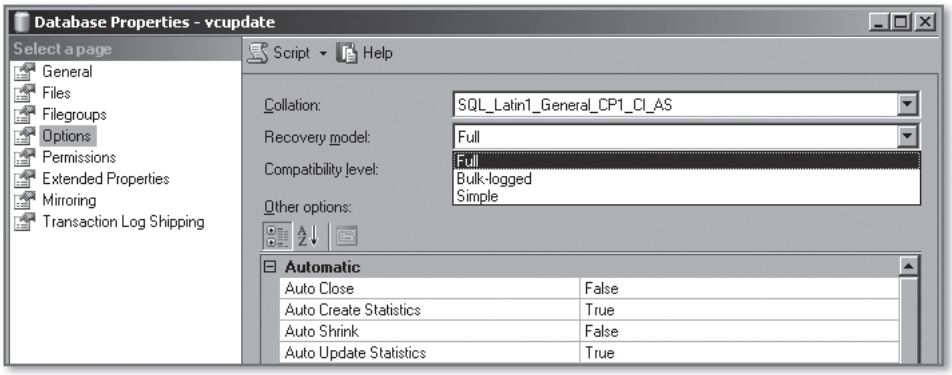


Abbildung 6.46 Simple-Recovery-Modell-Einstellung an der MS-SQL-Server-Datenbank

Kennwortänderung SQL-Benutzer

Bei einer Kennwortänderung ist der empfohlene Weg die Neuinstallation des VMware-vCenter-Servers unter Beibehaltung der bestehenden Datenbank.

Können Sie die Kennwortänderung planen, ist es am einfachsten, das Passwort im vCenter-Server zu ändern. Passen Sie dazu wie in Abbildung 6.47 das Datenbank-Passwort an (Administration • vCenter Server Settings • Advanced Settings), und stoppen Sie den vCenter-Server-Dienst. Ändern Sie danach den SQL-Benutzer auf dem SQL Server, und starten Sie den vCenter-Dienst wieder.

Tipp

Das Vorgehen ist übrigens unabhängig von der genutzten Datenbanksoftware.

Oracle

Nutzen Sie eine Oracle-Datenbank für die vCenter-Komponenten, müssen Sie den Oracle-Client installieren. Dieser bringt auch einen ODBC-Treiber für Windows mit. Im Beispiel arbeiten wir mit einer Oracle 11g-Installation.

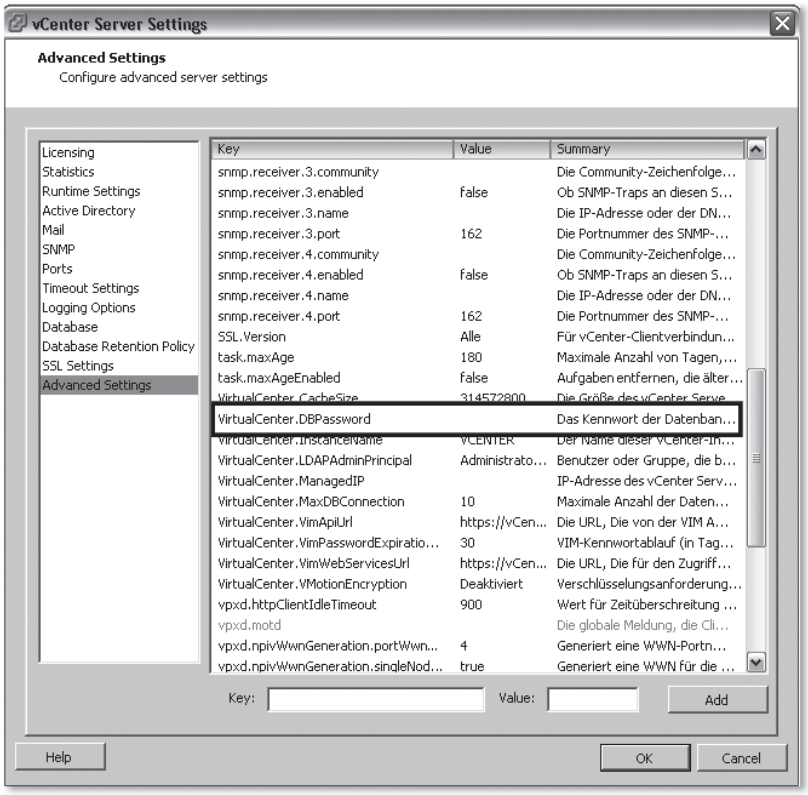


Abbildung 6.47 Änderung des Datenbank-Passworts im vCenter

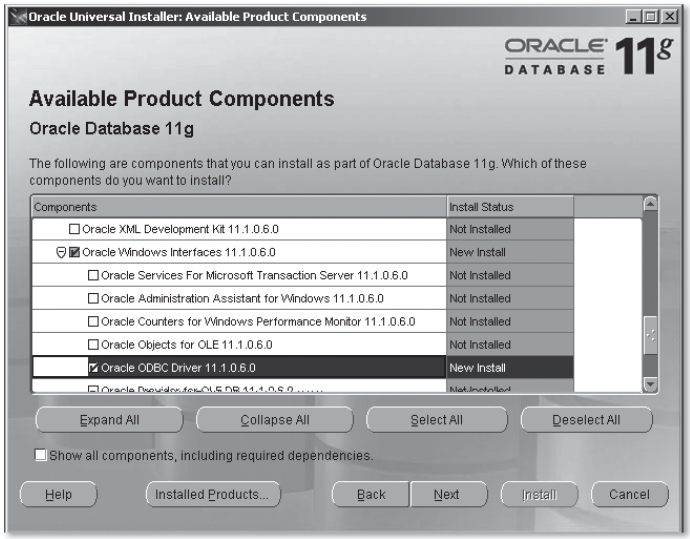


Abbildung 6.48 Oracle 11g-Installationsroutine ODBC-Treiber

Neben dem Oracle-ODBC-Treiber für Windows muss unter 11g der Connection Manager auf dem vCenter-Server vorhanden sein, um die ODBC-Verbindung zu nutzen (Abbildung 6.48, Abbildung 6.49).

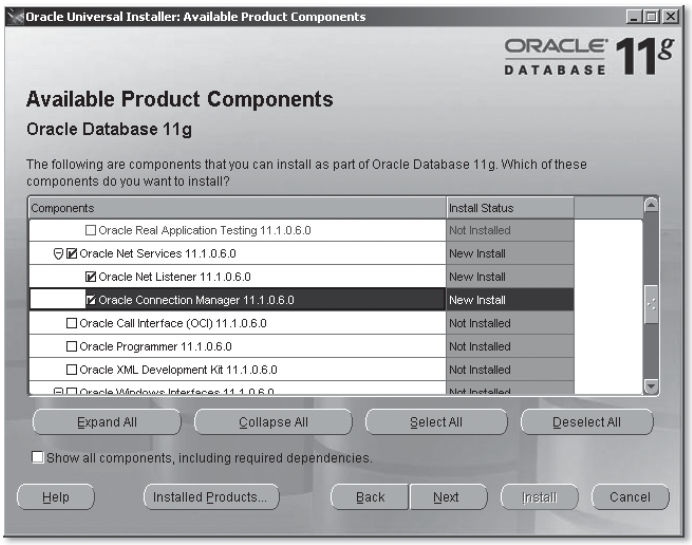


Abbildung 6.49 Oracle-Installationsroutine – Listener und Connection Manager

Nach der Installation der Oracle-Komponenten müssen Sie über den Connection Manager ein TNS-Profil einrichten. Im Endeffekt ist der Connection Manager lediglich eine grafische Oberfläche zur Erzeugung der Datei *tnsnames.ora*, die Oracle-Administratoren bekannt sein muss. Die *tnsnames.ora* enthält neben dem TNS-Service-Namen die Adresse des Oracle-Datenbank-Servers und den Datenbanknamen.

Beispiel »tnsnames.ora«:

```
VCENTER-DB =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = oracle)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = vcenter)
    )
  )
```

Beschreibung:

- `VCENTER-DB` = TNS-Service-**Name**
- `oracle` = Datenbank-Server (IP, Host-Name oder DNS-Name möglich)
- `vcenter` = Service-Name = Oracle-Datenbank-Listener

Nach erfolgreicher *tnsnames.ora*-Erstellung durch den Connection Manager legen Sie eine System-DSN an und wählen während der Konfiguration den Oracle-Treiber (Abbildung 6.50) aus.

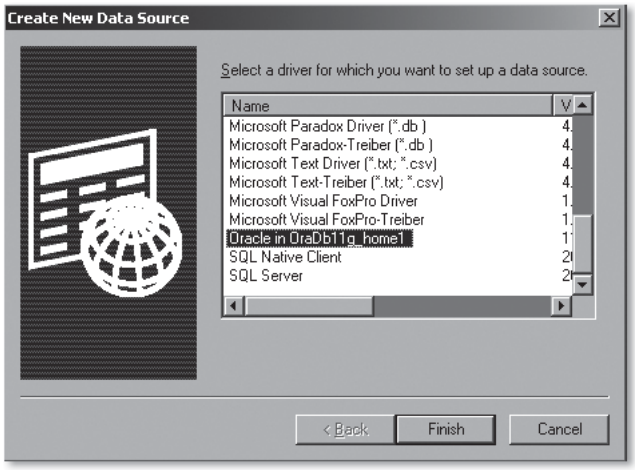


Abbildung 6.50 Oracle-ODBC-Treiber

Zum größten Teil ist die Erstellung der Oracle-ODBC-Verbindung mit der SQL-Server-Verbindung identisch, daher können Sie bei Bedarf gern in der SQL-Anleitung spicken (vergleiche Seite 242). Ein wesentlicher Unterschied ist jedoch die Frage nach dem TNS-Service-Namen (statt des SQL-Server-Namens), der durch die *tnsnames.ora* vorgegeben wird (Abbildung 6.51).

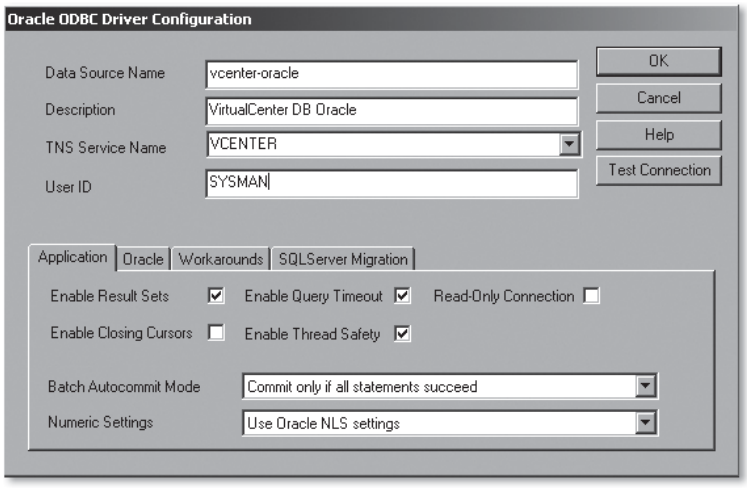


Abbildung 6.51 Konfiguration Oracle-ODBC-Treiber

Funktioniert die Verbindung nach dem Klick auf Test Connection, ist die Wahrscheinlichkeit groß, dass auch die vCenter-Installation reibungslos durchläuft.

6.3.4 Installation vCenter und Komponenten

Da nun alle Datenbankvorbereitungen getroffen sind, beginnen Sie mit der eigentlichen vCenter-Installation. Allerdings sollten Sie noch den Stand des Microsoft Windows Installers überprüfen und gegebenenfalls auf die Version 3.1 (*http://support.microsoft.com/?id=893803*) aktualisieren bzw. alle wesentlichen Windows-Patches einspielen. Prinzipiell ist die Installation absolut einfach und intuitiv gehalten, vorausgesetzt, alle Vorgaben sind erfüllt.

Auch in dieser Version hat VMware ein Autostartmenü auf die Installations-DVD gepackt und bietet hier die Auswahl der zu installierenden Komponenten an. Der Vorteil liegt auf der Hand: Möchten Sie nicht alle Komponenten auf einem Server installieren, so können Sie an dieser Stelle die passende Auswahl treffen.

Starten Sie die *autorun.exe* (manuell oder automatisch), erscheint das Begrüßungsfenster mit den verschiedenen Installationsoptionen (Abbildung 6.52). Wirklich gut gemacht ist, dass zu jedem Installationspaket auf der rechten Seite des Fensters die Voraussetzungen angezeigt werden. Sollten diese auf Ihrem System nicht erfüllt sein, so können sie über einen passenden Link die Installation der noch benötigten Applikation starten.

Abbildung 6.52 Custom-Auswahl vCenter-Installationsroutine

Der Lizenz-Server erscheint nicht als gesonderter Auswahlpunkt, sondern ist wieder Bestandteil des vCenters. Wird der vCenter-Server in einer Landschaft eingesetzt, in der noch ESXi 3.x-Systeme administriert werden müssen, müssen Sie separat einen alten Lizenz-Server installieren. Weiteres zu dieser Installation finden Sie weiter unten in diesem Kapitel im Abschnitt »Einzelinstallation VMware-Lizenz-Server« (Seite 276).

Bevor wir nun zu der eigentlichen Installation kommen, muss zuvor ein Check durchgeführt werden. Mit der Version vCenter 4.0 Update 1 ist der Agent Upgrade Checker hinzugekommen. Damit der Test durchgeführt werden kann, muss der Server, auf dem das vCenter läuft, mit dem vCenter 5.0 kompatibel sein. Es wird getestet, ob der vCenter Agent auf den Hosts geupdatet werden kann. Nach dem Aufruf der *autostart.exe*, markieren Sie den Auswahlpunkt, vCenter Host Agent Pre-Upgrade Checker und wählen dann INSTALL. Es wird keine Installation als solche durchgeführt; das Programm startet und führt die angegebenen Tests durch.

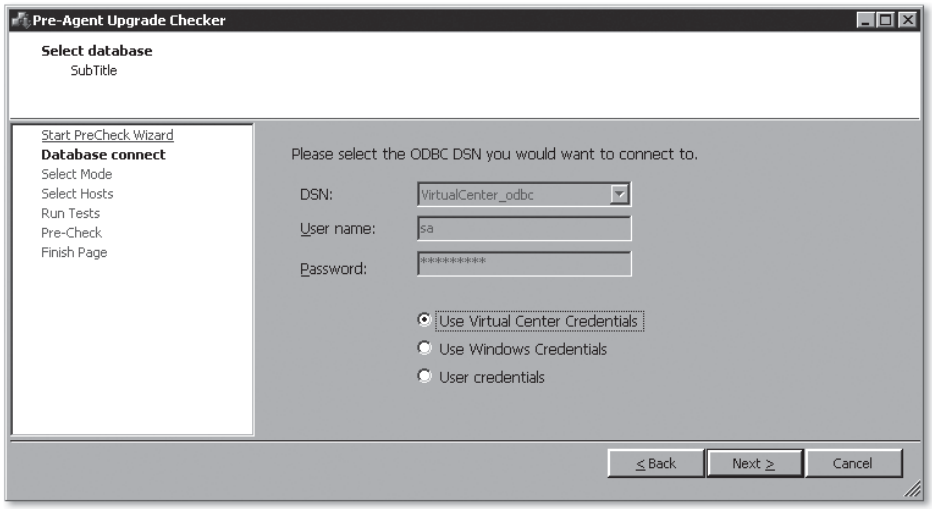


Abbildung 6.53 Verbindungsauswahl des Pre-Agent Upgrade Checkers

Jetzt wählen Sie aus, wie auf die Daten zugegriffen werden soll. Es kann direkt die DSN genutzt werden, oder die Verbindung wird über das vCenter geroutet.

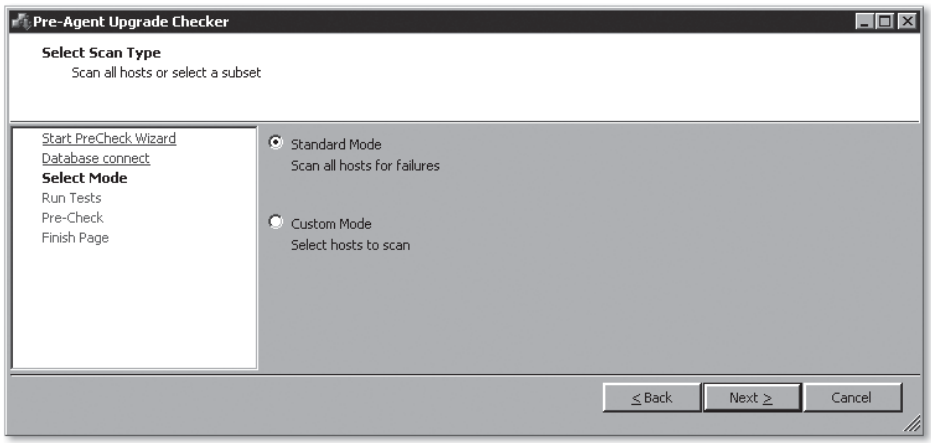


Abbildung 6.54 Host-Auswahl für den Agententest

Das Einfachste ist es, über Standard Mode alle vSphere-Hosts für den Test zu wählen. Sie können aber auch einzelne Hosts über den Custom Mode testen.

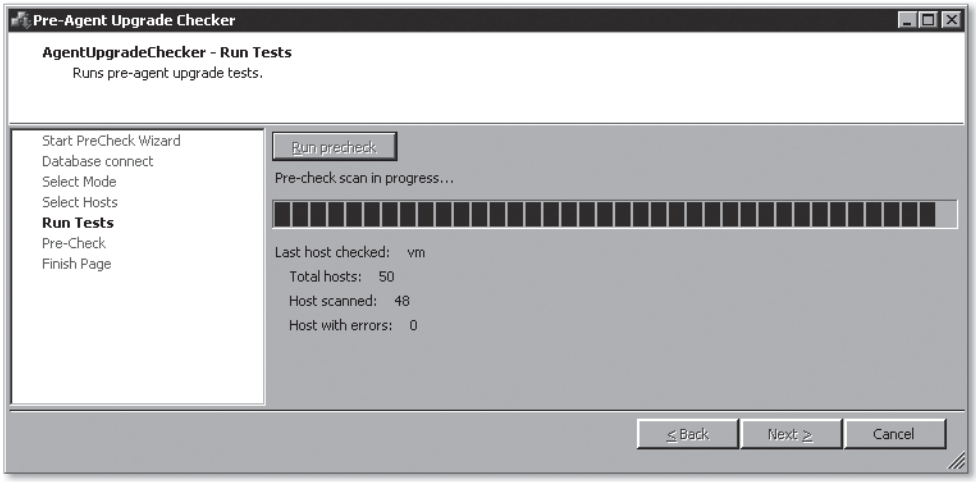


Abbildung 6.55 Lauf des Agententests

Abschließend findet sich eine Übersicht aller getesteten Hosts einschließlich des Testergebnisses. Für jeden Host können Sie sich das Ergebnis anschauen.

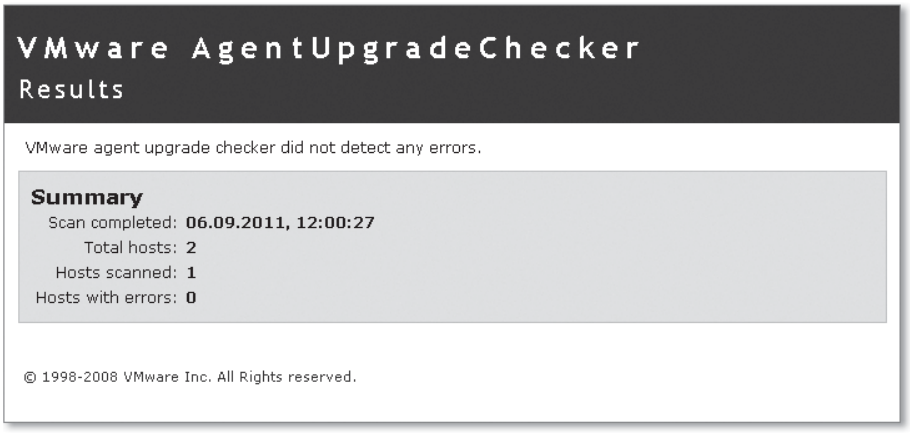


Abbildung 6.56 Testergebnis Host

Es werden das Release und die eventuellen Fehler angezeigt. In diesem Fall sind keine Probleme aufgetreten, und so können wir uns das Update vornehmen. Mit den folgenden Schritten werden erst alle Komponenten auf einem System installiert, um alle Fliegen mit einer Klappe zu schlagen. Die unterschiedlichen Komponenten können auf getrennten Systemen installiert werden. In diesem Fall fragt jede Installationsroutine nach der Netzwerkadresse des vCenter Servers.

Nach der Sprachauswahl werden benötigte Komponenten automatisch installiert. Anschließend wird der Registrierungsschlüssel erwartet (Abbildung 6.57). Geben Sie während der Installation keinen Key ein, installiert sich automatisch die Evaluation-Version des vCenter Servers. Diese erlaubt es, den vCenter Server für 60 Tage zu nutzen.

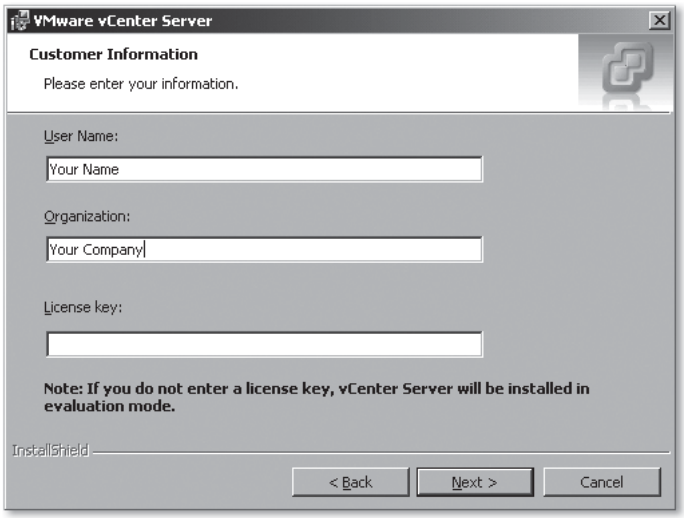


Abbildung 6.57 Software-Key für die vCenter-Installation

Anschließend haben Sie die Wahl zwischen der Nutzung einer bestehenden Datenbank und der Installation einer SQL-Server-2008-Express-Instanz mit der automatischen Anlage einer lokalen Datenbank (Abbildung 6.58).

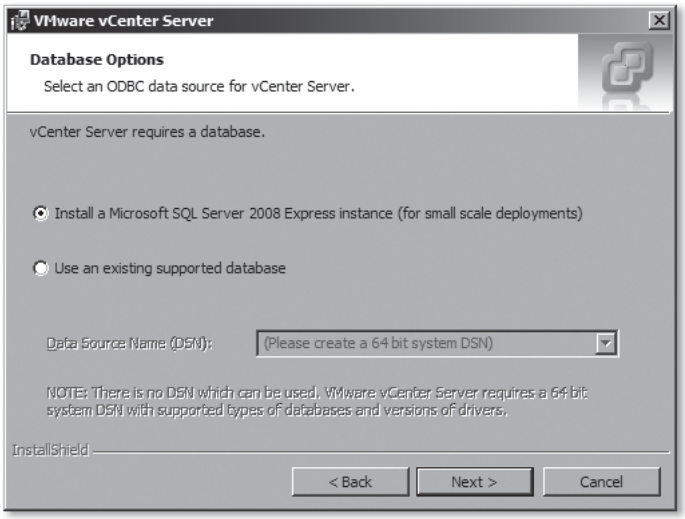


Abbildung 6.58 Angabe der vCenter-Datenbank

Diese Entscheidung treffen Sie allein durch die Aktivierung Use an existing supported database. Wählen Sie den Punkt Install a Microsoft SQL Server 2008 Express instance, stoßen Sie automatisch die SQL-2008-Express-Installation mit an, ansonsten müssen Sie die während der Vorbereitungen angelegte System-DSN iinklusive Benutzername und Passwort angegeben.

Geben Sie eine bereits bestehende Datenbank an, die schon vCenter-Informationen enthält, erscheint ein Dialog. Hier haben Sie zwei Möglichkeiten: Entweder ändern Sie die vorhandene Datenbank nicht, oder Sie löschen die existierende Datenbank komplett. Aktivieren Sie die Initialisierung durch Anklicken, werden alle bestehenden vCenter-Konfigurationen (auch alle historischen Performancewerte) gelöscht und müssen komplett neu eingerichtet werden. Dies empfiehlt sich meist bei Fehlern in der Datenbank. Wenn Sie das vCenter lediglich neu installieren, die Daten aber weiterhin Bestand haben sollen, müssen Sie immer den oberen Punkt (Abbildung 6.59) auswählen!

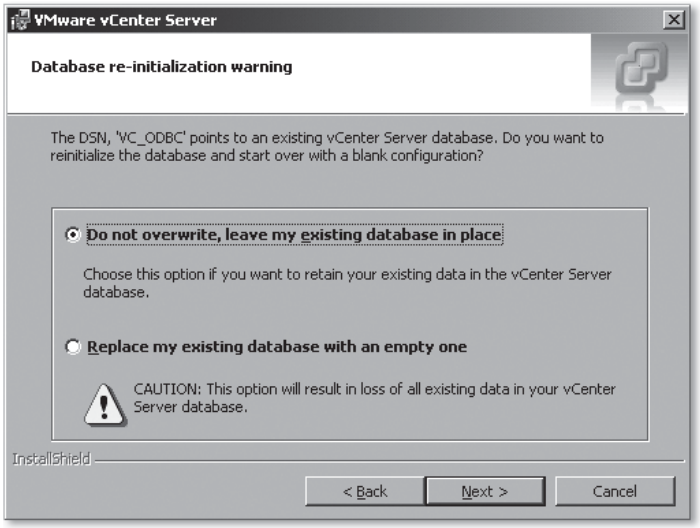


Abbildung 6.59 Abfrage bei bestehender vCenter-Datenbank

Als Nächstes folgt die Konfiguration des vCenter-Service. Entweder lassen Sie den Dienst unter einem System-Account laufen, oder Sie geben einen expliziten User-Account für den Dienst an (Abbildung 6.60). Wählen Sie einen dedizierten Account aus, wird diesem automatisch das Recht Log on as a service gewährt.

Die Auswahl der Zielordner für den vCenter-Server und den Inventory Service treffen Sie im nächsten Fenster. Die Konfiguration einer neuen Funktion des vCenter-Servers erfolgt im nächsten Schritt. Es gibt zwei Möglichkeiten, einen vCenter-Server zu nutzen (Abbildung 6.61): Entweder entscheiden Sie sich für die Variante Create a standalone VMware vCenter Server instance, oder Sie wählen die Variante Join a vCenter Server group using linked mode to share information. Was ist nun der Unterschied? Die erste Auswahl entspricht der Installationsmethode der Vorgängerversion des vCenter Servers, dem VMware Virtual Center

Server. Bei der zweiten Variante wird das vCenter in eine Gruppe von vCenter-Servern integriert, die über den vSphere-Client direkt angesprochen werden können. Diese Funktion ermöglicht Ihnen, sich an einem Punkt anzumelden, aber trotzdem die Server-Farmen und virtuellen Maschinen zu administrieren, die von anderen vCenter-Servern verwaltet werden.

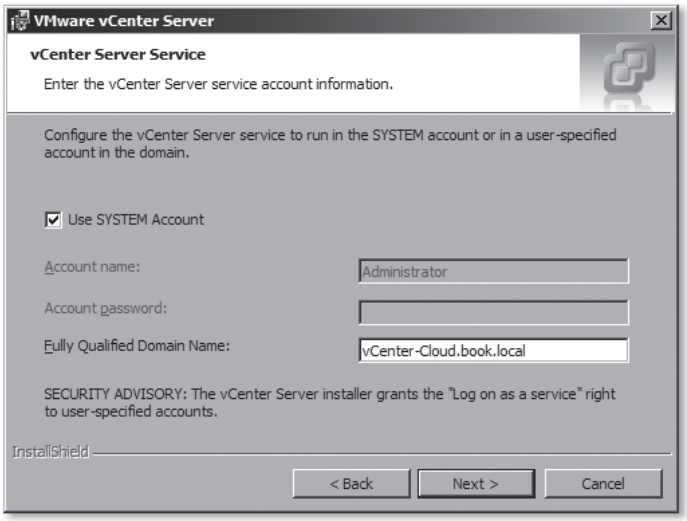


Abbildung 6.60 User-Account für den vCenter-Server-Dienst

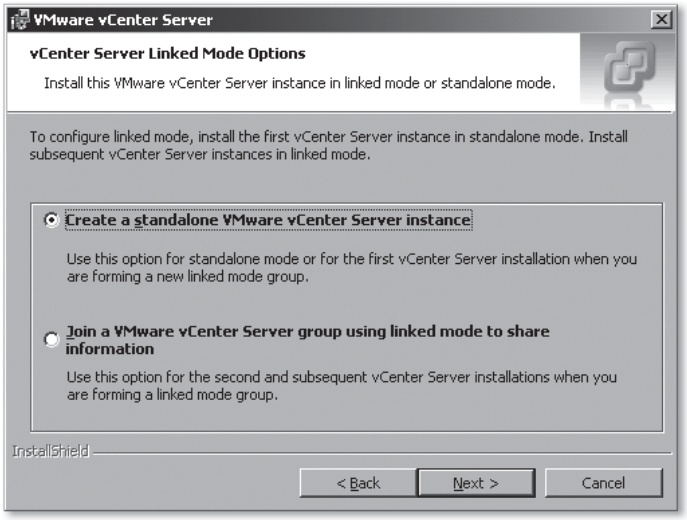


Abbildung 6.61 Auswahl des Installationstyps des vCenter-Servers

Die Standard-vCenter-Ports zur Kommunikation mit den vSphere-Servern bzw. dem Web-Access-Dienst sollten Sie wirklich nur in zwingenden Fällen vornehmen (Abbildung 6.62).

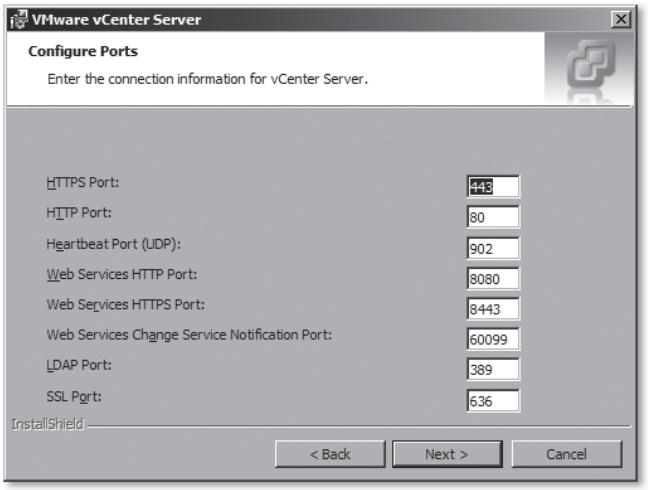


Abbildung 6.62 vCenter-Ports

Anschließend werden noch die Ports für den Inventory Service abgefragt. Auch hier ist es die beste Wahl, die vorgeschlagenen Ports zu übernehmen.

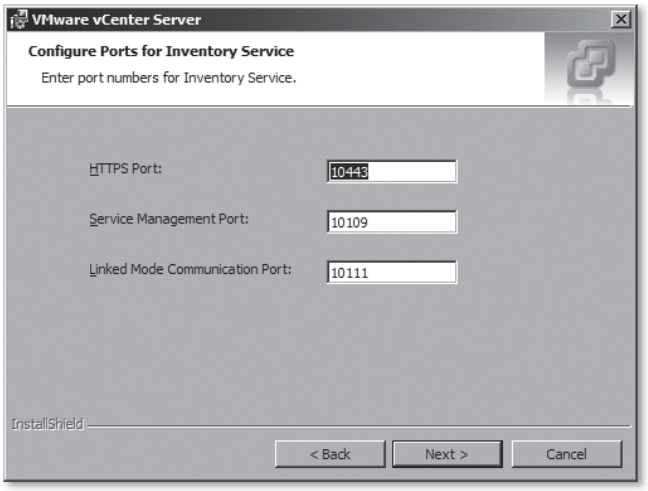


Abbildung 6.63 Ports für den Inventory-Dienst

Die Einstellungen im Dialog für die Größe der virtuellen Landschaft dienen als Basis für das automatische Setzen von Parametern. Die Konfigurationsgröße teilt sich dabei in drei Gruppen auf:

- bis 100 Hosts/1000 VMs
- 100 bis 400 Hosts/1.000 bis 4.000 VMs
- größer als 400 Hosts/4.000 VMs

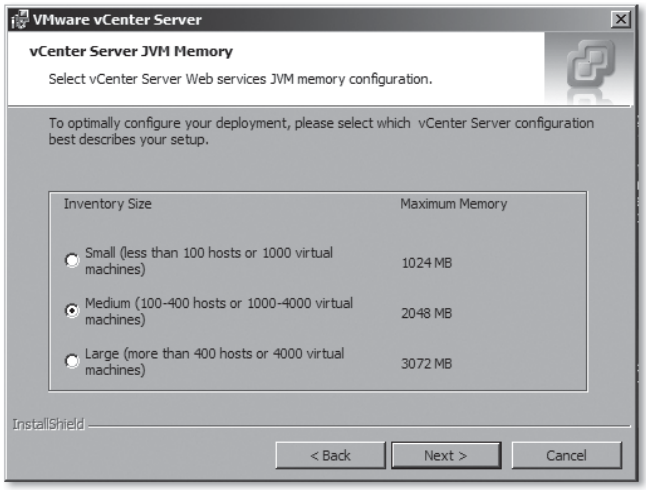


Abbildung 6.64 Einstellen der Konfigurationsgröße

Das letzte Einstellfenster war schon neu und ist mit der Version vSphere 5 neu im Programm. Auch der Dialog für die Beschleunigung des Restarts von virtuellen Maschinen findet sich zum ersten Mal in der Installationsroutine. Damit soll die Startzeit beim gleichzeitigen Starten vieler VMs drastisch reduziert werden. Zur Durchführung wird die Anzahl der parallel nutzbaren Ports erhöht.

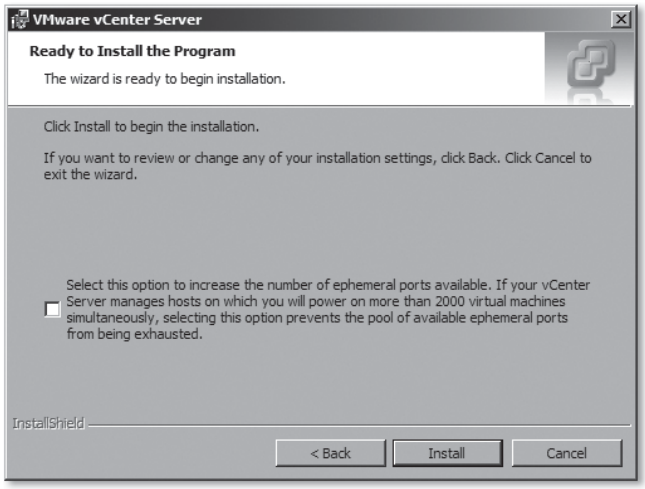


Abbildung 6.65 Anhebung der gleichzeitigen Verbindungen

Nach dem Reboot ist Ihr vCenter Server installiert, und Sie können ihn für Ihre virtuelle Infrastruktur nutzen. Im Gegensatz zur Vorgängerversion des vCenter Servers müssen Sie bei diesem Release verschiedene Komponenten händisch installieren. Automatisch wird nur der vCenter Orchestrator mitinstalliert. Ein dedizierter Lizenz-Server wird in reinen vSphere-

Umgebungen nicht mehr benötigt. Er ist integrativer Bestandteil des vCenter Servers. Betreiben Sie hingegen eine Mischumgebung, sind zwei Lizenz-Server einzusetzen: zum einen den im vCenter Server integrierten und zum anderen den aus der Virtual-Infrastructure-3.x-Umgebung bekannten Lizenz-Server. Zur Installation des alten Lizenz-Servers später mehr in diesem Kapitel auf Seite 276.

Installation vSphere-Client

Ist die Installation des Servers abgeschlossen und möchten Sie von diesem Server auf das Management Tool zugreifen, müssen Sie noch den vSphere-Client installieren. Nach dem Aufruf der *autostart.exe* der vCenter-Server-DVD wählen Sie den Punkt zur Installation des Clients.

Möchten Sie den Client auf einem anderen System installieren, haben Sie eine einfache Möglichkeit, sich die Installationsdateien herunterzuladen, ohne dass Sie die vCenter-DVD benötigen: Verbinden Sie sich über den Webbrowser mit dem vCenter Server – *https://<Name oder IP vCenter Server>*. Klicken Sie in dem folgenden Fenster auf Download vSphere-Client, liefert der vCenter Server direkt die Dateien zur Installation des Clients (Abbildung 6.66).

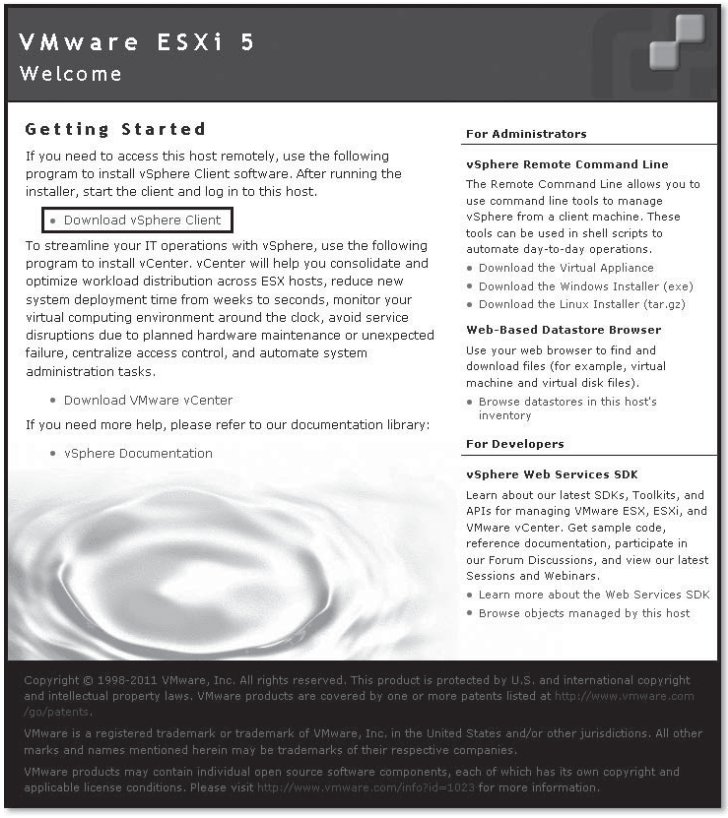


Abbildung 6.66 Download des Clients vom vCenter Server

Nach dem Download starten Sie die Installation durch den Aufruf der Datei. Damit die Installation nicht fehlschlägt, muss das .NET Framework 3.5 SP1 installiert sein. Sollte noch eine ältere Version des Clients oder der Client-Tools auf dem Computer installiert sein, ist es ratsam, die alten Versionen vorher zu deinstallieren. Andernfalls kann es zu Kompatibilitätsproblemen kommen. Haben Sie keine Bedenken, wenn Sie noch den Zugriff auf ESX-Hosts oder vCenter-Server mit einem älteren Release benötigen: Die Clients sind abwärtskompatibel, und so können Sie mit einem Client auch auf ältere Infrastrukturen zugreifen.

Die Dialoge der Installation sind selbsterklärend und bedürfen keiner großen Erklärung. Außer dem Installationspfad können Sie keine weitere Einstellung beeinflussen. Sollte Ihnen das Host Update Utility fehlen, dann haben Sie gut aufgepasst: Mit der Version 4.0 wurde es eingeführt, und mit der Version 5.0 ist es wieder von der Bildfläche verschwunden.

Rufen Sie den installierten Client auf, werden Sie, nach der Angabe des Benutzernamens und des zugehörigen Passworts, direkt mit dem vCenter-Server verbunden. Sie können Sich auch direkt mit einem vSphere-Host mit dem Client verbinden (Abbildung 6.67). Zusätzlich zu dem Server-Namen ist eine gültige Kennung mit passendem Passwort einzugeben.

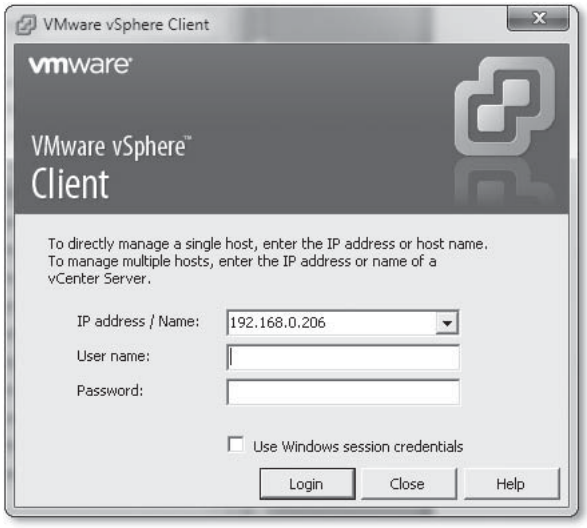


Abbildung 6.67 Client-Anmeldung

VMware vCenter Web Client (Server)

Soll der Zugriff per Webclient ermöglicht werden, so sind bei der Version 5.x des vCenter Servers dedizierte Komponenten zu installieren. Die Softwarepakete, die für diese Funktion benötigt werden, sind nicht Bestandteil der eigentlichen vCenter Installation. Für die Installation rufen Sie den Menüpunkt VMware vSphere Web Client (Server) auf und starten die Installationsroutine. Bei der Installation werden nur die Server-Komponenten installiert, was auch recht logisch ist, denn die Client-Komponente ist ja der Webbrowser.

Die ersten Dialoge sollten Sie schon fast auswendig können, also lassen wir sie einfach beiseite. Wie auch bei den anderen Komponenten sind die Ports für den Zugriff zu konfigurieren.

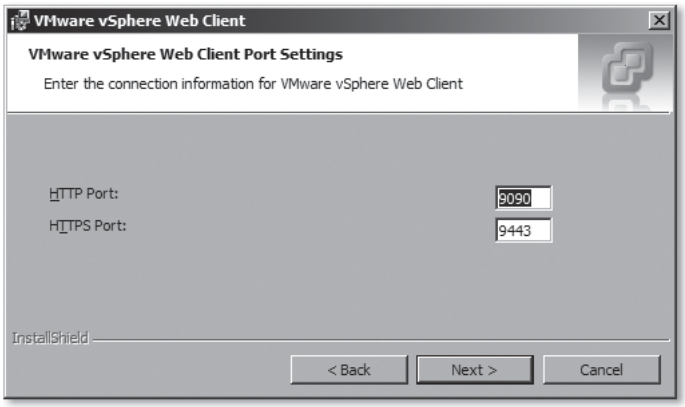


Abbildung 6.68 Konfiguration der Ports für den Webzugriff

Auch hier spricht nichts dagegen, die Ports bei den Defaulteinstellungen zu belassen. Nach der Einstellung des Installationspfads wird die Komponente installiert, und schon können Sie mit dem Browser auf Ihre Landschaft zugreifen.

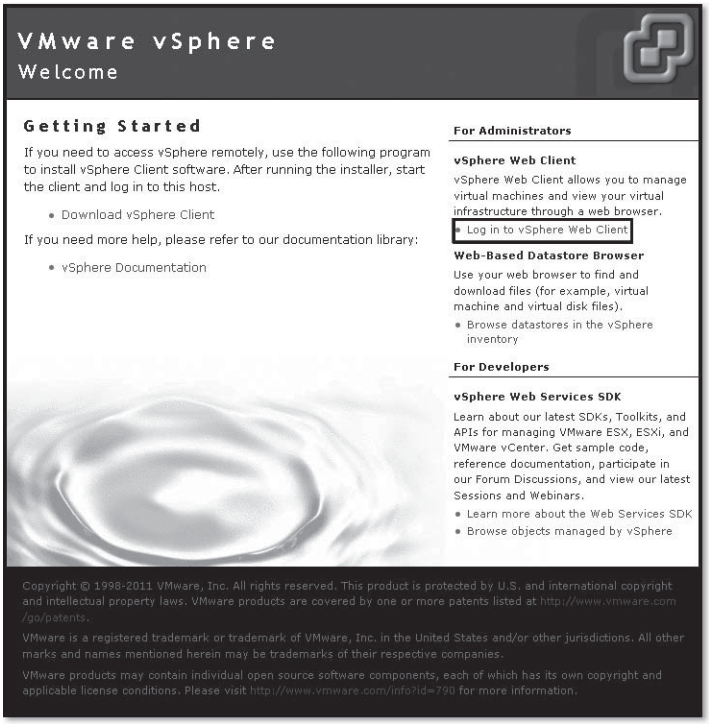


Abbildung 6.69 Aufruf des Webclients

Der Zugriff erfolgt dabei immer über das vCenter, und Sie müssen sich dann über den Link oben rechts auf die eigentliche Webclient-Anwendung durchklicken. Eine Voraussetzung ist indes nicht genannt. Möchten Sie den Client nutzen, dann benötigen Sie einen aktuellen Adobe Flash Player.

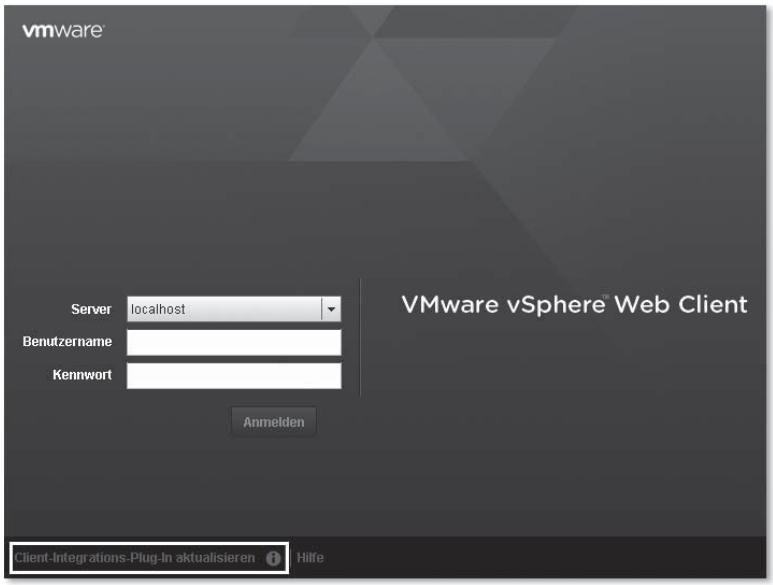


Abbildung 6.70 Anmeldefenster des Webclients

Sollte zusätzlich zur Administration der Bedarf bestehen über den Webclient auch auf die Konsole der virtuellen Maschinen zuzugreifen, dann ist das Client-Integrations-Plugin zu installieren. Das geschieht über den Link unten links im Anmeldefenster. Nach dem Durchklicken durch die bekannten Fenster können Sie auswählen, für welchen Browser Sie die Erweiterung installieren möchten.

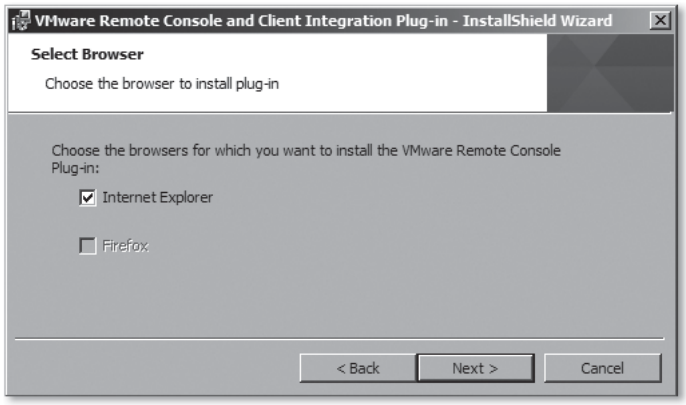


Abbildung 6.71 Browserauswahl für die Installation der Konsole

Beim Aufruf des Webclients wird die Sprache aufgerufen, die auf dem Gerät installiert ist, von dem aus der Client aufgerufen wurde. Damit Sie mit dem Webclient auf die virtuelle Infrastruktur zugreifen können, müssen Sie den vCenter Server registrieren. Nach dem erstmaligen Aufruf werden Sie automatisch auf die Registrierungswebseite weitergeleitet. Auf diese gelangen Sie aber nicht, wenn auf dem aufrufenden System kein Adobe Flash installiert ist. Nach der Flash-Installation können Sie aber die Registrierungswebseite selbst aufrufen; dazu geben Sie die folgende URL in den Browser ein: *https://<vcenter/ IP>:9443/admin-app*

Tragen Sie die geforderten Daten ein und schon können Sie Ihren vCenter Server aktivieren.

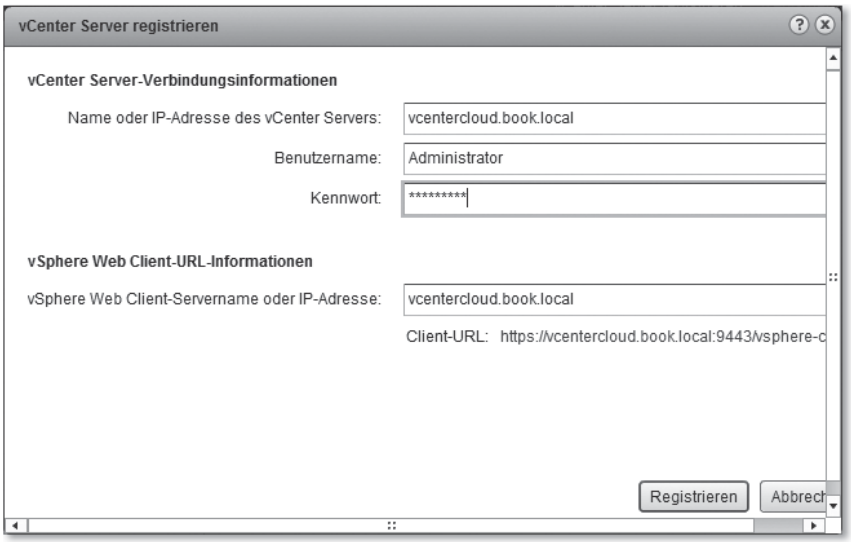


Abbildung 6.72 Registrierung des vCenter Servers für den Web-Zugriff

Nach der Registrierung wird Ihnen eine Zusammenfassung angezeigt. Dazu finden Sie auf der einen Seite den Server-Namen und auf der anderen Seite den zugehörigen SSL-Fingerprint.

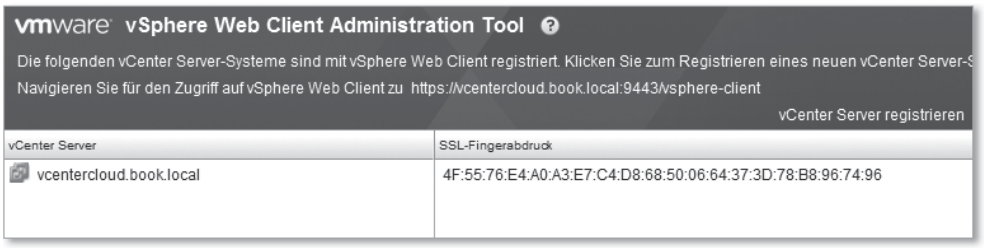


Abbildung 6.73 Erfolgreiche Webclient-Registrierung

Installation vCenter Update Manager

Die Installation des vCenter Update Managers gestaltet sich ebenfalls recht unspektakulär. Zuvor möchten wir Ihnen aber ein wichtiges Detail nicht vorenthalten.

Achtung

Der VMware Update Manager unterstützt nur noch das Patchen von vSphere-Hosts, die Aktualisierung von virtueller Hardware, die Aktualisierung von Appliances und das Patchen der VMware Tools. Betriebssysteme von virtuellen Maschinen können nicht mehr gepatcht werden.

Zum Patchen von Betriebssystemen virtueller Maschinen müssen Sie das Tool VMware Configuration Manager oder Drittanbieter-Tools nutzen.

Nach den üblichen Abfragen zu Beginn der Routine können Sie auswählen, ob die Installationsroutine sofort alle Patches herunterladen soll. Keine Angst, wenn Sie die Option deaktivieren, können Sie den Download selbstverständlich später nachholen.

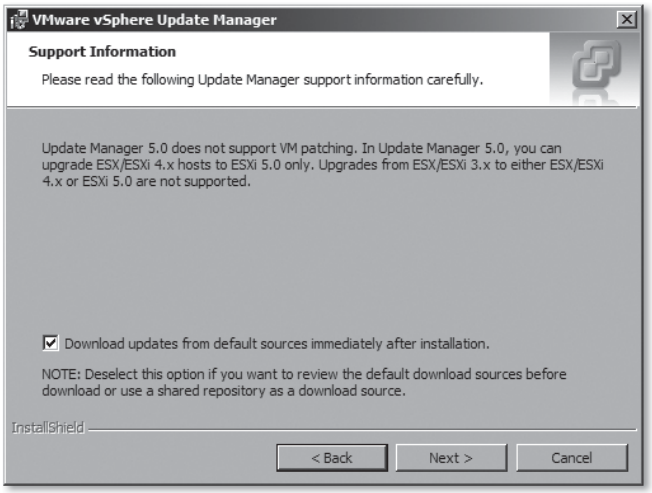


Abbildung 6.74 Automatischer Download des Patch-Repositorys

Es folgen die Parameter für die Integration des VMware Update Managers in den vCenter-Server. Dazu sind der Server-Name bzw. die Server-IP-Adresse einzugeben. Der genutzte IP-Port liegt standardmäßig auf 80. Sie können ihn an Ihre Bedürfnisse bzw. Firmen-Policies anpassen. Abschließend wird noch ein gültiger Account benötigt, der dem Update Manager die Zugriffsrechte auf das vCenter gewährt (siehe Abbildung 6.75).

Es folgt die Angabe der benutzten Zieldatenbank. Auch hier ist es, wie beim vCenter selbst, möglich, einen Microsoft-SQL-2008-Express-Datenbank-Server lokal zu installieren. Alternativ geben Sie eine gültige DSN-Verbindung zu einer bestehenden Datenbank an (Abbildung 6.76).

Wichtig

Die ODBC-Verbindung muss eine 32-Bit-Verbindung sein, unabhängig davon, ob der Datenbank-Server in 32 oder 64 Bit installiert ist.

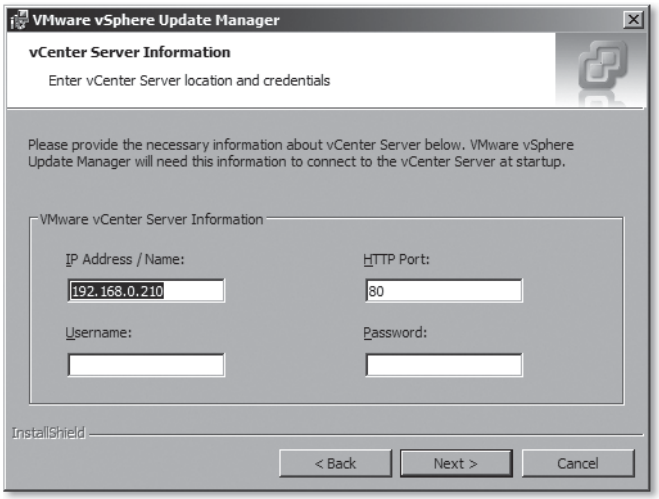


Abbildung 6.75 Update-Manager-Parameter

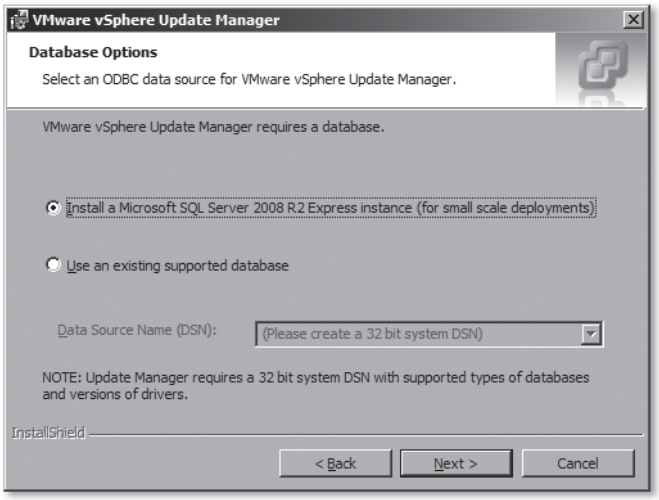


Abbildung 6.76 Konfiguration der Datenbankverbindung

Installieren Sie keine MS-SQL-Express-Datenbank-Version neu, ist im nächsten Schritt die passende Benutzerkennung nebst Passwort für die DSN-Verbindung einzugeben (Abbildung 6.77).

Wird eine bereits mit Daten gefüllte Datenbank gefunden, werden Sie gewarnt und gefragt, ob die Daten überschrieben werden sollen. Wünschen Sie, dass mit einer leeren Datenbank angefangen wird, wählen Sie JA aus. Führen Sie ein Update auf einen vorhandenen Update Manager durch und sollen die Daten in der vorhandenen Updatedatenbank erhalten bleiben, wählen Sie NEIN.

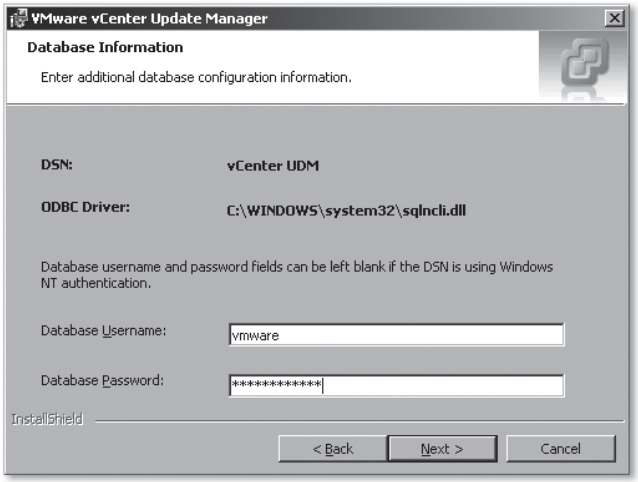


Abbildung 6.77 Accounting-Daten für die DSN-Verbindung

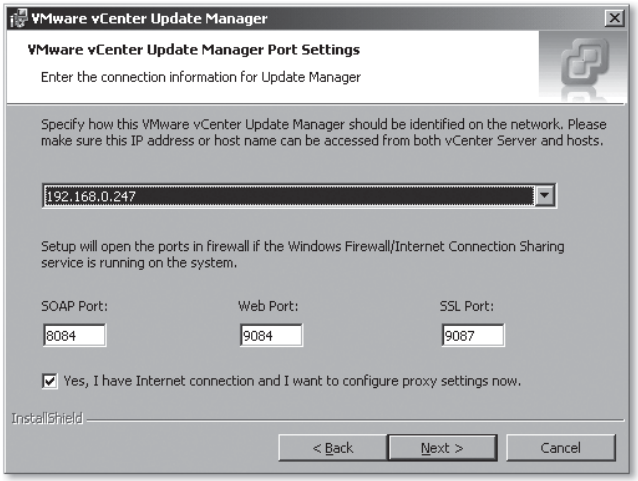


Abbildung 6.78 Portkonfiguration für den Update Manager

Die Identifizierung des vCenter Update Managers und die Konfiguration der IP-Ports finden im Folgenden statt (Abbildung 6.78). Auch wenn Sie die Applikation auf einen bereits vorhandenen vCenter-Server installieren, müssen Sie die IP-Ports nicht ändern. Mit den Defaultwerten gibt es keine Kollision.

Der Update Manager hat ein Interface, das dafür zuständig ist, die Patches für die zu patchenden Applikationen aus dem Internet zyklisch und automatisch herunterzuladen. Sollte in Ihrem Netzwerk ein Proxy-Server stehen, der das verhindert, dann können Sie während der Installation die Proxy-Konfiguration mit User und Passwort hinterlegen (Abbildung 6.79). So ist gewährleistet, dass die Patch-Datenbank immer auf dem aktuellen Stand ist.

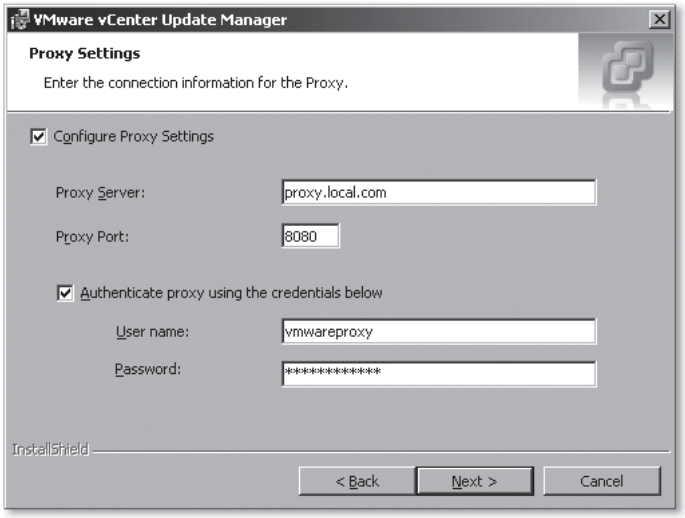


Abbildung 6.79 Proxy-Konfiguration für den Update Manager

Im folgenden Schritt sollten Sie den Pfad für das Zielverzeichnis der Patches anpassen. Nach unserer Ansicht gehören die Patches in ein separates Verzeichnis und nicht in den Profile-Ordner. Optimal ist ein eigenes Verzeichnis auf der Festplatte. Für die Berechnung des Plattenbedarfs können Sie nun auf das bereits in Abschnitt 6.3, »VMware vCenter«, erklärte Excel-Sheet zurückgreifen. Die Applikation bindet sich nahtlos in den vCenter Server ein.

Starten Sie jetzt den vSphere-Client, finden Sie an dieser Stelle zuerst einmal keine zusätzlichen Funktionen. Über den Menüpunkt PLUG-INS • PLUG-INS VERWALTEN müssen Sie zuerst die Client-Komponente für den Update Manager installieren.

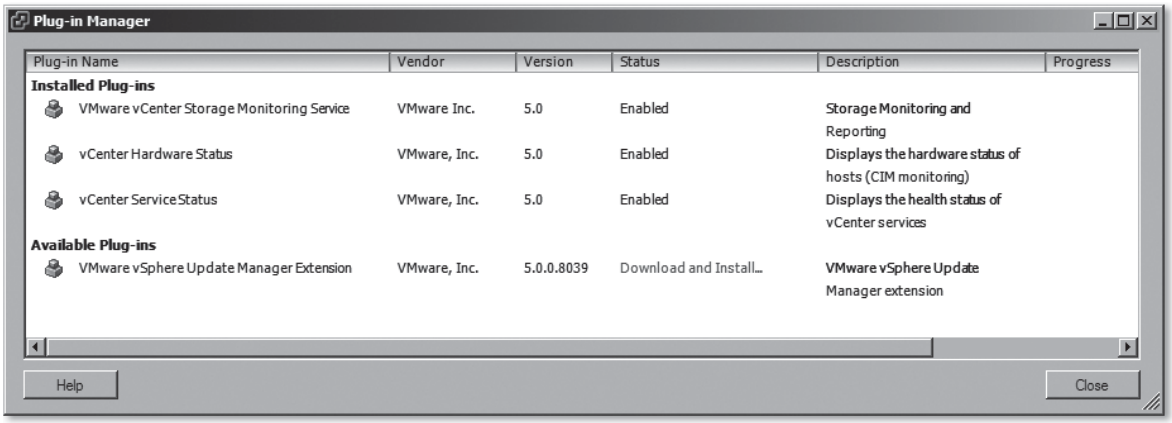


Abbildung 6.80 Auswahl des zu installierenden Plugins

Nachdem Sie die Installation des Plugins angestoßen haben und diese abgeschlossen ist, finden Sie auf der Homepage des vSphere-Clients unter dem Punkt SOLUTIONS AND APPLICATIONS eine neues Konfigurations-Icon für den Update Manager.

Nach dem Aufruf können Sie die Applikation weitergehend administrieren und konfigurieren (Abbildung 6.81).

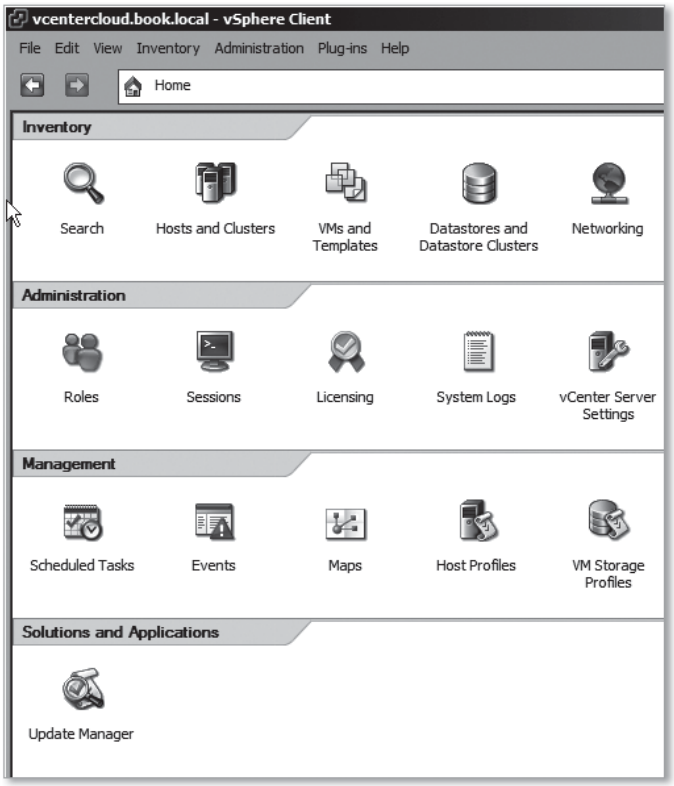


Abbildung 6.81 Update-Manager-Applikation

Installation Standalone-Download-Manager ohne Update Manager

Es ist nicht immer möglich, sich mit einer Maschine, die im Firmennetzwerk steht, ins Internet zu verbinden. Aus diesem Grund können Sie die Updates für den Update Manager mit dem Standalone-Download-Manager-Server herunterladen und per DVD auf den vCenter-Server übertragen. Diese Möglichkeit eignet sich auch, wenn Sie häufig Installationen durchführen. Die Inbetriebnahme gestaltet sich dadurch einfacher, weil der initiale Download durch den Import von der DVD ersetzt wird. Dadurch müssen Sie nicht immer das Herunterladen der vielen Patches abwarten.

Bevor Sie mit der Installation beginnen, ist es wichtig zu wissen, dass auch diese Komponente eine Datenbank benötigt. Die Auswahl ist Ihnen bereits bekannt: Entweder nutzen Sie die mit-

gelieferte MS-SQL-Express-Version, oder Sie verbinden sich via ODBC mit einer existierenden Datenbank. Die zugehörigen ODBC-Einstellungen finden Sie in Abschnitt 6.3.3, »Vorbereitung der Datenbank«.

Die Installation des Download Managers wird mit einer eigenen Installationsroutine gestartet. Sie finden sie auf dem Installationsmedium der vCenter-DVD unter *[DVD]\umds\VMware-UMDS.exe*. Ist die Installationsroutine gestartet und die entsprechende Sprachversion ausgewählt, müssen Sie das EULA bestätigen. Im folgenden Dialog geben Sie an, ob eine vorhandene Datenbank genutzt werden soll oder ob die Installationsroutine automatisch einen Microsoft SQL Express 2008 Server mitinstallieren soll. In diesem Fall arbeiten wir mit der Express-Version des Microsoft SQL Servers. Es ist nämlich sehr unwahrscheinlich, dass auf der einen Seite die Zugriffe ins Internet nicht erlaubt sind, es andererseits aber möglich ist, aus der DMZ (demilitarisierte Zone) auf ein zentrales Datenbanksystem zuzugreifen.

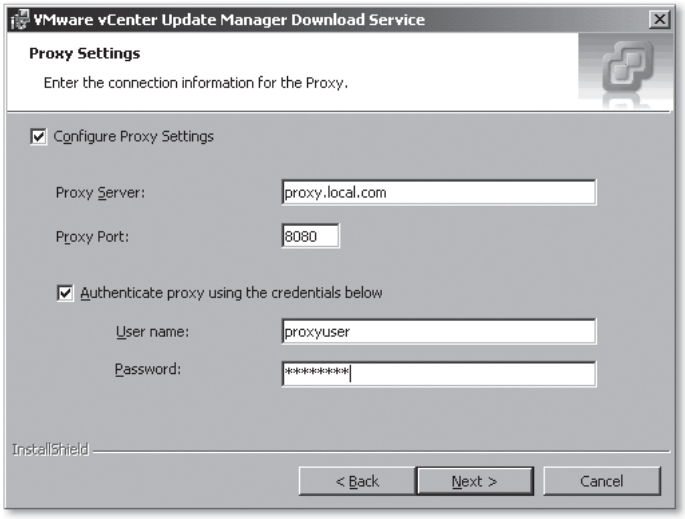


Abbildung 6.82 Proxy-Einstellungen für den Download Manager

Sollte der Zugriff auf das Internet nur über einen Proxy-Server möglich sein, sind in dem passenden Dialog die Einstellungen vorzunehmen (Abbildung 6.82). Jetzt benötigt die Routine die Angabe des Installationspfads. Auch das Zielverzeichnis für das Patch-Repository ist anzugeben. Nach der Festlegung des Pfades wird überprüft, ob mindestens 120 GB Plattenplatz frei sind. Ist das nicht der Fall, erhalten Sie eine Warnmeldung (Abbildung 6.83).

Der angegebene Pfad in der Fehlermeldung verweist auf das Excel-Sheet das die Sizing-Angaben für die Datenbank und das Patch-Repository enthält. Sollte die Prüfung ergeben, dass Softwarevoraussetzungen fehlen, erscheint ein Hinweis, und das Defizit wird behoben. Nach dem Abschluss der Installationsroutine ist ein Reboot erforderlich. Nach der Installation findet sich das Tool im Installationsverzeichnis. Sie kommen bei der Nutzung des Tools an der Kommandozeile nicht vorbei; ein GUI gibt es für diese Softwarekomponente nicht.

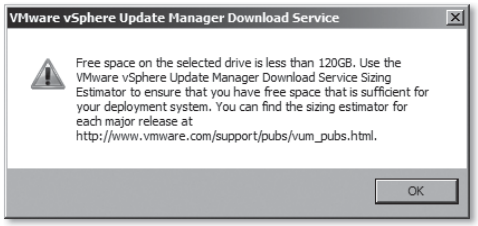


Abbildung 6.83 Plattenplatzwarnung der Installationsroutine

Installation vSphere ESXi Dump Collector

Eine neue Applikation hat VMware mit auf die Installations-DVD des vCenter Servers gepackt: Der Dump Collector ist eine zentrale Instanz, die Memory-Dumps des VMkernels von ESXi-Servern sammelt. Dieses Tool ist notwendig geworden, weil VMware es Ihnen ermöglicht, einen ESXi-Server nur im Arbeitsspeicher laufen zu lassen und damit ohne lokale Festplatte zu arbeiten. Der Dump Collector ist somit die zentrale Instanz, die sich um die Dumps kümmert. Konfigurieren können Sie die entsprechenden Einstellungen auch auf Hosts mit lokaler ESXi-Installation. Die Dumps liegen dann an zwei Stellen: zum einen lokal auf der Festplatte des Hosts und zentral auf dem Dump Collector. Installieren können Sie das System direkt auf dem vCenter-Server oder auf jeder anderen Windows-Maschine.

Hinweis

Das Management-Netzwerk darf nicht auf einem Distributed Switch konfiguriert sein. Etherchannel bzw. LACP ist ebenso wenig supportet wie IPv4.

Kommen wir nun zur Installation. Sind Sie bei dem Dialog angekommen, in dem Sie die Pfade für die Applikation angeben können, haben Sie, wie schon beim Update Manager, zwei zu konfigurierenden Pfadangaben: den Applikationspfad und das Ziel für die Memory-Dumps. Das Dump-Ziel kann sowohl lokal als auch im Netzwerk liegen. (siehe Abbildung 6.84)

Die Größe des Repositorys ist abhängig von der Anzahl der ESX-Hosts, die ihre Daten in das Ziel schreiben sollen. Unabhängig davon, wo die Daten abgelegt werden, sollte auf jeden Fall der entsprechende Plattenplatz auch nutzbar sein. Als Nächstes kommt die Abfrage, ob Sie die Installation auf den vCenter oder auf einem anderen Server vornehmen wollen. Bei einer Standalone-Installation müssen Sie noch den IP-Port festlegen und angeben, wie der Collector im Netz bekanntgemacht werden soll.

Bei der Installation auf dem vCenter-Server werden, ähnlich wie beim Update Manager, noch die folgenden Angaben benötigt: Name des vCenters, vCenter-Account mit zugehörigem Passwort und der IP-Port für dessen Zugriff. Den IP-Port für den Collector (Standard: 6500) übergeben Sie im folgenden Dialog und geben abschließend an, wie der Dump Collector im Netz erreichbar ist. Damit ist die Installation beendet, und wir können uns der nächsten Komponente zuwenden.

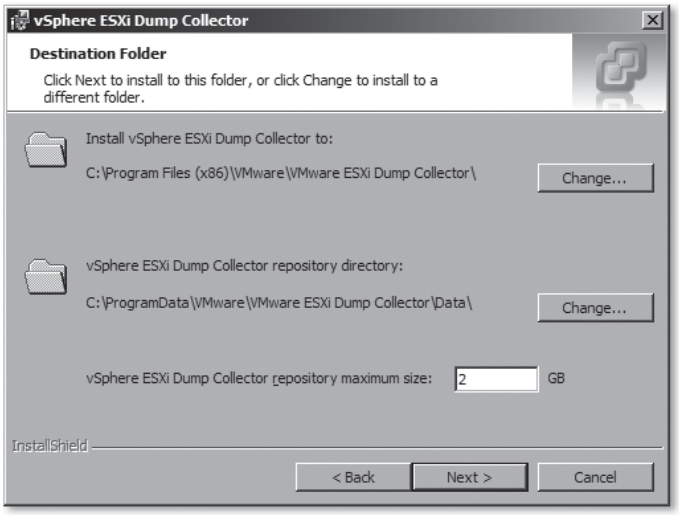


Abbildung 6.84 Dump Collector – Festlegen der Pfade und der Repository-Größe

Installation VMware Syslog Collector

Der Syslog Collector ist, analog zum Dump Collector, ein zentrales Management Tool, das die Syslogs der ESXi-Hosts auf einem zentralen Server sammelt. Die Voraussetzungen entsprechen denen des Dump Collector. Auch hier wird der Service an eine IPv4-Adresse gebunden. Somit kann der Dienst nur auf einem reinen IPv4- oder auf einem IPv4/IPv6-Misch-System installiert werden. Das Eingabefenster der Pfadangabe erfragt auch hier weitere Parameter. Die Repository-Größe spielt hier ebenso eine Rolle wie die Anzahl der zu behaltenden Log-Dateien, bevor durchgerollt wird.

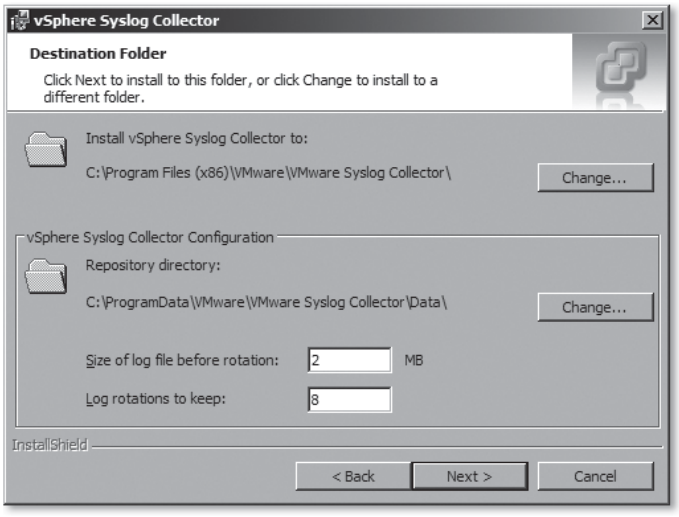


Abbildung 6.85 Pfadangabe für den Syslog Collector und Repository-Konfiguration

Es gibt zwei Optionen der Installation: standalone oder auf dem vCenter selbst. Die Eingabe variiert. Die Standalone-Installation fragt nach den Ports für die Kommunikation.

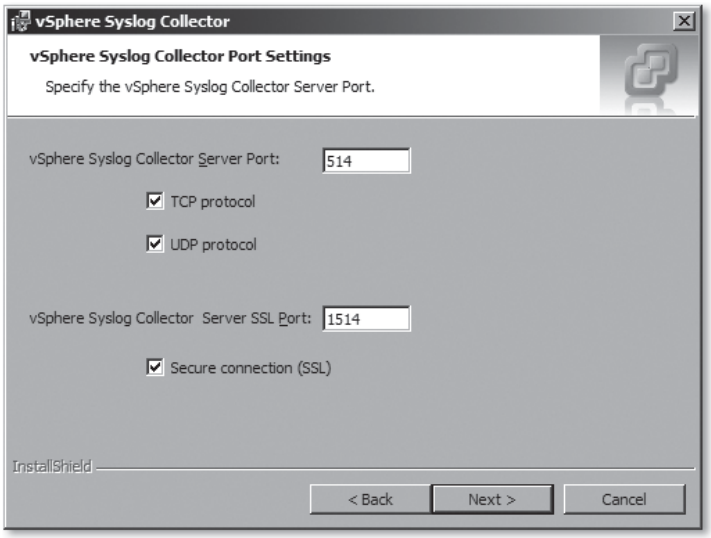


Abbildung 6.86 IP-Ports des Syslog Collectors

Die IP-Adresse, über die der Dienst über das Netzwerk angesprochen werden kann, ist die letzte Eingabe vor der Aktivierung des Installers. Bei der vCenter-Installation werden zu Beginn wieder die Angaben für den vCenter Server angefragt; neben dem Namen, dem IP-Port und einer Benutzerkennung mit entsprechendem Passwort werden in diesem Fenster keine Angaben gefordert. Jetzt folgen die gleichen Angaben, wie sie auch die Standalone-Installationsroutine fordert. Die mit vSphere 5.0 neue erschienene Komponente ist nun ebenfalls betriebsbereit und kann nun konfiguriert werden.

Installation VMware Image Builder

Eine Funktion, die schon lange gefehlt hat, ist mit vSphere 5.x ins Release gewandert: VMware hat den vSphere Image Builder vorgestellt. Diese Erweiterung des PowerCLI gibt Ihnen das Arbeitsmittel an die Hand, eigene Installationsimages herzustellen. Sie können dabei ein Image für die ESXi-Installation nehmen und nachträglich erschienene Patches integrieren. Eine Aufnahme von Treibern in das Image ist ebenfalls eine Option. Selbstverständlich können Sie anschließend ein neues ISO-File erstellen und damit wiederum einen neuen Host installieren. Mit dieser Funktion können Sie sich die Patch-Orgien sparen und müssen auch nicht immer auf die hardwareherstellerspezifischen Images warten. Sie können sich einfach ein angepasstes Installationsimage selbst konfigurieren und nutzen, sobald die Patches bzw. Treiber verfügbar sind.

Eine eigene Installationsroutine gibt es für den VMware Image Builder nicht. Die Komponente ist Teil des PowerCLI und wird mit diesem zusammen installiert.

Lassen Sie uns einen kurzen Blick auf den Image Builder und seine Funktion werfen. Dazu möchten wir zuallererst ein paar neue Begriffe klären. VMware nutzt im Rahmen des Auto Deploys und des Image Builders die Bezeichnungen *VIB*, *Depot* und *Profil*. Was ist damit gemeint?

Begriff	Erklärung
VIB	Ein VIB, VMware Infrastructure Bundle, ist ein Softwarepaket, das VMware oder andere Hersteller zur Verfügung stellen. Diese Pakete können Treiber, Erweiterungen, CIM Provider oder andere VMware-Komponenten und -Erweiterungen enthalten.
Depot	Eine Ablage, wo der Image Builder die Installationskomponenten finden kann. Das dafür benötigte Offlinebundle können Sie in der Basisversion bei VMware herunterladen. Es handelt sich dabei um die ZIP-Datei der ESXi-Version. Das Depot muss nicht zwingend auf dem lokalen Server liegen, es kann auch nur über einer URL erreichbar sein. Es ist möglich, mehrere Depots zu haben.
Profil	Das Profil fasst verschiedene Komponenten zusammen und bildet die Basis für die Installation eines Hosts.

Tabelle 6.3 Image-Builder-Begriffe

Ein Bild sagt mehr als tausend Worte, deshalb lassen Sie uns kurz einmal auf die Struktur des Image Builders eingehen.

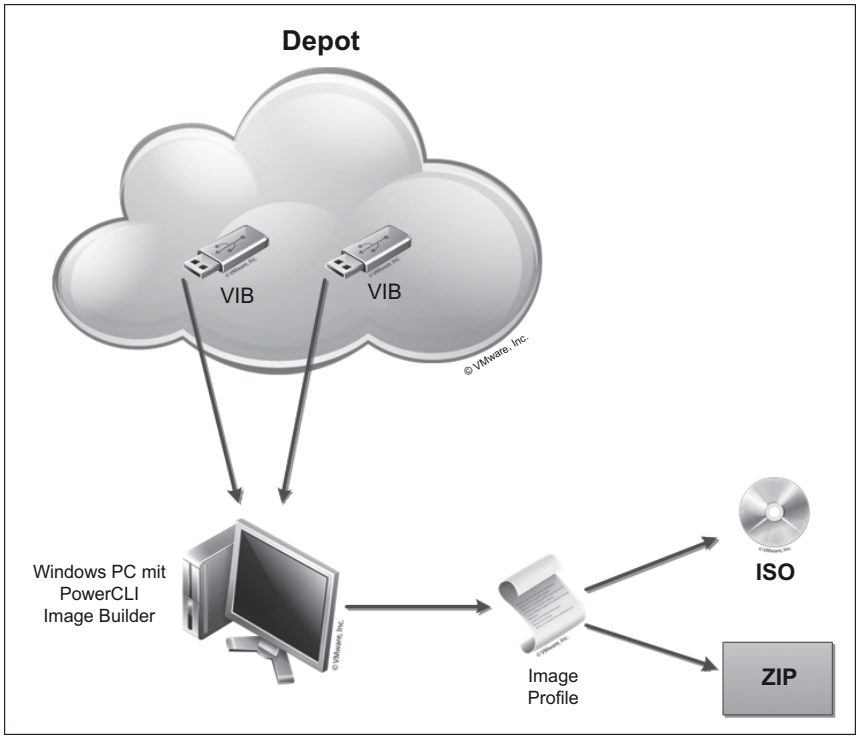


Abbildung 6.87 Image-Builder-Architektur

Mit den Befehlserweiterungen des PowerCLI für den Image Builder werden Ihnen die Befehle zur Verfügung gestellt, die Sie benötigen, um die Depots zu verwalten und die Profile zu erstellen. Letztendlich können Sie mit den Softwarekomponenten im Depot und den Profilen ein neues ISO für die Installation mit dem klassischen Medium erstellen, oder Sie erzeugen eine ZIP-Datei, die später wiederum als Basis für ein Depot dienen kann. Sie können das erstellte ISO auch nutzen, um per Auto Deploy einen Server neu zu betanken.

Installation VMware Auto Deploy

Ein ganz neues Tool, ebenfalls erstmalig mit der Version 5.0 von VMware vSphere veröffentlicht, ist der VMware Auto Deploy Server. Der Server gibt Ihnen die Mittel an die Hand, um vSphere-Hosts automatisch zu installieren und somit die Bereitstellung von VMware-Maschinen drastisch zu vereinfachen.

Auf den ersten Blick ist es »just an other boring« Installations-Server, wie es zum Beispiel die EDA-Appliance ist oder andere Auto-Installations-Server, die es am Markt gibt. Aber beim näheren Hinschauen kann das System doch einiges mehr. Es ist wohl überflüssig zu sagen, dass das System selbstverständlich auf die Installation von ESX-Systemen spezialisiert ist und somit keinen weiteren Ballast für die Installation anderer Systeme mit sich schleppt. Aber es hat die Möglichkeit, ohne eine Installation einen ESX-Server zu starten. Falls Sie sich fragen, wie das funktioniert: Der Server nutzt die üblichen Tools, um ein Image in den Speicher eines Hosts zu laden und zu starten. Sie brauchen also keine lokalen Platten im Server mehr. Das System nimmt sich einfach den Hauptspeicher, nimmt anschließend mit dem Hostprofil alle Konfigurationsanpassungen vor – fertig. Der Vorteil wird bei näherer Betrachtung ganz schnell klar: Stellen Sie sich vor, Sie haben eine Landschaft mit 50 Hosts und 120 virtuellen Maschinen. Nun steht ein Update an. Mit vMotion und dem Update Manager können Sie das Update fahren, und nach einer definierten Zeit wären alle Hosts neu installiert. Haben Sie keine lokale Installation, ist nur das Image zu tauschen, und beim nächsten Reboot wird der Host mit der neuen Version bereitgestellt.

Zu Beginn müssen Sie eine ESXi-Image-Datei erstellen und sie um alle Komponenten erweitern, die auf Ihren Hosts benötigt werden. Alle aktuellen Patches integrieren Sie ebenfalls integriert. Das Image erklären Sie zum Depot und verbinden es mit der MAC-Adresse des zu installierenden Hosts. Beim Boot des Servers wird der TFTP-Server angesprochen, der die Verbindung zum Auto Deploy Server sucht und anhand der MAC-Adresse das zugehörige Image bereitstellt.

Für die Einrichtung der Software selbst ist nur die beschriebene Installation auf dem vCenter Server durchzuführen. Für das Funktionieren der Applikation sind aber noch zusätzliche Applikationen auf dem Auto-Deploy-System bereitzustellen.

Zusätzlich benötigte Komponenten

- Microsoft PowerShell 2.0
- VMware PowerCLI 5.0
- TFTP Server
- DHCP-Server

Auf die Installation der weiteren Komponenten möchten wir an dieser Stelle nicht tiefer eingehen. VMware Auto Deploy unterstützt sowohl IPv4- als auch IPv6-Adressen. Sie können nicht einen Auto-Deploy-Server für mehrere Umgebungen benutzen, jeder vCenter-Server braucht zwingend seinen eigenen Auto-Deploy-Server. Das muss nicht auf dem vCenter selbst sein, aber es gibt hier eindeutig eine 1:1-Beziehung.

Die Installation ist ebenso einfach wie bei den beiden Komponenten zuvor. Neben der Pfadangabe für Applikation und Repository werden Sie auch hier gefragt, wie groß das Repository werden soll.

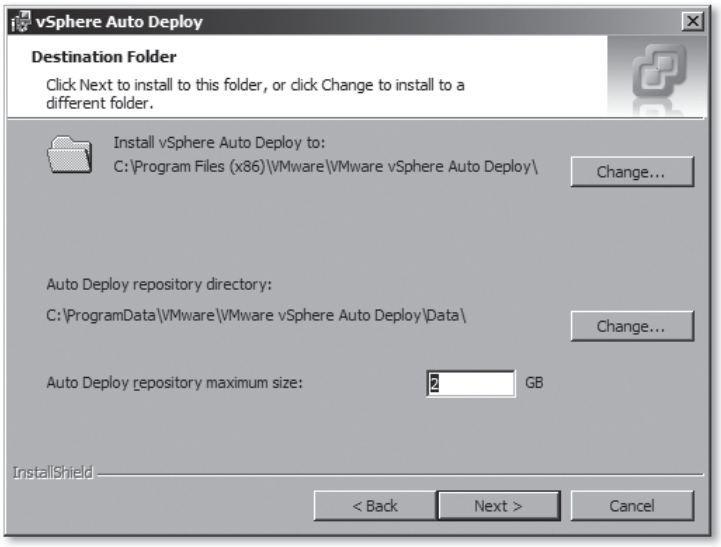


Abbildung 6.88 Auto-Deploy-Pfad und Repository-Größe

Es folgen nun – Sie kennen es schon – die Festlegung des IP-Ports (Standard: 6501) und die Identifikation des Dienstes im Netzwerk. Damit ist die Installation abgeschlossen, und Sie können sich der nächsten Funktion widmen.

Installation VMware vSphere Authentication Proxy

Der VMware Authentication Proxy ist ein Service, der die Sicherheit in VMware-Umgebungen erhöhen soll. Er ermöglicht die Aufnahme von ESXi-Hosts in ein Active Directory, ohne direkt

mit einem Domänenaccount arbeiten zu müssen. Der Vorteil dieser Vorgehensweise wird klar, wenn Sie sich die Funktionen des Auto-Deploy-Dienstes ansehen: Zur automatischen Funktion des Deployments müsste in der Konfiguration eine Kennung und ein Passwort hinterlegt werden. Mit der gewählten Vorgehensweise erhöht sich die Sicherheit in PXE-Umgebungen. Die Aufnahme des Servers erfolgt in diesem Fall mit der Angabe der Active-Directory-Domain und der IP-Adresse des Authentication Proxys.

Achtung

Der Authentication Proxy benötigt den Microsoft IIS-Server für seine Funktion. Der IP-Port 80 des IIS kollidiert aber mit dem vCenter Server. Sie haben also zwei Optionen: Passen Sie entweder den Port des IIS oder den Port des vCenters an. Letzteres funktioniert nur optimal, wenn Sie das vCenter und seine Komponenten noch nicht installiert haben.

Wird die Konfigurationsanpassung nicht vorgenommen, startet das vCenter nicht mehr.

Die Installation läuft in dem schon bekannten Muster ab. Hier haben Sie nicht die Option, den Dienst auf einer separaten Maschine bereitzustellen. Die Komponente ist auf dem vCenter Server zu installieren. Bei fehlender IIS-Installation erhalten Sie eine detaillierte Fehlermeldung.

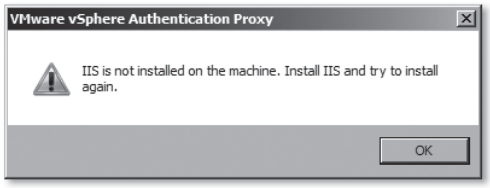


Abbildung 6.89 Fehlende IIS-Installation

Es folgen die Daten für die Verbindung mit dem vCenter-Server und die Auswahl, wie der Dienst über das Netzwerk erreichbar ist, und damit ist die Installation beendet. Achten Sie bitte darauf, dass die Verbindung mit dem IIS-Server hergestellt wird; aus diesem Grund müssen Sie beim IP-Port den Port des IIS-Servers angeben.

Zur einwandfreien Funktion des Authentication Proxys wird, wenn man näher darüber nachdenkt, ein Domänen-Account benötigt, damit sich der Proxy-Dienst gestartet werden kann. Diese Arbeit brauchen Sie nicht per Hand durchzuführen, das übernimmt die Installationsroutine für Sie. Es wird automatisch ein Domänenaccount angelegt, der die notwendigen Rechte besitzt, um einwandfrei arbeiten zu können. Dieser Benutzer beginnt mit der Zeichenkette »CAM-«, und er bekommt ein zufällig vergebenes 32-stelliges Passwort. Das Passwort läuft nicht ab.

Achtung

Bitte ändern Sie keine Parameter an dem Account!

Installation vCenter Converter

Auch der vCenter Converter wird über eine eigene Installationsroutine bereitgestellt. Dieses Tool wird genutzt, um Computersysteme in die virtuelle Infrastruktur zu importieren, wobei Sie die Parameter der zu importierenden Maschine während des Vorgangs anpassen können.

Mit der Version 5.0 ist der vCenter Converter nicht mehr Bestandteil der vCenter-DVD. Auf der Webseite von VMware findet sich nur noch die Standalone-Version, die ins vCenter integrierte Version sucht man vergebens.

Installation in einer virtuellen Maschine

Wurde seitens VMware die Sinnhaftigkeit eines vCenter Servers in einer virtuellen Maschine zu Zeiten einer Version 1.x noch beharrlich bestritten, wird seit Version 2.x diese Lösung als sehr vorteilhaft angepriesen. Dass es die Version vCenter 5.x auch als Appliance gibt, unterstreicht diesen Punkt zusätzlich. Die Vorteile liegen wirklich auf der Hand, da das System in der virtuellen Maschine auch deren Eigenschaften der unabhängigen Hardware und schnellen Wiederherstellbarkeit genießt. Zusätzlich fördert die VMware-HA-Funktion die Ausfallsicherheit.

Allerdings bestehen auch folgende zwei Nachteile, die Sie bei Ihrer Entscheidung, ob Sie die virtuelle oder die physische Variante wählen, im Vorfeld berücksichtigen sollten:

1. **Verwaltungssicherheit**
   Unabhängig von HA besteht bei einem Ausfall der virtuellen Infrastruktur die Gefahr, dass das betreuende Betriebsteam sich ohne den vCenter-Zugriff nicht zu helfen weiß und so der Wiederanlauf erschwert wird. Daher sollten Sie auf jeden Fall immer wissen, auf welchem Server die vCenter-VM läuft, und dem Betrieb den direkten vSphere-Client-Zugriff auf diesen vSphere-Server erklären. Alternativ bieten sich kleine Programme an, die automatisch die vCenter-VM (und gegebenenfalls Datenbank-Server) gezielt neu starten.
2. **Performance**
   Die Leistungsfähigkeit einer VM wird vor allem durch die Konsolidierung mehrerer Systeme auf eine Hardware eventuell eingeschränkt. Wird die virtuelle Infrastruktur zu groß und umfasst mehrere Hundert virtuelle Maschinen, ist womöglich die komplette Leistungsfähigkeit eines physischen Systems nötig, um schnelle Antwortzeiten zu gewährleisten.

Was ist nun zu beachten, wenn Sie den vCenter Server auf einer virtuellen Maschine installieren, und wie viele Ressourcen werden für die VM benötigt? Auch wenn VMware mindestens zwei CPUs für einen vCenter-Server fordert, so zeigt doch die Praxis, dass in kleinen Umgebungen auch eine CPU ausreichend ist. In Tabelle 6.4 haben wir einmal eine Auflistung zusammengestellt, wann wie viele Ressourcen für den vCenter-Server nötig sind, ohne dass die Datenbank mit auf dem System läuft, aber mit installierten Webclient.

Anzahl ESXi-Hosts	Anzahl VMs	CPUs (64 Bit)	Memory	Betriebssystem
≤ 100	≥ 1000	2	6 GB	Windows 64 Bit
≥ 100 ≤ 400	≤ 1000 ≥ 4000	2	10 GB	Windows 64 Bit
≥ 400	≤ 4000	2	15 GB	Windows 64 Bit

Tabelle 6.4 Ressourcenbedarf des vCenters Servers

Damit Sie den vCenter-Server in der virtuellen Umgebung auch wiederfinden, sollten Sie die entsprechende VM fest auf einem Host »verankern«. Dazu bietet sich entweder der erste oder der letzte Host in einer Farm an. Deaktivieren Sie das DRS für die virtuelle Maschine, auf der der vCenter Server aktiv ist. Bei den HA-Einstellungen für den virtuellen Server ist das Startup-Level auf HIGH zu setzen. Vernachlässigen Sie dabei nicht die virtuellen Server, die weitere wichtige Dienste für den vCenter-Server zur Verfügung stellen, wie z. B. ADS, DNS und den zugehörigen Datenbank-Server. Der virtuelle vCenter-Server startet nur einwandfrei, wenn die oben beschriebenen Dienste zur Verfügung stehen. Aus diesem Grund sollten Sie bei den Systemen, die ebenfalls virtuell sind, die Startpriorität heraufsetzen.

Zu guter Letzt sollten Sie die Shares der vCenter-VM auf HIGH setzen, damit immer genug Ressourcen für das Management der virtuellen Infrastruktur zur Verfügung stehen.

Einzelinstallation VMware-Lizenz-Server

In bestimmten Fällen, z. B. aufgrund von Unternehmensvorgaben, ist es notwendig, den Lizenz-Server des vCenters unabhängig von diesem auf einem anderen System zu installieren. Diese Vorgehensweise ist aber nur für einen Lizenz-Server möglich, der zusätzlich in einer Mischumgebung benötigt wird. Der Server für die noch vorhandenen VI3.x-Systeme kann separiert werden. Der Lizenz-Server für vSphere ist integraler Bestandteil des vCenters und kann nicht getrennt werden. Den getrennten VI3.x-Lizenz-Server können Sie mittels Download-Paket oder über die Installations-DVD (VI3.x) (Verzeichnis *VMware-VIMSetup-2.5.0-ESXi#\vpx\VMware-licenseserver.exe*) installieren.

Die Installation erfordert nur die Angabe eines Ports, den Sie bei Abweichung von 27000 dem vCenter-Server und den betroffenen VMware-vSphere-Servern mitteilen müssen. In jedem Fall müssen Sie die Netzwerkverbindung und die Portfreigabe (Firewall) gewährleisten. Würde die Verbindung zwischen vSphere-/VC-Server und dem Lizenz-Server für mehr als 14 Tage unterbrochen, wäre danach kein Neustart der virtuellen Maschinen mehr möglich.

Plugins

Mit der Version 3.5 wurde eine neue Schnittstelle im Virtual Center eingeführt. Diese sogenannte Plugin-Schnittstelle hat auch in der neuen Version 5.0 des vCenters weiterhin Bestand. So bindet sich z. B. der Update Manager als Plugin ins vCenter ein.

Abbildung 6.90 Verwaltung der Plugins

Die Plugins erreichen und verwalten Sie nach der erfolgreichen Verbindung mit einem vCenter-Server über PLUG-INS • PLUG-INS VERWALTEN (Abbildung 6.90).

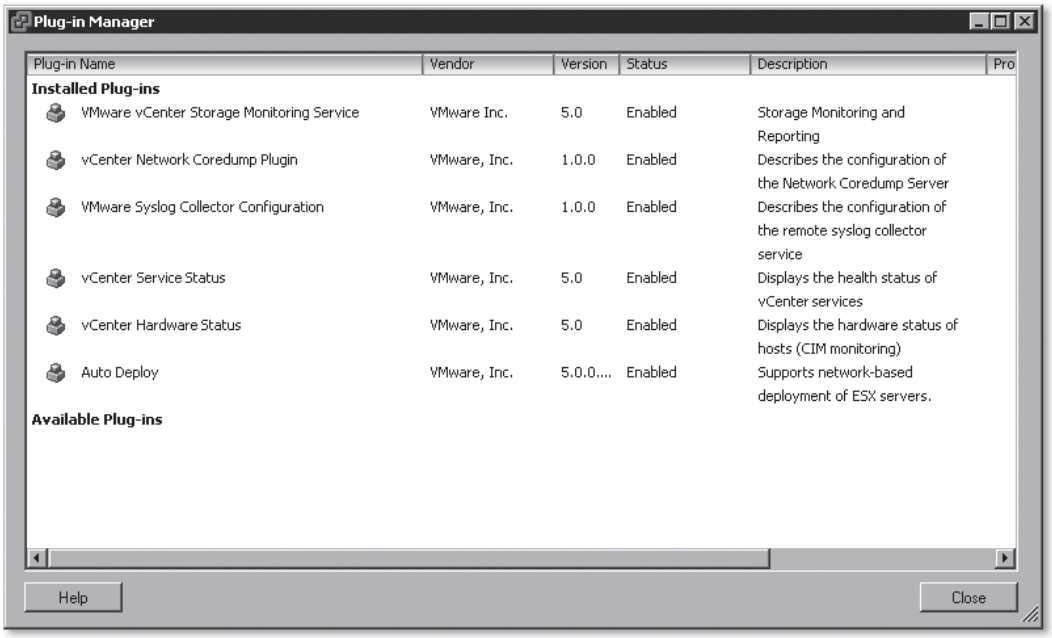


Abbildung 6.91 Verfügbare und bereits installierte Plugins

Innerhalb des Plug-in Managers (Abbildung 6.91 sehen Sie verfügbare und bereits installierte Plugins. Die Plugins werden auf dem Client-PC installiert und kommunizieren von dort mit dem vCenter.

Über das Kontextmenü aktivieren oder deaktivieren Sie die Plugins. Stehen Plugins zur Auswahl, die noch nicht installiert und aktiviert sind, dann führt ein Klick auf HERUNTERLADEN UND INSTALLIEREN genau die beschriebene Aktion durch.

6.3.5 vCenter-Protokolldateien

Damit eine erfolgreiche Analyse von möglicherweise auftretenden Problemen durchgeführt werden kann, sollten Sie wissen, wo die Dateien liegen, denen Sie nähere Informationen entlocken können. Die Dateien finden Sie in den folgenden Verzeichnissen.

Protokoll	Pfad
Installationsprotokoll	*%tmp%\vim*.log*
vCenter-Server- und Datenbankzugriff	*%ALLUSERSPROFILE%\VMware\VMware VirtualCenter\Logs*
Inventory Service	*%ALLUSERSPROFILE%\ VMware\Infrastructure\ Inventory Service\Logs*
Profile-Driven Storage	*%ALLUSERSPROFILE%\ VMware\Infrastructure\ Profile-Driven Storage\Logs*
vCenter-Update-Manager- und Datenbankzugriff	*%ALLUSERSPROFILE%\ VMware\ VMware Update Manager\Logs*
VMware Auto Deploy	*%ALLUSERSPROFILE%\ VMware\ VMware vSphere Auto Deploy\Logs*
vSphere ESXi Dump Collector	*%ALLUSERSPROFILE%\ VMware\ VMware ESXi Dump Collector\Logs*
VMware Syslog Collector	*%ALLUSERSPROFILE%\ VMware\ VMware Syslog Collector\Logs*
VMware vCenter Converter Standalone	*%ALLUSERSPROFILE%\ VMware\ VMware vCenter Converter Standalone\Logs*

Tabelle 6.5 Pfade zu den Protokolldateien der vCenter-Komponenten

6.4 VMware vCenter Server-Appliance

Sehr interessant ist eine neue Appliance, die VMware auf den Markt gebracht hat: VMware bietet nun eine vCenter Server-Appliance an. Dabei handelt es sich um einen vCenter Server, der in eine Linux Appliance integriert wurde. Sie sparen sich so das zusätzliche Betriebssystem für das vCenter und haben ein Paket, das funktioniert. Bevor wir auf die Installation der Appliance eingehen, möchten wir uns mit den Funktionen und den Einschränkungen der derzeitigen Version beschäftigen. Auch bei dieser vCenter-Appliance ist eine Datenbank enthalten; diese mitgelieferte Version unterstützt jedoch nur 5 Hosts und 50 virtuelle Maschinen. Es ist aber kein Problem, eine externe Datenbank an das System anzubinden, um so die Leistungsfähigkeit zu erweitern. An dieser Stelle werden allerdings nur Oracle-Datenbanken unterstützt; ob zu einem späteren Zeitpunkt auch andere Datenbanken unterstützt werden sollen, ist uns derzeit nicht bekannt. Damit erhöht sich die verwaltbare Umgebung auf 400 Hosts und 4.000 VMs. Laut Konfigurationshandbuch von VMware kann die zu managende Landschaft auch größer sein.

Aber die hier genannten Werte dürften für viele Umgebungen schon vollkommen ausreichen. Der Linked Mode fehlt ebenfalls in der Featureliste der Appliance. Behalten Sie Ihr System genau unter Beobachtung, wie es sich verhält, wenn Sie an die vermeintlichen Grenzen stoßen. Die folgenden Funktionen werden ebenfalls nicht unterstützt: VMware Update Manager, VMware Storage Appliance und vCenter Server Heartbeat. Die größte Einschränkung ist wohl

die festgelegte Datenbank und das Fehlen des Update Managers. Man wird sehen, wie sich die Appliance mit den nächsten Versionen weiterentwickelt.

Kommen wir nun zur Installation der vCenter-Appliance. Der Import erfolgt, wie schon beim vMA, über den vSphere-Client. Rufen Sie den passenden Menüpunkt auf, und suchen Sie im folgenden Dialog die Datei für die Appliance.

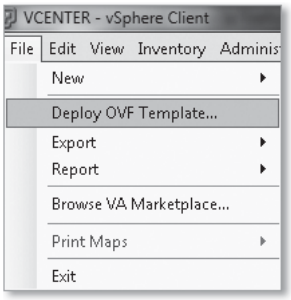


Abbildung 6.92 Import der vCenter-Appliance (VCVA)

Suchen Sie sich einen Datastore mit genügend Plattenplatz. Die VCVA benötigt ca. 90 GB. Mit der Konfiguration der vCenter-Appliance beschäftigen wir uns in Abschnitt 12.17.

6.5 VMware vCenter Converter Standalone

Der VMware vCenter Converter ist nur noch in einer Version erhältlich, die ohne vCenter Server lauffähig ist. Es handelt sich um eine reine Client-Server-Anwendung. Hier gehen wir kurz auf die Installation des Produktes ein.

Nach Start des Installationsprogramms und Bestätigung des EULAs erscheint das Fenster für die Angabe des Installationspfades. Es folgt die Auswahl des Installationstyps (Abbildung 6.93).

Der obere Punkt führt einfach eine Installation durch. Konvertierungen können von hier aus verwaltet werden. Keine weiteren Einstellmöglichkeiten trennen Sie von der endgültigen Installation. Beim zweiten Punkt besteht die Möglichkeit, Teile der Client-Server-Applikation vCenter Server Standalone zu installieren. Insgesamt ist es möglich, einen Agenten, einen Client oder den Server selbst zu installieren. Beim Server handelt es sich um den Server-Applikation-Teil. Der Client wird benötigt, um auf den Server-Teil zuzugreifen. Der Agent wird auf den Systemen installiert, die übernommen werden sollen.

Bei der Standardinstallation werden alle Komponenten zusammen installiert. Im folgenden Dialog können Sie die Auswahl der Komponenten aber noch anpassen. Auch diese Applikation benötigt Ports für die Kommunikation; diese sind jetzt einstellbar (Abbildung 6.94).

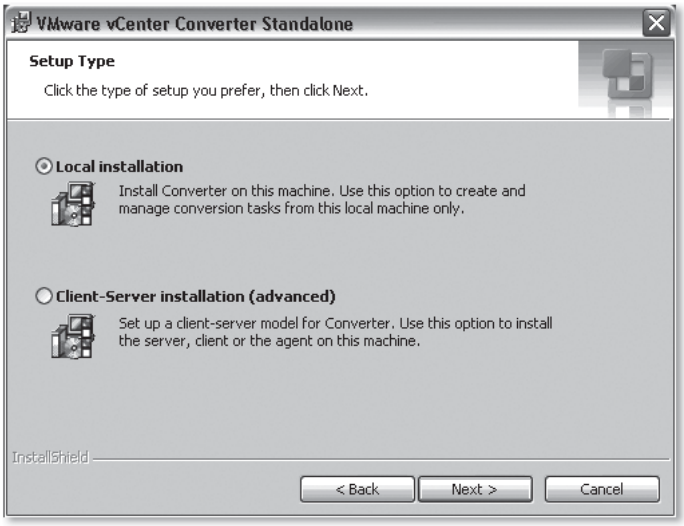


Abbildung 6.93 Installationsauswahl vCenter Converter Standalone

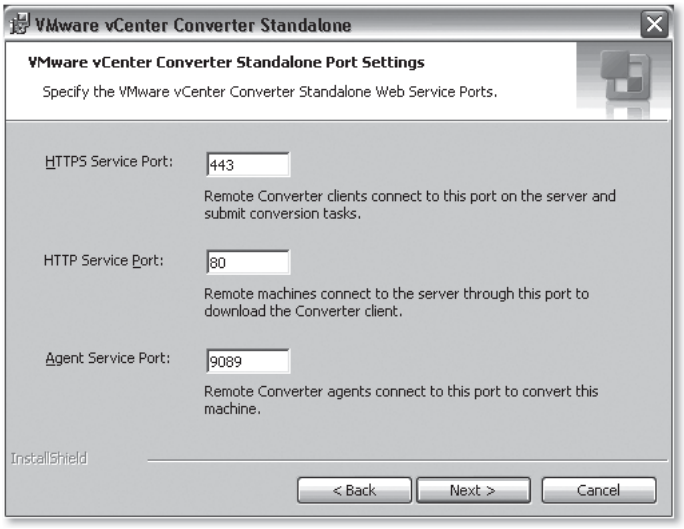


Abbildung 6.94 Portkonfiguration vCenter Converter Standalone

Auch hier gilt, dass Sie die Ports nur ändern sollten, wenn es zwingende Gründe dafür gibt. Passen Sie aber bitte auf, denn wenn Sie den vCenter Converter mit auf dem vCenter Server installieren wollen, dann kollidieren die Ports 443 und 80, und sie müssen sie umkonfigurieren. Alternativ erstellen Sie eine virtuelle Maschine, die den Converter aufnimmt. Sobald Sie die Eingabe bestätigen, beginnt die eigentliche Installation der Softwarekomponenten. Sie können die Installation mit dem automatischen Start des Clients abschließen. Jetzt steht das Tool für den Import von Computern in die virtuelle Infrastruktur bereit.

6.6 VMware Consolidated Backup

VMware Consolidated Backup (VCB) war die erste Backup-Lösung von VMware. Diese Lösung ist nicht mehr unterstützt und wird nicht mehr weiterentwickelt.

6.7 Hochverfügbarkeit vCenter Server

Der vCenter Server von VMware ist, genauso wie der Virtual Center Server für die früheren Versionen, extrem wichtig für das Management von virtuellen Infrastrukturen. Grundlegende Funktionen stehen nicht mehr zur Verfügung, wenn der Management-Server ausfällt. Diesen Aspekt sollten Sie bei der Planung von virtuellen Infrastrukturen berücksichtigen. In die Planung fließen die folgenden Faktoren ein: Welche Funktionen des vCenter Servers werden genutzt, ist die Datenbank auf dem vCenter-Server installiert, und wie lange kann ein Ausfall verkraftet werden?

6.7.1 Manuelle Hochverfügbarkeit

Eine manuelle Hochverfügbarkeit setzt im Problem- oder Fehlerfall den Eingriff eines Administrators voraus. Es sind aber weitere Voraussetzungen zu erfüllen, damit ein solches Konstrukt funktioniert.

Aber von Anfang an. Wir haben bereits beschrieben, dass der vCenter Server aus drei Komponenten besteht: zum Ersten die benötigte Datenbank, zum Zweiten die vCenter-Applikation selbst und zum Dritten die zusätzlichen Softwarekomponenten. Die manuelle Hochverfügbarkeit arbeitet mit einem sogenannten *Cold-Standby-Server*. Das bedeutet nichts weiter, als dass ein identischer vCenter-Server parat steht und aktiviert wird, wenn das produktive System ausgefallen ist oder Probleme bereitet. Diese Ausfallsicherheit kann aber nur funktionieren, wenn das abzubildende System ein statisches ist, also keine beweglichen Daten enthält. Für den vCenter-Server würde das bedeuten, dass die Datenbank auf einem separaten Server zur Verfügung gestellt werden muss.

Ist der Management-Server mit allen Komponenten fertig installiert, wie bereits beschrieben ohne Datenbank, erstellen Sie von ihm ein Duplikat. Es ist unerheblich, ob Sie den Server physisch oder virtuell aufbauen. Nutzen Sie ein virtuelles System, können Sie zur Erstellung des Standby-Servers einfach den VMware Converter einsetzen. Wichtig ist nur, dass Name und IP-Adresse der Server identisch sind. Beide Systeme dürfen aber nicht gleichzeitig am Netz hängen, das würde zu Problemen führen. Die absolut identische Identität der Systeme ist wichtig, damit nach der Inbetriebnahme des Standby-Systems der Management-Server unter dem gleichen Namen erreichbar ist. Andernfalls müssten bei einem Ausfall nicht nur der Server, sondern auch die Clients angepasst werden.

Im Fehlerfall schließen Sie einfach den Netzwerkport des produktiven Servers und öffnen den Port des Standby-Systems. Der Weg zurück läuft genauso ab.

Selbstverständlich müssen Sie sich für den Datenbank-Server ähnliche Gedanken machen. Schwierig ist in diesem Fall, dass alle Konfigurationsdaten des vCenter-Servers in der Datenbank abgespeichert werden. Auch hier könnte ein Cold-Standby-System zum Einsatz kommen. Wichtig ist an der Stelle, dass Sie regelmäßig Sicherungen der Datenbank durchführen. Vor der Produktivsetzung des Cold-Standby-Datenbanksystems müssten Sie den Datenbankbestand auf den letztmöglichen Stand bringen. Es sollte Ihnen klar sein, dass ein Teil der Performancedaten verlorengeht, wenn der Ausfall des Datenbank-Servers auf diese Art und Weise abgefangen werden soll.

6.7.2 Hochverfügbarkeit mit Microsoft Cluster

Achtung: VMware bietet keinen Support mehr für vCenter-Umgebungen, die mit Cluster-Software von Drittherstellern aufgebaut wurden. Es wird nur noch vCenter Server Heartbeat unterstützt.

6.7.3 vCenter Server Heartbeat

vCenter Server Heartbeat ist eine Softwareergänzung von VMware, die es Ihnen ermöglicht, den vCenter Server hochverfügbar zu machen. Dabei wird eine Schatteninstanz aufgebaut, die über ein privates Netzwerk mit dem produktiven Server online aktualisiert wird. Im Fehlerfall wird dann umgeschwenkt. So ist zu jeder Zeit eine einwandfreie Funktion des Management-Servers gewährleistet. Die Software ist keine Selbstentwicklung von VMware, sondern stammt ursprünglich von der Firma Neverfail. Der Einsatz der Software ist nicht sehr weit verbreitet, aus diesem Grund gehen wir auf dieses Paket nicht näher ein.

6.7.4 Zusätzliche Software

Möchten Sie, aus welchen Gründen auch immer, das Produkt VMware Heartbeat nicht einsetzen, so gibt es auch andere Produkte, die ähnliche Funktionen abbilden. Wichtig ist dabei, ob die gesamte Applikation einschließlich Datenbank auf einem Server läuft oder ob Datenbank und vCenter-Komponenten voneinander getrennt sind. Mögliche Programme sind in diesem Fall DoubleTake, Neverfail, Marathon und Ähnliche.

6.8 Lizenzierung

In diesem Abschnitt werden wir auf den aktuellen und den im vCenter integrierten Lizenz-Server eingehen. In einer reinen vSphere-Umgebung benötigen Sie nur den integrierten Lizenz-Server. Betreiben Sie Mischumgebungen, dann ist zusätzlich der Lizenz-Server der Vorgängerversion zu installieren.

6.8.1 Lizenzierung vSphere

Der vSphere-Lizenz-Server findet sich unter Administration • vCenter Server konfiguration • Licensing. Hier pflegen Sie die Lizenzen ein (Abbildung 6.95).

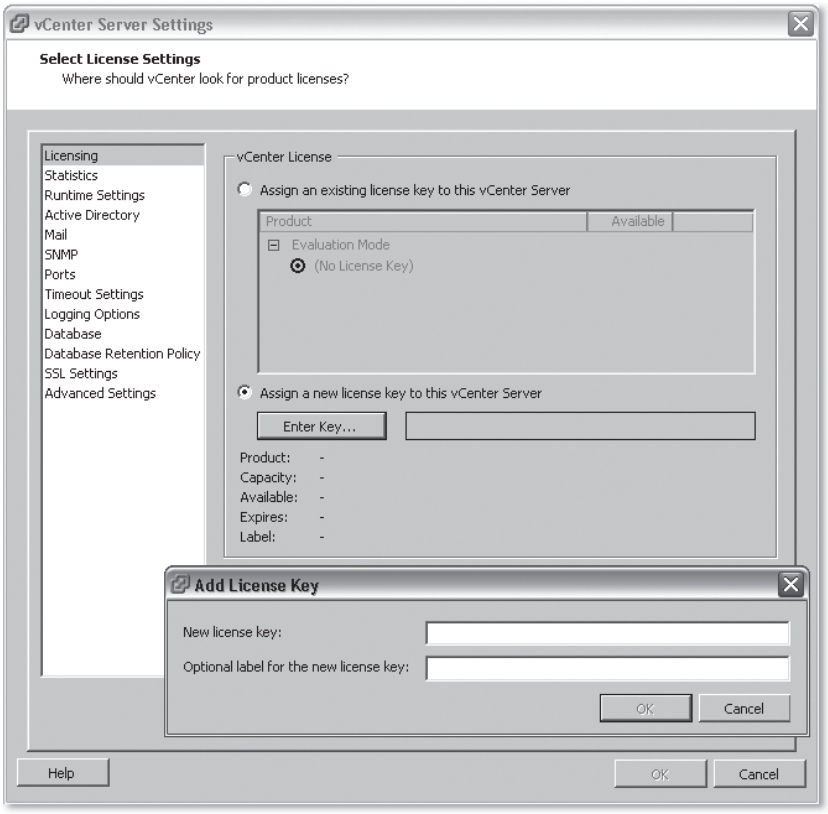


Abbildung 6.95 Lizenzen einpflegen

Gehören Sie zu den Administratoren einer Mischumgebung, dann müssen Sie zusätzlich den Lizenz-Server für die VI3.x-Umgebung angeben. Soll eine sanfte Migration von einer bestehenden Landschaft in eine vSphere-Farm erfolgen, dann ist nach dem Umzug eines VI3.x-Hosts die Lizenz im alten Lizenz-Server abzumelden. Anschließend pflegen Sie den vSphere-Lizenz-Key im vCenter ein. Die neue VMware-vSphere-Version läuft ohne Angabe einer Lizenz 60 Tage als Evaluation – mit vollem Funktionsumfang. Besitzen Sie bereits Lizenzen oder haben Sie Lizenzen bestellt, sind diese im VMware-Lizenzportal jederzeit abrufbar. Für weitere Informationen schlagen Sie bitte in Kapitel 18, »Die Lizenzierung von vSphere«, nach.

6.8.2 Lizenzen prüfen – VI3.x

Wenn die Lizenzen in das Lizenz-Server-Verzeichnis kopiert sind, müssen Sie in jedem Fall den Lizenz-Server daraufhin überprüfen, ob er die Lizenzen auslesen und dementsprechend

an vCenter- und VMware-vSphere-Server weitergeben kann. Dazu wurde auf dem System, auf dem der Lizenz-Server läuft, ein Lizenz-Server-Tool mitinstalliert, das Sie im START-Menü unter VMWARE • VMWARE LICENSE SERVER • VMWARE LICENSE SERVER TOOLS finden.

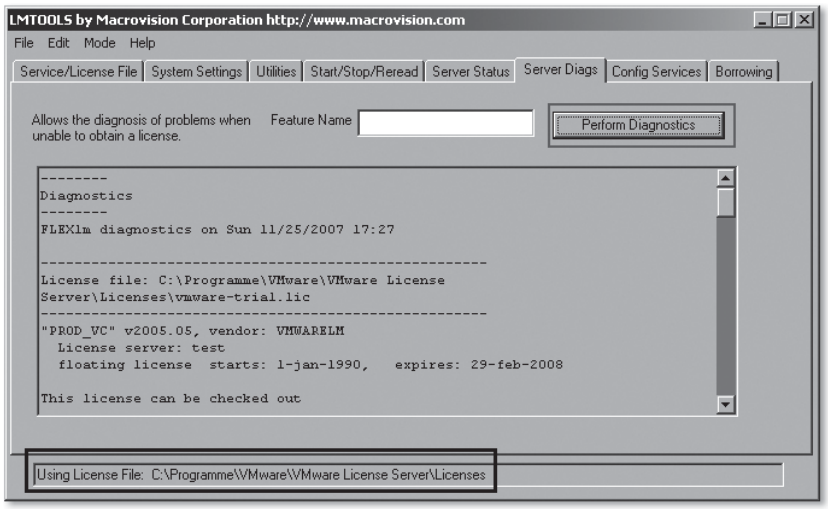


Abbildung 6.96 Diagnose des Lizenz-Servers

Dieses Tool besitzt zwei interessante Reiter zum Debuggen des Lizenz-Servers: SERVER DIAGS und START/STOP/REREAD. Der erste Weg sollte immer zum SERVER DIAG mit anschließendem PERFORM DIAGNOSTICS führen. Wird in dem unteren Feld keine Lizenz angezeigt, liegt definitiv ein Fehler vor. In diesem und in dem Fall fehlender Lizenzen sollten Sie zuerst auf einen richtigen Pfad (Abbildung 6.97) hin prüfen und anschließend die Lizenzdatei neu einlesen.

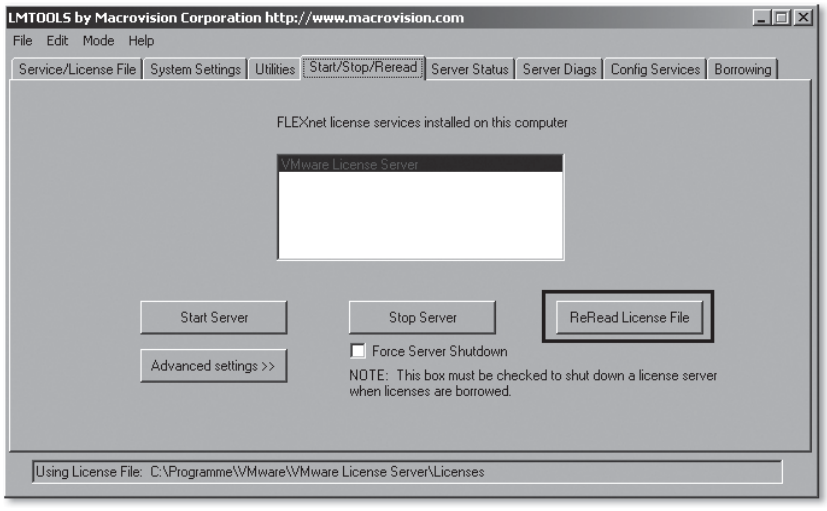


Abbildung 6.97 Verwaltung des Lizenz-Server-Dienstes

Hilft dies nichts, starten Sie erst den Lizenz-Server-Dienst neu und führen danach wieder einen Diagnoselauf durch. Der letzte Weg wäre ein Neustart des gesamten Systems. Dies ist zwar äußerst selten notwendig, es kann aber passieren, wenn der Lizenz-Server komplett abstürzt. Erkennt der Lizenz-Server alle Lizenzen korrekt, ist in vielen Fällen auch ein Neustart des vCenter-Diensts notwendig, um alle Lizenzen korrekt im Zugriff zu halten.

6.9 VMware Data Recovery

Bevor wir nun auf die Installation der VMware Data Recovery eingehen, möchten wir darstellen, wie das Ganze funktioniert. Das gesamte Konglomerat besteht aus mehreren Teilen, die ineinandergreifen. Zuallererst benötigen Sie eine virtuelle Maschine. Diese liegt im OVF-Format vor und verwaltet den Datensicherungsstrom. Es wird ein Plugin genutzt, das sich in den vSphere-Client einbindet. An dieser Stelle administrieren Sie Backups und Restores. Sehr wichtig ist, dass Sie die Daten auch sichern, wenn Sie die VM mit vMotion oder über DRS im Cluster verschieben! Als Ablageort für Daten sind alle Medien zugelassen, die als virtuelle Disk genutzt werden können, als da wären SAN, NAS und CIFS.

Die Daten werden dedupliziert, was das Datenaufkommen um ein Vielfaches reduziert.

Einschränkungen

Sie können nicht mehr als 100 virtuelle Maschinen gleichzeitig mit einer Backup-Appliance sichern. Es können maximal 8 parallele Jobs aktiv laufen.

Bevor die Datensicherung über die Sicherungsapplikation angestoßen wird, erzeugt das Data Recovery einen Snapshot. Unter Zuhilfenahme des Microsoft-Dienstes Volume Shadow Copy Service wird dafür gesorgt, dass dieser Snapshot auch konsistent ist. Wäre das nicht der Fall, könnte man mit den Daten in der Sicherung nichts anfangen. Vergewissern Sie sich vor der Installation, dass die Voraussetzungen erfüllt sind. Es muss ein vCenter Server in der aktuellen Version vorhanden sein.

Im Vorfeld ist es sehr schwierig, festzustellen, wie viel Plattenplatz für die Sicherung benötigt wird. Die Größe wird im Wesentlichen davon beeinflusst, wie viele unterschiedliche Systeme gesichert werden sollen, wie oft sie gesichert werden sollen und wie lange die Daten vorgehalten werden müssen. Zur Optimierung des Plattenplatzbedarfs fassen Sie identische oder ähnliche Systeme auf derselben Zielplatte zusammen. So optimieren Sie die Deduplizierungsrate. Die Installation erfolgt in zwei recht einfachen Schritten: Zu Beginn laden Sie das ISO-File für das VMware Data Recovery bei VMware herunter. Binden Sie das ISO-Image ein, erscheint über die Autostart-Funktion das Startfenster für den ersten Teil der Installation (Abbildung 6.98).

Abbildung 6.98 Installation Client VMware Data Recovery

Über den ersten Menüpunkt richten Sie den Client der VMware Data Recovery ein. Diese Komponente gliedert sich in den vSphere-Client ein und ermöglicht das Management der Backup-Appliance. Bei der Installation des Clients gibt es keine Möglichkeit, die Konfiguration anzupassen. Es ist nur dem EULA zuzustimmen, und der Rest läuft automatisch ab.

Im zweiten Schritt wird die Appliance zur Verfügung gestellt. Das gemountete ISO-File enthält den Pfad *VMwareataRecovery-ovf-x86_64\VMwareDataRecovery_ovf10.ovf*.

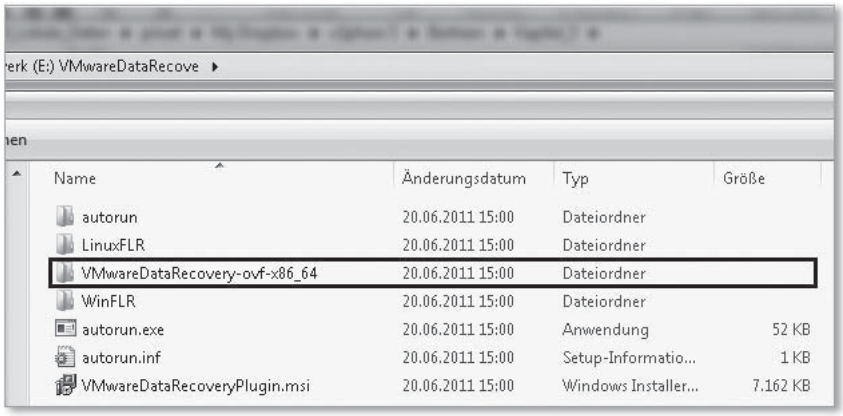


Abbildung 6.99 Pfad der Data Recovery Appliance

Darin befinden sich mehrere Dateien: unter anderem die Beschreibungsdatei mit der Endung *.ovf* und die Festplattendatei mit der Endung *.vmdk*. Über das vCenter und den Menüpunkt File • Virtual Appliance • Import können Sie die VM starten. Standardmäßig hat die VM zwei CPUs und 2 GB Arbeitsspeicher; je nachdem, wie viele VMs gesichert werden sollen, ist es erforderlich, den Hauptspeicher des Systems aufzurüsten.

Nachdem Sie die VM gestartet haben, können Sie sie weitergehend konfigurieren. Diese Arbeiten stellen wir, wie bei den anderen in diesem Kapitel beschriebenen Funktionen auch, in Kapitel 13, »Konfiguration von vCenter-Add-ons«, näher dar.

6.9.1 Installation des VMware Data Recovery Clients

Nach dem Start des Autostart-Fensters der VMware-Data-Recovery-CD habe Sie die Möglichkeit den Data Recovery Client zu installieren. Der Client kann nicht über das vCenter installiert werden, Sie müssen die Installation über das Medium durchführen. Einstellungen können Sie während der Installation nicht ändern, somit ist die Installation recht einfach und bedarf keiner näheren Beschreibung. Nach dem Neustart des vSphere-Clients findet sich unter Solutions and Applications auf der Homepage ein neues Icon. An dieser Stelle findet die weitere Konfiguration statt.

Es gibt mit der Version 5.x auch zwei Clients, die es ermöglichen, Dateien auf Filelevel-Ebene wiederherzustellen. Zwei Clients liefert VMware aus, einen für Windows-Systeme und einen für Linux-Systeme. Es ist aber keine Installation notwendig, es wird einfach nur eine ausführbare Datei aufgerufen. Aus diesem Grund gehen wir an dieser Stelle nicht weiter auf die Software ein.

6.10 VMware vSphere Storage Appliance (VSA)

Die Funktionalität und den strukturellen Aufbau der VSA beschreiben wir in Abschnitt 13.11 näher. Wir möchten hier auf die reine Installation der Appliance eingehen und Ihnen zeigen, welche Schritte notwendig sind, um einen VSA-Cluster in Betrieb zu nehmen.

Bevor wir jedoch zur Installation kommen, lassen Sie uns einen Blick auf die Voraussetzungen werfen – diese Liste ist nicht kurz:

- Server-Hardware muss volle vMotion-Kompatibilität haben.
- minimaler Arbeitsspeicher 6 GB, empfohlen 24 GB, maximal 72 GB
- minimal vier Netzwerkports
- redundante Netzwerkinfrastruktur
- RAID-Controller muss RAID 10 unterstützen.
- acht von der Größe her identische HDs; je mehr, desto besser (in einem RAID zusammengefasst)
- zwei getrennte Netzwerkbereiche
- zusätzliche statische IP-Adressen

Die Installation des ESXi muss in das Gesamt-RAID erfolgen und nicht auf ein eigenes RAID!

6.10.1 Installation des VSA-Managers

Die Installation gliedert sich in zwei Schritte. Sie beginnt mit der Installation des VSA-Managers auf dem vCenter Server. Hierzu laden Sie sich die passende Datei von VMware-Webserver herunter, legen sie auf dem vCenter-Server ab und rufen sie auf.

Der Dateiname des VSA-Managers hat das folgende Muster: *vmware-vsamanager-en-<Version>-<Buildnummer>.exe*

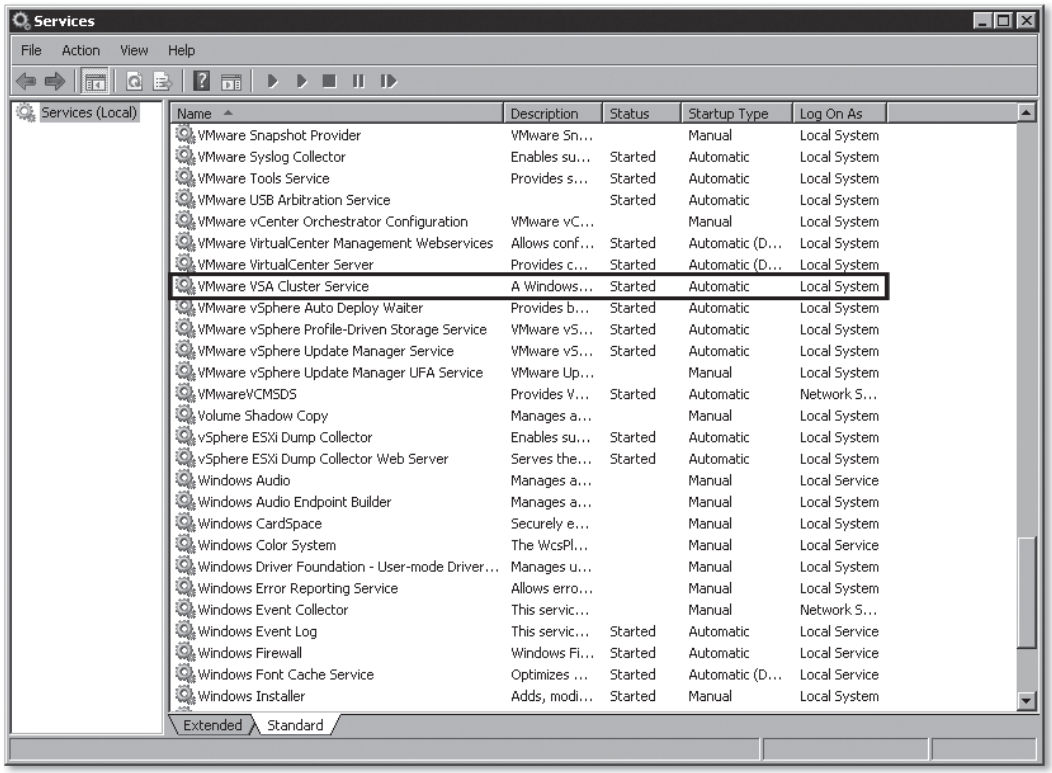


Abbildung 6.100 VSA-Dienst auf dem vCenter-Server

Melden Sie sich an dem vCenter-Server mit einem Windows-Account an, der auch administrative Rechte im vCenter hat. Nach dem Aufruf können Sie die Sprache auswählen, die während des Installationsprozesses genutzt werden soll. Nach einer etwas längeren Wartezeit, während der Dateien entpackt und kopiert werden, folgen die bekannten Fenster einschließlich des EULAs. Der nächste Dialog erfordert die Angabe der IP-Adresse des vCenter-Servers und gibt einen Kommunikationsport vor – bitte ändern Sie diesen nicht. Auch wenn Sie es an dieser Stelle nicht sehen, versucht die Installationsroutine nun, eine Verbindung mit dem vCenter herzustellen. Dabei wird der User benutzt, mit dem Sie sich an der Server-Konsole

angemeldet haben. Es folgt die Eingabe eines passenden Lizenzschlüssels, oder Sie nutzen den Evaluationsmodus. Die Installation wird nun durchgeführt, und die notwendigen Dateien werden auf das System kopiert. Anschließend findet sich ein neuer Dienst auf dem vCenter-Server.

Dieser Dienst ist für das Handling der VSA zuständig. Schauen Sie nun in den vSphere-Client, sehen Sie auf dem Datacenter-Objekt einen neuen Reiter. Sollte dieser nicht auftauchen, schauen Sie bitte bei den Plugins nach, ob das VSA-Manager-Plugin aktiv ist. Sollte das nicht so sein, können Sie es über das Kontextmenü einschalten.

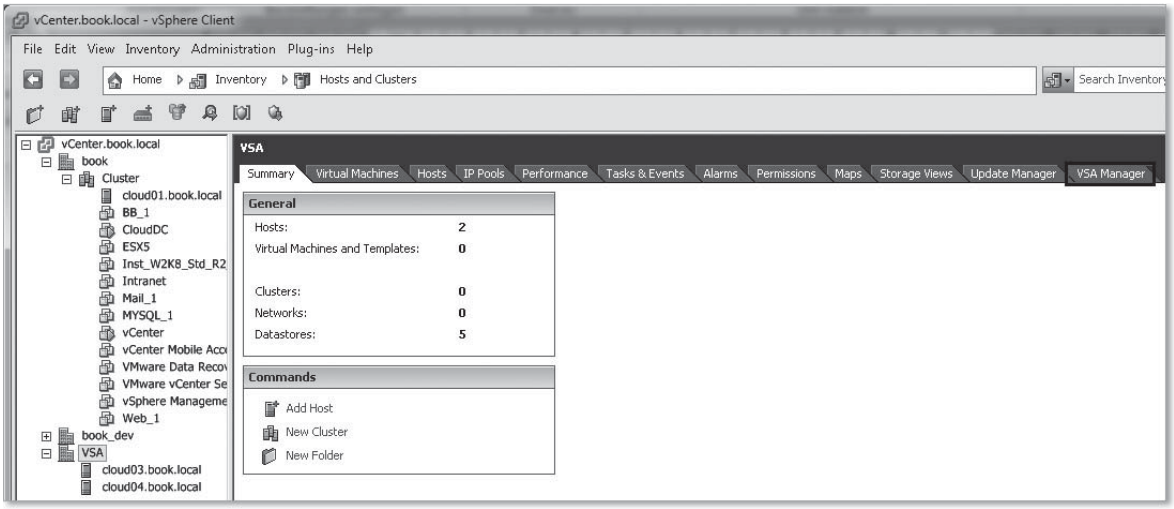


Abbildung 6.101 VSA-Manager: Reiter am Datacenter-Objekt

Damit ist der erste Teil der Installation abgeschlossen, und wir kommen zur Installation des eigentlichen Clusters.

6.10.2 Installation des VSA-Clusters

Damit Sie einen VSA-Cluster konfigurieren können, müssen Sie zuerst ein neues Datacenter erstellen und in dieses Datacenter die zwei oder drei Hosts aufnehmen (siehe Abbildung 6.102 auf der nächsten Seite), die Mitglieder des VSA-Clusters werden sollen. Des Weiteren muss auf dem System, auf dem Sie die Installation starten, der Adobe Flash Player installiert sein. Beim ersten Aufruf werden Sie eine Zertifikatsmeldung erhalten. Wechseln Sie nun im Datacenter-Objekt auf den Reiter VSA Manager.

Die Einstellungen für den Cluster nehmen Sie an dieser Stelle vor. Für die Konfiguration des VSA-Clusters schauen Sie bitte in Abschnitt 13.11, dort beschreiben wir die Vorgehensweise.

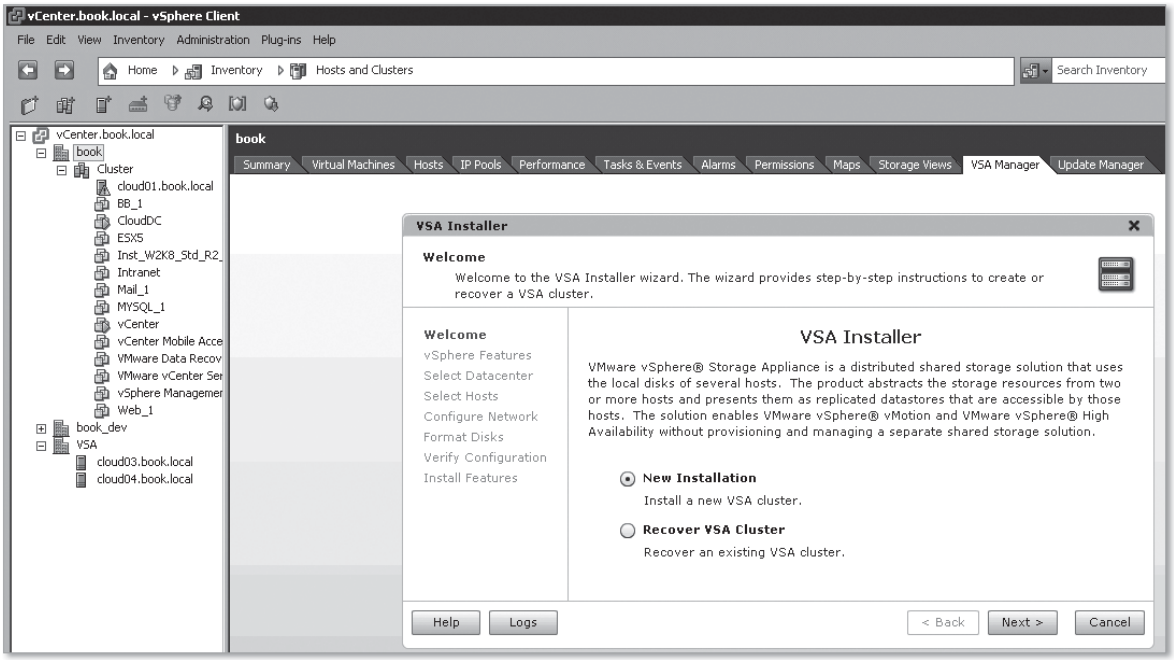


Abbildung 6.102 VSA-Cluster-Konfiguration

In diesem Kapitel erfahren Sie, wie Sie Ihre VMware Virtual Infrastructure verwalten. Wir werden auf alle Möglichkeiten der Verwaltung eingehen, die Sie in der VMware Virtual Infrastructure nutzen können.

7 Verwaltungsmöglichkeiten

Autor dieses Kapitels ist Bertram Wöhrmann, Ligarion, bwoehrmann@ligarion.de

Nachdem Sie dieses Kapitel gelesen haben, werden Sie alle Möglichkeiten kennen, die Ihnen die Firma VMware zur Verfügung stellt, um Ihre virtuelle Infrastruktur zu administrieren. Dabei werden wir näher beleuchten, wann Sie welches Tool verwenden sollten. Durch den richtigen Einsatz des richtigen Tools ist es möglich, die Landschaft effektiv zu administrieren.

7.1 Weboberfläche

Eine der ersten Möglichkeiten, sich mit dem vSphere-Server oder dem vCenter-Server zu verbinden, ist der Weg über die Weboberfläche. Der Zugriff auf die Weboberfläche ermöglicht einige grundlegende Möglichkeiten der Administration. Den Schwerpunkt der möglichen Administration über die Weboberfläche sehen wir bei Arbeiten im Zusammenhang mit virtuellen Maschinen. Es werden nur wenige Funktionen zur Administration von vSphere-Hosts angeboten.

Die Weboberfläche ist direkt nach der Installation des vSphere-Hosts erreichbar. Wenn Sie in Ihrem Browser *http://SERVER-IP* eingeben, werden Sie auf die Startseite weitergeleitet. Auf dieser Seite finden Sie auf der linken Seite keinen Link mehr, um sich an dem Host anmelden zu können.

Der Punkt An Webaccess anmelden, den Sie vielleicht von früheren Versionen her kennen, gibt es nicht mehr. Sie haben nur die Möglichkeit, sich den vSphere-Client, den vCenter Server oder die vSphere-Dokumentation aus dem Internet herunterzuladen. Auf der rechten Seite des Browserfensters können Sie auch verschiedene Aktionen starten. Das wäre zum einen das Herunterladen der Remote Command Line Tools. Dieses gibt es einmal als Appliance, als Windows-Softwarepaket und als Linux-Version.

Weiter unten ist es möglich, mehr über die Webservices-SDKs zu erfahren. Hier zeigt sich schon: Eine richtige Administration über den Webbrowser ist nicht möglich. Lediglich zwei

Aktionen können Sie in diesem Fenster durchführen. Sie können sich die Datastores des Hosts anzeigen lassen, oder Sie können sich die Host-Objekte im Browser ausgeben lassen.

Einen Webzugriff im eigentlichen Sinne bekommen Sie nur, wenn Sie sich mit dem vCenter-Server über den Browser verbinden. Ohne weitere Konfigurationen ist das aber nicht möglich.

Besteht der Wunsch, mit dem Webclient zu arbeiten, so müssen Sie dieses Softwarepaket auf dem vCenter Server installieren. Erst danach ist es möglich, mit dem Webclient auf den vCenter Server zuzugreifen; der Zugriff direkt auf einen Host ist nicht möglich.

Auch bei dieser Software handelt es sich um ein normales Windows-Installationspaket. Den Installationsablauf finden Sie in Abschitt 6.3.4.

Beim ersten Aufruf finden Sie eine Oberfläche vor, die der Weboberfläche eines Hosts sehr ähnlich ist. Erst wenn Sie genauer hinschauen, werden die Unterschiede deutlich.

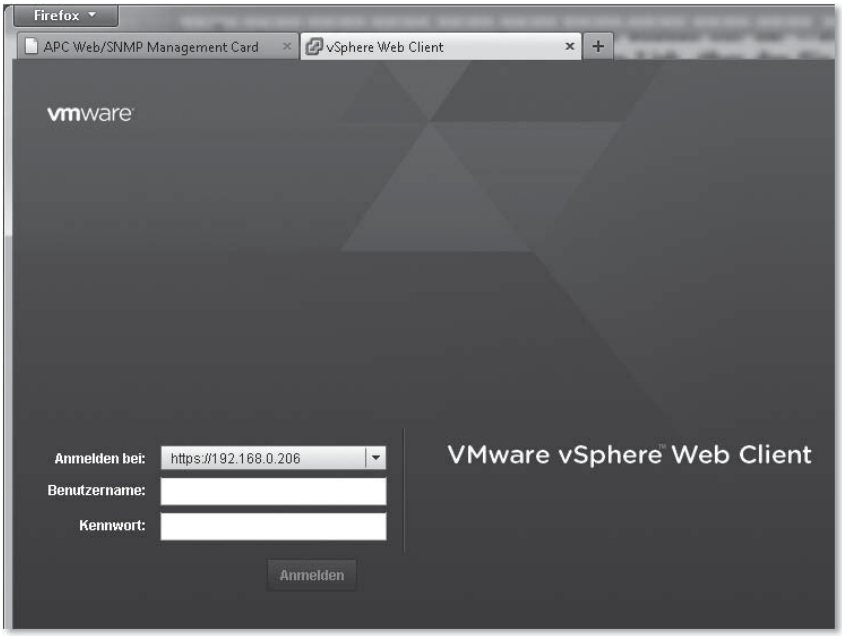


Abbildung 7.1 Anmeldung am Webclient

Auch hier können unterschiedliche Komponenten heruntergeladen werden, mit Ausnahme des vCenter Servers und der Remote-Tools. Oben rechts findet sich der Link für den Aufruf des Webclients.

Stellte die Weboberfläche der Vorversion nur rudimentäre Funktionen zur Verfügung, so deckt der neue Webclient schon viele der Funktionalitäten des vSphere-Clients ab. Der Schwerpunkt liegt hier aber eindeutig auf Funktionen zur Administration von virtuellen Maschinen. Konfigurationen am Host sollten über den klassischen vSphere-Client erfolgen, es

ist an dieser Stelle einfach nicht möglich. Sie können hier neue VMs anlegen und neue vApps erstellen. Einzig die Anlage von Resource-Pools ist hier noch möglich. Beachten Sie bitte, dass in der Hauptansicht nicht ersichtlich ist, ob eine VM eingeschaltet ist oder nicht. Im folgenden Bild ist das sehr schön zu sehen. Die grafische Unterscheidung am Icon findet sich nur im mittleren Fenster, wenn Sie sich dort die virtuellen Maschinen anzeigen lassen.

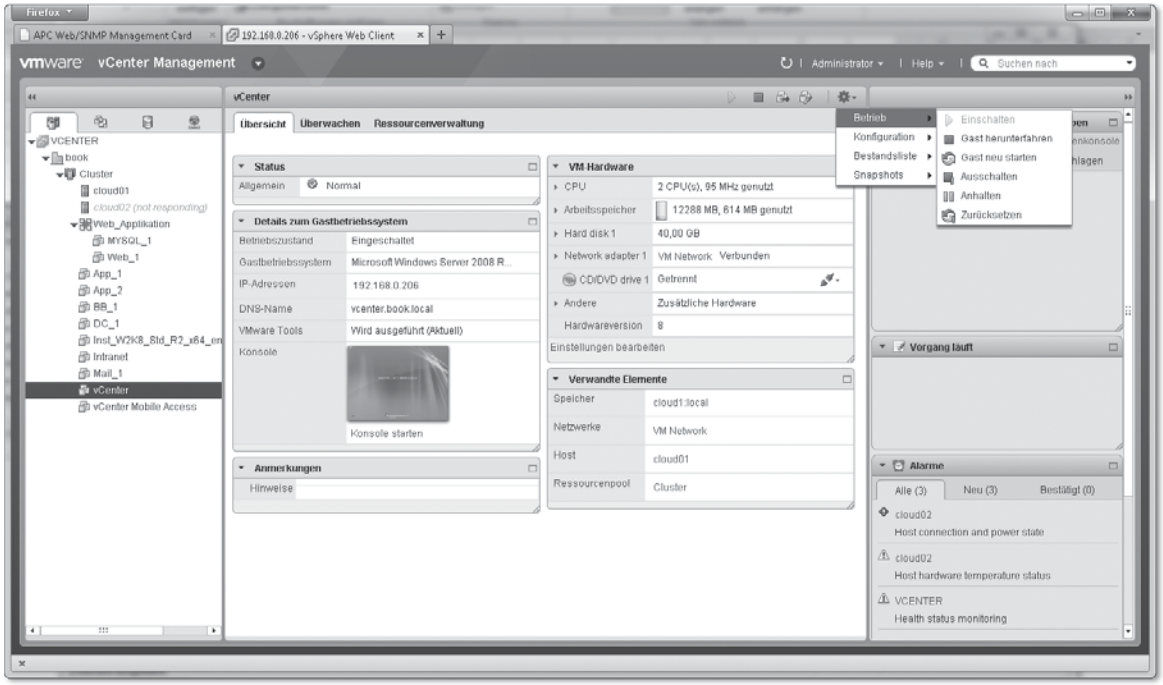


Abbildung 7.2 »Host and Clusters«-Ansicht im Webclient

In der oberen linken Ecke finden sich die unterschiedlichen Ansichten wieder: Host and Clusters, VMs and Templates, Datastores und Network wieder.

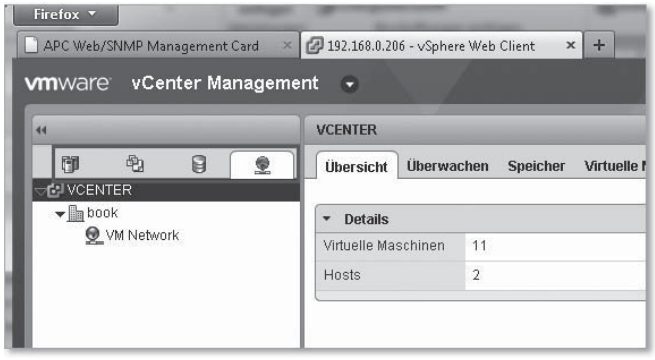


Abbildung 7.3 Ansichten im Webclient

Abschließend lässt sich sagen, dass die Oberfläche ideal ist für Anwender, die sich hauptsächlich um die Administration von virtuellen Maschinen kümmern. Der Vorteil liegt auf der Hand: Die Anwender, die nur mit den virtuellen Maschinen zu tun haben, können den Webclient nutzen. Es ist keine Versionspflege für den Client notwendig, denn der Anwender benötigt nur einen Browser. Eine Paketierung des vSphere-Clients ist so auch nicht erforderlich.

Tipp: Sprachenmix auf dem Client verhindern

Sollten Sie beim Webclient die Sprache fest einstellen wollen, dann müssen Sie in Ihrem Browser eine Einstellungsänderung vornehmen. In den Internetoptionen können Sie die Sprachen festlegen. Fügen Sie dort die gewünschte Sprache hinzu, und verschieben Sie sie in die in oberste Zeile der Wertigkeit.

Wir werden sehen, inwieweit VMware die Funktionalitäten in den folgenden Versionen weiter ausbaut.

7.2 Lokale Host-Konsole

Die Service Console gehört der Vergangenheit an. Nur beim Einsatz von VMware-Hosts unterhalb der Version 5.x gibt es noch eine Service Console, wenn die ESX-Version zum Einsatz kommt. Die Version ESXi stellt keine Service Console zur Verfügung.

Beim ESXi-Host stellt sich die Oberfläche anders dar. Sie gelangen über die Taste F2 zum Management (Abbildung 7.4).

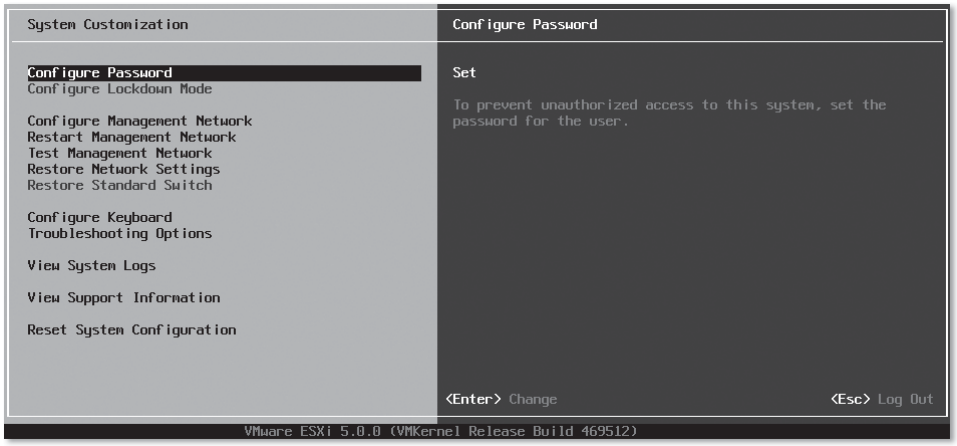


Abbildung 7.4 Managementoberfläche bei VMware ESXi

Hier lassen sich das Passwort, die Netzwerkeinstellungen und die Tastatur konfigurieren. Des Weiteren können Sie hier die Log-Dateien einsehen. Viel mehr als diese rudimentären Funktionen steht in der Console des ESXi Servers nicht zur Verfügung.

Unter ESXi können Sie außerdem den Lockdown Mode einstellen. Wird dieser aktiviert, ist es nicht mehr möglich, sich remote auf der Maschine mit typischen Administrator-Accounts anzumelden, z. B. »root« oder »admin«. Eine Konfiguration müssen Sie dann mit dem vCenter oder lokal an der Konsole durchführen.

Der Punkt Restart Management Agents findet sich jetzt unter dem Punkt Troubleshooting Options. Dort können Sie auch die SSH-Freischaltung vornehmen und deren Parameter konfigurieren. Die Option Remove Custom Extensions erlaubt es, Zusatzpakete wieder zu deinstallieren. Hier gibt es keine Auswahl; es können immer nur alle auf einmal deinstalliert werden. Diese Erweiterungen können Sie entweder über den vCenter Update Manager installieren oder über das vSphere-CLI mit dem Befehl `vihostupdate`.

7.3 Host-Konsole per SSH

Der direkte Zugriff auf den Host ist natürlich über die lokale Konsole möglich, aber mit vSphere 5.x sind einige Optionen dazugekommen, die es vorher so nicht gab. So können Sie, Freischaltung der Ports vorausgesetzt, einen Zugriff per SSH vornehmen (SSH Service).

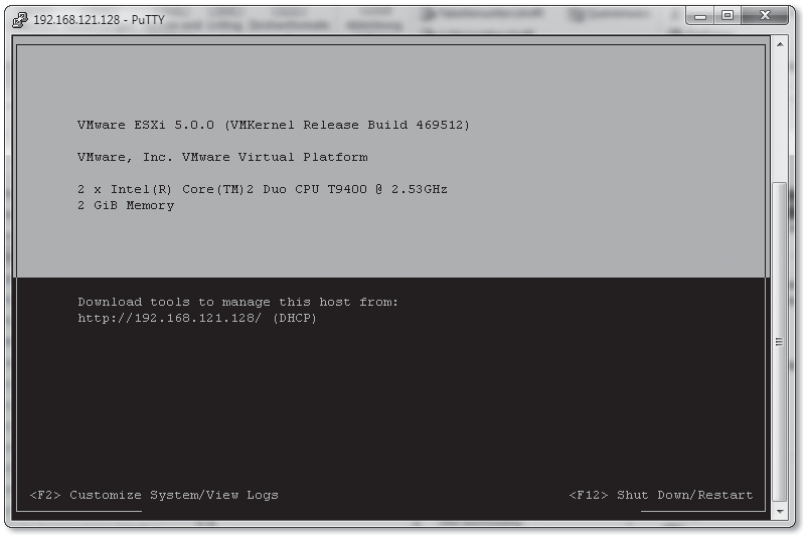


Abbildung 7.5 Hardwarekonsole über SSH

An der ein oder anderen Stelle kann es aber auch schwierig sein, direkt auf die Host-Konsole zuzugreifen. Hier hat VMware Abhilfe geschaffen: Starten Sie den Dienst Direct Console UI im vSphere-Client und den SSH-Dienst. Nachdem Sie eine SSH-Sitzung zum ESXi-Host geöffnet haben, geben Sie einfach den Befehl `dcui` ein, und Sie erhalten ein Fenster, das Ihnen nicht ganz unbekannt sein sollte.

Mit Strg+C kommen Sie wieder zurück in die Kommandozeile.

7.4 vSphere-Client

Der vSphere-Client bietet eine komfortablere und ergonomische Oberfläche, um vSphere-Server zu administrieren. Dieses GUI bietet mehr Komfort als die Weboberfläche. Der Client kann von jeder vSphere-Host-Weboberfläche heruntergeladen und unter Microsoft Windows installiert werden. Der Client ist auch kompatibel mit den Vorgängerversionen der aktuellen virtuellen Infrastruktur. Kommt bei Ihnen eine Mischumgebung zum Einsatz – bei der Migration von der Version ESX 3.x oder ESX 4.x nach vSphere 5.x ist das temporär auf jeden Fall so –, dann können Sie mit dem neuen Client auf alle Systeme zugreifen. Auf den folgenden Seiten lesen Sie, wie Sie den vSphere-Client installieren und ihn bedienen.

7.4.1 Download und Installation des vSphere-Clients

Um den vSphere-Client herunterzuladen, verbinden Sie sich einfach mit der Weboberfläche eines vSphere-Hosts. Dort finden Sie einen Link, über den Sie den Client herunterladen können.

Nachdem Sie den Client heruntergeladen haben, installieren Sie ihn wie jedes andere Windows-Programm auch. Die Installation ist nach ein paar Klicks abgeschlossen, und es wird automatisch ein Icon auf dem Desktop angelegt. Näheres zur Installation des vSphere-Clients finden Sie in Abschnitt 6.3.4.

7.4.2 Verwenden des vSphere-Clients

Nachdem Sie den Client gestartet haben, können Sie sich mit Host-Name, Benutzername und Passwort an einem vSphere- oder vCenter-Server anmelden (Abbildung 7.6). Alternativ zu einem Host-Namen können Sie auch die IP-Adresse des Hosts verwenden.

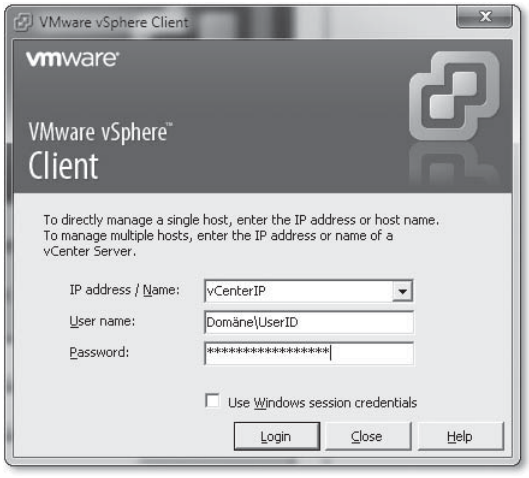


Abbildung 7.6 Die Anmeldung am vSphere-Client

Je nachdem, ob Sie sich mit einem Host oder mit einem vCenter-Server verbunden haben, werden in der Oberfläche verschiedene Informationen angezeigt. Nach dem Laden des Inventorys und dem Aufbau der Oberfläche sehen Sie einen Bildschirm mit zwei verschiedenen Fenstern. Auf der linken Seite der Oberfläche finden Sie bei der Anmeldung an einen Host den vSphere-Host wieder, mit dem Sie sich verbunden haben (Abbildung 7.7).

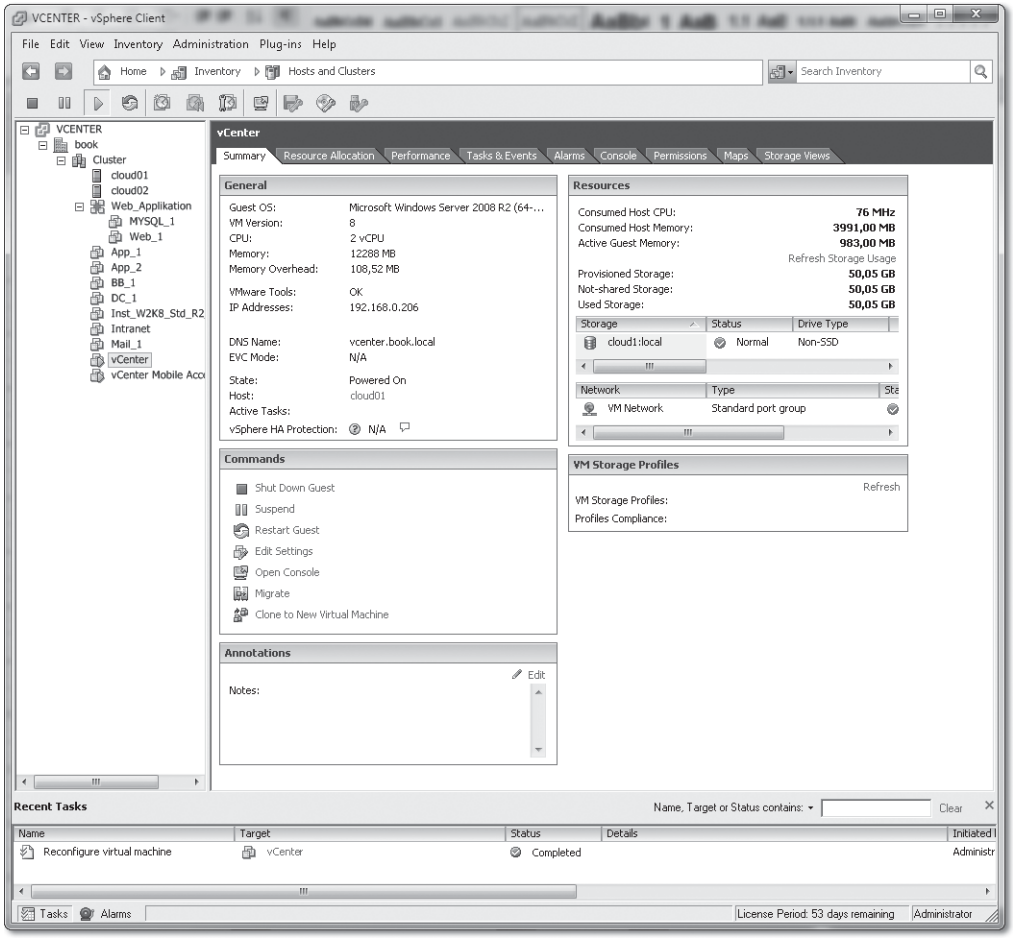


Abbildung 7.7 vCenter-Oberfläche

Auf der rechten Seite der Oberfläche sehen sich verschiedene Informationen und Reiter zur Administration des auf der linken Seite aktivierten Objekts.

Tabelle 7.1 listet die verschiedenen Reiter auf, die Ihnen angeboten werden, mit einer Erklärung, welche administrativen Möglichkeiten sich dahinter verbergen. Wundern Sie sich nicht, wenn sich der vSphere-Client auf verschiedenen Systemen in unterschiedlichen Sprachen darstellt. Das hängt mit der aktivierten Localen zusammen, auf dem der Client installiert ist; das System sucht sich automatisch die Informationen aus dem Betriebssystem.

Reiter	Beschreibung
Summary	Unter dem Reiter Summary finden Sie eine Zusammenfassung über das gerade ausgewählte Objekt. Wählen Sie zum Beispiel einen vSphere-Host aus, sehen Sie allgemeine Informationen zum Host wie zum Beispiel Hersteller, CPUs oder RAM. Außerdem werden Informationen über die Ressourcen des Hosts angezeigt, zum Beispiel die verwendeten Datastores, die angelegten virtuellen Netzwerke und die Auslastung von RAM und CPU.
Virtual Machines	Den Reiter Virtual Machines finden Sie nur bei Objekten wie dem vSphere-Host, der vApp oder einem Resource-Pool. Dort wird eine Liste aller virtuellen Maschinen angezeigt sowie deren Status bezüglich Ressourcen, Alarme und Power. Möglicherweise werden weitere Daten aufgelistet, abhängig davon, welche Ausgabefelder Sie in der Kopfzeile des Ausgabefensters aktiviert haben.
Hosts	Auf einem Cluster- oder Datacenter-Objekt findet sich dieser Reiter. Hier werden alle Hosts angezeigt, die unter dem entsprechenden Objekt zu finden sind.
DRS	Diesen Reiter werden Sie nur in der Cluster-Ansicht finden. Hier erhalten Sie die Informationen bzw. Empfehlungen zur DRS-Funktion.
IP Pools	Die IP-Pools finden Sie in der Ansicht des Datacenters. Hier werden IP-Adressen für die vApps abgelegt. Dabei können Sie unterschiedliche Pools anlegen.
Resource Allocation	Resource Allocation wird ebenfalls nicht bei virtuellen Maschinen angezeigt. Hier erhalten Sie eine komplette Übersicht über alle Ressourcen hinsichtlich CPU und RAM. Reservierungen, Shares usw. können Sie hier einsehen und verändern.
Performance	Unter Performance wird ein Diagramm dargestellt, das die Auslastung der verschiedenen Objekte illustriert. Die Ausgabewerte lassen sich den Erfordernissen des Administrators anpassen.
Configuration	Unter dem Tab Configuration können Sie alle Einstellungen eines vSphere-Hosts vornehmen. Dort ist es möglich, unter anderem das Netzwerk zu konfigurieren oder Datastores zu verwalten. Im weiteren Verlauf dieses Kapitels gehen wir noch einmal näher darauf ein.
Tasks & Events	Unter dem Reiter Tasks & Events werden alle protokollierten Tasks und Events aufgeführt.
Alarms	An dieser Stelle werden zum einen die Alarmdefinitionen angezeigt und zum anderen die aufgetretenen Alarme. Hier können Sie auch eine Quittierung der Alarme durchführen.
Console	Unter den Eigenschaften der virtuellen Maschine ist dieser Reiter zu finden. Hinter ihm verbirgt sich der Bildschirm der VM.
Permissions	Unter dem Reiter Permissions können Sie den Benutzern und Gruppen, die unter dem Reiter Users & Groups erstellt wurden, bestimmte Berechtigungen geben. Sie können mit vorgefertigten Benutzerrollen arbeiten, oder Sie legen eigene Rollen an, die die Arbeitsprozesse im Unternehmen widerspiegeln.
Maps	Eine grafische Darstellung der Infrastruktur der VM wird hier angezeigt.
Hardware Status	Dieser Reiter ist hostspezifisch. Der Status der einzelnen Hardwarekomponenten wird an dieser Stelle dokumentiert und grafisch dargestellt.
Storage Views	Ähnlich wie bei dem Reiter Maps wird eine grafische Ausgabe erzeugt, die darstellt, wie welche Komponenten miteinander verbunden sind. Es ist ebenfalls möglich, die Ausgabe als Report anzeigen zu lassen.

Tabelle 7.1 Reiter des vSphere-Clients

Reiter	Beschreibung
Update Manager	Sollten Sie Host und/oder VMs mit dem VMware Update Manager patchen, dann werden hier die Informationen zum Patch-Status des Objekts angezeigt.
Profile Compliance	Nutzen Sie die Hostprofile von VMware, können Sie hier den Status und die Compliance der Hosts einsehen.

Tabelle 7.1 Reiter des vSphere-Clients (Forts.)

Sie konfigurieren und verwalten einen vSphere-Host unter dem Reiter Configuration. Wie bereits in Tabelle 7.1 erwähnt, können Sie dort alle wichtigen Einstellungen vornehmen (Abbildung 7.8).

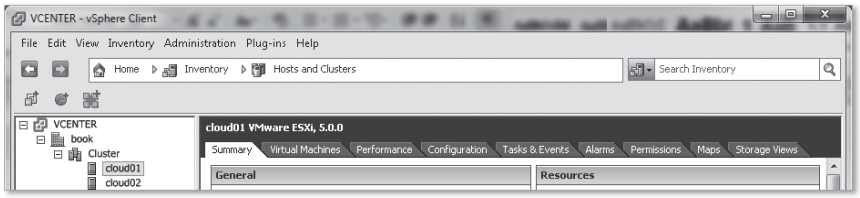


Abbildung 7.8 Reiter »vSphere Client«

Da es hierzu viele Fragen geben kann und eine falsche Konfiguration schnell zu Problemen führt, werden die einzelnen Punkte des Reiters in Tabelle 7.2 näher erläutert. Im Client stellt sich das dar wie in Abbildung 7.9.

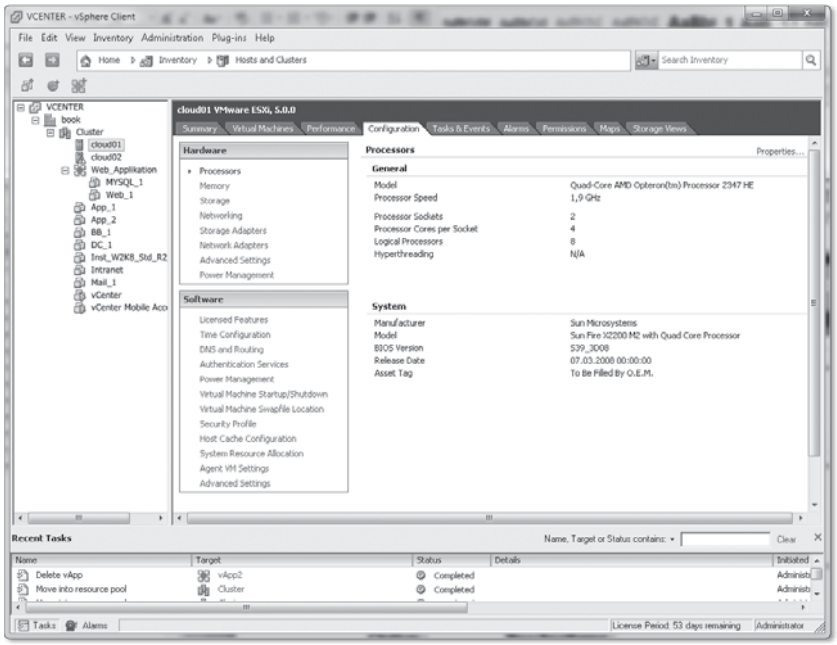


Abbildung 7.9 Host-Konfiguration

Option	Beschreibung
Processors	Die Option Processors zeigt alle vorhandenen Informationen zur im Server verwendeten CPU an. Außerdem werden allgemeine Informationen zum System wie zum Beispiel Hersteller, Modell und BIOS dargestellt. Über die Properties ist es möglich, Hyperthreading zu aktivieren oder zu deaktivieren.
Memory	Memory zeigt den physisch vorhandenen RAM an und wie viel Speicher dem vSphere-Host zugeordnet wird.
Storage	Die Option Storage ist eine der wichtigsten und gefährlichen Optionen. Hier gibt es die Möglichkeit, Datastores zu erstellen, zu löschen, zu formatieren und viele weitere Optionen. Die vorhandenen Datastores werden im oberen Fenster angezeigt. Wählen Sie einen solchen Datastore aus, sehen Sie im unteren Fenster die Details zu diesem Datastore. Bei ausgewähltem Datastore können Sie diesen über den Button Properties umbenennen und erweitern. Über den Button Add Storage erstellen Sie einen weiteren Datastore. Darauf gehen wir in Kapitel 8, »Netzwerk-Architektur«, näher ein.
Networking	Networking bietet die Möglichkeit, das Netzwerk des vSphere-Hosts zu konfigurieren. Dieser Teil ist sehr entscheidend bei der korrekten Konfiguration des Hosts. Ausführlich wird dieser Teil der Konfiguration in Kapitel 8 erläutert.
Storage Adapter	Storage Adapter zeigt alle vorhandenen Storage-Adapter im System an. Dazu zählen zum Beispiel Fibre-Channel-Host-Bus-Adapter, lokale SCSI-Adapter oder iSCSI-Adapter. Bei der Auswahl eines solchen Gerätes werden im unteren Fenster die Targets angezeigt, die dieser Adapter sieht. Über den Button Rescan scannt der Adapter einmal nach neuen LUNs. Wird zum Beispiel eine neue LUN präsentiert, müssen Sie erst einen Rescan durchführen, bevor diese sichtbar ist und damit Sie konfigurieren können. Wählen Sie eine LUN im unteren Fenster aus, können Sie die Pfade dieser LUN verwalten. Dafür aktivieren Sie mit der rechten Maustaste die LUN und wählen Manage Path aus. Darauf gehen wir ebenfalls detailliert in Kapitel 9 ein.
Network Adapter	Die Option Network Adapter zeigt alle installierten und verwendeten Netzwerkkarten des Hosts an.
Advanced Settings	An dieser Stelle wird die Funktion VMDirectPath parametriert. Diese Funktion erlaubt es, unterstützte Hardwarekomponenten direkt an eine virtuelle Maschine zu binden. Hier werden die Karten aufgelistet.
Power Management	Unter diesem Punkt lässt sich das Host-Verhalten im Hinblick auf die Einsparung von Strom konfigurieren. Das wird erreicht durch das Dynamic Voltage and Frequency Scaling (DVFS). Durch die Reduzierung der CPU-Frequenz wird eine Stromersparnis erzielt.
Licensed Features	Der Reiter Licensed Features zeigt die Lizenzierung des Hosts an. Über die Edit-Buttons passen Sie diese bei Bedarf an. Nähere Informationen zum Thema Lizenzen finden Sie in Kapitel 18, »Die Lizenzierung von vSphere«.

Tabelle 7.2 Optionen des Reiters »Configuration«

Option	Beschreibung
Time Configuration	Der Menüpunkt Time Configuration ermöglicht die Konfiguration der Uhrzeit sowie die Angabe von Time-Servern.
DNS and Routing	DNS and Routing zeigt alle Informationen über den Host-Namen und die DNS-Domäne an und ermöglicht die Bekanntgabe von DNS-Servern.
Authentication Services	An dieser Stelle können Sie festlegen, wie die Authentifizierung beim vSphere-Host erfolgt. Mögliche Optionen sind die lokale Authentifizierung oder die Anmeldung über einen Active-Directory-Server.
Power Management	Hier geben Sie die Parameter an, die benötigt werden, um einen Host aus- oder einzuschalten.
Virtual Machine Startup/ Shutdown	Es gibt die Option, die konfigurierten virtuellen Maschinen automatisch beim Starten oder Stoppen des vSphere-Hosts zu booten oder herunterzufahren. Dies können Sie hier über den Properties-Button konfigurieren.
Virtual Machine Swapfile Location	Das Swapfile, in das die virtuelle Maschine schreibt, kann im Ordner der virtuellen Maschine selbst oder in einem zentralen Ordner gespeichert werden. Dies konfigurieren Sie hier.
Security Profile	Hinter diesem Reiter versteckt sich die host-interne Firewall des vSphere-Servers. Eine Portfreischaltung erfolgt an dieser Stelle.
Host Cache Configuration	Auslagerung von Swap-Dateien auf schnelle SSD-Festplatten
System Resource Allocation	Der Reiter System Resource Allocation bietet die Möglichkeit, die Ressourcen des Host-Systems einzustellen. So können Sie zum Beispiel dem Host einen garantierten Wert an CPU und Memory zuweisen.
Agent VM Settings	Die Einstellung korrespondiert mit dem vSphere ESXi Agent Manager. Er dient zur Installation, Aktualisierung und Überwachung von Host-Agents.
Advanced Settings	Die Advanced Settings bieten eine große Zahl von Einstellmöglichkeiten. Bei den wenigsten ist genau bekannt, welche Folgen eine Änderung hat. Änderungen der Einstellungen sollten Sie mit VMware absprechen und intensiv testen. Es kann erforderlich sein, Anpassungen vorzunehmen, wenn der Hardwarehersteller es erfordert.

Tabelle 7.2 Optionen des Reiters »Configuration« (Forts.)

Tipp: Sprachenmix auf dem Client verhindern

Je nachdem, wie Sie den Client installiert und welche Sprachversion das Betriebssystem hat, kann es passieren, dass Sie einen Sprachenmix im vSphere-Client vorfinden. Mit einem Startparameter können Sie einen spracheinheitlichen Client forcieren:

- `locale en_US`: US-englisch
- `locale de`: deutsch
- `locale ja`: japanisch
- `locale zh_CN`: traditionell chinesisch

7.5 Administration über mobile Geräte

Auch wenn die Administration über die Multimedia Appliance immer noch im Beta-Status ist, so möchten wir hier darauf kurz eingehen und Ihnen zeigen, wie Sie die Konfiguration vornehmen. Als Beispiel werden wir den Zugriff über das Apple iPad zeigen. Schauen Sie auf der Webseite von VMware nach, welche weiteren Geräte mittlerweile von der Multimedia Appliance unterstützt werden. Importieren Sie das Paket für den vCenter Mobile Access (vCMA) über den vSphere-Client.

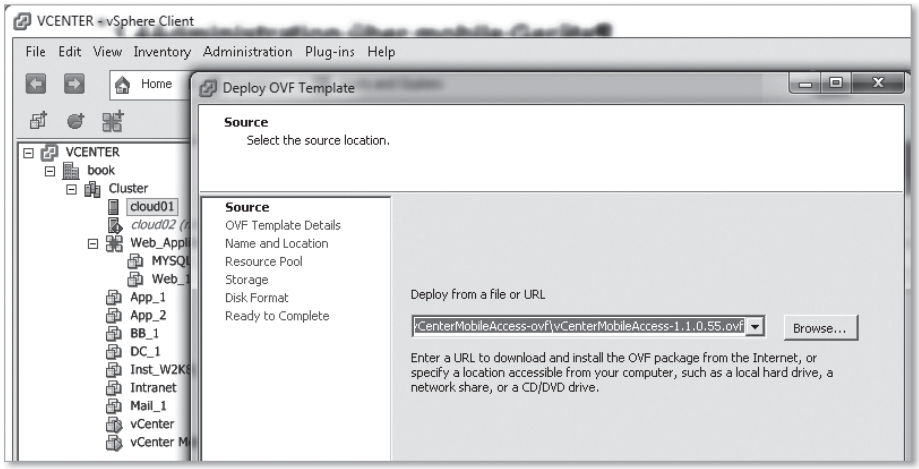


Abbildung 7.10 Import der vCMA-Appliance

Zuvor müssen Sie die Appliance von der VMware-Website herunterladen. Sie finden die Files unter *http://labs.vmware.com/flings/vcma*. Die Appliance stellt sich genauso dar wie andere VMware Appliances auch. Konfigurieren Sie einfach die IP-Adresse für die vCMA-Appliance, und schon können Sie mit dem mobilen Endgerät auf Ihre virtuelle Infrastruktur zugreifen.

Im Falle des iPads muss der vSphere-Client über den AppStore zuerst auf dem iPad installiert werden. Anschließend rufen Sie den Client auf und konfigurieren dort die IP-Adresse der vCMA-Appliance. Im Client selbst – dass sollte Ihnen bekannt vorkommen – müssen Sie den Namen oder die IP-Adresse des vCenter-Servers angeben und sich mit passenden User-Credentials anmelden, schon haben Sie Zugriff auf das vCenter mit allen Objekten. Bedenken Sie bitte, dass es sich nicht um einen vollwertigen Client handelt. Die Applikation bildet nur einen Teil der Funktionen ab, vergleicht man ihn mit dem Umfang der Version auf dem PC. Es folgen Screenshots, die Ihnen zeigen sollen, wie die Applikation auf dem iPad arbeitet.

Nach der erfolgreichen Anmeldung sehen Sie die Hosts in dem vCenter. Hier finden Sie leider nicht die einzelnen Datacenter bzw. VMware-Cluster. Auch wird ein Maintenance-Modus nicht angezeigt; wenn er aktiv ist. er ist nur dadurch sichtbar, dass er hier aber deaktiviert werden kann. Nach der Auswahl eines Hosts sehen Sie alle auf ihm registrierten VMs. Die Art

des Icons lässt direkt erkennen, welches Betriebssystem auf der VM installiert ist. Neben unterschiedlichen VM-spezifischen Informationen können Sie hier eine VM starten, stoppen, suspenden oder neu starten.

Abbildung 7.11 iPad-Ansicht für virtuelle Maschinen auf einem Host

Zu guter Letzt findet sich eine Anzeige der Performancewerte der einzelnen virtuellen Maschine, und zwar in vom vSphere-Client bekannter Art und Weise.

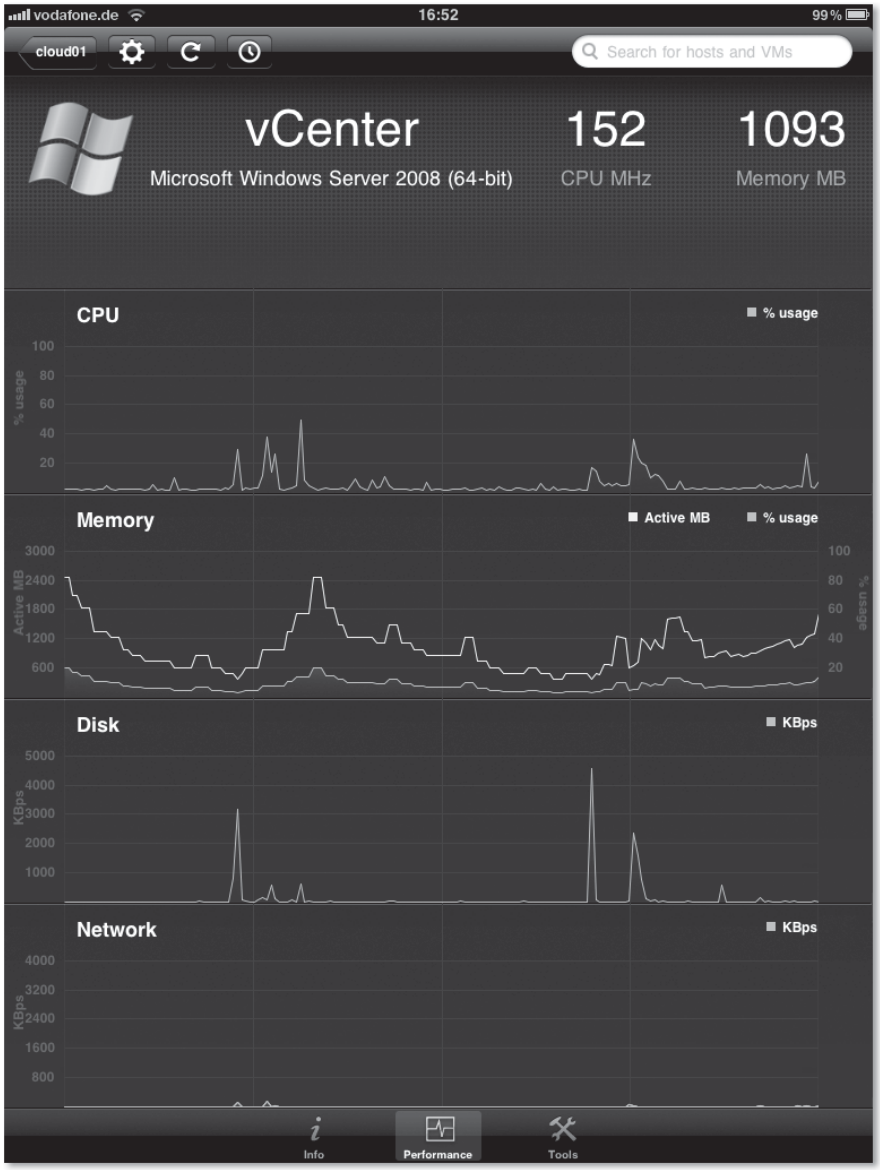


Abbildung 7.12 Anzeige der Performancewerte einer VM auf dem iPad

Auch wenn der vSphere-Client für das iPad nicht alle Funktionalitäten des Clients für den PC abdeckt, lassen sich einige rudimentäre Aufgaben mit ihm durchführen. Für eine einfache und schnelle Ansicht ist er allemal gut. Die Basis für mehr ist gelegt, und es bleibt abzuwarten, welche Funktionen noch in den vSphere-Client für mobile Geräte integriert werden.

7.6 vCenter-Server

Das vCenter ist, im Gegensatz zu den bisher vorgestellten Möglichkeiten der Administration, ein komplett eigenes Produkt. Das vCenter fasst die Administration von Hosts und virtuellen Maschinen in einem Tool zusammen. Des Weiteren stellt das Tool zusätzliche Funktionen zur Verfügung, die die Funktionalität der virtuellen Infrastruktur ausbauen, so dass Sie die Verfügbarkeit weiter erhöhen können. Für die Anmeldung am vCenter-Server wird der schon bekannte vSphere-Client eingesetzt. Statt des Host-Namens nutzen Sie zur Anmeldung den DNS-Namen des vCenters.

Ist die Anmeldung an einem vCenter-Server erfolgt, wird ein zweigeteiltes Fenster angezeigt (Abbildung 7.13). Auf der linken Seite finden Sie die Objekte der virtuellen Infrastruktur, wie Datacenter, Cluster, Hosts und VMs. Auf der rechten Seite sind die dem markierten Objekt zugeordneten Anzeige- und Konfigurationsparameter zu sehen. Welche Objekte gerade in der Oberfläche angezeigt werden, ist abhängig davon, welche Ansicht Sie gewählt haben. Auf die unterschiedlichen Ansichten werden wir später in den unterschiedlichen Konfigurationskapiteln näher eingehen.

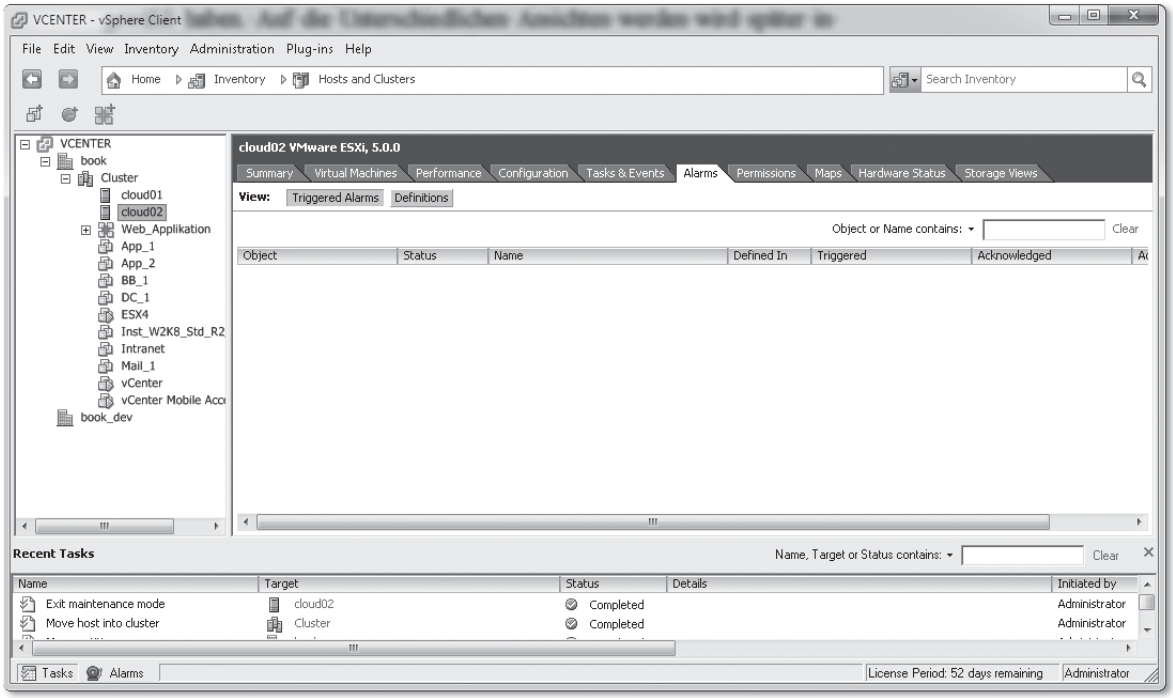


Abbildung 7.13 Startfenster des vCenter-Servers

Eine Übersicht über die einzelnen administrierbaren Funktionen wird beim Aufruf der Homepage sichtbar (Abbildung 7.14).

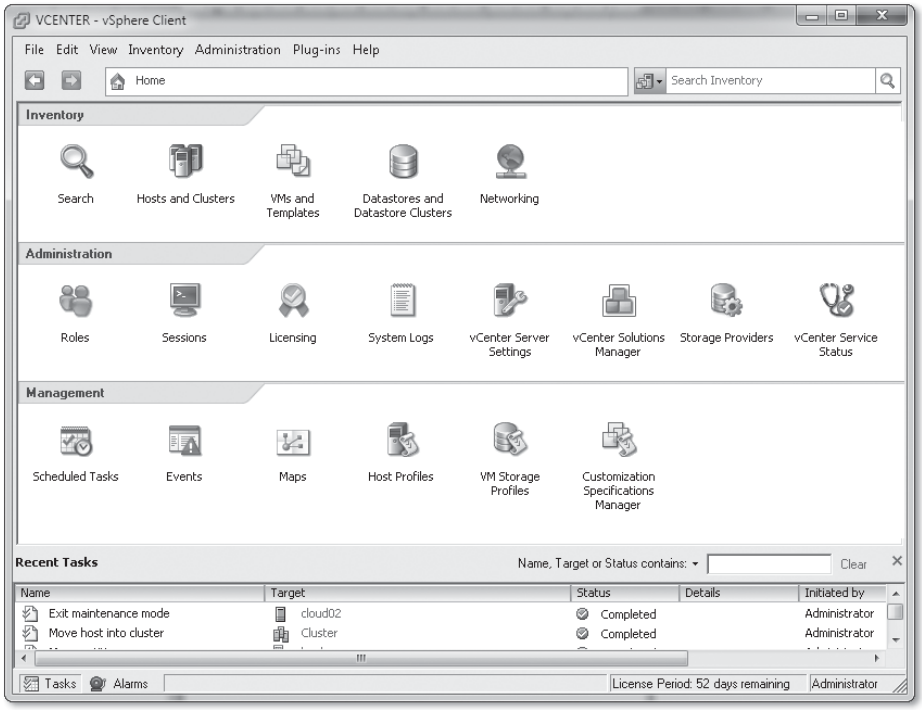


Abbildung 7.14 Homepage des vCenter-Servers

Die verwaltbaren Punkte sind nach Funktion gegliedert und übersichtlich angeordnet. Zu den Punkten Inventory, Administration und Management wird der Abschnitt Solutions and Applikations angezeigt, wenn z. B. der vCenter Converter, der vCenter Update Manager oder andere Zusatzsoftware installiert ist.

7.6.1 Installation des vCenter-Servers

Das vCenter kann unter Microsoft Windows installiert werden. Auch wenn es eine Unterstützung für Client-Betriebssysteme gibt, ist dies für den produktiven Einsatz nicht zu empfehlen. Für einen produktiven Einsatz ist unbedingt eines der unterstützten Server-Betriebsysteme zu verwenden (siehe Abschnitt 6.3.1), um Support von VMware zu erhalten. Alternativ nehmen Sie einfach die neue vCenter-Appliance. Das vCenter legt alle Daten in einer Datenbank ab, die lokal auf dem System des vCenter-Servers oder auf einem im Netzwerk befindlichen Datenbanksystem zur Verfügung gestellt wird.

Übrigens müssen Sie nicht zwingend eine Datenbank vorinstallieren, da die Installationsroutine des vCenters eine MS SQL 2008-Express-Datenbank mitinstallieren kann. Diese ist allerdings auf den Einsatz von wenigen vSphere-Hosts und einigen virtuellen Maschinen beschränkt. Eine genaue Anleitung zur Installation sowie alle weiteren wichtigen Randbedingungen finden Sie in Abschnitt 6.3, »VMware vCenter Server«.

7.6.2 Starten des vCenter-Servers

Nach der Installation des vCenters und einem Neustart des Systems können Sie auf das vCenter zugreifen. Zur Verbindung mit dem vCenter-Server benötigen Sie den vSphere-Client, den wir bereits in Abschnitt 7.4, »vSphere-Client«, beschrieben haben. Nachdem Sie diesen Client auf dem Administrations-PC oder einem beliebigen anderen PC, der das vCenter erreichen soll, installiert haben, kann er gestartet werden. Bei einer Installation auf derselben Maschine, auf der der vCenter-Server läuft, können Sie unter Host: »localhost« eingeben. Als Benutzername ist ein Windows-Benutzer mit den entsprechenden Rechten auszuwählen; es kann sich um einen lokalen oder einen Domänenbenutzer handeln. Laut Standardeinstellungen sind allerdings nur Benutzer mit lokalen Administratorrechten in den vCenter-Berechtigungen hinterlegt. Um einem »normalen« Benutzer Zugriff zu gewähren, müssen Sie für diesen zuerst in den vCenter-Berechtigungen ein Zugriffsrecht hinterlegen.

7.6.3 Hinzufügen von ESXi-Hosts ins vCenter

Ist die Oberfläche des Managementtools geladen, sehen Sie sofort die Ähnlichkeit zur direkten Verbindung des vSphere-Clients mit einem vSphere-Host. Beim erstmaligen Aufruf des nicht konfigurierten vCenter-Servers sehen Sie nur eine leere Oberfläche. Im ersten Schritt sind einige Konfigurationsschritte vorzunehmen, um das vCenter mit Leben zu füllen. Sie haben eine Reihe von Möglichkeiten der Gruppierung von Servern. Es empfiehlt sich, zuerst ein Datacenter anzulegen. Unter dieser Struktur können Sie dann Hosts in Clustern zusammenfassen. Um ein neues Datacenter anzulegen, klicken Sie mit der rechten Maustaste auf Host & Clusters und wählen aus dem Kontextmenü den Punkt New Datacenter. Nach der Anlage vergeben Sie für das Objekt einen passenden Namen, und damit ist die Arbeit abgeschlossen. Jetzt haben Sie zwei Optionen: Entweder hängen Sie die Hosts direkt unter dem Datacenter ein, oder Sie fassen sie in sogenannten *Clustern* zusammen. Darauf gehen wir in Kapitel 5 ein.

Ein Host fügt sich ebenfalls über das Kontextmenü ein, wenn es auf dem Datacenter geöffnet wird. Es startet ein Dialog, der dazu auffordert, hostspezifische Daten einzugeben (Abbildung 7.15).

Nach der Prüfung von Benutzername und Passwort wird eine Zusammenfassung des Hosts angezeigt, in der Sie u. a. den Namen des Hosts, den Server-Hersteller, die installierte vSphere-Version und bereits registrierte virtuelle Maschinen finden. Allerdings sollten Sie sich genau überlegen, ob Sie den Host mittels DNS-Name oder IP-Adresse hinzufügen. Gerade für spätere HA-Cluster und natürlich für die bessere Übersicht ist es sinnvoller, mit DNS-Namen zu arbeiten. Selbstverständlich können Sie auch im Nachhinein die Zuordnung des Hosts zur Organisationsgruppe ändern. Gehen Sie von einer Erstbenutzung des vCenters aus, müssen Sie erst ein Datacenter anlegen, bevor Sie einen Host ins Management aufnehmen können.

Jetzt wird der Host dem vCenter hinzugefügt. Nach ein paar Sekunden im Status Disconnected und dem Abschluss des Tasks Add Standalone Host ist der vSphere-Host über den vCenter-Server verwaltbar.

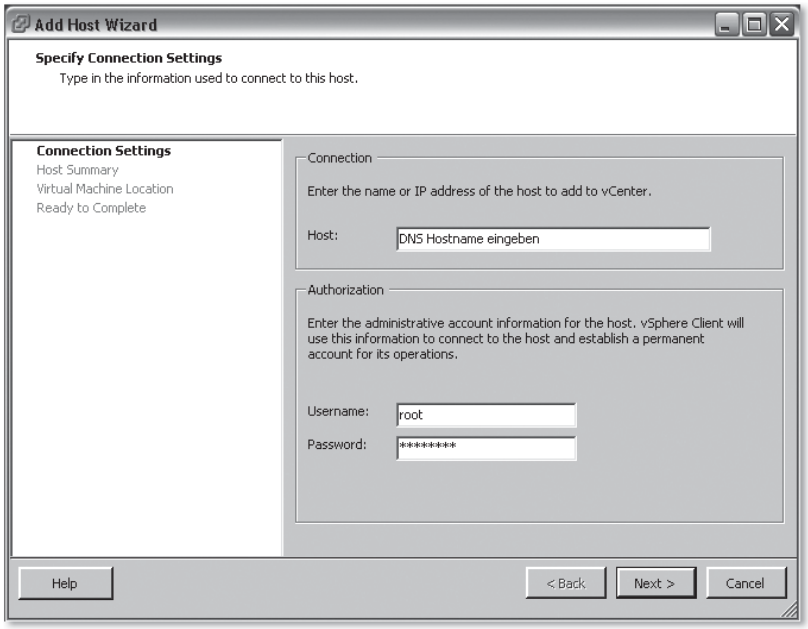


Abbildung 7.15 Einbinden eines Hosts ins vCenter-Management

7.6.4 Verwaltung von vSphere-Hosts

Nachdem die vSphere-Hosts hinzugefügt worden sind, ist es möglich, sie ähnlich wie bei der direkten Verbindung mit dem vSphere-Client auf einen Host zu verwalten. Wählen Sie im linken Fenster einen Host aus, werden im rechten Fenster verschiedene Informationen und Reiter angezeigt. Über diese Reiter verwalten Sie den Host und legen zum Beispiel ein virtuelles Netzwerk an. Die Reiter unterscheiden sich etwas von denen, die Sie sehen, wenn Sie sich direkt mit einem Host verbinden. Zur besseren Übersicht fügen wir noch einmal die gesamte Tabelle ein:

Reiter	Beschreibung
Summary	Unter dem Reiter Summary finden Sie eine Zusammenfassung über das gerade ausgewählte Objekt. Wählen Sie zum Beispiel einen vSphere-Host aus, sehen Sie allgemeine Informationen zum Host wie zum Beispiel Hersteller, CPUs oder RAM. Außerdem werden Informationen über die Ressourcen des Hosts angezeigt, zum Beispiel die verwendeten Datastores, die angelegten virtuellen Netzwerke und die Auslastung von RAM und CPU.
Virtual Machines	Den Reiter Virtual Machines finden Sie nur bei Objekten wie dem vSphere-Host oder einem Resource-Pool. Dort wird eine Liste aller virtuellen Maschinen angezeigt sowie deren Status bezüglich Ressourcen, Alarme und Power. Möglicherweise werden weitere Daten aufgelistet, abhängig davon, welche Ausgabefelder Sie in der Kopfzeile des Ausgabefensters aktiviert haben.

Tabelle 7.3 Reiter des vSphere-Clients

Reiter	Beschreibung
Performance	Unter Performance wird ein Diagramm dargestellt, das die Auslastung der verschiedenen Objekte illustriert. Die Ausgabewerte lassen sich den Erfordernissen des Administrators anpassen.
Configuration	Unter dem Tab Configuration können Sie alle Einstellungen eines vSphere-Hosts vornehmen. Dort ist es möglich, unter anderem das Netzwerk zu konfigurieren oder Datastores zu verwalten. Im weiteren Verlauf dieses Kapitels gehen wir noch einmal näher darauf ein.
Tasks & Events	Unter dem Reiter Tasks & Events werden alle protokollierten Tasks und Events aufgeführt.
Alarms	An dieser Stelle werden zum einen die Alarmdefinitionen angezeigt und zum anderen die aufgetretenen Alarme. Hier können Sie auch eine Quittierung der Alarme durchführen.
Permissions	Unter dem Reiter Permissions können Sie den Benutzern und Gruppen, die unter dem Reiter Users & Groups erstellt wurden, bestimmte Berechtigungen geben. Sie können mit vorgefertigten Benutzerrollen arbeiten, oder Sie legen eigene Rollen an, die die Arbeitsprozesse im Unternehmen widerspiegeln.
Maps	Eine grafische Darstellung der Infrastruktur der VM wird hier angezeigt.
Hardware-Status	Dieser Reiter ist hostspezifisch. Der Status der einzelnen Hardwarekomponenten wird an dieser Stelle dokumentiert und grafisch dargestellt.
Storage Views	Ähnlich wie bei dem Reiter Maps wird eine grafische Ausgabe erzeugt, die darstellt, wie welche Komponenten miteinander verbunden sind. Es ist ebenfalls möglich, die Ausgabe als Report anzeigen zu lassen.
Update-Manager	Sollten Sie Host und/oder VMs mit dem VMware Update Manager patchen, dann werden hier die Informationen zum Patch-Status des Objekts angezeigt.

Tabelle 7.3 Reiter des vSphere-Clients (Forts.)

Der Reiter Configuration stellt sich so dar, wie bereits in Tabelle 7.2 gelistet.

7.6.5 Weitere Funktionen durch vCenter-Server

Durch den Einsatz des vCenter-Servers ist es nicht nur möglich, mehrere vSphere-Hosts gleichzeitig zu verwalten. Es kommen viele Funktionen hinzu, die erst durch n + 1 Hosts und vCenter möglich werden. Einen Teil dieser Funktionen und Möglichkeiten werden wir in diesem Abschnitt kurz erläutern.

HA-Cluster

Durch einen Cluster erhalten Sie die Möglichkeit, einige neue Features zu verwenden, die ohne vCenter und ohne den Cluster so nicht möglich wären. So können Sie zum Beispiel *vSphere HA* (High Availability) verwenden. Dies bietet die Möglichkeit, eine virtuelle Maschine hochverfügbar zu machen. Hosts, die in einem Cluster zusammengefasst sind, prüfen untereinander gegenseitig die Verfügbarkeit der restlichen Hosts im Cluster. Beim Ausfall

eines physischen Hosts werden die virtuellen Maschinen, die auf diesem System betrieben wurden, automatisch auf den verbleibenden Hosts neu gestartet.

Virtual Machine Monitoring kommuniziert ständig mit den VMware Tools der virtuellen Maschine. Sollten diese in einem frei konfigurierbaren Zeitfenster nicht antworten, wird die virtuelle Maschine automatisch neu gestartet.

DRS-Cluster

VMware DRS (Distributed Resource Scheduling) bietet eine automatische Lastverteilung der virtuellen Maschinen über alle Hosts in einem Cluster. Erreicht wird diese Funktion durch die Unterstützung von vMotion. vMotion verschiebt virtuelle Maschinen ohne spürbare Unterbrechung von einem Host auf einen anderen. Eine Unterfunktion des DRS ist das Power-Management. Diese Option gibt dem Administrator ein Mittel an die Hand, zu lastarmen Zeiten vSphere-Hosts auszuschalten oder automatisiert ausschalten zu lassen. Steigt der Ressourcenbedarf wieder an, werden die vSphere-Hosts automatisch wieder gestartet.

EVC-Cluster

VMware EVC (Enhanced vMotion Compatibility) bietet einen Kompatibilitätsmodus, der vMotion zwischen Hosts ermöglicht, die unterschiedliche CPU-Typen verbaut haben. Der CPU-Herstellertyp muss schon identisch sein. Damit können Sie Cluster mit neueren Servern erweitern und die VMs in aktivem Zustand auf die neuen vSphere Server migrieren, ohne eine Unterbrechung zu haben. Nach abgeschlossener Migration können die alten Hosts dann abgebaut werden.

All diese Funktionen sind nur durch die Verwendung des VMware vCenter Servers möglich. Sie sehen also, dass das VMware vCenter nicht nur eine leichtere und komfortablere Administration mehrerer vSphere-Hosts ermöglicht, sondern dass auch viele weitere Funktionen hinzukommen.

7.6.6 Einbindung ins Active Directory

Auch wenn die Möglichkeit besteht, sich am vCenter-Server mit lokalen Accounts anzumelden, ist das sicherlich nicht immer das Mittel der Wahl. Viele Unternehmen haben bereits ein Active Directory, in dem User gepflegt werden, und da ist es nicht sehr sinnvoll, zusätzlich lokale User für einen vCenter-Server zu pflegen oder dort neue Benutzer einzurichten. Das hat auch VMware erkannt und deshalb die Möglichkeit geschaffen, den vCenter-Server in ein vorhandenes Active Directory einzubinden. Dort haben Sie die Option, Gruppen für den Zugriff auf das vCenter anzulegen und diese dann im vCenter zu berechtigen. Als Ergebnis werden die User nur noch an einer Stelle gepflegt, was den administrativen Aufwand stark reduziert.

Für diese AD-Integration sind keine aufwendigen Arbeiten notwendig. Es genügt, den vCenter-Server in die Domäne aufzunehmen, in der die User-Konten liegen. Nach der Berechti-

gungserteilung an die User bzw. Gruppen im vCenter ist der Zugriff mit Domänen-Accounts möglich (Abbildung 7.16).

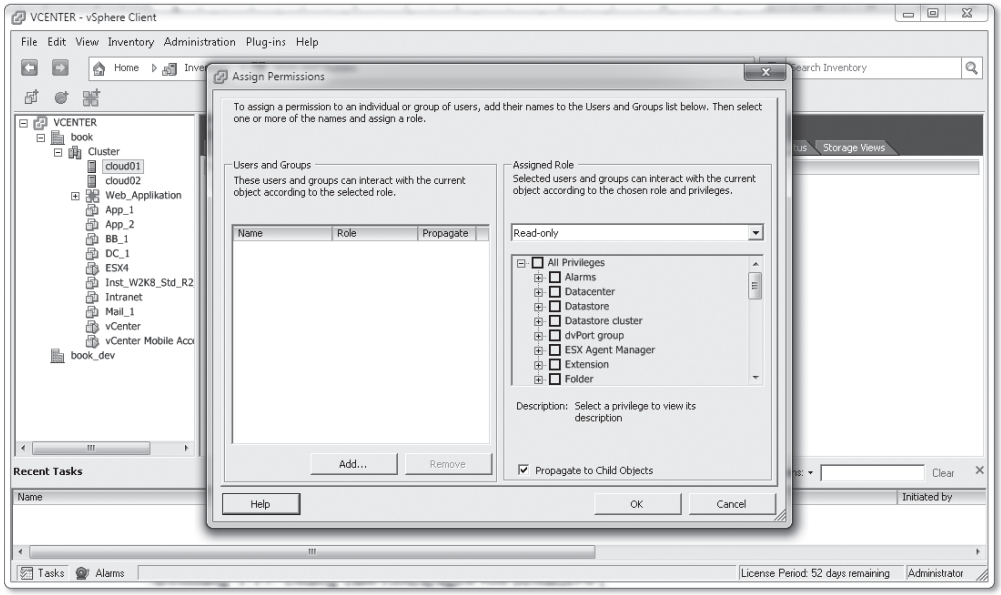


Abbildung 7.16 Dialog zum Hinzufügen von Benutzern

Über Add fügen Sie einen Benutzer hinzu, indem Sie im Folgedialog die Domäne als Basis der Benutzerauswahl angeben. Mit Assign Role weisen Sie dem entsprechenden Benutzer passende Rechte zu. Neue Rollen lassen sich über Home • Administration • Role anlegen (Abbildung 7.17). Empfehlenswert ist es, an der Stelle vorhandene Rollen so zu belassen, wie sie sind, und nicht zu manipulieren. Möchten Sie ähnliche Rollen erstellen, dann besteht die Möglichkeit, eine vorhandene Rolle zu kopieren und entsprechend anzupassen. Näheres dazu finden Sie in Kapitel 12, »Konfiguration von ESXi und vCenter«.

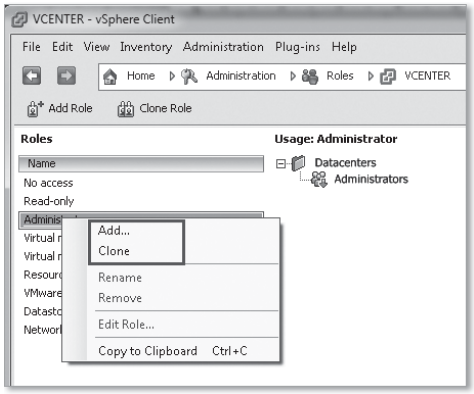


Abbildung 7.17 Anlegen von neuen Rollen

7.6.7 Troubleshooting vCenter-Server

Sollte der Dienst des vCenters nicht starten, können Sie den Vorgang auch über die Kommandozeile initiieren. In diesem Fall ist besser sichtbar, welche Probleme den Start des Dienstes verhindern. Auf diese Art sehen Sie genau, bei welcher Aktion das Starten des vCenters abgebrochen wurde.

Dazu führen Sie einfach den Befehl:

`C:\Program Files\VMware\VirtualCenter Server\vpxd.exe -s` aus.

Nachdem Sie das vCenter mit dem Parameter `-s` aufgerufen haben, erscheint ein DOS-Fenster, das die verschiedenen Arbeitsschritte beim Starten des vCenters anzeigt. Bleibt beim Start die Ausgabe bei einem Fehler hängen, können Sie diesen schnell und einfach analysieren.

Des Weiteren lassen sich die vCenter-Log-Dateien für die Fehleranalyse exportieren. Auch die Tiefe des Log-Levels lässt sich genau einstellen (Abbildung 7.18).

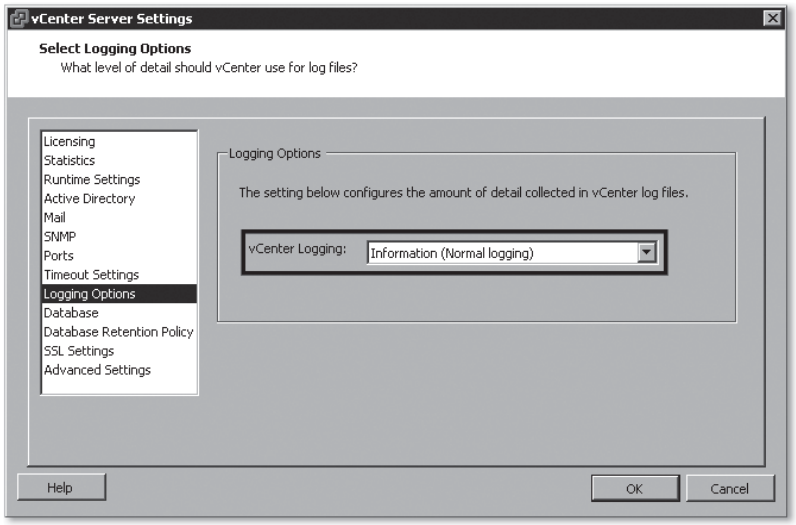


Abbildung 7.18 Einstellen des Log-Levels im vSphere-Client

Ändern Sie das Log-Level nur, wenn Sie Probleme haben und die Ursachen erforschen wollen. Sind die entsprechenden Arbeiten abgeschlossen, setzen Sie das Level, im eigenen Interesse, wieder auf den Standard (INFORMATION) zurück.

Möchten Sie ein Log der gesamten Infrastruktur oder von Teilen der Infrastruktur haben, dann lässt sich das über das Menü bewerkstelligen (Abbildung 7.19).

Erschrecken Sie nicht – das kann durchaus einige Zeit in Anspruch nehmen. Die Granularität des Exports lässt sich parametrieren.

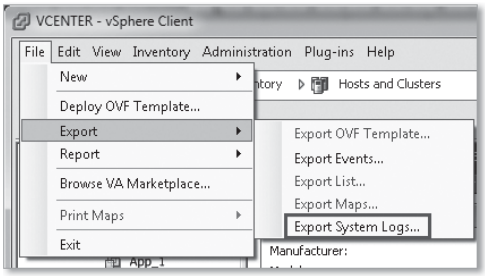


Abbildung 7.19 Export von Log-Dateien

7.7 Remote Command-Line Interface

Das Remote Command-Line Interface (folgend auch *Remote CLI* genannt) gewinnt stark an Bedeutung. Es wird genutzt, um remote Befehle auf ESXi-Hosts abzusetzen. Die Service Console ist ja passé. Um weiterhin Skripte und Anwendungen ausführen und Konfigurationen vorzunehmen zu können, ohne den vSphere-Client nutzen zu müssen, wird das Remote CLI verwendet.

Alternativ können Sie auch den vSphere Management Assistant nutzen (vMA). Hierbei handelt es sich, einfach ausgedrückt, um eine Linux-basierte Appliance, in der das Remote Command-Line Interface direkt installiert ist.

7.7.1 Installation

Alle Installationsdateien des Remote CLI sind auf der Webstartseite des Hosts herunterladbar. Verbinden sie sich einfach mit dem Browser auf die Startseite des ESXi-Hosts, und laden Sie dort die nötigen Tools herunter (Abbildung 7.20). Die Links routen Sie auf die Webseite von VMware, wo Sie die gewünschte Software zum Download finden.

Die Namen der vSphere-CLI-Befehle entsprechen denen der Befehle auf der Service Console. Hier sehen wir einen großen Vorteil: So müssen Sie sich für eine Funktion nicht unterschiedliche Befehle merken und können so auf einfachem Wege Ihre Arbeiten durchführen.

Installation unter Linux

Für eine Installation unter Linux ist zuerst zu untersuchen, ob das Zielsystem eine 32-Bit- oder eine 64-Bit-Plattform ist. Laden Sie dann die entsprechende Version herunter.

Kopieren Sie die Datei *VMware-vSphere-CLI-5.0.0-#####.i386.tar.gz* auf das gewünschte Linux-System in den Ordner */tmp*, und entpacken Sie sie mit `tar xzvf VMware-vSphere-CLI-5.0.0-#####.i386.tar.gz`.

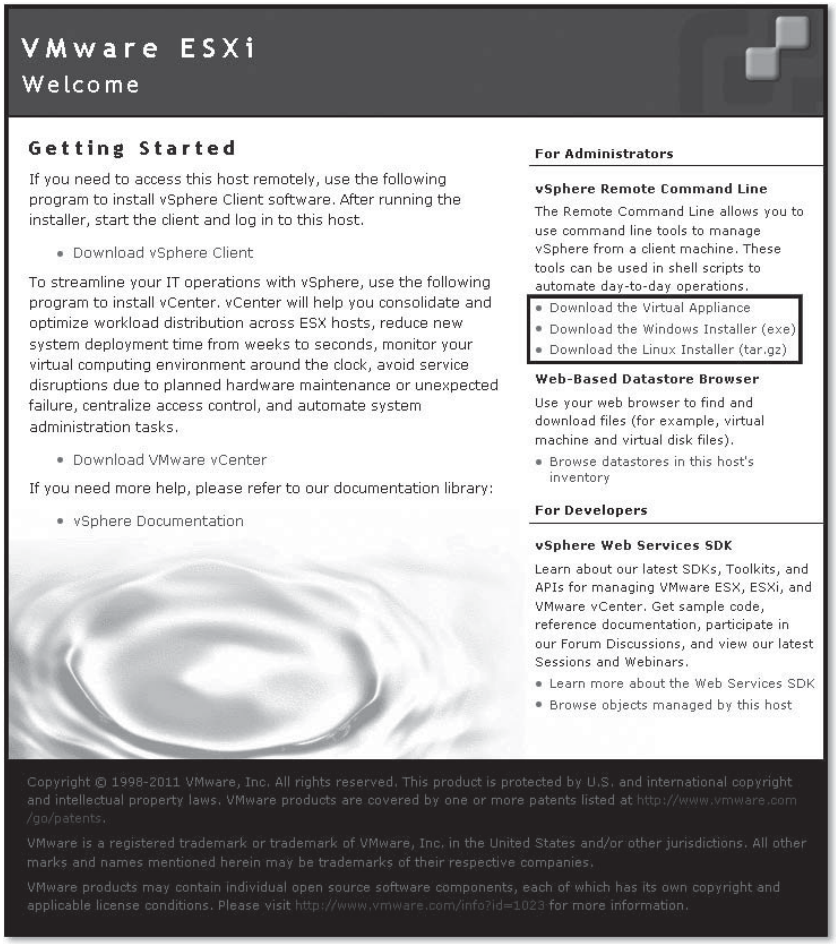


Abbildung 7.20 Download des vSphere CLI

Es wird dadurch ein Verzeichnis *vmware-vsphere-cli-distrib* erstellt, in dem alle entpackten Dateien gespeichert werden. Die Installation wird mit `/tmp/vmware-vsphere-cli-distrib/vmware-install.pl` ausgeführt, wodurch alle Dateien laut Standardeinstellungen nach */usr/bin* kopiert werden. Eine Deinstallation führen Sie mit `/usr/bin/vmware-uninstall-vSphere-CLI.pl` durch.

Nach der erfolgreichen Installation finden sich viele `vicfg-` und `esxcfg-` Kommandos auf dem System wieder, die Ihnen nicht fremd sein sollten.

Arbeiten Sie mit einem 64-Bit-Linux-Derivat, dann wählen Sie die passende Datei. Diese trägt den Namen *VMware-vSphere-CLI-5.0.0-#####.x86_64.tar.gz*. Das Entpacken und Installieren erfolgt wie oben beschrieben.

Windows-Installation

Das Remote CLI für die Installation unter Windows kommt als normale Setup-Routine daher und läuft nach dem Start komplett selbständig durch. Nach Fertigstellung befindet sich eine ActivePerl-Installation auf dem Endgerät. Im Verzeichnis *%Programfiles%\VMware\VMware vSphere CLI\bin* liegen die Perl-Skripte.

vSphere Management Assistant (vMA 5.0)

Eine weitere Alternative ist der Import der Management-Appliance von VMware, die alle benötigten vSphere-CLI-Komponenten samt Gastbetriebssystem enthält. Die Virtual Appliance importieren Sie idealerweise mit dem vSphere-Client über File • Virtual Appliance • Import. Sie bietet den großen Vorteil, dass keine Client-Komponenten installiert werden müssen und so alle Administratoren immer mit der gleichen Version arbeiten!

7.7.2 Ausführen des vSphere CLI

Nach der Installation des vSphere CLI können Sie die mitgelieferten vSphere-Befehle ohne Probleme in der Kommandozeile ausführen. Für die Syntax der Befehle ist eine passende Hilfe in der Kommandozeile selbstverständlich enthalten.

Ausführen auf Linux-Systemen

Um auf einem Linux-System die Remote-CLI-Befehle auszuführen, müssen Sie als erstes ein Command-Prompt öffnen. In diesem Fenster setzen Sie den gewünschten Befehl ab. Als Beispiel soll hier mit dem folgenden Kommando ein Storage-vMotion-Vorgang durchgeführt werden:

```
svmotion --server <virtual_center_server> --username <user>
  --password <user_password> --help
```

Ausführen auf Windows-Systemen

Das Ausführen unter Windows ist ähnlich wie unter dem Betriebsystem Linux. Öffnen Sie auch hier ein Command-Prompt. Das Wechseln in das Installationsverzeichnis des vSphere CLI ist nicht notwendig, weil der Pfad in die entsprechende Environment-Variable aufgenommen wird.

Auch hier können Sie anschließend den gewünschten Befehl absetzen. Wie auch unter Linux nehmen wir dafür als Beispiel den Storage-vMotion-Befehl:

```
svmotion --server <virtual_center_server> --username <user>
  --password <user_password> --help
```

Ausführen auf der Virtual Appliance

Die Installation des vMA 5.0 haben wir bereits in Abschnitt 6.5.1, »Installation«, beschrieben. Zwei Optionen stehen Ihnen bei der Nutzung des vMA zur Verfügung: Entweder stellen Sie direkt eine Verbindung zu einem ESX-/ESXi-Host her, oder Sie initiieren die Verbindung zu einem vCenter-Server. Bei einer Verbindung zu einem vCenter-Server ist es nicht mehr notwendig, sich zusätzlich mit den einzelnen Hosts zu verbinden. Diese Verbindungen sind über das vCenter automatisch vorhanden.

Auf der Appliance werden unterschiedliche Schnittstellen zur Verfügung gestellt. Tabelle 7.4 listet die Schnittstellen mit ihren Funktionen auf.

Schnittstelle	Typ	Kommando	Funktion
`vifptarget`		`vifptarget`	Festlegen des Default-Ziels
`vifp`	Administrative Interface	`addserver`	Hinzufügen eines Hosts oder vCenter-Servers
		`listservers`	Listet alle Target-Systeme auf.
		`removeserver`	Entfernen eines Hosts oder vCenter-Servers
		`rotatepassword`	Lebensdauer des Passworts für des gemanagte System (nicht für vCenter-Server)
		`reconfigure`	Anpassen der Authentifizierungsart
`vmatargetlib`	Library	`enumerate_targets`	Auflistung der mit dem vMA gemanagten Systeme
		`Query_target`	Anzeigen der Verbindungsinformationen zu den Ziel-Servern
		`login`	Verbindung zum Ziel-Server herstellen
		`logout`	Verbindung zum Ziel-Server unterbrechen

Tabelle 7.4 Schnittstellen des vMA 5.0

Findet die Verbindung der Zielsysteme mit VI-FASTPASS statt, werden die Passwörter nicht verschlüsselt! VI-FASTPASS managt die Accounts für die Verbindung zwischen vMA und den Zielsystemen. So ist es nicht erforderlich, jedes Mal beim Absetzen eines Befehls die Accounting-Daten erneut einzugeben.

Ist alles eingerichtet, stehen Ihnen die Befehle des vSphere CLI und die vSphere-SDK-Perl-Skripte zur Verfügung.

7.8 VMware vSphere PowerCLI

Das VMware vSphere PowerCLI (im Folgenden auch *PowerCLI* genannt) setzt auf die Microsoft Windows PowerShell auf und ermöglicht eine sehr schnelle, einfache und unkomplizierte Administration der VMware Virtual Infrastructure. Die Basis bildet die PowerShell von Microsoft. Microsoft hat mit diesem Kommandozeilentool, das Schnittstellen in viele bekannte Systeme, wie z. B. das .NET Framework, hat, eine übergreifende Shell programmiert, die sich an bereits bekannten Systemen orientiert. Das PowerCLI gliedert sich in diese Shell ein und stellt Ihnen eine große Anzahl von Befehlen zur Administration von vSphere-Umgebungen zur Verfügung. So reichen zum Teil nur wenige Zeichen Code zur Abarbeitung von Aufgaben in der virtuellen Infrastruktur.

Die erstellten Skripte können Sie an einzelnen oder mehreren Objekten gleichzeitig ausführen. Damit Sie ein Gefühl für die geringe Komplexität der Skripte bekommen, sei hier ein Beispielskript aufgeführt, das einen Rescan aller Host-Bus-Adapter der angewählten Hosts durchführt:

```
$_ | Get-VMHostStorage -RescanAllHBA
$_ | Get-VMHostStorage -Refresh
```

Mit etwas Einarbeitung ist es schnell möglich, komplexe Skripte zu erstellen, mit denen der Administrator die Aufgaben erfüllen kann, die ihm im Tagesgeschäft begegnen. Die Möglichkeiten, die sich Ihnen hier eröffnen, werden jedem sofort bewusst, wenn er sich seine täglichen administrativen Aufgaben anschaut. Nun ist es nicht jedermanns Sache, auf der Kommandozeile herumzuzaubern.

Welche Wichtigkeit die PowerShell-Schnittstelle für VMware hat und wie VMware diese Schnittstelle den Administratoren noch näherbringen möchte, zeigt die Software Onyx. Die Software zeichnet Aktionen auf, die Sie im vCenter durchführen, und erzeugt im Anschluss daran ein lauffähiges PowerShell-Skript. Man darf gespannt sein, wie sich das Thema noch weiterentwickelt. Außerdem bestätigt sich das mit den neuen Funktionen, die VMware bereitgestellt hat. Diese Funktionen betten sich tief in das PowerCLI ein und erweitern die Funktionalitäten dieser Managementschnittstelle um ein Vielfaches. So gibt es manche Funktionen, die nur über das PowerCLI abgebildet werden können.

Aus welchen Elementen besteht die Netzwerkanbindung von vSphere? In welcher Situation verwende ich welche Netzwerk-Designs? Wie integriere ich vSphere in bestehende Netzwerkumgebungen? Diese Fragen rund um das Netzwerk behandeln wir in diesem Kapitel.

8 Netzwerk-Architektur

Autor dieses Kapitels ist Urs Stephan Alder, KYBERNETIKA AG/d-on-d, usa@kybernetika.ch

Das Netzwerk spielt in jeder Server- oder Client-Virtualisierungs-Lösung eine zentrale Rolle. Findet darüber doch die Kommunikation zwischen den beteiligten Elementen im Netzwerk statt: vom vSphere-Client und vCenter zu den Virtualisierungs-Hosts, der Netzwerkverkehr zwischen den Virtualisierungs-Hosts untereinander, die Kommunikation zu und von den virtuellen Maschinen, der Zugriff vom Virtualisierungs-Host zu IP-basierten Speichersystemen. Die Netzwerkanbindung kann von sehr einfach bis hochkomplex ausfallen, je nach der gewünschten Leistung und Integration in bestehende Netzwerkumgebungen.

8.1 Grundsätzliche Planungsaspekte

Bei der Planung für eine zukünftige Netzwerk-Implementation müssen Sie sehr viele Aspekte berücksichtigen. Der Planungsablauf stellt ein Wechselspiel zwischen vorhandener und zu beschaffender Technologie im Kontrast zu den Konfigurationsmöglichkeiten im Netzwerk-Stack von vSphere dar.

8.1.1 Gutes Netzwerk-Design

Das Netzwerk-Design unter vSphere sollte mehr enthalten als »ich kann den Host pingen – alles ist gut«. Designfehler können üble Folgen haben, bis zum gleichzeitigen Totalausfall aller VMs in einem Cluster, weil das Netzwerk-Design den Anforderungen von HA (High Availability) nicht genügte.

Was macht also ein gutes Design aus? Folgende Punkte sollten erfüllt sein:

- **Das Netzwerk ist robust gegenüber Ausfällen.**
  Hier ist insbesondere wichtig, dass das Design nicht an den Netzwerkschnittstellen des ESXi-Hosts aufhört. Die physische Netzwerkinfrastruktur muss einbezogen werden, und

die Verteilung der physischen Netzwerkkarten auf die physischen Switches muss korrekt sein. Die physische Verteilung der Netzwerkkomponenten muss dann entsprechend auf den virtuellen Switches umgesetzt werden. Das bedeutet, dass für die Uplinks an den virtuellen Switches auch die Netzwerkkarten verwendet werden, die je an einen anderen physischen Switch gesteckt sind.

- **Das Netzwerk erfüllt die Leistungsanforderungen.**
  Alle I/O-Muster können auch zu Spitzenzeiten abgedeckt werden.
- **Die vorhandenen Ressourcen sollen gut genutzt werden.**
  Das bedeutet, dass die idealen Load-Balancing-Policies verwendet werden, so dass die I/O-Last auf den Netzwerkkarten gleichmäßig verteilt wird.
- **Verschiedene Verkehrsmuster trennen**
  Wie I/O der VMs, vMotion, FT, iSCSI, NFS, HA-Heartbeat, Management-Verkehr – sollten möglichst voneinander getrennt werden. Wenn das nicht geht, weil nicht genügend Netzwerkkarten zur Verfügung stehen, sollten Sie die Verkehrsmuster entweder vernünftig kombinieren oder mittels Active-/Standby-Adaptern oder Network I/O Control modellieren.
- **Sicherheitsaspekte sollten berücksichtigt werden.**
  Verschiedene Netze gehören getrennt. Es ist zum Beispiel eine sehr schlechte Idee, das Benutzernetz mit dem iSCSI-Storage-Netz zu kombinieren. Wenn denn ein Benutzer einmal eine statische IP-Adresse an die Netzwerkkarte seines Notebooks vergibt, die derjenigen des iSCSI-Targets entspricht, dann ist viel Spaß in der Infrastruktur garantiert.

8.1.2 1- und 10-Gigabit-LAN, maximale Anzahl physischer NICs

Eine der ersten Fragen ist: Welche Technologie wird eingesetzt, 1 Gigabit oder 10 Gigabit? In dieser Hinsicht gibt es Unterschiede bei der maximal zugelassenen Anzahl von physischen Ports. Bei 1 Gigabit ist das Maximum, abhängig vom verwendeten Netzwerkkarten-Produkt, 32 Ports, bei 10 Gigabit sind es 8 physische Ports. Eine Kombination von beiden Adaptern ergibt 4 × 1 Gigabit und 6 × 10 Gigabit. Diese Grenze können Sie in der Dokumentation »Configuration Maximums for VMware vSphere 5.0« nachschlagen:

http://www.vmware.com/pdf/vsphere5/r50/vsphere-50-configuration-maximums.pdf

Da sich diese Angaben bei neuen Versionen von vSphere ändern können, ist jeweils das passende Dokument zu der entsprechenden vSphere-Version zu verwenden. Zu beachten ist auch, dass neben den von VMware angegebenen Maxima auch solche vom Hersteller des Servers existieren können. Es ist zum Beispiel wenig sinnvoll, 8 Mal eine 10-GB-NIC in ein 2-CPU-Server-Modell zu verbauen, weil der I/O-Stack eines solchen Servers gar nicht fähig ist, diese große Datenmenge zu bewältigen, und hinsichtlich vieler Interrupts in der Leistung einbricht.

8.1.3 1 und 10 Gigabit versus Load-Balancing und Verkehrsmuster-Kontrolle

Nebst der maximalen Anzahl physischer Ports, die im Host verbaut werden können, hat die Verwendung von 1- oder 10-Gigabit-Technologie auch Einfluss auf die Verwendung der Load-Balancing-Policy. Bei 1 Gigabit geht es eigentlich immer darum, »den Kanal« zu vergrößern und über ein entsprechendes Teamkonstrukt ein möglichst ideales Load-Balancing zu erreichen. Wird 10-Gigabit-Technologie verwendet, so steht weniger der Load-Balancing-Mechanismus im Vordergrund, vielmehr müssen verschiedene Verkehrsmuster in dem »breiten Kanal« ideal getrimmt werden. Verkehrsmuster auf einem Kanal zu trimmen, bedeutet zwingend die Verwendung eines vNetwork Distributed vSwitches, da der vNetwork-Standard-vSwitch keine Möglichkeit für Network I/O Control bietet.

8.1.4 Wie viel Bandbreite benötige ich in der Praxis wirklich?

Bandbreiten- und designtechnisch gesehen ist 10 Gigabit sicher die erste Wahl, weil es einfach die flexibelsten Möglichkeiten bietet. Informatik ist meist budget-getrieben, und es stehen nicht für alle IT-Betreiber die Mittel für 10-Gigabit-Backbones zur Verfügung. Was in der Praxis sicher gesagt werden kann: Mit 1 Gigabit, in Zusammenhang mit einem intelligenten Design, kommen Sie sehr weit. Für heutige Server mit 2 CPUs genügt mehrfaches 1 Gigabit im Aggregat vollumfänglich. 4-CPU-Server gehen mit 1-GB-Aggregaten an der Grenze. Bei Blade-Systemen mit vollen Chassis und Blades, prall gefüllt mit RAM, ist 10 Gigabit ein Muss, um die I/O-Leistung der vielen Server im Blade-Chassis optimal nutzen zu können. In Bezug auf Storage-Anbindung ist mehrfaches 1 Gigabit im Entry-Level-Bereich unproblematisch und reicht vollauf. Sobald eine Stufe höher geschaltet wird, ist 10 Gigabit zu bevorzugen oder gar ein Muss.

8.1.5 VLANs oder keine VLANs?

ESXi-Hosts können Sie mit oder ohne VLANs betreiben. Selbstverständlich ist auch ein Mischbetrieb möglich. Keine VLANs zu verwenden, führt bei mehreren Netzwerksegmenten dazu, dass diese Segmente physisch ab dem ESXi-Host erschlossen werden müssen. Eine hohe Anzahl an physischen Ports im ESXi-Host ist damit die Folge (Abbildung 8.1).

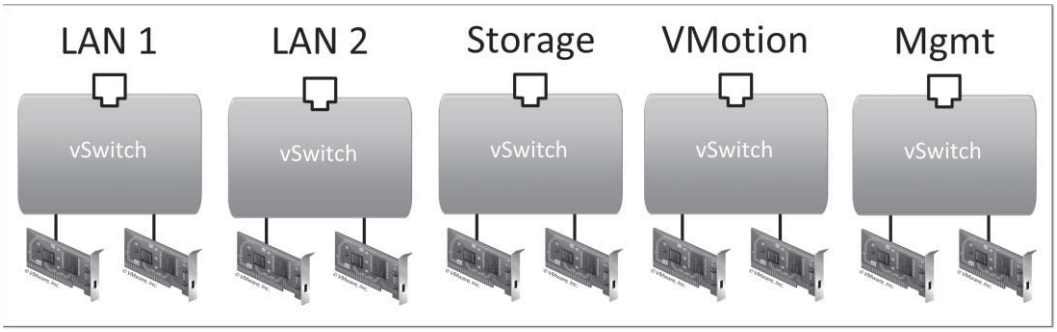


Abbildung 8.1 5 Segmente ohne VLAN, redundant

Ein Beispiel:

Anforderung: Es sollen fünf Segmente gebildet werden. VLANs werden nicht eingesetzt. Es ist ferner erforderlich, dass Redundanz vorhanden ist.

Das bedeutet, dass mit physischen Netzwerkkabeln in jedes einzelne Segment verbunden werden muss. Für jedes Segment muss ein virtueller Switch gebildet werden. Damit die Redundanz gewährleistet ist, müssen zwei physische Netzwerkkarten an einem virtuellen Switch vorhanden sein. Da eine Netzwerkkarte nur einem virtuellen Switch zugeordnet werden kann, führt dies zu einer Anzahl von 10 physischen Netzwerkkarten.

Verwenden Sie VLANs verwendet und konsolidieren Sie alles auf einen vSwitch, so können Sie massiv physische Netzwerkkarten, Kabelverbindungen und Switch-Ports und letztendlich auch Kosten einsparen. Das Beispiel in Abbildung 8.2 zeigt, dass es möglich ist, 60 % der Netzwerkkarten einzusparen und trotzdem praktisch dieselbe Qualität der Netzwerkanbindung zu erreichen.

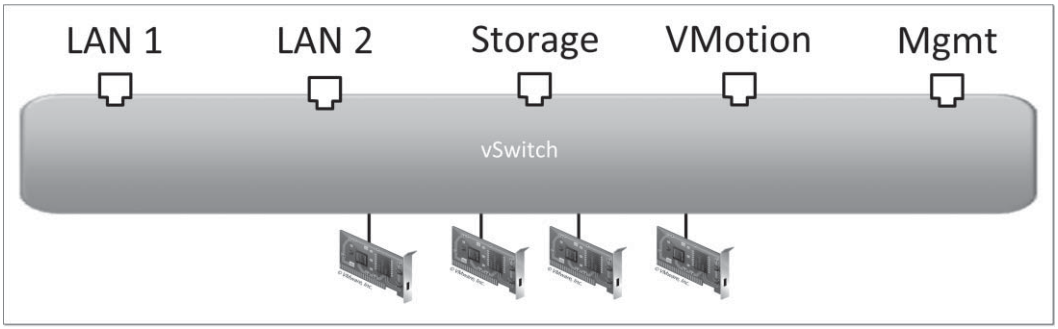


Abbildung 8.2 5 Segmente mit VLAN, mehrfach redundant

8.1.6 Physische Switches können die Load-Balancing-Policy beeinflussen

Um ein voll redundantes Design zu erhalten, müssen die Netzwerkkarten in einem Host auf mindestens zwei physische Switches verteilt werden. Die verwendeten Switch-Komponenten im LAN haben einen Einfluss auf die zu verwendende Load-Balancing-Policy in vSphere. Die Load-Balancing-Policy »IP-Hash« bedingt, dass die physischen Switch-Komponenten einen Etherchannel, statisches LACP oder eine Link-Aggregation nach IEEE 802.3ad bilden. Damit ergibt sich die zentrale Frage: Kann ich mit den eingesetzten Switches einen Channel über die Switch-Ports von mehreren Switches erzeugen (Abbildung 8.3)?

Nur wenn sich diese Frage mit »ja« beantworten lässt, können Sie die Load-Balancing-Policy »IP-Hash« verwenden. Selbstverständlich können Sie in diesem Fall auch alle anderen Policies auf diesen Switches benutzen, ohne ein Aggregat auf diesem physischen Switch zu konfigurieren. Lautet die Antwort »nein«, so können Sie alle Policies, außer »IP-Hash«, verwenden.

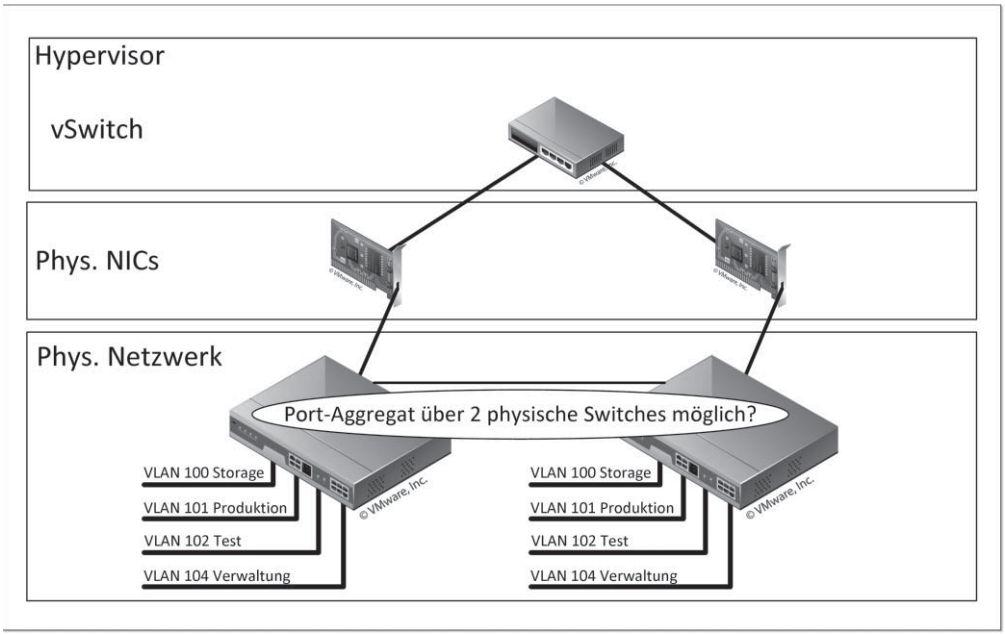


Abbildung 8.3 Channel über mehrere Switches möglich?

8.1.7 Links zwischen den physischen Switches

Ein Aspekt, dem Sie unbedingt Rechnung tragen sollten, sind die Verbindungen von physischen Switches untereinander. Es nutzt nichts, wenn Ihr ESXi-Host-Netzwerk-Design nach Best Practice durchgeführt wurde, aber die Kommunikation von einem ESXi-Host zu einem anderen ESXi-Host, die je an verschiedenen physischen Switches verbunden sind, über einen 1-Gigabit-Link zwischen den physischen Switches stattfindet. Verbindungen zwischen physischen Switches sind so auszulegen, dass der Verkehr zwischen physischen Switches nicht als Begrenzer wirkt! Im extremsten Fall muss solch ein Link mehrfaches vMotion, Storage-Zugriff, Fault Tolerance und VM-Netzwerkverkehr verdauen. Können Sie die Links zwischen den physischen Switches nicht entsprechend gestalten, so sollten das Design mit Active und Standby-Adaptern in den ESXi-Servern und der Konzentration auf einen physischen »Haupt-Switch« erfolgen. Damit ist gewährleistet, dass sich die Kommunikation zwischen den Netzwerkteilnehmern auf einen Switch konzentriert und der Verkehr über dessen leistungsfähige Backplane abgewickelt wird.

8.2 Die physischen und virtuellen Netzwerkschichten

Viele aus der physischen Netzwerkwelt bekannte Elemente finden sich auch in der virtuellen Welt wieder. Im folgenden Abschnitt arbeite ich mit Analogien zur physischen Welt, die den meisten Lesern bestens vertraut sein dürften.

- **Netzwerkkarten**
  Physische Clients und Server haben physische Netzwerkkarten mit einer MAC-Adresse. Der ESXi-Host hat physische Netzwerkkarten, wie jeder andere Server auch. Diese werden als Uplink-Adapter zu den virtuellen Switches eingesetzt. Die virtuellen Maschinen haben virtuelle Netzwerkkarten. Diese Netzwerkkarten haben eine virtuelle MAC-Adresse. Diese MAC-Adresse beginnt mit 00:50:56:, das bedeutet, VMware hat einen eigenen MAC-Adress-Bereich. Das zu wissen, kann bei der Fehlersuche hilfreich sein, zum Beispiel bei einem IP-Adress-Konflikt. Wenn Sie eine MAC-Adresse sehen, die mit 00:50:56: beginnt, dann wissen Sie, dass es sich um einen »VMware-Netzwerkadapter« einer VM oder eines VMkernels handelt.
- **Switches**
  In der physischen Welt gibt es den physische Switch und demzufolge in der virtuellen Welt den virtuellen Switch. In der Tat sind die virtuellen Switches physischen Layer-2-Switches nachgebildet. Die virtuellen Switches haben aber nicht alle Eigenschaften von physischen Switches. Zum Beispiel sind virtuelle Switches nicht STP-fähig (Spanning Tree Protocol).
- **Port**
  Ein physischer Switch hat physische Anschlüsse, auch *Ports* genannt. Je nach Switch-Modell existiert eine bestimmte Anzahl an physischen Anschlüssen. Wenn dieser Switch zum Beispiel 48 physische RJ45-Ports hat, so können Sie 48 Netzwerkkarten von Servern oder Clients mittels Netzwerkkabel daran anschliessen. Ein virtueller Switch hat ebenfalls eine bestimmte Menge an Ports, analog zu einem physischen Switch. Je nach Typ und Einstellungen des virtuellen Switches variiert die Anzahl an Ports von 8 bis 4.096.
- **Portgruppe**
  In den physischen Switches gibt es, je nach Modell, unterschiedliche Module/Steckverbinder für verschiedene Anwendungsgebiete, zum Beispiel 10-GB-CX4-Module für das Stacking von Switches oder Private Ports, die mit GBICs bestückt werden können, um längere Distanzen mittels LWL zu überbrücken . Kurz gesagt: Für verschiedene Anwendungszwecke gibt es verschiedene Module. In der virtuellen Welt gibt es zwei unterschiedliche »Module«, sogenannte *Portgruppen*. Diese dienen für den Anschluss von virtuellen Maschinen oder um dem Hypervisor Netzwerkzugang über TCP/IP zu gewährleisten. Die Aufteilung der Schichten ist in Abbildung 8.4 dargestellt.

Wenn Sie sich die Verbindungen in Abbildung 8.4 von den VMs an die virtuellen Switches und von diesen an die physischen Netzwerkkarten etwas genauer betrachten, so fällt Ihnen auf, dass die Ausprägung sehr unterschiedlich sein kann. Da gibt es:

- **VMs an virtuellen Switches mit einer Netzwerkkarte**
  Diese können in das physische Netzwerk kommunizieren, besitzen aber keine Redundanz. Sind VMs an demselben virtuellen Switch angeschlossen, so kommunizieren sie direkt über diesen Switch miteinander, ohne das physische Netzwerk zu benutzen.

- **VMs an virtuellen Switches mit zwei Netzwerkkarten**
  Diese können in das physische Netzwerk kommunizieren, besitzen aber Redundanz und automatische Lastverteilung (Load-Balancing). Sind VMs an demselben virtuellen Switch angeschlossen, so kommunizieren sie direkt über diesen Switch miteinander, ohne das physische Netzwerk zu benutzen.
- **VMs an virtuellen Switches ohne Netzwerkkarten**
  Diese können nicht direkt in das physische Netzwerk kommunizieren. Sind VMs an demselben virtuellen Switch angeschlossen, so kommunizieren sie direkt über diesen Switch miteinander.

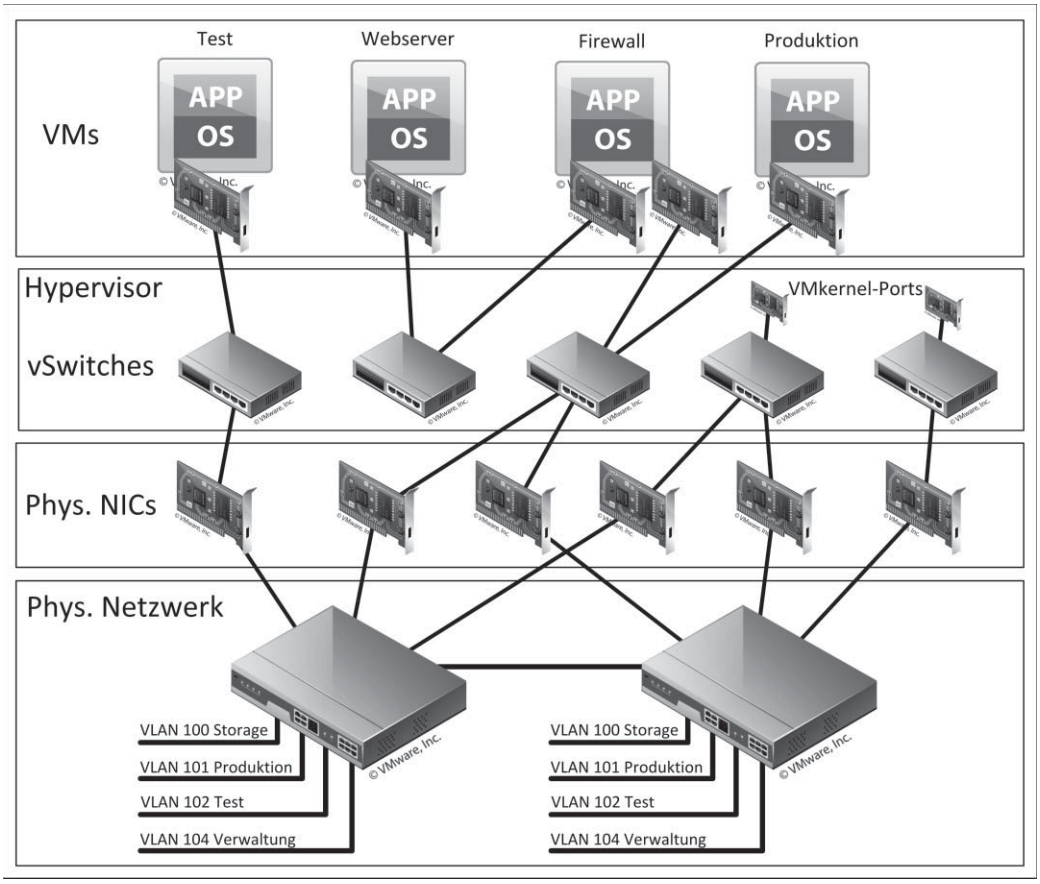


Abbildung 8.4 Die Schichten im virtuellen und physischen Netzwerk

In unserer Abbildung sehen Sie, dass die Webserver-VM an solch einem virtuellen Switch angeschlossen ist. Sie kann nicht direkt in das physische Netzwerk kommunizieren. Eine Kommunikation in das physische Netzwerk ist nur über die Router-VM möglich. Ist eine VM mit einer aktiven Verbindung an solch einen Switch angeschlossen, so kann sie mittels vMotion nicht auf einen anderen ESXi-Host bewegt werden.

8.3 Die physischen Netzwerkkarten im Host

Beide Arten der vSwitch-Typen benötigen als Uplinks physische Netzwerkkarten im Server. Diese Netzwerkkarten werden als vmnic# angezeigt. Die Nummerierung beginnt bei 0; somit ist die erste Netzwerkkarte die »vmnic0«, die nächste »vmnic1«, etc. Die vergebene vmnic-Nummer hängt von der PCI-Nummer der physischen Netzwerkkarte ab. Das bedeutet für Standard-Server, dass On-Board-Netzwerkkarten zuerst kommen. Danach folgen die in einen PCI-Bus gesteckten Netzwerkkarten. Je tiefer die PCI-Nummer in der Reihenfolge bei mehreren Netzwerkkarten, umso tiefer ist die vmnic-Nummer. Bei der Nummerierung ist es egal, ob es sich um 1-Gigabit- oder um 10-Gigabit-Adapter handelt. Bei Blade-Systemen, die synthetische Netzwerkadapter verwenden, kann die Nummerierung eingestellt werden.

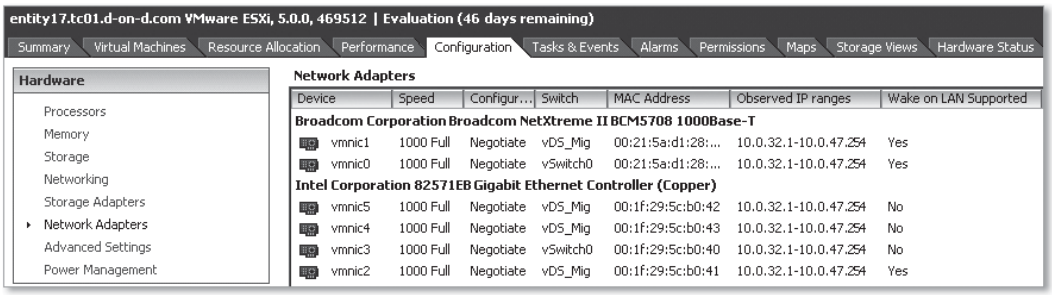


Abbildung 8.5 Die physischen NICs im Server

Wie Abbildung 8.5 zeigt, sehen Sie nebst dieser vmnic-Nummerierung unter der Spalte Device diverse andere Informationen: Die Spalte Speed informiert über den Verbindungsstatus und die Geschwindigkeit der Karte. Die Spalte Configuration zeigt auf, ob die Netzwerkkarte die Verbindungsgeschwindigkeit aushandelt oder ob diese fix eingestellt ist. In der Spalte Switch erfahren Sie, ob die Netzwerkkarte an einem vSwitch-Typen verwendet wird und wenn ja, an welchem. Die Spalte MAC-Address zeigt die MAC-Adresse des physischen Netzwerkadapters an.

Unter der Spalte Observed IP ranges ist das Netzwerksegment, mit dem die Karte verbunden ist, zu sehen. Dieses Netzwerk wird durch sogenanntes *Snooping* erkannt. Dabei werden die IP-Adressen im Segment ausgewertet, und der IP-Bereich hochgerechnet. Diese Angaben können Sie als Hilfsmittel verwenden, um die korrekte Netzwerkkarte als Uplink einem vSS oder vDS zuzuordnen.

Die Spalte Wake on LAN Supported zeigt auf, ob die betreffende Netzwerkkarte Wake-on-LAN (WOL) unterstützt oder nicht. Diese Information ist für DPM (Distributed Power Management) wichtig, falls die Server mittel WOL aus dem Standby-Modus eingeschaltet werden sollen.

8.4 Gegenüberstellung vSS und vDS

Wie schon erwähnt, gibt es bei den beiden vSwitch-Typen Gemeinsamkeiten, aber auch starke Differenzen im Konzept. Der folgende Abschnitt stellt die zuerst die Eigenschaften der zwei vSwitch-Konzepte einander gegenüber. Danach folgt eine Gegenüberstellung der gemeinsamen Eigenschaften. Auf die spezifischen Eigenschaften gehen wir in Abschnitt 8.5, »Arbeiten mit dem vNetwork-Standard-Switch«, und Abschnitt 8.6, »Arbeiten mit dem vNetwork Distributed Switch«, ein.

8.4.1 Die Eigenschaften der vSwitch-Typen im Überblick

Tabelle 8.1 veranschaulicht die Fähigkeiten der beiden vSwitch-Typen.

Eigenschaft	Standard-vSwitch	dvSwitch
Layer-2-Switch	ja	ja
VLAN 802.1q	ja	ja
NIC-Teaming	ja	ja
CDP (Cisco Discovery Protokoll)	ja	ja
Traffic-Shaping ausgehend	ja	ja
Traffic-Shaping eingehend	nein	ja
NetFlow	nein	ja
LLDP (Link Layer Discovery Protocol)	nein	ja
Port-Mirroring	nein	ja
Enterprise-Level-Management	nein	ja
PVLAN	nein	ja
Blocken von individuellen Ports	nein	ja
vSwitch-Support für Dritthersteller	nein	ja
Network I/O Control	nein	ja
Port-Mirroring	nein	ja
Verwaltung durch vCenter	nein	ja

Tabelle 8.1 Eigenschaften Standard- und Distributed vSwitch

Wie Sie unschwer erkennen, bietet der vNetwork Distributed Switch einiges mehr an Möglichkeiten als der vNetwork-Standard-Switch. Auch wenn bei den zwei verschiedenen vSwitch-Typen bei den Eigenschaften ein »ja« aufgeführt ist, können sich die jeweiligen vSwitch-Typen in den Einstellungsmöglichkeiten unterscheiden Als Beispiel seien hier die Konfigurationsoptionen bei VLANs und Ports genannt.

8.4.2 Die beiden vSwitch-Typen

Innerhalb des ESXi-Hosts gibt es zwei Typen von virtuellen Switches: den *vNetwork-Standard-Switch* (Synonyme: *vSS*, *vSwitch*) und den *vNetwork Distributed Switch* (Synonyme: *vDS*, *dvSwitch*).

Wir werden in den folgenden Netzwerkabschnitten der Einheitlichkeit halber primär folgende Begriffe verwenden:

- vNetwork-Standard-Switch: »vSS«
- vNetwork Distributed Switch: »vDS«
- sind der vNetwork Standard und der vNetwork Distributed Switch zusammen gemeint: »vSwitch-Typ(en)«

Diese vSwitch-Typen bilden einen Layer-2-Ethernet-Switch ab (OSI-Modell Layer 2), ohne jedoch alle Eigenschaften eines physischen Layer-2-Switches zu besitzen. Als Beispiel sei hier STP (Spanning Tree Protocol) aufgeführt, das physische Layer-2-Switches besitzen, die vSwitch-Typen jedoch nicht implementiert haben. Beide vSwitch-Typen stellen ein Verbindungselement dar, das auf der einen Seite sogenannte Portgruppen und auf der anderen Seite physische Netzwerkadapter innerhalb des Hosts verwendet. Diese physischen Netzwerkadapter sind als VMNIC# bezeichnet.

Es gibt zwei Typen von Portgruppen. Die eine ist die Virtual-Machine-Portgruppe; sie wird verwendet, um virtuelle Maschinen mit einem der vSwitch-Typen zu verbinden, damit die VM über diese eine Netzwerkverbindung erhält. Die zweite ist die VMkernel-Portgruppe, die es dem ESXi-Kernel/Hypervisor ermöglicht, über TCP/IP im Netzwerk zu kommunizieren.

Die TCP/IP-Kommunikation des Kernels/Hypervisors ist für folgende Kommunikationsbeziehungen des Hosts nötig:

- vom vSphere-Client zum Host
- vom vCenter Server zum Host
- vom Host zu IP-basierten Speicher-Systemen
- zwischen den Hosts für vMotion, HA-Heartbeat, HA und Fault Tolerance

Die beiden Switch-Typen weisen auf den ersten Blick viele gemeinsame Merkmale auf. Bei näherer Betrachtung ergeben sich dann aber doch signifikante Unterschiede. Während der vSS schon seit der VMware ESX-Version 3.0 existiert, wurde der vDS mit der VMware ESX-Version 4.0 eingeführt. Der vDS erfuhr Erweiterungen mit den vSphere-Versionen 4.1 und 5.0. Der vDS ist definitiv das modernere Konzept mit mehr Flexibilität. VMware implementiert neue Netzwerk-Features primär in den vDS. Damit der vDS verwendet werden kann, wird die größte vSphere Edition, Enterprise Plus, benötigt.

Die Screenshots in Abbildung 8.6 und in Abbildung 8.7 zeigen die Elemente für vNetwork-Standard- (vSS) und vNetwork Distributed Switches (vDS) auf.

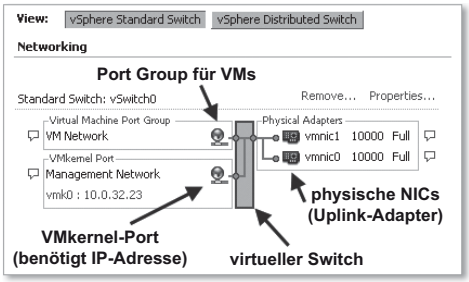


Abbildung 8.6 vSS – vNetwork-Standard-Switch

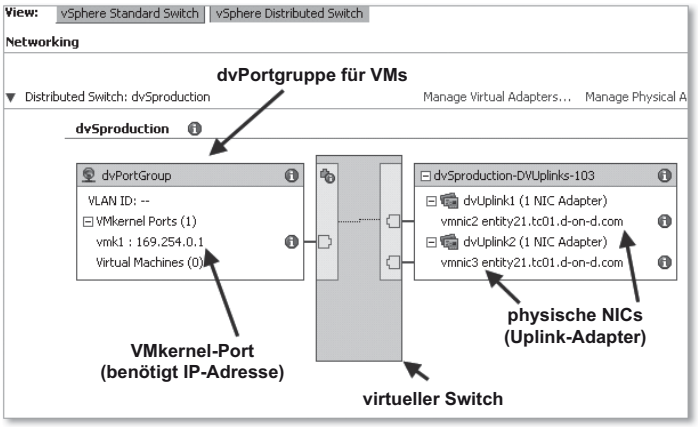


Abbildung 8.7 vDS – vNetwork Distributed Switch – Sicht Host

8.4.3 Der Switch-Teil bei vSS und vDS

In den beiden vorhergehenden Abbildungen (Abbildung 8.6 und Abbildung 8.7) ist der Switch-Teil als grauer Kasten in der Mitte dargestellt. Links sind die Portgruppen, rechts sind die Uplink-Adapter. Dieses Konzept ist bei beiden vSwitch-Typen aus Sicht des Hosts dasselbe.

Die Einstellungsmöglichkeiten und Eigenschaften der beiden vSwitch-Typen sind bezogen auf den reinen Switch-Teil recht unterschiedlich. Tabelle 8.2 listet die Möglichkeiten auf. Festzuhalten ist, dass für den vDS die wenigsten Einstellungen direkt auf dem ESXi-Host machbar sind. Die meisten Konfigurationen müssen über das vCenter erfolgen.

Einstellungen vornehmen	vSS Host	vDS Host	vDS vCenter
Anzahl Ports einstellen	ja	ja	nein
MTU-Size	ja	nein	ja
CDP bearbeiten	ja (CLI)	nein	ja
LLDP bearbeiten	nein	nein	ja

Tabelle 8.2 vSS- und vDS-Einstellungsmöglichkeiten auf Switch-Ebene

Einstellungen vornehmen	vSS Host	vDS Host	vDS vCenter
Layer-2-Security-Policies	ja	nein	nein
Traffic-Shaping *outbound*	ja	nein	nein
NIC-Teaming	ja	nein	nein
Uplink-Adapter bearbeiten	ja (alles)	ja (alles)	ja (Link)
VMkernel bearbeiten	ja	ja	ja
Portgruppe bearbeiten	ja	nein	ja
NetFlow bearbeiten	nein	nein	ja
Port-Mirroring bearbeiten	nein	nein	ja

Tabelle 8.2 vSS- und vDS-Einstellungsmöglichkeiten auf Switch-Ebene (Forts.)

8.4.4 Portgruppen bei vSS und vDS

Bei den Portgruppen-Einstellungen sind für vSS und vDS die Eintellungen aus Tabelle 8.3 möglich. Auch hier ist deutlich sichtbar, dass die meisten Einstellungen für den vDS ausschließlich über das vCenter erfolgen müssen.

Einstellungen vornehmen	vSS Host	vDS Host	vDS vCenter
Anzahl Ports einstellen	nein	ja	ja
Layer-2-Security-Policies	ja	nein	ja
Traffic-Shaping *inbound*	nein	nein	ja
Traffic-Shaping *outbound*	ja	nein	nein
VLAN	ja	nein	ja
NIC-Teaming	ja	nein	ja
Ressource-Allocation	nein	nein	ja
Monitoring	nein	nein	ja
VMkernel bearbeiten	ja	ja	ja
Portgruppe bearbeiten	ja	nein	ja
Alle Ports blocken	nein	nein	ja

Tabelle 8.3 vSS- und vDS-Einstellmöglichkeiten auf Portgruppen-Ebene

Was ebenfalls auffällt, ist, dass diverse Einstellungen bei den vSS auf Switch-Ebene, bei den vDS in die Portgruppe verschoben wurden. Beispiele sind: Layer-2-Security-Policies, NIC-Teaming, Traffic-Shaping.

8.4.5 Ports bei vSS und vDS

Die Einstellung der Anzahl der Ports ist bei den vSS sehr begrenzt. Das heißt, dass es nur einen Ort gibt, an dem diese Einstellung überhaupt vollzogen werden kann, und zwar auf dem Switch-Teil direkt. Zudem werden die Ports ausschliesslich statisch bereitgestellt.

Bei den vDS sind die Einstellungen auf den Portgruppen vorzunehmen; hier gibt es drei Auswahlmöglichkeiten.

Weil diese beiden Ansätze völlig voneinander abweichen, sind die Details dazu in den entsprechenden Abschnitten der vSwitch-Typen hinterlegt. Dies sind für den:

- vSS Abschnitt 8.5 Arbeiten mit dem vNetwork-Standard-Switch – vSS
- vDS Abschnitt 8.6 Arbeiten mit dem vNetwork Distributed Switch – vDS

8.4.6 Die Layer-2-Security-Policies

Die Security-Policies auf Layer 2 sind bei beiden Switch-Typen absolut identisch. Es gibt drei Einstellungen, wie Abbildung 8.8 zeigt.

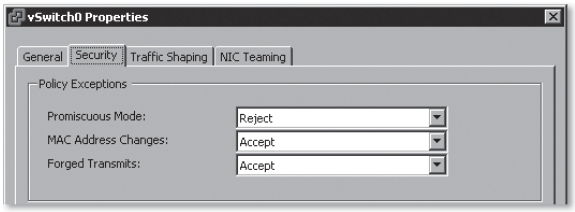


Abbildung 8.8 vSS-Konfiguration – »Security« (Switch und Portgruppen identisch)

Die Security-Einstellungen sind auf dem vSS und dem vDS absolut identisch. Sie beziehen sich auf den Ethernet-Stack (Layer 2). Für drei Policies können Sie REJECT oder ACCEPT einstellen.

Promiscuous Mode

Dieser Modus ist standardmäßig auf REJECT eingestellt. Im Promiscuous Mode ist es möglich, den gesamten Netzwerkverkehr auf dem betreffenden vSS oder vDS an eine entsprechend eingestellte Portgruppe zu leiten. Diese Funktion wird für das Sniffing mit Paket-Analyse-Software innerhalb einer VM benötigt. Eine andere Anwendung ist die Verwendung eines IDS (Intrusion Detection System) innerhalb einer VM.

MAC Address Changes

Dieser Modus ist standardmäßig auf ACCEPT eingestellt. Wenn innerhalb des Betriebssystems in der VM die MAC-Adresse verändert wurde, so wird dies mit den Security-Standardeinstellungen akzeptiert, und die VM kann normal in das Netzwerk kommunizieren. Ändern Sie diese Einstellung in REJECT, so wird der eingehende Verkehr der nicht originalen MAC-Adresse verworfen.

Die MAC-Adresse einer virtuellen Netzwerkkarte ist in der Konfigurationsdatei *.vmx* hinterlegt. Somit weiß der ESXi-Host, welches die Original- und somit gültige MAC-Adresse ist.

Forged Transmits

Dieser Modus ist standardmäßig auf Accept eingestellt. Wenn innerhalb des Betriebssystems in der VM die MAC-Adresse verändert wurde, so wird dies mit den Security-Standardeinstellungen akzeptiert, und die VM kann normal in das Netzwerk kommunizieren. Ändern Sie diese Einstellung in Reject, so wird der ausgehende Verkehr der nicht originalen MAC-Adresse verworfen.

8.4.7 Traffic-Shaping

Die Traffic Shaping-Eigenschaften sind bei beiden vSwitch-Typen im Bereich *outbound* oder Egress (ausgehend vom ESXi-Host ins physische Netzwerk) praktisch identisch. Der einzige Unterschied besteht darin, dass beim vSS diese Einstellung nebst einer Portgruppe auch auf dem virtuellen Switch selbst getroffen werden kann. Beim vDS können Sie Traffic-Shaping nur auf einer Portgruppe einstellen.

Ingress oder *inbound* (vom physischen Netzwerk in den ESXi-Host) kann nur der vDS. Darum schauen wir uns an dieser Stelle nur den gemeinsamen Outbound-Traffic an.

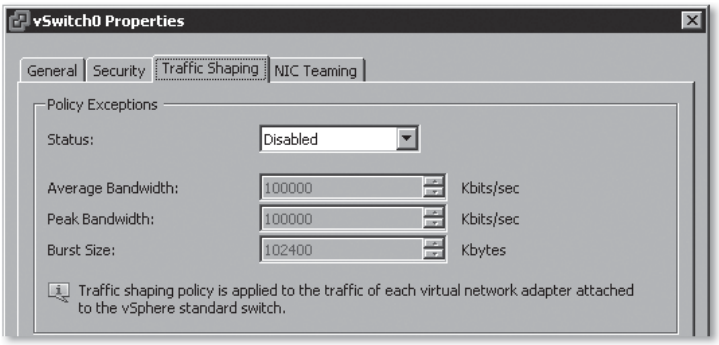


Abbildung 8.9 vSS-Konfiguration Traffic-Shaping (Switch und Portgruppen identisch)

Traffic-Shaping ist im Standard auf Disabled gesetzt, also nicht aktiv. Das bedeutet, dass die volle zur Verfügung stehende Netzwerk-Bandbreite genutzt werden kann. Mit Traffic-Shaping besteht die Möglichkeit, die Gesamtbandbreite zu beschränken. Es gibt drei Einstellungen zum Traffic-Shaping:

- **Average Bandwidth**
  Mit Average Bandwidth stellen Sie die zulässige Bandbreite in Kbit/Sek. ein. Aktivieren Sie Traffic-Shaping, so ist der Standardwert 100.000 Kbit/Sek., anders ausgedrückt 100 Mbit/Sek. Das bedeutet, dass bei einem 1-Gigabit-Anschluss nur ein Zehntel der Bandbreite verwendet wird.
- **Peak Bandwidth**
  Mit Peak Bandwidth können Sie die Average Bandwidth nach oben ausdehnen. Eine Bedingung ist, dass genügend Bandbreite vorhanden ist. Der eingegebene Wert von

Peak Bandwidth ist das effektive Maximum. Die Peak Bandwidth kann nicht kleiner sein als die Average Bandwidth.

- **Burst Size**
  Mit Burst Size können Sie auf die Peak Bandwidth eine Volumen-Grenze durchsetzen. Es ist die maximale Datenmenge, die in einem Burst versendet werden kann.

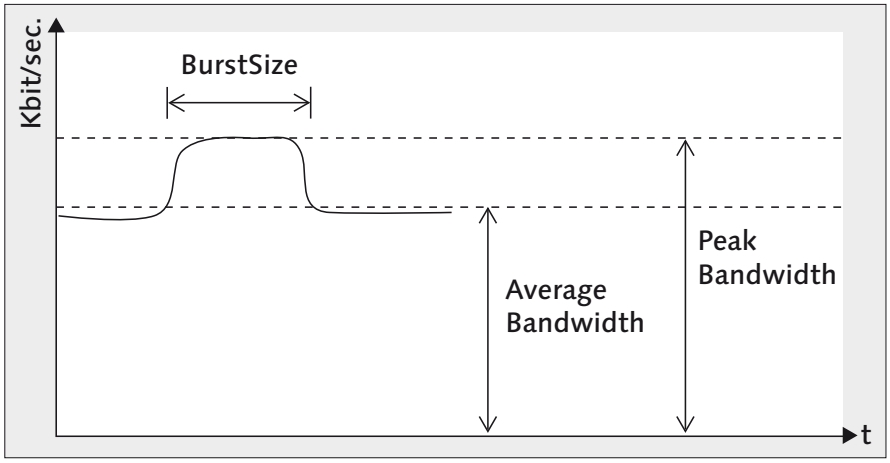


Abbildung 8.10 Traffic-Shaping-Einstellungen als Diagramm

8.4.8 Die VLAN-Einstellungen der vSwitch-Typen

Bevor wir auf die Unterschiede der VLAN-Einstellungen bei den vSwitches eingehen, schauen wir uns die VLANs aus Sicht von VMware an. VLANs sind eine Layer-2-Eigenschaft, »da wo das Ethernet-Protokoll stattfindet«. VMware unterstützt den IEEE-Standard 802.1q. Für die VLAN-Tags sind 12 Bits vorgesehen. 12 Bits entsprechen einem Adressraum von 2^{12}, also 4.096 unterschiedlichen Werten. Da die Nummerierung mit 0 beginnt, ist die höchste VLAN-ID 4095; somit betragen die gültigen Werte 0 bis 4095. 0 heißt kein TAG und ist die Standardeinstellung einer Portgruppe. Das bedeutet, sie selbst macht kein Tagging, sondern leitet den Verkehr 1 : 1 an die VM weiter. 4095 bedeutet Trunk-Port, also alle Pakete eine Schicht höher weitergeben; die Auswertung des eigentlichen Tags findet in der VM statt.

In der Praxis am meisten angewendet wird das VST oder Virtual Switch Tagging. Dieses wird von beiden vSwitch-Typen gleichwertig unterstützt. Bei VST wird eine VLAN-ID auf einer Portgruppe eingegeben (gültige Werte: 1–4094). Die Uplink-Adapter, die der vSwitch verwendet, werden an einen Trunk-Port des physischen Switches angeschlossen.

Sendet nun eine VM Netzwerkpakete ins physische Netz, so baut die Portgruppe das konfigurierte TAG ein, das wären in Abbildung 8.11 TAG 50 oder TAG 51. Das mit dem TAG bestückte Netzwerkpaket wird über die Netzwerkkarte an den Trunk-Port des physischen Switch geliefert. Der physische Switch wertet das TAG aus und behandelt es entsprechend. »Entsprechende Behandlung« bedeutet: Wenn das Endziel ein Access-Port ist, so wird das

TAG aus dem Netzwerkpaket entfernt und dann von diesem als normales Netzwerkpaket an den Client, Server, oder was sich auch immer an diesem Anschluss befindet, abgeliefert, wie in Abbildung 8.11 dargestellt.

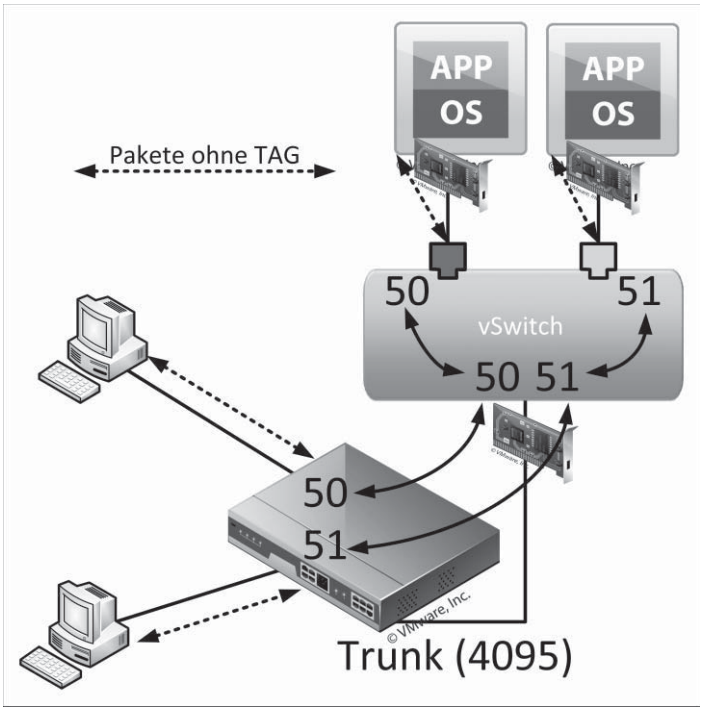


Abbildung 8.11 VST (Virual Switch Tagging)

Sind weitere Trunk-Ports an dem physischen Switch vorhanden, so werden alle Netzwerkpakete belassen, wie sie sind, und an diese Ports ausgegeben. Hat ein Trunk-Port am physischen Switch Begrenzungen (Filter), so werden nur diejenigen Netzwerkpakete durchgelassen, die auch der Filter unterstützt.

Die folgenden Screenshots zeigen die Einstellungen bei den verschiedenen vSwitch-Typen bezüglich VST.

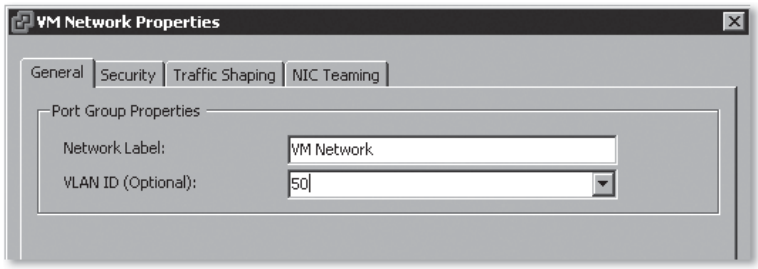


Abbildung 8.12 Standard-vSwitch im VST-Modus, VLAN 50 auf Portgruppe

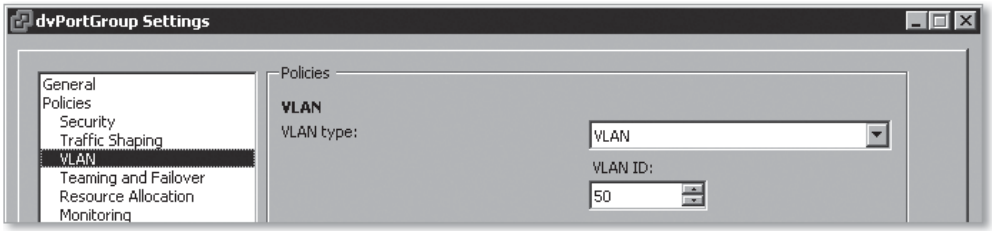


Abbildung 8.13 Distributed vSwitch im VST-Modus, VLAN 50 auf Portgruppe

Nebst Tagging auf vSwitch-Ebene wird das Tagging in der VM unterstützt. In diesem Fall ist die VLAN-ID der Portgruppe 4095. Das führt dazu, dass alle Pakete unabhängig von den enthaltenen TAGs der VM weitergegeben werden. Das Betriebssystem innerhalb der VM kann, wenn es die Fähigkeit besitzt, die TAGs auswerten. Der eingestellte TAG wird verwendet, die anderen TAGs werden ignoriert. Abbildung 8.14 veranschaulicht den Vorgang. VMT (Virtual Machine Tagging) wird in der Praxis relativ wenig verwendet.

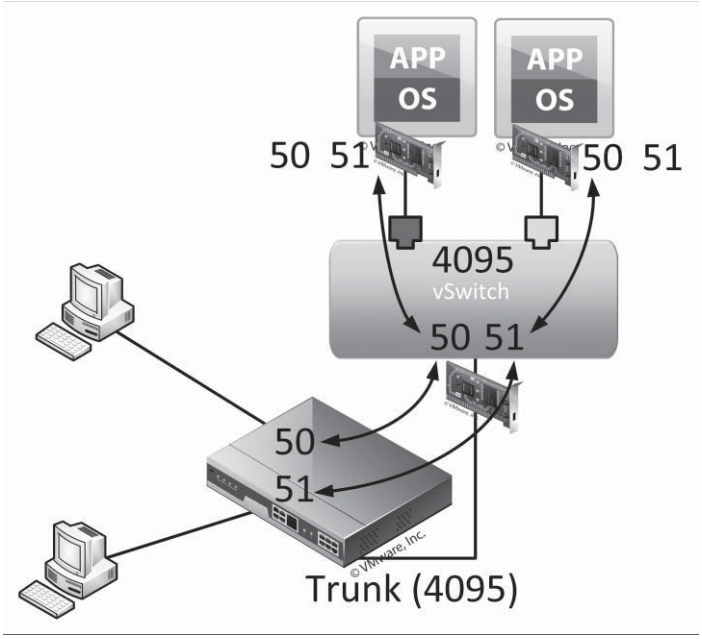


Abbildung 8.14 VMT (Virtual Machine Tagging)

Wie Sie unschwer erkennen, bietet der dvSwitch (Abbildung 8.16) noch mehr Einstellmöglichkeiten für einen Trunk-Port. Es kann ein Filter im Eingabefeld VLAN TRUNK RANGE gesetzt werden. Möchten Sie nur bestimmte VLAN-IDs durchlassen, so geben Sie diese im freien Feld an. Eine Eingabe von »5,19,55-57« würde bedeuten, dass nur Netzwerkpakete mit den TAGs 5, 19, 55, 56 und 57 durchgelassen würden.

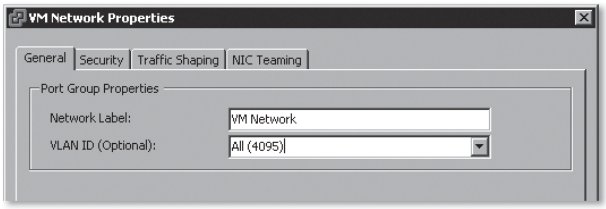


Abbildung 8.15 Standard-vSwitch im VMT-Modus, VLAN 4095

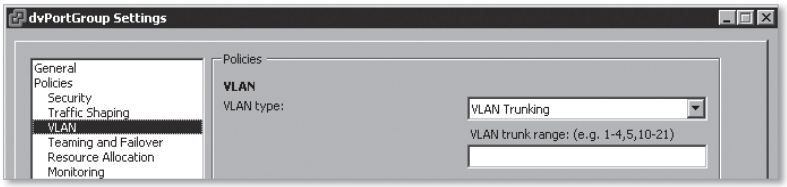


Abbildung 8.16 Distributed vSwitch im VST-Modus, VLAN 4095

Eine weitere Einstellung, die nur vDS besitzen, sind PVLANs oder Private VLANs. Auf diese gehen wir in Abschnitt 8.6.4, »Private VLAN«, ein, da sie ein Alleinstellungsmerkmal des vDS sind.

8.4.9 Die NIC-Teaming- und die Load-Balancing-Policies der vSwitch-Typen

Die Wirkungsweise der Load-Balancing-Policies ist bei beiden vSwitch-Typen identisch. Ein Unterschied besteht jedoch: Bei den Distributed vSwitches gibt es eine (sehr interessante) Policy mehr. Dies ist die Route based on physical NIC load. Tabelle 8.4 listet die vorhandenen Policies auf, abhängig von den vSwitch-Typen.

Einstellung	vSS	vDS	Konfiguration physischer Switch
Route based on the originating virtual port ID	ja	ja	nein
Route based on IP hash	ja	ja	ja
Route based on source MAC hash	ja	ja	nein
Route based on physical NIC load	nein	ja	nein
Use explicit failover order	ja	ja	nein

Tabelle 8.4 Load-Balancing-Policies

8.4.10 Die Arbeitsweise der Load-Balancing-Policies

Nachfolgend stellen wir die Arbeitsweise der vorhandenen Einstellungen zum Load-Balancing dar. Ein Aspekt gilt für alle Policies: Sie wirken von innen nach außen, also vom ESXi-Host ins Netz. Für die umgekehrte Richtung, aus dem Netz zum ESXi-Host, sind die physischen Switches zuständig.

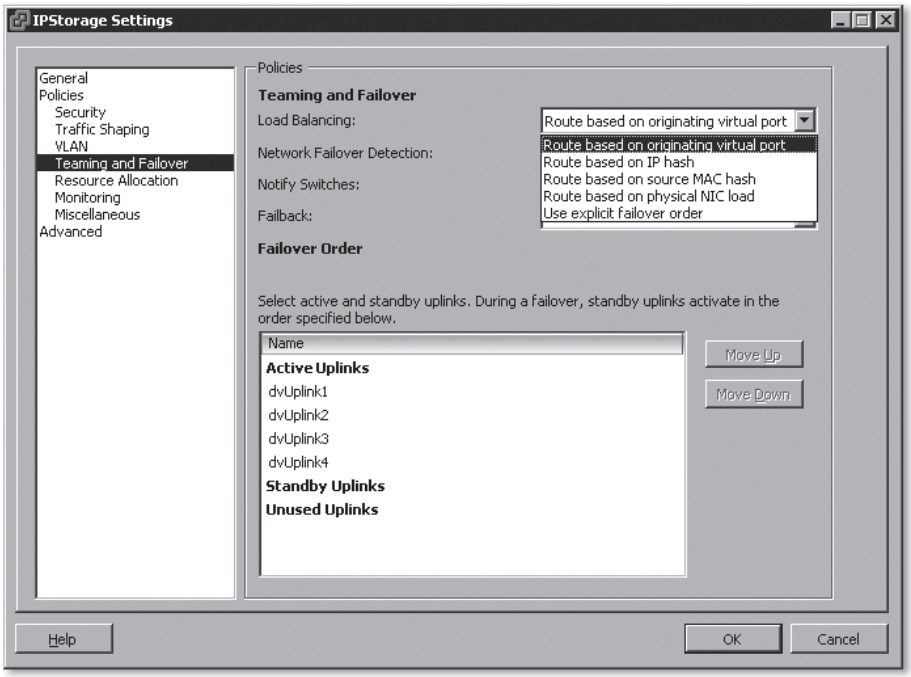


Abbildung 8.17 »Teaming and Failover«-Einstellungen für den vDS

Weil die TEAMING AND FAILOVER-Einstellungen beim vSS außer einer einzigen Policy dieselben sind, verzichten wir hier auf eine weitere Abbildung der vSS-Einstellungen.

Teaming and Failover – Route based on the originating virtual port ID

ROUTE BASED ON THE ORIGINATING VIRTUAL PORT ID ist die Standardeinstellung bei jeder neu erstellten Portgruppe auf einem dvSwitch oder jedem Standard-Switch. Diese Policy kommt ohne Konfigurationsschritte auf Seiten der physischen Switch-Hardware aus. Diese Policy wendet eine Round-Robin-Verteilung an. Das bedeutet bei einem Team mit zwei Netzwerkkarten: Die erste VM wird an die erste physische Netzwerkkarte »gepinnt«, die zweite VM an die zweite physische Netzwerkkarte, die dritte an die erste etc. Anders dargestellt: VM1-NIC1, VM2-NIC2, VM3-NIC1, VM4-NIC2, VM5-NIC1 etc. Abbildung 8.18 stellt die Verteilung grafisch dar.

Der Nachteil dieser Policy kann sein, dass die zwei VMs mit der höchsten benötigten Netzwerkleistung genau an dieselbe NIC gepinnt werden. Was dazu führt, dass jede VM nur noch die Hälfte der Netzwerk-Bandbreite zur Verfügung hat. Eine Umverteilung von VMs kann erst stattfinden, wenn diese ausgeschaltet und wieder eingeschaltet werden oder wenn ein Failover-Event vorliegt. Diese Policy bedingt keine Konfiguration am physischen Switch.

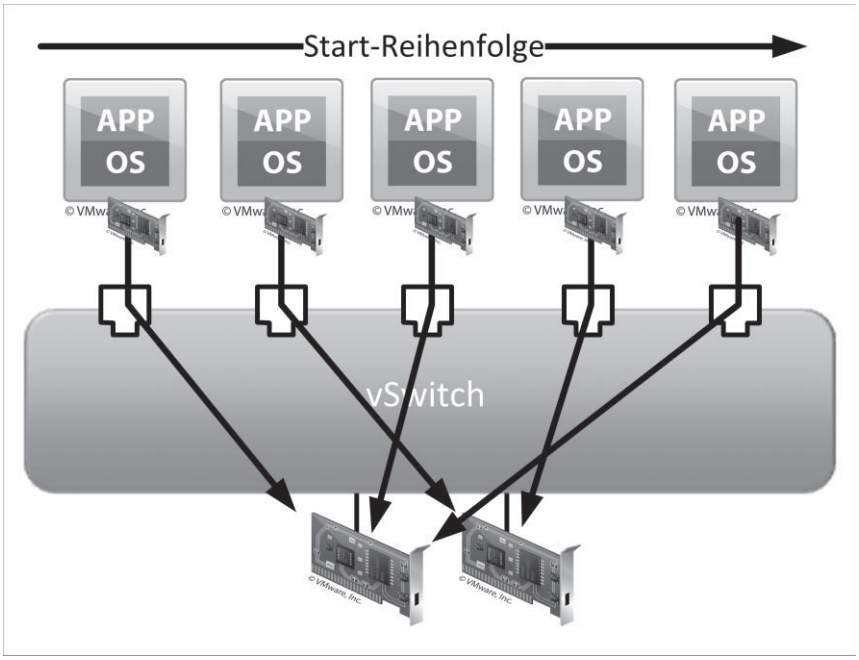


Abbildung 8.18 Load-Balancing »based on the originating virtual port ID«

Teaming and Failover – Route based on IP hash

Wählen Sie die Policy ROUTE BASED ON IP HASH, so müssen Sie darauf achten, dass Sie den physischen Switch ebenfalls konfigurieren. Dies geschieht, indem Sie statisches LACP, Etherchannel oder 801.3ad etc. aktivieren. Die Arbeitsweise ist wie folgt: Die Quell- und Ziel-IP-Adresse, oder anders ausgedrückt die Client-zu-Server-IP-Adresse in einer Kommunikationsbeziehung, wird genommen und zu einem Hashwert verrechnet. Wenn viele Kommunikationsbeziehungen zwischen vielen Clients und einem Server existieren, gibt es entsprechend viele unterschiedliche Hashwerte. Diese verschiedenen Hashes werden auf die vorhandenen physischen Netzwerkkarten verteilt.

Diese Policy skaliert ideal, wenn es 1:n-Verbindungen gibt. Bei 1:1-Verbindungen findet keine Verteilung über mehrere Netzwerkkarten statt, da ja nur ein Hashwert existiert. Dies ist vielfach ein Problem bei einer VMkernel-Konfiguration in Verbindung mit IP-basiertem Storage. Wird nur ein VMkernel auf eine Storage-IP verwendet, so werden die weiteren Netzwerkadapter im Netzwerkteam nicht für den Datentransport verwendet. Sie stehen dann nur für einen allfälligen Failover zur Verfügung. Diese Policy bedingt eine Konfiguration am physischen Switch.

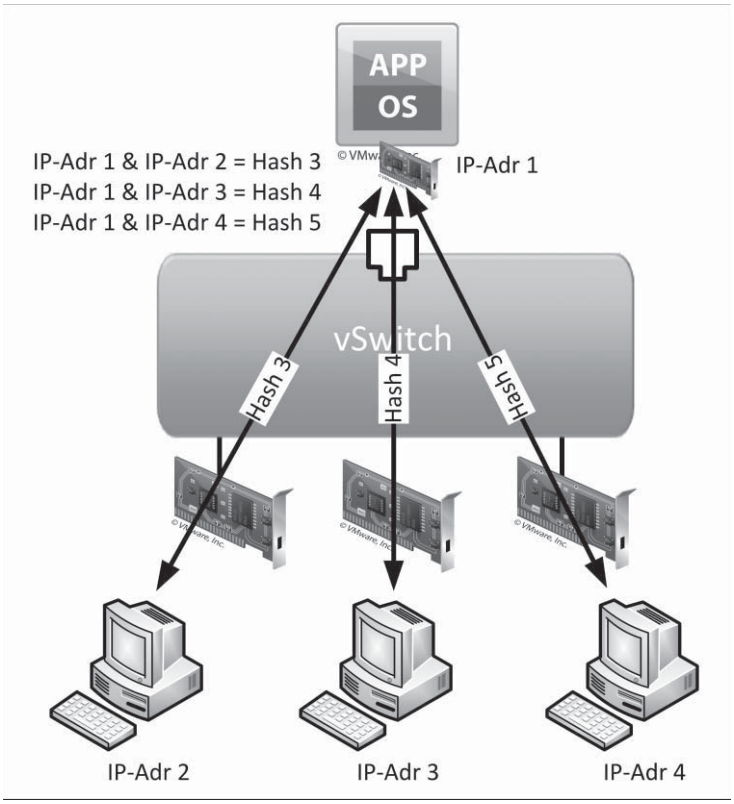


Abbildung 8.19 Wirkungsweise der »Route based on IP hash«-Policy

Teaming and Failover – Route based on source MAC hash

Bei der Load-Balancing-Policy ROUTE BASED ON SOURCE MAC HASH wird die MAC-Adresse einer virtuellen Netzwerkkarte als Grundlage der Verteilung genommen. Diese Arbeitsweise dieser Policy entspricht ansonsten derjenigen der Load-Balancing-Policy ROUTE BASED ON THE ORIGINATING VIRTUAL PORT ID. Diese Policy bedingt keine Konfiguration am physischen Switch.

Teaming and Failover – Route based on physical NIC load

Die Load-Balancing-Policy ROUTE BASED ON PHYSICAL NIC LOAD kann nur bei einer Portgruppe an einem dvSwitch verwendet werden. Diese Policy skaliert sehr gut, da der Netzwerkverkehr auf einem Netzwerk-Interface im ESXi-Host beobachtet wird. Ist die Saturierung des Netzwerkinterfaces 75 % während 5 Sekunden, so werden die Verkehrsströme der verschiedenen Teilnehmer umverteilt Diese Policy bedingt keine Konfiguration am physischen Switch.

Teaming and Failover – Use explicit failover order

Die Policy Use explicit failover order verwendet immer den ersten Adapter unter den Active Uplinks. Ein Load-Balancing im eigentlichen Sinne findet damit nicht statt.

Dies Policy können Sie zum Beispiel dann verwenden, wenn zwei physische Switches untereinander mit relativ wenig Bandbreite verbunden sind. Dann sollte der Verkehr auf einen physischen Switch konzentriert werden, da die interne Backplane des Switches wesentlich mehr I/O bewältigen kann als ein schwacher Link zwischen den physischen Switches. Werden alle ESXi-Hosts auf einen primären physischen Switch konzentriert, wird dessen Backplane benutzt, und der Verkehr bleibt auf diesem physischen Switch. Das kann erreicht werden, wenn bei allen ESXi-Hosts der erste Adapter in der Liste der Active Uplinks auf den einen und der zweite Netzwerkadapter in der Liste der Active Uplinks auf den zweiten physischen Switch angeschlossen sind. Fällt der primäre physische Switch aus oder wird zum Beispiel ein Firmware-Upgrade mit Reboot am physischen Switch durchgeführt, wird die Kommunikation aller ESXi-Hosts über den zweiten Adapter auf dem zweiten physischen Switch fortgesetzt. Fällt bei einem einzelnen ESXi-Host der erste Adapter in der Liste der Active Uplinks aus, so wird der zweite Adapter über den zweiten physischen Switch kommunizieren. In diesem Fall muss die Kommunikation dieses ESXi-Hosts mit den anderen ESXi-Hosts über den schwachen Link zwischen den physischen Switches erfolgen.

Teaming and Failover – Network Failover Detection

Bei der Network Failover Detection geht es darum, wie der ESXi-Host einen Fehler oder Ausfall im Netzwerk wahrnimmt. Die Standardkonfiguration ist Link status only. Bei dieser Konfiguration liegt ein Fehler vor, wenn das Netzwerkkabel keine Verbindung mehr zu einem physischen Switch-Port hat, der physische Switch-Port abgeschaltet wurde oder ein ganzer physischer Switch ausfällt. Logische Fehler, wie ein physischer Port im falschen VLAN, kann Link status only nicht auflösen.

Mittels der Einstellung Beacon Probing können auch logische Fehler kompensiert werden. In dieser Einstellung werden kleine UDP-Netzwerkpakete über die Uplinks versandt. Kommen alle Pakete zwischen allen Uplinks an, so ist alles in Ordnung. Gibt es einen Uplink, der nichts empfängt und von dem nichts empfangen werden kann, liegt ein Fehler vor. Dieser Uplink wird mit Failover behandelt, in diesem Fall nicht mehr verwendet. Damit die Einstellung zuverlässig funktioniert, müssen drei oder mehr Uplinks vorhanden sein. Beacon-Probing darf nicht mit der Load-Balancing-Policy Route based on IP hash verwendet werden.

Teaming and Failover – Notify Switches

Die Standardeinstellung von Notify Switches ist Yes, und somit ist die Option aktiv. Die andere Möglichkeit wäre die Einstellung No und damit die Deaktivierung dieser Einstellung.

Bei einem Ausfall einer Netzwerkverbindung über eine physische Netzwerkkarte werden alle virtuellen Netzwerkkarten über einen anderen Uplink oder eine andere Netzwerkverbindung

geleitet. Somit sind die auf einen physischen Switch-Port registrierten MAC-Adressen nicht mehr aktuell. Dasselbe geschieht auch bei vMotion oder wenn eine neue virtuelle Netzwerkkarte an eine Portgruppe verbunden wird. Beispiel vMotion: Damit bewegen Sie eine VM von einem auf einen anderen ESXi-Host. Die MAC-Adresse der virtuellen Netzwerkkarte befindet sich dann auf einmal an einem anderen physischen Switch-Port. Damit die Konvergenz im Netzwerk möglichst schnell wiederhergestellt wird, setzt der ESXi-Host ein ARP-Paket ab, damit sich die Lookup-Tables der physischen Switches aktualisieren.

In den meisten Fällen ist die Einstellung Yes sinnvoll. Es gibt jedoch Ausnahmen. Im Speziellen sei hier Microsoft NLB (Network Load Balancing) im Unicast-Mode genannt, bei dem die Einstellung No sein muss.

Teaming and Failover – Failback

Wurde ein Failover durchgeführt, weil ein Uplink die Netzwerkverbindung verloren hat, werden alle Netzwerkteilnehmer dieses Uplinks auf andere Uplinks verteilt. Wurde der Defekt des ausgefallen Uplinks behoben, so werden die verschobenen Verbindungen wieder auf den alten Uplink zurückgeführt.

Dies ist besonders bei nicht dynamischen Load-Balancing-Policies (Route based on the originating virtual port ID, Route based on source MAC hash, Use explicit failover order) wichtig, damit der Netzwerkverkehr wieder optimiert wird.

Bei Ausfällen und Wiederverfügbarkeit von physischen Switches, wie zum Beispiel bei Firmware-Updates, gilt es, Folgendes zu beachten: Der ESXi-Host hat mitunter von einem bootenden Switch relativ früh wieder eine scheinbar intakte Verbindung am Uplink. Mitunter nimmt der Switch aber an den Ports noch keine Daten entgegen. Dies kann zu Störungen führen. Um dies möglichst zu verhindern, ist die Empfehlung, an den physischen Switches die Ports auf Portfast zu konfigurieren.

Failover Order

Mittels der Einstellung Failover Order können Netzwerkadapter in einen von drei Abschnitten zugeordnet werden:

- Active Uplinks
- Standby Uplinks
- Unused Uplinks

In dieser Einstellung kann der Verkehr für alle Load-Balancing-Policies, außer der Policy Route based on IP hash, modelliert werden. Modellierung bedeutet in diesem Fall, dass zum Beispiel ein vSwitch-Typ mit sechs Uplink-Adaptern erzeugt wird und danach die Uplink-Adapter spezifisch auf einzelne Portgruppen sortiert werden. Tabelle 8.5 zeigt ein Beispiel.

NIC	Management	vMotion	Storage	Produktions-VMs	Test-VMs
vmnic0	Active	Standby	Standby	Standby	Active
vmnic1	Active	Unused	Standby	Active	Unused
vmnic2	Standby	Unused	Standby	Active	Unused
vmnic3	Standby	Unused	Active	Standby	Unused
vmnic4	Standby	Unused	Active	Standby	Unused
vmnic5	Standby	Active	Standby	Standby	Unused

Tabelle 8.5 Modellierung von Verkehrsmustern im Netzwerk

Damit wird erreicht, dass der Verkehr bei größeren Aggregaten über spezifische Netzwerkadapter abgewickelt wird. Bei einem Ausfall eines aktiven Uplinks würde ein Standby-Uplink hinzugenommen. Bei den Standby-Uplinks wäre noch die Sortierreihenfolge zu beachten, um eine absolut perfekte Konstellation zu erzeugen. Beim Ausfall eines aktiven Uplinks wird der erste Standby-Adapter ins Team eingebunden.

8.4.11 CDP – Cisco Discovery Protocol der vSwitch-Typen

CDP (Cisco Discovery Protocol) ist ein proprietäres Protokoll der Firma Cisco. Das Gegenstück dazu wäre das herstellerunabhängige LLDP (Link Layer Display Protocol), das nur vom vDS unterstützt wird. CDP wird von beiden vSwitch-Typen unterstützt.

CDP stellt Informationen (siehe Abbildung 8.20) über die Geräte im Netzwerk bereit. Damit lässt sich feststellen, an welchem physischen Switch-Port ein NIC-Port (vmnic#) des Hosts angeschlossen ist und in welchem VLAN er sich befindet, wie der physische Switch heißt, welches OS auf ihm läuft, welche IP-Adresse dieser physische Switch besitzt oder wie die SNMP-Location des Gerätes ist.

CDP wird primär im Backbone-Bereich der Server und Switches verwendet. Unter den Netzwerk-Professionals herrschen unterschiedliche Meinungen, ob es verwendet werden soll oder nicht. Die zwei Hauptargumente der »Gegner« von CDP: Erhöhung des Grundrauschens im Netzwerk und Verbreiten von Informationen, die abträglich für die IT-Sicherheit sein könnten. Bei statischen Infrastrukturen mag die Betrachtungsweise stimmig sein, bei dynamischen Infrastrukturen, in denen sich die Konfigurationen ständig ändern, weniger. Bei vielen Änderungen schleichen sich schnell Fehler in eine Konfiguration ein. Wer schon einmal auf Fehlersuche in einem komplexen Netzwerk gegangen ist, kann ein Lied davon singen, wie einfach die Nachverfolgung von Konfigurationen mit wenig Informationen ist. In so einem Fall ist CDP extrem hilfreich.

Die vSwitch-Typen des ESXi-Host sind in der Standardeinstellung im CDP-Listen-Modus aktiv. Das bedeutet, dass der ESXi-Host CDP-Informationen empfängt, wenn der Switch Advertising betreibt. Der physische Switch hingegen bekommt keine Informationen vom ESXi-Host. Dies können Sie selbstverständlich ändern. Tabelle 8.6 zeigt die Einstellmöglichkeiten.

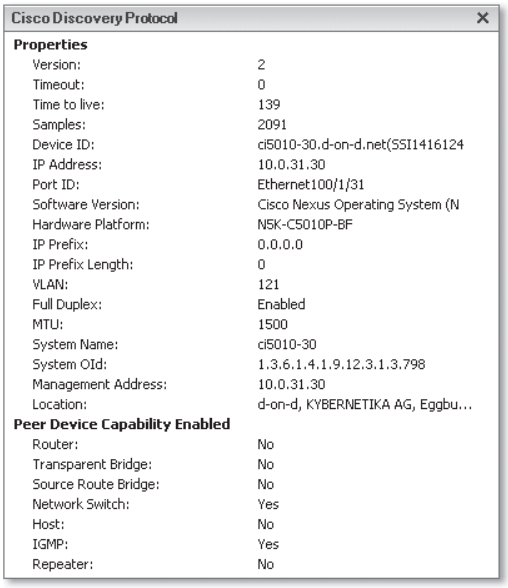


Abbildung 8.20 CDP-Informationen

Einstellung	Auswirkung
DISABLED	kein CDP
LISTEN (Standard)	CDP wird empfangen.
ADVERTISE	CDP wird gesendet.
BOTH	CDP wird empfangen und gesendet.

Tabelle 8.6 CDP-Modi

Bei vSS müssen Sie die Modi über die Befehlszeile festlegen. Beim vDS können Sie die Modi über das GUI einstellen. Die Konfiguration erfolgt immer pro einzelnen vSS oder vDS.

8.4.12 Configuration Maximums für vSS und vDS

Für vSS und vDS gibt es eine maximale Anzahl (*Configuration Maximum*) an Elementen, die erzeugt werden können.

Gegenstand	Maximum
Gesamtanzahl virtueller Netzwerk-Switch-Ports pro Host (vDS- und vSS-Ports)	4.096
Maximum aktive Ports pro Host (vDS und vSS)	1.016
maximale Anzahl Ports pro vSS	4.088
maximale Anzahl Portgruppen pro vSS	256
maximale Anzahl vDS-Ports pro vCenter	30.000

Tabelle 8.7 Configuration Maximums für vSS und vDS

Gegenstand	Maximum
maximale Anzahl statischer Portgruppen pro vCenter	5.000
maximale Anzahl *ephemeral (flüchtige)* Portgruppen pro vCenter	256
maximale Anzahl Hosts pro vDS	350
maximale Anzahl vDS pro vCenter	32

Tabelle 8.7 Configuration Maximums für vSS und vDS (Forts.)

8.5 Arbeiten mit dem vNetwork-Standard-Switch – vSS

Der vNetwork-Standard-Switch, Kurzbezeichnung vSS, wird in der Praxis nach wie vor häufig verwendet. Die Gründe hierfür sind sehr einfach:

- **Rückwärts-Kompatibilität**
  Er existiert seit der ESX-Version 3.0 und ist im Umgang bis heute weitestgehend identisch geblieben. Bestehende Umgebungen müssen nicht verändert werden.
- **Lizenzkosten**
  Der vNetwork Distributed Switch bedingt die höchste Lizenzstufe von vSphere. Sind die Enterprise-Plus-Lizenzen nicht vorhanden, so muss mit dem vSS gearbeitet werden.
- **Eigenschaften**
  Die vorhandenen Eigenschaften des vSS reichen aus.
- **Unabhängigkeit**
  Es ist absolute Unabhängigkeit vom vCenter gewünscht. Alles, was mit dem vSS zu tun hat, findet auf dem Host statt.
- **Kleine Umgebung**
  Die Umgebungsgröße bedingt keinen vDS.

8.5.1 Der vSS ist hostbezogen

Der vSS existiert immer pro VMware ESXi-Host. Das bedeutet, dass Änderungen an einem vSS nur auf dem einen, betroffenen ESXi-Host stattfinden. Diese Änderungen übertragen sich nicht automatisch auf andere ESXi-Hosts weiter. Bei vielen Hosts bedeutet dies eine Menge Handarbeit. Das Erstellen eines Scripts oder die Verwendung von Hostprofilen können bei einer größeren Anzahl von Hosts und vSS die Arbeit erleichtern.

Eine kurze Anmerkung zur Verwendung von Hostprofilen im Zusammenhang mit Netzwerkkonfigurationen: Wird ein Hostprofil an einem ESXi-Host angewendet, so muss dieser Host in den Maintenance-Modus versetzt werden. Damit ist er aus Sicht der Produktion offline. Somit sind Hostprofile kein Ersatz für die Eigenschaft »Enterprise Level Management« eines vDS. Enterprise Level bedeutet indirekt auch, dass Equipment nicht vollständig außer Betrieb genommen werden muss.

8.5.2 Die Konfigurationsmöglichkeiten zum vSS

Alle Verwaltungsarbeiten zum vSS, ob direkt mit dem vSphere-Client oder über das vCenter, finden in der Ansicht CONFIGURATION statt.

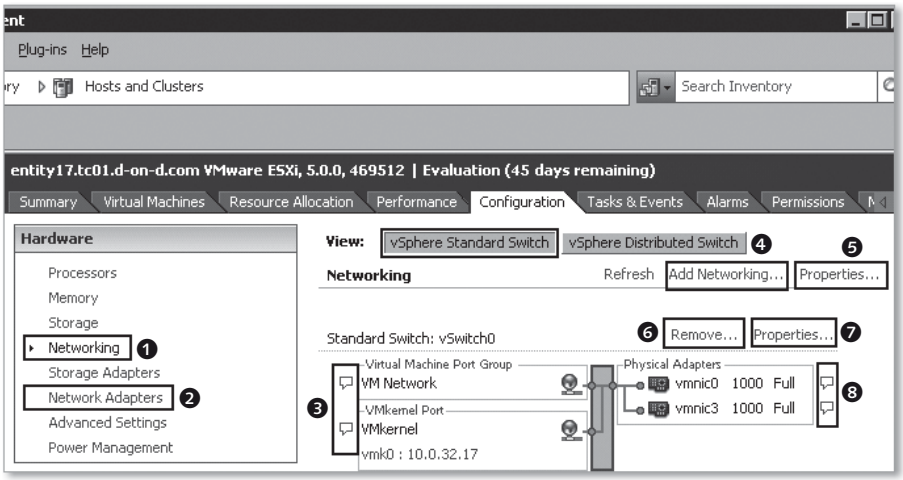


Abbildung 8.21 Die Konfigurations- und Informationselemente des vSS

Markieren Sie einen Host und wählen die Ansicht CONFIGURATION, so haben Sie alle Informationen und Konfigurationsmöglichkeiten des vSS im Zugriff. Der Screenshot (Abbildung 8.21) zeigt diese Ansicht mit nummerierten Elementen. Die Legende dazu:

❶: Die NETWORKING-Ansicht ermöglicht den Zugriff auf die Informationen und Konfigurationen des vSS.

❷: NETWORK ADAPTERS zeigt alle Informationen über die physisch vorhandenen Netzwerkkarten im ESXi-Host auf.

❸: Zeigt Informationen über die Konfigurationen der Portgruppen an. Diese Informationen umfassen die Properties (Network-Label und VLAN-ID), die Layer-2-Security-Policies, das Traffic-Shaping und NIC-Teaming.

❹: ADD NETWORKING erzeugt einen neuen vSS oder eine neue Portgruppe auf dem ESXi-Host.

❺: PROPERTIES ermöglicht es, IPv6 zu aktivieren.

❻: REMOVE entfernt einen vSS.

❼: PROPERTIES ermöglicht, die Einstellungen des vSS zu überprüfen oder zu verändern. An dieser Stelle ist es auch möglich, eine neue Portgruppe an dem entsprechenden vSS anzulegen, wobei Sie darauf achten müssen, dass eine spezifische Portgruppe auf allen ESXi-Hosts denselben Namen, inklusive Groß- und Kleinschreibung, trägt.

❽: Zeigt die CDP-Informationen pro Netzwerkkarte an.

8.5.3 Einstellungen auf dem Switch oder den Portgruppen

Über Properties beim entsprechenden vSS erreichen Sie die Konfigurationsmöglichkeiten für den Switch, die Portgruppe, oder die Netzwerkadapter.

Die Einstellungsmöglichkeiten für den Switch und die Portgruppen sind weitestgehend identisch. Der einzige Unterschied ist, dass Sie beim Switch die Anzahl Ports, die MTU-Size und die physischen NICs einstellen können.

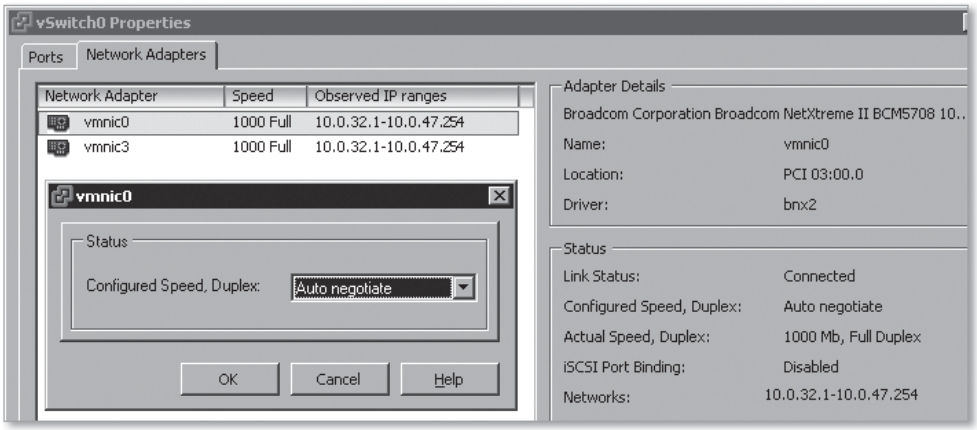


Abbildung 8.22 vSS NIC-Konfiguration

In dieser Ansicht (Abbildung 8.22) können Sie Netzwerkkarten hinzufügen und entfernen. Sie können die Informationen einer Netzwerkkarte, wie PCI-Slot-Position, NIC-Treiber etc., beziehen. Die Datenübertragungsgeschwindigkeit einer Netzwerkkarte können Sie auf die Modi Auto Negotiate, 10 MB, Half Duplex/10 MB, Full Duplex/100 MB, Half Duplex/100 MB, Full Duplex/1000 MB, Full Duplex stellen. Bei 10-Gigabit-Karten existiert nur 10000Mb, Full Duplex, was nicht verändert werden kann.

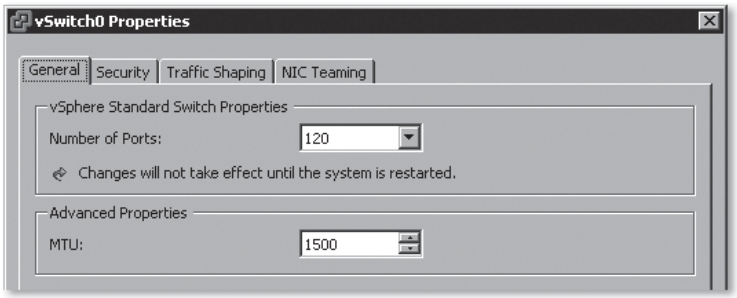


Abbildung 8.23 vSS-Konfiguration – Anzahl Ports, MTU-Size (nur Switch)

In der Ansicht aus Abbildung 8.23 kann die MTU-Size vom Standard 1.500 auf z. B. 9.000 für Jumbo-Frames angehoben werden. Werden Jumbo-Frames konfiguriert, so muss dies die gesamte Infrastrukturkette bis zum Ziel unterstützen.

Eine weitere Einstellung sind die Ports. Die Voreinstellung ist 120. Genau genommen sind es 128. Da aber der ESXi-Host für die Verwaltung 8 Ports schon abzieht, bleiben noch 120. Von diesen 120 Ports wird jedes Mal einer belegt, sobald ein virtueller Netzwerkadapter oder ein Uplink-Adapter an den vSS angeschlossen wird. Die Anzahl der Ports ist so einzustellen, dass die Höchstbelegung abgedeckt werden kann. 120 mag für einen 2-CPU-/8-Core-Server genügen, für einen 8-CPU-/64-Core-Server wird es dann wahrscheinlich zu eng. Die maximale Anzahl Ports ist 4.088. Das sollten Sie nicht wählen, wenn Sie mehr als ein vSS auf dem System konfigurieren, da dies die maximal unterstützte Anzahl Ports auf einem Host überhaupt darstellt.

Port-Anzahl	Ports nutzbar
16	8
32	24
64	56
128	120
256	248
512	504
1.024	1.016
2.048	2.040
4.096	4.088

Tabelle 8.8 vSS – mögliche Port-Einstellungen

Die Themen aus Tabelle 8.9 haben wir im gemeinsamen Abschnitt für vSS und vDS behandelt. Darum führen wir sie hier nicht nochmals auf. Dies gilt auch für den gleich folgenden Abschnitt 8.6.

Thema	Abschnitt	Titel	Seite
Layer-2-Security-Policy	8.4.6	»Die Layer-2-Security-Policies«	331
Traffic-Shaping	8.4.7	»Traffic-Shaping«	332
VLAN	8.4.8	»Die VLAN-Einstellungen der vSwitch-Typen«	333
Teaming and Failover	8.4.9	»Die NIC-Teaming- und die Load-Balancing-Policies der vSwitch-Typen«	336
CDP	8.4.11	»CDP – Cisco Discovery Protocol der vSwitch-Typen«	342

Tabelle 8.9 An früherer Stelle behandelte Themen

8.6 Arbeiten mit dem vNetwork Distributed Switch – vDS

Der vNetwork Distributed Switch (vDS) unterstützt alle Features des vNetwork-Standard-Switches (vSS) und noch sehr viele mehr (siehe Tabelle 8.1). Der vDS hat sehr wichtige spezifische Eigenschaften, die ihn vom vSS stark unterscheiden; nachfolgend ein paar der wichtigen Merkmale:

- **Massenkonfiguration**
  Der vDS ist auf die Konfiguration von großen Infrastrukturen konzipiert. Eine Änderung überträgt sich auf alle Mitglieder. Dies ergibt weniger Arbeitsschritte und ist weniger fehleranfällig.
- **Network vMotion**
  Der Status einer Netzwerkverbindung wird übertragen und bleibt intakt. Auch werden die Counter, wie viele Daten übertragen wurden, nicht auf null zurückgesetzt, sondern laufen kumulativ weiter.
- **Erweiterung durch Dritthersteller**
  Es ist möglich, den vDS in seinen Funktionen mit zum Beispiel Cisco Nexus 1000v zu erweitern.
- **VMsafe-API**
  Dank VMsafe können Dritthersteller von Sicherheitsprodukten eine netzwerknahe Integration dieser Produkte vornehmen.

8.6.1 Der vDS existiert im vCenter und im Host

Ein wesentliches Element des vNetwork Distributed Switches (vDS) ist, dass sich Änderungen, die an ihm vorgenommen werden, sofort auf die in ihm registrierten Hosts übertragen. Sind zum Beispiel 50 ESXi-Hosts in einem vDS registriert und wird an diesem eine neue Portgruppe erstellt, so wird diese Änderung an die 50 ESXi-Hosts übertragen. Diese Übertragung ist möglich, weil sich der Bauplan zum vDS in der vCenter-Datenbank befindet. Jede Änderung wird vom vCenter lokal in die einzelnen Hosts geschrieben. Dass die Informationen lokal auf die Hosts abgelegt werden, ist essentiell. Ansonsten würde der Ausfall des vCenter dazu führen, dass Netzwerkverbindungen verlorengingen. Der Ausfall des VMware vCenters führt jedoch dazu, dass ein vDS nicht mehr konfiguriert werden kann.

Eine Strategie, das Management-Netzwerk vor dieser Situation zu schützen, ist, dass das Management-Netzwerk nach wie vor als vSS ausgeprägt ist. Zum einen ist die vSS-Konfiguration über die Befehlszeile vollständig gegeben, beim vDS nur in Teilen, und der vSS ist vom vCenter völlig unabhängig.

Abbildung 8.24 zeigt die Architektur des vDS auf.

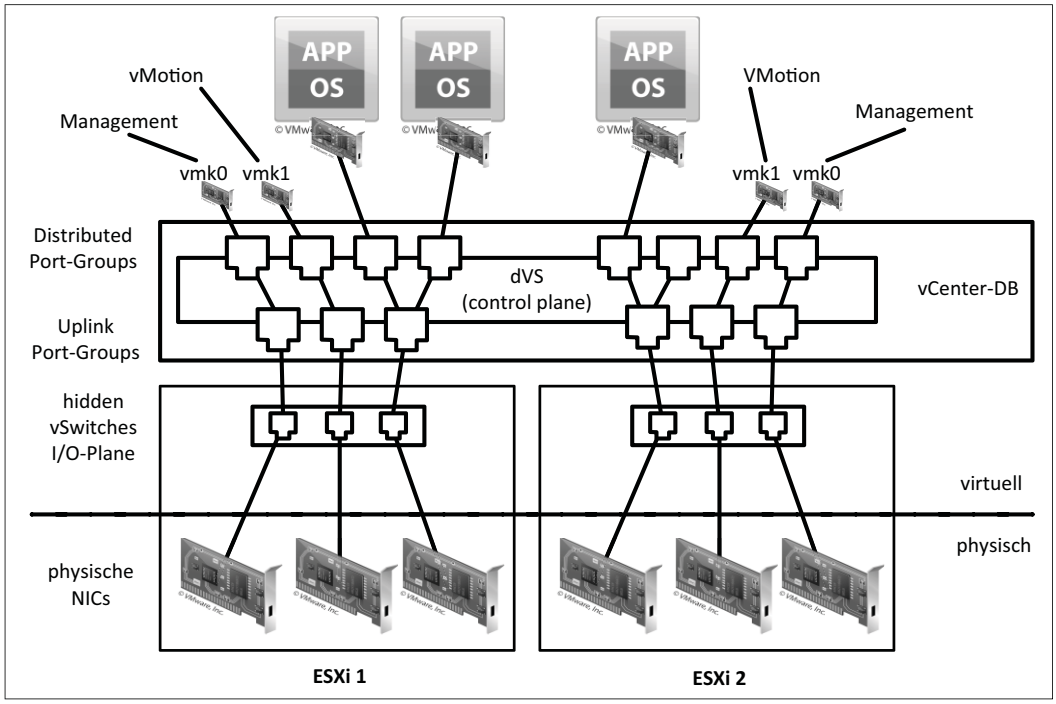


Abbildung 8.24 Architektur des vDS

8.6.2 Die Konfigurationsmöglichkeiten des vDS

Um einen vDS zu erzeugen, wechseln Sie in die vCenter-Ansicht NETWORKING. Danach markieren Sie das Datacenter, zu dem der vDS gehört. Ein vDS kann nur einem Datacenter zugeordnet werden, das bedeutet, er ist nicht datacenter-übergreifend. Der Screenshot (Abbildung 8.25) veranschaulicht die Schritte.

Ein Assistent führt mit Dialogen durch die Erstellung des vDS. Die erste geforderte Angabe ist, welche vDS-Version erzeugt werden soll: vDS 4.0, vDS 4.1, vDS 5.0. Jede dieser vSphere-Versionen brachte neue Eigenschaften im vDS. Die wesentliche Frage ist, welche ESX- beziehungsweise ESXi-Host-Version die älteste ist, die in den vDS aufgenommen wird. Damit ist Rückwärtskompatibilität – auf Kosten der Features – gewährleistet. Ein Aktualisieren auf eine höhere vDS-Version, sobald keine älteren Hosts mehr vorhanden sind, ist jederzeit möglich.

Die nächste Seite betrifft die Anzahl der Uplinks; die Konfiguration ist auf 4 eingestellt. Maximal sind 32 Uplinks möglich, analog zum Configuration Maximum mit 32 × 1-Gigabit-Adaptern. Diese Werte können später, falls nötig, verändert werden. In dieser Ansicht können Sie auch einen Namen für den vDS eingeben. Diesen Namen können Sie später gegebenenfalls ebenfalls verändern.

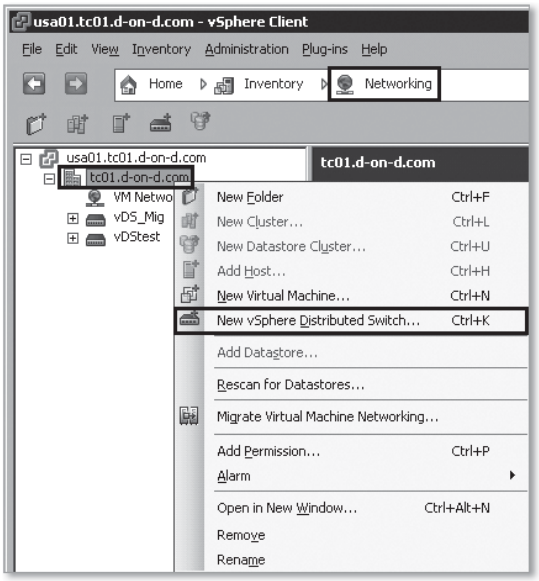


Abbildung 8.25 Ansicht des vSphere-Clients zur Erzeugung eines vDS

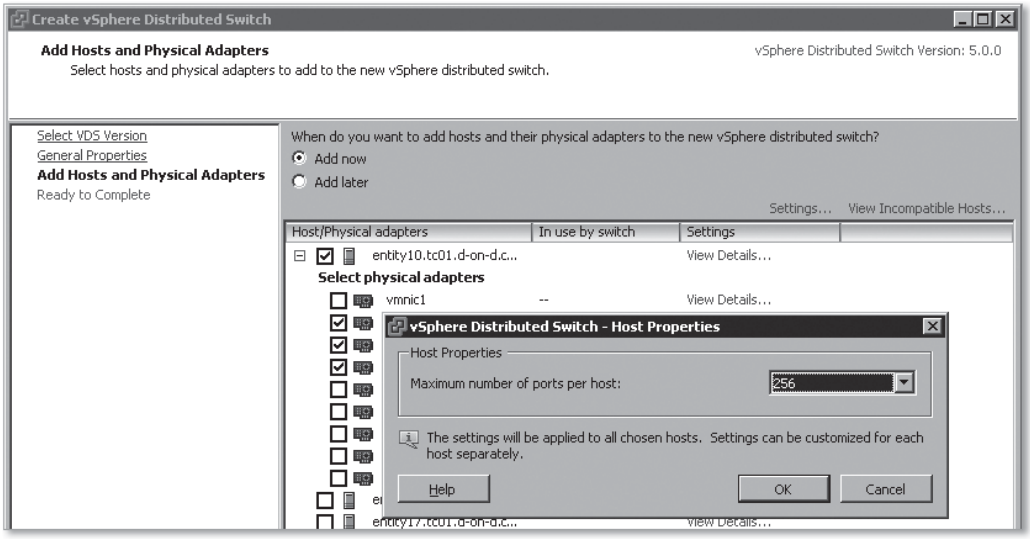


Abbildung 8.26 vDS, Ansicht zum Hinzufügen von Hosts

In der nächsten Ansicht (Abbildung 8.26) fügen Sie die Hosts hinzu. Mit dem Hinzufügen von Hosts können Sie die zu verwendenden vmnic# als Uplink-Adapter bestimmen. Bei der Aufnahme von vmnic# in dieser Ansicht werden nur die vmnic# präsentiert, die noch nirgends verwendet werden. Beim späteren Hinzufügen von ESXi-Hosts ist das nicht mehr der Fall. Wenn gewünscht, bestimmen Sie die Anzahl der zu erstellenden Ports pro Host für diesen

vDS. Die abschließende Ansicht zeigt auf, was mittels Bestätigen von FINISH erzeugt wird. Standardmäßig ist in der Check-Box AUTOMATICALLY CREATE DEFAULT PORT GROUP ein Häkchen gesetzt, so dass eine Portgruppe erzeugt wird. Wünschen Sie das nicht, können Sie das Häkchen natürlich entfernen.

8.6.3 Einstellmöglichkeiten auf dem Switch-Teil des vDS

Ist ein vDS existent, so können Sie die Distributed Portgruppe(n) an ihm konfigurieren. Sie erreichen den Konfigurationsdialog, indem Sie den vDS markieren und mittels rechter Maustaste das Kontextmenü öffnen, siehe Abbildung 8.27.

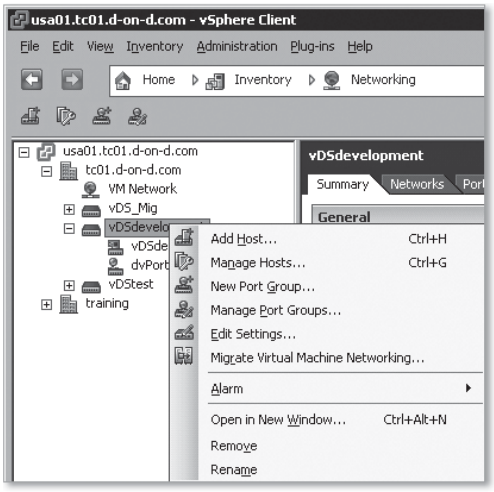


Abbildung 8.27 Einstellmöglichkeiten auf dem vDS

Add Host

Der Menüpunkt ADD HOST... ermöglicht, neue Hosts aufzunehmen, deren Netzwerkkarten für die Uplink-Verwendung zuzuordnen, die virtuellen Adapter (VMkernel-Ports) der ESXi-Hosts zum Beispiel von einem vSS auf den vDS zu migrieren und VMs im Netzwerk zu migrieren. Die Migrationsfunktionen behandeln wir ausführlich in Abschnitt 8.7, »Die Migration von vSS auf vDS«, ab Seite 370.

Manage Hosts

MANAGE HOSTS ist ADD HOSTS... sehr ähnlich. Hier können Sie die Zuordnung der vmnics zu den Uplinks ändern, die virtuellen Adapter (VMkernel-Ports) der ESXi-Hosts verwalten und das Netzwerk der VMs migrieren.

New Port Group

NEW PORT GROUP... erzeugt eine neue Portgruppe.

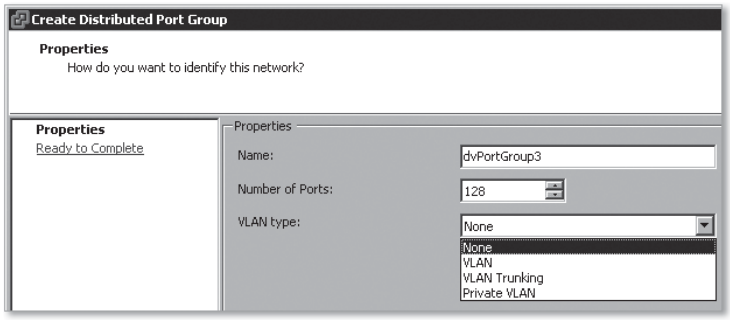


Abbildung 8.28 Konfigurationsdialog beim Erstellen einer Portgruppe

Im Konfigurationsdialog zum Erstellen einer neuen Portgruppe (Abbildung 8.28) können Sie einen Namen vergeben, die Anzahl der Ports einstellen und, wenn gewünscht, einen der drei VLAN-Typen zuordnen und konfigurieren.

Manage Port Groups

Über Manage Port Groups... nehmen Sie Veränderungen über alle Portgruppen an einem vDS gleichzeitig vor. Die Änderungen betreffen Einstellungen wie die Security-Policies, Traffic Shaping oder VLAN, etc. siehe Abbildung 8.29.

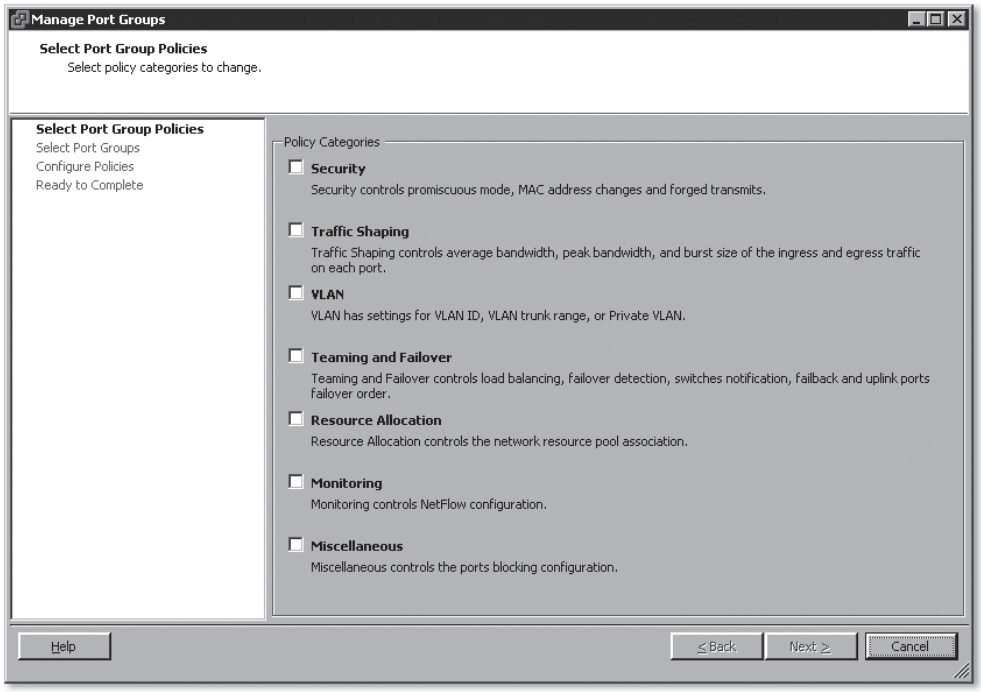


Abbildung 8.29 Konfigurationsdialog »Manage Port Groups«

Edit Settings

Unter Edit Settings konfigurieren Sie den Switch-Teil des vDS, siehe Abbildung 8.30.

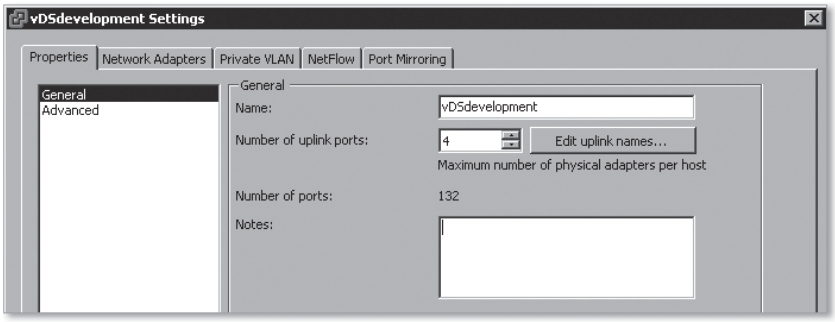


Abbildung 8.30 Eigenschaften des vDS

Properties

In den Eigenschaften des vDS finden Sie unter Properties die Konfigurationspunkte General und Advanced. Unter General können Sie den Namen des vDS ändern, die Anzahl der Uplinks anpassen und die Uplinks benennen. Standardmäßig wird als Name »dvUplink#« vergeben. Grundsätzlich können Sie beliebige Namen nutzen. Ideal ist es, die Hosts, die gemeinsam einem vDS zugeordnet sind, hart zu standardisieren. Das bedeutet: Die gleiche Anzahl vmnics, die entsprechenden vmnic-Nummern über die ESXi-Hosts haben jeweils dieselbe Funktion. Dann können vmnic# und Uplinks einander zugeordnet werden: vmnic1 zu Uplink-Name vmnic1, vmnic2 zu Uplink-Name vmnic2 etc.

- **Advanced**
  Unter Advanced können Sie die MTU Size 1500 und auch CDP oder LLDP in allen bekannten Modi konfigurieren.
- **Network Adapters**
  Bietet eine Ansicht darüber, welche vmnic an welchen Uplink gebunden ist. Dies sind reine Informationen; konfigurieren können Sie in dieser Ansicht nichts.
- **Private VLAN**
  Dient der Konfiguration von Private VLANs, auf die wir in Abschnitt 8.6.4, »Private VLAN«, eingehen.
- **NetFlow**
  Dient der Konfiguration von NetFlow. Mit diesem Thema beschäftigen wir uns in Abschnitt 8.6.7, »NetFlow«.
- **Port-Mirroring**
  Dient der Konfiguration von Port-Mirroring. Port-Mirroring beschreiben wir näher im gleichnamigen Abschnitt 8.6.8.

Migrate Virtual Machine Networking

Migrate Virtual Machine Networking... ermöglicht die Migration von VMs von einer zugewiesenen auf eine neue Portgruppe. Diese Funktion erklären wir ausführlich im Abschnitt 8.7, »Die Migration von vSS auf vDS«.

8.6.4 Private VLAN

Private VLANs (PVLANs) ermöglichen eine bessere Ausnutzung der Netzwerk-Ressourcen. In Abschnitt 8.4.8, »Die VLAN-Einstellungen der vSwitch-Typen«, haben wir die VLAN-Möglichkeiten beschrieben. Normale VLANs sind auf 4.094 verwendbare Möglichkeiten begrenzt. Private VLANs ermöglichen eine erweiterte Konfiguration.

Der erste Konfigurationsschritt, um PVLAN benutzen zu können, muss auf dem Switch-Teil des vDS erfolgen, siehe Abbildung 8.31.

Geben Sie zuerst eine VLAN-ID für das Primary Private VLAN ein (linke Seite in der Eingabemaske). Markieren Sie sie anschließend, und geben Sie in einem zweiten Schritt die Secondary Private VLAN-IDs (rechte Seite in der Eingabemaske) und deren Typ ein.

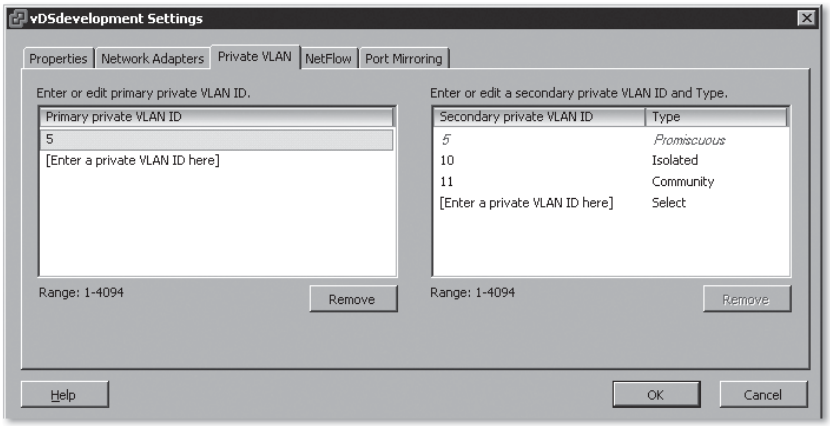


Abbildung 8.31 PVLAN-Einstellungen auf dem Switch-Teil des vDS

Es gibt drei Typen der Secondary Private VLANs, die Sie erzeugen und später den Portgruppen zuweisen können:

- Promiscuous
- Community
- Isolated

In Abbildung 8.32 sehen Sie die Zuweisung eines der erzeugten Secondary VLANs.

Diese verschiedenen Typen haben verschiedene Reichweiten, was die Netzwerk-Kommunikationsmöglichkeiten betrifft. Tabelle 8.10 zeigt eine Zusammenfassung.

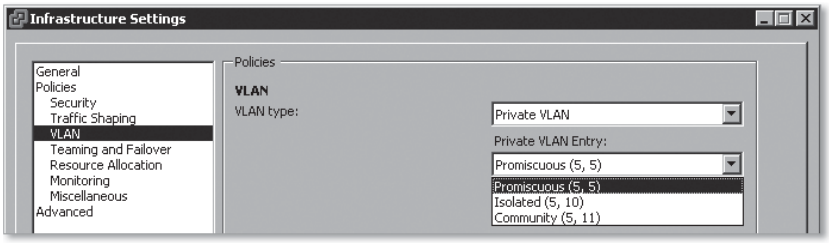


Abbildung 8.32 PVLAN-Einstellungen auf der Portgruppe

	Promiscuous (5, 5)	Community (5, 11)	Isolated (5, 10)
Promiscuous (5, 5)	erreichbar	erreichbar	erreichbar
Community (5, 11)	erreichbar	erreichbar	nicht erreichbar
Isolated (5, 10)	erreichbar	nicht erreichbar	nicht erreichbar

Tabelle 8.10 Kommunikations-Reichweite der PVLAN-Typen

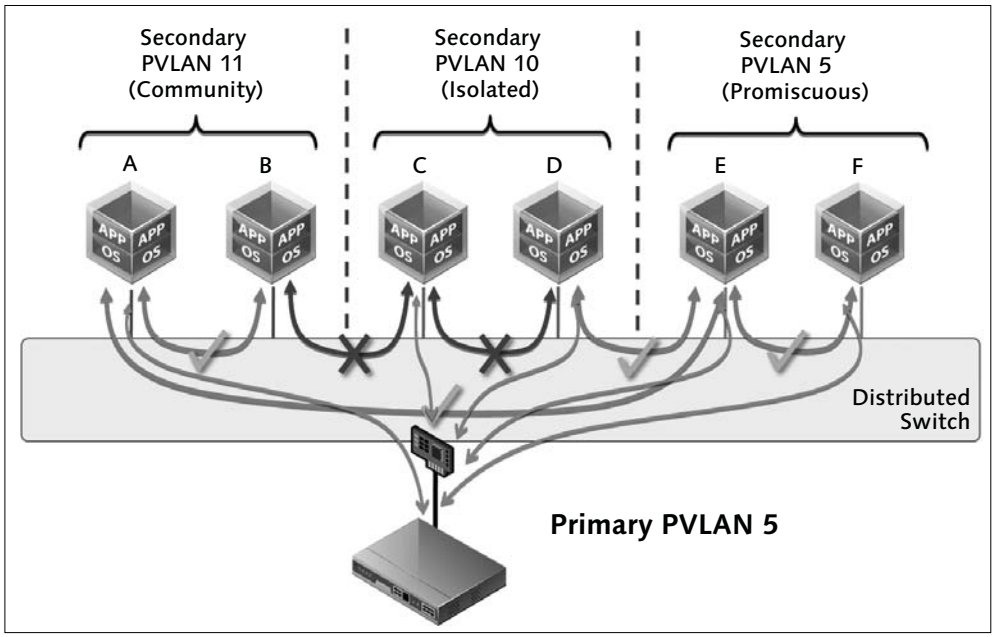


Abbildung 8.33 Kommunikationsbeziehungen der PVLAN-Typen als Grafik

- **Typ »Promiscuous«**
  Dieser Typ hat die größte Reichweite. Ein Client in solch einem PVLAN kann mit den Isolated- und Community-Typen und untereinander kommunizieren.

Anwendungsgebiet: Hier befindet sich zum Beispiel das Standard-Gateway, damit Clients aus dem ISOLATED- und COMMUNITY-VLAN nach außen in das physische Netzwerk kommunizieren können.

- **Typ »Community«**
  Dieser Typ hat eine mittlere Reichweite. Ein Client in diesem PVLAN kann mit den PROMISCUOUS-VLANs innerhalb derselben Community, aber nicht mit den ISOLATED-VLANs kommunizieren.

  Anwendungsgebiet: Hier werden Client und Server einer Firma zusammengefasst, so dass die Firmenressourcen untereinander kommunizieren können, vor anderen Community VLAN-IDs aber geschützt bleiben.

- **Typ »Isolated«**
  Dieser Typ hat die kürzeste Reichweite. Ein Client in diesem PVLAN kann mit den PROMISCUOUS-, aber nicht mit den COMMUNITY- und nicht mit den ISOLATED-VLANs kommunizieren.

  Anwendungsgebiet: Einzelne Private Clients, die sich nicht sehen sollen, obwohl sie sich im selben IP-Bereich und in der gleichen Secondary-VLAN-ID befinden.

8.6.5 Einstellmöglichkeiten auf der Distributed Portgruppe

Bei der Erzeugung einer Portgruppe auf einem vDS können Sie nicht alle möglichen Einstellungen sofort vornehmen, sondern erst später, wenn diese erstellt wurde. Markieren Sie dazu die Portgruppe, und öffnen Sie mittels EDIT SETTINGS die Konfigurationsmasken.

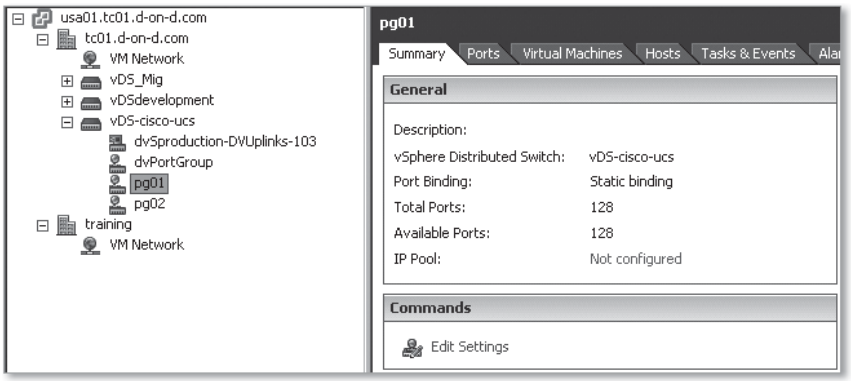


Abbildung 8.34 Übersicht der Eigenschaften einer Portgruppe

Es gibt zwei Typen von Portgruppen im vDS, wie Abbildung 8.34 zeigt. Die eine Portgruppe ist für die Verbindung von VMs und VMkernel gedacht. Die andere enthält ausschließlich die Uplink-Adapter.

In der ersten Einstellung GENERAL können Sie den Namen anpassen und die Anzahl der Ports und die Art des PORT BINDINGS konfigurieren (Abbildung 8.35).

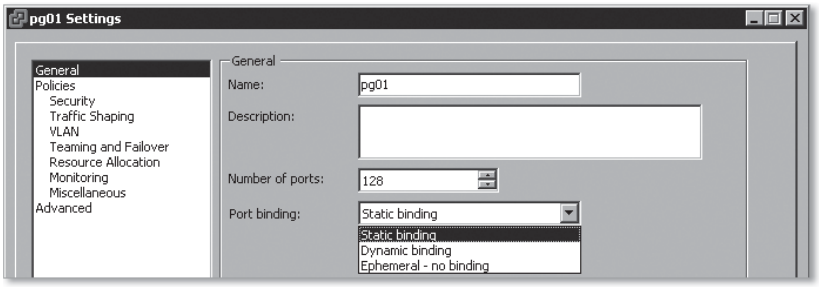


Abbildung 8.35 Geöffnete Konfigurationsmaske einer Portgruppe

- **Port binding: Static binding**
  Dies ist die Standardeinstellung. Die Wirkungsweise ist folgende: Wird eine virtuelle NIC einer VM oder ein VMkernel dieser Portgruppe zugeordnet, so belegt sie einen Port. Der Port gilt als belegt, sobald ein Device an ihn angeschlossen wurde. Eine VM, die zum Beispiel nicht läuft, belegt trotzdem einen Port. In der Einstellung NUMBER OF PORTS: 128 ist demzufolge die Anschlussmöglichkeit bei 128 Teilnehmern erschöpft, egal in welchem Modus sie sich befinden.
- **Port binding: Dynamic binding**
  Bei DYNAMIC BINDING gilt ein Port dann als belegt, wenn ein Teilnehmer aktiv ist. Eine VM, die läuft, gilt als aktiv und belegt einen Port. Haben Sie 128 Ports und 150 Teilnehmer, so ist dies kein Problem, wenn nie mehr wie 128 VMs parallel laufen.
- **Port binding: Ephemeral – no binding**
  Bei EPHEMERAL – NO BINDING gibt es keine fixe Portanzahl. Für jeden angeschlossenen Teilnehmer wird automatisch ein Port erhöht.

Die meisten der folgenden Einstellungen haben wir schon an anderer Stelle dargestellt oder beschreiben sie später. Tabelle 8.11 zeigt, in welchen Abschnitten Sie die Erläuterungen zu diesen Themen finden.

Thema	Abschnitt	Titel	Seite
Layer-2-Security-Policy	8.4.6	»Die Layer-2-Security-Policies«	331
Traffic-Shaping	8.4.7	»Traffic-Shaping«	332
VLAN	8.4.8	»Die VLAN-Einstellungen der vSwitch-Typen«	333
Teaming and Failover	8.4.9	»Die NIC-Teaming- und die Load-Balancing-Policies der vSwitch-Typen«	336
Resource-Allocation	8.6.6	»Network I/O Control«	359
Monitoring	8.6.7	»NetFlow«	363

Tabelle 8.11 Portgruppe-Themen, die an anderen Stellen behandelt werden

Auf der Portgruppe gibt es außerdem Einstellmöglichkeiten für POLICIES – MISCELLANEOUS und ADVANCED.

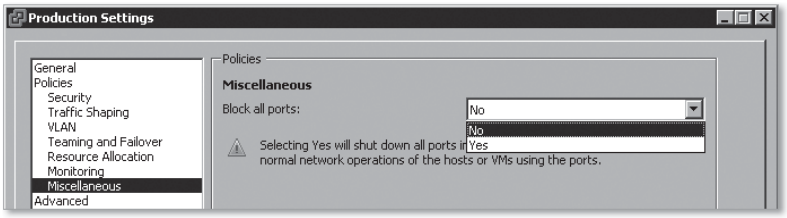


Abbildung 8.36 Portgruppen-Einstellung »Miscellaneous«

Unter Miscellaneous (Abbildung 8.36) können Sie alle Ports für die ausgewählte Portgruppe auf einen Schlag blockieren. Auf »einen Schlag« heißt: alle daran angeschlossenen VMs auf allen in dem vDS aufgenommenen Hosts (bis 350). Das bedeutet, Sie können Tausende von VMs innerhalb von Sekunden sofort vom Netz nehmen. Wenn sie dasselbe mit vSS-Portgruppen machen möchten, wären Sie bei 350 Hosts locker eine Stunde und mehr beschäftigt, weil Sie jeden einzelnen Host behandeln müssten.

Wofür ist so etwas sinnvoll? Wenn zum Beispiel ein bis dato unbekannter und hoch aggressiver Virus oder Wurm durch das Netz ginge, so wäre es möglich, sehr schnell zu intervenieren, auch wenn die Infrastruktur Tausende von VMs hätte. Einzelne Abschnitte könnten sofort stillgelegt werden.

Die Einstellung Advanced ermöglicht, die Policy-Einstellungen auf eine Portgruppe zu fixieren (Abbildung 8.37). Fixierte Teile (Overrides Allowed? – No) können dann nicht mehr auf einem Port direkt verändert werden. Ist die Portgruppen-Policy nicht fixiert (Overrides Allowed? – Yes), so ist es möglich, die Einstellung auf dem Port zu verändern (Abbildung 8.38).

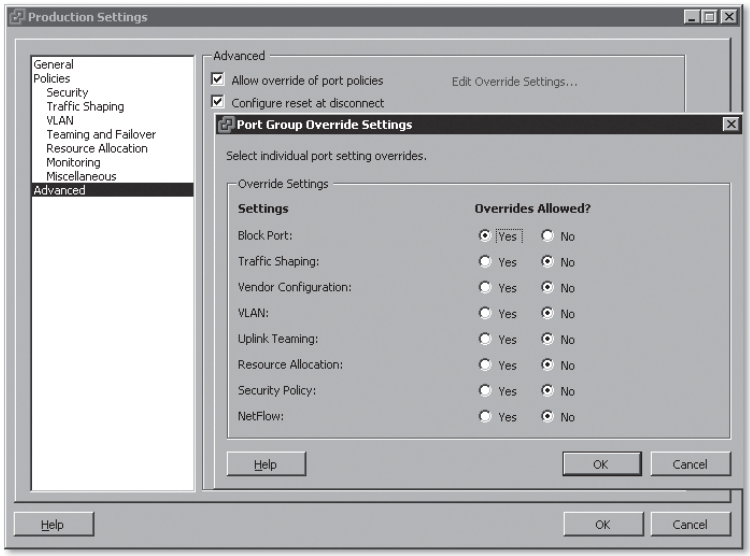


Abbildung 8.37 Portgruppen-Einstellung »Advanced«

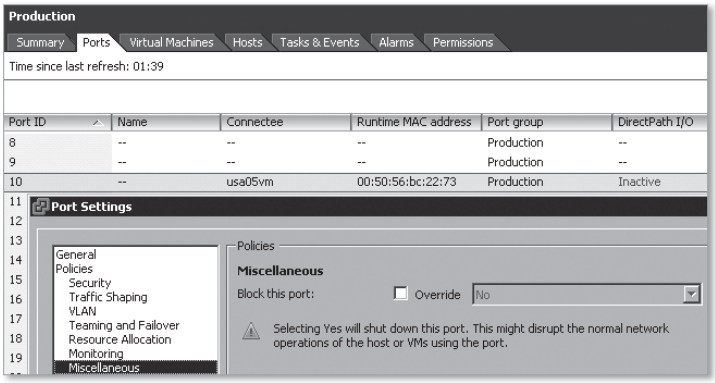


Abbildung 8.38 Einstellungen Port-Policy

8.6.6 Network I/O Control

Mittels Network I/O Control können Sie den Netzwerkverkehr bei den vDS sehr granular modellieren. In den Standardeinstellungen ist die Network I/O Control ausgeschaltet, siehe Abbildung 8.39. Mit vSphere 5.0 wurde Network I/O Control um die Features benutzerdefinierte Ressource-Pools und Quality-of-Service-(QoS-)Tagging (802.1p) erweitert.

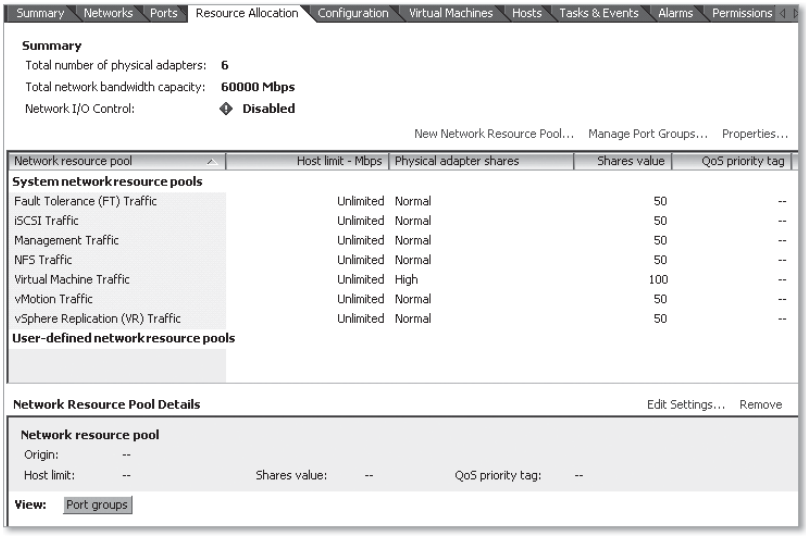


Abbildung 8.39 Ressource-Allocation Network I/O Control

Unter Ressource Allocation sehen und ändern Sie die Konfigurationen für Network I/O Control.

Unter Summary erfahren Sie die Anzahl der Netzwerkadapter und die daraus resultierende Bandbreite. Im Beispiel in Abbildung 8.39 stehen sechs physische Adapter an dem vDS zur

Verfügung. Diese zusammen ergeben eine Bandbreite von 60.000 MBps. Daraus resultiert, dass an diesem vDS 10-Gigabit-Adapter zum Einsatz kommen.

In der Spalte Network resource pool gibt es zwei Unterteilungen. Im ersten Bereich, System network resource pools, sehen Sie die vordefinierten Netzwerk-Verkehrsmuster von VMware vSphere 5.0. Diese können Sie ändern, aber nicht löschen. Im zweiten Bereich, User-defined network resource pools, finden Sie die vorhandenen benutzerdefinierten Netzwerk-Resource-Pools. Diese können Sie über New Network Ressource Pool… erstellen, jederzeit ändern und wieder löschen. In den weiteren Spalten können Sie die Netzwerk-Bandbreiten-Zuordnungen zu den verschiedenen Netzwerk-Resource-Pools einsehen.

Bevor Sie Einstellungen bei den Ressourcen treffen können, müssen Sie Network I/O Control aktivieren, und zwar über Properties… mittels Setzen des Häkchens bei Enable Network I/O Control on this vSphere distributed switch, siehe Abbildung 8.40. Die Network I/O Control wird immer pro einzelnen vDS aktiviert.

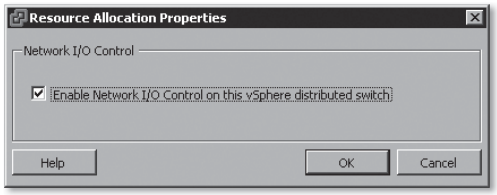


Abbildung 8.40 Aktivieren der Network I/O Control

Durch einen Doppelklick auf eines der sieben Netzwerk-Verkehrsmuster öffnet sich ein Fenster, in dem Sie alle Einstellungen vornehmen können (Abbildung 8.41).

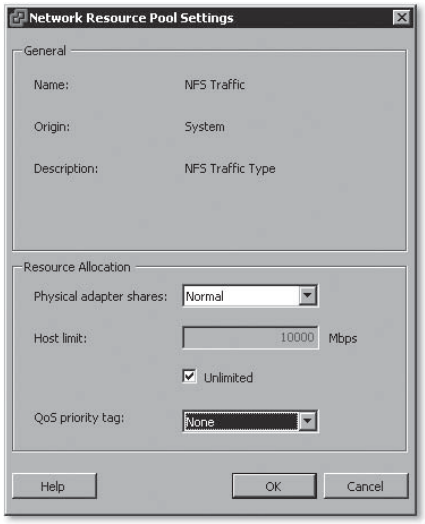


Abbildung 8.41 Einstellmöglichkeiten im Netzwerk-Resource-Pool »NFS Traffic«

Unter Resource Allocation greifen Sie auf die folgenden Einstellungen zu:

- **Physical adapter shares**
  Das Konzept der Shares ähnelt demjenigen, wie es schon lange bei CPU und Memory bekannt ist. Es gibt vordefinierte Werte: Low (25), Normal (50), High (100) und Custom (benutzerdefiniert). Shares kommen nur dann zum Einsatz, »wenn der Hunger größer ist als der Kuchen«, wenn also mehr Bandbreite als vorhanden verwendet werden sollte. Mehr Shares geben ein größeres Stück vom Kuchen. Anders ausgedrückt: Wenn ein Verkehrsmuster 25, das andere 50 Shares besitzt, so bekommt das mit 50 doppelt so viel Bandbreite wie das mit 25 Shares.
- **Host Limit**
  Im Standard ist Unlimited gesetzt. Entfernen Sie das Häkchen, können Sie das Netzwerk-Verkehrsmuster eingrenzen. Diese Obergrenze an Bandbreite wirkt im Gegensatz zu den Shares immer, also auch dann, wenn noch viel Bandbreite zur Verfügung stünde. Die Werte sind in MBps definiert.
- **QoS priority tag**
  Der Standard ist auf None gesetzt, also inaktiv (0), was »best Effort« im Netzwerk bedeutet. Sie können Werte von 1 bis 7 eingeben. 1 hat die tiefste, 7 die höchste Priorität. Die QoS im Network I/O Control von vSphere 5.0 ist nach Standard IEEE 802.1p (Layer 2) definiert und kann somit die QoS-Informationen in das physische Netzwerk weitergeben, falls die physischen Komponenten dies unterstützen.

Konfiguration	Network Priority	Akronym	Verkehrsmuster
1	0 (tiefste)	BK	Hintergrund
KEINE (0)	1	BE	Bester Effort
2	2	EE	Exzellenter Effort
3	3	CA	Kritische Applikationen
4	4	VI	Video, <100ms Latenzzeit
5	5	VO	Stimme, <10ms Latenzzeit
6	6	IC	Internetzwerk Kontrolle
7	7 (höchste)	NC	Netzwerk Kontrolle

Tabelle 8.12 QoS-Skala

Benutzerdefinierte Netzwerk-Resource-Pools

Einen benutzerdefinierten Netzwerk-Resource-Pool erstellen Sie über New Network Resource Pool... Sehen wir uns dazu ein Beispiel an, in dem wir zwei Netzwerk-Resource-Pools anlegen – einen mit hoher Priorität, den anderen mit einer sehr tiefen Priorität.

Schritt 1:

Erstellen Sie zwei neue Netzwerk-Resource-Pools. Abbildung 8.42 zeigt die Erstellung eines der Resource-Pools.

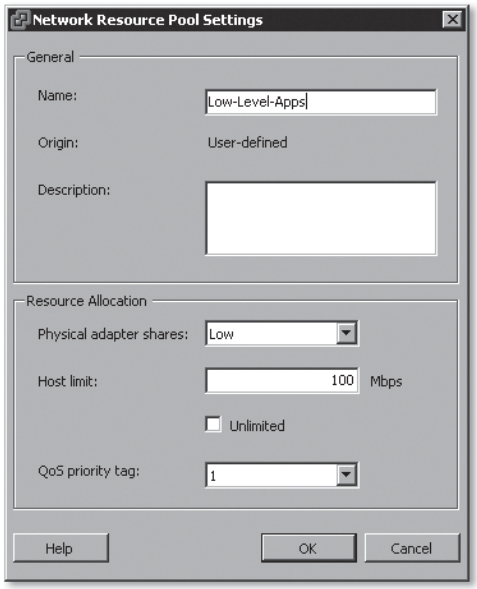


Abbildung 8.42 Erstellung Netzwerk-Resource-Pool »Low-Level-Apps«

In Abbildung 8.43 sehen Sie die beiden erzeugten Resource-Pools.

Abbildung 8.43 Zwei benutzerdefinierte Netzwerk-Resource-Pools

Schritt 2:

Nun ordnen Sie wie in Abbildung 8.44 die Portgruppen den entsprechenden Network-Resource-Pools zu.

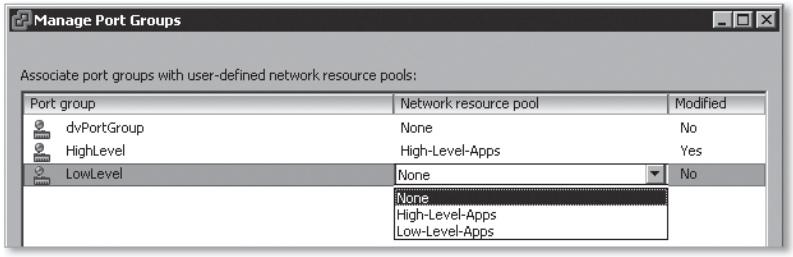


Abbildung 8.44 Zuordnung der Portgruppen zu den Netzwerk-Resource-Pools

Schritt 3:
Abschließend ordnen Sie die entsprechenden VMs den jeweiligen Portgruppen zu, und fertig ist die Konfiguration.

8.6.7 NetFlow

NetFlow ist eine neue Funktion, die mit vSphere 5.0 eingeführt wurde. NetFlow wurde ursprünglich von Cisco entwickelt und wird mittlerweile von vielen Herstellern unterstützt. Mittels NetFlow – der Name sagt es eigentlich schon – können Daten über den Netzwerkverkehr gesammelt werden. Für NetFlow benötigen Sie zusätzliche Software. Die eine Komponente ist diejenige, die die Daten sammelt, auch *Kollektor* genannt. Eine weitere Komponente dient der Auswertung der gesammelten Daten, dies wäre der *Analyzer*. Es gibt diverse kostenlose Produkte, vor allem im Linux-Umfeld; für Windows existieren deutlich weniger. Ich habe für den folgenden Implementierungsteil das kostenlose Tool *SolarWinds Real-time NetFlow Analyzer* der Firma SolarWinds verwendet.

Die folgenden Schritte zeigen die Einrichtung von NetFlow mit den vDS auf.

Schritt 1:
Der erste Schritt ist die Aktivierung von NetFlow auf den vDS (Abbildung 8.45).

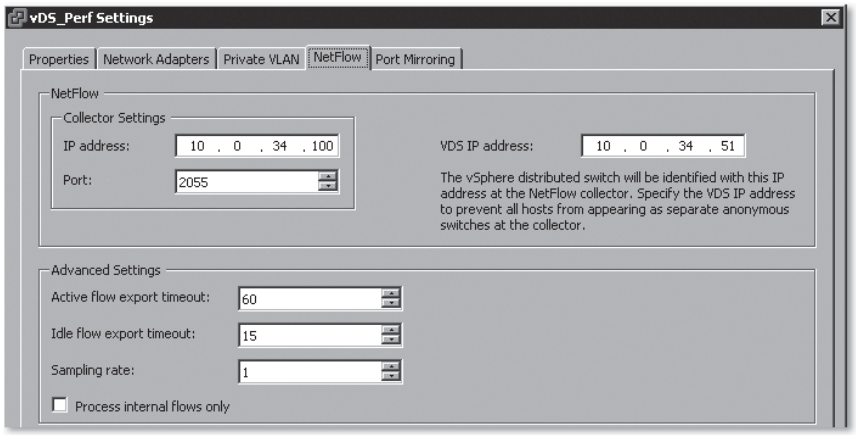


Abbildung 8.45 NetFlow-Einrichtung auf dem vDS

Für die Konfiguration von NetFlow auf dem vDS geben Sie unter Collector Settings die IP-Adresse des NetFlow-Collectors an und stellen die Portnummer ein. Beim vDS ist der Standard Port 1, bei SolarWinds Port 2055. Passen Sie entweder vDS- oder den Collector-Port an. In unserem Beispiel habe ich den Port auf dem vDS angepasst. Unter VDS IP address geben Sie für den vDS eine IP-Adresse an, damit der Collector die Daten abgreifen kann. Unter Advanced Settings können Sie Timeout-Werte für den Datenfluss und die Sampling-Rate vorgeben. Ich habe bei Sampling rate den Wert von 1 angegeben. Mit dieser Einstellung wird jedes

Paket erfasst. In der Praxis wird diese Sampling-Rate meist höher gesetzt, damit die Systemlast nicht zu hoch wird. So bedeutet ein Wert von 3, dass jedes dritte, ein Wert von 10, jedes zehnte Paket erfasst wird.

Schritt 2:
Nachdem Sie den vDS für NetFlow vorbereitet haben, müssen Sie auch die Portgruppe auf dem vDS für NetFlow aktivieren, wie in Abbildung 8.46 auf der Portgruppe PRODUCTION.

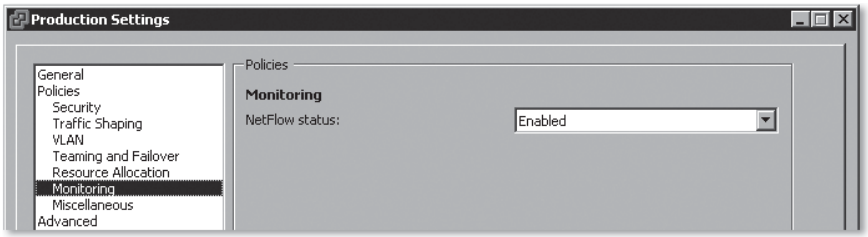


Abbildung 8.46 NetFlow auf der Portgruppe aktivieren

Schritt 3:
Nachdem Sie den vDS und die Portgruppe(n) aktiviert haben, können Sie die NetFlow Software konfigurieren. Der erste Schritt beim NetFlow-Collector ist, die IP-Adresse des vDS anzugeben, damit die Software weiß, von wo Daten gesammelt werden sollen. In unserem Beispiel war das die IP-Adresse 10.0.34.51.

Haben Sie Ihr NetFlow-Device registriert, so werden alle erkannten Port-IDs dargestellt (Abbildung 8.47).

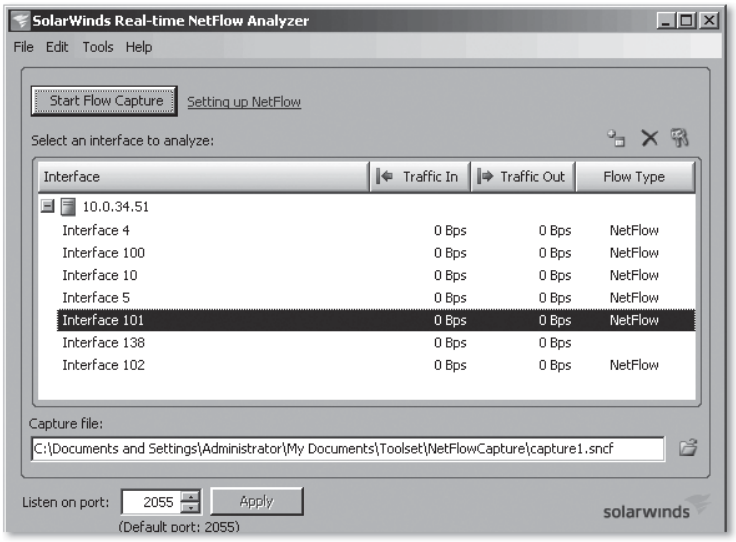


Abbildung 8.47 Selektieren des Ports für die Messung

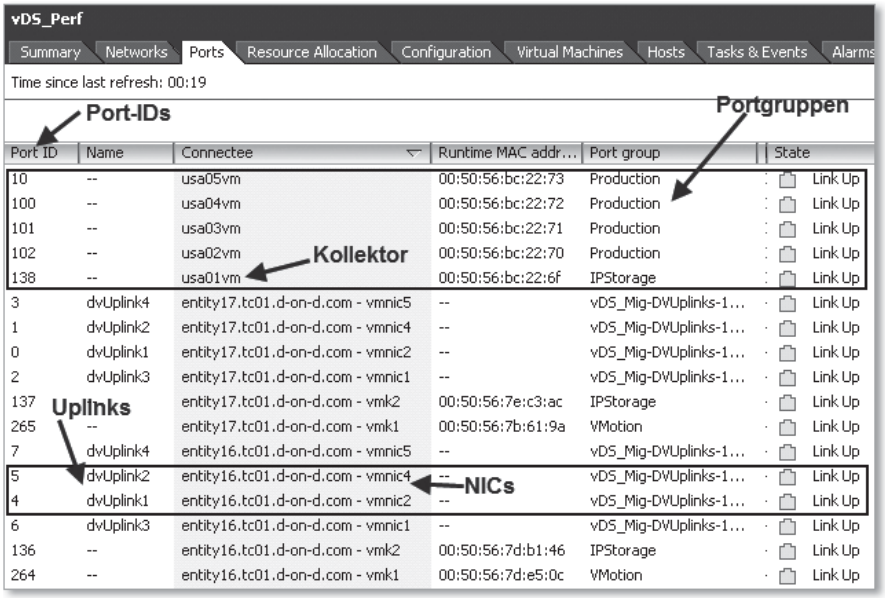


Abbildung 8.48 Port-Informationen auf dem vDS

In welcher Beziehung stehen die abgebildeten Ports (Abbildung 8.47)? Es sind die Port-IDs, an denen im vDS die verschiedenen Komponenten angeschlossen sind. Ich habe, um dies zu veranschaulichen, einen Screenshot der Ports des vDS gemacht (Abbildung 8.48). Wenn Sie die beiden Abbildungen vergleichen, sehen Sie genau, dass die aufgelisteten Objekte in einem 1:1-Bezug zueinander stehen. Die VMs sind auf Port-ID 10, 100, 101, 102, 138. Bei allen läuft das NetFlow-Protokoll, außer auf 138. Die VM »usa01vm« an Port 138 ist der Kollektor. Diese VM wurde an die Portgruppe »IPstorage« angeschlossen, die nicht für NetFlow aktiviert ist. Die angezeigten Uplinks werden von den Netzwerkkarten des ESXi-Hosts belegt, über die der NetFlow-Verkehr abgewickelt wird.

Schritt 4:

In diesem Schritt können die Daten visualisiert und überprüft werden (Abbildung 8.49). Da die Port-ID 101 in der Software ausgewählt wurde, sind die Daten dieses Ports dargestellt. Nach kurzer Zeit sind die Daten im Kollektor sichtbar – die übermittelte Datenmenge, aber auch verschiedene Protokolle.

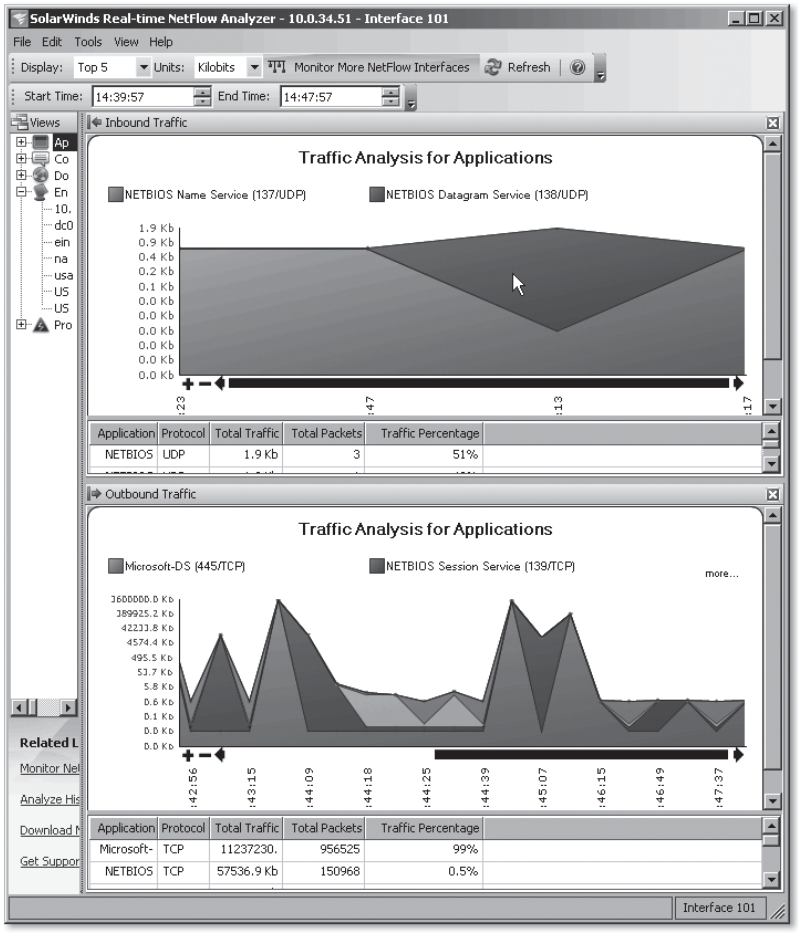


Abbildung 8.49 NetFlow-Informationen grafisch dargestellt in SolarWinds

8.6.8 Port-Mirroring

Vor vSphere 5.0 konnte Netzwerkverkehr von anderen Teilnehmern nur im Promiscuous Mode aufgezeichnet werden. Das Problem daran ist, dass dann gleich alle Teilnehmer an dem betreffenden vSwitch-Typ wahrgenommen wurden. Selbstverständlich konnte man Filter in der Sniffer-Software setzen, um Einschränkungen vorzunehmen. Praktischer ist auf jeden Fall, den Port zu spiegeln, wenn nur der Verkehr eines Teilnehmers verfügbar sein soll (siehe auch Abbildung 8.50). Oder Sie erstellen n:1-Beziehungen, spiegeln also mehrere Ports auf einen einzigen.

Port-Mirroring muss auf dem vDS eingerichtet werden. Nachfolgend stellen wir die Konfiguration eines Mirrorings dar.

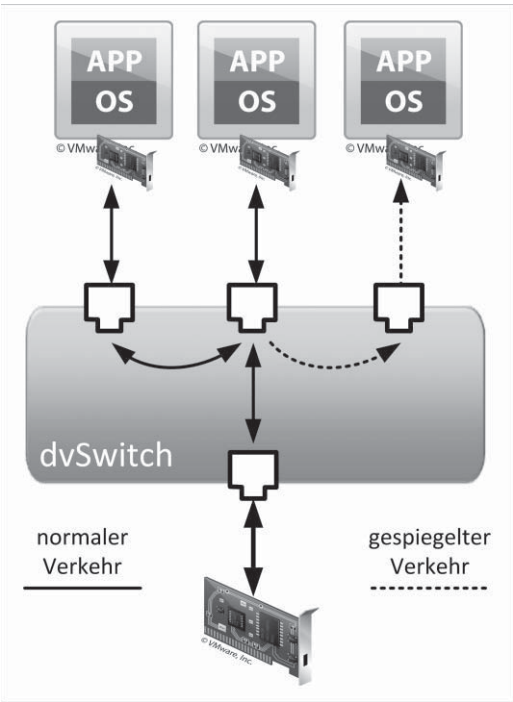


Abbildung 8.50 Schema-Mirroring

Schritt 1:

Die Identifikation der Portnummer ist der erste Schritt. Selektieren Sie dazu den vDS, und wählen Sie anschließend die Registerkarte PORTS aus (siehe Abbildung 8.51). Wie Sie in der Abbildung sehen, gibt es drei VMs: an den Port-IDs 100, 101,102. Wir zeigen nun die Einrichtung eines Port-Mirrors der Port-ID 101 zu Port-ID 100.

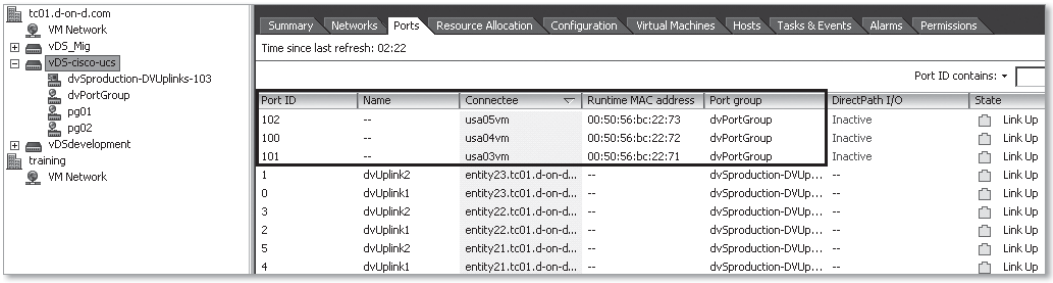


Abbildung 8.51 Die wichtigen Informationen für Port-Mirroring

Schritt 2:

Öffnen Sie auf dem vDS über EDIT SETTINGS den Konfigurationsdialog, und wählen Sie PORT MIRRORING, siehe Abbildung 8.52. Mit ADD… starten Sie den Assistent zur Einrichtung.

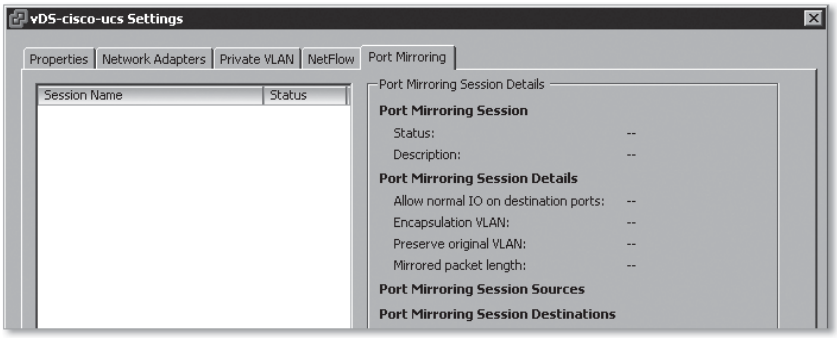


Abbildung 8.52 vDS, »Edit Settings«-Ansicht »Port Mirroring«

Schritt 3:

In diesem Schritt erstellen wir die Grundkonfigurationen. Geben Sie dem Port-Mirror einen Namen. Sie können weitere Details eingeben wie das Umleiten auf ein anderes VLAN, Paketgrößen etc. (siehe Abbildung 8.53).

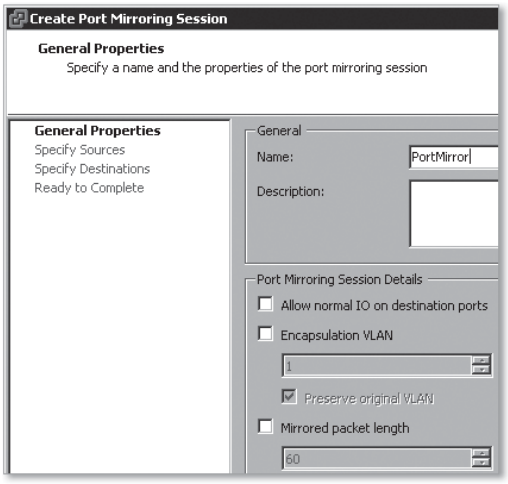


Abbildung 8.53 »General Properties«

Schritt 4:

Geben Sie wie in Abbildung 8.54 die Quelle, von der Daten bezogen werden, ein. Tragen Sie dazu die Port-ID in das linke Feld ein. Über den Selektor stellen Sie die Richtung des Netzwerkverkehrs ein. Drei Möglichkeiten sind vorhanden:

- Ingress/Egress (eingehend/ausgehend)
- Ingress (eingehend)
- Egress (ausgehend)

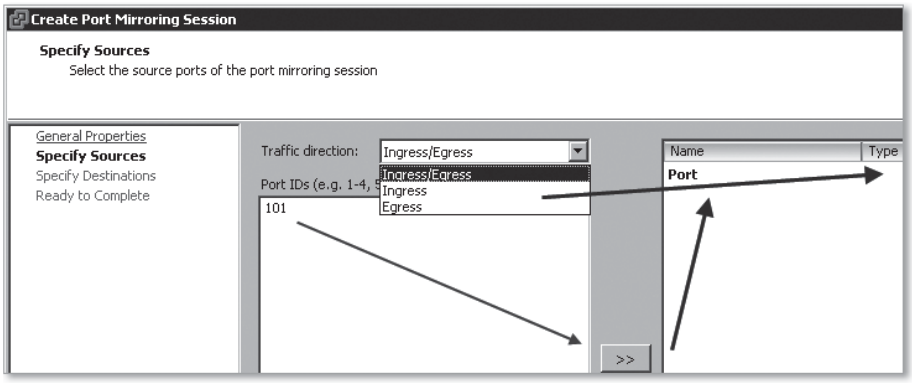


Abbildung 8.54 Quelle für das Port-Mirroring wählen

Schritt 5:

Geben Sie wie in Abbildung 8.55 das Ziel an.

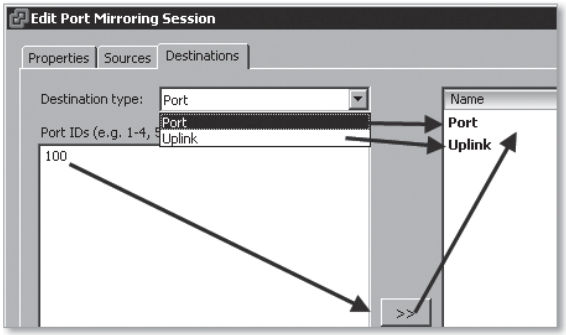


Abbildung 8.55 Ziel für das Port-Mirroring angeben

Schritt 6:

In Schritt 6 (vergleiche Abbildung 8.56) ist es wichtig, die Checkbox ENABLE THIS PORT MIRRORING SESSION zu aktivieren.

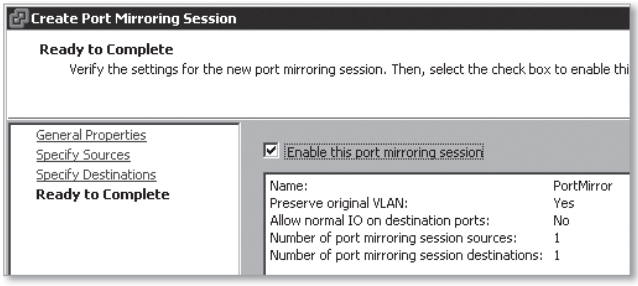


Abbildung 8.56 Bestätigung – Aktivieren der Port-Monitoring-Session

Schritt 7:
Überprüfen Sie abschließend Ihre Eingaben. Müssen Sie Korrekturen vornehmen, so markieren Sie wie in Abbildung 8.57 den Session Name und öffnen durch anklicken von Edit die Konfiguration.

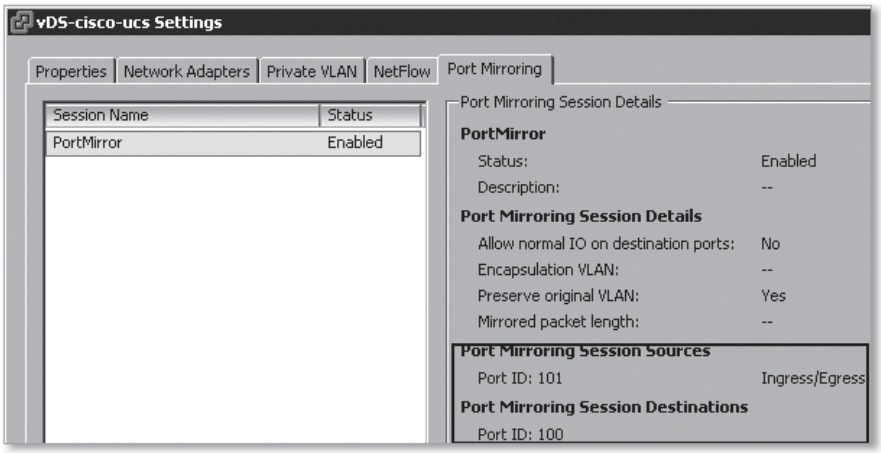


Abbildung 8.57 Zusammenfassung der Konfiguration der Port-Mirroring-Session

8.7 Die Migration von vSS auf vDS

Bei bestehenden Infrastrukturen ist es mitunter erwünscht, dass von den bestehenden Standard-vSwitches zu den dvSwitches migriert werden kann. Diesen Vorgang können Sie, wenn Sie gut geplant und bestimmte Voraussetzungen eingehalten haben, ohne Unterbrechung durchführen.

Das folgende Szenario zeigt, wie Sie diese Migration Schritt für Schritt durchführen. Folgende Ziele sollen erreicht werden:

- Es darf zu keinerlei Unterbrüchen in der Netzwerkkommunikation kommen.
- Das Management-Netzwerk soll als Standard-vSwitch erhalten bleiben.
- Die virtuellen Maschinen sollen von der Portgruppe »VM Network« auf eine neue Portgruppe »Production« migriert werden.
- Die Verkehrsmuster sollen mittels Active und Standby-Adaptern getrennt werden.

Wie Sie im Screenshot (Abbildung 8.58) sehen, existieren drei vSS, die jeweils Redundanz besitzen. In einem ersten Schritt lösen Sie bei allen Hosts die Redundanz auf, damit physische Netzwerkadapter frei werden, die Sie bei dem vDS (vNetwork Distributed Switch) verwenden können. Dies sieht aus wie in Abbildung 8.59.

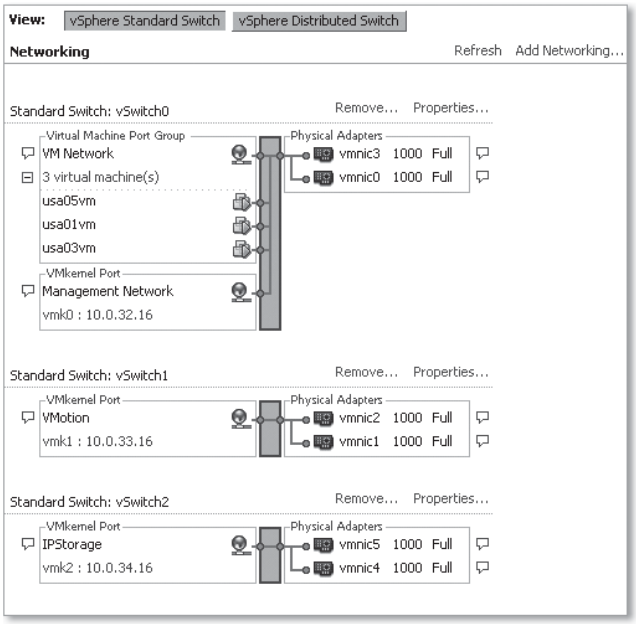


Abbildung 8.58 Ausgangslage für die Migration

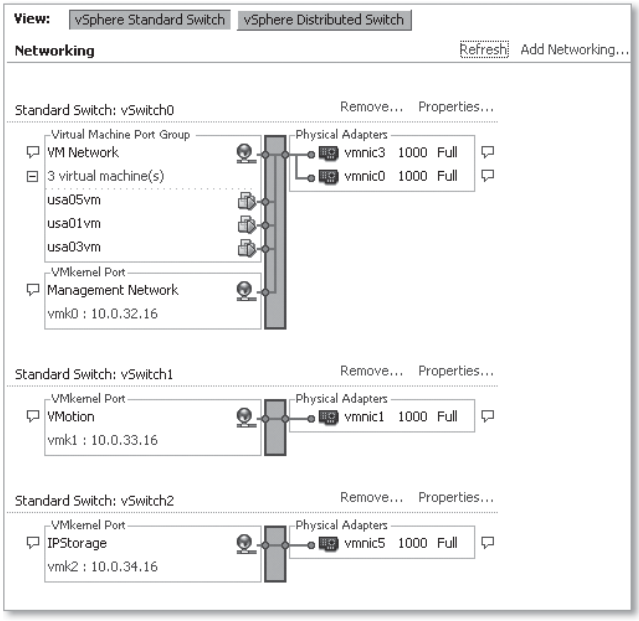


Abbildung 8.59 Redundanz vSwitch1 und vSwitch 2 aufgelöst

Etwaige Alarmmeldungen, die sich auf den Verlust von Netzwerkredundanz beziehen, können Sie ignorieren oder quittieren (Abbildung 8.60).

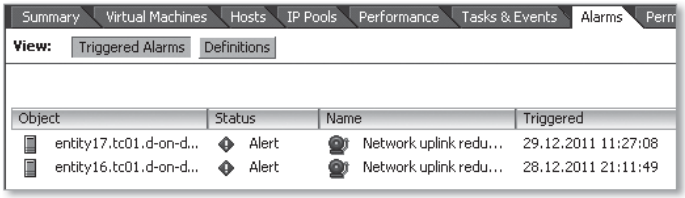


Abbildung 8.60 Alarme über Redundanzverlust können Sie ignorieren.

Nachdem wir freie Netzwerkadapter haben, können wir nun den vDS erzeugen und die frei gewordenen Netzwerkadapter als Uplinks verwenden. Das ganze Gebilde sieht danach aus wie in Abbildung 8.61. Sie sehen, dass beide Hosts im vDS registriert wurden und ihre Netzwerkkarten vmnic2 und vmnic4 als Uplink-Adapter zur Verfügung stellen.

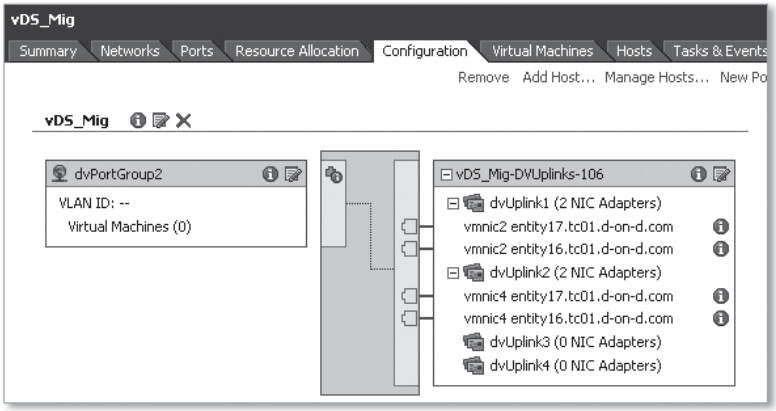


Abbildung 8.61 vDS erzeugt

In einem weiteren Schritt erzeugen wir die Portgruppen. Da wir als Anforderung haben, dass die Verkehrsmuster mit Active und Standby-Adaptern gehandhabt werden müssen, ist es zwingend, zwei weitere Portgruppen zu erzeugen. Mit der Erzeugung des vDS wurde schon eine Standard-Portgruppe namens »dvPortGroup2« (siehe Abbildung 8.61) erstellt. Diese können wir zum Beispiel für die virtuellen Maschinen verwenden, indem wir sie in »Production« umbenennen. Danach erstellen Sie die zwei noch fehlenden Portgruppen namens »vMotion« und »IPStorage«.

Das Endresultat sieht aus wie in Abbildung 8.63.

Der nächste Schritt ist die Migration der VMkernel-Ports, entweder über eine Migrationsfunktion auf dem einzelnen Host oder global im vCenter (Abbildung 8.64). Eine Netzwerkunterbrechung im eigentlichen Sinne findet dabei nicht statt. Trotzdem sollten Sie solche Migrationen – vor allem wenn es sich um den VMkernel handelt, der für den IP-Storage verwendet wird – auf Randzeiten legen, also dann, wenn nicht der größte I/O zum IP-Storage stattfindet.

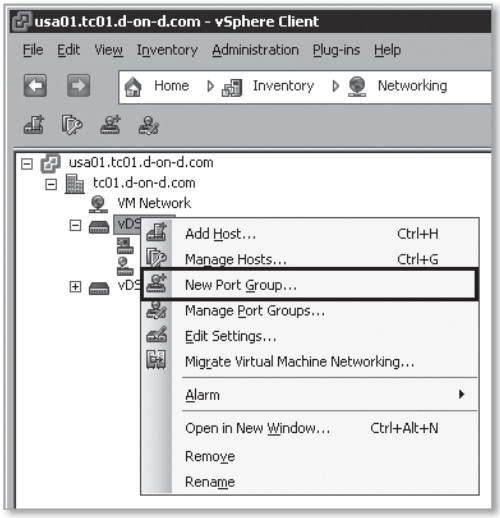


Abbildung 8.62 Erzeugen einer Portgruppe

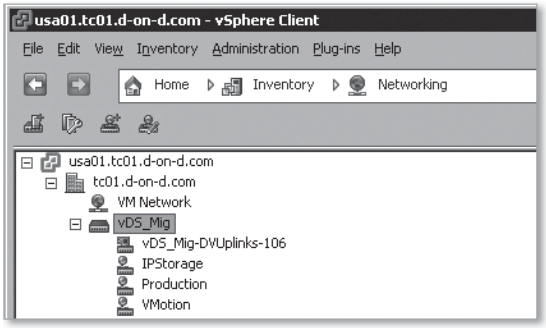


Abbildung 8.63 Alle Portgruppen wurden erzeugt.

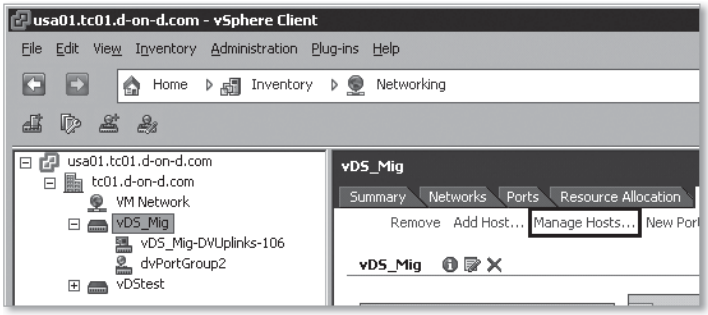


Abbildung 8.64 VMkernel-Migration über vCenter – Schritt 1

Nachdem Sie MANAGE HOSTS... angeklickt haben, erscheint ein Assistent, und leitet die Migration ein. Die erste Ansicht des Assistenten heißt SELECT HOSTS. Hier markieren Sie die

beteiligten Hosts für die VMkernel-Migration (dafür wurde nicht extra ein Screenshot angefertigt). In der zweiten Ansicht, SELECT PHYSICAL ADAPTERS (siehe Abbildung 8.65), können Sie die physischen Adapter der Hosts auf den vDS übertragen. Da Sie mit der Migration der zwei VMkernel »vMotion« und »IPStorage« die Adapter vmnic1 und vmnic5 nicht mehr an den vSS benötigen, können Sie dies gleich mit erledigen. Anmerkung: Die Migration erfolgt koordiniert, das heißt, dass zuerst die VMkernel migriert werden.

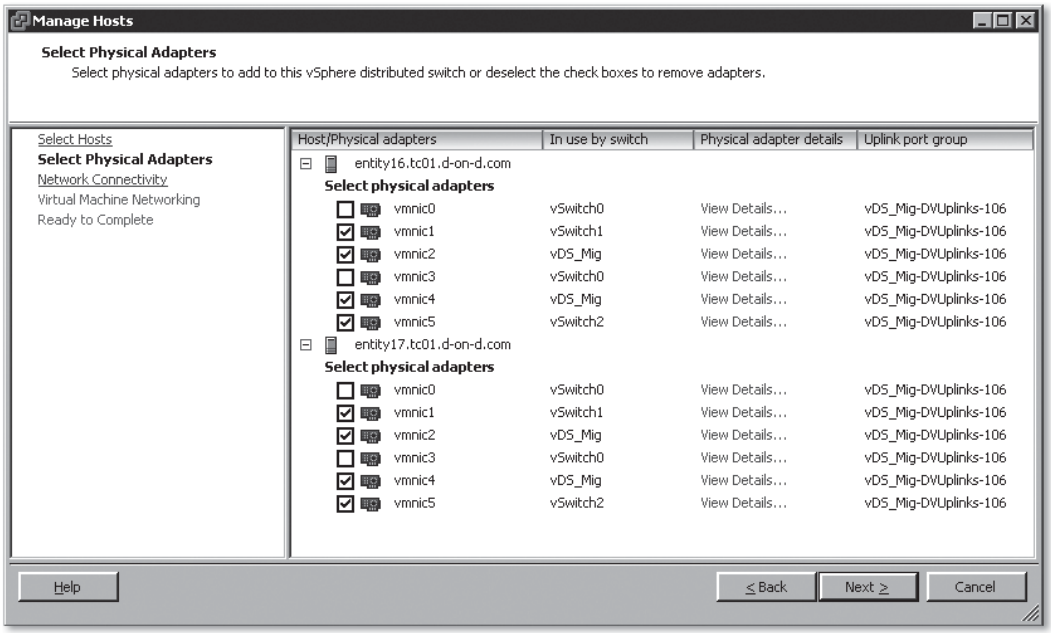


Abbildung 8.65 vmnic1 und vmnic5 werden gleich auf den vDS migriert.

Die nächste Ansicht, NETWORK CONNECTIVITY, stellt die vorhandenen VMkernel dar und testet deren Netzwerkverbindung. Jeder VMkernel, der nach der Migration ohne Netzwerkverbindung dastünde, wird mit einem Warnsymbol versehen. Hier ist es wichtig, dass die Ziele, also auf welche Portgruppen die einzelnen VMkernel migriert werden, netzwerktechnisch korrekt funktionieren, damit es nicht zu Unterbrüchen kommt.

In der nächsten Ansicht, VIRTUAL MACHINE NETWORKING, können Sie die virtuellen Maschinen ab der existierenden Portgruppe auf eine andere Portgruppe migrieren. Sie können jede VM, wenn gewünscht, speziell behandeln. Anmerkung: Müssen Sie viele virtuelle Maschinen migrieren, so ist dieser Assistent etwas mühsam, da Sie relativ viel »herumklicken« müssen. Als Alternative bietet sich der Weg über das Migrationstool für die Netzwerkkonfiguration der virtuellen Maschinen an. Dieses erreichen Sie, indem Sie einen vDS markieren und mittels rechter Maustaste das Kontextmenü öffnen. In diesem wählen Sie den Menüpunkt MIGRATE VIRTUAL MACHINE NETWORKING… aus.

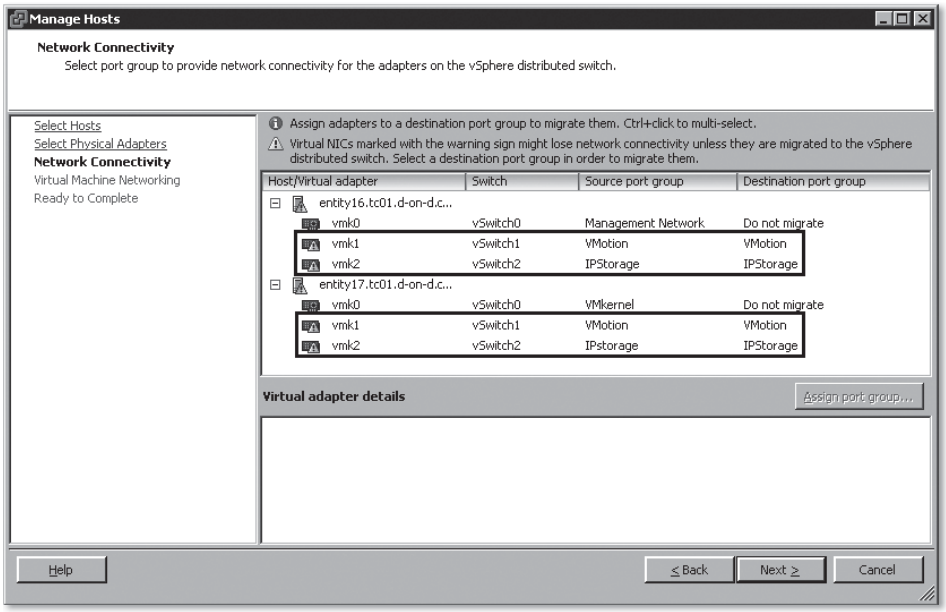


Abbildung 8.66 »vmk1« und »vmk2«

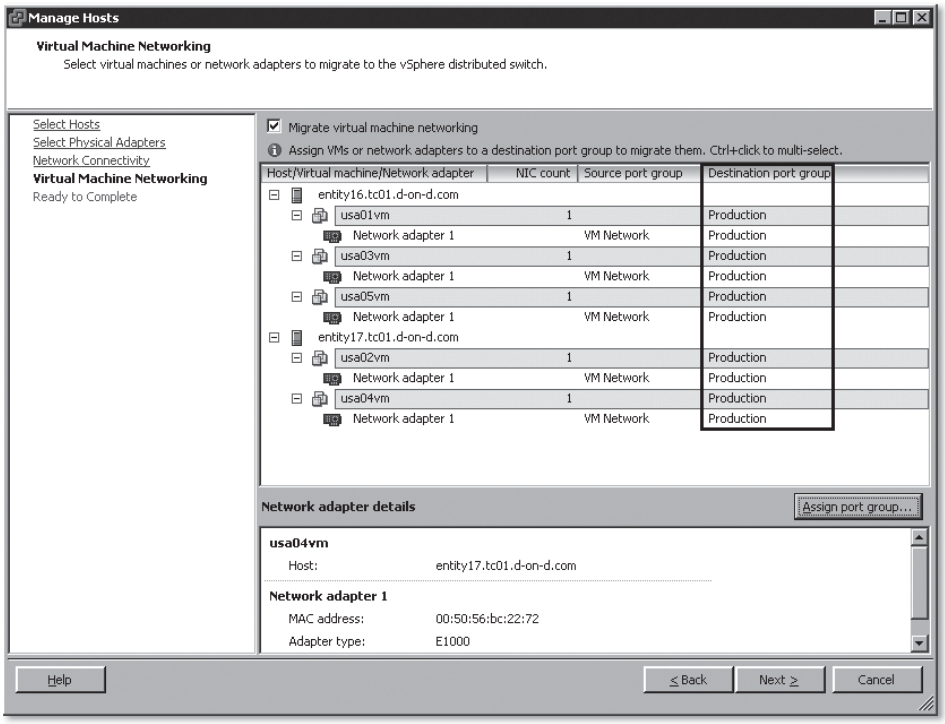


Abbildung 8.67 Alle VMs werden auf die Portgruppe »Production« migriert.

Die abschließende Ansicht nennt sich Ready to Complete und zeigt, wie das endgültige Konstrukt aussehen wird.

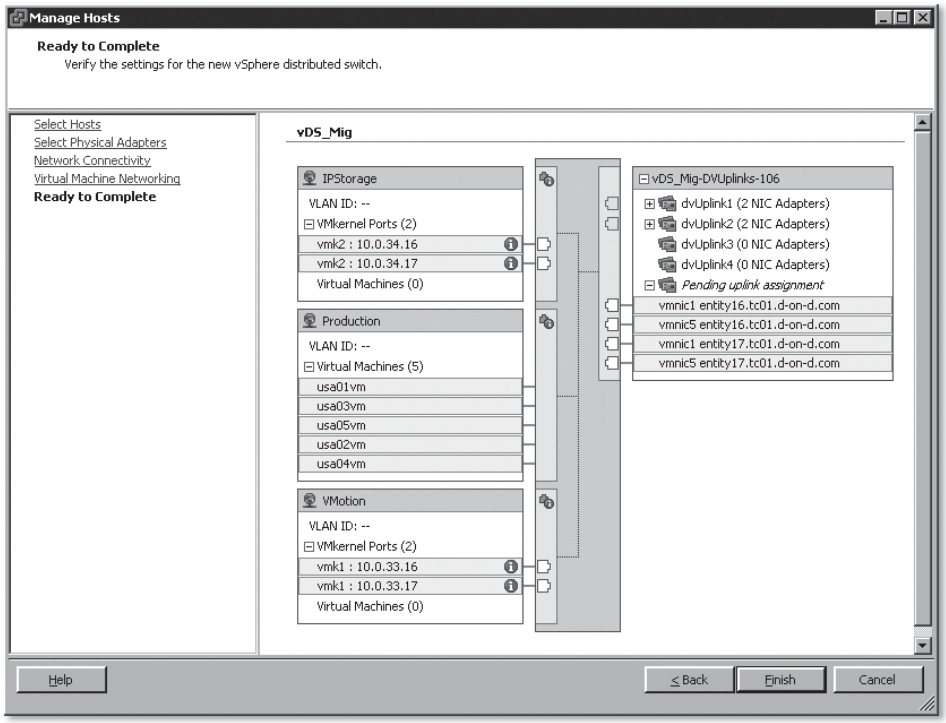


Abbildung 8.68 Die Zielansicht der Migration

Starten Sie die Migration in der Ansicht Ready to Complete durch Betätigen der Schaltfläche Finish, sehen Sie unter Recent Tasks im vSphere-Client den Fortschritt. In unserem Beispiel war die Migration in ca. 30 Sekunden abgeschlossen. Ich habe während der Migration diverse Ziele mittels `ping` überprüft. Möglicherweise geht ein Paket verloren, wie in Abbildung 8.69 zu sehen. Dies ist in der Praxis kaum problematisch, wenn Sie die Migration zudem in Randzeiten verlegen.

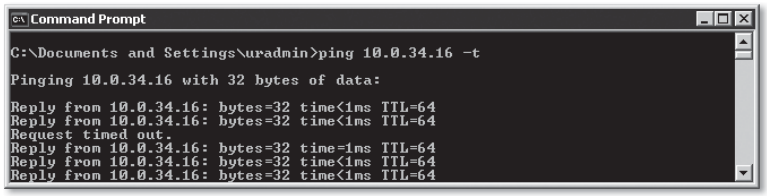


Abbildung 8.69 Ping auf den »IPStorage«-VMkernel während der Migration

Eine Überprüfung der abgeschlossenen Migration (siehe Abbildung 8.70) ergibt, dass alles wie geplant stattgefunden hat und somit der Hauptteil der Migration abgeschlossen ist.

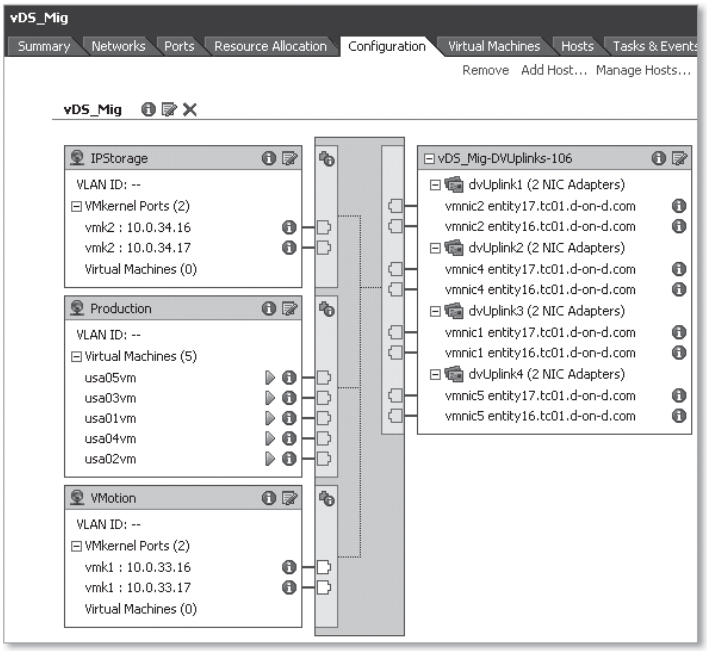


Abbildung 8.70 Das Resultat der Migration

Damit wir unsere ursprünglich definierten Ziele erreichen, müssen wir noch die Verkehrsmuster modellieren. Zusätzlich können wir die nicht mehr benötigten vSS auf den Hosts löschen. Diese Arbeit müssen Sie pro Host vornehmen (siehe Abbildung 8.71) und können Sie leider nicht zentral über einen Assistenten im vCenter erledigen.

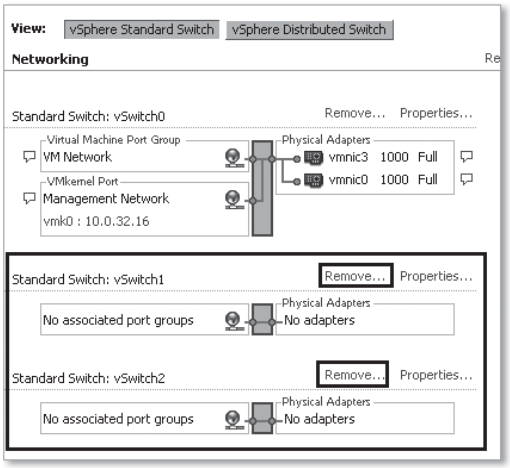


Abbildung 8.71 Löschen der nicht mehr benötigten vSS

Die Modellierung des Verkehrs über verschiedene Netzwerkadapter erfolgt pro Portgruppe.

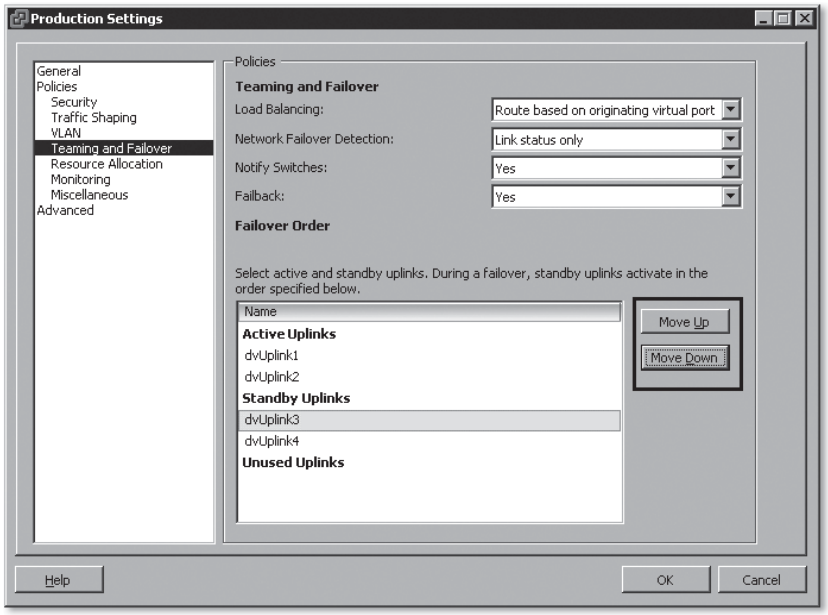


Abbildung 8.72 Modellierung der Verkehrsmuster auf einer Portgruppe

8.7.1 Was wäre, wenn etwas falsch migriert wurde?

Dies ist in den meisten Fällen kein gravierendes Problem, denn die Migrationstools arbeiten in beide Richtungen. Etwas mühsam wird es natürlich, wenn viele virtuelle Maschinen von einer Portgruppe auf eine falsche Portgruppe, an der schon viele korrekt verbundene virtuelle Maschinen existieren, migriert wurden. In diesem Fall bleibt Ihnen nichts anderes übrig, als die falsch migrierten Maschinen zu identifizieren und zurückzuverschieben.

8.7.2 Was wäre, wenn das Management-Netzwerk verlorenginge?

Es kann bei Fehlüberlegungen passieren, dass ein Management-Netzwerk ins Leere migriert wird. In diesem Fall folgen Sie den Anweisungen in Abschnitt 8.8, »Wiederherstellung des Management-Netzwerks«.

8.8 Wiederherstellung des Management-Netzwerks

In Situationen, in denen eine Fehlkonfiguration dazu führt, dass die Netzwerkverbindung zum ESXi-Host nicht mehr möglich ist, müssen Sie direkt an der Konsole des Servers arbeiten, um die Verbindung wiederherzustellen. Diese Situationen können sehr einfach entstehen, wenn zum Beispiel eine Migration zu vDS ins Leere erfolgt, d. h. zum Beispiel an einen vDS

ohne Uplinks oder wenn an den Uplink-Adaptern des Standard-vSS gearbeitet wird und auf der Seite des physischen Switch falsche Access-Ports eingerichtet wurden.

Es gibt zwei Wege für eine Wiederherstellung über die Konsole: Der eine Weg führt ausschließlich über das Menü des ESXi-Hosts, der andere über das CLI in der Konsole. Nachfolgend stellen wir den Weg über das Menü des ESXi-Servers dar.

***Ausgangslage*:**
Nach Konfigurationen an den virtuellen Switches eines ESXi-Hosts ist dieser nicht mehr ansprechbar. Es ist keine Verbindung zum Host mehr möglich.

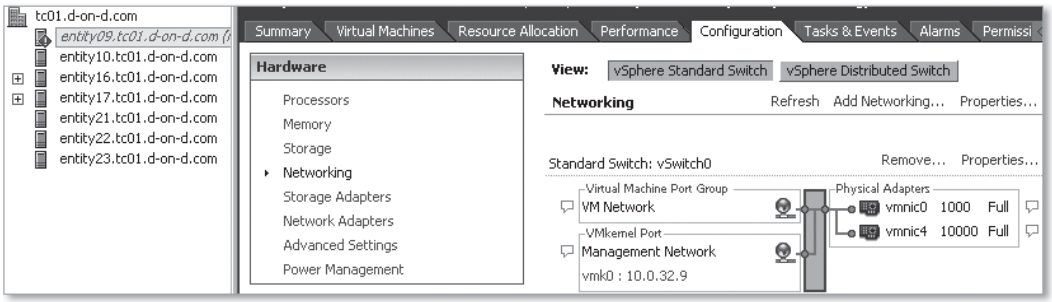


Abbildung 8.73 ESXi-Host nicht mehr ansprechbar

In Abbildung 8.73 erkennen Sie, dass sich der Host im Status »disconnected« befindet.

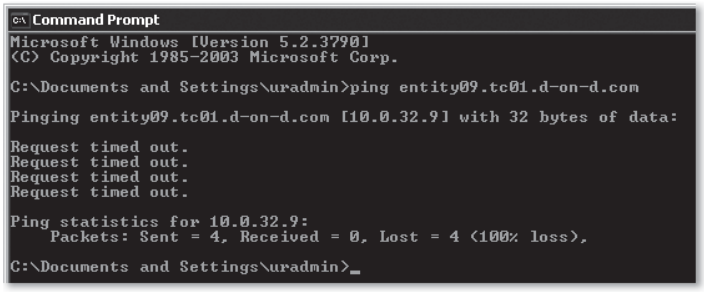


Abbildung 8.74 Host mit »ping« nicht erreichbar

Ein Verwenden von `ping` zeigt, dass der Host nicht erreichbar ist, siehe Abbildung 8.74. Als nächster Schritt erfolgt die Anmeldung direkt an der Konsole des Servers. Ist diese Anmeldung erfolgreich, ist klar, dass der ESXi-Host grundsätzlich läuft.

Abbildung 8.75 zeigt die möglichen Auswahlpunkte. In Frage kommen Configure Management Network und Restore Network Settings. Wählen Sie Configure Management Network.

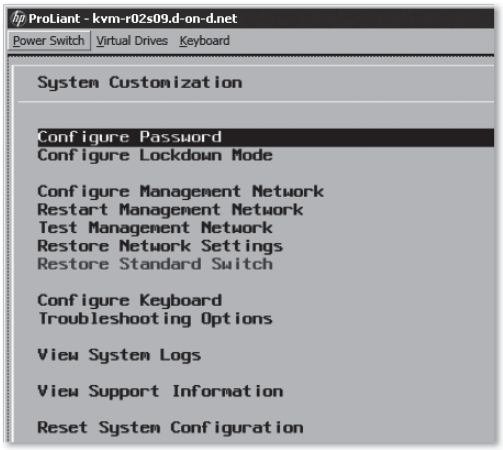


Abbildung 8.75 Menüauswahl in der Konsole des ESXi-Hosts

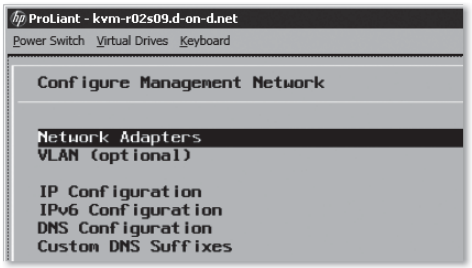


Abbildung 8.76 Menü »Configure Management Network«

In der Ansicht des Management Networks (Abbildung 8.76) wählen Sie Network Adapters.

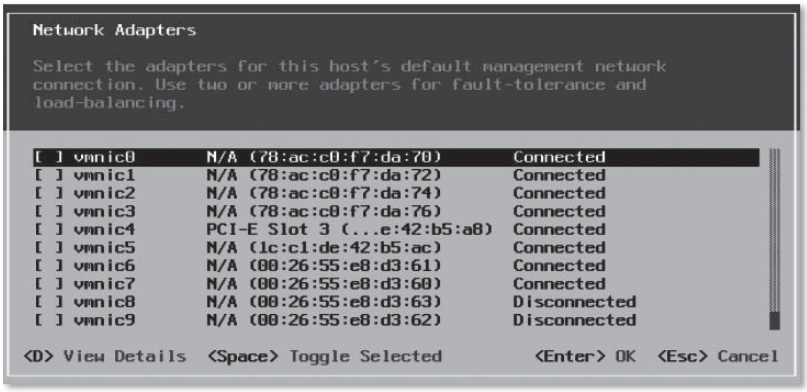


Abbildung 8.77 Menü »Network Adapters«

In der Ansicht Network Adapters (Abbildung 8.77) sehen Sie alle vorhandenen Netzwerkadapter und deren Status. Es fällt auf, dass kein einziger Adapter mehr an dem vSS für die

Verwaltung vorhanden ist. Die Korrektur ist sehr einfach: Markieren Sie den gewünschten Adapter, und wählen Sie ihn mit der Leertaste aus. Mit der ↵-Taste bestätigen Sie die Auswahl und verlassen das NETWORK ADAPTERS-Menü. Mit der Esc-Taste schließen Sie das CONFIGURE MANAGEMENT NETWORK-Menü. Es erscheint die Dialogbox aus Abbildung 8.78.

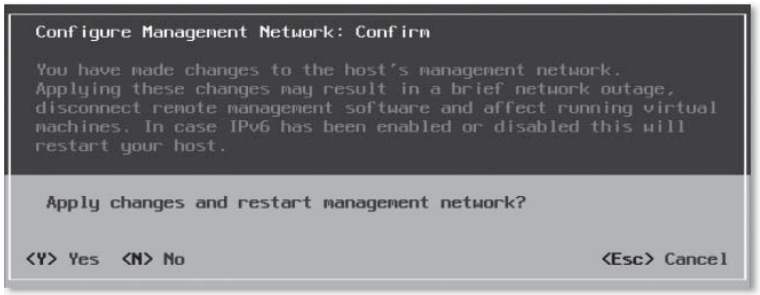


Abbildung 8.78 Bestätigung der Konfigurationsänderungen

Bestätigen Sie die Konfigurationsänderungen nun mit der Taste Y.

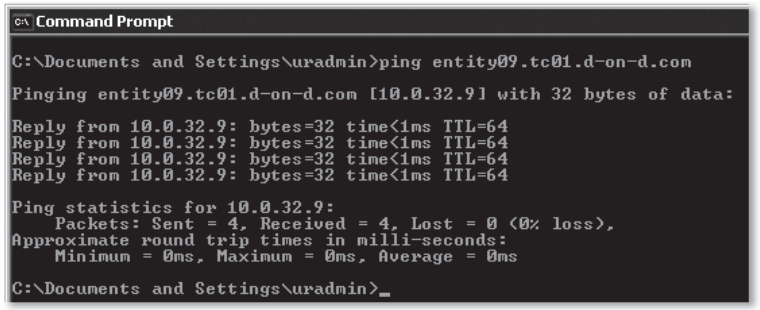


Abbildung 8.79 Host mit »ping« wieder erreichbar

Setzen Sie nun ein `ping` ab (Abbildung 8.79), sehen Sie, dass der Host im Netzwerk wieder zur Verfügung steht.

8.9 Architekturbeispiele

Die folgenden Abschnitte wurden von Sebastian Wischer und Dennis Zimmer erstellt.

8.9.1 Empfehlungen und Best Practice

Für die Umsetzung von Netzwerkkonzepten in der Praxis gibt es einige Empfehlungen und Anmerkungen. Diese sollen helfen, eine hohe Verfügbarkeit sowie ausreichende Performance und Sicherheit zu gewährleisten. Da die Anforderungen und Gegebenheiten aber sehr unterschiedlich sein können, ist es sehr schwer, einen goldenen Regelsatz zu entwerfen. Die folgen-

den Empfehlungen und Anmerkungen sind also immer für die eigene Umgebung entsprechend einzuschätzen und eventuell anzupassen.

Verwaltungsnetz – Management-Netzwerk

Für die Verbindung des Management-Netzwerks sind vor allem Verfügbarkeit und Sicherheit entscheidend. Die Performance spielt im Verhältnis zu Netzen für die Storage- oder VM-Anbindung eher eine geringere Rolle. Im Schnitt hat das Management-Netzwerk eine Auslastung von ca. 100 Mbit/s. Dabei ist zu bedenken, dass dieser Durchschnitt sich aus sehr hohen Lastspitzen, aber auch längeren Zeitfenstern mit geringer Last errechnet. Eine Kombination mit anderen Netzen, ist zu überlegen, aber generell nicht abzulehnen.

Aus Sicherheitsgründen sollte das Management-Netzwerk in einem separaten Verwaltungsnetzwerk eingebunden sein. Das kann bedeuten: physische Trennung oder Segmentierung mit Hilfe von VLANs. Letztere Lösung bietet dabei eine viel höhere Flexibilität im Design. Es sollte sichergestellt sein, dass die Service Console vom vCenter und von den anderen ESX-Hosts im Cluster erreichbar ist. Der Zugriff sollte aber nur möglich sein für Administratoren oder von Systemen aus, die den direkten Zugriff auch wirklich benötigen.

Die Verfügbarkeit des Management-Netzwerks ist vor allem beim Einsatz eines VMware-HA-Clusters wichtig. Sofern die Service Console eines ESX-Hosts nicht von den anderen Hosts erreicht werden kann, wird von einer Isolation oder gar einem Ausfall ausgegangen. Daher sollten Sie beim Design überlegen, ob bei Ausfall eines Netzwerkports im Server oder bei Ausfall eines Switches die Verfügbarkeit gegeben ist. Sofern das vCenter das Managment-Netzwerk eines ESX-Hosts nicht mehr erreicht, wird der Server als »disconnected« angezeigt. Die Verfügbarkeit der virtuellen Maschinen muss damit aber nicht direkt in Bezug stehen.

Das Management-Netzwerk sollten Sie also immer in einem möglichst kleinen, abgeschlossenen Verwaltungsnetzwerk einbinden. Eine Verfügbarkeit muss auch bei Ausfall eines Netzwerkadapters oder Switches gegeben sein. Eine Gigabit-Verbindung ist aus Sicht der Performance definitiv ausreichend.

NFS-Netz – VMkernel

Für die Anbindung eines NFS-Datastores ist sicher das größte Thema die Performance gefolgt von der Verfügbarkeit und Sicherheit. Sofern die Verbindung zum NFS-Datastore nicht den Durchsatz ermöglicht, den die virtuellen Maschinen zum Lesen und Schreiben auf ihren virtuellen Disks benötigen, sind direkt mehrere Systeme betroffen. In vielen Umgebungen reicht daher eine einfache Gigabit-Verbindung nicht aus. Es müssen mehrere Netzwerkports im ESXi-Host aktiv verwendet werden. Das bedeutet: Abhängig von den externen Switches müssen Sie ein Teaming mit entsprechender Paketverteilung einrichten. Sinnvoll ist es, auch eine Skalierbarkeit nach oben einzuplanen. Dies gewährleisten Sie durch freibleibende Netzwerkports im Server oder Switch.

Im Server lässt sich natürlich auch nachträglich ein freier Slot mit einem zusätzlichen Netzwerkadapter bestücken. vMotion ermöglicht dies zudem, ohne die Verfügbarkeit der virtuellen Maschinen zu beeinflussen. Durch das Zusammenfassen von Ports erreichen Sie auch gleich eine ausreichende Verfügbarkeit der Netzwerkports. Achten Sie jedoch darauf, Ports auf unterschiedlichen Adaptern zu kombinieren, sonst würde der Ausfall einer einzelnen Karte eine Trennung der Netze bedeuten. Sofern die externen Switches keinen Etherchannel über mehrere getrennte Systeme unterstützen, müssen Sie zusätzlich mit mindestens einem Standby-Port arbeiten.

Für ausreichend Sicherheit können Sie den NFS-Export nur für bestimmte Server freigeben. Zudem ist der Einsatz von VLANs wieder eine gute Trennung des NFS-Netzes von zum Beispiel dem Verwaltungsnetzwerk. Natürlich können Sie auch auf physischer Ebene trennen, der Einsatz separater Switches und Leitungen ist aber immer mit Kosten verbunden, nicht nur wegen des erhöhten Hardwarebedarfs, sondern auch aufgrund des Verwaltungsaufwandes.

Für ein NFS-Netz sollten Sie demnach von Beginn an für eine gute Bandbreite mit Erweiterungsmöglichkeit sorgen. Die Verfügbarkeit gewährleisten Sie dadurch direkt mit, Sie müssen sie aber unbedingt überprüfen. Da ein Storage-Netz meist separiert ist – gleich ob physisch oder per VLAN –, können Sie dadurch eine grundlegende Sicherheit schaffen. Optional erweitern Sie dies noch auf dem Storage-System durch gezielte Freigaben.

iSCSI-Netz – VMkernel

Für ein iSCSI-Netz gilt ziemlich das Gleiche in Bezug auf Performance, Verfügbarkeit und Sicherheit. Ein wesentlicher Unterschied besteht jedoch: Sie können nicht nur Ports durch ein Teaming zusammenpassen, sondern auch Multipathing einsetzen. Erstellen Sie zum Beispiel zwei VMkernel-Ports für die iSCSI-Anbindung in unterschiedlichen Netzen auf dem ESXi-Host und Storage-System, können Sie die Last mit Hilfe von Multipathing wie bei einer Fibre-Channel-Anbindung verteilen.

Die iSCSI-LUN wird einmal über das erste VMkernel-Netz in Netz A erkannt, ein weiteres Mal über den zweiten VMkernel-Port in Netz B. Dadurch können Sie zum Beispiel auf Etherchannels komplett verzichten. Selbst bei zwei getrennten physischen Switches, die keine systemübergreifenden Etherchannels unterstützen, erreichen Sie so aktiv über beide Switches mit Hilfe des Round-Robin-Verfahrens eine Lastverteilung.

Für die Anbindung von iSCSI- und NFS-Datastores auf einem NetApp-System empfiehlt sich ein Blick in den Technical Report 3749; dieser enthält eine Menge Tipps und Tricks für die Optimierung des Storage-Netzwerkes: *http://media.netapp.com/documents/tr-3749.pdf*

Für iSCSI-Netze müssen Sie eine gute Performance und Verfügbarkeit gewährleisten! Eine Erhöhung der Sicherheit erreichen Sie durch Separieren des Netzes und gezielte Zugriffssteuerung auf dem Storage-System. Der wesentliche Unterschied zum NFS-Netz ist: Sie haben mehr Möglichkeiten beim Zusammenfassen von Ports durch Multipathing-Technologie.

vMotion-Netzwerk – VMkernel

Bei vMotion-Netzwerken gilt als Erstes immer noch die Empfehlung: ein dediziertes Gigabit-Netzwerk. Fällt ein vMotion-Netz einmal aus, bedeutet das nicht einen direkten Ausfall der virtuellen Maschinen. Es nimmt Ihnen aber die Flexibilität, virtuelle Maschinen zu verschieben, um zum Beispiel eine defekte Netzwerkkarte auszutauschen.

Die Last auf einem vMotion-Netz ist vor allem hoch, wenn Sie viele virtuelle Maschinen verschieben müssen, zum Beispiel während eines Patch-Vorganges mit Hilfe des Update Managers. Wie bei der Service Console gibt es also Spitzenzeiten mit hohen Anforderungen und Phasen, in denen kaum Last erzeugt wird.

Eine gute Konfiguration für ein vMotion-Netzwerk wären dedizierte Ports pro ESXi-Host, die vielleicht auf einen dedizierten Unmanaged Switch zusammengeführt werden. Dieses wäre eine Möglichkeit, nicht zu kostenintensiv ein dediziertes physisches Netz aufzubauen. Natürlich erreichen Sie eine Trennung auch über VLANs, um nicht in einen zusätzlichen Switch investieren zu müssen.

Ein Ausbau auf mehrere Ports pro ESX oder gar 10-Gigabit-Ethernet beschleunigt den vMotion-Prozess erheblich! Die Verfügbarkeit wird durch einen weiteren Port erhöht, ist aber kein Muss. Sofern es sich um ein dediziertes Netz zwischen den ESXi-Hosts oder ein definitiv abgeschottetes Netzwerk handelt, ist für ausreichend Sicherheit gesorgt!

Bei vMotion-Netzen ist in erster Linie immer zu gewährleisten, dass das Netz exklusiv für vMotion und nur für die notwendigen ESX-Hosts zugänglich ist. Dadurch ist eine ausreichende Sicherheit gleich mit gegeben, und die Verfügbarkeit lässt sich durch mehr Ports und Switches erhöhen. Letzteres bietet damit auch gleich mehr Performance, ausgenommen bei Active/Standby-Konfigurationen.

Fault Tolerance – VMkernel

Für Fault Tolerance ist die Mindestanforderung ein Gigabit-Netzwerk, VMware empfiehlt sogar ein 10-Gigabit-Netzwerk. Letzteres gilt sicher nur dann, wenn auch viele virtuelle Maschinen über Fault Tolerance abgesichert werden sollen. Die Belastung dieses Netzwerktyps hängt stark von der Auslastung der virtuellen Maschinen und, wie zuvor erwähnt, von der Anzahl abgesicherter Systeme ab. Im Gegensatz zu vMotion-Netzen sind enorme Lastspitzen und lange Phasen mit wenig Last eher die Ausnahme.

Für den Performance-Aspekt bietet es sich ebenfalls an, zukunftsorientiert zu denken. Fault Tolerance ist eine Funktion mit ein paar Einschränkungen, die sich aber hoffentlich in Zukunft verringern. Damit steigt voraussichtlich auch die Anzahl der abgesicherten virtuellen Maschinen über diese Funktion. Freie Ports und Steckplätze für eine optionale Erweiterung und damit Erhöhung des Durchsatzes sind auch hier sicher interessant.

Im Gegensatz zu vMotion ist die Verfügbarkeit dieses Netzwerktyps jedoch kritischer. Fällt ein Fault-Tolerance-Netzwerk aus, ist kein Schutz für die virtuellen Maschinen mehr gegeben.

Eine Trennung des Netzwerkes von den anderen Netzen ist auch hier wieder sehr sinnvoll. Dies erhöht zudem die Sicherheit und reduziert die Systeme in diesem Netzwerk auf die Anzahl der ESXi-Hosts. Ein Fault-Tolerance-Netzwerk stellt eventuell sehr hohe Anforderungen an die Performance, die unbedingt erfüllt werden sollten, in manchen Fällen sogar bis zu 10 Gigabit – eine Skalierbarkeit sollte möglich sein! Die Verfügbarkeit sollten Sie dabei nicht außer Acht lassen, und auch im Fehlerfall muss ausreichend Performance gegeben sein. Ansonsten gewährleistet Fault Tolerance keinen Schutz für die virtuellen Maschinen. Sicherheitstechnisch reduziert sich das Netz auch hier auf die ESXi-Hosts selbst, und es sollte in der Regel ein getrenntes Netz sein.

Virtual-Machine-Netzwerke

Netzwerke virtueller Maschinen sind sehr variabel, hier müssen Sie also wirklich genau auf die eigene Umgebung und damit verbundene Anforderungen schauen. Handelt es sich um ein Produktivnetz mit hohen Durchsätzen und großen Anforderungen an Verfügbarkeit und Sicherheit? Oder ist es ein Testnetzwerk, das vielleicht auch einmal ausfallen darf und nicht die durchgehend hohen Durchsätze benötigt? Genauso kann es ein Netzwerk sein, über das Anwender sich auf virtuelle Desktops verbinden.

Grundsätzlich sollten Sie wie zuvor darauf schauen, welche Anforderungen es in Richtung Performance, Verfügbarkeit und Sicherheit gibt. In den meisten Fällen wird mit mindestens zwei Ports gearbeitet, um Ausfälle abzufangen. Zur Sicherheit sollten Sie darauf achten, dass unterschiedliche Netze mit Hilfe von VLANs voneinander abgeschottet sind. Es gelten hier schon fast die gleichen Regeln wie bei der Anbindung physischer Server.

Eine häufige Frage während des Designs ist die Kombination unterschiedlicher Netze auf einem vSwitch. Dies lässt sich nach den Anforderungen von Performance und Verfügbarkeit gut einstufen.

Beim Konzeptionieren von Lösungen für Netze von virtuellen Maschinen sollten Sie immer möglichst viele Informationen zum Verhalten der Netze sammeln. Bei mehreren Netzen sollten Sie über die Kombination lastintensiver mit weniger lastintensiven Netzen nachdenken. Außerdem sollten Sie in Betracht ziehen, einen vSwitch mit mehreren aktiven Ports zu erstellen. Die aktiven Ports können dann auf der Portgruppeneben für jede Portgruppe individuell in den Modus »aktiv«, »Standby« oder »nicht zu verwenden« umgeschaltet werden. So kann eine erste Portgruppe Uplink 1 und 2 aktiv, Uplink 3 als Standby verwenden. Die zweite Portgruppe könnte Uplink 3 und 4 aktiv, Uplink 2 jedoch als Standby benutzen. Dadurch lässt sich noch genauer die Verteilung der Netzlast der einzelnen Portgruppen auf einem gemeinsamen vSwitch konfigurieren.

Server-Management-Karten

Die Vernetzung von Server-Management-Controllern (iLOM, iRMC …) kann auch, gerade beim Einsatz von DPM, für das Netzwerkdesign des ESX-Hosts interessant werden. Für die

Anbindung der Server-Verwaltungsschnittstellen ist keine enorm performante Verbindung notwendig. Daher können Sie diesen Aspekt getrost vernachlässigen. Verfügbarkeit ist gerade im Fehlerfall sehr wichtig. Fällt zum Beispiel die Verbindung zur Service Console aus, kann dies die letzte Möglichkeit sein, irgendwie den Server zum Beispiel per Remote-KVM (Keyboard Video Mouse) zu verwalten oder einfach, um einen Server-Status zu bekommen: eingeschaltet oder ausgeschaltet?

Da aber über diese Verbindung unter anderem Server ein- und ausgeschaltet werden können, sollte die Sicherheit ein große Rolle spielen. Kurzum: Es gilt das Gleiche wie für das Management-Netzwerk. Es handelt sich um eine Verwaltungsschnittstelle, die leider häufig in Konzepten vergessen wird!

8.9.2 Beispiel auf Basis verfügbarer Ports im Server

Es ist nicht einfach, eine optimale Konfiguration seines Netzwerkes zu finden. Die folgenden drei Beispiele sollen Ihnen helfen, eine Vorstellung davon zu bekommen, wie eine mögliche Konfiguration aussehen könnte. Für die eigene Umgebung sollten Sie aber zwingend zunächst die Bedingungen und den Bedarf ermitteln, bevor Sie eines dieser Beispiele übernehmen. Vor allem sind in den meisten Fällen Anpassungen nötig und gegebenenfalls sogar eine bessere Konfiguration.

Für die Beispiele sind wir davon ausgegangen, dass VLANs eingesetzt werden. Geben wir in den folgenden Beispielen für eine Portgruppe keinen Uplink mit »A« für »aktiv« oder »S« für »Standby« an, wird dieser nicht für die Portgruppe verwendet und muss also auch als nicht zu verwenden in der Portgruppe konfiguriert werden. Grundlegend gilt natürlich: Je mehr Ports zur Verfügung stehen, umso mehr Konfigurationen sind möglich, und Sie können wesentlich besser optimieren.

Wir haben auch immer nur einen Standby-Adapter konfiguriert, da bei Ausfall eines Ports immer nur ein Standby-Adapter aktiviert wird. Es gibt keine Möglichkeit, Uplink-Portgruppen zu definieren. Haben Sie also zwei aktive Uplinks auf Switch0 und zwei Standby-Adapter auf Switch1 verbunden, kann es bei Ausfall nur eines aktiven Adapters dazu kommen, dass die Performance sinkt, da ein Etherchannel/LACP auf Switch1 und einer auf Switch0 konfiguriert wurde. Der ESX-Server wird daher nicht auch noch den zweiten Uplink umschalten. Fällt auch der zweite Link aus oder der komplette Switch, würden beide Standby-Uplinks aktiviert und komplett auf den anderen Switch umgeschaltet.

8.9.3 ESX-Hosts mit zwei Netzwerkports

Die wohl kleinste sinnvolle Konfiguration sind zwei Ports in einem ESX-Server. Theoretisch könnten Sie auch mit nur einem Port arbeiten, dabei dürfen Sie aber keine Verfügbarkeit oder hohe Performance erwarten.

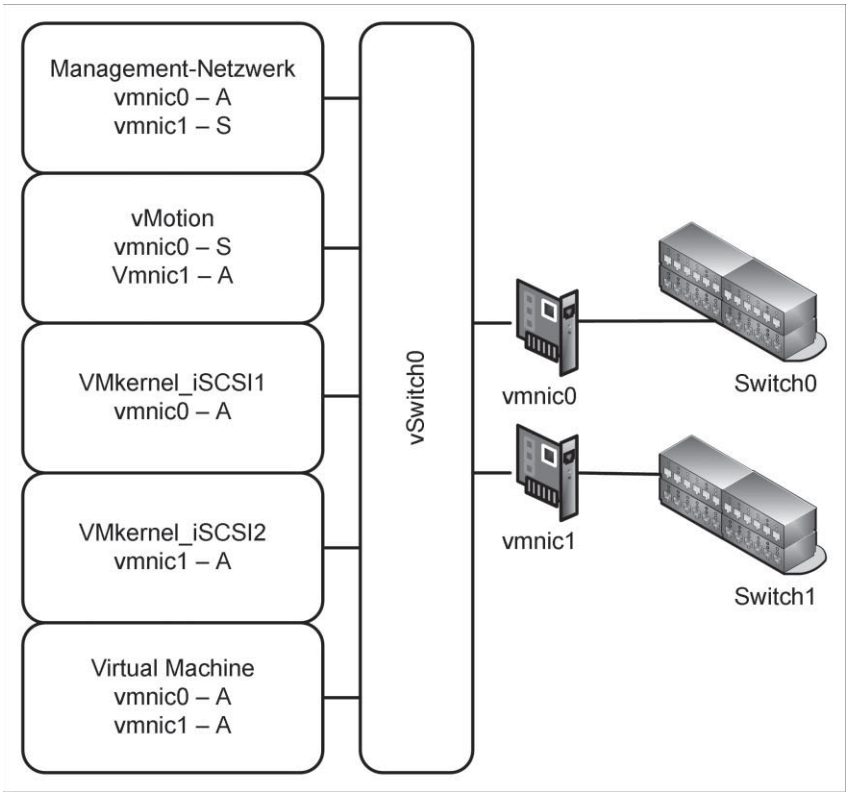


Abbildung 8.80 Beispielkonfiguration mit zwei Uplink-Ports

Bei der Aufteilung der Ports an die unterschiedlichen Portgruppen wurde versucht, eine möglichst gleiche Auslastung der Ports bei ausreichender Verfügbarkeit zu erhalten. Im normalen Zustand werden über vmnic1 die Service Console, »VMkernel_iSCSI1« und ein Teil des Virtual-Machine-Netzwerkes kommunizieren, über vmnic2 der »VMkernel_iSCSI2«, vMotion und der andere Teil des Virtual-Machine-Netzwerkes.

Die Aufteilung des Virtual-Machine-Netzwerkes auf beide Uplinks ist nur möglich, sofern ein switchübergreifender Etherchannel unterstützt wird oder mit einer Paketverteilung auf Basis der Source-MAC oder des vSwitch-Ports eingerichtet ist.

Für die Anbindung eines iSCSI-Datastores wurden zwei VMkernel-Netze zum Storage gewählt, eine Verteilung der Last erfolgt durch das Multipathing des ESXi-Hosts. Dabei wurde für jeden VMkernel ein anderer Uplink festgelegt. Warum iSCSI als Beispiel? Bei einer Zwei-Port-Konfiguration handelt es sich meist um eine günstige Lösung, und sie ist daher meist in Verbindung mit iSCSI-Storage zu finden. Management-Netzwerk und vMotion sind auf unterschiedlichen Uplinks, der zweite Uplink ist aber jeweils als Standby-Adapter für den Fehlerfall konfiguriert.

8.9.4 ESX-Hosts mit vier Netzwerkports

Gegenüber dem Beispiel mit zwei Ports arbeiten wir in diesem Beispiel mit NFS. Für NFS müssen Sie im Netzwerk immer für die Performance und Verfügbarkeit sorgen. Sie können kein Host-Multipathing verwenden.

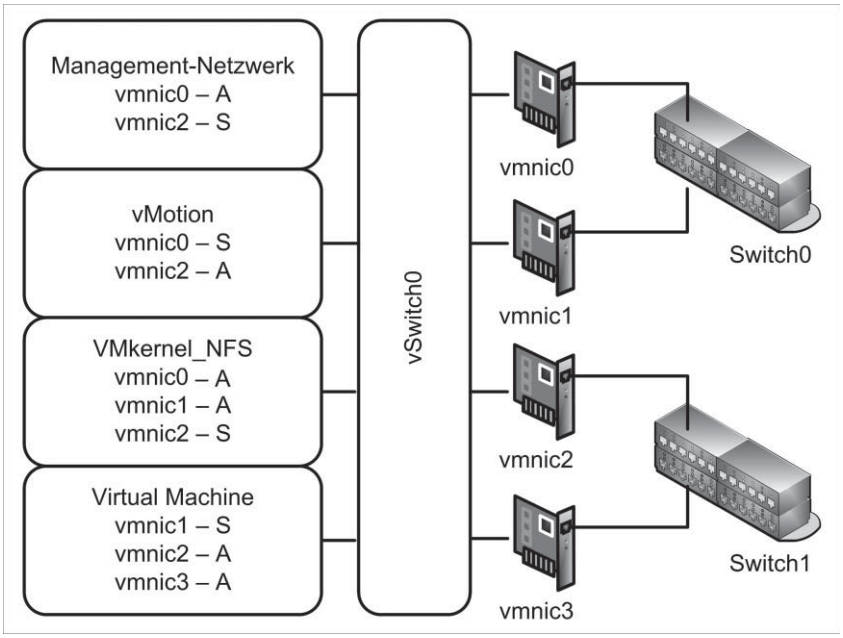


Abbildung 8.81 Beispielkonfiguration mit vier Uplink-Ports

Aus Sicht der Uplinks sind vmnic0 und vmnic1 auf Switch0 verbunden. Über diese Ports wird der VMkernel verbunden. Um einen Switch-Ausfall abzufangen, konfigurieren wir noch vmnic2 als Standby.

Das Management-Netzwerk ist mit vmnic0 verbunden und für den Ausfall des Ports oder Switches zusätzlich über vmnic2 als Standby-Adapter abgesichert. Über Switch1 kommunizieren vmnic2 und vmnic3. Das Virtual-Machine-Netzwerk verwendet diese beiden Ports aktiv und ist über vmnic1 gegen den Ausfall von Switch1 abgesichert. Das vMotion-Netzwerk ist im Normalzustand über vmnic2 verbunden und bei Ausfall des Ports oder Switches mit vmnic0 als Standby-Adapter konfiguriert.

Für Netzwerke mit mehr als einem aktiven Port müssen Sie eine Paketverteilung einrichten, die wie bei der Zwei-Port-Konfiguration von den externen Switches abhängig ist. Bei einem switchübergreifenden Etherchannel müssen Sie IP-Hash oder LACP einstellen oder entweder MAC-Source oder Originating-Port-ID als Paketverteilung auswählen.

8.9.5 ESX-Hosts mit sechs Netzwerkports

Für die Sechs-Port-Konfiguration haben wir das vorherige Beispiel um wesentliche Best-Practice-Empfehlungen erweitert. So stehen pro Netzwerk im Normalfall dedizierte Ports zur Verfügung. Bei Ausfall eines Ports oder Switches kann es aber auch wieder dazu kommen, dass zwei Netzwerke über einen Port verbunden sind. Bei der Einstellung der Paketverteilung gilt das Gleiche wie in den beiden Beispielen zuvor.

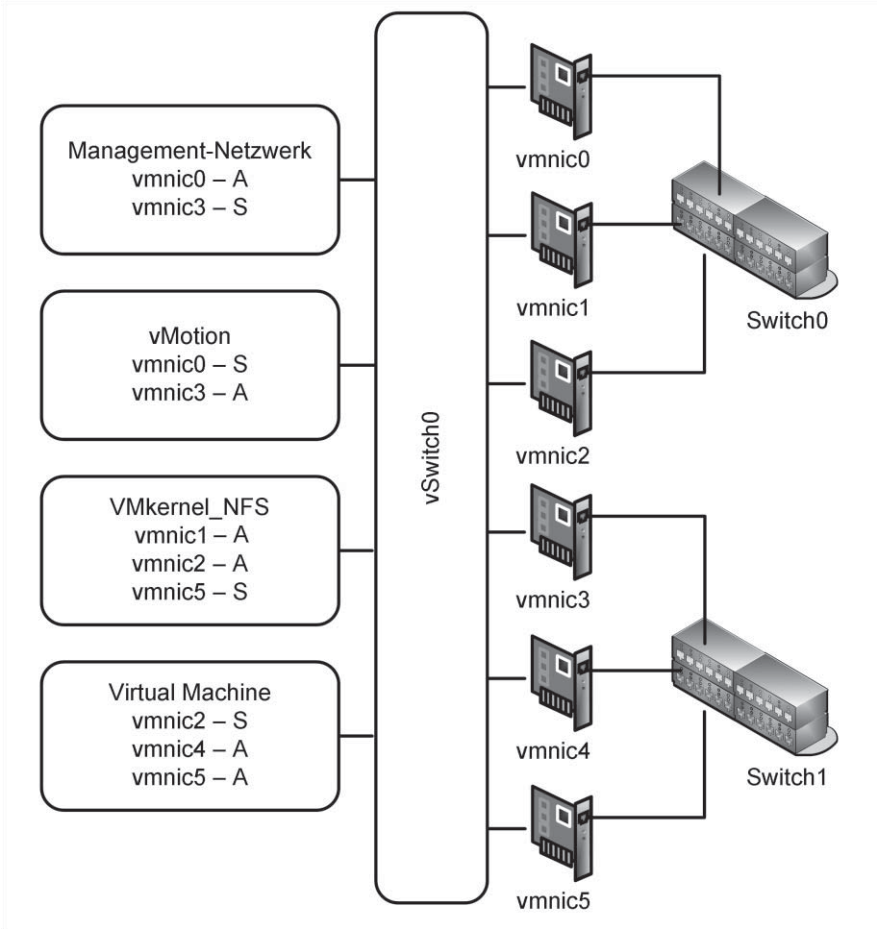


Abbildung 8.82 Beispielkonfiguration mit sechs Uplink-Ports

Natürlich ist es auch möglich, eine Konfiguration mit mehr als einem vSwitch zu erstellen. Die bisherigen Empfehlungen gelten dabei genauso. Eine Konfiguration mit mehr als einem vSwitch kann helfen, klarer abzugrenzen und Konfigurationen nicht zu komplex werden zu lassen. In diesem Beispiel wurden so das VMkernel- und das Virtual-Machine-Netzwerk getrennt. Der Netzwerkverkehr für NFS-Datastores wird über vmnic1 und vmnic2 verteilt, die beide an Switch0 verbunden sind.

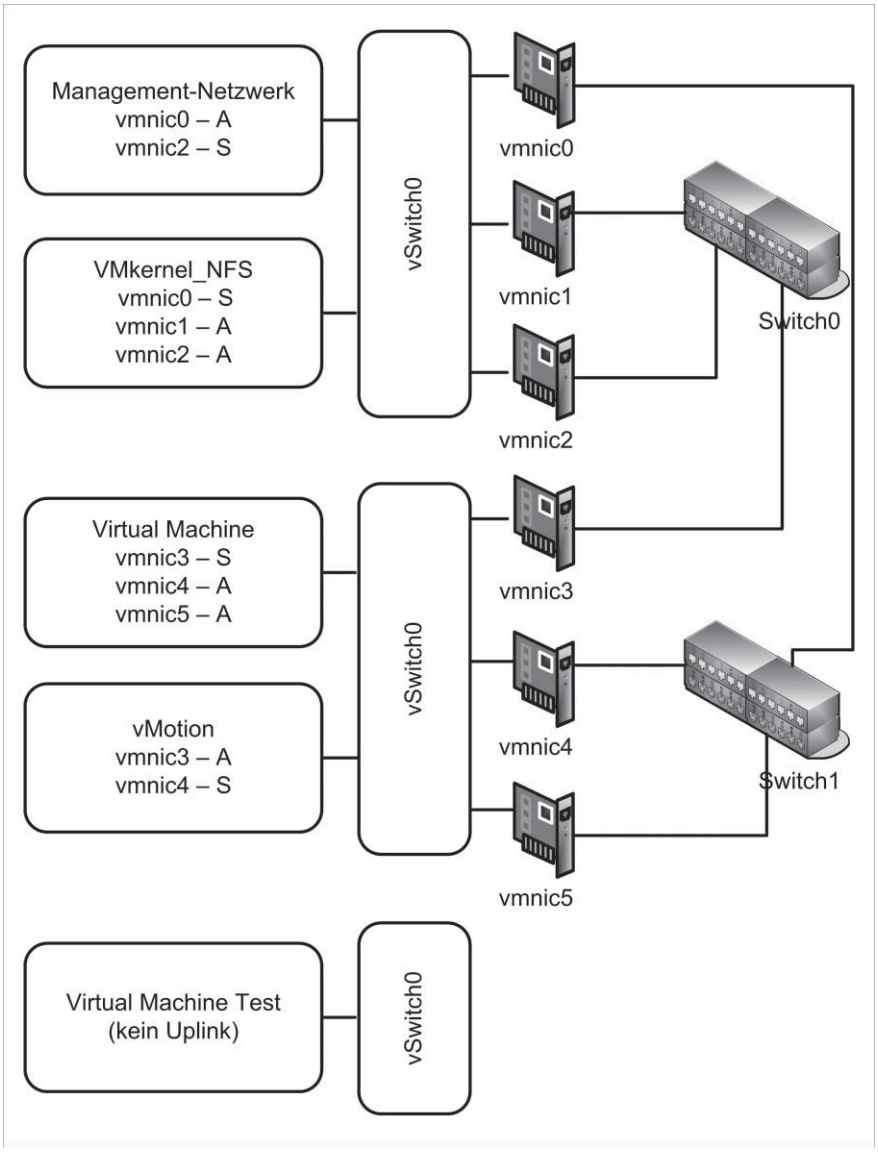


Abbildung 8.83 Weitere Beispielkonfiguration mit sechs Uplink-Ports

Die virtuellen Maschinen sind im Normalfall über vmnic4 und vmnic5 angebunden. Sollte ein Link oder Switch ausfallen, können beide Portgruppen auf einen Standby-Adapter zurückgreifen, der mit dem jeweils anderen physischen Switch verbunden ist. Damit diese Konfiguration bei Ausfall nur eines Ports ordnungsgemäß funktioniert, müssen Sie entweder mit der Paketverteilung auf Basis der Source-MAC-Address oder der Originating-Port-ID arbeiten. Alternativ, sofern die physischen Switches einen übergreifenden Channel unterstützen, nutzen Sie IP-Hash.

Für das Management-Netzwerk wurde wieder vmnic0 im Normalfall exklusiv reserviert. vMotion auf dem zweiten vSwitch arbeitet über vmnic3. Beiden Portgruppen haben wir wieder einen Standby-Port zugewiesen. Der Ausfall eines Ports oder Switches ist damit berücksichtigt. Für eventuelle Tests haben wir einen internen vSwitch für virtuelle Maschinen eingerichtet. Manchmal wird ein solcher vSwitch ohne externen Uplink auch für den Aufbau einer DMZ-Umgebung genutzt. Wichtig ist aber, dass Sie die Einschränkungen der angebundenen virtuellen Maschinen für vMotion berücksichtigen.

VMware vSphere 5 bringt wesentliche Neuerungen und Verbesserungen bei der Speicherunterstützung mit. Außerdem können viele Funktionen der virtuellen Infrastruktur nur mit zentralem Massenspeicher genutzt werden. Das folgende Kapitel schafft Grundlagen und gibt Anhaltspunkte zu Performance und Ausfallsicherheit.

9 Storage-Architektur

Autor dieses Kapitels ist Dennis Zimmer, opvizor GmbH – opvizor.com, virtuellemaschinen@email.de

Die korrekte Planung der Storage-Architektur ist einer der wichtigsten Faktoren für eine erfolgreiche Virtualisierungslösung. Laut VMware sind fast 90 % der Supportanfragen auf Storage-Probleme zurückzuführen. Dabei sind mit Storage-Problemen weniger physische Störungen, sondern vielmehr Planungsfehler gemeint, die z. B. zu Zugriffs- oder Leistungsproblemen führen. Es ist allerdings zu leicht, einfach alles auf die anfängliche Planung zu schieben, da viele der Schwierigkeiten erst auftreten, nachdem die virtuelle Infrastruktur über eine längere Zeit betrieben wurde und über gewisse Grenzwerte wuchs. Das folgende Kapitel soll helfen, sowohl eine korrekte Planung für jetzt als auch für das kommende Wachstum zu finden. Außerdem zeigen wir Hilfestellungen auf, wie Sie derzeitige und zu erwartende Engpässe adressieren können.

9.1 Lokale Medien

VMware ESX unterstützt die Installation und den Start des Systems auf bestimmten Typen lokaler Festplatten. Dabei bieten die unterschiedlichen Festplattentypen auch unterschiedliche Eigenschaften; z. B. ist der Betrieb virtueller Maschinen nicht von jedem Medium möglich oder empfohlen. Allerdings ist es möglich, beispielsweise über externe USB-Festplatten Sicherungen durchzuführen.

9.1.1 SATA

Die offizielle Unterstützung von SATA-Festplatten kam relativ spät – mit Erscheinen der VMware-Version 3.5. Vorher war der SATA-Einsatz nur im SAN, NAS durch zertifizierte Storage-Anbieter oder an »zufällig« unterstützten SATA-Controllern möglich gewesen. »Zufällig« bedeutet in diesem Fall, dass der gleiche Treiber für SCSI- und SATA-Controller verwendet

werden konnte, wodurch verschiedene Intel- und LSI-Controller »versehentlich« wurden. Allerdings gab es nie einen offiziellen Herstellersupport.

Seit VI3.5 und damit auch mit vSphere kann nun problemlos auf SATA Festplatten zugegriffen werden, vorausgesetzt, der SATA-Controller besitzt offiziellen Support (*http://www.vmware.com/go/hcl*). Eine Installation auf SATA-Festplatten ist uneingeschränkt möglich, allerdings sollten Sie immer eine ausfallsichere RAID-Variante, z. B. RAID 1 oder RAID 5, wählen. Der Betrieb virtueller Maschinen auf lokalen SATA-Festplatten ist allerdings nicht zu empfehlen, wenn die VMs produktiv eingesetzt werden und entsprechend Leistung benötigt wird. Hinzu kommt, dass VMware keine offizielle Unterstützung für lokale IDE und SATA-RAID-Controller anbietet.

Die Leistungsfähigkeit bei Random-Zugriff von SATA- gegenüber Fibre-Channel- oder SAS-Festplatten kann mit weniger als 50 % angegeben werden. Da beim Betrieb mehrerer VMs auf dem gleichen VMFS nahezu ausschließlich Random-Zugriff herrscht, entsteht mit SATA leicht ein Performanceengpass. Hintergrund ist u. a. die Datendichte, also reine Physik. Vergleichen Sie 1 TB SATA mit 300 GB SAS, so sind auf ungefähr gleicher Fläche dreimal mehr Daten abgelegt.

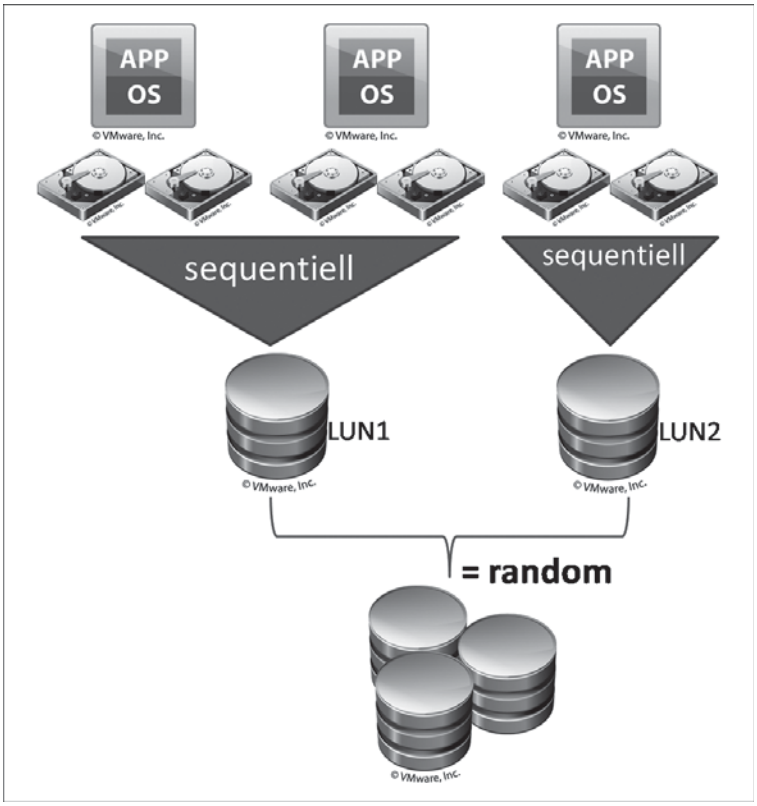


Abbildung 9.1 Aus sequentiellem wird dank mehrerer virtueller Festplatten und LUNs reiner Random-Zugriff.

Dies ist im beim sequentiellen Lesen und Schreiben von Vorteil, allerdings nicht bei Random-Zugriff, wo der Schreib-/Lesekopf sich stetig bewegen muss, um die Daten auszulesen.

Random-Zugriffe auf einer LUN

Sie müssen immer bedenken, dass die Random- oder sequentiellen Zugriffe nicht pro LUN, sondern pro RAID-Gruppe stattfinden. Daher ist es nahezu unmöglich, dass sequentiell Zugriffe vorkommen, wenn mehrere VMs über mehrere LUNs auf einer RAID-Gruppe liegen. Daher ist sequentiell nur zu gewährleisten, wenn eine VM oder ein RDM auf einer LUN liegt, die wiederum allein auf einer RAID-Gruppe liegt.

SATA-Festplatten sind zumeist mit 5.400 oder 7.200 Umdrehungen (RPM) erhältlich und wesentlich billiger als die FC-Typen. Mittlerweile verfügen die SATA-Platten über bis zu 64 MB Cache, was deutliche Leistungsvorteile bringt. Allerdings kann die einzelne SATA-Festplatte nicht mit einer FC-/SAS-Platte mithalten. Es ist davon auszugehen, dass eine SATA-Platte zwischen 70 und 90 IOPS je nach Umdrehungen erreicht.

Dagegen hilft nur das Bündeln mehrerer SATA-Festplatten zu einem großen RAID-Verbund, allerdings führen Sie dies besser im SAN (Storage Area Network) oder NAS (Network-attached Storage) als im DAS (Direct-attached Storage) durch.

Unter vSphere 4 mussten Sie noch einen wesentlichen Punkt bedenken, und zwar die Limitierung von VMware auf zwei TB-LUNs. Je nach Storage-System und der Umrechnung von 2 TB in Byte sollten Sie nur mit 1,99 TB formatieren, um VMFS-Probleme zu vermeiden. Dieses Limit von 2 TB pro LUN wurde mit vSphere 5 auf 64 TB angehoben!

Würden Sie fünf 1-TB-SATA-Festplatten in einem RAID 5 bündeln, so kämen Sie auf eine Nutzkapazität von etwa 4 TB. Existieren keine Möglichkeiten des lokalen RAID-Controllers oder des Storage-Systems, diese RAID-Gruppe nochmals logisch zu unterteilen – z. B. 2 × 2 TB –, dann ist diese RAID-Gruppe nicht mit VMware nutzbar. Mit ein wenig Glück erkennt VMware vSphere 4 dieses RAID als 1,6-TB-Platte, allerdings ist es nicht empfehlenswert, in einem solchen Zustand produktiv zu arbeiten. Unter vSphere 5 ist die LUN-Größe kein Problem mehr, und die 4 TB wären komplett nutzbar. Allerdings sollten Sie sich zweimal überlegen, ob die Leistungsfähigkeit von vier Festplatten im RAID 5 ausreicht, um virtuelle Maschinen zu betreiben.

Außerdem müssen Sie daran denken, dass SATA-Festplatten ursprünglich aus dem Desktop-Bereich kommen und dort MTBF (Mean Time between Failure) nicht wirklich ein wichtiges Kriterium ist. Momentan beginnt zwar ein Trend, SATA im professionellen Umfeld einzusetzen und die Festplatten als »RAID-ready« oder »Enterprise-ready« zu kennzeichnen, allerdings sind die Ausfallraten derzeit noch höher als im SCSI-, SAS- oder Fibre-Channel-Umfeld.

Kommt es nicht auf Festplattenleistung an und ist nur Festplattenkapazität von Bedeutung, ist SATA eine erstklassige Wahl. Übrigens sind SATA-Festplatten aufgrund ihrer sehr guten sequentiellen Leistung sehr gut im Backup-/Restore-Umfeld einsetzbar.

9.1.2 SCSI und SAS

SAS (Serial-attached SCSI) hat das parallele SCSI (finaler Standard Ultra-320) in rasanter Geschwindigkeit abgelöst. Die parallele SCSI-Anbindung hatte die physischen Belastungsgrenzen erreicht, da die Signallaufzeit der einzelnen Bits auf dem Bus zu sehr abwich. SAS überträgt das traditionelle SCSI seriell und ermöglicht damit höhere Übertragungsraten, nämlich bis zu 3 GBit/s, 6 GBit/s und bald 12 GBit/s (2013) vor. Außerdem nutzt SAS Punkt-zu-Punkt-Verbindungen, wodurch ein SCSI-Terminator überflüssig wird. SAS hat aber noch zwei weitere Vorteile:

Expander

SAS unterstützt die Erweiterung durch Expander, um Domänen von SAS-Geräten aufzubauen, was mit Netzwerk-Switches vergleichbar ist. Damit ist es möglich, bis zu 128 Endgeräte über ein SAS-Kabel zu betreiben. Real existieren derzeit 36er-Anschlüsse.

Dual Porting

SAS bietet die Möglichkeit, Festplatten mit einem oder mit zwei Ports zu nutzen, entweder gebündelt (Performance) oder zur Ausfallsicherheit. Eine Dual-Port-SAS-Platte kann somit an zwei unterschiedliche SAS-Controller angeschlossen werden, womit eine Ausfallsicherheit sehr einfach realisierbar ist.

Kein Hersteller verbaut noch SCSI-Festplatten in den Servern; SAS- und SSD-Festplatten sind in diesem Feld mittlerweile gesetzt. Auch im Storage-Bereich ist immer öfter SAS zu finden, z. B. bei Dell-EqualLogic- oder HDS-Systemen. Da SAS eine Weiterentwicklung von SCSI darstellt, besitzt SAS die gleichen positiven Eigenschaften: sehr gute Zugriffs- und Übertragungswerte. Hier ist von 120 IOPS (10.000 Umdrehungen) und 180 IOPS (15.000 Umdrehungen) auszugehen.

SCSI- und SAS-Platten sind ideale Kandidaten zur Verwendung als lokaler Speicher mit VMware ESX. Auch bei SCSI und SAS gilt, lokal ein ausfallsicheres RAID 1 oder RAID 5 aufzubauen, bevor Sie den ESX-Server installieren.

Beide Plattentypen eignen sich zudem bei entsprechender Festplattenanzahl und entsprechendem RAID-Level (1, 10 oder 5, 50) zum Betrieb virtueller Maschinen auf lokalem Speicher. SAS-Festplatten werden inzwischen auch sehr oft im kleinen 2,5"-Faktor ausgeliefert und sind damit echte Allrounder.

9.1.3 Fibre-Channel

Fibre-Channel-Festplatten gehören (abgesehen von Solid-State-Festplatten) definitiv zu den schnellsten Festplattentypen im Storage-Bereich. Aufgrund des teuren FC-Anschlusses sind diese Festplatten im Server-Bereich sehr selten zu finden, dafür im Storage-Bereich umso

öfter. Wegen der guten Zugriffsgeschwindigkeit und der hohen Datenübertragungsraten wird FC meist in Bereichen eingesetzt, in denen Geschwindigkeit und Zuverlässigkeit gefragt sind.

Die Spindeln der FC-Platten drehen 10.000 oder 15.000 Mal die Minute (RPM), und man kann von den minimal höheren IOPS-Raten wie bei SAS-Festplatten ausgehen. FC ist trotz des Aufholens von SAS nach wie vor die schnellste Festplattenvariante.

9.1.4 IDE

Aus der Not geboren, integrierte VMware auch eine IDE-Unterstützung, nicht nur für Wechselmedien (CD/DVD), sondern auch für lokale Festplatten zur Installation unterstützt. Die Not wurde durch die ersten Blade-Server ausgelöst, die mit 2,5"-IDE-Festplatten ausgestattet waren. Allerdings ist nur die Installation des ESX-Servers auf diesem Medium unterstützt, VMFS-Unterstützung besteht nicht! Dies hat auch einen guten Grund, denn IDE-Festplatten bieten weder die Verfügbarkeit noch die Leistungsfähigkeit, die man sich zum Betrieb virtueller Infrastrukturen wünscht.

Bei IDE-Nutzung gilt genau wie bei anderen Festplattentypen, dass Sie zumindest ein RAID 1 über zwei Festplatten erstellen sollten, um den Defekt einer Festplatte ohne Datenverlust und Ausfall zu überstehen.

9.1.5 SSD

SSD steht für »Solid State Disk« und bezeichnet Festplatten, die aus Speicherchips und nicht aus den in der traditionellen Festplattenwelt bekannten Magnetscheiben bestehen. Als Speicherchips dienen entweder Flash oder SDRAM. Die beiden Speichertypen unterscheiden sich hauptsächlich in Geschwindigkeit und Flüchtigkeit, wie Tabelle 9.1 zeigt.

Merkmal	SSD Flash	SSD SDRAM	Festplatte
Geschwindigkeit	mittel – hoch	sehr hoch	hoch
Zugriffszeit	gut	sehr gut	mittel – schlecht
Datenflüchtigkeit	nicht flüchtig	flüchtig	nicht flüchtig
Robustheit	hoch	hoch	niedrig
Leistungsaufnahme	niedrig	niedrig	hoch
Lautstärke	lautlos	lautlos	mittel – hoch
Preis	mittel – hoch	sehr hoch	günstig – hoch

Tabelle 9.1 Vergleich SSD-Typen zu herkömmlicher Festplatte

SSD-Festplatten dienen z. B. auch als Installationsbasis für die Embedded-Version des VMware ESXi, die bei Server-Auslieferung bereits vorinstalliert ist. Dort werden entweder SSD-Festplatten oder USB-Memory-Sticks genutzt.

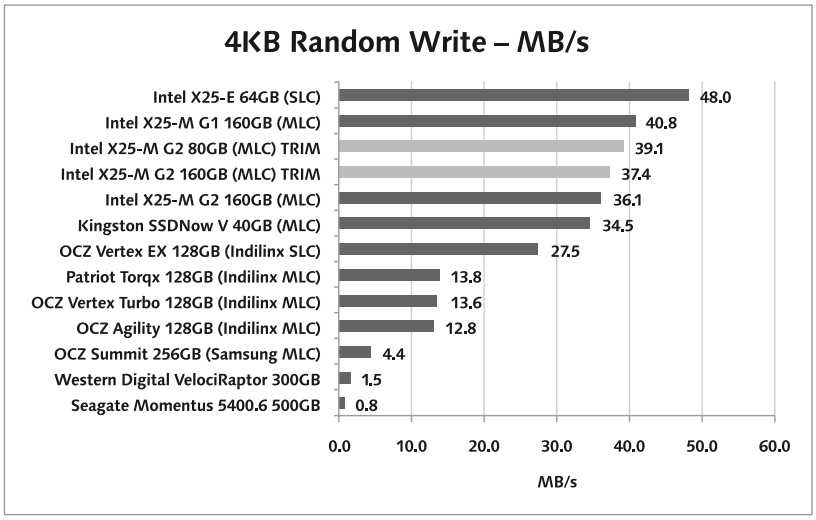


Abbildung 9.2 Deutliche Vorteile bei Random-Write durch die Verwendung von SSD gegenüber den letzten beiden Magnetplatten

Der Test der verschiedenen SSDs und die Gegenüberstellung mit den beiden Magnetfestplatten von Western Digital und Seagate zeigen sehr deutlich die Vorteile für die Solid-State-Laufwerke. Dieser Test und auch die Grafiken sind auf AnandTech (*http://www.anandtech.com/storage/showdoc.aspx?i=3667&p=6*) zu finden.

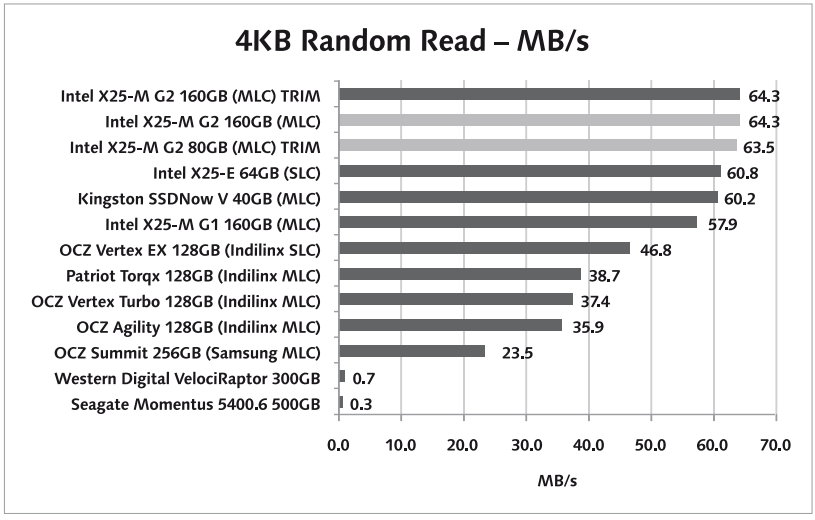


Abbildung 9.3 Noch deutlichere Vorteile bei Random-Read durch die Verwendung von SSD gegenüber den letzten beiden Magnetplatten

Derzeit sind die Preise von SSD-Platten noch höhere als Standard-SATA oder SAS-Festplatten, allerdings ist es sehr sicher, dass SSD-Festplatten die Zukunft sind und in den nächsten Jahren

herkömmliche Festplatten zum großen Teil als Leistungsgeber ersetzen werden. Herkömmliche Festplatten werden dann nur noch als Massenspeicher und nicht mehr als Performancelieferant genutzt. Diese Aussage soll für den Desktop-, Notebook- und Server-Markt gelten. Außerdem werden sie aufgrund der enormen Leistungsmöglichkeiten im Random-Zugriff sehr schnell im Storage-Markt Einzug erhalten (HDS, EMC und NetApp haben bereits Module im Programm, Texas Memory hat mit den RAMSAN-Modellen seit Längerem enorm schnelle Speichersysteme im Portfolio).

Eine SSD-Festplatte kann im unteren Segment (MLC) ca. 1.000 – 2.000 IOPS aufweisen, teure EFD (Enterprise Flash Drive) mit SLC-Technologie 6.000–30.000 IOPS.

Aber auch wenn man mit den hohen Preisen kalkuliert, so sind diese nur auf die Kapazität bezogen hoch – auf die I/O und damit die Leistungsfähigkeit gerechnet sind die SSD-Laufwerke deutlich günstiger als die SAS- oder SATA-Festplatten, da Sie von diesen die 30- bis 50-fache Menge benötigen würden. Gerade im VMware-, aber auch im Datenbank- und Exchange-Umfeld sind die Kapazitäten der Festplatten zumeist wesentlich uninteressanter als die Leitungsfähigkeit, daher ist der Erfolg der SSD-Laufwerke nur eine Frage der Zeit.

Eine sehr interessante Flash-PCIe-Karte, die enorme Geschwindigkeiten bietet, wurde von dem Unternehmen Fusion-io entwickelt (*www.fusionio.com*). In die gleiche Richtung entwickelt mittlerweile auch Texas Memory und bietet eine Flash-Storage-Karten an, die mit 120.000 IOPS (im Vergleich EFD bis zu 30000 IOPS) und 700 MB/s Random-Durchsatz enorme Performance aufweist.

SSD-Karten werden besonders gerne in Storage-Systemen zur Cache-Erweiterung eingesetzt.

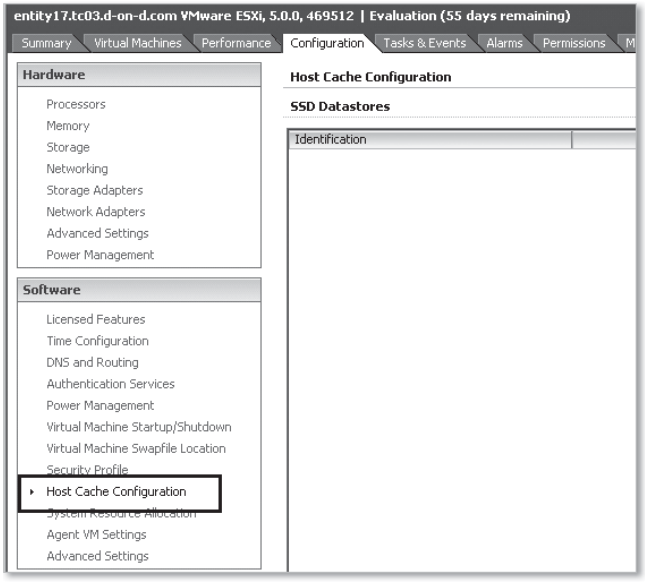


Abbildung 9.4 SSD-Datastores als Host-Cache

Mit vSphere 5 können SSD-Massenspeicher als Host-Cache eingesetzt werden, um eine Beschleunigung bei der Auslagerung des VM-Hauptspeichers (Swap) zu erreichen (Abbildung 9.4) – siehe Abschnitt 9.10, »Flash-basiert«.

9.1.6 USB

USB-Festplatten bieten aufgrund der guten Geschwindigkeit und des guten Preises eine schöne Möglichkeit, virtuelle Maschinen zu sichern und wiederherzustellen.

Nachweislich kommt es allerdings bei einer Vielzahl von Server-Systemen zu Leistungseinbußen, wenn der USB-Anschluss aktiviert ist. Daher sollten Sie dies bei den Server-Systemen vorher prüfen! Falls es zu Leistungsproblemen kommt (im schlimmsten Fall Absturz des Systems), empfiehlt es sich, den On-Board-USB-Controller abzuschalten. Wenn Sie dennoch USB einsetzen möchten, ist eine USB-Zusatzsteckkarte die bessere Wahl.

Tipp

Trotz der Möglichkeit, virtuelle USB-Controller in den virtuellen Maschinen zu konfigurieren, können Sie keine USB-Sticks oder USB-Festplatten an den ESX-Host anschließen und diese Geräte an die virtuelle Maschine direkt weiterreichen. Dies würde außerdem vMotion und DRS und sogar HA verhindern.

9.1.7 Cache

Cache ist der transparente Beschleuniger in der Mitte der Kommunikation zwischen Abnehmer (Server) und Storage-System. Je nach Architektur sitzt der Cache auf dem Storage-Adapter (z. B. lokale SCSI-Controller) oder im Storage-Controller und kann in Größe und Geschwindigkeit beliebig abweichen, was natürlich auch mit finanzieller Mehrbelastung zu tun hat.

Mit Cache versucht man, den Zugriff auf die langsamen Festplatten zu vermeiden oder besser zu reduzieren. Kann ein Block aus dem Cache gelesen werden, wurde der I/O auf den Festplatten gespart. Kann man diesen Vorgang maximieren, kann man im Hintergrund sogar Festplatten einsparen.

Cache ist zwar kein Wundermittel, ist aber bei vielen Lastprofilen nutzbringend, wie beispielsweise NetApp PAM (Read-Cache im Storage-System) oder Fusion-io-Karten (Flash-Karte im Serversystem), bei VMware-View-Umgebungen, wo Sie sehr oft mit den gleichen Blockabfragen konfrontiert werden, da die View-VMs aus einen großen Anteil gleicher Daten bestehen (Template – Clone).

Eine Unart vieler Storage-Hersteller ist allerdings, dass sie die Messdaten ihrer Storage-Systeme mit Cache optimieren. Somit sind die typischen Performancevergleiche der Konkurrenten immer mit Vorsicht zu genießen, und die Tests entsprechen nicht den realen Lastdaten einer typischen Produktionsumgebung.

9.2 Die Wahl: Block oder File

Grundlegend sei vorweggesagt, dass bei vSphere alle Dateien, aus denen virtuelle Maschinen bestehen, zusammen in einem Unterverzeichnis oder mehreren Unterverzeichnissen (je nach Verteilung der virtuellen Festplatten) liegen. Dieses Verzeichnis liegt wiederum in einem sogenannten *Datastore* – einem Ablageort für virtuelle Maschinen. Dabei ist es für die virtuellen Maschinen im Alltagsbetrieb völlig transparent, um welche Art von Datastore es sich handelt, das heißt, eine VM kann nicht unterscheiden, ob sie auf einem VMFS-3-formatierten – somit blockbasierten – Datastore gespeichert ist, oder ob sie auf einem NFS-Datastore liegt.

Beide Arten von Datastores haben ihre Vor- und Nachteile. Die Entscheidung ist hier sicherlich nicht trivial und auch nicht durch ein »gut« oder »schlecht« zu beantworten. Es kommt hier immer auf die eigenen Anforderungen und Voraussetzungen an, um die Entscheidung zu vereinfachen. Klassisch wurden von ESX in Version 2 ausschließlich Fibre-Channel-Datastores unterstützt. Daher war zu diesem Zeitpunkt die Wahl sehr einfach. Doch VMware begann mit Version 3.0 auch, iSCSI- und NFS-Datastores zu erlauben.

Es sei Ihnen selbst überlassen, die für sich richtige Wahl zu treffen. Als Entscheidungshilfe können Sie Tabelle 9.2 heranziehen.

Eigenschaften	FCP	iSCSI	NFS
Durchsatz	hoch (100 %)	niedriger (92 %); eventuell besser bei 10GE	mittel (95 %); eventuell besser bei 10GE
Latenz	sehr niedrig	mittel	mittel
Kosten	hoch; neue HBAs und eventuell Switches nötig	sehr niedrig; alles in zumeist kostenloser Software	niedrig; Infrastruktur und Wissen meist vorhanden
Redundanz	sehr gut und einfach	gut, abhängig von LAN Switches, mittelschwer	gegeben, aber relativ komplex zu konfigurieren
Komplexität	hoch; oft neues Know-how nötig	mittel; iSCSI-Know-how schnell lernbar	niedrig; NFS-Know-how meist vorhanden
Skalierbarkeit	gut (Beschränkungen von VMFS bis Version 3)	mittel (Beschränkungen von VMFS bis Version 3)	sehr gut, keine VMFS-Limits
Management	komplex	mittelschwer	einfach
Platzverbrauch	normal, nur mit Thin Provisioning niedrig	normal, nur mit Thin Provisioning niedrig	niedrig, Thin Provisioning per Default

Tabelle 9.2 Vergleich der Datastore-Protokolle

Neben diesen Kriterien spielen bei der Wahl auch oft die bereits im Einsatz befindlichen Technologien eine ausschlaggebende Rolle:

- Sind bereits eine FCP-Infrastruktur und Know-how vorhanden?
- Ist eine 10-GBit-Ethernet-Infrastruktur vorhanden?
- Womit hat der Administrator am meisten Erfahrung, insbesondere beim Troubleshooting und Design der Infrastruktur?
- Welche Protokolle sind auf dem Storage-System lizenziert?

Um weitere Vorteile und Nachteile der entsprechenden Anbindungsarten kennenzulernen, haben wir die Storage-Themen auf insgesamt drei Kapitel verteilt, um Ihnen die bestmöglichen Angaben zu bieten.

9.3 Storage Area Network – Was ist eigentlich ein SAN?

Zu dieser kurzen Frage könnte man mit einem oder mehreren Büchern antworten, allerdings fassen wir uns kurz und gehen nur auf das im VMware-Umfeld Wesentliche ein.

Ein *Storage Area Network* ist ein eigenes Netzwerk, in dem Massenspeichersysteme mit Server-Systemen verbunden sind. Man unterscheidet mittlerweile FC-SAN (Fibre-Channel) und IP-SAN (iSCSI), allerdings stammen die Basiskonzepte aus der Fibre-Channel-Welt.

Traditionell wird ein SAN mit Fibre-Channel verbunden und in einer *Switched Fabric* betrieben. Die Switched Fabric ist eine Sternvernetzung, die durch Fibre-Channel-Switches realisiert wird. Um die Ausfallsicherheit zu gewährleisten und auch Wartungen zu vereinfachen, werden meist mehrere Switched Fabrics aufgebaut, die komplett voneinander unabhängig sind, aber trotzdem die gleichen Endgeräte an anderen Ports miteinander verbinden.

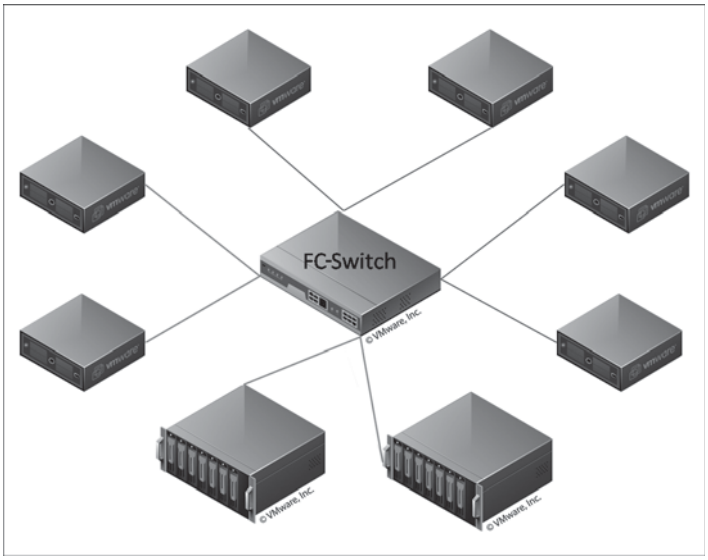


Abbildung 9.5 Switched Fabric

Neben der Switched Fabric existiert der *Arbitrated Loop*, der für Speichernetze allerdings veraltet ist und von VMware auch keine Unterstützung findet. Er ist wie ein Ring aufgebaut und kann durch die Nutzung von FC-Hubs vereinfacht verkabelt werden. Eine enorme Einschränkung bei der Verwendung des Arbitrated Loops ist, dass die Gesamtbandbreite zwischen allen Teilnehmern aufgeteilt wird, da immer nur zwei Teilnehmer gleichzeitig miteinander kommunizieren können. Stehen 2 GBit in einem Ring mit 8 Knoten zur Verfügung, kann im Durchschnitt nur mit 256 MBit pro Knoten kalkuliert werden. Arbitrated Loop wird jedoch nach wie vor oft intern in Storage-Systemen verwendet, was allerdings für die VMware-Infrastruktur nicht sichtbar ist.

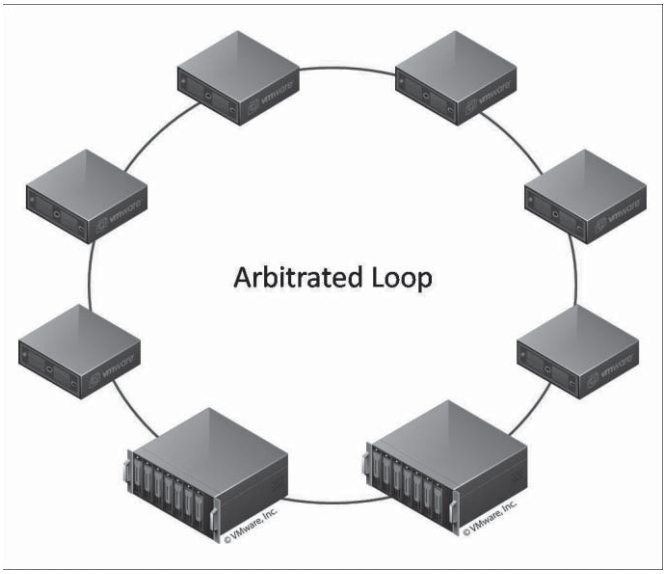


Abbildung 9.6 Arbitrated Loop im SAN

Mit der Einführung von iSCSI wurde auch Ethernet als Basis für Speichernetze populär, und man spricht hier von *IP-SAN*.

Ein wesentliches Unterscheidungsmerkmal zwischen SAN und LAN ist aber in jedem Fall, dass nur Speichergeräte und Server miteinander verbunden sein sollten und nur mit Speicherprotokollen kommuniziert wird (iSCSI, FCP). Diese Trennung ist unabhängig von der physischen Basis sinnvoll und sehr zu empfehlen.

Im aktuellen Fibre-Channel-Umfeld fällt die Trennung zum LAN leicht, da Fibre-Channel nicht zur »normalen« Netzwerkkommunikation genutzt wird. So ist es unwahrscheinlich, jemanden mit einem mit FC-Adapter bestückten Notebook im Rechenzentrum beim Datenschnüffeln zu erwischen. Bei iSCSI können jedoch Standard-Ethernet-Switches und Netzwerkkarten verwendet werden. In diesem Fall können wir nur dringend anraten, entweder das IP-SAN vom LAN mit separaten Switches komplett zu trennen oder zumindest mit einer Trennung mittels VLAN zu arbeiten.

9.4 Infiniband

Eine nicht ganz neue, aber wiederentdeckte Technologie ist Infiniband. Infiniband ist ein Hochgeschwindigkeitsnetz mit sehr geringen Latenzzeiten, das auch im VMware-Umfeld mit vielen Vorteilen glänzt. Ursprünglich wurde Infiniband für High-Performance-Computing-Umgebungen entwickelt, allerdings stellt sich Infiniband nach und nach als sehr gute Lösung für konsolidierte Umgebungen heraus, da neben der hohen Leistungsfähigkeit eine Konsolidierung der I/O-Adapter stattfinden kann. Ein Infiniband-HCA (Host Channel Adapter) kann derzeit 20 GBit Durchsatz erzielen und damit etliche GB-Ethernet und FC-Adapter ersetzen. Gerade Heartbeat-Netze und vMotion-/FT-Netzwerke profitieren sehr von Infiniband. Allerdings wird sich diese Technologie sehr schwer gegen die 10-GBit-Konkurrenz durchsetzen können.

9.5 Kommunikationsadapter

Unabhängig von iSCSI-, SCSI- oder Fibre-Channel-Netzwerken wird immer von *Initiator* und *Target* gesprochen. Diese Ausdrücke haben ihren Ursprung im SCSI-Protokoll und bezeichnen den Client-seitigen bzw. Host-/Storage-seitigen Endpunkt einer SCSI-Verbindung.

9.5.1 Initiator

Der Initiator stellt die Datenverbindung zum Speicherendpunkt (Target) her. Es gibt zwei Arten von Adaptern, die im VMware-Umfeld als Initiatoren genutzt werden können: HBA (Hardware-Initiator) und Software-Initiator.

Host-Bus-Adapter (FC, iSCSI)

Sowohl Fibre-Channel- als auch iSCSI-Verbindungen können mittels physischem Host-Bus-Adapter (HBA) zum Speichersystem hergestellt werden. Diese Adapter müssen über einen schnellen Bus zum Server-System verfügen, daher sind sie zumeist als PCI-X- oder PCI-Express-Karten erhältlich.

Ein großer Vorteil von HBAs ist die eingebaute CPU, die die FC- oder iSCSI-Pakete empfängt, bearbeitet oder verschickt. Dadurch werden die Prozessoren des Host-Systems nicht belastet. In Abbildung 9.7 ist klar zu sehen, dass der HBA die FC-Frames verwaltet und der VMkernel nur den Treiber zur Nutzung stellen muss.

Im iSCSI-Fall dient die HBA-CPU zum Entpacken und Verpacken der SCSI-Kommandos in das TCP/IP-Protokoll.

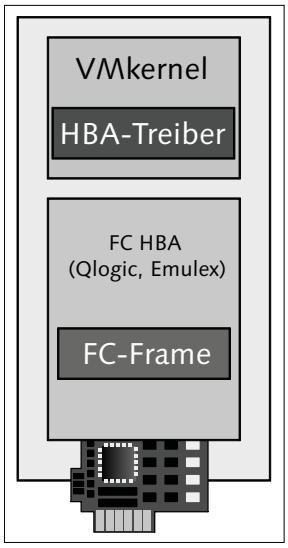


Abbildung 9.7 Fibre-Channel-HBA mit VMware-Treiber

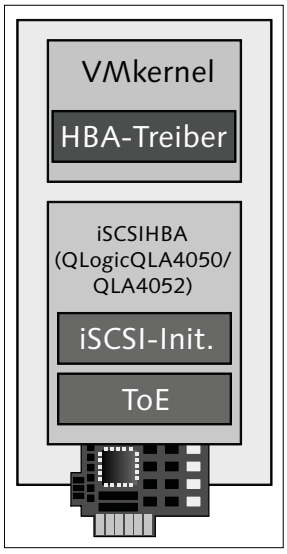


Abbildung 9.8 iSCSI-HBA mit VMware-Treiber

Die meisten HBAs verfügen außerdem über ein BIOS, das auch den Systemstart über den HBA ermöglicht. Durch diese Funktion ist die Nutzung von festplattenlosen Systemen möglich, deren Systempartitionen im SAN liegen. Auch diese Funktion entstand wie die IDE-Unterstützung aufgrund von Anforderungen aus den Blade-Systemen. Bei der Verwendung von HBAs in der gleichen Broadcast-Domäne sollten Sie immer die Firmwareversionen identisch halten, um Inkompatibilitäten zu vermeiden.

VMware-HBA und Software-Initiator

VMware unterscheidet bei der Unterstützung von Storage-Systemen zwischen der Zertifizierung für HBAs und Software-Initiator, worauf Sie in jedem Fall achten sollten.

Software-Initiator

Software-Initiatoren bzw. emulierte Controller, die als Initiator dienen, kommen unter VMware ESX nur im iSCSI-Umfeld vor. Der große Vorteil der Software-Initiatoren ist die Verwendbarkeit von herkömmlichen Netzwerkkarten zur iSCSI-Kommunikation, was einen erheblichen Kostenvorteil bringt.

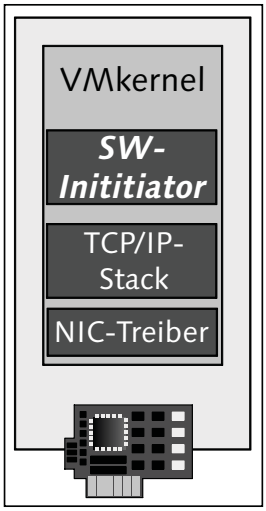


Abbildung 9.9 Der Software-iSCSI-Initiator wird komplett vom Kernel gestellt, basierend auf dem Netzwerkkartentreiber.

Unter VMware ESXi besteht nur der Nachteil der Belastung der Host-CPU. Die Host-CPU-Belastung wird mit neueren VMware ESX-Versionen nach und nach durch TOE-fähige (TCP/IP Offload Engine) Netzwerkkarten und die Verteilung der VMkernel-Last auf unterschiedliche CPU-Kerne minimiert oder gar komplett wegfallen.

Bei Verwendung moderner Server-Systeme ist der Geschwindigkeitsunterschied zwischen Software- und Hardware-Initiatoren kaum spürbar. Allerdings ist es mit Software-Initiatoren nicht möglich, das System über SAN zu booten, das heißt, Sie benötigen zwingend lokale Systemfestplatten.

iSCSI und Gateways

Obwohl es möglich ist, die iSCSI-Anbindung über Router und Gateways zu betreiben, sollten Sie dies unter allen Umständen vermeiden.

Hier ist besonders auf eine performante Verbindung zwischen dem VMkernel-Port und dem Storage-Target zu achten. Die Service-Console-Verbindung, die für die Metadaten zuständig ist, ist nicht minder wichtig, aber etwas anspruchsloser als der Datenkanal.

Software-Initiator im Gastbetriebssystem

Neben der Möglichkeit der Software-iSCSI-HBA-Nutzung im VMkernel bringen sowohl Linux als auch Windows eigene iSCSI-Initiator-Treiber mit, die über das Netzwerk der virtuellen Maschine die Verbindung mit dem Target aufnehmen. Diese Variante ist die schnellstmögliche iSCSI-Nutzung, da die Software-iSCSI-Initiatoren der Gastbetriebssysteme MPIO-Multipathing unterstützen, wodurch gleichzeitig mehrere Verbindungen (Netzwerkkarten) zum Storage-System hergestellt und genutzt werden können.

Ansonsten ist dieses Verfahren mit Raw Device Mapping vergleichbar, da die LUN nur der einzelnen VM, also dem einzelnen Software-iSCSI-Initiator, zur Verfügung steht. In diesem Fall benötigt der ESX-Host keinerlei Zugriff auf den iSCSI-Storage.

Da kein Booten von iSCSI mittels Gastbetriebssystem möglich ist, müssen Sie diese Technik allerdings mit lokalen VMFS-Partitionen, NFS oder iSCSI über VMkernel kombinieren, z. B. Boot-Platte über VMkernel und Datenplatte über Software-iSCSI im Gast. Der größte Nachteil besteht in der recht hohen CPU-Belastung für das Gastsystem und damit den VMware ESX-Host, da die komplette iSCSI-Berechnung im Gastsystem stattfindet. Abhilfe schaffen hier aber VMXNET-3-Adapter oder sogar VMDirectpath-I/O-Adapter.

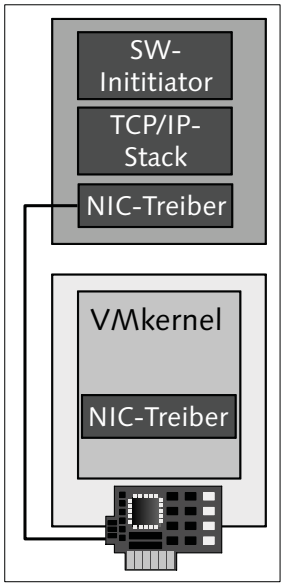


Abbildung 9.10 Der Software-iSCSI-Adapter im Gast (oberer Bereich) wird komplett vom Gastbetriebssystem betrieben, die Netzwerkverbindung basiert auf dem Netzwerkkartentreiber des VMkernels (vSwitch + Uplink).

Host-Channel-Adapter (Infiniband)

Im Infiniband-Umfeld spricht man nicht von Host-Bus-Adaptern, sondern von Host-Channel-Adaptern. Diese sind die Initiatoren und dienen zum Zugriff auf die Storage-Systeme. Infiniband hat wesentliche Vorteile bei Latenzzeiten, Konsolidierung und Gesamtgeschwindigkeiten. Seit Version 3.5 des ESX-Servers werden HCAs der Firma Mellanox als Community-Support unterstützt, das heißt, der Hersteller übernimmt den Support für die VMware-Komponenten. Die Infiniband-Technik ist im hochpreisigen Segment angesiedelt und ist mit FC vergleichbar.

AoE-(ATA over Ethernet-)Adapter

ATA over Ethernet (AoE) ist definitiv der Außenseiter unter den Möglichkeiten einer Storage-Anbindung und wird nur vom Unternehmen Coraid angeboten. ATA over Ethernet ist ein Storage-Protokoll auf Layer 2 (Ethernet-Frames) und wurde ursprünglich von dem Unternehmen Brantley Coile entwickelt. Da keine Protokolle höherer Layer wie IP, UDP oder TCP verwendet werden, ist AoE schlanker als iSCSI.

Um AoE unter VMware ESX zu nutzen, müssen Sie spezielle Ethernet-Adapter der Firma Coraid einsetzen und entsprechende Treiber im VMkernel einbinden. AoE ist im Niedrigpreissegment anzusiedeln und sogar günstiger als iSCSI und vom technischen Aufbau schneller. Außerdem dürfen Sie einen unfreiwilligen Sicherheitsaspekt nicht vergessen: Da AoE auf Ethernet-Frames basiert, sind die Pakete nicht routingfähig, wodurch sie ein physisches Ethernet-Segment nicht verlassen können.

FCoE-(Fibre-Channel over Ethernet-)Adapter

Fibre-Channel over Ethernet (FCoE) ist ein Protokoll, das Fibre-Channel-Frames über den Standard-Ethernet-Bus transportiert. So können Sie trotz Nutzung von Fibre-Channel die 10-GBit-Ethernet-Technologie einsetzen.

Somit ist es dank FCoE auch möglich, existierende FC-Architekturen zu nutzen und gleichzeitig Teile von FC über die Ethernet-Komponenten zu betreiben. Dazu müssen Sie z. B. die Fibre-Channel-N_Port-IDs und die Ethernet-MAC-Adressen miteinander verbinden, was FCoE als Funktion liefert. Dies bietet den Vorteil eines sanften Übergangs oder Wechsels von FC nach Ethernet bei weiterer Nutzung von »Altlasten« im FC-Umfeld.

Weitere Vorteile sind:

- Reduzierung der Anzahl von Anschlusskarten, die zur Storage- und Netzwerkverbindung genutzt werden
- Reduzierung von Kabeln und Switches
- Reduzierung von Energiebedarf und Kühlungskosten

FCoE wurde schon sehr früh von NetApp und Cisco in Angriff genommen, daher sind deren Integrationen derzeit technologisch führend.

9.5.2 Target

Initiatoren nützen nichts, wenn kein Target zur Verfügung steht, um an der Kommunikation teilzunehmen. Als Target wird allgemein das Storage-System bezeichnet, allerdings ist technisch jeder Storage-Prozessor, eigentlich sogar jeder Storage-Prozessor-Port, für den Initiator ein gültiges Target. Schauen wir uns den Aufbau eines Storage genauer an.

Systemaufbau (Storage-Prozessor)

Als *Storage-Prozessor* wird allgemein die Intelligenz des Storage-Systems bezeichnet. Andere Begriffe hierfür sind »Head« (Kopf), »Controller« oder herstellerspezifische Angaben wie »Slammer« (Pillar Data Systems). Jeder Storage-Prozessor, kurz SP, kann über einzelne oder viele Ports verfügen, die entweder als Target zum Frontend (z. B. ESX-Server) oder selbst als Initiator ins Backend (weitere Storage-Systeme – typischerweise bei Verwendung von Storage-Virtualisierung) dienen.

Außerdem besitzen die SPs individuelle Technologien zur Leistungssteigerung, die auch speziell auf die Eigenschaften des Herstellers abgestimmt sind (z. B. Steigerung der Double-Parity-Geschwindigkeit). Dazu gehören auch leichter verständliche Konfigurationen wie die Menge des verfügbaren Lese- und Schreibcache.

Abhängig von Hersteller, Modell und Typ verfügen die SPs über eine unterschiedliche Anzahl unterschiedlicher Technologien (FC, Ethernet, iSCSI, AoE, NFS ...), die die Leistungsfähigkeit und die Ausfallsicherheit für die angeschlossenen Server-Systeme bestimmen. Im Normalfall sind alle Anschlüsse eines SPs immer im *Active/Active-Zustand*, das heißt, jegliche Speicheranbindung ist gleichwertig und gleich performant. Sind mehrere SPs miteinander verbunden (interne Cluster), so ist die Architektur des Herstellers dafür ausschlaggebend, ob weiterhin alle Pfade aktiv sind oder manche passiv oder langsamer.

Anschlüsse (FC, iSCSI, Infiniband etc.)

Natürlich verfügt auch das Target über entsprechende Host-Bus-Adapter, die die entsprechenden Speicherprotokolle unterstützen müssen. Daher kommt es auch auf das jeweilige Speichersystem an, ob Fibre-Channel, iSCSI, Infiniband, FCoE oder AoE unterstützt wird. Die Anzahl der HBA-Ports bestimmt die Designmöglichkeiten und die Punkte Ausfallsicherheit und Lastverteilung. Die Storage-Anschlüsse oder -Ports sind der sichtbare Storage-Teil aus VMware ESX-Sicht, das heißt, die Pfade werden über Intitiator:Target-Portverbindungen dargestellt.

9.5.3 Logical Unit Number – LUN

Die Logical Unit Number oder kurz LUN ist das eigentliche Medium, das vom Initiator erkannt und genutzt wird. Statt einer physischen Festplatte kann dies auch eine logische Festplatte oder ein Bandlaufwerk sein.

Grob ausgedrückt, spiegelt die LUN für den ESX die Festplatte im SCSI-Bus wieder, die entweder mit VMFS formatiert oder als Raw Device Mapping genutzt werden kann. Allerdings geht die LUN keine zwingende 1:1-Beziehung mit den physischen Festplatten ein, sondern kann auch eine logische Aufteilung darstellen. Legen Sie beispielsweise ein RAID-Set mit fünf Platten im RAID 5 an, können Sie dieses RAID je nach Speichersystem problemlos als zehn LUNs, auch mit unterschiedlicher Größe, herausgeben. Für das Initiator-System stellt sich diese LUN immer wie ein einzelnes nutzbares Medium zum Zugriff dar.

Durch die Nutzung von LUN-IDs statt fester SCSI-IDs ist es möglich, weit mehr Geräte nach außen zu geben bzw. aus Initiatorsicht zu unterscheiden.

LUNs werden durch eine ID von 0 bis 255 gekennzeichnet und bilden in Verbindung mit HBA und Target den Pfad im SCSI-Umfeld.

Die LUN-ID spielte unter ESX 3 eine wesentliche Rolle, da sie bei der Erstellung der VMFS-Metadaten einbezogen wurde, um Snapshots von Original-Volumes zu unterscheiden. Mit ESX 3.5 Update 4 wurde die LUN-ID-Abhängigkeit bereits aufgebrochen, und seit vSphere wird der NAA-(Network Address Authority-)Namespace oder, wenn das Storage-System die LUN-WWN (World Wide Number) nicht liefert, der T10-Namespace genutzt.

9.5.4 Pfadmanagement (Active/Active, Active/Passive)

Die Verwaltung und Nutzungsmöglichkeiten der verschiedenen Pfade zur Kommunikation und Datenübertragung zwischen Server-System und Storage-System sind ein wesentliches Leistungsmerkmal in der Virtualisierung. Pfade sind alle Wege, die zwischen Initiator und Target möglich sind. Erfolgt keine Aufteilung (Zoning), so wären bei einem ESX-Host mit zwei Anschlüssen, der mit einem Storage-System mit zwei Anschlüssen über eine Fabric kommuniziert, vier Pfade sichtbar.

Es wird grob zwischen *Active/Active-*, *Asymmetric Active/Active-* und *Active/Passive-* sowie *Active/Standby-Systemen* unterschieden.

Active/Active

Ein *Active/Active-System* bietet die Möglichkeit, auf allen Anschlussports des Storage Area Networks mit gleicher Geschwindigkeit und zur gleichen Zeit auf die vom Storage-System bereitgestellten Ressourcen zuzugreifen.

Dies ermöglicht zum einen die Ausfallsicherheit über die Controller, zum anderen aber auch die gleichzeitige Nutzung mehrerer Pfade zu den LUNs, was eine höhere Leistung und Lastverteilung bedeutet.

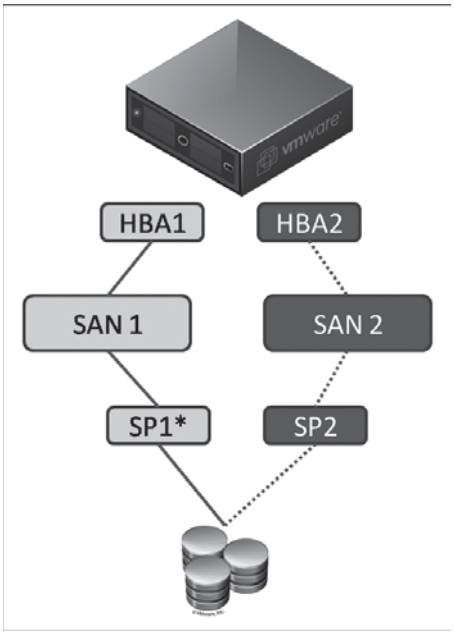


Abbildung 9.11 Active/Active-Speichersystem

Beim Pfadmanagement beginnen viele Hersteller, die Tatsachen etwas zu beschönigen, da Mischvarianten existieren, die zwar das beste Preis-Leistungs-Verhältnis bieten, allerdings nicht dem entsprechen, was man erwarten würde. Wer sich mit den verschiedenen Speichersystemen und Controller-Architekturen auskennt, weiß mit Sicherheit bereits, wovon ich rede: *Asymmetric Active/Active* oder *Pseudo-Active/Active*

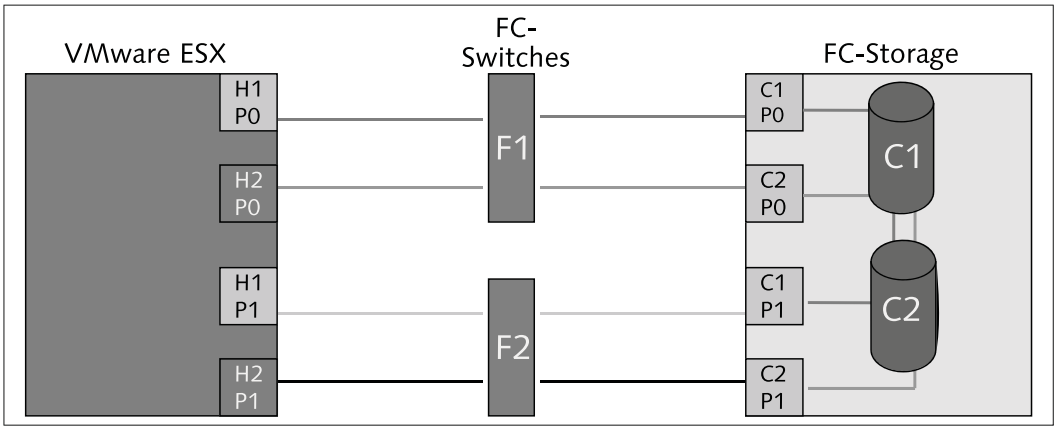


Abbildung 9.12 Active/Active-Anbindung in der Praxis

Die meisten vollwertigen *Active/Active-Systeme* sind im High-End- und damit auch Höchstpreissegment zu finden, wie HDS USP, EMC DMX, 3PAR oder IBM DS8000. Eine Ausnahme

existiert mit der Hitachi-AMS2000-Reihe (Hitachi Adaptable Modular Storage 2000 Family), die im Mid-Range-Bereich ebenfalls ein vollwertiges *Active/Active* liefert.

Active/Passive

Im Gegensatz zu *Active/Active-Systemen* können die Storage-Prozessoren der *Active/Passive-Systeme* nicht gleichzeitig auf eine RAID-Gruppe und deren LUNs zugreifen und diese im SAN bereitstellen. Der aktive Storage-Prozessor ist der Eigner (Owner) der LUN und steuert alle Zugriffe. Allerdings übernimmt der passive Storage-Prozessor bei Ausfall des aktiven Storage-Prozessors dessen Funktion (Trespassing) und dessen RAID-/LUN-Zugriff. Dieser Trespassing-Vorgang kann mehrere Sekunden dauern.

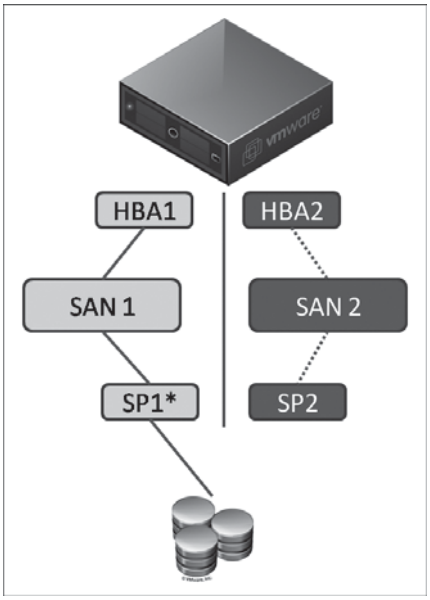


Abbildung 9.13 Active/Passive-Speichersystem

Daher ist nur ein manuelles Load-Balancing möglich, aber die Ausfallsicherheit ist gewährleistet. Normalerweise existieren Path-Management-Anwendungen wie EMC PowerPath/VE, um die Pfadnutzung zu optimieren und ein sogenanntes Path-Trashing zu verhindern.

Path-Trashing bedeutet, dass auf eine LUN über den Pfad des passiven Storage-Prozessors zugegriffen wird. Dieser Zugriff kann allerdings nicht direkt an die LUN erfolgen, sondern entweder einen internen Umweg über den LUN-Eigner machen oder ist schlichtweg nicht möglich.

Um dieses Path-Trashing zu verhindern, schalten viele Storage-Systeme den Eigner auf den zugreifenden Storage-Prozessor um, damit der Host bedient werden kann. Diese Schutzfunktion steht bei ESX-Hosts jedoch unter keinem guten Stern, da der gleichzeitige Zugriff vieler Hosts über verschiedene Pfade auf eine LUN möglich und realistisch ist.

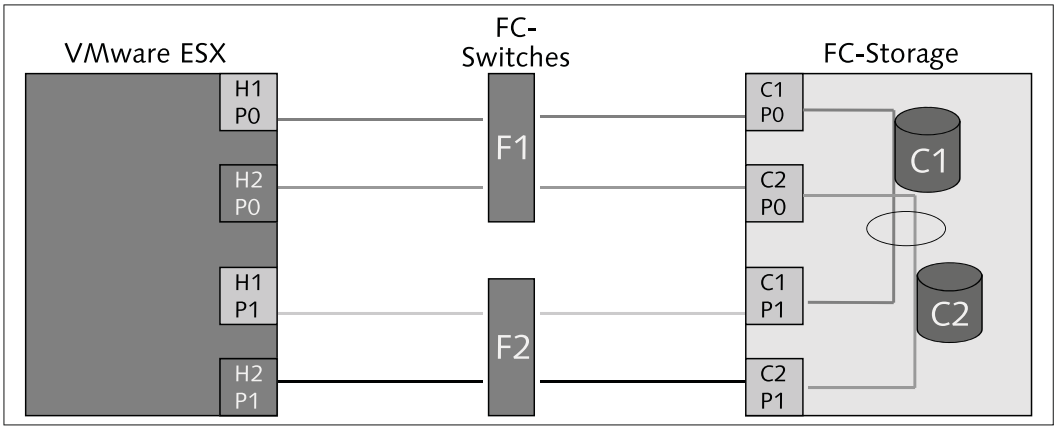


Abbildung 9.14 Active/Active-Anbindung in der Praxis – Anbindung innerhalb des Storage beachten

Dadurch schwenkt das Storage-System stetig den Eigner in Richtung Pfadnutzung, was die Leistung des Storage-Systems enorm senkt. Daher ist es sehr wichtig, die vorgeschriebenen Multipathing-Einstellungen und das Zoning im SAN zu beachten, um das Path-Trashing zu verhindern.

Zumeist ist die Empfehlung bei *Active/Passive-Systemen*, MRU (Most Recently Used) zu nutzen.

Pseudo-Active/Active

Pseudo-Active/Active oder *Active/Active Asymmetric* ist eine Zwitterform zwischen *Active/Active* und *Active/Passive*. Zwar bieten alle Frontend-Anschlüsse (in Richtung ESX-Host) die Möglichkeit, gleichzeitig auf die vom Storage-System bereitgestellten Ressourcen zuzugreifen, allerdings ist die Geschwindigkeit der einzelnen Anschlüsse unterschiedlich.

Dies kommt daher, dass wie beim *Active/Passive-System* Ressourceneigner (= LUN-Owner) existieren, womit nur einer von zwei Storage-Prozessoren die volle Geschwindigkeit erreichen kann, während der zweite immer über den Eigner auf die LUNs zugreifen muss, was zu teilweise sehr deutlichen Leistungsengpässen führt.

ESX 3.x hat keinerlei Möglichkeiten, die vom Storage kommenden Pfade zu klassifizieren und der Geschwindigkeit nach einzuordnen. vSphere geht dieses Problem mit 3rd-Party-Multipathing und ALUA an.

Pseudo-Active/Active-Systeme sind im Entry- als auch im Mid-Range-Level zu finden. Ein kleiner Auszug, es sind wesentlich mehr:

- EMC CLARiiON (nur bei entsprechender Konfiguration, ansonsten *Active/Passive*)
- HP EVA
- NetApp

- LSI und IBM DS (Ausnahme 8000er-Serie)
- Pillar Data Systems AXIOM

Bei all diesen Systemen sollten Sie beim Einsatz von VMware ESX die Nutzung des langsameren (nicht-optimalen) Pfads möglichst vermeiden, entweder durch entsprechendes SAN-Design und Hilfsprogramme oder durch die Integration von 3rd-Party-Multipathing-Module (EMC PowerPath/VE). Außerdem bringt VMware vSphere das ALUA (Asymmetric LUN Unit Access) Path Management mit, das u. a. von NetApp-Systemen unterstützt wird.

ALUA ermöglicht die Kommunikation zwischen Storage und ESX-Server, indem der Status der Pfade (*active-optimized*, *active-unoptimized*, *unavailable*, *standby*) übermittelt wird. Damit kann der ESX-Server die optimierten Pfade bevorzugt behandeln.

9.6 FC-Speichernetzwerk

Schauen wir uns den Aufbau des Fibre-Channel-Netzwerks einmal aus 10.000 Meter Höhe an, das heißt, wir kratzen nur die Oberfläche der Technologie und des Designs an. Ein sehr gutes, tiefgehendes Buch zum Thema Storage nennt sich »Speichernetze« und ist beim dpunkt.verlag erschienen (ISBN: 978-3-89864-393-1).

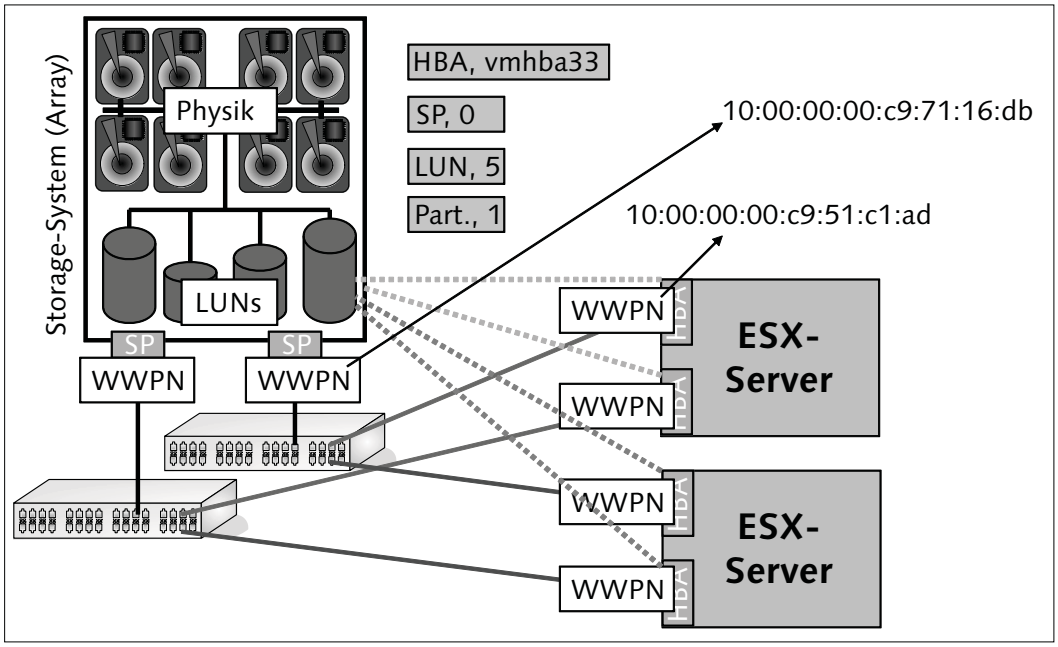


Abbildung 9.15 Beispiel eines Fibre-Channel-Netzes mit den einzelnen Komponenten

9.6.1 Vorteile und Nachteile

- **Vorteile von FCP**
  - hohe Geschwindigkeiten möglich
  - niedrige Latenzen
  - niedrige CPU Belastung am Host
  - Load-Balancing und Failover einfach realisierbar
  - Raw Device Mappings sind möglich

- **Nachteile von FCP**
  - relativ hohe Kosten durch Infrastruktur
  - eventuell fehlendes Know-how
  - Skalierbarkeitsprobleme mit LUN-SCSI-Locking bei VMFS (viele VMs pro Datastore)
  - Umgang mit LUN-Clones teilweise komplizierter als NFS (Resignatur)
  - VMFS-Datastores nicht verkleinerbar
  - Thin Provisioning nicht per Default

9.6.2 Support Matrix

Gerade im Zusammenhang mit Fibre-Channel sei ausdrücklich darauf hingewiesen, dass Sie sich unbedingt an die Supportmatrix aller beteiligten Hersteller halten sollten. Besonders zu berücksichtigen sind dabei folgende Hersteller:

- Server-Hersteller
- HBA-Hersteller
- Switch-Hersteller
- Storage-System-Hersteller

Alle Komponenten müssen füreinander zertifiziert und freigegeben sein, und Sie müssen auch auf die eingesetzten Software- und Firmwarestände achten. Obwohl Fibre-Channel seit vielen Jahren auf dem Markt etabliert ist, hat der Standard in puncto Interoperabilität noch nicht ganz das Niveau von LAN-Komponenten erreicht. Beim LAN geht man meist davon aus, dass jede LAN-Karte mit jedem Switch funktioniert, doch diese Selbstverständlichkeit ist im SAN noch nicht gegeben. Selbst zertifizierte HBA-Karten können – je nach Firmwareversion – im einen Fall funktionieren, im anderen jedoch nicht.

Wichtige Datenbank zu Herstellerfreigaben

Sie müssen daher zwingend auf die Freigaben der Hersteller achten. VMware hat für vSphere eine eigene Datenbank für die Freigabe von Speichersystemen und I/O-Karten (SAN und LAN) im Internet bereitgestellt. Sie finden diese Freigabematrix unter: *http://www.vmware.com/go/hcl*

Zusätzlich zur Freigabe der Hersteller sollten Sie darauf achten, dass die Anbindung des Storage-Systems zwingend redundant erfolgt (z. B. durch Multipath-I/O) und das Speichersystem selbst auch redundant ausgelegt ist (z. B. Clustering). Der Redundanzaspekt ist bei virtueller Infrastruktur genauso hoch oder noch höher als bei normaler Speicherzentralisierung – die Verfügbarkeit aller VMs hängt direkt von der Verfügbarkeit des Speichersystems ab.

9.6.3 Switch vs. Loop

VMware ESX unterstützt bis auf wenige Ausnahmen nur Switched-Fabric-Umgebungen im FC-Umfeld. Manche Systeme wie z. B. HP MSA können auch direkt an die FC-Adapter des ESX-Servers angeschlossen werden. Ein Arbitrated Loop, also die »Hub«-Version von Fibre-Channel, ist durch VMware nicht unterstützt, da es im FC-Umfeld als veraltet gilt.

9.6.4 Fabric

Fabric wird ein abgegrenztes Netzwerk genannt, das Intitiatoren (Hosts, Workstations) mit Targets (Storage-Systeme, Tape-Library) verbindet. Eine Fabric kann über mehrere FC-Switches verbunden sein.

Zumeist werden zwei oder mehr Fabrics im FC-Umfeld eingerichtet, um die FC-»Broadcasts« im kleinsten Rahmen zu halten (ähnlich Ethernet) und außerdem eine klare Trennung für Wartungsfenster herzustellen.

Ein besonderer Vorteil der FC-Fabric ist, dass alle Geräte mit voller Bandbreite senden und empfangen können. Die HBAs der ESX-Server sind in diesem Fall mit einem oder mehreren Pfaden zu Fabric1 und Fabric2 verbunden, so dass im Wartungsfall einer Fabric die Verbindung zum Storage-System immer noch über die verbleibende Fabric zur Verfügung steht.

9.6.5 Verkabelung

Prinzipiell versucht man immer, über Kreuz zu verkabeln, was besonders bei *Active/Passive-* und *Asymmetric Active/Active-Systemen* sehr sinnvoll ist, um die Zuordnung von aktiven Ports über die Fabrics zu verteilen. In Abbildung 9.16 sehen Sie dies bei der Verbindung zur EMC CX. Setzen Sie ein vollwertiges *Active/Active-System*, wie im Beispiel die HDS AMS2000, ein, so ist die Verkabelung eher Geschmackssache als wirklich notwendig.

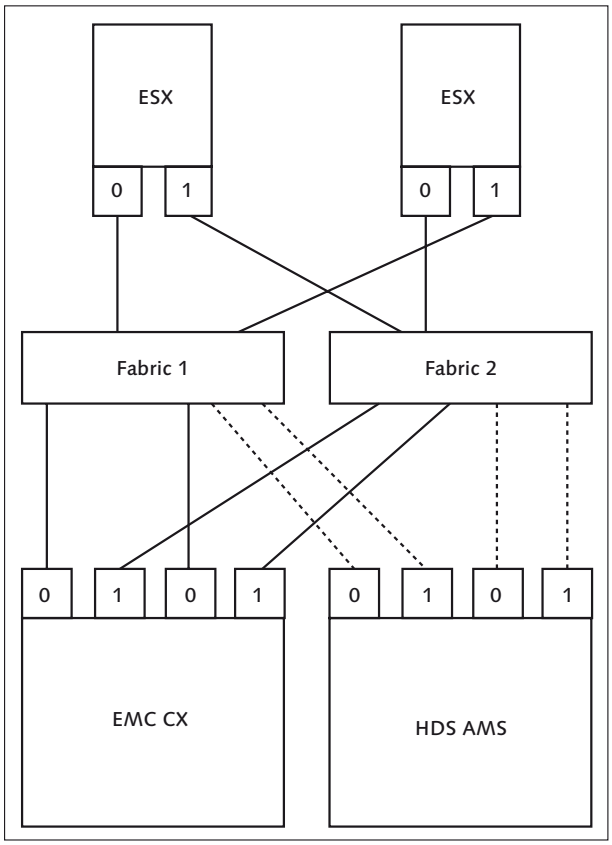


Abbildung 9.16 Verkabelungsmöglichkeiten

9.6.6 Zoning

Zoning nennt sich die Aufteilung der FC-Ports eines FC-Switches, ähnlich der VLANs im Ethernet-Segment. Mittels Zoning erstellen Sie Gruppen, die eine Kommunikation zwischen den enthaltenen Ports oder WWNs ermöglichen. Das Erstellen von Zonen, die auf Ports basieren, nennt sich *Port-Zoning*, das heißt, man fasst FC-Ports zur Kommunikation zusammen. Damit können Sie auch einen Systemwechsel oder Hardwaretausch ohne erneute Änderung an den SAN-Zonen durchführen.

Dies steht im Gegensatz zum *WWN-Zoning*, wo die WWNs, also die eindeutigen Identifikationsnummern des Ports oder des Systems, in Gruppen zusammengefasst werden. Dies hat den Vorteil, dass der HBA mit einer erlaubten WWN auf einem beliebigen Port auf dem FC-Switch angeschlossen werden kann. Kommt es jedoch zu einem Hardwareaustausch, müssen Sie auch das Zoning anpassen.

Zumeist ist Port-Zoning wegen der vereinfachten Verwaltung bei Hardwareaustausch beliebter.

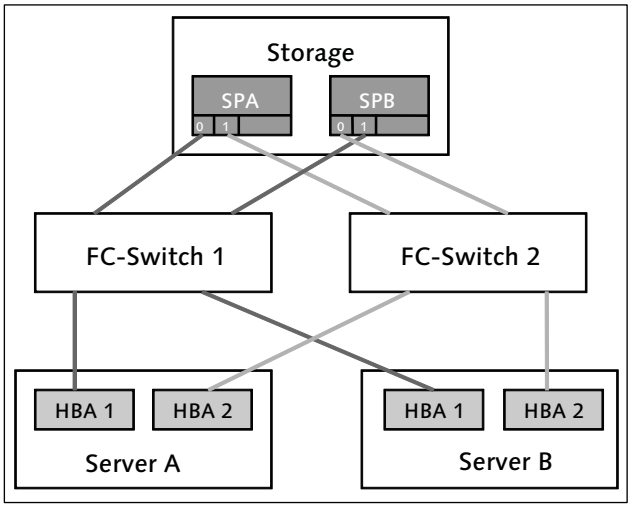


Abbildung 9.17 Zoning-Beispiel

Abbildung 9.17 zeigt, dass jeweils zwei Zonen auf jedem FC-Switch angelegt werden müssen. Dies wäre bei Single-Initiator-Zoning wie in Tabelle 9.3 zu konfigurieren.

FC-Switch	Zonenbeschreibung
FC-Switch 1	Server A, HBA 1 ⇔ Storage SPA Port 0
	Server A, HBA 1 ⇔ Storage SPB Port 1
FC-Switch 1	Server B, HBA 1 ⇔ Storage SPA Port 0
	Server B, HBA 1 ⇔ Storage SPB Port 1
FC-Switch 2	Server A, HBA 2 ⇔ Storage SPA Port 1
	Server A, HBA 2 ⇔ Storage SPB Port 0
FC-Switch 2	Server B, HBA 2 ⇔ Storage SPA Port 1
	Server B, HBA 2 ⇔ Storage SPB Port 0

Tabelle 9.3 Single-Initiator-Zoning

VMware empfiehlt übrigens mindestens vier Pfade zu einem Storage-System.

Single-Initiator-Zoning

Beim Single-Initiator-Zoning wird pro Zone immer nur ein Initiator mit einem oder mehreren Targets verbunden. Das heißt, ein ESX-Server mit zwei FC-Anschlüssen muss in wenigstens zwei Zonen mit dem oder den Targets verbunden werden.

Diese Form des Zonings ist beim Einsatz von VMware äußerst empfehlenswert, um FC-Broadcasts zu limitieren. Außerdem ist es nie sinnvoll, dass sich mehrere Initiatoren »sehen« und miteinander kommunizieren können. Ignorieren Sie das Single-Initiator-Zoning und erstellen

Sie eine Zone mit vielen Initiators und Targets, so stört möglicherweise nur eine fehlerhafte Komponente jegliche Kommunikation in der Zone, was zum Ausfall der Storage-Verbindung führen kann.

9.6.7 Mapping

Unter dem Begriff *Mapping* versteht man die Zuordnung von Initiator-WWNs zu LUNs des Targets.

Beim Mapping wird übrigens auch die LUN-ID festgelegt. Nur wenige Storage-Systeme wie beispielsweise Dell EqualLogic verwenden immer die LUN-ID 0 (dafür verschiedene Targets). Das Mapping wird im Storage-System durchgeführt und sieht zum Beispiel wie in Tabelle 9.4 aus.

Initiator	Target	LUN	LUN-ID	Zugriff
WWN ESX1	WWN-Target	400-GB-LUN	10	R/W
WWN ESX2	WWN-Target	400-GB-LUN	10	R/W

Tabelle 9.4 Mapping im Storage

Da viele Funktionen der virtuellen Infrastruktur nur bei gemeinsamem Zugriff mehrerer ESX-Server auf die gleichen LUNs möglich sind, ist es sinnvoll, die entsprechenden ESX-Server einer Gruppe zuzuordnen und diese beim Mapping zu verwenden. Damit ist gewährleistet, dass keine unterschiedlichen LUN-IDs für die gleiche LUN verwendet werden, was in VI3-Umgebungen schnell zum Chaos führt.

9.6.8 NPIV (N-Port ID Virtualization)

In der Historie des Fibre-Channel-Protokolls existierten immer Punkt-zu-Punkt-Verbindungen zwischen HBA und Switch (Netzwerk). Ein FC-Port hatte eine eindeutige WWPN (World Wide Port Number) und ein FC-Host eine eindeutige WWN (World Wide Number), über die die Kommunikation adressiert wurde. Das Konzept war bis zur Einführung der Virtualisierung auch für die meisten Installationen absolut ausreichend.

Durch die Virtualisierung und die Mehrfachbelegung der FC-Ports durch virtuelle Maschinen wurde eine entsprechende Technologie gesucht und mit NPIV (N-Port ID Virtualization) entwickelt. Somit war es auch problemlos möglich, einer virtuellen Maschine die Festplatten einer anderen virtuellen Maschine zuzuordnen. Aus Sicherheitsaspekten ist NPIV daher sinnvoll, da einer virtuellen Maschine eine LUN direkt zugeordnet werden kann. Nur der ESX-Host muss noch Read-only-Berechtigung besitzen. Dies verhindert Fehlkonfiguration oder nicht autorisierte Zugriffe auf die LUNs. Als Nachteil muss ganz klar aufgezeigt werden, dass die virtuelle Maschine »direkten« Zugriff auf den Storage bekommt und daher theoretisch per Schadsoftware Schäden anrichten könnte.

NPIV bedeutet, dass, wenn HBA und Switch diese Technik unterstützen, mehrere WWPNs auf einem HBA-Switch-Port genutzt werden können. VMware ESX unterstützt seit Version 3.5 die NPIV-Funktion, mit der Sie virtuellen Maschinen bis zu vier virtuelle WWNs zuweisen können. Allerdings ist die Funktion noch nicht komplett implementiert, das heißt, die virtuellen WWNs werden nach wie vor vom VMkernel verwaltet, da noch keine virtuellen Fibre-Channel-Karten im Gast möglich sind. Bis dahin hat die NPIV-Nutzung hauptsächlich Sicherheitsvorteile; Path-Management-Tools im Gast können nach wie vor nicht verwendet werden.

9.7 FCoE

Fibre-Channel over Ethernet wurde entwickelt, um die Kompatibilität mit Fibre-Channel zu behalten, jedoch auf die flexible Ethernet-Basis umstellen zu können. Da Ethernet und Fibre-Channel über komplett getrennte Infrastrukturen verfügen mussten, ist der Schritt zu FCoE eine deutliche Vereinfachung für Architekten und Administratoren, um beide Technologien zusammenzuführen.

Damit wird die Verkabelung vereinfacht und reduziert, und Sie können eine weitere Konsolidierung im Rechenzentrum betreiben. Dabei gilt allerdings zu beachten, dass die FC Pakete nicht routingfähig sind und auch nicht in IP-Pakete gepackt werden, um diese routingfähig zu machen, wie dies bei iSCSI der Fall ist. Durch den Verzicht auf die Nutzung von Transportschichten wie TCP/IP und den damit verbundenen Overhead profitieren Sie von einer verbesserten Performance.

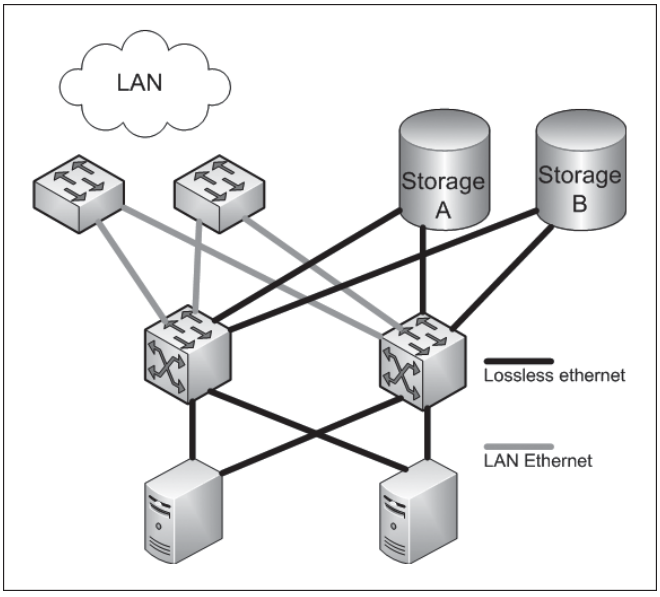


Abbildung 9.18 FcoE-Übersicht (Quelle: Autor Abisys, http://de.wikipedia.org/w/index.php?title=Datei:Storage_FCoE.png)

VMware unterstützte bereits mit vSphere 4.1 die FCoE-Hardwareschnittstellen (CNA) und hat diese Unterstützung mit vSphere 5 um einen Software-FCoE-Initiator erweitert.

9.8 iSCSI-Speichernetzwerk

Das iSCSI-Speichernetzwerk, oder auch IP-SAN genannt, ist neben dem FC-SAN die beliebteste Methode, zentralen Speicher an die ESX-Server zu koppeln. Statt WWN-/WWPN-Adressen zur eindeutigen Identifizierung im Fibre-Channel-Umfeld werden MAC-Adressen, IP-Adressen und iNames genutzt. Während MAC-Adressen eher auf Ethernet-Level Verwendung finden, sind IP-Adresse und iName zum Mapping des Storage notwendig. Zur Absicherung der Netzwerke können Sie mit eigenen physischen Switches oder VLANs arbeiten.

Zur Authentifizierung wurde CHAP (Challenge Handshake Authentication Protocol) als Protokoll integriert, was eine erste Sicherheitshürde bietet, da nur Systeme mit dem gleichen Schlüssel miteinander kommunizieren können. Die Integration einer Gesamtverschlüsselung mit IPsec (Internet Protocol Security) ist jedoch nicht möglich.

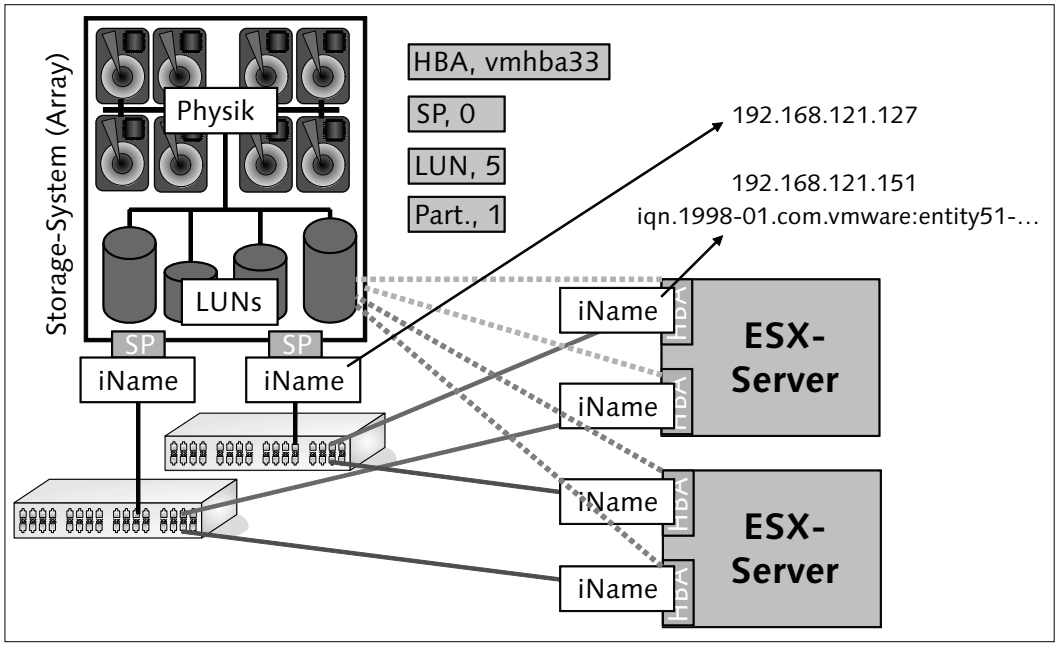


Abbildung 9.19 Komponenten im iSCSI-Netzwerk

Das sehr oft gewählte Argument, die Ethernet-Technologie sei im Gegensatz zu Fibre-Channel bereits bekannt und damit sei auch die iSCSI-Einführung in jedem Fall kostengünstiger, kann nicht immer bestätigt werden.

Zuallererst ist es wichtig, sich mit der iSCSI-Technologie auseinanderzusetzen, mit ihren Anforderungen, Stärken und Schwächen. Zweitrangig ist die Verwaltbarkeit des Ethernet-Switches oder der IP-Adressen. Im direkten Vergleich halten sich die Neuerungen von Standard-Ethernet nach IP-SAN oder FC-SAN eigentlich die Waage, da in beiden Technologien viele neue Themen beachtet werden müssen. Setzen Sie bereits FC-SAN ein, entfällt das Argument komplett.

Die Aussage »kostengünstiger« hängt sehr stark von den Anforderungen des Unternehmens an Leistungsfähigkeit und Ausfallsicherheit ab. Dazu sollten Sie sich Abschnitt 9.8.3, »IP-SAN-Trennung«, näher anschauen.

9.8.1 Vorteile und Nachteile

- **Vorteile von iSCSI**
  - mittlere bis hohe Geschwindigkeiten möglich, je nach Anzahl der 1 GBit/s Abschlüsse oder 10 GBit/s
  - mittelgute Latenzen
  - Load-Balancing und Failover einfach realisierbar
  - Raw Device Mappings sind möglich
  - sehr niedrige Einstiegskosten
  - relativ wenig Know-how erforderlich
- **Nachteile von iSCSI**
  - höchste CPU-Belastung am Host
  - Skalierbarkeitsprobleme mit LUN-Locking bei VMFS (viele VMs pro Datastore)
  - Umgang mit LUN-Clones teilweise komplizierter als NFS (Resignatur)
  - VMFS-Datastores nicht verkleinerbar
  - Thin Provisioning nicht per Default

9.8.2 Kommunikation

Die Kommunikation läuft aufgrund der SCSI-Verwandtschaft auch über Initiator und Target ab. Der Initiator kann entweder ein iSCSI-HBA, der Software-iSCSI-Initiator des VMkernels oder der Software-iSCSI-Initiator im Gastbetriebssystem sein.

In jedem Fall empfiehlt es sich, über den Einsatz von Jumbo-Frames (MTU bis 9.000 statt Standard MTU 1.500) nachzudenken, da dies eine Beschleunigung des Datenverkehrs aufgrund der größeren Netzwerkpakete und der sich damit verringernden Header-Informationen zur Folge hat. Generell wurde die iSCSI-Implementierung in vSphere seit ESX 4 wesentlich beschleunigt, was in Abbildung 9.20 sehr gut zu erkennen ist.

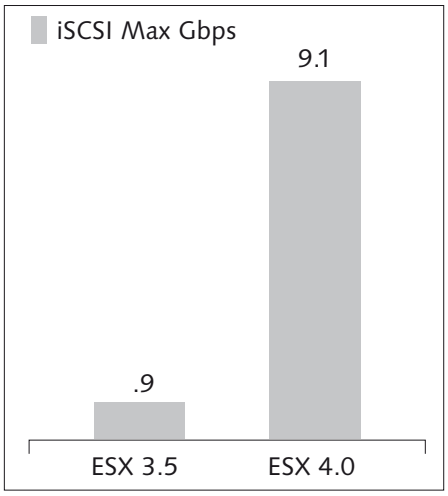


Abbildung 9.20 Verbesserungen mit ESX 4.0 im iSCSI-Netzwerk

Da unter ESX 5 keine Service Console mehr existiert, wird in jedem Fall ausschließlich der VMkernel Adapter für die iSCSI Verbindung genutzt. In Kapitel 8, »Netzwerk-Architektur«, finden Sie weitere Informationen, wie die entsprechende Netzwerkkonfiguration aussehen kann.

9.8.3 IP-SAN-Trennung

Selbst kleine Umgebungen von 20 VMs bekommen bei entsprechendem Leistungsbedarf schnell große Probleme bei der Performance, das iSCSI-Netzwerk nicht physisch vom produktiven IP-Netzwerk (LAN) getrennt ist.

In den meisten Fällen nützt auch keine Auftrennung mittels VLANs. Damit wäre zwar die Sicherheit der Pakete gewährleistet, aber nicht die Leistungsfähigkeit pro Port. Je nach eingesetzten Ethernet-Switches im LAN müssen Sie zusätzlich ein eigenes physisches Netzwerk mit eigenen Switches nur als Storage-Netzwerk aufbauen.

Sie sollten unbedingt auf eine entsprechend leistungsfähige Switch-Architektur achten, damit die Backplanes der Switches nicht an ihre Grenzen stößt und es nicht zu Leistungsengpässen beim Betrieb der Netzwerkinfrastruktur kommt. Dieses Thema sollten Sie auch sehr ernst nehmen, da es auch mit höherwertigen Switches im Preissegment von mehreren Tausend Euro zu erheblichen Problemen kommen kann.

Zwei solcher Fälle sind bekannt:

1. **Überbuchung**
   Der sehr einfach zu erklärende Fall ist das Overbooking von Switch-Ports, das heißt, die Backplane des Switches verfügt nicht über ausreichend Leistung, um alle Frontports mit voller Bandbreite gleichzeitig zu bedienen. Bei einem 24-Port-Switch beispielsweise, der

nur mit 12-GBit-Backplane ausgestattet ist, entsteht ein Problem bei Volllast. 24 Ports Full Duplex bedeuten maximal 48 GBit Last, was auf der 12-GBit-Backplane nur zu einem Viertel abgedeckt wird. Daher ist jeder Port dreimal überbucht. Achten Sie daher immer auf *non-blocking* beim Switch-Kauf achten.

2. **Lastverteilung**
   Ein sehr unschönes und nur schwierig festzustellendes Problem ist die mangelhafte Lastverteilung mancher Ethernet-Switches, die bei Volllast mehrerer Ports nicht anteilig verteilen, sondern wahllos auf Ports Last zulassen und verteilen. Dies führt im schlimmsten Fall dazu, dass Anwendungen nicht genügend Bandbreite zur Verfügung haben und es zu Applikationsabbrüchen im Sekundenbereich kommt.

   Auch hier ein kleines Beispiel: Es ist ein iSCSI-Storage-System mit einem GBit-Port auf einem Switch mit vier iSCSI-Initiatoren (ESX-Server) angeschlossen, die miteinander kommunizieren. Der Port des Storage-Systems erhält 90 % Last (*Utilization*), allerdings schwankt die Kommunikation der vier Initiatorenports aufgrund der Lastverteilungsprobleme des Switches zwischen 20 und 80 %. Im Ergebnis kommt es zu Applikationsproblemen auf den virtuellen Maschinen des ESX-Servers mit der geringsten zugeordneten Priorität, da Pakete zu langsam verteilt oder sogar verworfen werden.

   Die Backplanes kostengünstigerer Switches sind einfach nicht auf die Volllast aller Ports, sondern nur eines Bruchteils der Portvolllast ausgelegt. Damit würden das LAN und das IP-SAN sich gegenseitig stören, da die Switch-Backplane diese Leistung nicht erbringen kann.

   Selbst bei der Trennung der physischen Netzwerke mit eigenen Switches differenzieren die Leistungsanforderung und die Switch-Leistung stark voneinander. Nicht selten müssen daher Backbone-Switches angeschafft werden, um das iSCSI-Netzwerk, das zumeist höhere Anforderungen als die LAN-Kommunikation hat, vernünftig zu betreiben.

Solche Leistungsprobleme sind nicht immer leicht erkennbar, stellen sich aber oft durch »Hänger« in virtuellen Maschinen dar. Diese Stopps der Applikation in einer VM führen von der Verlangsamung der Anwendung für den Benutzer bis hin zum sporadischen Absturz der VM, da die iSCSI-Informationen nicht schnell genug umgesetzt werden können.

Daher ist es sehr wichtig, die Leistungsanforderungen genau zu bestimmen und ein entsprechendes Design der Ethernet-Infrastruktur aufzubauen. Sehr oft stellt sich heraus, dass sich Planungsschwächen viel schlimmer darstellen als bei Nutzung von FC-SAN. Durch die Einführung von 10-GBit-Ethernet wird sich das Performanceproblem nochmals relativieren, wenn die Backplane der Ethernet-Switches entsprechende Leistung vorhält – wird empfehlen an dieser Stelle einen Blick auf die Switches von Arista Networks (*http://www.aristanetworks.com*).

Übrigens findet sich eine sehr gute Abhandlung über die Möglichkeiten des iSCSI Netzwerkes und deren Implementierung auf dem Blog von Chad Sakac (Virtual Geek):

http://virtualgeek.typepad.com/virtual_geek/2009/09/a-multivendor-post-on-using-iscsi-with-vmware-vsphere.html.

9.9 Network-attached Storage

Vom notwendigen Aufbau des Netzwerks unterscheidet sich NFS nur unwesentlich von iSCSI, das heißt, auch hier sollte ein Speichernetzwerk dediziert genutzt werden, und der VMkernel stellt die Verbindung zum NFS-Storage her.

Allerdings arbeitet NFS nicht blockorientiert, sondern dateiorientiert, NFS nutzt also kein VMFS im Backend. Die Erklärung liegt schon im Namen, »Network File System« (NFS). Im Endeffekt ist es dem Storage-System überlassen, welches Dateisystem im Hintergrund die Dateien verarbeitet und organisiert, für den ESX-Server ist nur interessant, dass über NFS-Version 3 mit ihm kommuniziert wird.

NFS arbeitet im Gegensatz zu den blockorientierten VMFS-Datastores immer im Thin-Provisioning-Modus (Ausnahme VAAI-Nutzung), das heißt, nur die real abgespeicherten Daten verbrauchen im NFS wirklich Festplattenplatz, unabhängig von der angegebenen VMDK-Festplattendatei der virtuellen Maschine. Darüber hinaus ist es bei der Nutzung des standardisierten NFS-Protokolls möglich, von jedem anderen NFS-Client auf die NFS-Freigaben zuzugreifen, was Sicherungen sehr flexibel und einfach macht. Da auch das NAS-Storage-System selbst in der Lage ist, die Daten einzusehen, existieren auch dort sehr mächtige Sicherungsmöglichkeiten (z. B. NetApp Filer).

Ein weiterer Vorteil von NFS besteht darin, dass keine SCSI-Reservations auf dem kompletten Datastore (LUN) ausgeführt, sondern nur sogenannte File-Locks angewendet werden. Dadurch werden nur die im Zugriff befindlichen Dateien gesperrt und nicht die komplette LUN, was NFS eine sehr gute Flexibilität und Skalierbarkeit einbringt. Diese Vorteile werden besonders in großen VDI-(Virtual Desktop Infrastructure-)Umgebungen geschätzt, wodurch sich NFS in diesem Anwendungsbereich auch durchsetzt.

Kommunikation

Bei der Kommunikation von NFS handelt es sich um ein Client-Server-Protokoll, das heißt, der NFS-Client verbindet (authentifiziert) sich mit dem NFS-Server und beginnt eine Standardkommunikation, die für NFS-Version 3 vordefiniert ist. Ein sehr wichtiger Aspekt ist dabei die Nutzung von IP-Adressen oder DNS-Namen, wobei IP-Adressen meist bevorzugt werden, um die Abhängigkeit vom DNS-Server zu minimieren. Da es bei NFS kein Multipathing gibt, sind Sie auf die Möglichkeiten des Storage-Systems angewiesen, intern Cluster abzubilden. Dies ist meist über Round-Robin-Mechanismen, MAC-adressen-basiert oder IP-basiert möglich. Das Gleiche gilt für die Load-Balancing-Möglichkeiten.

Ein großes Problem ist hierbei, Ausfallsicherheit und Lastverteilung abzuwägen, wie es bei den blockbasierten Protokollen durch Multipathing möglich ist. Hier entscheiden die Anzahl der Netzwerkports und die Möglichkeiten der Ethernet-Switches darüber, wie weit Sie gehen können. Auch hier brillieren Arista Networks mit ihren kostengünstigen 10-GBit-Switches, die eine Port-Aggregation über Switch-Grenzen erlauben. Dies ist bei anderen Herstellern nur mit vielfach teureren Switches möglich.

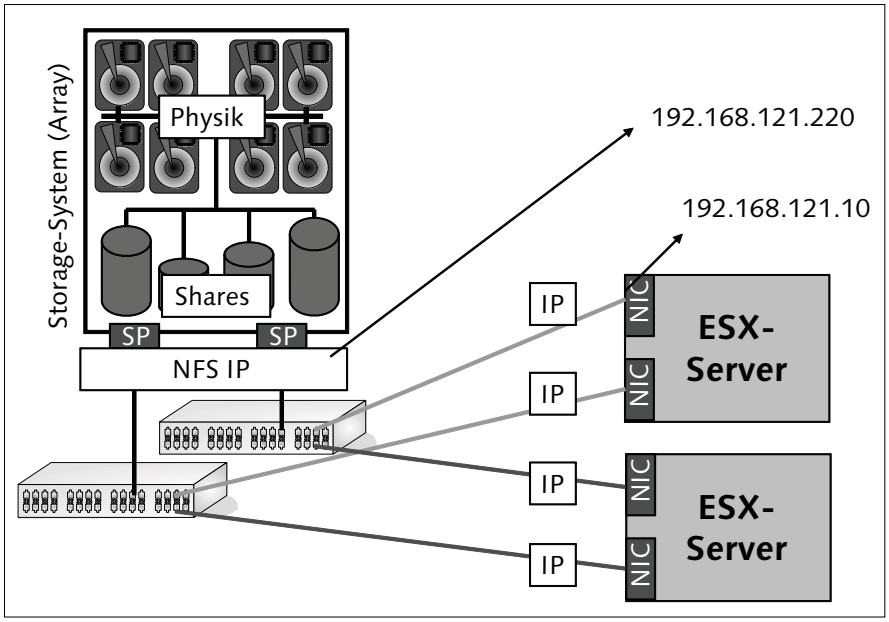


Abbildung 9.21 Komponenten bei NFS-Nutzung

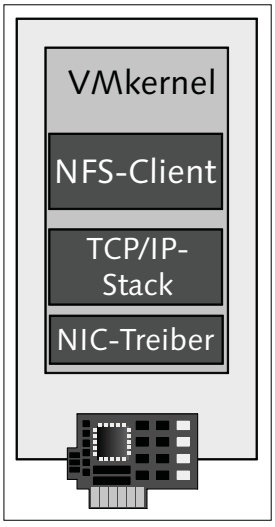


Abbildung 9.22 NFS-Modul VMkernel

In jedem Fall empfiehlt es sich, über den Einsatz von Jumbo-Frames (MTU bis 9.000, statt Standard MTU 1 .500) nachzudenken, da dies aufgrund der größeren Netzwerkpakete und der sich damit verringernden Header-Informationen eine Beschleunigung des Datenverkehrs zur Folge hat. Die Kommunikation findet über den VMkernel statt, der über das IP-hash-basierte Load-Balancing-Verfahren die Last verteilen kann.

Lastverteilung unter NFS

Eine Lastverteilung mit NFS ist auch bei IP-hash-basiertem Load-Balancing nur möglich, wenn dem ESX-Server mehrere IP-Adressen auf NFS-Server-Seite angeboten werden. Ansonsten würde der VMkernel-Port immer nur einen Adapter nutzen, da immer die gleiche Netzwerkkarte pro IP-Verbindung verwendet würde.

Durch die Nutzung von 10-GBit-Netzwerkkarten sind mit NFS enorme Geschwindigkeiten bei Datendurchsatz und Latenzzeiten möglich. Dies bringt weitere Marktdurchdringung für NFS und Entspannung, was die Verwendung von Load-Balancing auf ESX-Seite angeht.

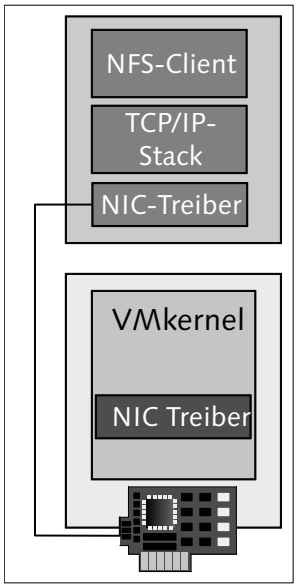


Abbildung 9.23 NFS im Gastbetriebssystem

Selbstverständlich ist es auch möglich, NFS-Systeme aus dem Gastbetriebssystem anzubinden und nur für eine dedizierte virtuelle Maschine zu nutzen. Der Netzwerkverkehr liefe in diesem Fall über die Portgruppe der virtuellen Netzwerkkarte ab. Um mehr Performance im Gast zu erreichen, müssten Sie mit mehreren virtuellen Netzwerkkarten und mehreren NFS-Servern arbeiten.

Vorteile und Nachteile

- **Vorteile von NFS**
  - mittlere bis hohe Geschwindigkeiten möglich, je nach Anzahl der 1 GBit/s Anschlüsse oder 10 GBit/s
  - mittelgute Latenzen
  - sehr niedrige Einstiegskosten

- relativ wenig Know-how erforderlich
- VMFS-Datastores sehr einfach verkleinerbar
- Thin Provisioning per Default
- sehr einfaches Management
- Zugriff auf die VMs mit jedem NFS-Client möglich (Backup)
- keine VMFS-Skalierungsprobleme

- **Nachteile von NFS**
  - Raw Device Mappings sind nicht auf NFS möglich
  - Load-Balancing und Failover schwieriger realisierbar, je nach eingesetzter LAN-Infrastruktur
  - wenige Sicherheitsfunktionen im Protokoll
  - bei Nutzung von 1 GBit geringere Geschwindigkeit als FC

9.10 Flash-basiert

Flash-basierte PCI-Express-Karten werden auch im VMware-Umfeld immer beliebter und sind seit Version 4.0 auch in der HCL fester Bestandteil. Der bekannteste Hersteller in diesem Umfeld ist Fusion-io, der auch bei IBM, HP oder Fujitsu als OEM-Partner hinter den Flash-basierten Beschleunigerkarten steckt.

Zwei dieser Karten (640 GB, MLC, Single Channel) konnten wir auch in unserer Buchumgebung testen, um ein Gefühl für die Geschwindigkeitsunterschiede zu bekommen und natürlich auch, um die Verwaltungsmöglichkeiten unter vSphere in diesem Buch erläutern zu können.

Die Fusion-io Karte ist schnell installiert, da sie nur in einen Server eingebaut und ein ESXi 5-Treiber installiert werden muss. Danach muss der ESX-Host neu gestartet werden, und die Flash-Karte präsentiert sich als Block-Device, also als SSD-Festplatte.

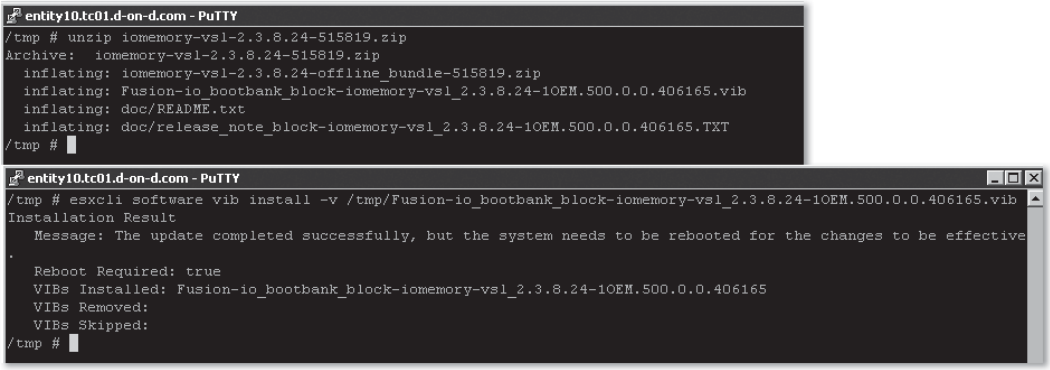


Abbildung 9.24 Installation des Fusion-io-ioMemory-Treibers

Sie müssen zwingend diesen Treiber (Abbildung 9.24) installieren, da Fusion-io bewusst aus Leistungsgründen auf die Implementierung eines SCSI-Stacks verzichtet hat.

Im nächsten Schritt können Sie sich zwischen drei Varianten der Nutzung entscheiden bzw. diese auch miteinander kombinieren.

1. als Datastore nutzen (Formatierung mit VMFS), um VMs und VMDK-Dateien abzulegen
2. VMDirectPath
3. als Host-Cache nutzen

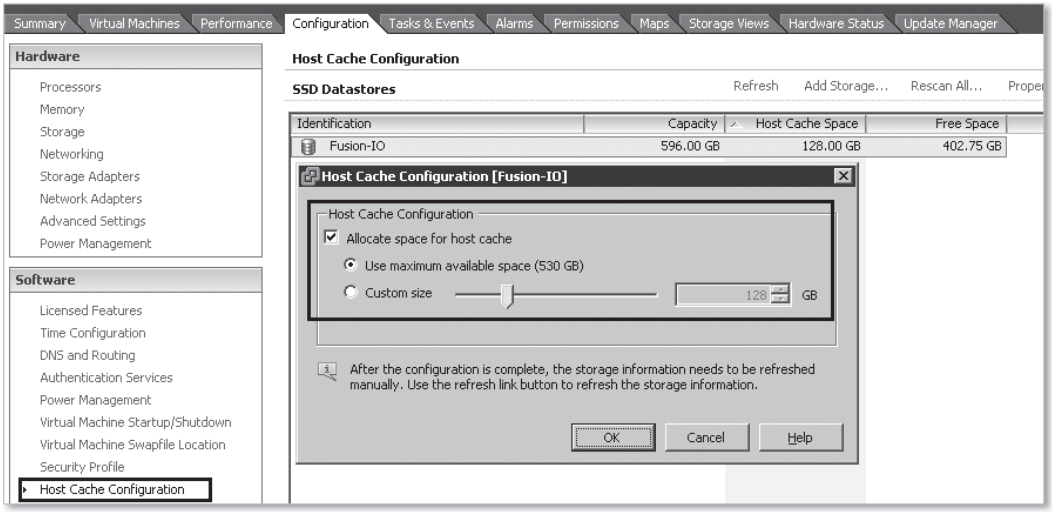


Abbildung 9.25 Nutzung der SSD-Datastores in Teilen oder im Ganzen als Host-Cache

Die Formatierung einer SSD oder Flash-Karte mit VMFS geschieht genau gleich wie bei einer normalen LUN oder SAS-Festplatte.

Variante 1 (VMFS) und 3 (Host-Cache) können Sie miteinander kombinieren, und per Schieberegler (Abbildung 9.25) stellen Sie die Nutzkapazität der SSD-Festplatte für die Auslagerungsdateien (*.vswp*) der VMs ein.

9.10.1 VMFS-Datastore

Variante 1 bietet natürlich den großen Vorteil, dass die darauf abgelegten virtuellen Maschinen einen deutlichen Leistungsschub bezüglich I/O-Durchsatz und Latenzzeiten erhalten. Variante 2 geht sogar einen Schritt weiter und lässt nur eine VM per RDM für den Zugriff zu, das heißt, dies wäre für leistungsfressende Datenbank-Server oder auch Webserver mit hoher I/O-Last interessant.

Stellen Sie sich die Frage der Ausfallsicherheit, so ist es korrekt, dass eine Flash-basierte PCIe-Karte kein Hardware-RAID-Level unterstützt, so dass Sie entweder auf Software-RAID in den Gastbetriebssystemen zurückgreifen oder Storage-Virtualisierer wie DataCore müssen, um Flash-Karten zu bündeln.

Oft ist es aber überhaupt nicht notwendig, die Datastores ausfallsicher aufzusetzen, da die Anforderungen der Anwendung dies nicht erfordern. Ein Beispiel wären Linked Clones in einer VMware-View-Umgebung.

Die Golden-Images (oder auch Master-VM, von welcher sämtliche Kopien, Linked Clones genannt, erzeugt werden) und die Linked Clones liegen auf dem SSD-Datastore, und wenn dieser ausfallen sollte, müssen sich die Anwender einfach neu anmelden und werden durch den Desktop-Pool mit einem neuen Server verbunden.

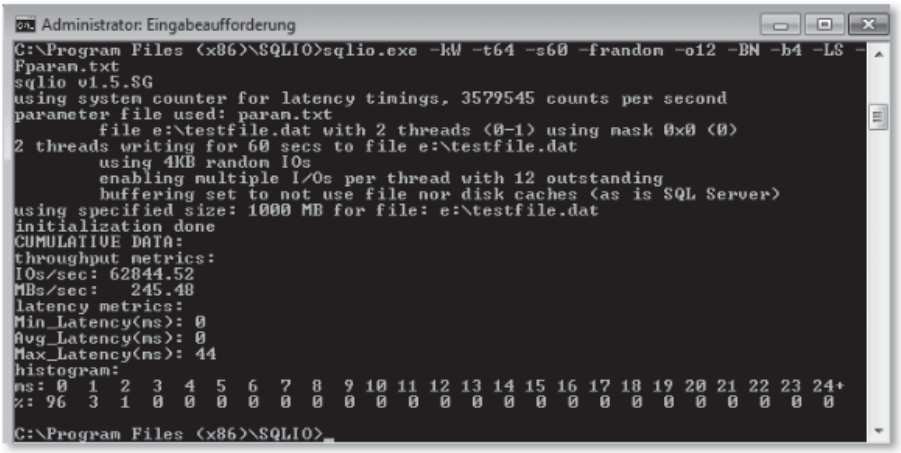


Abbildung 9.26 SQLIO-Test 4-KB-Blöcke Fusion-io ioDrive als VMFS-Datastore

9.10.2 VMDirectPath

Bei der zweiten Variante wird die Fusion-io-ioDrive-PCIe-Karte direkt einer VM mittels VMDirectPath zugeordnet. Dadurch erhält die virtuelle Maschine alleinigen und schnellsten Zugriff auf die Cache-Karte.

Auf dem ESX-Host muss die Cache-Karte aus der VMkernel-Nutzung ausgeschlossen werden, damit eine virtuelle Maschine auf das PCI-Gerät direkt zugreifen kann (Abbildung 9.27 und Abbildung 9.28).

Den Adapter können Sie jetzt in den Eigenschaften der VM als PCI-Gerät hinzufügen. Nach dem Start des Gastbetriebssystems sollte die Fusion-io-ioMemory-Software installiert werden, die eine Überwachung des Status und der Performance erlaubt.

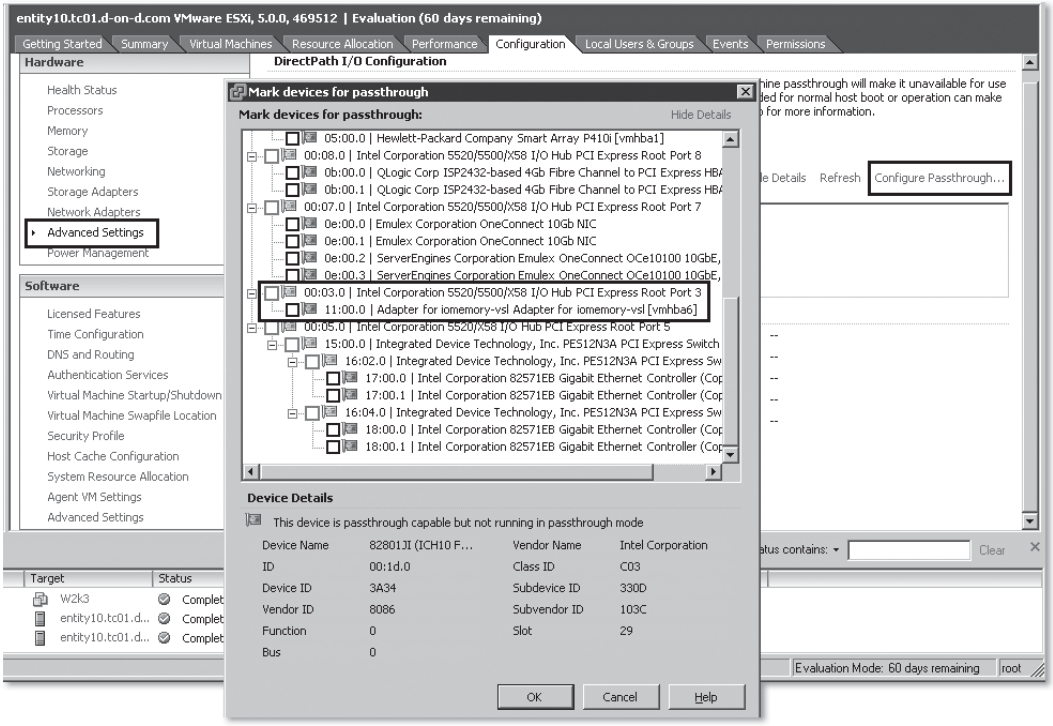


Abbildung 9.27 Auswahl der ioDrive-Karte

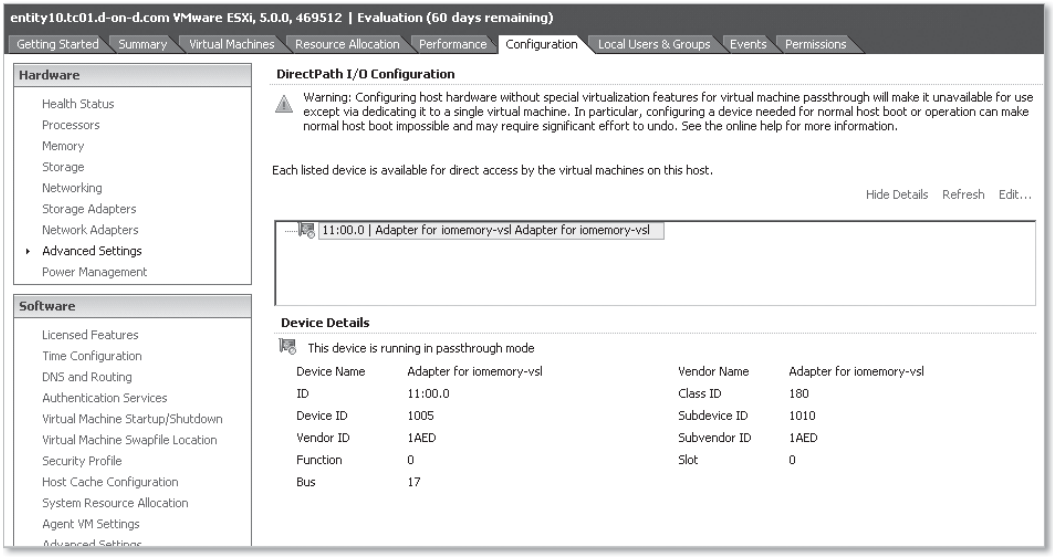


Abbildung 9.28 Zuordnung der ioMemory-vsl-Karte zu DirectPath-I/O

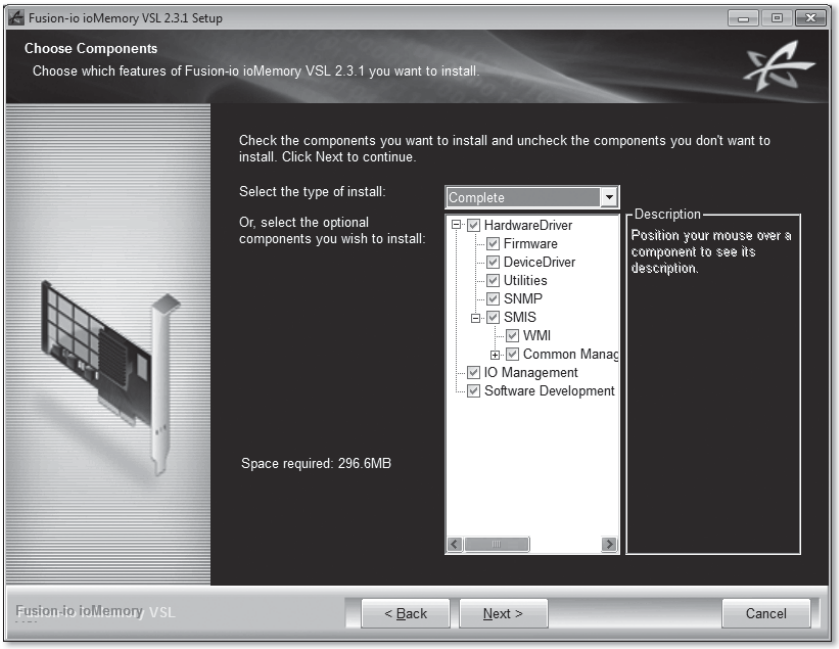


Abbildung 9.29 Installation der Fusion-io-ioMemory-Software unter Windows

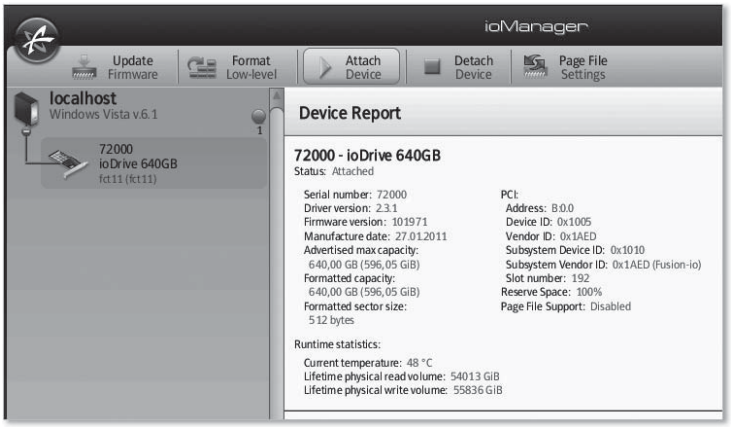


Abbildung 9.30 Ansicht im Gast (ioManager-Software für MS Windows)

Die getestete Leistung zeigte eine ungefähr 10 %ige Steigerung der I/O-Performance (bis zu 70.000 IOPS) gegenüber der Nutzung mit VMFS (ca. 63.000 IOPS) bei 4 KB Blockgröße.

9.10.3 Host-Cache

Variante 3 ist sehr interessant, da man die Flash-Karte anstatt der NFS-, iSCSI- oder FC-LUN des Storage-Systems nutzt, um im Falle eines Engpasses von physischem RAM die VM mittels

Auslagerungsdatei (*.vswp*) über den VMkernel zu versorgen. Dieses seit Jahren genutzte Verfahren vom Memory-Overcommitment, d. h., es wurde deutlich mehr Hauptspeicher an die virtuellen Maschinen vergeben als physisch vorhanden ist, kann mittels Host-Cache beschleunigt werden. Dies erleichterte die Ressourcenplanung und die Ausfallplanung.

Der VMkernel optimiert die Hauptspeichernutzung außerdem mit Memory-Ballooning, Memory-Compression sowie dem Transparent Page-Sharing (Content-based Memory-Sharing). Hat der VMkernel alle Möglichkeiten zur Optimierung ausgeschöpft und ist kein physischer RAM mehr verfügbar, so greift die letzte Instanz in Form der virtuellen Swap-Datei im Verzeichnis der VM. Da diese Swap-Datei auf dem im Vergleich zum RAM äußerst langsamen Datastore liegt, kann es zu massiven Geschwindigkeitseinbussen kommen.

Setzen Sie den Host-Cache ein, so wird statt der Swap-Datei im VM-Datastore die Swap-Datei der SSD-Karte genutzt, die zwar immer noch langsamer als der RAM ist, aber dennoch deutlich schneller (20–100 Mal schneller) als traditionelle Festplatten. Damit ist es möglich, den Geschwindigkeitsnachteil deutlich abzufedern und SSD-basierten Speicher als gangbare Alternative für Spitzen oder Ausfälle einzuplanen.

9.10.4 Fusion-io ioTurbine

Fusion-io hat mit der Software ioTurbine eine vierte Alternative entwickelt, die superschnelle Cache-Karte in virtuelle Infrastrukturen zu integrieren und aus jeder Server-Hardware deutlich mehr Leistung rauszuholen, um die Konsolidierungsrate VM:Server noch weiter zu erhöhen. Leider war ioTurbine zur Drucklegung des Buches nur für vSphere 4.x verfügbar und noch nicht für vSphere 5, daher konnten wir die Software nicht umfangreich testen.

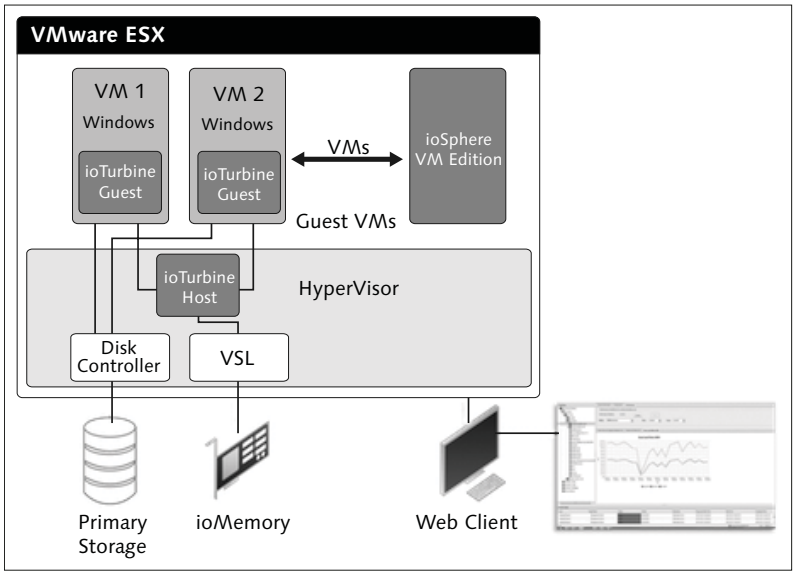


Abbildung 9.31 Integration von ioTurbine in VMware ESX und VMs

ioTurbine wird als VM betrieben (wird als virtuelle Appliance ausgeliefert) und integriert sich im Hypervisor (ESX/ESXi 4.x) und in die Gastbetriebssysteme (Microsoft Windows 2008 64-Bit, Microsoft Windows 2008 R2) der virtuellen Maschinen. Voraussetzung ist natürlich, dass in jedem ESX-Host, der von ioTurbine verwaltet wird, eine Fusion-io-ioDrive-Cache-Karte eingebaut ist.

ioTurbine optimiert den I/O der virtuellen Maschinen und priorisiert die Zugriffe der VMs. Durch die Sichtung der Dateisystemzugriffe im Gast und die Weiterleitung der I/O-Pattern auf die Cache-Karte entsteht ein sehr wirksamer Lese-Cache für jede überwachte virtuelle Maschine auf dem ESX-Host.

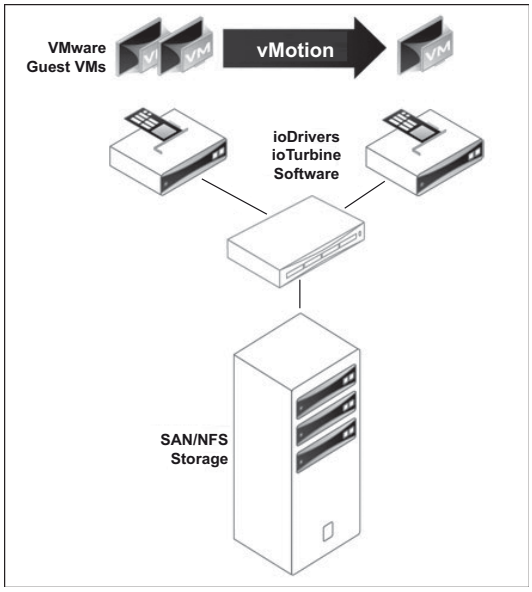


Abbildung 9.32 ioTurbine ist transparent zum ESX-Host, daher wird vMotion nicht gestört.

Da ioTurbine transparent für den ESX-Host funktioniert, wird vMotion nicht gestört, da der ESX-Host keine Nutzung lokaler Ressourcen zuordnet. Mit ioTurbine lassen sich daher Kosten im Storage-Backend einsparen, da viele Zugriffe nicht bis zum Storage-System durchgereicht werden müssen, was die Anzahl der benötigten Festplatten, um Durchsatz zu erzeugen, reduziert.

9.11 VMware-Storage-Architektur

VMware besitzt seit der ersten Version des ESX-Servers eine eigene Storage-Architektur und -Implementierung. Diese besteht aus den verschiedenen Storage- und Netzwerk-Stacks sowie eigenen Multipathing-Möglichkeiten. Außerdem wird das Dateisystem VMFS stetig weiterentwickelt und ist seit dem ersten vSphere-Release in Version 3.33 verfügbar.

Wer sich für eine Performancestudie zwischen VMware ESX 3.5 und ESX 4 bzw. zwischen FC, iSCSI und NFS unter VMware interessiert, sollte sich dieses Whitepaper einmal näher anschauen: *http://www.vmware.com/files/pdf/perf_vsphere_storage_protocols.pdf*

Neuere Dokumente zu ESX 5 waren zur Drucklegung noch nicht verfügbar.

9.11.1 VMkernel-Storage-Stack

Der VMware-Storage-Stack ist zuständig für die Anbindung der verschiedenen Datenträger, die Verwendung von SCSI-Protokollen und NFS sowie das Multipathing.

Speicherstack VMkernel

VMware ESX besitzt einen eigenen SCSI-Stack, der die Nutzung von lokalem und entferntem Storage (iSCSI, FC) möglich macht. Dieser Stack verfügt auch über eigene Queuing-Mechanismen und eigene Multipathing-Funktionen. Seit vSphere ist es allerdings auch für Drittherstellern möglich, eigene Multipathing-Funktionen in den VMkernel zu integrieren. Dazu wird die PSA (Pluggable Storage Architecture) genutzt.

TCP/IP-Protokoll VMkernel (vMotion, iSCSI)

Der VMkernel enthält neben dem Storage-Stack auch einen Netzwerk-Stack, der das TCP/IP-Protokoll unterstützt. Unter diesem VMkernel-Stack kommunizieren unter ESXi Management, vMotion, Fault Tolerance, NFS, die Software-iSCSI-Funktion und die Software-FcoE-Funktion. Da es sich bei TCP/IP um ein Standardprotokoll handelt, funktionieren auch Teile der Denial-of-Service-Attacken gegen dieses Protokoll. Daher sollten Sie diese Ports immer vom Netzwerk der virtuellen Maschinen und des produktiven LANs trennen. Dies ist z. B. mit VLANs für vMotion, iSCSI und Fault Tolerance möglich, ohne an Flexibilität bei den physischen Adaptern zu verlieren.

Multipathing

VMware setzte bis vSphere komplett auf die eigenen Multipathing-Möglichkeiten, das heißt, wenn mehrere Pfade zum Storage erkannt wurden, entschied VMware durch eigene Komponenten, wie damit umzugehen war.

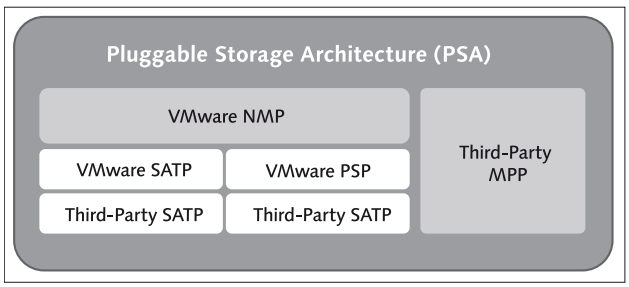


Abbildung 9.33 Multipathing unter vSphere

Zu den Multipathing-Komponenten gehören MPP (Multi-Path-Plugin, VMware-eigene und 3rd-Party-Plugin-Kontrolle), NMP (Native-Multipathing-Plugin, VMware-eigene Pfadkontrolle), SATP (Storage-Array-Type-Plugin, Failover-Kontrolle und Überwachung) und PSP (Path-Selection-Plugin), Lastverteilung, Pfadauswahl anhand Fixed, MRU oder Round-Robin).

Multipathing-Vorgang (Weg der I/Os)

1. Das NMP-Modul ruft das entsprechende PSP-Modul auf (Fixed, MRU oder RR).
2. PSP wählt den optimalen physischen Pfad aus, um die I/O zu versenden.
3. Wenn die I/O-Operation erfolgreich ist, gibt NMP dies zurück.
4. Wenn die I/O-Operation fehlschlug, wird ein SATP ausgewählt.
5. Wenn SATP den I/O-Fehler erkennt, wird bei Notwendigkeit ein inaktiver Pfad aktiviert.
6. PSP sendet die I/O über den neuen Pfad.

Multipathing-Module

Führen Sie auf der Konsole (oder im vCLI) des ESX-Hosts den Befehl `esxcli nmp satp list` aus, so erhalten Sie eine Übersicht über die verschiedenen integrierten Module und deren Funktion.

Modulname	Standard-PSP	Beschreibung
VMW_SATP_ALUA_CX	VMW_PSP_FIXED	Supports EMC CX that use the ALUA protocol
VMW_SATP_SVC	VMW_PSP_FIXED	Supports IBM SVC
VMW_SATP_MSA	VMW_PSP_MRU	Supports HP MSA
VMW_SATP_EQL	VMW_PSP_FIXED	Supports EqualLogic arrays
VMW_SATP_INV	VMW_PSP_FIXED	Supports EMC Invista
VMW_SATP_SYMM	VMW_PSP_FIXED	Supports EMC Symmetrix
VMW_SATP_LSI	VMW_PSP_MRU	Supports LSI and other arrays compatible with the SIS 6.10 in non-AVT mode
VMW_SATP_EVA	VMW_PSP_FIXED	Supports HP EVA
VMW_SATP_DEFAULT_AP	VMW_PSP_MRU	Supports non-specific active/passive arrays
VMW_SATP_CX	VMW_PSP_MRU	Supports EMC CX that do not use the ALUA protocol
VMW_SATP_ALUA	VMW_PSP_MRU	Supports non-specific arrays that use the ALUA protocol
VMW_SATP_DEFAULT_AA	VMW_PSP_FIXED	Supports non-specific active/active arrays
VMW_SATP_LOCAL	VMW_PSP_FIXED	Supports direct attached devices

Tabelle 9.5 VMware-Multipathing-Module

Die Multipathing-Policies Fixed und Most Recently Used (MRU) existierten schon seit vielen Versionen, während Round-Robin mit VMware ESX 3.5 experimentell Einzug erhielt. Seit vSphere ist Round-Robin offiziell unterstützt.

Abhängig vom Storage-Hersteller ist die entsprechende Policy auszuwählen, allerdings hat VMware auch eigene Tabellen hinterlegt, so dass bei vielen Storage-Systemen automatisch das korrekte Multipathing genutzt wird.

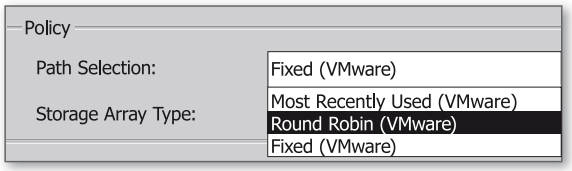


Abbildung 9.34 Multipathing von VMware

Fixed

Der angegebene bevorzugte Pfad wird immer genutzt, bis er ausfällt. Dann wird auf einen noch verfügbaren Pfad gewechselt. Ist der bevorzugte Pfad allerdings wieder online, so wird er direkt wieder genutzt. Fixed empfiehlt sich für manuelle Lastverteilung zwischen den Pfaden, birgt aber die Gefahr des »Ping-Pongs«, wenn der bevorzugte Pfad immer einmal wieder ausfällt, z. B. aufgrund eines Portproblems. Fixed Multipathing ignoriert ALUA (Asymmetric Logical Unit Access).

MRU

Most Recently Used empfiehlt sich bei den meisten *Active/Passive-Storage-Systemen*. Der große Nachteil an MRU ist, dass immer nur ein Pfad genutzt wird und Sie somit kein manuelles Load-Balancing einstellen können. MRU hat jedoch den Vorteil, dass immer nur beim Ausfall eines Pfades auf einen noch aktiven Pfad gewechselt und dort geblieben wird. Dadurch sind fehlerhafte Ports nicht so dramatisch wie bei Fixed. MRU ist ALUA-fähig und ist damit Fixed Multipathing bei *Asymmetric Active/Active-Systemen* vorzuziehen.

Round-Robin

Die neueste Form der Pfadverwaltung ist Round-Robin, das auf den Möglichkeiten eines *Active/Active-Arrays* aufsetzt. Der Pfad wird anhand der Anzahl von durchgeführten I/O-Operationen oder Datendurchsatz stetig gewechselt, wodurch eine sehr effektive Lastverteilung entsteht. Round-Robin ist bei *Active/Passive* nicht sinnvoll einsetzbar und wird daher nicht empfohlen.

Handelt es sich um einen *Asymmetric Active/Active-Storage*, so erkennt Round-Robin die optimalen Pfade mittels ALUA und benutzt die nicht-optimalen nur im Notfall.

3rd-Party-Multipathing

vSphere bringt eine komplett neue Storage-Architektur mit, die es Drittherstellern erlaubt, eigene Multipathing-Plugins zu integrieren. Dies ist auch von großem Vorteil, da der Storage-Hersteller seine eigenen Produkte am besten kennt. So können Sie mittels Hersteller-Multi-

pathing-Plugins ein Storage-System wesentlich performanter und optimaler anbinden. Zur Drucklegung des Buches war PowerPath/VE vom Hersteller EMC verfügbar. Außerdem hat VMware den Standard ALUA, auf den beispielsweise NetApp setzt, als Multipathing-Möglichkeit implementiert.

SCSI-Timeout

Aufgrund des möglichen Zeitverzugs beim Ausfall des aktiven Pfades und des damit verbundenen Wechsels auf einen neuen Pfad wird empfohlen, die SCSI-Timeout-Zeiten in Windows-Gastbetriebssystemen zu kontrollieren und gegebenenfalls neu zu setzen. Dies ist im VMware-Knowledge-Base-Artikel 1014 beschrieben: *http://kb.vmware.com/kb/1014*.

Der folgende Registry-Wert wird bei der Installation der VMware Tools automatisch auf 60 gesetzt und ist im Standard 30:

```
HKLM/System/CurrentControlSet/Services/Disk/TimeOutValue (REG_DWORD /180
  decimal)
```

Unter Linux müssen Sie nach der VMware-Tools-Installation eine UDEV-Datei manuell umkonfigurieren. VMware ESX 4 setzt den Wert direkt auf `180`, was im Normalfall ausreicht. Möchten Sie den Wert ändern, passen Sie die Datei */etc/udev/rules.d/99-vmware-scsi-udev.rules* an, indem Sie den `echo`-Wert in den `RUN`-Zeilen manipulieren:

```
RUN+="/bin/sh -c 'echo 180 >/sys$DEVPATH/device/timeout'"
```

Alternativ finden die Timeouts auch bei Red-Hat-basierten Systemen unter

`/sys/block/<disk>/device/timeout`.

9.11.2 Festplattendateien

Virtuelle Maschinen ohne Daten sind selten, daher sind die genutzten Festplattendateien natürlich äußerst wichtig, und Sie müssen wissen, wie diese angebunden werden und funktionieren. Die Standardfestplatten unter vSphere sind im VMFS-Umfeld vom Typ thick und im NFS-Umfeld vom Typ thin. Allerdings sind die Thin-Festplatten seit vSphere 4.x auch auf VMFS-Partitionen unterstützt.

2gbsparse

2gbsparse-Festplattendateien sind aus den VMware-Versionen Workstation und Server bekannt. Die Festplatte ist in maximal 2 GB große Stücke eingeteilt und wächst mit ansteigendem Datenvolumen in der Festplattendatei mit, das heißt, eine virtuelle 40-GB-Festplatte benötigt als 2gbsparse nicht zwingend reale 40 GB auf dem Datenspeicher, sondern nur die wirklich verbrauchten Daten.

monolithic sparse

Eine Monolithic-sparse-Festplatte wächst wie 2gbsparse dynamisch, ist allerdings nicht in 2-GB-Dateien aufgeteilt, sondern existiert als eine einzelne Datendatei. Dieses Format hat Nachteile in Sachen Mobilität, da bei 2gbsparse beispielsweise eine DVD als Backup-Medium genutzt werden könnte. Eine Monolithic-sparse-Platte hingegen kann sehr groß werden und müsste demnach umkonvertiert werden. Unter VMware ESX nennen sich diese Festplatten *thin*.

monolithic flat

Monolithic-flat-Festplattendateien sind leistungsfähiger als die Monolithic-sparse-Festplatten. Sie werden bei dem Anlegen in voller Größe erstellt, das heißt, eine 40-GB-Festplattendatei verbraucht 40 GB auf dem Datenspeicher. Außerdem ist die Datei nicht aufgeteilt, sondern als eine Datei vorhanden.

Des Weiteren existieren Festplattentypen, die nicht als Datei auf einem VMFS oder NFS angelegt werden, sondern als Verlinkung zu einer LUN über den direkten SCSI-Weg dienen. Das heißt, die LUN steht roh (Raw Device Mapping) der virtuellen Maschine zur Verfügung und kann nach Belieben genutzt werden (z. B. mit NTFS-Formatierung bei einer Windows-VM). Bei diesen Festplattentypen wird zwischen Physical und Virtual Compatibility Mode unterschieden. Physical wird nur gebraucht, wenn Cluster zwischen virtuellen und physischen Systemen benötigt werden.

Zu jeder Festplattendatei existiert seit Version 3.x des VMware ESX-Servers eine Beschreibungsdatei, die folgende Informationen enthält (Auszug):

```
# Disk DescriptorFile
version=1
CID=6a5e7aa0
parentCID=ffffffff
createType="vmfs"
# Extent description
RW 8388608 FLAT "test4mig2-flat.vmdk" 0
# The Disk Data Base
#DDB
ddb.adapterType = "lsilogic"
ddb.geometry.sectors = "63"
ddb.geometry.heads = "255"
ddb.geometry.cylinders = "522"
ddb.virtualHWVersion = "3"
```

Die Einträge haben folgende Bedeutung:

- **`version`**
  `version` gibt die Version der Beschreibungsdatei an. Derzeit verwendet VMware immer die Version 1.

- **`CID`**
  `CID` ist ein einmalig berechneter Zufallswert, den VMware als ID zur internen Zuordnung nutzt.
- **`parentCID`**
  Anhand dieser Identifikation wird bei Snapshots die Eltern-Festplatte erkannt. Existiert kein Snapshot oder ist es die Eltern-Festplatte, enthält `parentCID` immer den Wert `ffffffff`.
- **`createType`**
  Dieser Parameter beschreibt den Dateityp. Es existiert knapp ein Dutzend verschiedener Werte, wenn man alle VMware-Produkte betrachtet. Im VMware ESX-Umfeld ist dieser Wert meist `vmfs`.

  Versuchen Sie bitte nicht, den `createType` manuell zu ändern, da dies die Festplatte unbenutzbar machen kann.

Datentypen

VMware ESX unterscheidet beim Anlegen zwischen vier Typen:

- thick
- zeroedthick
- eagerzeroedthick

Diese drei Dateitypen sind nicht durch die Konfigurationsdatei voneinander zu unterscheiden. Alle drei Typen sind monolithic flat, das heißt, auf der Festplatte wird die volle Dateigröße verbraucht.

- thin

Dieser Dateityp ist ein Monolithic-sparse-Typ und wächst daher beim Beschreiben dynamisch. Thin-Festplatten-Dateien erkennen Sie an zwei Eigenschaften:

- Der Wert `ddb.thinProvisioned = "1"` steht in der Konfigurationsdatei.
- Die Dateigröße durch Anzeige mit `ls -sh "disk-flat.vmdk"` oder `stat "disk-flat.vmdk"` ist kleiner als die angelegte Größe. Ein `ls -lah` bringt die angelegte Maximalgröße und nicht die reale Größe auf der Festplatte zum Vorschein.

- **`Extent description`**
  Der verwendete Festplattentyp hat direkte Auswirkungen auf die `Extent description`-Passage.
  - Die Zeilen sind nach dem folgenden Schema aufgebaut: Zugriffsmodus, Festplattengröße in Sektoren, Typ des Extents, Ort der Festplattendatei.
  - Die Festplattengröße in Sektoren wird bei der Verwendung der Festplattendateien durch das VMware-Server-Produkt benötigt. Diese Information ist vor allem dann wichtig, wenn der VMware-Server ESX 2-Festplattendateien mit nutzen soll oder die Beschreibungsdatei verlorenging. Dieser Wert wird folgendermaßen berechnet:

Größe in Sektoren = (VMDK-Größe in Bytes) / Bytes pro Sektor (immer 512)
Bei einer 2,7-GB-Festplatte wäre das beispielsweise:
(2902327296 512) / 512 = 5668607

Im Folgenden zeigen wir Beispiele für zwei Arten von Festplatten gezeigt:

- monolithicFlat

```
RW 8388608 FLAT "test4mig2-flat.vmdk" 0
```

- 2gbMaxExtendSparse

```
RW 4192256 SPARSE "sol10-hdd1-s001.vmdk"
RW 4192256 SPARSE "sol10-hdd1-s002.vmdk"
RW 4192256 SPARSE "sol10-hdd1-s003.vmdk"
RW 4192256 SPARSE "sol10-hdd1-s004.vmdk"
RW 8192 SPARSE "sol10-hdd1-s005.vmdk"
```

- **`Disk Data Base`**

  Der `Disk Data Base`-Abschnitt beschreibt die Festplattengeometrie, die Hardwareversion und den Festplattenadaptertyp.

  - `ddb.adapterType`: Festplattenadapter, kann `buslogic`, `lsilogic` etc. sein.
  - Die weiteren Geometriedaten können Sie sehr leicht anhand von Tabelle 9.6 und der folgenden Formel berechnen (*Bytes pro Sektor* ist immer gleich 512):
    Cylinders = (VMDK-Größe in Bytes) / (Heads × Sectors × Bytes pro Sektor)
  - Der Parameter `ddb.virtualHWVersion` beschreibt die Version der VMware-Plattform, unter der die Festplatte genutzt wird.

Format	Vorteile	Nachteile
thin	▸ effektive Speicherplatznutzung ▸ schnelle Erstellung der Festplattendateien	▸ Speicherplatz im Datastore ist zu überwachen, da dieser leicht überläuft ▸ Belastung des Host-Systems ▸ häufige SCSI-Reservierungen bei Datenwachstum im Gast
thick	▸ keine Überprovisionierung des Datastores möglich ▸ keine SCSI-Reservierungen bei Datenwachstum im Gast ▸ schnelle Erstellung der Festplattendateien	▸ Teurer Speicherplatz geht verloren, da bei geringem Füllgrad der Gast-Festplatten alle Bytest trotzdem verbraucht werden
zeroedthick	▸ gleiche Vorteile wie thick ▸ Überschreiben eventuell vorhandener Altdaten beim ersten Blockzugriff ▸ Standardformat für thick	▸ Es bestehen die gleiche Nachteile wie bei thick, ▸ Theoretisch ist ein Data-Leaking möglich, das heißt, Altdaten könnten gelesen werden. Derzeit sind allerdings keine Fälle bekannt.

Tabelle 9.6 Festplattenformate im Vergleich

Format	Vorteile	Nachteile
eagerzero-edthick	▸ gleiche Vorteile wie thick, bis auf die Geschwindigkeit der Plattenerstellung ▸ Überschreiben der kompletten Festplatte mit Nullen ▸ kein Data-Leaking möglich	▸ Die Nachteile sind die gleichen wie bei thick. ▸ Erstellung der Festplattendatei dauert sehr lange. ▸ Thin-Provisioning-Effizienz im Storage kann deutlich gestört werden.

Tabelle 9.6 Festplattenformate im Vergleich (Forts.)

Thin Provisioning ist nicht gleich Thin Provisioning

Man muss genau wie bei den Snapshots ganz klar zwischen Thin Provisioning im VMware-Umfeld und Thin Provisioning im Storage-Umfeld unterscheiden. Aus Performancegründen sind zweifellos die Thin-Provisioning-Möglichkeiten des Storage-Systems (falls vorhanden) vorzuziehen.

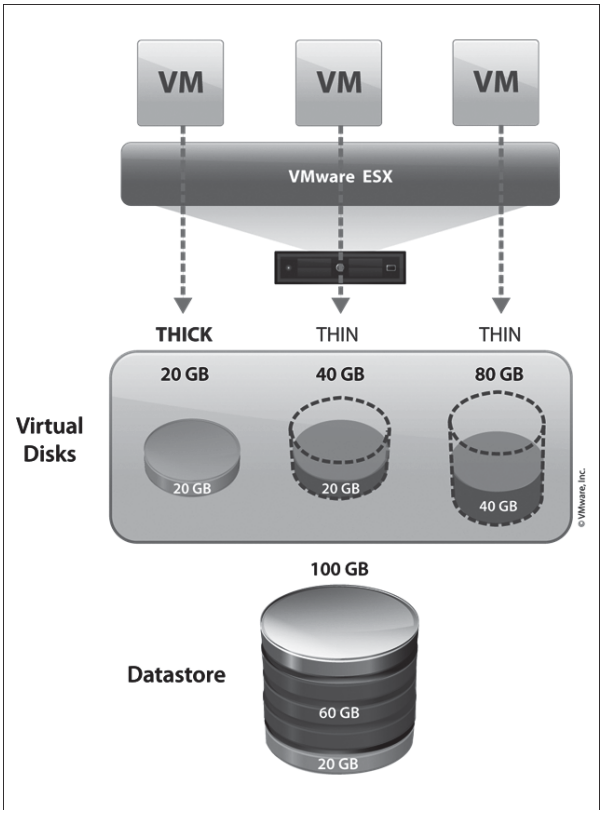


Abbildung 9.35 Thin Provisioning unter VMware

Thin Provisioning ist allerdings unabhängig von der ausführenden Komponente (VMkernel, Storage) schnell erklärt: Legen Sie eine Festplatte von 40 GB an und werden nur 20 GB Daten

im Gast generiert, so sorgt Thin Provisioning dafür, dass die 40-GB-Festplatte physisch nur 20 GB belegt.

Damit können Sie die Storage-Effizienz deutlich steigern, da eine einfachere Vergabe von Storage möglich ist und sogar eine Überbelegung, das heißt, es wird mehr Storage verwendet als physisch vorhanden. Letzteres birgt natürlich auch die Gefahr, dass der Datastore (VMware) oder die physischen Kapazitäten (Storage-System) überlaufen und es zu massiven Problemen kommt. Dies kann bis zu Datenverlust und Systemausfällen führen, weswegen es äußerst wichtig ist, die Plattenkapazitäten zu überwachen, wo Thin Provisioning aktiviert ist.

In diesem Moment sollte auch klar werden, warum es sehr problematisch wäre, Thin Provisioning auf zwei Ebenen (VMware und Storage) gleichzeitig zu nutzen. Es gibt allerdings mehr zu beachten als nur die Verwaltung. Thin Provisioning belastet zwangsweise das ESX-Host-System mehr als Thick-Festplatten, da diese Festplattendateien mit den Daten wachsen, das heißt, das ESX-System muss sich neben dem Schreiben der Daten auch um das Wachstum kümmern. Dieses Wachstum führt auch zu SCSI-Reservations, was vor allem bei der Verwendung älterer VMFS-Versionen sehr problematisch wird, wenn diese zu oft vorkommen. Ein Dokument von VMware zeigt, dass die SCSI-Reservations mit VMFS-Version 3.31 nur zu einer minimalen Beeinträchtigung nahe 0 % führen.

Die neue VMFS-Version 5 in Verbindung mit VAAI verzichtet komplett auf SCSI-Reservations auf LUN-Ebene und beschränkt sich auf die zu veränderten Blöcke. Dies gilt natürlich nur, wenn das genutzte Storage-System VAAI unterstützt. Außerdem kommt es bei der Nutzung von Thin Provisioning zur Fragmentierung im VMFS. VMware hat jedoch in einem internen Test angegeben, dass die Fragmentierung nur in seltenen Fällen zum Leistungsverlust führt.

Die Gründe für den Leistungsverlust:

- Eine Fragmentierung führt nur zu Performancenachteilen, wenn die I/O-Anfragen auf Blöcke gehen, die nicht nachfolgend sind, also weit verstreut auf dem Storage. Die VMFS-Blockgröße ist jedoch so groß (VMFS-5: 1 MB, VMFS-3: 1 MB und höher), dass die meisten Storage-Anfragen davon nicht betroffen sind. Sogar wenn die Blöcke nicht direkt aufeinanderfolgen, sind sie doch in sehr begrenzten Regionen zu finden.
- Virtuelle Festplatten sind sehr große Dateien, so dass die »Datenlücken« und damit die I/O-Blockanfragen ebenfalls sehr groß sind. Die größte Leistungsverzögerung entsteht dann, wenn die Schreib-/Leseköpfe der Festplatten viele Blöcke suchen müssen, um eine komplette Datei bereitzustellen. Im Falle von einzelnen oder wenigen »Datenlücken« innerhalb größer Datensektionen ist die Suchzeitverzögerung vernachlässigbar. Dies gilt insbesondere für Thick-provisioned Festplatten.
- Da Massenspeicher zumeist sehr große Caches (Datenpuffer) vorhalten, werden die meisten Schreibzugriffe bereits dort absorbiert. Daher führt die Fragmentierung der Daten sehr selten zu nennenswerten Performancenachteilen bei der Nutzung von SAN-Storage. Lokaler Datenspeicher (DAS) ist davon wesentlich mehr betroffen, da die Caches kleiner sind

- Selbst sequentielle Datenzugriffe auf einem Storage-System werden Random, da die I/O Anfragen mehrerer VMs über unterschiedliche ESX-Hosts gleichzeitig passieren. Daher kann man nicht von einem einzelnen Datenstrom einer einzelnen VM sprechen, sondern viele Systeme greifen gleichzeitig auf den Massenspeicher zu. Höhere Performance schaffen Sie daher besser durch Eingrenzung der Zugriffe (Hot Blocks) auf einen Datastore (RAID-Set), als nur häufig und selten genutzte Blöcke (Cold Blocks) zu mischen. VMware spricht hier von Hot Blocks, also Datenblöcke die sehr häufig genutzt werden, und Cold Blocks, die nur selten oder gar nicht verwendet werden (z. B. Betriebssystemdateien nach der Installation).
- Dies betrifft auch Thin-provisioned VMs, das heißt, die meisten Anpassungen an der Thin-provisioned Disk passieren während der Installation des Betriebssystems oder einer Anwendung. Danach nehmen das stetige Wachstum und die Änderungen and der virtuellen Festplatte zumeist ab. Trägt man nun beide Fakten zusammen, bedeutet es, dass die Hot Blocks vieler VMs werden auf einem Datastore sehr nah aneinander geschrieben, was zu Leistungssteigerungen im Storage-System führt. Abbildung 9.36 stellt abstrakt dar, dass die Blöcke der Anfangsinstallationen (Hot Blocks) recht nah beieinander sind.

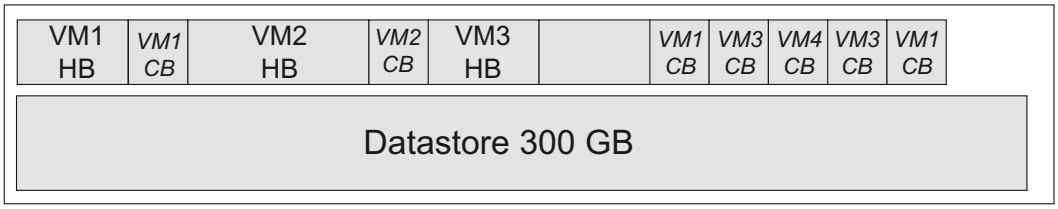


Abbildung 9.36 VM1 – VM4 Thin-provisioned mit Aufteilung Hot Blocks (HB) und Cold Blocks (CB) zur vereinfachten Darstellung

Damit geht VMware nicht davon aus, der Fragmentierung entgegenwirken zu müssen, was in KB-Artikel 1006810 (*http://kb.vmware.com/kb/1006810*) nachzulesen ist.

Formatierung mit Nullen

Ein Problem, das jede Thin-Provisioning-Implementierung betrifft, sind Formatierungsvorgänge, bei denen Nullen geschrieben werden, das heißt, obwohl keine Nutzdaten geschrieben werden, entstehen trotzdem Daten. Bei VMware-Thin-Provisioning-Festplatten führt dies direkt zu einer enormen Ineffizienz, da die Festplatte nach einiger Zeit in voller Größe auf dem Datastore liegt, weil ja alle Daten mit Nullen geschrieben wurden. Durch Thin Provisioning wird das Problem noch schlimmer, da die Festplatte langsam wächst (MB-Bereich) und bei jedem Wachstum eine SCSI-Reservation ausführt. Dies führt zur Verlangsamung des Formatvorgangs und zur Belastung aufgrund der vielen SCSI-Reservations. Dies ist mit dem Wachstum von Snapshot-Dateien zu vergleichen.

Viele Storage-Systeme beginnen damit, genau diese Nullen zu erkennen, und begegnen dem Problem auch, indem sie die unnötig verbrauchten Kapazitäten nachträglich wieder freigeben

(z. B. 3PAR, HDS) oder schon direkt beim Schreiben erkennen und ignorieren (z. B. 3PAR, IBM SVC, DataCore).

Datenwachstum

Findet ein Datenwachstum durch Generierung neuer Daten im Gast statt, so wächst die Thin-Festplatten-Datei mit an. Werden Daten gelöscht, so schrumpft sie allerdings nicht automatisch. Das gleiche Problem findet sich auch bei der Verwendung von VCB (VMware Consolidated Backup) oder den Kopiervorgängen mit Storage vMotion. Geschriebene Daten müssen kopiert werden. Da viele Dateisysteme die Daten nicht wirklich löschen, sondern nur als gelöscht markieren, befindet sich die Festplattendatei immer nur im Wachstum. Das Gleiche gilt übrigens auch für die Formatierung.

VMware hat von außerhalb des Gastes keine Möglichkeit zu erkennen, welche Daten gelöscht wurden. Dies ist nur im Gast über die VMware Tools möglich.

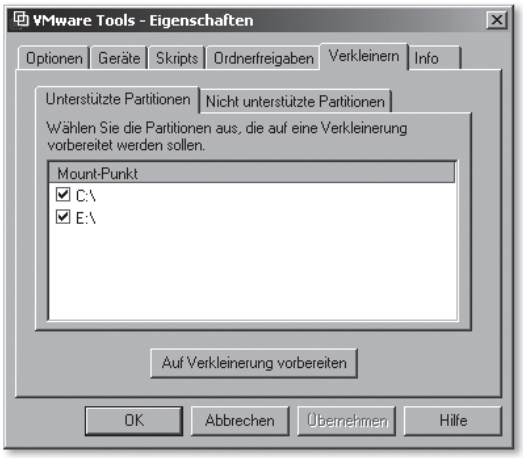


Abbildung 9.37 Shrink/Verkleinerung mittels VMware Tools im Gast

In den Eigenschaften der VMware Tools befindet sich allerdings ein Reiter VERKLEINERN oder SHRINK, der es ermöglicht, die nicht genutzten Datenbereiche so zu bearbeiten, dass die VMDK-Datei mittels Storage vMotion oder auch VCB wieder kleiner wird, da die vormals als gelöscht markierten Daten nun wirklich gelöscht sind. In diesem Zusammenhang ist auch Defragmentierung im Gast sehr interessant.

VMware-Tools-Shrink-Funktion und Thin-Festplatten

Die VMware-Tools-Shrink-Funktion kann leider nicht auf Thin-Festplatten ausgeführt werden. Möchten Sie diese Funktion nutzen, um ungenutzten Plattenplatz nochmals freizugeben, müssen Sie auf die Festplatte erst ein Inflate über den Datastore-Browser durchführen oder per Storage vMotion auf thick migrieren.

Danach funktioniert die Shrink-Funktion, und sie können den Plattenplatz optimieren. Ab jetzt sind VCB-Sicherungen wieder optimiert. Stellen Sie wieder auf thin um, so wird die Festplatte nur mit den realen Daten und ohne Altlasten (Dateilöschungen, SDelete etc.) angelegt. Dies ist zwar umständlich und Sie benötigen Plattenplatz, aber es ist derzeit die einzig mitgelieferte Möglichkeit.

SDelete

Anders verhält es sich bei Tools wie SDelete von Microsoft, die die gelöschten Daten nochmals mit Nullen überschreiben, um diese nicht wiederherstellbar zu machen. Je nach Parameternutzung wird keine Basis für die Festplattenoptimierung wie bei dem VMware-Tools-Shrink-Verfahren ermöglicht. Ganz im Gegenteil, die Parameter `-z` (Zero Free Space) und `-c` (Clear Free Space) beispielsweise führen zu einem Wachstum der Thin-Festplatten-Datei bis zur Maximalgröße oder natürlich auch eines Snapshots bis zur Maximalgröße der Ursprungsdatei.

Dies kann äußerst ärgerlich sein, wenn Plattenplatz stark überbucht wurde und jemand einen SDelete- oder einen SDelete-ähnlichen Befehl auf einer großen Festplatte ausführt, z. B. einem 500-GB-Fileserver, um auf Nummer sicher zu gehen.

9.11.3 Auslagerungsdateien

Schauen Sie sich das Gesamtkonstrukt VMware ESX inklusive der virtuellen Maschinen an, stellen Sie drei Orte fest, an denen Auslagerungsdateien genutzt werden: VMkernel und im Gastbetriebssystem der virtuellen Maschine. Die Auslagerungsdatei der Service Console entfällt mit ESX 5. Jede dieser Auslagerungsdateien hat ihre Daseinsberechtigung.

Allerdings müssen Sie immer bedenken, dass die Auslagerungsdatei virtuellen Hauptspeicher auf den lokalen oder entfernten Datenträgern abbildet. Da die Zugriffs- und Durchsatzzeiten von Datenträgern wesentlich langsamer sind als die von physischem Hauptspeicher, bedeutet ausgiebiges Auslagern immer auch verlangsamten Systemzugriff.

Eine Verwendung von SSD oder Flash-Speichern ist mit vSphere 5 als Cache-Erweiterung möglich und führt dazu, dass eine Überprovisionierung nicht zwingend zu starken Leistungseinbrüchen führt – siehe Abschnitt 9.10, »Flash-basiert«.

Service Console (nur ESX vor vSphere 5)

Da die Service Console ein getuntes Red-Hat-Linux ist, gelten auch alle Regeln für Red-Hat-Linux. Diese besagen unter anderem, dass man die doppelte Hauptspeichergröße für die Swap-Partition (Auslagerungsdatei) verwenden sollte. Dies sollten Sie bei der Installation des ESX-Servers bedenken, da spätere Partitionsänderungen so mühsam sind, dass meist eine Neuinstallation schneller wäre.

Diese Swap-Partition dient dem Red-Hat-Betriebssystem als Puffer für kurzzeitige Spitzen bei der Hauptspeicherverwendung.

Möchten Sie die derzeitige Hauptspeichernutzung inklusive Swap-Nutzung auslesen, sollten Sie auf den Befehl `free` zurückgreifen.

VMkernel

Warum benötigt der VMkernel Swapspace? – Der VMkernel benutzt den Swapspace zum sogenannten Memory-Overcommitment, also der Überprovisionierung von Hauptspeicher. Bei Standardkonfiguration würde dies bedeuten, dass auf 14 GB verfügbaren Hauptspeicher für virtuelle Maschinen 14 GB weiterer Hauptspeicher als Swapspace hinzukäme, es wären also maximal 28 GB RAM für virtuelle Maschinen nutzbar. Auch hier gilt: Swapping macht die Systeme nicht schneller, sondern langsamer. Allerdings ist die Nutzung der Auslagerungsdatei für die Abdeckung kurzer Spitzen ideal.

Außerdem verbrauchen die Gastbetriebssysteme in den seltensten Fällen den konfigurierten Hauptspeicher. Gäbe es kein Overcommitment, könnten nur so viele virtuelle Maschinen betrieben werden, wie physisch Hauptspeicher verfügbar ist, selbst wenn dieser nicht durch die VMs genutzt würde – den Hypervisor interessiert nur der konfigurierte Speicher der aktiven VMs.

Die Auslagerungsdatei selbst wird bei Standardkonfiguration pro virtueller Maschine im gleichen Heimatverzeichnis der VM bei Start jener angelegt. Die Größe der Swap-Datei entspricht der Größe des VM-Hauptspeichers. Daher müssen Sie bei der Planung der richtigen LUN-Größe die Swap-Datei jeder virtuellen Maschine mit einrechnen.

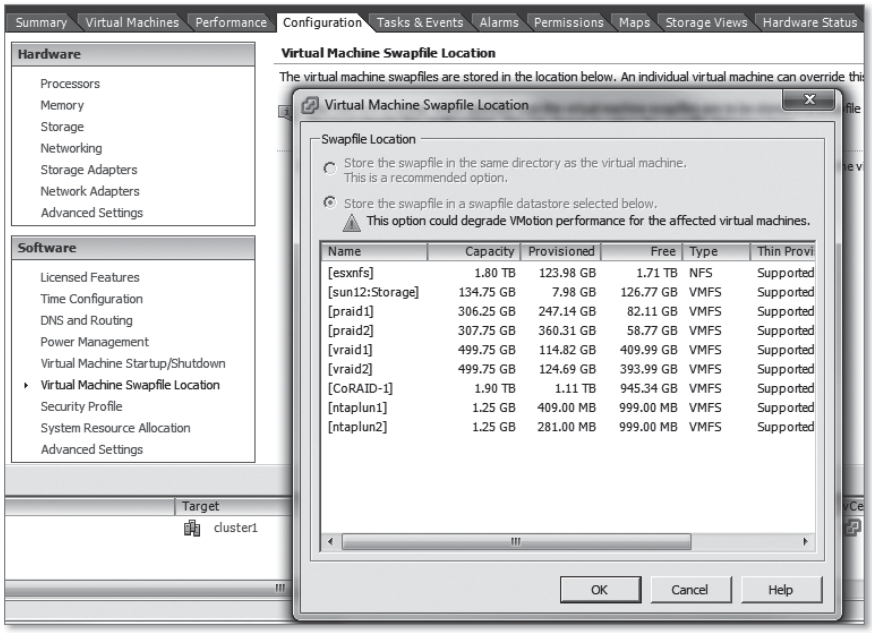


Abbildung 9.38 Anpassung des Speicherorts der Swap-Datei

Zwar ist es möglich, die Auslagerungsdateien auf den lokalen Storage der ESX-Server zu legen, dies bringt aber Nachteile mit sich, da bei vMotion und damit auch bei DRS zusätzlich die Swap-Datei auf das Zielsystem übertragen werden muss.

Des Weiteren besteht die Möglichkeit, alle Auslagerungsdateien auf einer einzigen LUN zu betreiben, die im Zugriff aller von vMotion betroffenen Server ist. Damit schaffen Sie sich allerdings bei schlechter Planung ein potentielles Nadelöhr bei der Leistung.

Eine Alternative außerhalb der GUI ist die Einstellung der Swap-Datei in der VMX-Datei der virtuellen Maschine (`sched.swap.dir= "/vmfs/volumes/<volume_name>/<dir_name>"`). Damit verteilen Sie die Swap-Dateien auf wenige LUNs, womit Sie eine gute Performance erreichen können. So könnten Sie beispielsweise die Swap-Dateien auf günstigerem Speicher als die VMs ablegen.

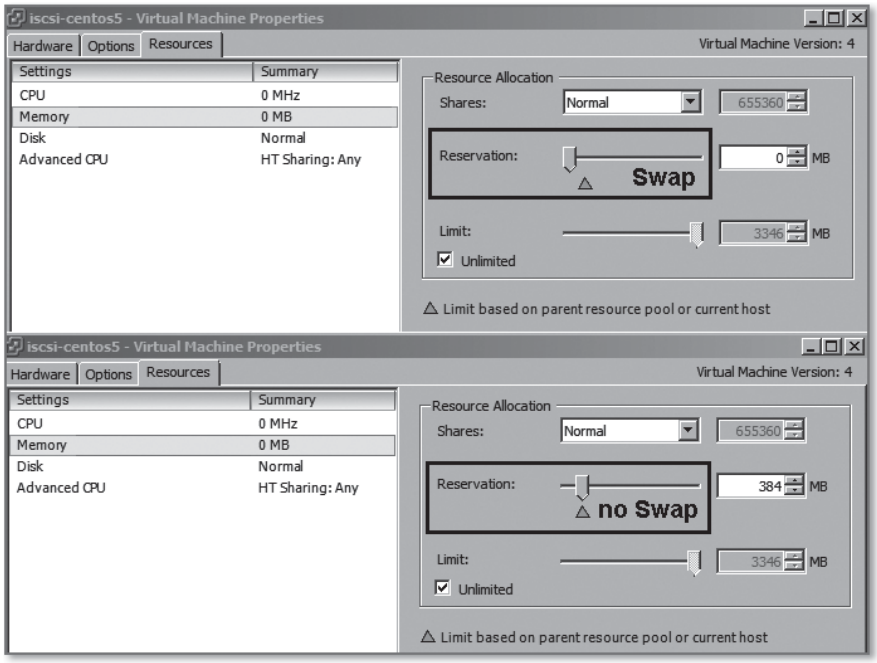


Abbildung 9.39 Die Memory-Reservierung beeinflusst die Erstellung der Swap-Datei.

Diese Größe können Sie durch Anpassung der Hauptspeicherreservierung in den Eigenschaften der virtuellen Maschine heruntersetzen. Wählen Sie eine Reservierung von 100 %, entsteht beim Start der virtuellen Maschine keine Auslagerungsdatei.

Gastbetriebssystem

In den Foren liest man viel zum Thema Auslagerungsdateien. Fragen wie »Warum noch eine Auslagerungsdatei im Gast-OS, der VMkernel swappt doch bereits?« oder »Wie groß soll die Auslagerungsdatei im Gast-OS geplant werden?« sind dort zu finden.

Generell gilt, dass eine Auslagerungsdatei den meisten Nutzen bringt, wo die Daten entstehen, die ausgelagert werden können. Da der ESX-Server keinen Einblick in die Aktivitäten der jeweiligen Betriebssysteme hat, ist der VM-Swap nur als »Notnagel« bei physischen Hauptspeicherengpässen und natürlich für Peaks gedacht. Einen Ersatz für die Auslagerungsdatei im Gast stellt dies nicht dar, daher sollten Sie alle Empfehlungen der Gastbetriebssysteme betreffend der Auslagerungsdateien weiterhin annehmen.

9.11.4 VMFS im Detail

VMFS, das VMware-proprietäre Virtual Machine File System, ist ein auf den Betrieb virtueller Infrastrukturen ausgelegtes und optimiertes Dateisystem. »Optimiert« bedeutet genauer:

- Cluster-fähig: Mehrere ESX-Server können zeitgleich auf die VMFS-Partitionen zugreifen, ohne Daten zu beschädigen.
- Dateioptimiert: Sehr große und sehr kleine Dateien werden unterstützt, womit die kleinen Konfigurationsdateien sowie große CD-/DVD-Images und sehr große Festplattendateien schnell und zuverlässig im Zugriff sind. Es wird offiziell nur eine Verzeichnisebene unterstützt.

Außerdem ist VMFS ein journalisiertes Dateisystem, was die Fehlersuche und die Fehlerbehandlung wesentlich erleichtert, und arbeitet mit einem LVM (Logical Volume Manager), der für Funktionen wie Extents oder VMFS-Vergrößerung zuständig ist.

Die Version 5 bringt deutliche Veränderungen mit sich:

- GTP: VMFS-5 nutzt GPT statt MBR als Partitionstabelle, wodurch die maximale Partitionsgröße wesentlich steigt und die Partition-Offset-Probleme umgangen werden (Partition Alignment).
- 64 TB: Es werden bis zu 64 TB große VMFS Partitionen und Raw Device Mappings unterstützt, VMFS hat zur Drucklegung des Buches allerdings noch eine Limitierung der VMDK-Dateien (2 TB – 512 Byte)
- 1 MB Blocksize: Statt der Auswahl 1, 2, 4, 8 MB Blockgröße abhängig von der maximal möglichen VMDK-Datei-Größe wird mit VMFS-5 auf eine einheitliche Blockgröße von 1 MB unabhängig von der VMDK-Datei-Größe gesetzt. Dies gilt allerdings nur für neue und nicht für bestehende VMFS-Partitionen, die aktualisiert werden, das heißt, eine 8-MB-Blocksize bleibt bestehen und wird nicht reduziert.
- Kleinere Sub-Blocks: Statt 64 KB Sub-Block Größe wurde auf 8 KB reduziert, das heißt, dass die Performance bei Anfragen kleiner Blöcke im VMFS deutlich steigt.
- Sehr kleine Dateien (1 KB) werden unterstützt.
- Unterbrechungsfreies Upgrade von VMFS-3 auf –5: Bisher mussten Aktualisierungen vom VMFS immer durch eine Formatierung erfolgen, was zu Datenverlust führte. Mit vSphere 5 ist ein Upgrade von VMFS-3 auf Version 5 ohne Unterbrechung und Datenverlust möglich.

- ATS Locking (Atomic Test & Set – VAAI-Funktion): Vor VMFS-5 und ATS wurden SCSI-Reservations ausgeführt, wenn neue Dateien angelegt oder vergrößert wurden. ATS führt dazu, dass solche Aktivitäten nicht mehr zu SCSI-Reservierungen führen.

VMFS-Aufbau

VMFS erlebte bereits mit Version 3 viele Änderungen, die sichtbar vor allem den Strukturaufbau der VMFS-Partitionsinformationen betrafen. Die neu eingeführten LVM-Offsets enthalten folgende Informationen:

- Volume-ID (Signatur)
- Anzahl Extents (Spanning mehrerer VMFS-Volumes)
- Anzahl der Geräte
- Volume-Größe

Außerdem dienen die LVM-Offset-Informationen zum Erkennen eines Snapshot-Volumes.

In den Volume-Metadaten sind folgende Informationen zu finden:

- Eigenschaften aller Dateien inklusive
  - Name
  - Größe
  - letzte Zugriffszeit
  - Änderungszeit
  - Berechtigungen
  - Eigner
  - Gruppennamen

VMFS-UUID

Die VMware-Foren wimmeln von Einträgen verloren geglaubter Datastores, und kaum ein Administrator oder Berater von VMware ESX-Umgebungen war noch nicht mit »falsch« erkannten Snapshot-LUNs konfrontiert. Dieser Aspekt ist den neu eingeführten LVM-Offset- und Volume-Metadaten zu verdanken.

Schauen wir uns die Details an:

Snapshots

Neben Snapshots virtueller Maschinen auf VMware-Host-Ebene existieren Snapshots auf Storage-Ebene. Abhängig vom Storage-Hersteller handelt es sich entweder um einen Snapshot (das heißt, Änderungen werden in einen weiteren Speicherbereich geschrieben – ähnlich ESX-Snapshot) oder einen Snapshot-Clone oder Clone (1:1-Kopie einer LUN, also doppelte Platten-

belegung). Dabei ist zu bedenken, dass LUN-Serials vom Storage bei der Anlage einer LUN automatisch vergeben werden und nicht mehr nachträglich zu ändern sind.

Beim Formatieren einer LUN mit dem VMFS wird automatisch der LVM-Header eingerichtet, in dem eine SCSI-Disk-ID anhand der LUN-Seriennummer (Serial) eingetragen wird (vergleiche Abbildung 9.40). Sobald es zu Änderungen in der Konfiguration kommt, die die Seriennummer betreffen, wird die LUN automatisch als Snapshot erkannt.

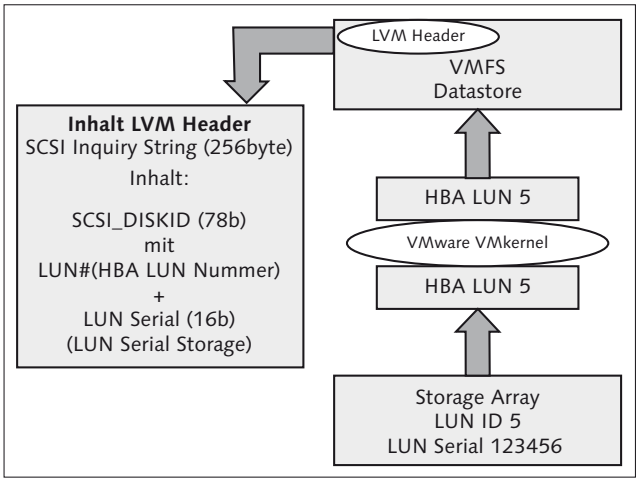


Abbildung 9.40 LVM-Header-Informationen zum Volume

Dieses Vorgehen schützt die LUNs vor Dateninkonsistenz oder Datenverlust, falls durch Konfigurationsfehler im SAN oder bei Nutzung von Snapshots oder bei einem Umschalten einer Spiegelung (Sicherung) eine LUN doppelt ist oder eine falsche LUN in der virtuellen Infrastruktur sichtbar wird.

Sie sollten bedenken, dass zumeist nicht nur ein ESX-Server, sondern viele ESX-Server auf die gleichen LUNs zugreifen. Mit dem LVM-Header werden LUNs für alle Server der Infrastruktur eindeutig gekennzeichnet.

Sobald eine neue LUN mit VMFS-Partition auf einem ESX-Server erkannt wird, findet ein Vergleich der SCSI-Inquiry-Daten (u. a. LUN-Serial) mit den geschriebenen Daten des LVM-Headers statt. Damit sind auch neu in die Infrastruktur integrierte ESX-Server direkt in der Lage, zwischen korrekten Konfigurationen und möglichen Fehlkonfigurationen oder Snapshots zu unterscheiden.

Beispiel: Erkennung Snapshot

```
LUN Anlage
LUN ID: 5
LUN Serial: 3030304230383030303030303031383830
VMFS UUID: 47f77067-244ed1d5-bde0-0015173f9345
```

```
ESX-Server: esx1
LUN-Kopie auf ESX-Server ESX2
LUN ID: 5
LUN Serial: 3030304230383030303030303031383850
```

Durch die Erkennung der Snapshot-LUN anhand der veränderten Seriennummer herrscht auf dem System kein direkter Zugriff mehr auf die trotzdem noch vorhandene VMFS-Partition. Die LUN ist jedoch nach wie vor physisch zu sehen (`esxcfg-mpath -l` oder über vSphere-Client).

Die Informationen zur LUN-ID und LUN-Serial lassen sich sehr gut mit dem Befehl `esxcfg-mpath -l -v` auslesen. Mit `esxcfg-volume` können Sie die Volumes auch wieder anzeigen und integrieren.

Einen erkannten Snapshots machen Sie sehr leicht in der */var/log/vmkwarning*-Protokolldatei ausfindig:

```
ALERT: LVM: 4475: vml.0100060000303030423038303030303031383830417869666d20:1
may be snapshot: disabling access. See resignaturing section in SAN config guide.
```

Folgende Fälle, die zum Erkennen eines Snapshots führen, kommen sehr häufig vor:

- LUN-Snapshot im Storage wird auf einen ESX-Server gemappt (LUN-Serial).
- LUN-Spiegel wird auf einen ESX-Server gemappt (LUN-Serial).

`esxcfg-volume -l` als Befehl sollten Sie daher immer auf der Konsole oder vCLI bereithalten.

VMFS-Partition-Alignment

Als hätte man mit dem Thema Storage unter VMware nicht schon genug Sorgen, so muss man sich auch noch um die Partitionen und deren Zuordnung kümmern … Ganz so schlimm ist es nicht, allerdings kann es bei einer inkonsistenten Zuordnung zu merklichen Leistungsverlusten beim Zugriff auf den Storage kommen. Aber eines vorweg: Wenn Sie LUNs mittels vSphere-Client (über die API) formatieren, wird bei Sektor 128 gestartet, was zu einer optimalen Leistung führt (minimale Latency, hohe Leistung).

Es ist zumeist nicht interessant, welches Alignment genau eingetragen wird, – d. h. 64, 128 … –, sondern eher, dass auf Basis 64 überhaupt ein durchgehendes Alignment sowohl im VMFS als auch im Gastbetriebssystem erfolgt. Durch eine ungleiche Zuordnung kommt es zu Umrechnungen auf dem Storage, was zu Verzögerung sowie Leistungsverlust führt.

Gastsystem

Allerdings ist dies noch nicht alles, da in der virtuellen Maschine ebenfalls mit Zuordnungen im Dateisystem gearbeitet wird. Wie Sie im Beispiel in Abbildung 9.41 sehen, kann eine falsche Zuordnung den Storage dazu veranlassen, drei Chunks einzulesen, obwohl nur eine Cluster-Abfrage im Gast stattfand.

Daher ist anzuraten, auch die Partitionen des Gastbetriebssystems anzupassen, um die bestmögliche Leistung zu erreichen. Die Windows-Versionen 7 und 2008 passen das Alignment bereits automatisch an, wenn sie nicht auf eine bereits bestehende Partition installiert werden.

Achtung: Datenverlust!

Anpassungen an der Zuordnung können immer nur beim Anlegen einer Partition erfolgen und nicht nachträglich. Sollten Sie die folgenden Befehle auf produktive LUNs anwenden, ist ein Datenverlust sehr sicher.

Unter Linux geschieht dies exakt wie bei der vorher beschriebenen Partitionierung des VMFS, außer dass Sie statt des Partitiontyps `fb` einen anderen Typ, z. B. `83` (Linux), auswählen müssen.

Unter Windows müssen Sie das Programm `diskpart` bemühen, das seit der Version 2003 zur Standardausrüstung von Windows gehört. Unter Windows XP und Windows 2000 müssen Sie es mit den Support Tools installieren. Da es sich um eine nicht formatierte Festplatte handeln muss, um das Alignment anzupassen, ist die Systempartition entweder so zu belassen, wie sie ist, oder zuvor mit einem anderen System zu partitionieren (oder Nutzung von WinPE) und zu formatieren und dann nachträglich an das neu zu installierende System anzuschließen:

- `diskpart.exe`
- `list disk` (Anzeigen der verfügbaren Festplatten)
- `select disk 1` (Auswahl der Festplatte – im Beispiel Disk 1)
- `create partition primary align=64` (Partition mit 64-KB-Offset anlegen)
- `exit`

Danach können Sie die Festplatte mit dem Disk Manager formatieren – allerdings sollten Sie als ALLOCATION UNIT SIZE 32K auswählen.

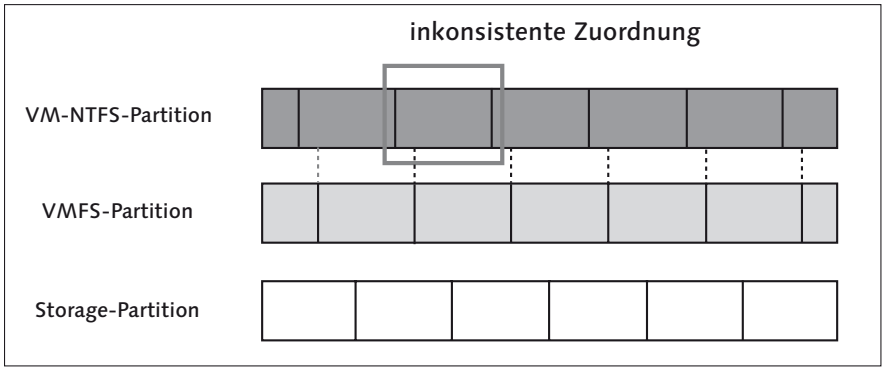


Abbildung 9.41 Partition-Alignment/Storage, VMFS, Gast

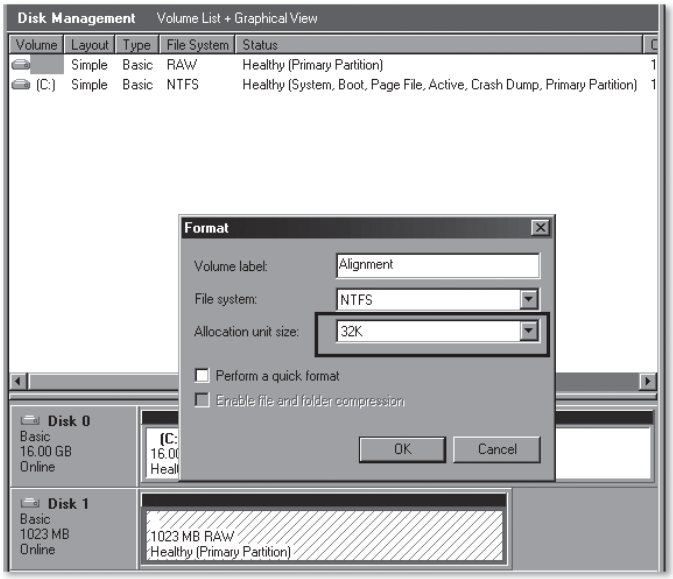


Abbildung 9.42 NTFS-Formatierung mit 32K

Nach dem korrekten Alignment sieht die Zuordnung aus wie in Abbildung 9.43.

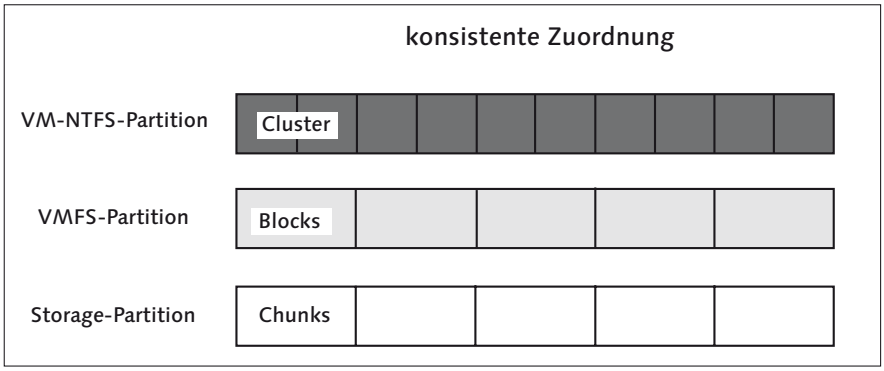


Abbildung 9.43 Konsistente Zuordnung vom Storage bis zum Gast

Es existieren kommerzielle Produkte um das Partition Alignment zu korrigieren wie Paragon PAT und Quest vOptimizer, aber auch freie Werkzeuge von Storage-Herstellern (NetApp mbralign).

VMFS-Version 5 Migration

Mit VMware ESX 5.0 wurde die VMFS-Version 5 veröffentlicht, die neben einer erneuten Minimierung der SCSI-Reservierungen weitere Leistungsverbesserungen mit sich bringt. Mit vSphere 5 ist es im Gegensatz zu vorherigen VMFS Versionen möglich, ein Upgrade von Ver-

sion 3.31 und höher auf Version 5 durchzuführen, ohne dass es zu einer Neuformatierung und damit einem Ausfall der VMs kommt (bzw. diese wegmigriert werden müssen).

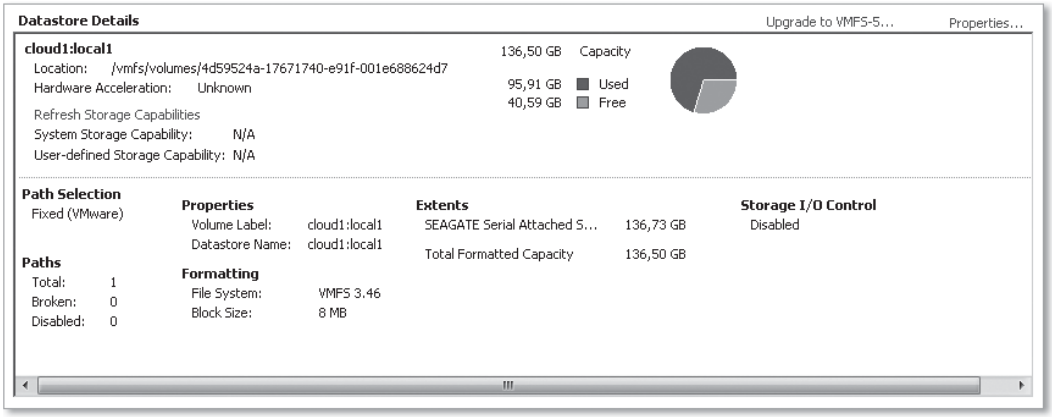


Abbildung 9.44 VMFS-5-Upgrade in den Eigenschaften eines Datastores

Ein Upgrade können Sie in den Eigenschaften des VMFS-3-Datastores durchführen.

SCSI-Reservation

SCSI-Reservierungen sind SCSI-2-Sperrmechanismen, um Datenverlust durch gleichzeitigen Zugriff mehrerer Systeme auf gleiche Daten zu verhindern. VMware ESX nutzt sie zur Änderung der Metadaten einer LUN. Wichtig: Der ESX-Server sperrt die komplette LUN, um exklusiven Schreibzugriff auf die Metadaten zu erhalten. Sämtlicher I/O der VMs des reservierenden Hosts ist nach wie vor auf die LUN zugelassen, abgesehen von weiteren Metadaten-Updates. Dazu muss ein erneuter SCSI-Lock stattfinden. Lesezugriffe der anderen ESX-Hosts sind während der Reservierung weiterhin erlaubt, allerdings keine schreibenden I/Os (weder Host noch VM).

SCSI-Reservierungen kommen nur bei blockorientiertem Zugriff über das SCSI-Protokoll vor. Somit sind Fibre-Channel, iSCSI, FCoE und AoE betroffen.

Getrieben durch Aktivitäten wie Snapshots oder Thin Provisioning verschiedener virtueller Maschinen auf der gleichen LUN treten Metadatenänderungen relativ häufig und zu beliebigen Zeiten auf. Finden die Änderungen gleichzeitig statt, kommt es zu einem SCSI-Reservation-Conflict.

Reservierungen dauern zwischen 1 und 12 Millisekunden an, bei einer Standarddauer von ca. 7 Millisekunden. Sehr kleine Änderungen, z. B. an Berechtigungen, Zugriffszeiten oder Eignern, dauern in der Regel nur 1 bis 2 Millisekunden. Allerdings liegt das zeitliche Problem nicht an den SCSI-Reservation-Requests selbst, sondern an der Statusmeldung des Targets über das Fibre-Channel-Netz. Obwohl die SAN-Storage-Systeme SCSI-Reservations direkt bearbeiten, kann es bis zu 200 ms dauern, bis der ESX-Server eine Antwort erhält.

Folgende Aktionen führen zu SCSI-Reservations:

- Erstellung einer Datei (auch bei Erstellung eines Snapshots)
- Löschung einer Datei (auch bei Löschung eines Snapshots)
- Wechsel der VMDK-Datei in den REDO-Modus (Update alle 15 MB)
- Bei der Vergrößerung von 2-GB-Sparse- oder -Thin-Festplatten (Update alle 15 MB). Bei der Verwendung von NFS werden NFS-Locks statt SCSI-Reservations genutzt.
- Bei der Migration von VMDK-Dateien (je eine Reservierung bei Quelle und Ziel). vMotion kann bei Konflikten fehlschlagen.
- Suspend der virtuellen Maschine (Suspend-Datei wird erstellt)
- VMDK-Festplatte mit aktivem Persistent Mode (aufgrund des Erstellens und Löschens des REDO-Logs – und alle 16 MB beim Datenwachstum)
- VM-Erstellung mittels Template (wenn das Template auch auf einem VMFS liegt, werden Reservations auf Quelle und Ziel gesetzt)
- Template-Erstellung aus VM (wenn Quelle und Ziel im VMFS liegen, wird neben der Standardreservierung auch alle 16 MB eine SCSI-Reservierung im Target durchgeführt)
- Export einer VMDK-Datei
- Dateisystemanpassung via `fdisk` etc.
- bei Ausführung von `vm-support`
- Änderung von Berechtigungen, Eigner, Zugriffs-/Änderungszeiten
- Größenänderung einer Festplattendatei
- beim ersten Hinzufügen einer LUN an einen ESX-Server

Wird eine SCSI-Reservierung fehlerhaft aufrechterhalten, ist dieser Befehl nützlich, um sie wieder aufzuheben:

```
vmkfstools -L lunreset /vmfs/devices/disks/vmhba#\:#\:#\:0
```

VMFS-Extents

Eine sehr häufig gestellte Frage ist, ob VMFS-Partitionen problemlos erweitert werden können, wie es bei vielen modernen Dateisystemen der Fall ist. Dies wünschen sich z. B. Administratoren, wenn sie eine stark gefüllte LUN auf dem Storage-System vergrößert haben. Die Antwort ist seit vSphere: Ja! Es ist möglich, die VMFS-Partition online zu vergrößern, ohne Extents zu nutzen. Daher werden Extents nur noch über die Kommandozeile oder bei einer Verbindung von zwei oder mehr LUNs miteinander verbunden. Befinden sich die zu verknüpfenden Partitionen auf der gleichen LUN, wird die VMFS-Partition einfach vergrößert.

Ein großes Problem besteht bei Extents, dass sie per Konkatenation an bestehende Partitionen geknüpft werden und nicht per Stripe. Hat dies Nachteile? Auch hier ist die Antwort definitiv: Ja! Da beim Concat einfach mehrere Partitionen logisch verbunden werden, werden die Daten

nicht gleichmäßig über alle Partitionen verteilt wie beim Striping. Der ESX-Server legt die Daten schlicht, wie sie entstehen, nacheinander über die Partitionen ab, als wäre es eine einzige. Das heißt, zuerst wird das erste Extent mit Daten gefüllt, dann das zweite etc. bis zum letzten Extent. Sind die Daten größer als ein Extent, z. B. 60-GB-VMDK-Datei bei 5 × 50-GB-Extents, wird zwangsweise über zwei LUNs geschrieben. Fällt eine der beiden genutzten LUNs aus, wird die VMDK-Datei entweder verschwinden, da der Header fehlt, oder beschädigt, da Datenteile fehlen.

Allerdings versucht der ESX-Server, falls vom Plattenplatz möglich, VMDK-Dateien komplett auf ein Extent zu legen, um zumindest einen Teil der Ausfallsicherheit zu wahren. Sobald nicht mehr genügend Plattenplatz für eine VMDK-Datei auf einem der Extents ist, beginnt der ESX-Server, die Lücken zu füllen, was entfernt mit einer Fragmentierung vergleichbar ist. Ist nicht mehr genügend Platz auf einem der Extents für eine Festplatte frei, so kann die Festplattendatei oder VM nicht mehr angelegt werden! Das Gemeine hierbei ist, dass Sie nicht sehen, wie stark die Extents belegt sind, sondern nur, wie stark der Datastore belegt ist. Besteht ein Datastore aus vier Extents à 74 GB und sind noch insgesamt 100 GB auf dem Datastore frei, können Sie trotzdem niemals eine Festplattendatei größer als 74 GB anlegen.

Thin Provisioning und Extents

Dieses Problem verschlimmert sich mit Thin Provisioning, da die Festplattendatei dann zwar angelegt werden kann, allerdings wird die Festplatte spätestens bei 74 GB nicht mehr weiter beschrieben werden können.

Das Gleiche gilt bei Snapshots, die zwar immer angelegt werden können, aber unter Umständen irgendwann aufgrund der Größenbeschränkung eines Extents nicht mehr wachsen können.

Entgegen der Meinung, bei Extents würden die VMDK-Dateien sinnvoll verteilt, wird sogar bei gleichzeitiger Anlage mehrerer VMs auf dem gleichen Extent-Datastore die gleiche LUN genutzt, falls genügend freier Platz vorhanden ist. Daher ist eine Erhöhung der Leistung durch Zugriff auf mehrere Partitionen nicht steuerbar, sondern rein zufällig, abhängig vom Füllgrad. Wie erwähnt ist es ganz fatal, Extents in Verbindung mit Linked Clones (Lab Manager) oder Thin-VMDK-Dateien zu nutzen, da im schlimmsten Fall alle VMs auf der ersten Festplatte des Extents angelegt würden und dieses irgendwann vollaufen würde, ohne dass es am Füllgrad des Datastores erkennbar wäre. Der Vorteil an der Konkatenation ist, dass bei Ausfall eines Extents im besten Falle nur die VMs nicht mehr im Zugriff sind, die auf genau dieser LUN lagen.

Beim Striping (wird allerdings von VMware nicht verwendet) werden alle Partitionen logisch miteinander verknüpft, und die Daten werden beim Schreiben nahezu gleichmäßig über alle Partitionen oder Festplatten verteilt. Das führt wirklich zu mehr Performance, da eine bessere Verteilung herrscht. Striping hätte allerdings bei Ausfall eines der Extents den Ausfall des kompletten Datastores zur Folge.

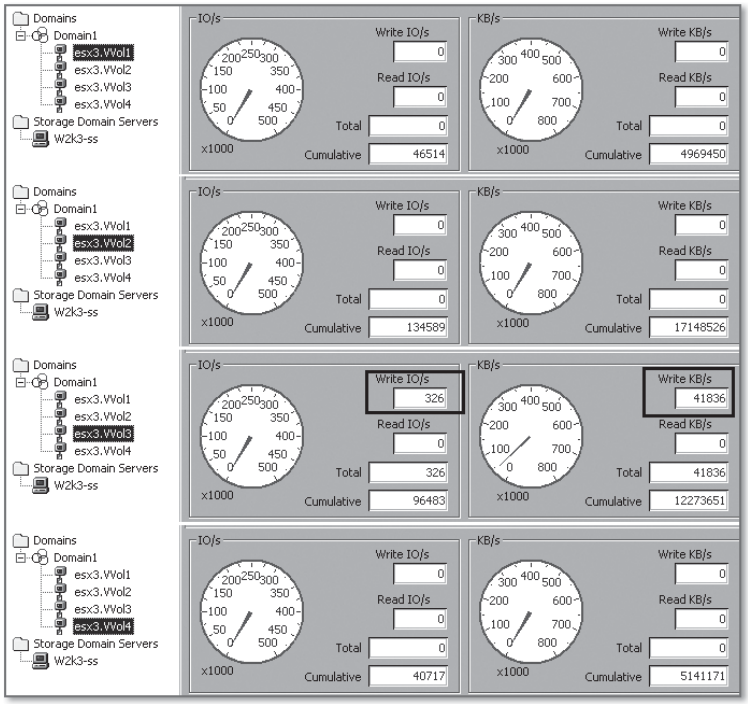


Abbildung 9.45 Kopierprozess auf Datastore, bestehend aus vier Extents – nur Volume 3 wird genutzt (Storage wurde in einer VM auf lokalen Festplatten mit DataCore SANSymphony virtualisiert, was zu den schlechten Performancewerten führt).

Bevor Sie Extents verwenden, sollten Sie erst alle Möglichkeiten durch Erstellen einer größeren LUN mit VMFS-Formatierung ausschöpfen. Die VMs verschieben Sie dann mit Storage vMotion. Extents wären nur im äußersten Notfall sinnvoll.

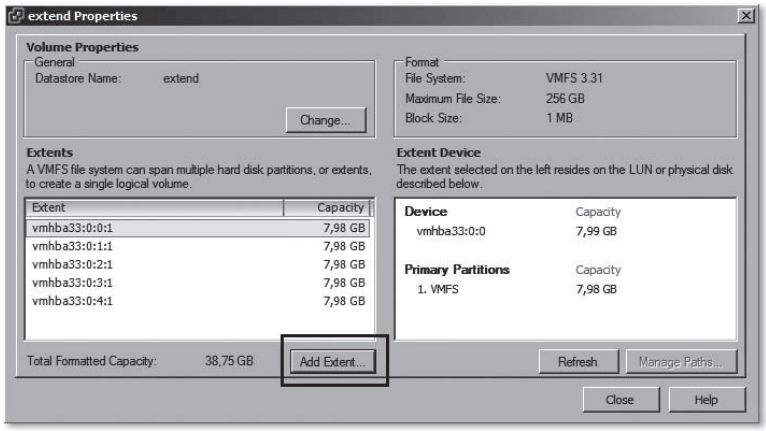


Abbildung 9.46 Ansicht eines Datastores mit vier Extents
(Grafik noch mit VMware ESX 3.5 – unter vSphere jedoch ähnlich)

Nutzung von Extents

Neben der Vergrößerung von bestehenden Datastores durch Anlegen weiterer Partitionen per Concat auf der gleichen LUN können Sie Extents auch auf beliebige Raw LUNs anwenden, sogar solche, die von unterschiedlichen Storage-Systemen kommen. Dabei sollten Sie aber mehrere Aspekte bedenken:

- Datensicherheit, da bei Ausfall einer der LUNs beliebige Zugriffe auf den Datastore versagen.
- Datensicherheit, die Zweite – verteilen Sie Extents über mehrere Storage-Systeme, entstehen mehrere potentielle Ausfallpunkte, die sehr schwer adressierbar sind.
- QoS (Quality of Service) – bei Verteilung auf mehrere LUNs müssen Sie sehr darauf achten, dass diese immer gleicher Natur sind, also keine unterschiedlichen Performance, RAID- oder QoS-Einstellungen besitzen. Dies würde zu unvorhersehbaren Problemen führen.

VMFS-Blockgröße

Die Spekulationen um die richtige VMFS-Blockgröße haben sich mit VMFS-5 erledigt, da VMFS-5 nur noch eine einzige Blockgröße zulässt, nämlich 1 MB. Nur bereits mit VMFS-3 angelegte Datastores, die auf VMFS-5 aktualisiert werden, behalten ihre bestehende Blockgröße bis zu 8 MB. VMFS-5 unterstützt Dateigrößen (z. B. VMDK) bis 2 TB (512 Byte), das heißt, eine virtuelle Festplatte kann maximal ca. 1,99 TB groß angelegt werden. Allerdings spielt die Blockgröße hierbei keine Rolle mehr.

Auch hier ist nicht alles Gold, was glänzt, da es bei Verwendung von Datastores, welche von VMFS-3 auf VMFS-5 migriert wurden zusammen mit VMFS-5 formatierten Datastores bei Storage vMotion zu unschönen Überraschungen bei der Datenübertragung kommen kann. Hintergrund ist, dass Storage vMotion nur die VAAI-Funktionen zum Offload der Datenübertragung vom ESX-Host auf den Storage nutzt, wenn die Blockgrößen gleich sind. Daher sollte man bei der Verwendung von Datastores mit VMFS-3-Blockgrößen größer 1 MB über die Neuformatierung mit VMFS-5 nachdenken, um die optimale Storage vMotion Leistungsfähigkeit zu erreichen. Allerdings ist es wichtig zu verstehen, dass eine Abfrage aus der Applikation im Gast nichts mit der Blockgröße des VMFS und auch nichts mit der Blockgröße im Storage zu tun hat. Erstens ist es so, dass sowohl NTFS unter Windows als auch VMFS unter VMware, Dateisysteme sind und die Block- bzw. Cluster-Größe hier für die Zuordnungen in der Dateiallokationstabelle eine Rolle spielt. Zweitens hat beides nichts mit der blockorientierten Welt des Storage-Systems zu tun.

1-MB-Blockgröße im VMFS bedeutet, dass jede Datei mindestens 1 MB belegt, unabhängig davon, ob sie kleiner ist. VMDK-Dateien betrifft dies nie, sondern nur VMX-, LOG- und andere Dateien. Kleinstdateien wie zum Beispiel VMX- oder LOG-Dateien existieren aber nicht millionenfach auf dem Datastore, sondern eher im Dutzend oder wenige Hundert, daher ist die Verschwendung uninteressant.

Werden aus dem Windows-Gast 4 KB angefordert, so weiß das Dateisystem aus der File Allocation Table, wo diese 4 KB auf der Festplatte stehen, und gibt die Anfrage an den SCSI-Treiber weiter. Dies betrifft den VMkernel, der die Zuordnung zwischen dem angefragten Datenblock und der Ablage auf dem Storage kennt. Daher werden auch bei einer Blockgröße des VMFS von 8 MB bei einer 4-KB-Abfrage die 64 KB (bzw. was im Storage eingestellt ist) des Storage zählen und nicht die 8 MB des VMFS. VMware hat allerdings bis VMFS-3 selbst mit 64 KB Sub-Blöcke verwendet und mit VMFS-5 auf 8 KB Sub-Blöcke reduziert, das heißt, falls die Abfrage aus dem Gast 4 KB beträgt, fragt VMware in jedem Fall 8 KB ab.

Fazit: Alignment ist wichtig, Blockgröße und Alignment-Wert sind für die Leistungsfähigkeit zweitrangig.

VMFS-SCSI-Errorcodes

Alle Fehler, die beim Betrieb von VMFS-Partitionen auftreten, sind in der Protokolldatei */var/log/vmkwarning* zu finden, unterscheiden sich jedoch zwischen den VMware ESX-Versionen. Ein sehr hilfreiches Knowledge-Base-Dokument (289902) erreichen Sie hier:

http://kb.vmware.com/kb/289902

Ein Beispielaufbau einer SCSI-Fehlermeldung sieht wie folgt aus:

```
H:0x8 D:0x0 P:0x0 Possible sense data: 0x0 0x0 0x0
```

Tabelle 9.7 stellt die generelle Syntax für ESX 5.0 dar.

Code	Eigenschaft
A	Host-Status (Initiator)
B	Gerätestatus (Target)
C	Plugin (VMware-spezifisch)
D	Fehlercode
E	erweiterter Fehlercode
F	Kennzeichner des erweiterten Fehlercodes

Tabelle 9.7 SCSI-Fehlercode-Aufbau

9.11.5 Virtuelle Maschinen

Die virtuellen Maschinen haben zwar technisch nicht allzu viel mit Storage zu tun, allerdings sind sie der erste Ansatzpunkt, an dem die Leistungsengpässe als Erstes bemerkt und gespürt werden. vSphere bringt für die virtuellen Maschinen mittlerweile fünf verschiedene Adapter mit und unterstützt Raw Device Mappings und NPIV. Nach wie vor können die VMware-Snapshots die Speicherleistung doch deutlich verschlechtern.

IDE-Adapter

Für ältere Gastbetriebssysteme hat VMware nun auch den IDE-Adapter, der bei den VMware-Workstation-Produkten schon seit jeher verfügbar ist, mit vSphere ins Enterprise-Segment gebracht. Während der Anlage einer virtuellen Festplatte müssten Sie statt SCSI den IDE-Controller wählen. Diesen Adapter sollten Sie wirklich nur im Notfall verwenden, da er keinerlei Leistungsvorteile bringt, sondern nur Kompatibilitätsvorteile.

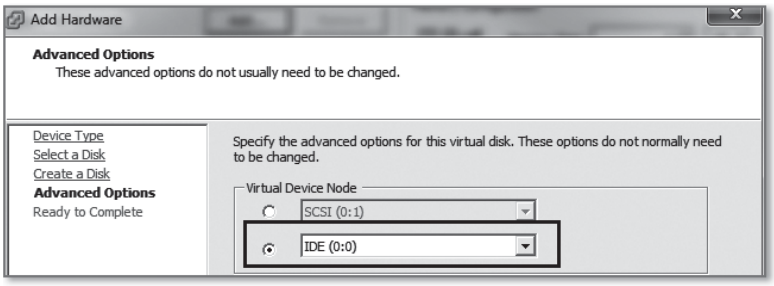


Abbildung 9.47 IDE-Adapter unter VMware vSphere

Standard-SCSI-Adapter

An Standard-SCSI-Adaptern sind die bereits bekannten BusLogic-Parallel- und LSI-Logic-Parallel-Emulationen wieder mit dabei. BusLogic sollten Sie nur bei älteren Systemen auswählen und immer LSI Logic vorziehen. Reichen Sie notfalls während der Installation den LSI-Treiber per Diskette nach (F6 unter Windows). LSI Logic Parallel ist optimiert für SAN-Umgebungen, dank der besseren Busbandbreite und der besseren Cache- und Queue-Möglichkeiten.

Um den neuen LSI-Logic-SAS-Controller zu verwenden, muss die virtuelle Maschine über die neue Hardwareversion 7 verfügen, und er ist als Adapter für geclusterte Windows 2008-Gastsysteme gedacht.

Paravirtualized SCSI

Mit vSphere kam ein neuer SCSI-Adapter für die virtuellen Maschinen hinzu, der paravirtualisiert läuft. Dies bedeutet, dass der Treiber dieses Gerätes ähnlich der VMXNET-Netzwerkkarte über seine Virtualisierung »Bescheid weiß«. Dies ermöglicht eine optimierte Kommunikation zwischen Gastkomponente und VMkernel und bietet daher erhebliche Leistungsvorteile. Der paravirtualisierte SCSI-Adapter kann mit ESX 4.0 nur als Datenfestplatte und nicht als Bootfestplatte verwendet werden. Des Weiteren werden nur die Betriebssysteme Windows 2003, 2008 und Red Hat Enterprise Linux 5 unterstützt.

Außerdem existieren Limitierungen bei den Hot-Add- und Hot-Remove-Funktionen, und Sie sollten bedenken, dass paravirtualisierte SCSI-Platten mit Snapshots keine Leistungsvorteile mehr besitzen. Weitere Informationen erhalten Sie in der VMware Knowledge Base unter *http://kb.vmware.com/kb/1010398*.

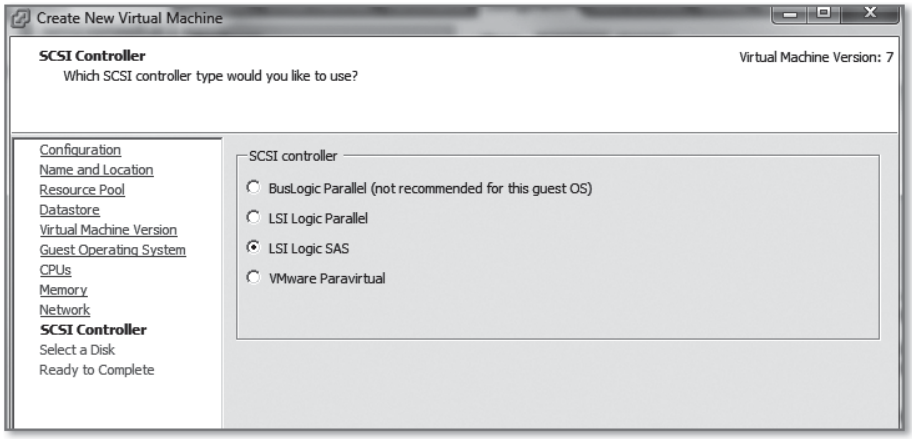


Abbildung 9.48 Paravirtueller SCSI-Adapter unter VMware vSphere

RDM

Bei Raw Device Mappings handelt es sich um 1:1-Zuordnungen zwischen virtueller Festplatte und physischer LUN. Daher funktionieren RDMs auch nur mit blockorientierten Systemen und nicht mit NFS. VMware nutzt zur Zuordnung ein Mapping-File, das als Proxy für die SCSI-Befehle dient. Man unterscheidet zwischen Physical und Virtual Mode, wobei der Physical Mode für Cluster zwischen virtuellen und physischen Systemen eingesetzt wird und der Virtual Mode Funktionen wie Snapshots unterstützt.

Sie sollten bei der Verwendung von RDMs sehr vorsichtig agieren, da das Betriebssystem im Gast die Festplatten mit eigenen Daten und Dateisystemen beschreibt. Während VMware NTFS und EXT3 als Daten erkennt, was beim Überschreiben von RDM-LUNs mit VMFS zumindest eine Hürde darstellt, sind z. B. Oracle-Raw-Daten nicht erkennbar. Daher sollten Sie die LUN-IDs für RDMs in einem bestimmten Bereich, z. B. größer 100, halten, um Missverständnisse und Datenverlust zu vermeiden.

Vorteile von RDMs sind die bessere Unterstützung von Storage-Snaphots, die Lesbarkeit der Daten von anderen Systemen (z. B. NTFS statt VMFS) und die effektive Einzelnutzung durch die VM oder den VM-Cluster. Nachteile liegen in der Verwaltung, da Sie für jede virtuelle Festplattendatei einen RDM und eine LUN anlegen und verwalten müssen.

Die LUNs müssen bei der RDM-Verwendung mit dem ESX-Server verbunden werden. Dies unterscheidet sich nicht von VMFS-Datastores. vMotion, HA und DRS funktionieren in diesem Fall dann auch wie normal.

Setzen Sie Storage vMotion ein, sollten Sie unbedingt beachten, dass aus der RDM-LUN eine VMDK-Datei erzeugt wird, wenn Sie dies nicht dediziert ausschließen. Dies hat zur Folge, dass eine 1-TB-RDM-LUN urplötzlich als 1-TB-VMDK-Datei auf dem Ziel-Datastore erstellt wird.

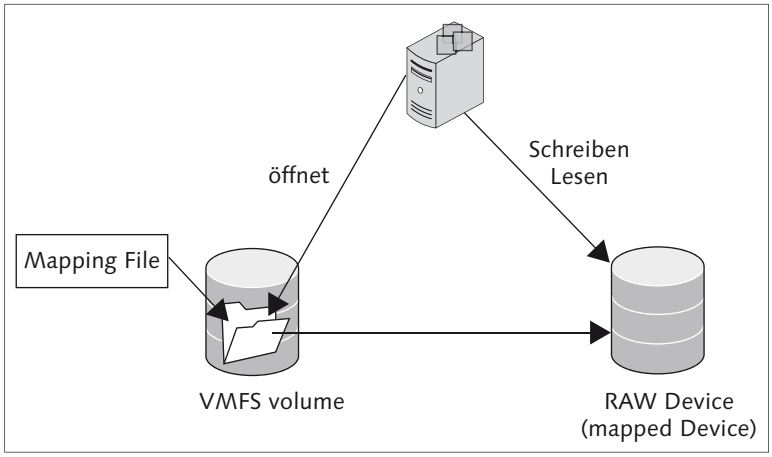


Abbildung 9.49 Raw-Device-Mapping-Zuordnung

NPIV ist nur bei der Verwendung von RDMs möglich und erlaubt eine direkte Zuordnung der virtuellen Festplatte der virtuellen Maschine zu einer LUN, da auf den virtuellen Maschinen zusätzliche virtuelle WWPNs konfiguriert werden. Diesen virtuellen WWPNs, die der ESX-Server an die FC-Ports weitergibt (daher müssen Sie die Funktion auf den FC-Switches freischalten), können Sie auf die LUNs schreibenden Zugriff erlauben, während der ESX-Host nur lesenden Zugriff erhält. Damit sichern Sie ab, dass die entsprechende LUN nicht aus Versehen oder absichtlich einer anderen, nicht autorisierten VM zugeordnet wird.

VMDirectPath-I/O

Der I/O-Zugriff von VMDirectPath belastet die CPU beim Verarbeiten von Storage-Last weniger, wenn dauerhaft und regelmäßig auf die Speichersysteme zugegriffen wird, indem er der VM ermöglicht, direkt auf die physische Hardware zuzugreifen.

Dies führt allerdings dazu, dass andere Virtualisierungsfunktionen, wie z. B. vMotion, nicht mehr zur Verfügung stehen, da die Virtualisierungsschicht ausgeklammert wird. Mit Verwendung von VMDirectPath-I/O sind die folgenden Funktionen nicht mehr möglich:

- vMotion
- Hot Add/Hot Remove von virtuellen Festplatten
- Suspend und Resume
- Fault Tolerance
- vSphere HA
- Memory-Overcommitment und Transparent Page-Sharing

Um VMDirectPath-I/O für Netzwerkkarten zu nutzen, benötigen Sie 10-Gigabit-Ethernet-Controller Intel 82598 oder Broadcom 57710 oder 57711 im ESX-Server. Experimentelle

Unterstützung wird bei HBAs von QLogic (QLogic QLA25xx 8GB Fibre-Channel), Emulex (LPe12000 8GB Fibre-Channel) sowie LSI-3GB-SAS-Adaptern (3442e-R und 3801e – basierend auf dem 1068-Chip) angeboten.

9.11.6 VMware-Snapshots

Erstellen Sie einen Snapshot auf einer virtuellen Maschine, so wird ein bestimmter Zeitpunkt festgehalten, das heißt, ab dem Zeitpunkt des Snapshots bleiben die Ursprungsdateien der VM unangetastet, und alle Änderungen werden in neue Dateien geschrieben. Dies kann im laufenden Betrieb der virtuellen Maschinen geschehen. Ebenfalls ist es möglich, die aktuellen Daten mit den Daten des Snapshots zusammenzuführen, was auch keine Ausfallzeiten mit sich bringt. Nur wenn Sie die Daten seit dem Snapshot verwerfen möchten, wird die virtuelle Maschine gestoppt, auf den alten Stand gebracht und nochmals aktiviert.

Theoretisch können Sie beliebig viele Snapshots anlegen, allerdings ist dies natürlich aufgrund der fehlenden Transparenz bei der Snapshot-Verwaltung und dem aufwendigen Management wenig sinnvoll.

Sobald ein Snapshot angelegt wurde, wachsen die neu erstellten Deltadateien dynamisch mit der Aktivität im Gast, jede Änderung auf den Festplatten führt also zum Wachstum der Delta-Festplattendatei. Damit ist jede Änderung gemeint, vom Kopieren einer Datei über sicheres Formatieren der Festplatte mit Nullen bis zum Löschen von Dateien. Es findet niemals eine Reduzierung des Plattenbedarfs statt. Allerdings kann eine Deltadatei niemals größer werden als die Originaldatei, von der sie abstammt, da alle Speicherblöcke 1:1 abgebildet wurden. Wird der gleiche Block hundert Mal überschrieben, ändert dies nichts an der Größe der Deltadatei. Sobald ein neuer Block geschrieben wird, wächst die Deltadatei mindestens in 15-MB-Schritten mit.

Daher ist es wichtig zu verstehen, dass zwar nach Anlage des Snapshots der zusätzliche Speicherbedarf maximal verdoppelt werden kann, dies gilt aber für jeden Snapshot; das heißt, wenn die Deltadatei nach dem ersten Snapshot 5 GB groß ist und ein zweiter Snapshot angelegt wird, so summieren sich die Deltadateien insgesamt auf dem Datastore. Somit gilt es, sowohl die Anzahl der Snapshots als auch deren Größe im Auge zu behalten.

Snapshots werden übrigens fast immer von Backup-Produkten genutzt, um virtuelle Maschinen im aktiven Zustand von außen zu sichern (nicht mittels Agent im Gast, sondern VCB). Dies hat als Hintergrund, dass die Festplattendateien einer VM im exklusiven Lese-/Schreibzugriff durch den VMkernel sind, bis ein Snapshot angelegt wird. Ab diesem Zeitpunkt können die Ursprungsfestplattendateien gelesen werden, und die letzte Deltadatei ist im exklusiven Schreib-/Lesezugriff durch den VMkernel.

Tabelle 9.8 zeigt den technischen Ablauf eines Snapshots.

Aktion/Dateien der VM	VMDK-Größe	NTFS-Größe	freie Kapazität NTFS
Anlage der VM mit Thick-Platte			
Vm1.vmdk (c:\)	10,2 GB	10 GB	5 GB
Kapazitätsnutzung im VMFS durch VM	**10,2 GB**		
Kopieren einer DVD im Gast (1 GB)			
Vm1.vmdk (c:\)	10,2 GB	10 GB	4 GB
Anlage von Snapshot 1			
Vm1.vmdk (c:\)	10,2 GB	10 GB	4 GB
Vm1-000001.vmdk	> 1 MB	10 GB	4G B
Kopieren einer Datei im Gast (500 MB)			
Vm1.vmdk (c:\)	10,2 GB	10 GB	4 GB
Vm1-000001.vmdk	~500 MB	10 GB	3,5 GB
Anlage von Snapshot 2			
Vm1.vmdk (c:\)	10,2 GB	10 GB	4 GB
Vm1-000001.vmdk	~500 MB	10 GB	3,5 GB
Vm1-000002.vmdk	> 1 MB	10 GB	3,5 GB
Kopieren einer DVD im Gast (2 GB)			
Vm1.vmdk (c:\)	10,2 GB	10 GB	4 GB
Vm1-000001.vmdk	~500 MB	10 GB	3,5 GB
Vm1-000002.vmdk	~2 GB	10 GB	1,5 GB
Kapazitätsnutzung im VMFS durch VM	**12,5 GB**		
Entfernen der beiden Snapshots			
Vm1.vmdk (c:\)	10,2 GB	10 GB	1,5 GB
Kapazitätsnutzung im VMFS durch VM	**10,2 GB**		

Tabelle 9.8 Snapshot – Entwicklung in der Übersicht

Wie Sie in der Tabelle sehen, sind Deltadateien leicht an der Nummerierung *-######.vmdk* zu erkennen und wachsen mit den Daten im Gast mit. Die Plattenbelegung im Gastdateisystem wird mit Anlage des Snapshots konserviert und auf den Deltadateien mitgepflegt. Sobald die Snapshots entfernt werden, werden alle Änderungen in die Originalfestplattendateien geschrieben. Die Deltadateien werden gelöscht und belegen keinen zusätzlichen Plattenplatz mehr. Jedes Wachstum der Deltadateien und das Anlegen und Entfernen der Snapshots führt übrigens im FC-Umfeld zu SCSI-Reservations, wodurch exzessiver Gebrauch von Snapshots auch schnell zu Leistungsengpässen führt.

Snapshots sind keine Backups

Snapshots werden zwar zur Sicherung von außen durch Software oder Skripte genutzt, dienen aber selbst nicht als Ersatz für Backup-Lösungen. Snapshots sind, wenn überhaupt, kurzzeitig einzusetzen bei Anpassungen im Gast (Aktualisierung des Gastbetriebssystem oder der Applikation) oder eben durch die Backup-Software, die die Snapshots direkt wieder löscht, sobald die Sicherung abgeschlossen wurde.

Wie bereits in der Erklärung zu verstehen war, bauen die Snapshots per Copy-on-write-Verfahren aufeinander auf. Daher dürfen Sie niemals die Snapshot-Kette unterbrechen, indem Sie beispielsweise Snapshot-Dateien manuell entfernen. Dies führt im schlimmsten Fall zu massivem Datenverlust.

Entfernen von Snapshots

Das Entfernen von Snapshots – das technisch dem Zurückschreiben aller Änderungen seit Anlegen der Snapshots auf die Original-VMDK-Dateien respektive Raw Device Mapping entspricht – wurde bereits mit vSphere 4 Update 2 entscheidend angepasst.

Die Änderung betrifft die Auswahl Delete All im Snapshot Manager, um sämtliche Snapshots zu entfernen und alle Änderungen auf die Originalplatte zurückzuschreiben.

Vorgehen bei allen Versionen bis vSphere 4 Update 2:

1. Originalfestplatte *vm1.vmdk* – 20 GB
2. Snapshot 1 *Vm1-000001* – 1 GB = kann bis auf 8 GB anwachsen
3. Snapshot 2 *Vm1-000002* – 1 GB = kann bis auf 7 GB anwachsen
4. Snapshot 3 *Vm1-000003* – 1 GB = kann bis auf 6 GB anwachsen
5. Snapshot 4 – 5 GB

Durch Auswahl von Delete All im Snapshot Manager wird zuerst Snapshot 4 in Snapshot 3 zurückgeschrieben, danach Snapshot 3 in Snapshot 2, Snapshot 2 in Snapshot 1 und Snapshot 1 schließlich in die Originalfestplatte, um danach alle Snapshots zu löschen. Während der Zeit des Zurückschreibens wird zusätzlicher Festplattenplatz benötigt. Kurz vor dem finalen Zurückschreiben könnte VM1 mit all ihren Festplatten bis zu 36 GB verbrauchen (5+ 6+ 7+ 8 +10 GB).

Neuer Vorgang ab Version vSphere 4 Update 2:

1. Originalfestplatte *vm1.vmdk* – 20 GB
2. Snapshot 1 *Vm1-000001* – 1 GB
3. Snapshot 2 *Vm1-000002* – 1 GB
4. Snapshot 3 *Vm1-000003* – 1 GB
5. Snapshot 4 – 5 GB

Durch Auswahl von DELETE ALL im Snapshot Manager wird zuerst Snapshot 1 in die Originalfestplatte zurückgeschrieben, danach Snapshot 2, Snapshot 3 und schließlich Snapshot 4, und alle Snapshots werden gelöscht. Es wird kein zusätzlicher Festplattenplatz verbraucht, das heißt, es bleibt bei 28 GB. Diese Neuerung hat einen entscheidenden Vorteil, da die Festplattennutzung mit Löschung jedes Snapshots nicht zunimmt. Besonders im Falle eines vollen Datastores aufgrund wachsender Snapshots ist diese Änderung von unschätzbarem Vorteil.

Snapshot Consolidator

VMware hat reagiert und ermöglicht mit dem integrierten Snapshot Consolidator auch das Erkennen und Löschen von Snapshots, die im Snapshot Manager nicht mehr sichtbar sind. Diese unsichtbaren Snapshots haben in der Vergangenheit manchen Administratoren zur Verzweiflung getrieben, da die Datastores vollliefen, ohne dass man erkennen konnte, weshalb. Tools wie der icomasoft Opvizor konnten diese Snapshots bereits früher aufspüren, indem auf die genutzte Festplatte der VM geachtet wurde und nicht auf den Snapshot Manager.

Snapshots können aus den verschiedensten Gründen aus dem Snapshot Manager verschwinden, wenn die Beschreibungsdatei der VM-Snapshots korrupt ist.

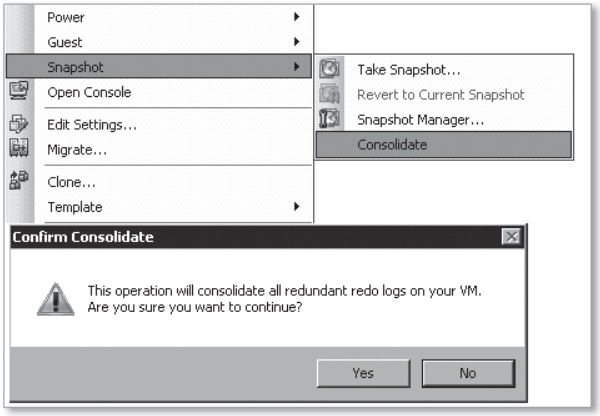


Abbildung 9.50 Snapshot-Consolidator-Auswahl

9.11.7 VM-Speicherprofile

VM-Speicherprofile sind auf den ersten Blick nur bestimmte Attribute, die Sie zentral am vCenter anlegen (ähnlich Custom Attributes) und dem Storage-System zuweisen.

So könnten Sie drei Speicherprofile anlegen – SLA1, SLA2, SLA3 – und sie den jeweiligen Datastores oder Datastore-Clustern zuordnen. Somit wäre ein Datastore mit SATA-Platten SLA3, ein Datastore mit SAS-Platten SLA2 und ein Datastore mit SSD-Platten SLA1 – die Zuordnung erfolgt manuell.

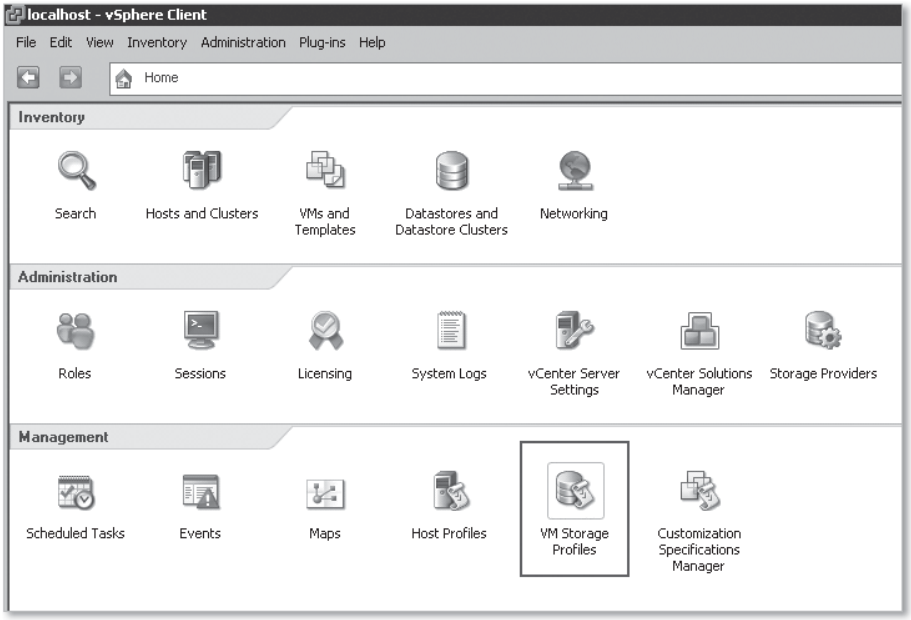


Abbildung 9.51 Verwaltung der VM-Speicherprofile

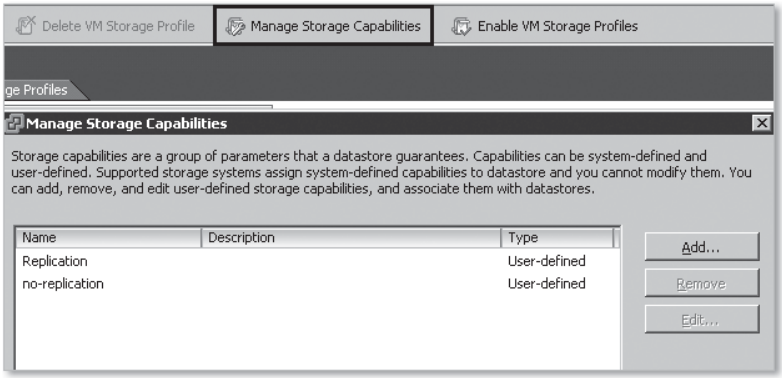


Abbildung 9.52 Anlage einer Storage-Eigenschaft

Die VM-Speicherprofile sind allerdings nur leere Hüllen, wenn Sie ihnen keine Storage-Eigenschaften (Storage-Capability) zuordnen. Diese können manuell angelegt werden (Abbildung 9.52) oder bereits vorhanden sein (SYSTEM-DEFINED).

Sobald die VM-Speicherprofile (Abbildung 9.53) angelegt sind, können Sie sie virtuellen Maschinen beim Erstellen zuweisen, um diese immer auf dem richtigen Datastore zu halten. Damit die VM-Speicherprofile korrekt funktionieren, müssen Sie natürlich die Zuordnung zwischen dem Profil und der gewünschten Storage-Capability treffen (Abbildung 9.54).

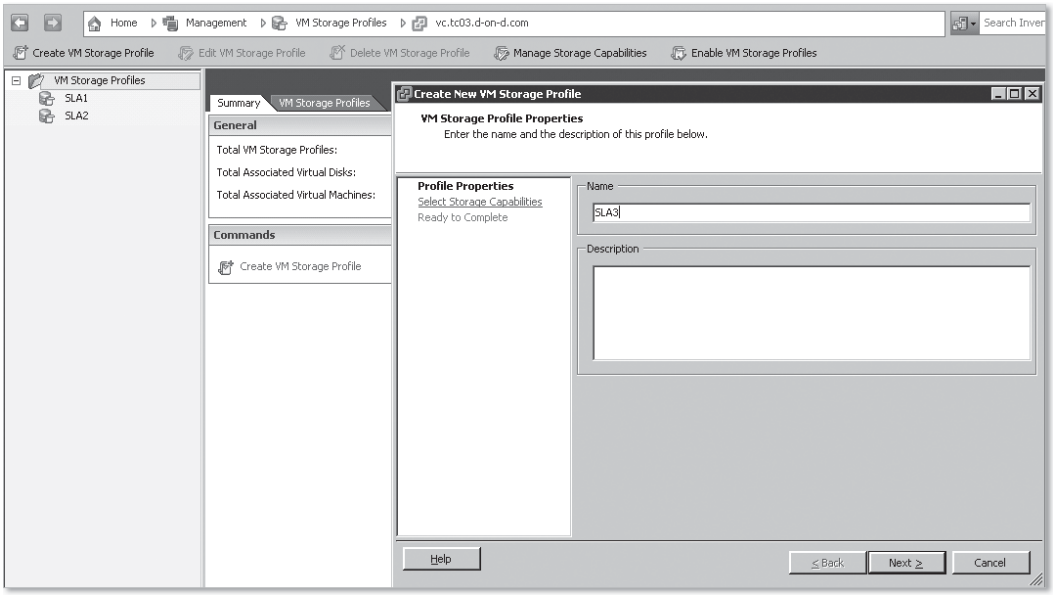


Abbildung 9.53 Anlage eines VM-Speicherprofils

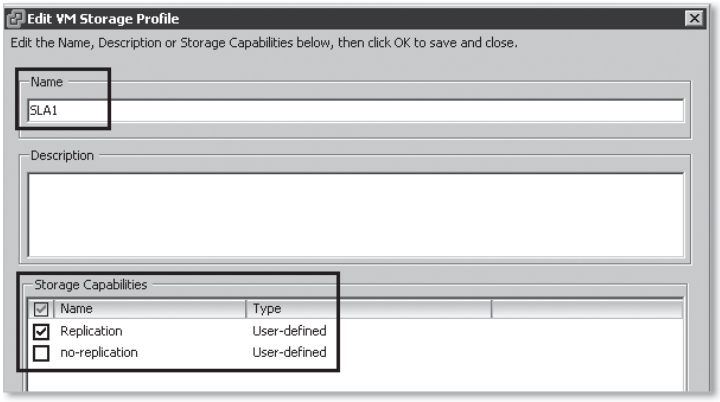


Abbildung 9.54 Zuordnung des VM-Speicherprofile und der Storage-Eigenschaft

Neben den manuell angelegten VM-Storage-Capabilities existieren allerdings noch Speicherprofile (SYSTEM-DEFINED), die mittels der VASA-Erkennung von vSphere angelegt werden. Bei Anbindung eines VASA-fähigen Storage-Systems kann vSphere 5 einige Funktionen und Eigenschaften der Storage-Systeme automatisch auslesen, die später zur Ablage von VMs genutzt werden können.

Um dem Datastore die manuell angelegten Storage-Eigenschaften zuzuordnen, wählen Sie in der Storage-Ansicht des vSphere-Clients den Menüpunkt ASSIGN USER-DEFINED STORAGE CAPABILITY (Abbildung 9.55) aus.

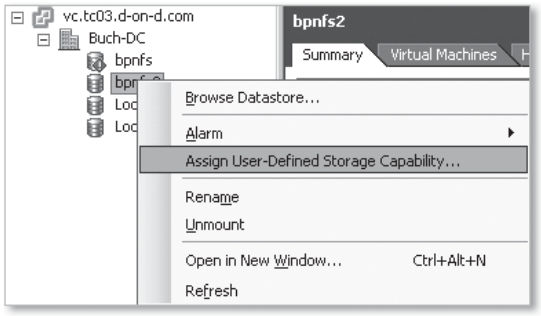


Abbildung 9.55 Zuordnung der Storage-Eigenschaft zum Datastore

9.12 VAAI

VAAI, VMware vStorage APIs for Array Integration, ist ein Paket von Programmierschnittstellen, das VMware vSphere die Kommunikation mit den angeschlossenen Storage-Systemen ermöglicht. VAAI wurde bereits mit vSphere 4.1 eingeführt und mit vSphere 5 deutlich erweitert. Die Storage-Hersteller sind auf den Zug aufgesprungen, wodurch der mögliche Funktionsumfang sich deutlich verbessert hat.

VAAI bringt vor allem in der Performance enorme Vorteile, da Storage vMotion vom ESX-Host komplett auf das Storage-System verlagert werden kann. Das Storage-System erhält lediglich Informationen von vSphere, welche Blöcke kopiert werden sollen und wohin. Statt Datenübertragungen finden nur Pointer-Übertragungen statt, was die Last auf dem Storage-Netzwerk wesentlich verringert.

Weitere Funktionen sind:

- **Atomic Test & Set** (ATS) ermöglicht es, Dateianlagen und -änderungen vorzunehmen, ohne SCSI-Reservations auf der kompletten LUN zu setzen.
- **Clone Blocks/Full Copy/XCOPY** wird von Storage vMotion genutzt.
- **Zero Blocks/Write Same** wird genutzt, um Blöcke zu löschen bzw. mit Nullen zu beschreiben.
- **Thin Provisioning ESXi 5.x** ermöglicht dem ESX-Hosti, Informationen ans Storage-System zu senden, welche Blöcke nicht mehr durch virtuelle Maschinen mit Daten belegt sind (z. B. da eine VM gelöscht oder auf einen anderen Datastore migriert wurde – reclaim)

vSphere 5 bringt außerdem neue Funktionen für die Nutzung im NAS-Umfeld mit:

- **Full File Clone** erlaubt, ungenutzte VMDK-Dateien (VM abgeschaltet) auf dem NAS-System zu kopieren (sehr nützlich für Massenprovisionierung).
- **Reserve Space** ermöglicht die Erstellung von Thick-provisioned VMDK-Dateien – vormals war nur thin auf NAS Storage-Systemen möglich.

- Dank **Native Snapshot Support** können Snapshots direkt durch den Storage erzeugt werden (dies sind keine VMware-Snapshots). Diese Funktion kann für VDI-(Desktop-)Umgebungen als performanter Ersatz für Linked Clones dienen.
- **Extended Statistics** verbessern die Auswertung des real genutzten und provisionierten Plattenspeichers des Datastores (sehr nützlich bei Verwendung von Thin- und Thick-VMDK-Dateien und Snapshots).

Voraussetzung für die Nutzung der VAAI-Funktionen ist ein unterstütztes Storage-System. Meist wird ein Firmware-Upgrade auf dem Storage-System benötigt.

Den VAAI-Status können Sie mittels vCLI auslesen:

```
esxcli -s vcenter -h esx1 storage core device vaai status get
```

Eine Übersicht über die verfügbaren VAAI-Funktionen erhalten Sie mit folgendem Befehl:

```
esxcli -s vcenter -h esx1 storage core claimrules list -c all
```

Folgende Advanced Settings sind VAAI-relevant:

- `/DataMover/HardwareAcceleratedMove`
- `/DataMover/HardwareAcceleratedInit`
- `/VMFS3/HardwareAcceleratedLocking`

9.12.1 VAAI-Einschränkungen

vSphere 5 bietet bei der Umstellung auf VMFS-5 die Möglichkeit einer unterbruchsfreien Aktualisierung. Wie so oft steckt aber der Teufel im Detail, in diesem Fall in der VAAI-Unterstützung.

Die VAAI-Funktionalität Atomic Test & Set (ATS), die die bekannten SCSI-Reservation-Probleme aufhebt, funktioniert nur teilweise, wenn Sie einen von VMFS-3 auf VMFS-5 aktualisierten Datastore benutzen. Das heißt, während VMFS-5 immer auf ATS setzt, kann es bei einem VMFS-3->VMFS-5-Datastore zu einem Rückfall auf die SCSI-Reservations kommen, wenn ein Problem auftritt.

Außerdem müssen Sie beachten, dass VMFS-5 immer eine Blockgröße von 1 MB benutzt, VMFS-3 allerdings zwischen 1 und 8 MB verwendete. Ein VMFS-5-Upgrade verändert die Blockgröße nicht, das heißt, ein VMFS-3-Datastore, der mit 8 MB Blockgröße formatiert wurde, bleibt bei 8 MB, auch nachdem er auf VMFS-5 aktualisiert wurde.

Die VAAI-Storage-vMotion-Verlagerung zum Storage (XCOPY) funktioniert nur, wenn die Blockgrößen gleich sind. Haben Quell- und Ziel-Datastore 1 MB, wird die schnelle VAAI-Variante gewählt; sind Quell- und Ziel-Datastore unterschiedlich, wird nicht mit VAAI, sondern wie früher über das Storage-Netzwerk übertragen, was sehr langsam sein kann.

Weitere Limitierungen sind:

- Quelle ist ein RDM, Ziel ist ein Datastore (VMDK).
- Quell-VMDK-Typ ist eagerzeroedthick, und Ziel-VMDK-Typ ist thin.
- Quell- oder Ziel-VMDK-Datei sind Sparse- oder Hosted-Typen (VMware Server, VMware Workstation).
- Das Klonen einer VM mit existierenden Snapshots
- VMFS-Datastore ist nicht aligned (Partition Alignment), was nur bei manuell angelegten VMFS-Datastores passieren kann; vSphere-Client und API legen die VMFS-Partition immer korrekt an.
- Die VM liegt auf einem VMFS-Datastore, der aus mehreren Erweiterungen (Extents) auf unterschiedlichen Storage-Systemen besteht.

9.13 VASA

Die Schnittstelle VASA – VMware vStorage APIs for Array Awareness – dient, wie der Name, dazu, den vSphere-Systemen Informationen vom Storage-System zu übertragen, die dessen Status wiedergeben. Zu diesen Informationen gehören Pfadfehler, ausgefallene RAID-Sets, Status der Replikation, Snapshot-Fähigkeit oder Festplattentyp.

Der sogenannte *VASA-Provider* übergibt die Storage-Informationen an den vCenter Server, der diese weiterverarbeiten kann, z. B. in Form der VM-Speicherprofile.

Der VASA-Provider wird durch den Storage-Hersteller geliefert und muss auf dem vCenter Server installiert werden. Viele Storage-Hersteller, wie EMC, IBM, Fujitsu usw. stellen bereits VASA-Provider zum Download bereit. Zur Drucklegung des Buches war leider kein NetApp-VASA-Provider öffentlich verfügbar (private Beta), wodurch ein Test in unserer Buchumgebung leider nicht möglich war.

Informationen zu den VASA-Providern finden Sie in folgender HCL-Kategorie:

http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vasa

9.14 Storage I/O Control

Storage I/O Control (SIOC) erweitert seit vSphere 4.1 die Ressourcenkontrolle um die Einschränkung oder Priorisierung der Kommunikation zwischen ESX-Host und Datastore bzw. LUN. Der Unterschied von der Storagepriorisierung und den Ressourcenkontrollmöglichkeiten von CPU und Hauptspeicher ist allerdings recht groß, da es komplexer, ist, Storage-Kommunikation zu messen und zu kontrollieren. Zum einen existiert die reine Datenüber-

tragungsmenge (Datendurchsatz in IOPS), zum anderen gibt es die Latenzzeiten (Latency in Millisekunden).

Der ein oder andere VMware-Erfahrene wird jetzt kontern, dass es doch schon länger pro virtueller Festplatte möglich war, die Storage-Kommunikation zu kontrollieren. Das ist zwar richtig, allerdings müssen Sie sich im Klaren darüber sein, dass ein großer Unterschied zwischen der Priorisierung auf vmdk-Festplatten-Ebene und der Priorisierung auf Storage-Level besteht. Wurden 20 virtuelle Maschinen mit Festplatten hoher Priorisierung auf einem Host angelegt, so wurde die Ressourcenkontrolle nutzlos. Es war dem ESX-Host schlichtweg egal, wie viele VMs miteinander konkurrierten und ob Systeme per vMotion auf andere ESX-Hosts migriert wurden, auf denen komplett andere Bedingungen herrschten.

Mit Storage I/O Control passiert ein Austausch zwischen ESX-Hosts und dem Storage-System, so dass eine Priorisierung mit Berücksichtigung der realen Leistungssituation im SAN oder NAS stattfinden kann. Außerdem ist Storage I/O Control in der Lage, die Anteile (Shares) der VMs übergreifend aus vCenter-Sicht zu überwachen.

9.14.1 Voraussetzungen

Aus dem Grund der Zentralisierung sind allerdings auch bestimmte Konfigurationen vorausgesetzt:

- Alle Systeme (ESX-Hosts, Datastores), auf denen SIOC aktiviert ist, müssen durch den gleichen vCenter Server verwaltet werden.
- Unterstützung für VMFS-Datastores auf Basis FC, FCoE, iSCSI vorhanden
- Unterstützung für NFS-Datastores vorhanden
- keine Unterstützung für Raw Device Mappings (RDM) vorhanden
- keine Unterstützung für VMFS-Datastores mit mehreren Extents vorhanden, es ist nur ein Extent erlaubt
- Storage-Array muss in der Hardware Compatibility List (HCL) als SIOC-fähig aufgeführt sein.

9.14.2 Konfiguration

Storage I/O Control wird in zwei Schritten konfiguriert: der Aktivierung von SIOC auf dem Datastore und die Konfiguration von Anteilen (Shares) auf den entsprechenden VMS.

SIOC eines Datastores aktivieren Sie in der Datastores und Datastore Clusters-Ansicht (Abbildung 9.56). Dort wählen Sie den gewünschten Datastore aus und schalten dann in den Eigenschaften (Properties) in der Datastore-Konfiguration (Configuration-Tab) SIOC aktiv.

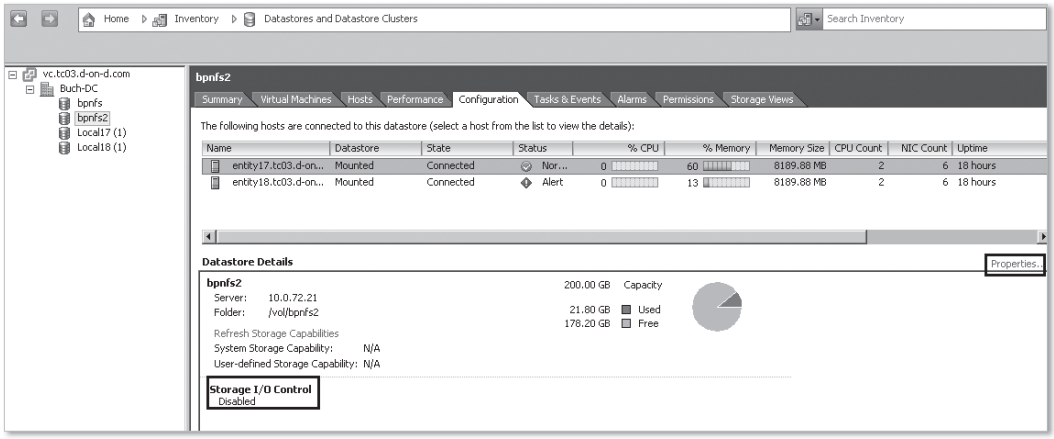


Abbildung 9.56 Konfiguration des Datastores für SIOC

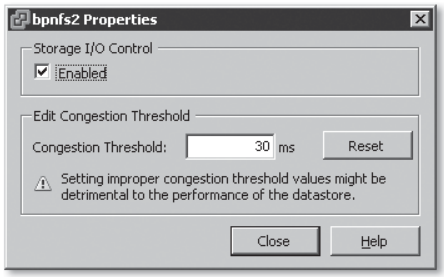


Abbildung 9.57 Aktivierung von Storage I/O Control

Die Einstellung Congestion Threshold ist die Latenzzeit in Millisekunden, die auf dem Datastore gemessen wird, ab der Storage I/O Control aktiv wird und anhand der VM Shares die Priorisierung beginnt.

Basierend auf Empfehlungen von Herstellern und Experten im Storage-Umfeld sollte der Congestion Threshold nur selten angepasst werden. Es ist vor allem sinnvoll, wenn die Storage-Systeme über wesentlich schnellere Zugriffe verfügen (z. B. bei Verwendung von SSD-Festplatten – Wert auf 10 ms senken) oder langsamere (z. B. 7.200 RPM SATA – Wert auf 50 ms erhöhen).

Übrigens ist SIOC auf Datastore-Clustern, die für Storage DRS (Details in Kapitel 5, »Cluster«) genutzt werden, automatisch aktiv; einzelne Datastores außerhalb von Datastore-Clustern müssen Sie manuell konfigurieren.

Im nächsten Schritt nehmen Sie die Priorisierung auf VM-Ebene vor, genauer in den Eigenschaften der virtuellen Maschine (Abbildung 9.58). Diese Einstellung erfolgt wie in früheren VMware-Versionen mit Shares (High, Normal, Low, Custom), nun aber auf eine zentralisierte Art und Weise in Verbindung mit vCenter und Datastore.

Außerdem ist es möglich, die I/O-Operationen der virtuellen Festplatte pro Sekunde zu limitieren (LIMIT IOPs).

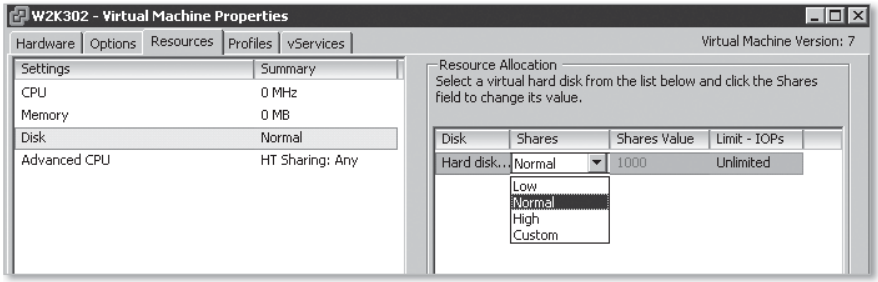


Abbildung 9.58 Konfiguration der »Shares«-Einstellung in den virtuellen Maschinen

Es ist wichtig zu erwähnen, dass diese Einstellungen nur greifen, falls Ressourcenengpässe herrschen, so dass es zwischen virtuellen Maschinen zu »Konkurrenzkämpfen« kommt und die Latenzen des Storage höher als der CONGESTION THRESHOLD sind.

Genau wie bei CPU- oder Memory-Ressourcen ist es seit vSphere 5 möglich, die Storage-Ressourcen zentral z. B. auf Cluster-Ebene einzusehen und gegebenenfalls auch zu verändern (Abbildung 9.59).

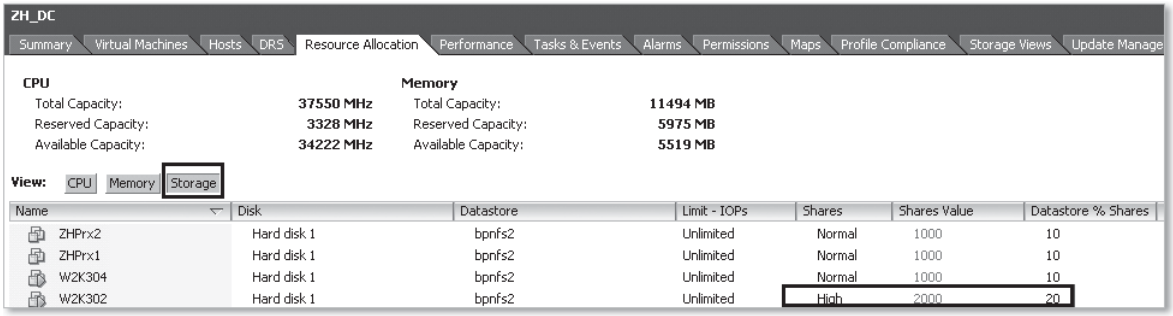


Abbildung 9.59 Zentrale Ressourcenüberwachung

9.15 VMware vSphere Storage Appliance

VMware hat sich mit vSphere 5 zum ersten Mal auf den Storage-Markt gewagt und eine eigene Storage-Appliance für kleine Umgebungen im KMU-Umfeld entwickelt. Zusammenfassend könnte man die VMware Storage Appliance (VSA) als NFS-Storage bezeichnen, der eine zentrale, ausfallsichere Einheit aus den lokalen Plattenkapazitäten der einzelnen ESX-Hosts bereitstellt. Übrigens finden Sie ein eigenes Kapitel zur VSA im Videotraining zu VMware vSphere 5 von Bertram Wöhrmann, ebenfalls erschienen bei Galileo Computing, ISBN 978-3-8362-1856-6.

9.15.1 Funktionsumfang

- Bereitstellung von lokalem Storage als zentraler Storage für alle ESX-Hosts in einem Cluster
- Ausfallsicherheit durch Redundanz und Spiegelung
- Spiegelung lokalen Storages auf andere Hosts
- Bereitstellung über das NFS-Protokoll
- Verbund von zwei bis drei ESXi-Hosts
- vMotion- und HA-kompatibel
- Hardware- und Software-Ausfall-Szenarien (mindestens 50 % des Clusters müssen noch bereitstehen)

9.15.2 Komponenten

- 2 – 3 ESX 5-Hosts
- vCenter Server 5.x
- VSA
- VSA Manager
- Cluster Service
- Cluster Leader

Der *Cluster Service* wird immer auf dem vCenter installiert, aber nur bei zwei ESX-Hosts verwendet, da er den dritten Knoten emuliert. Die *VSA* steuert die Kommunikation, Redundanz und die Fehlerverwaltung der Hard- und Software und kann sich im Leader- oder im Member-Modus befinden.

Der *Leader* wird unter allen Knoten gewählt und erhält die Cluster-IP-Adresse und hat die Aufgabe, mit dem *VSA Manager* (vCenter-Extension) zu kommunizieren. Nur der Leader kommuniziert den Status an den VSA Manager.

Der *VSA Manager* ist eine vCenter-Extension zum Provisionieren der VSA-Knoten, zur Fehlererkennung und zum Exportieren des lokalen Massenspeichers zur Verbindung (NFS-Mount) zum ESX-Host. Der vCenter Server darf nicht innerhalb eines VSA-Clusters betrieben werden, und es ist nur eine Appliance pro Host erlaubt.

9.15.3 Voraussetzungen

- identische Hardware bei allen beteiligten ESX-Hosts
- Minimum 6 GB Hauptspeicher, empfohlen 24 GB Hauptspeicher
- RAID-Controller mit Unterstützung für RAID-Level 10
- 8 identische HDs (nur SATA oder nur SAS)
- 180 GB Minimalkapazität und 2 TB Maximalkapazität der Festplatten

- keine Unterstützung für JBOD und Kombinationen aus SATA und SAS
- minimal vier Netzwerkports
- zwei getrennte Netzwerke
- zusätzliche IP-Adressen
  - 2er-Cluster: 10 statisch
  - 3er-Cluster: 13 statisch
- verwendete Netzwerkports: 2181, 2888, 3888, 2375

9.15.4 Kapazität

Es existiert eine einfache Formel, mit der es möglich ist, die Plattenkapazität zu berechnen, die über die VSA zur Verfügung steht. Verfügen die ESX-Hosts über unterschiedliche Festplattenkapazitäten, dann entscheidet der Server mit der geringsten Plattenkapazität über die Gesamtkapazität.

VSA-Kapazität = (Bruttokapazitätsserver (ohne ESXi-Installation)/4) × Anzahl Server

9.15.5 Architektur

Aktuell sieht die vSphere Storage Appliance nur zwei Architekturen vor, entweder mit zwei oder mit drei ESX-Knoten. Diese unterscheiden sich in Leistungsfähigkeit und Ausfallsicherheit.

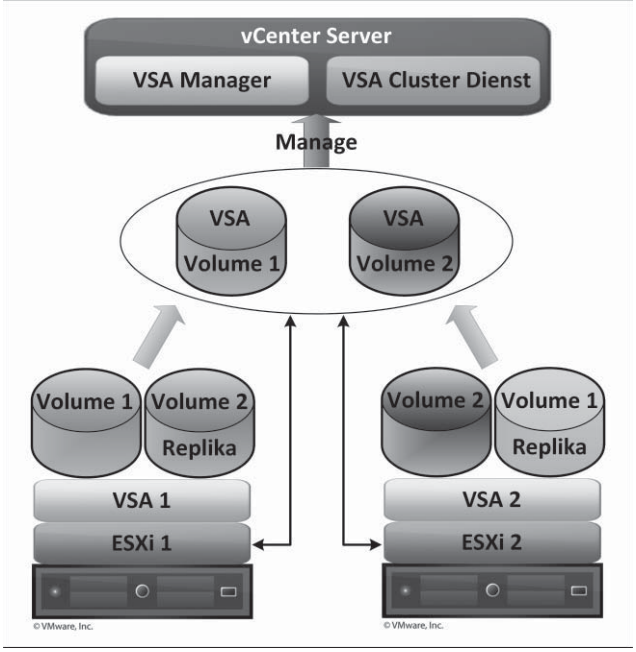


Abbildung 9.60 VSA-Architektur mit zwei ESX-Hosts

Die nutzbaren Festplatten der Knoten werden in zwei gleich große Volumes aufgeteilt (Abbildung 9.60). Ein Volume wird als Datastore exportiert und das zweite Volume als Replik für die Redundanz genutzt.

Der VSA Cluster Service wird immer installiert und in dieser Zweier-Konfiguration genutzt. Er stellt keinen Datastore zur Verfügung! Bei der Netzwerkkonfiguration müssen Sie auf die Trennung zwischen Front-End und Back-End-Netzwerk achten (Abbildung 9.61).

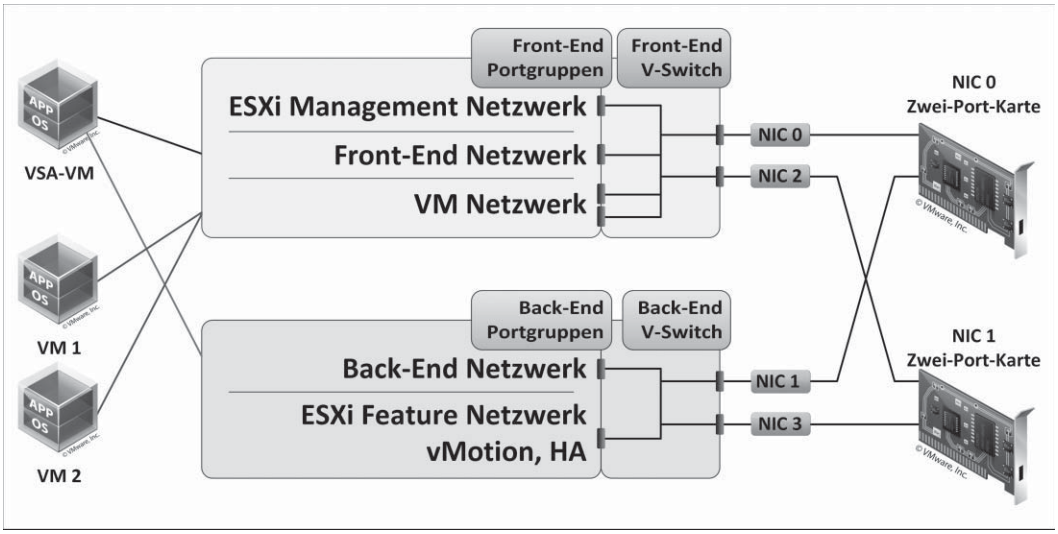


Abbildung 9.61 Logische Netzwerkkonfiguration VSA

Kommt es in der Zweier-Architektur zu dem Ausfall eines der beiden ESX-Knoten oder der VSA , dann wird dies vom VSA-Cluster-Dienst in Kommunikation mit dem noch aktiven VSA-Member bemerkt, und es wird automatisch das Replika-Volume genutzt, um dieses per NFS nach außen zu geben. Die Umstellung ist unterbruchsfrei, und die ESX-Hosts merken nichts vom Austausch des ausgefallenen Originals durch das Replika-Volume (Abbildung 9.62).

Bei der Architektur mit drei ESX-Hosts wird der VSA Cluster Service nicht mehr genutzt, da es in dieser Konstellation zu keinem Split-Brain kommen kann (Abbildung 9.63). Im physischen Netzwerk sollten Sie unbedingt auf eine hohe Redundanz achten (Abbildung 9.64).

Ein Ausfall eines ESX-Hosts in der Dreier-Architektur wird von den noch verbleibenden VSA-Members untereinander erkannt. Ist der Leader ausgefallen, wird einer der beiden Members zum Leader hochgestuft. Die VSA, die über die Replik des ausgefallenen Volumes verfügt, nutzt automatisch das Replika-Volume, das vom VSA Manager per NFS nach außen gegeben wird. Genau wie bei der Zweier-Architektur ist die Umstellung unterbruchsfrei und wird von den ESX-Hosts und natürlich von den VMs nicht bemerkt (Abbildung 9.65).

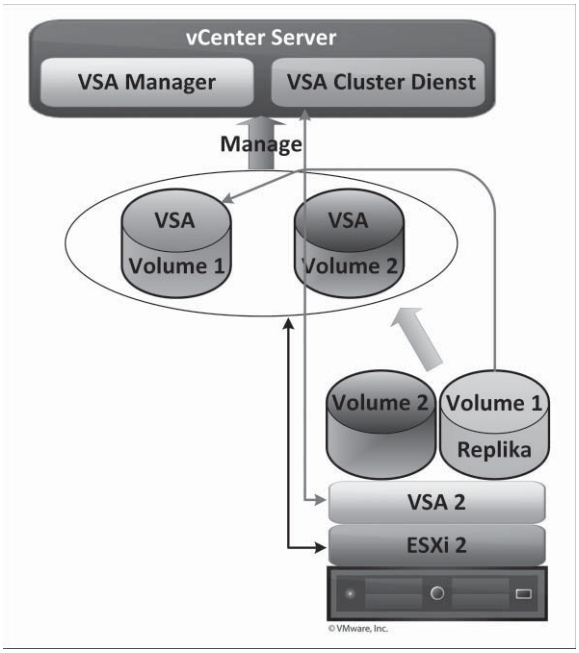


Abbildung 9.62 Vorgang beim Ausfall eines Knotens in der Zweier-Architektur

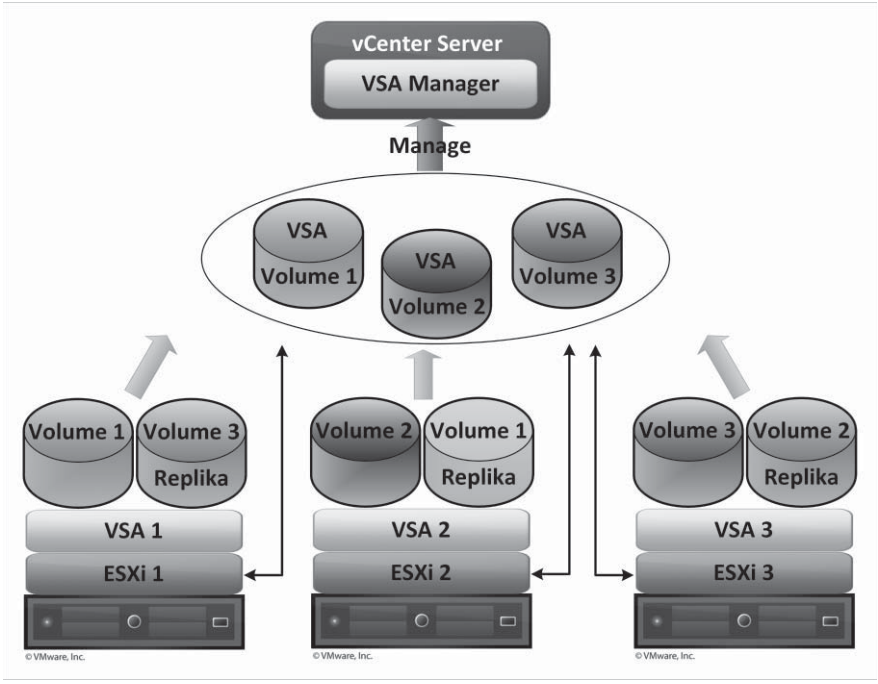


Abbildung 9.63 VSA-Architektur mit drei ESX-Hosts

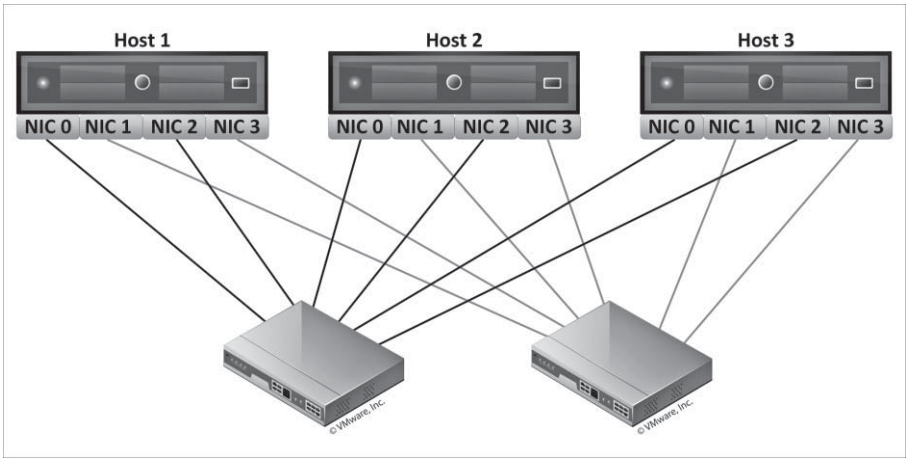


Abbildung 9.64 Physische Netzwerkredundanz bei drei Knoten

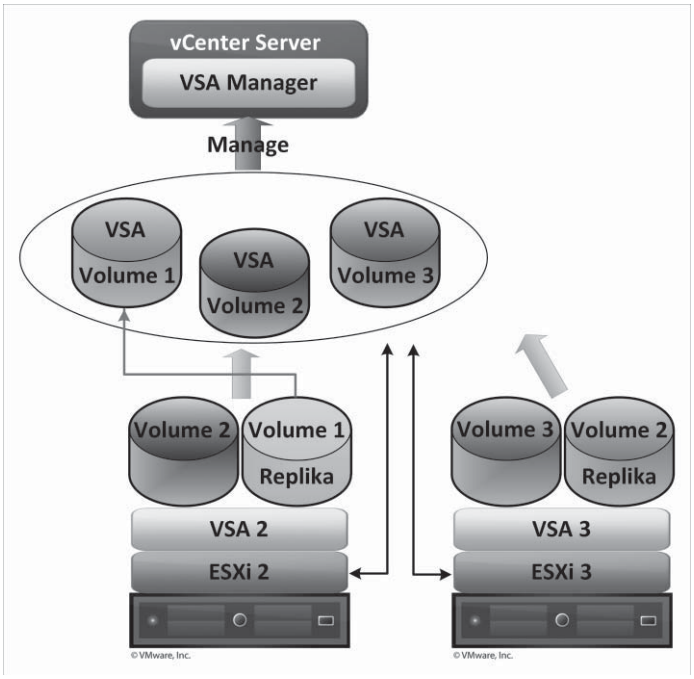


Abbildung 9.65 Vorgang beim Ausfall eines Knotens in der Dreier-Architektur

9.16 Best Practices Storage

Neben den Best Practices der Hersteller existieren natürlich ein paar mehr oder weniger allgemeingültige Ansätze. Die folgenden Informationen sind nur ein Auszug und keine vollstän-

dige Liste. Die bereits in diesem Kapitel erwähnten Themen Single-Initiator-Zoning, Partition-Alignment und SCSI-Reservations sollten Sie in jedem Fall beachten.

9.16.1 RAID-Leistungsfähigkeit

Auf den RAID-Typ gehen wir hier nicht detailliert ein, dafür ist die Wikipedia eine sehr gute Anlaufstelle: *http://de.wikipedia.org/wiki/RAID*

Allerdings möchten wir an dieser Stelle gerne die oft gehörten und gelesenen Fragen zur RAID-Leistung für die bekanntesten RAID-Level beantworten, siehe Tabelle 9.9.

RAID-Level	1 Frontend-Schreib-I/O = # Backend-I/O
RAID 0	1
RAID 1	2
RAID 5	4
RAID 6	6

Tabelle 9.9 Frontend-I/O vs. Backend-I/O im RAID-Vergleich

In Tabelle 9.9 erkennen Sie, dass ein I/O, das auf die RAID-Gruppe geschrieben wird, im Backend wesentlich mehr I/O-Operationen auslöst. Bei RAID 5 wären dies vier I/Os (Block lesen, Parity lesen, Block schreiben, Parity schreiben). Lesend sind die meisten RAID-Typen zumindest ähnlich, das heißt, bei RAID 0 kann beispielsweise gleichzeitig von beiden Platten gelesen werden, da diese die gleichen Daten enthalten. RAID 0, RAID 10 und RAID 50 erreichen lesend noch höhere Raten als RAID 1 oder RAID 5 bzw. RAID 6.

Dies muss man ins Verhältnis mit den I/Os der Festplatten stellen: SATA ~70–90 I/Os, SCSI ~120–150 I/Os, SAS/FC 150–180 I/Os. Die Umdrehungsgeschwindigkeit hat natürlich ebenfalls Auswirkungen auf die I/O-Raten. Möchten Sie daher eine mögliche I/O-Geschwindigkeit in einem RAID 5 mit drei FC-Festplatten errechnen, so könnte dies so aussehen:

150 × 3 = 450 I/Os maximal lesen pro Sekunde
450 / 4 = 112,5 I/Os maximal schreiben pro Sekunde

Ginge man von 4-KB-Blöcken wie bei Exchange aus, so wäre der Durchsatz:

450 × 4 = 1.800 KB Durchsatz pro Sekunde
112,5 × 4 = 450 KB Durchsatz pro Sekunde

Dies hört sich alles nicht so berauschend an, allerdings sind wir nun auf der reinen Physik, ohne Tuning. Dies wäre beispielsweise bei einem Direct-attached Storage (DAS = lokaler Speicher) der Fall, da dort kaum Caching ins Spiel kommt.

Ginge man den Weg ins SAN, dann könnte man nicht mehr einfach sagen, was die zu erwartende Performance der Platten wäre, da neue Faktoren hinzukämen. Einer der besten Beschleuniger ist zweifelsfrei der Cache und natürlich auch die Anzahl der Festplatten im RAID.

Außerdem verfügen die Hersteller über die verschiedensten Ansätze, Zugriffsprofile der Anwendungen zu erkennen und diese zu optimieren. Daher ist es unmöglich, ohne Messungen und weitreichende Kenntnisse der verwendeten Applikationen eine Aussage zu treffen.

Im VMware-Umfeld wird dies noch schwieriger, da über die einzelnen Datastores die unterschiedlichsten I/O-Abfragen eingehen, weil viele virtuelle Systeme mit unterschiedlichen Anwendungen gleichzeitig auf dem gleichen gemeinsamen RAID arbeiten. Dadurch entsteht auch ein hoher Anteil an Random-I/O, weswegen die Treffer im Cache abnehmen. Dies bedeutet, dass kleine Caches unter Umständen nutzlos werden.

Als Fazit sind RAID 1, 10 und 50 sehr gut, um hohe Performance zu erreichen, RAID 5 und 6 liefern schlechtere Performance bei höheren Kapazitäten. Daher sollten Sie sich die durch die virtuellen Maschinen zu erwartenden Speicherprofile gut anschauen und nach benötigter Leistung oder Kapazität entscheiden. Außerdem ist das Storage-System mit seiner Architektur gegebenenfalls ideal für die angestrebte Anwendung.

9.16.2 RAID-Größe

Neben der natürlich am häufigsten gestellten Frage nach der richtigen LUN-Größe ist auch immer wieder die Anzahl der Festplatten im einem RAID-Verbund eine spannendes Thema, das gerne angefragt wird. Generell gilt natürlich: Je mehr Leistung in den Systemen benötigt wird, desto mehr Festplatten sind sinnvoll. Allerdings muss man bei dieser Behauptung immer beachten, dass die Ausfallsicherheit nicht vernachlässigt werden darf. Würden Sie eine RAID-5-Gruppe mit 100 Festplatten erstellen (vorausgesetzt, es ist technisch möglich), so nähme die Berechnung der Parität wesentlich mehr Zeit in Anspruch als bei einer kleineren RAID-Gruppe.

Des Weiteren skaliert eine RAID-Gruppe nicht unendlich, so dass ein RAID 5 mit 4 Platten bei einer Vergrößerung auf 6 Platten noch linear skaliert, eine Erhöhung auf 12 und mehr mit sehr großer Wahrscheinlichkeit nicht mehr. Wie weit technisch skaliert werden kann, hängt auch vom Design der RAID-Lösung des Storage-Anbieters ab.

Außerdem ist es vom Leistungsaspekt her egal, ob auf einem RAID 5 mit 4 Platten 10 VMs gut performen oder auf einem RAID 5 mit 16 Platten 40 VMs. Ganz im Gegenteil, die kleinere RAID-Gruppe könnte sogar wesentlich bessere Leistung bringen, da weniger SCSI-Reservations und natürlich Random-I/O passiert. Daher ist es hier sinnvoll, nach einer optimalen RAID-Konfiguration zwischen Leistung und Ausfallsicherheit zu schauen. Idealerweise testen Sie daher verschiedene RAID-Konfigurationen und achten darauf, ob ein Engpass bei Kapazität oder Leistung besteht, und passen dementsprechend die RAID-Sets an. Oft hilft hier auch die Arraybelegung der Storage-Hersteller, da bei einem Array mit 14 Festplatten z. B. entweder zwei RAID-5-Gruppen à 6 Platten (Benennung 5 + 1 = 5 × Datenkapazität + 1 × Parity-Kapazität) mit zwei Hot-Spare-Platten oder 13 Platten (12 + 1) mit einer Hot-Spare-Platte oft empfohlen werden.

Diese Zuordnung unterscheidet sich natürlich bei der Nutzung von RAID 1, RAID 6, RAID 10 oder RAID 50 und sollte mit dem Storage-Hersteller hinsichtlich der benötigten Leistung und Ausfallsicherheit abgesprochen werden. Abhängig von Typ und Leistungsfähigkeit der Festplatte können Sie unterschiedlich viele LUNs auf diesem RAID-Set anlegen und mit virtuellen Maschinen befüllen. Generell müssen Sie immer beachten, dass jede LUN und jede virtuelle Maschine auf einer RAID-Gruppe zur Mehrbelastung des Systems mit Random-Zugriffen führt. Daher sind in diesem Fall SCSI-, FC- oder SAS-Platten gegenüber SATA-Festplatten im Vorteil.

Manche Systeme unterstützen die Möglichkeit, RAID-Gruppen miteinander zu vermischen, z. B. über mehrere RAID-5-Gruppen eine RAID-0-Gruppe zu legen. Damit erhöhen Sie die Anzahl der Festplatten eines RAID-Sets und damit die möglichen Datendurchsatzraten. Pillar Data Systems verfolgt z. B. ein solches Konzept.

HP bietet mit der EVA ein Konzept, die RAID-Level generell über alle verfügbaren Festplatten zu verteilen, das heißt, ein RAID besteht nicht aus beispielsweise 6 Festplatten, sondern nur aus Segmenten von 100 Festplatten, bei gleicher Datenmenge. Dies führt zwar zu sehr hoher Performance, ist aber bei der Bedienung und Planung sehr fehleranfällig. Daher sollten Sie bei diesem Storage-System immer sehr professionell arbeiten und genau wissen, was Sie machen.

9.16.3 Geschwindigkeit vs. Kapazität

Das Thema Geschwindigkeit vs. Kapazität wird seit der Einführung von SATA-Festplatten und den damit verbundenen enormen Festplattenkapazitäten leider immer mehr vernachlässigt, und es kommt stetig zu Leistungsproblemen im SAN oder zu Diskussionen über den Preis der Storage-Systeme.

Aber warum muss dieses Thema so genau angeschaut werden? Dazu müssen Sie sich wieder ins Gedächtnis rufen, was vor der Virtualisierung war: Man hatte zumeist zwei SCSI- oder FC-Festplatten im RAID 1 in jedem Server. In diesem RAID-Set wurden System-, Auslagerungsdatei und Applikationen abgelegt.

Sobald dieses physische System virtualisiert wird, sinkt der Plattenbedarf nicht, das heißt, wenn früher 25 % der Festplattenleistung ausgeschöpft wurde, so besteht diese Notwendigkeit auch nach der Virtualisierung.

Schauen Sie sich die virtuelle Infrastruktur genauer an, so sind viele virtuelle Maschinen auf einer oder mehreren LUNs gebündelt, die wiederum auf einer oder mehreren RAID-Gruppen abgelegt sind. Hinzu kommt, dass beim Betrieb mehrerer VMs auf dem gleichen VMFS nahezu ausschließlich Random-Zugriff herrscht, was bei größerer Datendichte automatisch zu mehr Bewegung des Schreib- Lese-Kopfes führt.

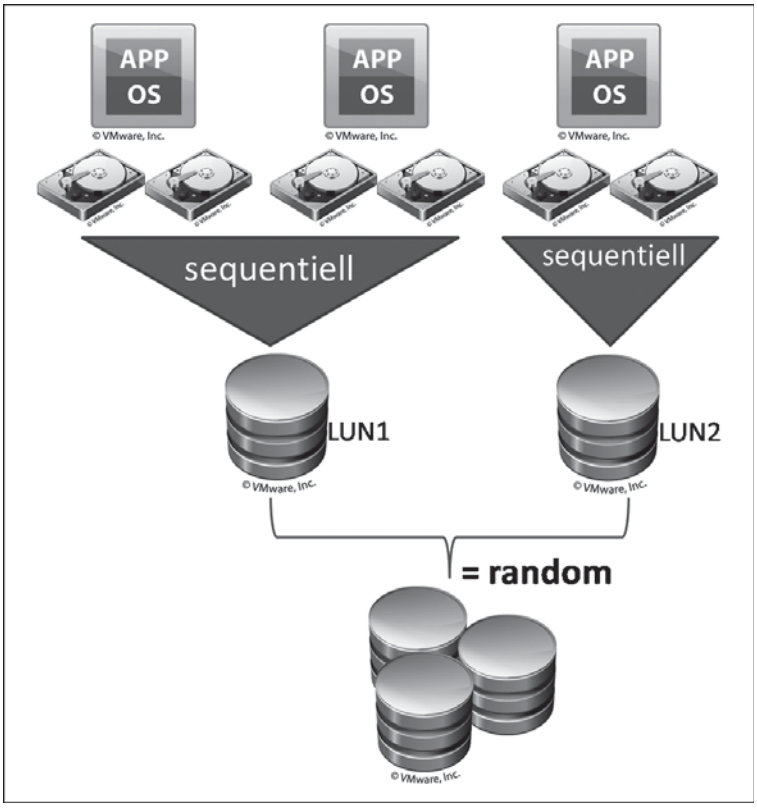


Abbildung 9.66 Sequentielle Zugriffe durch virtuelle Maschinen auf das gleiche RAID-Set führen zu Random-Zugriffen.

Würden Sie nun fünf 1-TB-SATA-Festplatten in einem RAID 5 bündeln, so kämen Sie auf eine Nutzkapazität von etwa 4 TB, die Sie in vier LUNs à 1 TB aufteilen würde. Damit stehen 4 TB Nutzkapazität aufgeteilt auf vier LUNs, die mit VMFS formatiert werden, zur Verfügung. Gingen wir im einfachsten Fall von virtuellen Maschinen mit einer Plattennutzung von 40 GB aus, so fänden knapp 25 VMs auf einer LUN Platz. Ziehen wir noch ein wenig Puffer für Snapshots und Swap-Dateien ab, wären es noch 24 VMs. Auf allen LUNs wären es 96 virtuelle Maschinen.

Vergleichen wir dies mit der physischen Hardware von früher.

Vorher:
96 Systeme à 2 Festplatten = 192 SCSI-Festplatten
(pro Platte 72 GB, d. h. eine theoretische Nutzkapazität von 6,75 TB)

Nachher:
96 Systeme = 5 SATA-Festplatten

Aber – haben diese Festplatten jetzt auch die Leistungsfähigkeit der 192 SCSI-Festplatten? Selbst wenn wir davon ausgingen, dass die heutigen SATA-Platten mit den früheren SCSI-Festplatten vergleichbar wären (was bei der Performance nicht der Fall ist), dann wäre der Leistungsnachteil der SATA-Lösung immer noch enorm. Gehen wir von 70 IOPS aus, so wäre die SCSI-Lösung gebündelt 38,4 Mal schneller, was 13.090 IOPS mehr entspricht.

Diese Rechnung ist natürlich nicht genau und betrachtet auch nicht die Unterschiede zwischen den RAID-Gruppen, allerdings spiegelt sie den Leistungsunterschied ziemlich gut wider. Somit können Sie sich sehr einfach überlegen, wie leistungsfähig diese RAID-Gruppe mit den fünf SATA-Festplatten wirklich ist und dass Sie die zur Verfügung stehenden Kapazitäten nur ausnutzen könnten, wenn Sie die virtuellen Maschinen immer abgeschaltet ließen.

Bedenken Sie daher immer, dass die Leistungsfähigkeit in IOPS eine viel wichtigere Maßgabe ist als die Kapazitätsmöglichkeiten. Somit ist es auch keine Seltenheit, dass zwar 4 TB zur Verfügung stehen, allerdings nur 1 TB sinnvoll genutzt werden kann, da somit die Performance für die virtuellen Maschinen gewährleistet ist. Es kommt auch immer wieder vor, dass aufgrund der Performance auf einer VMFS-Partition nur fünf virtuelle Maschinen betrieben werden können, ganz unabhängig von weiteren Aspekten wie SCSI-Reservation-Conflicts.

9.16.4 LUN-Größe

Wenn Sie die beiden vorherigen Abschnitte, »RAID-Größe« und »Geschwindigkeit vs. Kapazität«, bereits gelesen haben, sollte Ihnen bereits der ein oder andere Gedanke zu der richtigen LUN-Größe gekommen sein. Idealerweise versuchen Sie, die LUN-Größe auf einen gemeinsamen Nenner zu bringen, um möglichst gleiche LUNs zu erstellen. Das erleichtert die Verwaltung und die Verteilung.

Geht man von VMs mit 40 GB Festplattenkapazität aus, so landet man meist bei acht bis zehn VMs, basierend auf den dahinterliegenden IOPS-Möglichkeiten und dem davon abhängigen Lastbedarf der virtuellen Maschinen. In einem solchen Fall wären 400-GB-LUNs bei einer Planung optimal.

Haben Sie weniger leistungsfressende VMs, so können Sie natürlich mehr Systeme auf einer LUN unterbringen. Arbeiten Sie mit Thin Provisioning auf dem VMFS oder mit Snapshots, so sollte die Anzahl der VMs auf einer LUN aufgrund der SCSI-Reservations kleiner ausfallen. Dort können Sie auf maximal 1,99 TB LUN-Größe gehen. Die Limitierungen beim ESX-Host-Zugriff können Sie durch die sehr hohen Grenzwerte von vSphere mittlerweile vernachlässigen.

Umgekehrt gilt bei sehr leistungsintensiven Systemen wie Datenbanken oder Exchange-/SAP-Systemen, dass weniger VMs pro LUN besser pro RAID-Gruppe betrieben werden. Existieren Ausreißer, z. B. ein System mit 1,5 TB statt der üblichen 40 GB, so sollten Sie die VM entweder mit Raw Device Mappings oder einer großen LUN versorgen, auf der Sie die VM alleinig betreiben.

9.16.5 RAID-Rebuild und HP-EVA-Levelling

Immer wieder haben Kunden während des laufenden Betriebs das Problem, dass die I/O-Leistung der virtuellen Maschinen sich für einen gewissen Zeitraum deutlich verringert und plötzlich wieder normal ist. Daran ist nicht selten eine Überlastung des Storage-Prozessors in den Storage-Systemen schuld, die z. B. durch RAID-Rebuild, Deduplizierung, Datenmigrationen oder Levelling ausgelöst wird.

Fällt beispielsweise eine Festplatte in einer RAID-5-Gruppe aus, so muss diese Festplatte ersetzt werden, und die verlorenen Daten werden anhand der Parity berechnet und wiederhergestellt. Es kommt hierbei zu keinem Datenverlust, allerdings wird das RAID-System dadurch belastet, was Geschwindigkeitsnachteile für alle an diesem RAID-Controller angeschlossenen Platten bedeutet. Intelligente Storage-Systeme (EMC, HDS ...) erkennen bereits im Vorfeld, wenn sich bei Festplatten Abnutzungserscheinungen aufbauen, und füllen die Hot-Spare-Platte schon mit den Daten der entsprechenden Festplatte, bevor diese wirklich ausfällt. In diesem Fall wird der RAID-Rebuild-Prozess minimiert. Ist dies nicht der Fall, so kann ein RAID-Rebuild auch weit über 24 Stunden dauern, in denen ein RAID-5-Set natürlich stark durch Ausfall der nächsten Festplatte gefährdet ist, und es kommt zur Leistungsverringerung.

Ein äußerst problematischer Fall ist das Levelling, wie es beispielsweise die HP EVA ausführt. Da das EVA-System die RAID-Informationen nicht mittels kompletter Festplatten, sondern Festplattenfragmenten über alle zugeteilten Festplatten verteilt, ist die Performance zwar sehr hoch, allerdings müssen die Daten notfalls neu organisiert (verschoben, migriert) werden. Dies ist zum Beispiel der Fall, wenn dem EVA-Pool neue Festplatten zugewiesen werden und die Daten auch mit auf die neuen Festplatten verteilt werden müssen. Dieser Vorgang kann die Speicherleistung enorm verschlechtern, daher sollten Sie einen solchen Schritt auch zeitlich gut überdenken und niemals während der Produktionszeiten ausführen.

Nach den theoretischen Grundlagen aus dem vorherigen Kapitel soll das Buch auch eine praktische Anleitung anhand echter Beispiele liefern. An dieser Stelle erhalten Sie neben den eigentlichen Erläuterungen für die Umsetzung der verschiedenen Speicheranbindungen von vSphere auch nützliche Tuning- und Optimierungstipps.

10 Storage-Konfiguration unter VMware

Autor dieses Kapitels ist Oliver Kügow, teamix GmbH, ok@teamix.de

Wer die Wahl hat, der hat bekanntlich auch die Qual. Dies gilt umso mehr bei der Auswahl der »richtigen« Speicherumgebung, wenn es um die Virtualisierung geht. Ohne ein zentrales Storage-System sind viele interessante Funktionen von ESX/vSphere nicht verfügbar, genau genommen alle Features, die auf sogenannten Shared Storage aufsetzen. Dazu zählen alle Cluster-Funktionen, u. a. vMotion, DRS, HA und FT.

Neben den von VMware mitgelieferten Funktionen bieten die meisten Enterprise-Storage-Hersteller auch Mehrwerte gegenüber lokalem Direct-attached Storage (kurz DAS), die auf den ersten Blick nicht ersichtlich sind. Folgende interessante Features auf einem Storage-Array können den Wert einer VMware-Umgebung deutlich erhöhen:

- Snapshots
- Thin Provisioning
- Deduplizierung
- Replikation

VMware bietet uns seit der Version 3.0 von ESX die Auswahl für verschiedene Speicheranbindungen, aktuell stehen Fibre-ChanneliSCSI und NFS zur Verfügung – in der noch älteren Version 2.5 von ESX gab es nur FCP, dadurch stand damals die Wahl der Storage-Anbindung automatisch fest. Neu in vSphere 5.0 kam Fibre-Channel over Ethernet (FCoE) hinzu.

Die Auswahl wird ganz klar auch durch den Kauf oder den Besitz einer zentralen Speicherlösung beeinflusst. In vielen Fällen muss gar nicht gewählt werden, da verschiedene Hersteller gerne auf festgelegte Technologien setzen. So verwenden EqualLogic/Dell und HP/Lefthand ausschließlich iSCSI, die Firmen Hitachi Data Systems und HP/EVA zum Beispiel hingegen ausschließlich Fibre-Channel-Konnektivität.

Um einen einfachen und direkten Vergleich zwischen den verschiedenen Technologien zur Speicheranbindung zu liefern, fiel die Wahl für dieses Kapitel auf den Hersteller NetApp, da

dieser als Vorreiter im Unified-Storage-Umfeld gilt. Unified Storage bedeutet, dass der Kunde mit einem einzigen Speicher-Controller alle Storage-Protokolle gleichzeitig anbieten und verwenden kann. Daher sprechen wir in diesem Kapitel auch gelegentlich von »FAS«, kurz für Fabric Attached Storage, der offiziellen Bezeichnung von NetApp für die Storage-Systeme. Bei NetApp-FAS-Systemen handelt es sich allerdings trotz technischer Detail-Unterschiede um ein zentrales Storage-System, das heißt, wenn Sie IBM, HP, EMC oder andere Systeme einsetzen, können Sie die Erläuterungen dieses Kapitels größtenteils 1 : 1 nutzen.

Im Block-Storage-Umfeld unterstützt NetApp neben dem klassischen FCP und iSCSI neuerdings auch das Protokoll Fibre-Channel over Ethernet (kurz FCoE) unterstützt. Für den Zugriff auf filebasierten Storage stehen bei NetApp die beiden bekannten Protokolle CIFS und NFS zur Verfügung. CIFS wird von VMware in vSphere/ESX nicht unterstützt, deshalb wird es hier in diesem Kapitel keine Beachtung finden. Auch auf FCoE können wir leider nicht eingehen, da die dafür notwendige Testinfrastruktur leider nicht zur Verfügung steht.

Im Laufe dieses Kapitels werden wir die Anbindungen über FCP, iSCSI und NFS konfigurieren und verwenden. Außerdem erklären wir Ihnen den Umgang mit Datastores, Pfaden und den Speicheransichten (Storage Views). Es wird der gesamte Weg aufgezeigt, vom Storage-Array über die verschiedenen Switches hin zum ESX-Host und die Verwendung des Speicherplatzes als VMware-Datastore. Da dieser Vorgang nicht beim Mapping der LUNs an den ESX-Hosts beginnt, geht dieses Kapitel in der richtigen Reihenfolge vor und beginnt beim Einrichten der Switches und des Storage.

10.1 Verwendungszwecke von Storage

Bei der Verwendung von Storage im Zusammenhang mit vSphere denkt man zuerst daran, wie die virtuellen Maschinen und ihre (VMDK-)Dateien abgelegt werden, bzw. daran, über welche Technologie der zentrale Massenspeicher angebunden wird. Mit anderen Worten: Storage in Form eines Datastores, egal ob block- oder filebasiert.

Jedoch gibt es auch einige andere Einsatzgebiete zu beachten: Dazu gehörte beim ESX Classic die Verwendung von Storage für die Service Console (das sogenannte Console Operating System, COS). Einige Backup-Tools benötigten zum Beispiel Zugriff auf Storage vom COS aus, um ihre Backup- und Restore-Arbeiten erledigen zu können.

Durch die Umstellung auf ESXi und die damit einhergehende Einführung von APIs für den Zugriff auf die Daten ist die direkte Storage-Verwendung in der ESXi-Shell eher ungewöhnlich worden, wenn auch nicht komplett unmöglich oder gar ausgeschlossen, siehe Abschnitt »Alignment-Probleme: LUNs, VMFS, NFS und VMDK-Dateien« auf Seite 560.

Aber auch der Anwendungsfall »Speicherplatz innerhalb der virtuellen Maschine« bringt noch andere Aspekte mit sich als eine ausschließliche Nutzung von VMDK-Dateien. So kann Speicher für VMs beispielsweise auch über Software-iSCSI-Initiatoren direkt von der VM aus über das LAN angefordert werden oder eine unformatierte LUN per Raw Device Mapping (RDM) vom zentralen Speicher über den ESXi-Host an die VM durchgereicht werden.

Alle diese Aspekte der schlussendlichen Verwendung von Speicher sind für eigentliche Anbindung der ESXi-Hosts an einem zentralen Storage nur nachgelagerte Anwendungsfälle, deshalb erklären wir sie in diesem Kapitel nicht. Primär wollen wir hier aufzeigen, wie Sie die eigentliche Verbindung zwischen Hosts und Speichersystem bestmöglich konfigurieren und wie Sie anschließend den Speicherplatz für VMs verwenden und administrieren.

10.2 Einrichtung und Konfiguration von Datastores

Im Folgenden gehen wir die Konfiguration von Datastores Schritt für Schritt durch, beginnend bei der Storage-/Netzwerkinfrastruktur bis zur eigentlichen Erstellung der Datastores.

10.2.1 Fibre-Channel

Notwendige Infrastruktur

Um eine Fibre-Channel-Infrastruktur aufzubauen, benötigen Sie mehrere Komponenten. Auf der Seite der ESX-Hosts wird im FCP-Umfeld von den sogenannten *Initiators* gesprochen, die Seite des Speichersystems wird meist als *Target* bezeichnet. Die Initiators stellen sich in Form von HBAs (Host-Bus-Adapter) dar, also FCP-Karten. Pro ESX-Host sollten mindestens zwei FCP-Ports zur Verfügung stehen, am besten in Form von zwei Karten mit mindestens einem Port. Eine Dual-Port-Karte funktioniert zwar auch, ist aber weniger redundant.

Zwischen den Initiatoren (ESX-Hosts) und dem Target (Speichersystem) wird als Transportweg die Fabric verwendet, meist ein Verbund aus einem oder mehreren Fibre-Channel-Switches. Für eine echte Redundanz benötigen Sie mindestens zwei unabhängige Switches: Jeder dieser Switches stellt eine eigene Fabric dar. Auf der Target-Seite findet man in der Regel geclusterte Controller vor, die über mehrere Target-Ports verfügen, einen Target-Port für jede Fabric. Wenn Sie also z. B. pro Cluster-Knoten des Speichersystems zwei Target-Ports haben (einen für jede Fabric), so stehen insgesamt vier Target-Ports zur Verfügung, über die Sie LUNs ansprechen können. Je nachdem, ob es sich um einen Active/Active-Cluster oder um einen Active/Standby-Cluster handelt, stehen möglicherweise nur zwei aktive Target-Ports zur Verfügung.

Das Schaubild in Abbildung 10.1 zeigt einen NetApp-Active/Active-Cluster mit einem ESX-Host und zwei Fibre-Channel-Switches.

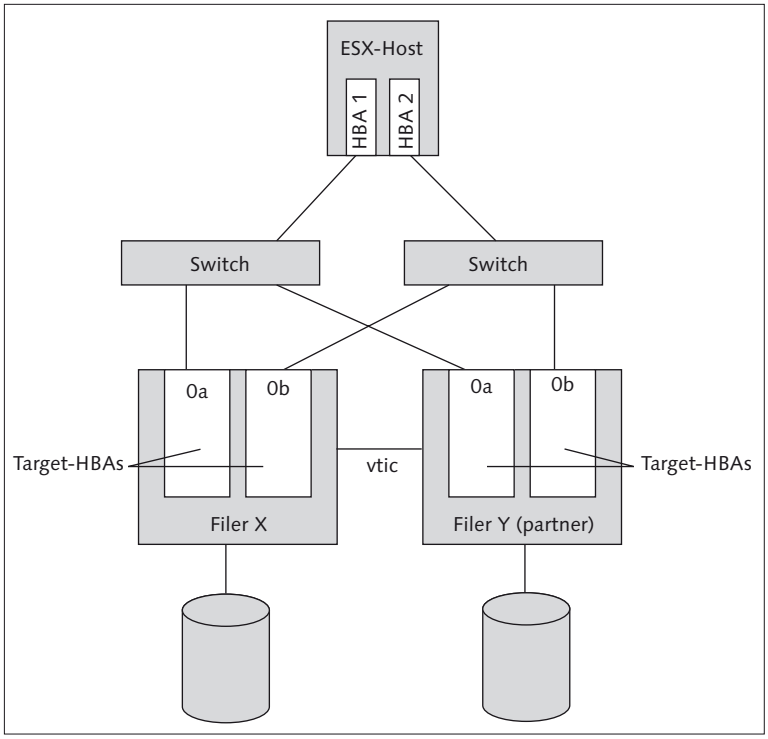


Abbildung 10.1 Blaupause einer Infrastruktur vom ESX-Host mit den entsprechenden HBAs bis zum redundanten Storage

Arbeiten an der Infrastruktur

Bevor Sie das Speichersystem oder den ESX-Host konfigurieren, müssen Sie zuerst die Infrastruktur aufbauen, verkabeln und konfigurieren. Bei Fibre-Channel sind damit konkret die Switches gemeint. Über das sogenannte *Zoning* werden Kommunikationswege im Fibre-Channel-Netzwerk festgelegt, also »welcher Host darf mit welchem Storage sprechen«. Das Zoning dient neben den offensichtlichen Sicherheitsgründen auch dem Ausschluss von Fehlern – Rechner, die nicht miteinander kommunizieren sollen, können sich dank des Zonings nicht stören. Das Zoning zeigen wir hier kurz anhand von Brocade-FCP-Switches:

```
br2003:admin> switchshow
switchName:   br2003
switchType:   34.0
switchState:  Online
switchMode:   Native
switchRole:   Principal
switchDomain: 1
switchId:     fffc01
switchWwn:    10:00:00:05:1e:04:54:09
zoning:       ON (c_vSphere)
```

```
switchBeacon: OFF

Area Port Media Speed State     Proto
==========================================
  0   0   id    N2   Online     F-Port  50:0a:09:81:96:68:33:2c
  1   1   id    N2   Online     F-Port  50:0a:09:81:86:68:33:2c
  2   2   id    N4   Online     F-Port  10:00:00:00:c9:70:3f:23
```

Es handelt sich bei `br2003` um einen der beiden Brocade-Switches aus der 200er-Serie. Auf den Ports 0 und 1 sind die beiden Target-Ports (0a) der NetApp-Controller na3021 und na3022, auf Port 2 ist ein ESX-Host angeschlossen. In der Praxis sähen Sie von allen ESX-Hosts jeweils einen Initiator-Port, hier haben wir lediglich ein einziges System zur Verfügung. Wichtig ist, dass Sie auch für die Initiatoren jedes ESX-Hosts eine eigene Zone anlegen, um spätere Probleme zu vermeiden. Sie sollten nie eine einzige Zone, die alle ESX-Host-Initiatoren und Target-Ports enthält, nutzen. Nun vergeben Sie für die nur schwer lesbaren WWPNs (World Wide Port Names) sprechende Namen, die »Aliasse«:

```
br2003:admin> alicreate "na1_p1","50:0a:09:81:96:68:33:2c"
br2003:admin> alicreate "na2_p1","50:0a:09:81:86:68:33:2c"
br2003:admin> alicreate "esx_p1","10:00:00:00:c9:70:3f:23"
```

Bei jeglicher Art von Zoning ist es übrigens sehr empfehlenswert, immer nur per Cut & Paste zu arbeiten und sich niemals dazu hinreißen zu lassen, die WWPNs per Hand einzugeben – das ist schlichtweg zu fehleranfällig. Anschließend erstellen Sie eine Zone, die Sie sich am einfachsten als eine Art »Kommunikationszone« vorstellen. Alle Geräte (genauer: alle Portnummern), die sich in dieser Zone befinden, dürfen miteinander kommunizieren:

```
br2003:admin> zonecreate "z_vSphere_Fabric1","na1_p1; na2_p1;
  esx1_p1"
```

Schließlich müssen Sie die gerade erstellte Zone noch zur laufenden Konfiguration hinzufügen oder wie hier – falls noch keine Konfiguration vorhanden ist – eine solche erstellen:

```
br2003:admin> cfgcreate "c_vSphere","z_vSphere_Fabric1"
```

Nun aktivieren Sie die eben erstellte Konfiguration des Switches – gespeichert wird anschließend immer automatisch:

```
br2003:admin> cfgenable "c_vSphere"
This action will replace the old zoning configuration with the
current configuration selected.
Do you want to enable 'c_vSphere' configuration  (yes, y, no, n): [no] y
zone config "c_vSphere" is in effect
Updating flash ...
```

Das Ergebnis des Zonings und die fertige Konfiguration für unsere Testumgebung mit einem ESX-Host und einem NetApp-Cluster (zwei Knoten) schaut auf dem Brocade-Switch wie folgt aus:

```
br2003:admin> cfgshow
Defined configuration:
 cfg:    c_vSphere
         z_vSphere_Fabric1
 zone:   z_vSphere_Fabric1
         na1_p1; na2_p1; esx1_p1
 alias:  esx1_p1     10:00:00:00:c9:70:3f:23
 alias:  na1_p1      50:0a:09:81:96:68:33:2c
 alias:  na2_p1      50:0a:09:81:86:68:33:2c

Effective configuration:
 cfg:    c_vSphere
 zone:   z_vSphere_Fabric1
      50:0a:09:81:96:68:33:2c
      50:0a:09:81:86:68:33:2c
      10:00:00:00:c9:70:3f:23
```

Die entsprechende Konfiguration müssen Sie anschließend auch noch in der anderen Fabric durchführen – quasi die gleiche Arbeit noch einmal machen, nur mit den anderen WWPNs der restlichen Initiator-Ports (auf ESX-Seite) und Target-Ports (auf NetApp-Seite). Hier nur zum Nachvollziehen die Befehle, ohne den gesamten Output zu wiederholen:

```
br2004:admin> alicreate "esx1_p2","10:00:00:00:c9:70:47:44"
br2004:admin> alicreate "na1_p2","50:0a:09:82:86:68:33:2c"
br2004:admin> alicreate "na2_p2","50:0a:09:82:96:68:33:2c"
br2004:admin> zonecreate "z_vSphere_f2","esx1_p2;na1_p2;na2_p2"
br2004:admin> cfgcreate "c_vSphere","z_vSphere_Fabric2"
br2004:admin> cfgenable "c_vSphere"
```

Ist auch dies geschafft, so ist die grundsätzliche Kommunikation hergestellt, und Sie stellen im nächsten Schritt auf dem Storage-System eine gewisse Menge Speicher für unseren VMware-Datastore zur Verfügung (Provisionierung).

Arbeiten am Storage-System

Um dem ESX-Host eine gewisse Menge Speicherplatz zur Verfügung zu stellen, müssen Sie zuerst auf der NetApp eine LUN anlegen. Diese LUN wird später vom ESX mit dem VMware-eigenen Cluster-File-System VMFS formatiert und somit zu einem nutzbaren Datastore, auf dem die Files für virtuelle Maschinen abgelegt werden.

Auf dem NetApp-Storage-System werden – anders als bei den meisten Herstellern – die LUNs nicht direkt auf einer RAID-Gruppe eingerichtet. LUNs sind bei NetApp immer in einem Container abgelegt, dem sogenannten *Volume*. Bildlich können Sie sich vorstellen, dass eine LUN nur eine sehr große Datei in einem Volume ist – ähnlich wie ein VMDK-Disk-Image auch nur eine sehr große Datei in einem normalen Dateisystem ist (z. B. in einem NTFS-File-System im Falle von VMware Workstation). Deshalb müssen Sie zuerst ein Volume anlegen. Dieses

Volume ist wiederum ein Bestandteil eines sogenannten *Aggregats*, das – vereinfacht gesprochen – ein großer RAID-Verbund auf einer NetApp ist. Wir gehen davon aus, dass ein Aggregat bereits vorhanden ist, weil das Anlegen der Aggregate auf NetApp-Systemen meistens schon bei der Grundinstallation erfolgt.

Das Volume erstellen Sie wie folgt:

```
na3021> vol create esxfcp aggr0 500g
Creation of volume 'esxfcp' with size 500g on containing aggregate 'aggr0' has
completed.
```

Da in diesem Volume nur LUNs (und keine Files) abgelegt werden, sollten Sie die Snapshot-Reserve abschalten – auch den automatischen Snapshot-Scheduler müssen Sie deaktivieren:

```
na3021> snap reserve esxfcp 0
na3021> vol options esxfcp nosnap on
```

Als Ergebnis steht der gesamte angegebene Platz von 500 GB zur Verfügung.

Nun legen Sie in diesem Volume eine LUN mit 100 GB an. Wegen des Parameters `-o noreserve` ist die LUN thin-provisioned, brauchen also weniger Platz, als sie groß sind (mehr dazu erfahren Sie auf Seite 546 im Abschnitt »Thin Provisioning«):

```
na3021> lun create -s 100g -t vmware -o noreserve
  /vol/esxfcp/fcp_ds1.lun
```

Generell sollten Sie Ihre LUNs nicht zu groß oder klein erstellen, da einige Faktoren abzuwägen sind:

Backup- und Restore-Zeiten

Je nachdem, wie gesichert wird, dauern das Backup und die Rücksicherung einer sehr großen LUN unter Umständen zu lange, um die vorgegebenen SLAs (Service-Level Agreements) und die damit verbundenen Rücksicherungszeiten (RTO: Recovery Time Objectives) einzuhalten.

Anzahl der VMs pro LUN

Viele virtuelle Maschinen pro LUN haben zwar den Vorteil, dass Sie insgesamt weniger Datastores verwalten müssen, allerdings wird dadurch auch die Performance negativ beeinflusst, da ein VMFS in Version 3 bei Metadatenupdates die gesamte LUN sperrt (SCSI-Locking). Je mehr VMs, desto mehr Metadatenupdates und auch mehr Locks. Diese durch Locks induzierte Problematik wurde in VMFS-5 deutlich verbessert, fällt also nicht mehr so stark ins Gewicht. Dieses verbesserte Locking funktioniert durch die VAAI-Integration mit unterstützten Storage-Arrays und bietet die Möglichkeit, nur noch Byte-Range-Locks auf die LUN durchzuführen. Weil die LUN nun nicht mehr komplett gesperrt ist, sondern nur noch ein kleiner Bereich, kommt es zu deutlich weniger Geschwindigkeitsverlust. Der verwendete SCSI-Mechanismus der VAAI heißt *Atomic Test & Set* (ATS) und wird NetApp-seitig ab der Betriebssystemversion Data ONTAP 8.0.1 im 7-Mode unterstützt.

Die Anzahl der VMs pro LUN hängt auch von den Outstanding I/Os auf dem Storage-Array ab (LUN Queue Length). Unterstützt das Array z. B. 256 I/Os pro LUN und erzeugt eine durchschnittliche VM vier I/Os pro Sekunde, so sollten Sie maximal 64 VMs pro Datastore ablegen (256 / 4 = 64). Best Practice ist aber aus der Praxiserfahrung, maximal ca. 30 VMs pro LUN-Datastore abzulegen. Diese Zahlen sind in jedem Fall abhängig vom Lastverhalten der virtuellen Maschinen und davon, wie stark Snapshots und Thin Provisioning bei virtuellen Maschinen genutzt wird.

In unserem Fall gehen wir von ca. 25 GB Platzverbrauch pro virtueller Maschine aus, somit könnten wir auf einem 500-GB-Datastore circa 20 VMs ablegen; da aber Auslagerungsdateien und VM-Snapshots auch Platz belegen, lautet die Empfehlung, nur etwa 15 VMs einzurichten. Die dabei augenscheinlich entstehende Platzverschwendung existiert aber nicht, da die LUN mit Thin Provisioning erstellt wurde, also nicht sofort den gesamten Platz belegen. Mehr Details und Hintergründe zu Thin Provisioning finden Sie im Abschnitt »Thin Provisioning«.

An diesem Punkt sind wir so weit, dass:

- die ESX-Hosts und der NetApp-Cluster sich aufgrund des Zonings bereits »sehen« können,
- auf dem NetApp-System eine LUN erstellt wurde.

Jetzt ist es noch notwendig, die LUN auch den ESX-Hosts zu »zeigen«, in Fachtermini spricht NetApp vom sogenannten *Mapping*. Andere Hersteller bezeichnen einen ähnlichen Vorgang als *Masking*. Eine LUN wird nie direkt an eine WWPN des ESX-Hosts gezeigt, sondern immer nur an eine Gruppe von WWPNs, da ja ein einzelner Host meist mehrere FC-Adapter und somit auch mehrere WWPNs besitzt. Diese Gruppe von WWPNs wird als *Initiator-Group* oder kurz *iGroup* bezeichnet. Im Falle des ESX-Clusters ist ja sogar erwünscht, dass mehrere Hosts auf die gleiche LUN zugreifen (»Shared Storage«), also sollten Sie die LUN in diesem Fall auch an alle sichtbaren ESX-Hosts zeigen – Sie nehmen einfach alle WWPNs in die iGroup auf. Die momentan verbundenen Initiator-WWPN lassen Sie sich wie folgt anzeigen:

```
na3021> fcp show initiator
Initiators connected on adapter 0a:
Portname                 Group
--------                 -----
10:00:00:00:c9:70:3f:23

Initiators connected on adapter 0b:
Portname                 Group
--------                 -----
10:00:00:00:c9:70:47:44
```

Sie sehen also zwei Initiatoren, einen über jeden FC-Target-Port des Storage-Systems. Anschließend nehmen Sie diese in die neue Initiator-Group auf:

```
na3021> igroup create -f -t vmware esxfcp_all
na3021> igroup add esxfcp_all 10:00:00:00:c9:70:47:44
```

```
na3021> igroup add esxfcp_all 10:00:00:00:c9:70:3f:23
na3021> igroup show
        esxfcp_all (FCP) (ostype: vmware):
        10:00:00:00:c9:70:47:44 (logged in on: 0b, vtic)
        10:00:00:00:c9:70:3f:23 (logged in on: 0a, vtic)
```

Die beiden WWPNs sind also in der iGroup, und Sie sehen sehr schön, dass jede WWPN zweimal eingeloggt ist: einmal direkt über den Adapter 0a oder 0b, und ein zweites Mal indirekt über den VTIC, den **V**irtual **T**unnelled **I**nter**c**onnect. NetApp verwendet im FCP-Umfeld einen Cluster-Modus (*cfmode)*, der sich *single_image* nennt.

Die beiden Cluster-Knoten des NetApp-Storages, die ja eigentlich zwei Systeme sind, melden sich den Hosts gegenüber als ein einziges System – eben dem Single Image –, indem sie die gleiche WWNN (World Wide Node Name) präsentieren. Der Host sieht also ein und dieselbe LUN über vier Pfade: die zwei direkten und die zwei indirekten, die über den Cluster-Partner laufen.

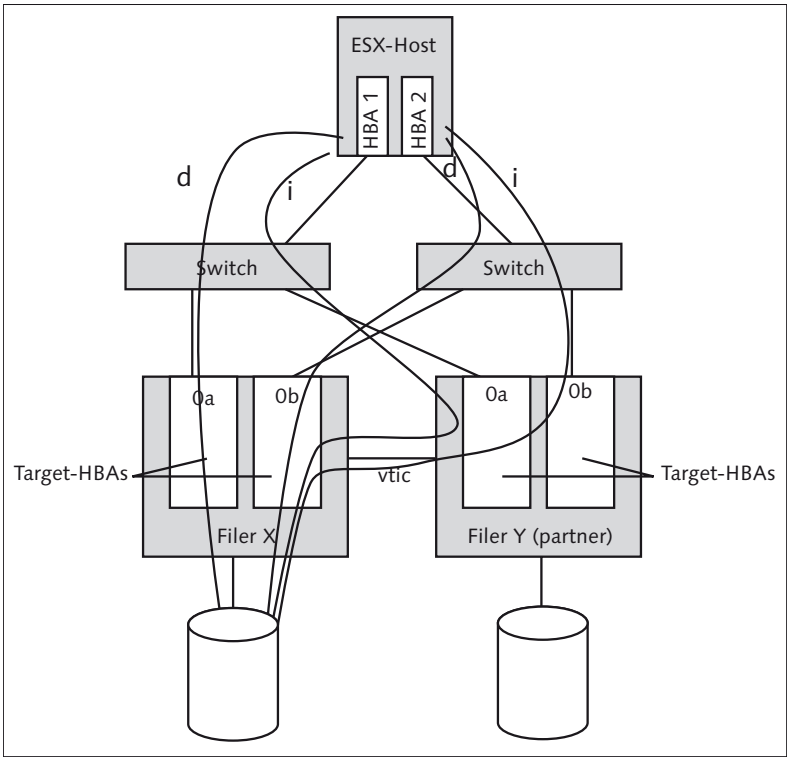


Abbildung 10.2 Direkte (d) und indirekte (i) Pfade im Überblick

Die beiden direkten Pfade sind dabei den indirekten vorzuziehen, da die indirekten Pfade über den NetApp-Cluster-Interconnect transportiert werden, was zu höherer Last auf dem Partner führt, den Interconnect unnötig belastet und auch gesteigerte Latenz mit sich bringt.

Stellt die Multipathing-Software auf dem ESX-Host die Pfade nicht korrekt ein, bekämen Sie auf der NetApp die Fehlermeldung »FCP Partner Path misconfigured«.

Unter ESX 3.x war es noch nötig, die bevorzugten Pfade auf dem Host manuell auszuwählen oder ein NetApp-Tool zur Auswahl zu installieren (FCP Host Utilities); seit Version vSphere 4 können Sie auf dem ESX-Host und dem NetApp-Speichersystem auch einfach das Feature ALUA (Asymmetric LUN Access) aktivieren – die NetApp teilt dem ESX-Host über das SCSI-Protokoll mit, welche Pfade zu bevorzugen sind. Neu seit ESX 4 ist auch, dass Sie nun pro LUN mehrere Pfade gleichzeitig aktiv nutzen, also echtes Load-Balancing mit Round Robin beim Loadbalancing realisieren können. Also schalten Sie für die iGroup auf der NetApp-Seite ALUA ein (ALUA ist bei NetApp nur im Fibre-Channel-Umfeld zu nutzen):

```
na3021> igroup set esxfcp_all alua yes
```

Im letzten Schritt sollten Sie auf dem NetApp-System noch die Verbindung zwischen der LUN und der iGroup herstellen – Sie müssen das LUN-Mapping durchführen. Beachten Sie dabei, dass LUN-IDs nie doppelt vergeben werden dürfen – sowohl in der selben iGroup als auch über die beiden Cluster-Knoten hinweg, da sich ja beide Knoten dem Host gegenüber wie das gleiche Speichersystem ausweisen. Beim Umgang mit ALUA empfiehlt NetApp aus Gründen der Übersichtlichkeit, die iGroups auf beiden Cluster-Partnern anzulegen, nicht nur auf dem Controller, dem die LUNs gehören.

Das LUN-Mapping ist relativ einfach und logisch zu erklären, im Prinzip wird nur konfiguriert: »Welche LUN zeige ich welcher iGroup als welche ID?«

```
na3021> lun map /vol/esxfcp/fcp_ds1.lun esxfcp_all 111
na3021> lun show -m
LUN path                Mapped to    LUN ID  Protocol
----------------------------------------------------------
/vol/esxfcp/fcp_ds1.lun  esxfcp_all   111      FCP
```

Nun sind alle Tätigkeiten zum Provisionieren von LUN-Storage auf NetApp-Seite geschafft:

- Volume angelegt
- LUNs angelegt
- iGroup erstellt
- LUNs an iGroup gemappt

Jetzt können Sie zum ESX-Host wechseln, um die bereitgestellten LUNs zu finden und anschließend als VMFS-Datastore zu labeln (formatieren).

Arbeiten am ESX-Host

Damit Sie die neuen Block-Devices (unsere eben erstellten LUNs) auf dem ESX-Host finden, müssen Sie zunächst einmal an den entsprechenden Host-Bus-Adaptern nach neuen Geräten suchen.

Um die folgenden Vorgänge anschaulicher zu gestalten, demonstrieren wir die Beispiele anhand von Screenshots. Für die Arbeiten ist ein Virtual Infrastructure Client nötig, der sich entweder direkt auf einen ESX-Host verbindet oder auf einen vCenter-Server, der den entsprechenden Host verwaltet.

Im Reiter KONFIGURATION wählen Sie SPEICHERADAPTER aus; Abbildung 10.3 zeigt die vorhandenen Fibre-Channel-Karten vom Hersteller Emulex und deren dazugehörige WWPN, die wir schon bei der NetApp-Konfiguration mit in die iGroup genommen haben. Das Bild zeigt noch einen dritten HBA, den Sie aber ignorieren können; wichtig sind die HBAs VMHBA1 und VMHBA6.

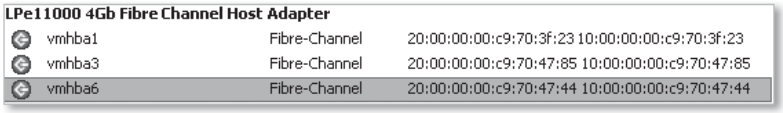


Abbildung 10.3 Die Speicheradapter und ihre WWPNs

Nun scannen Sie auf diesen HBAs nach neuen Geräten. Es gibt zwei Arten von Scans: Die »kleine« Variante durchsucht nur einen speziellen ausgewählten Adapter (Rechtsklick auf den gewünschten Adapter) nach neuen LUNs/Targets und ignoriert den Inhalt der gefundenen LUNs. Den etwas ausführlicheren Scan hingegen erreichen Sie per Klick auf ERNEUT PRÜFEN oben rechts im Bild; er scannt alle vorhandenen Adapter gleichzeitig nach neuen LUNs/Targets und prüft, ob auf den neu gefundenen LUNs bereits ein VMFS (VMware Filesystem) vorhanden ist. Neu seit vSphere 4 ist eine Möglichkeit, auch gesamte Hosts und deren HBAs zu scannen, ebenso neu ist die Möglichkeit, den gesamten Cluster zu scannen. Dazu klicken Sie rechts auf den Cluster und wählen den entsprechenden Menüpunkt, siehe Abbildung 10.4.

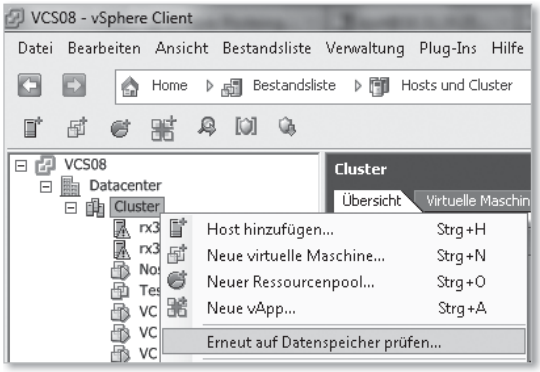


Abbildung 10.4 Gesamten Host oder Cluster nach neuen LUNs scannen

Wir wählen den ausführlicheren Scan, damit alle Adapter geprüft werden.

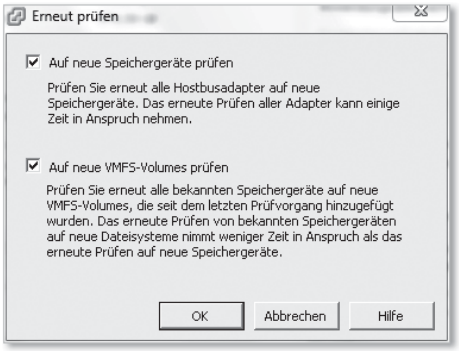


Abbildung 10.5 Beim ausführlichen Scan Geräte und VMFS-Volumes suchen

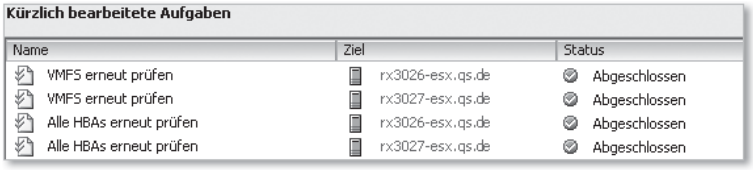


Abbildung 10.6 Der Scan wird als Task angezeigt.

Nach dem Scan wird die LUNs gefunden, wie Abbildung 10.7 zeigt. Die gleiche LUN wird natürlich auch noch einmal auf dem anderen HBA angezeigt.

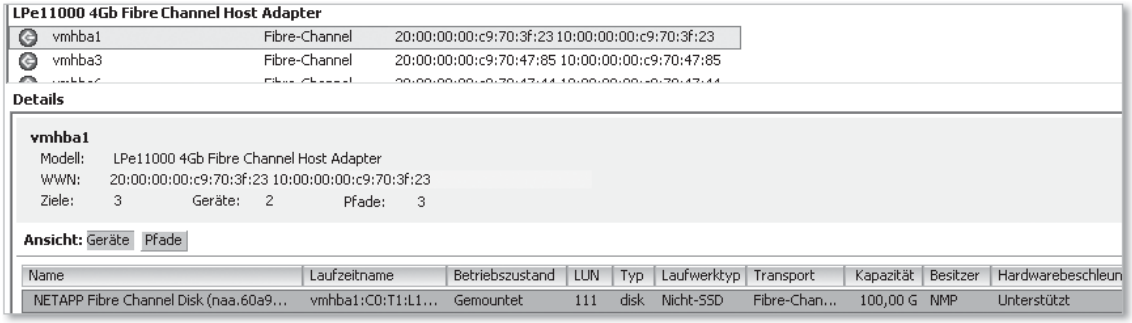


Abbildung 10.7 Am vmhba1 wird die 100-GB-LUN erkannt.

Nachdem unsere LUN nun erkannt wurde, müssen wir prüfen, ob sie auch die volle Redundanz der Pfade besitzt. Ein Rechtsklick auf die LUN und die Auswahl Pfade verwalten zeigt vier Pfade zur selben LUN.

Warum es vier Pfade zur gleichen LUN gibt, haben wir im vorherigen Abschnitt schon erklärt, und an dieser Stelle sehen Sie diese Tatsache sehr schön. Auf der rechten Seite in Abbildung 10.8 erkennen Sie, dass alle vier Pfade funktionieren (Aktiv) und die I/O-Befehle (E/A) automatisch über zwei verschiedene Pfade per Round-Robin verteilt werden. Dies ist der Idealzustand: Beide Controller und beide Fibre-Channel-Fabrics werden gleichzeitig ausgelastet.

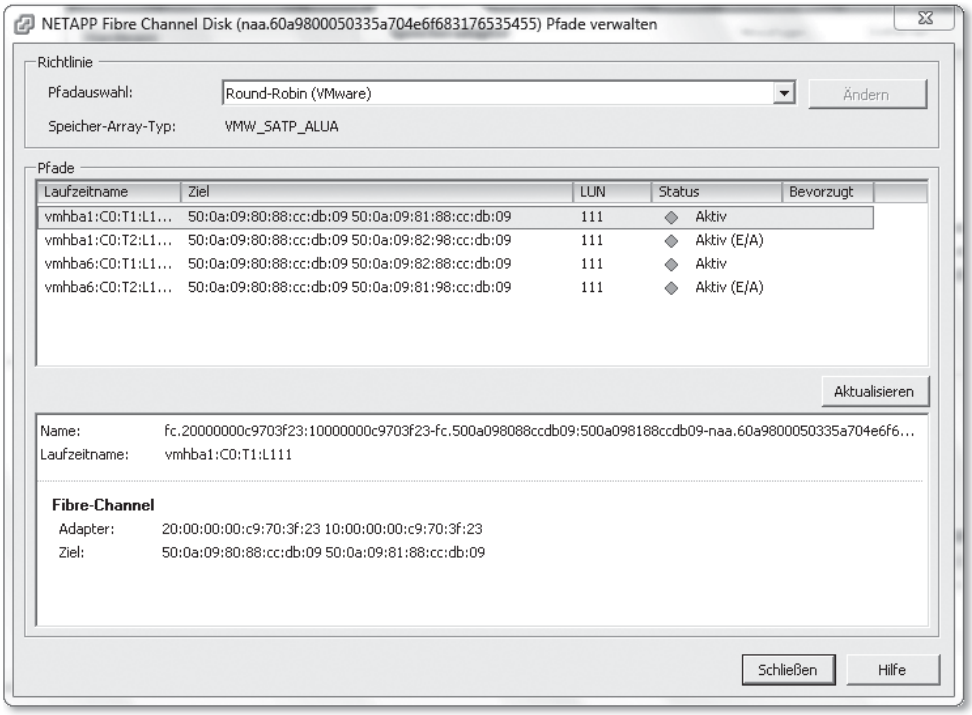


Abbildung 10.8 Vier Pfade zur gleichen LUN

Bei den Multipathing-Einstellungen kann es zu zwei typischen Fehlern kommen: Entweder wird vergessen, auf Storage-Seite ALUA zu aktivieren, oder die Round-Robin-Konfiguration wird bei der Pfadauswahl nicht eingeschaltet. Dann laufen die I/Os über falsche oder zu wenige Pfade. Das liegt daran, wie das Native Multipathing von vSphere funktioniert: Zuerst erkennt ein Storage-Array-Type-Plugin (SATP) den Typ des Speichersystems, anschließend wird durch das Path-Selection-Plugin (PSP) festgelegt, wie die I/Os über die verschiedenen Pfade verteilt werden. Die Standardeinstellung des PSP für ALUA ist VMW_PSP_MRU, oder Most Recently Used. Also immer nur ein Pfad, und zwar der letzte, der aktiv war.

Sollte bei der Pfadanzeige wie in Abbildung 10.9 noch VMWARE_DEFAULT_AA anstelle von ALUA stehen, so wurde die iGroup nicht richtig auf ALUA umgestellt. Nach der Umstellung muss der Host neu gestartet werden, ein Rescan reicht nicht aus.

Um optimale Performance zu den LUNs zu bekommen, sollten Sie das Load-Balancing nach Round-Robin-Algorithmus aktivieren – dadurch werden die I/Os über alle direkten Pfade zum NetApp-Controller geschickt. Welche die direkten Pfade sind und welche die indirekten, teilt die NetApp dem ESX-Host über die ALUA-SCSI-Kommandos automatisch mit.

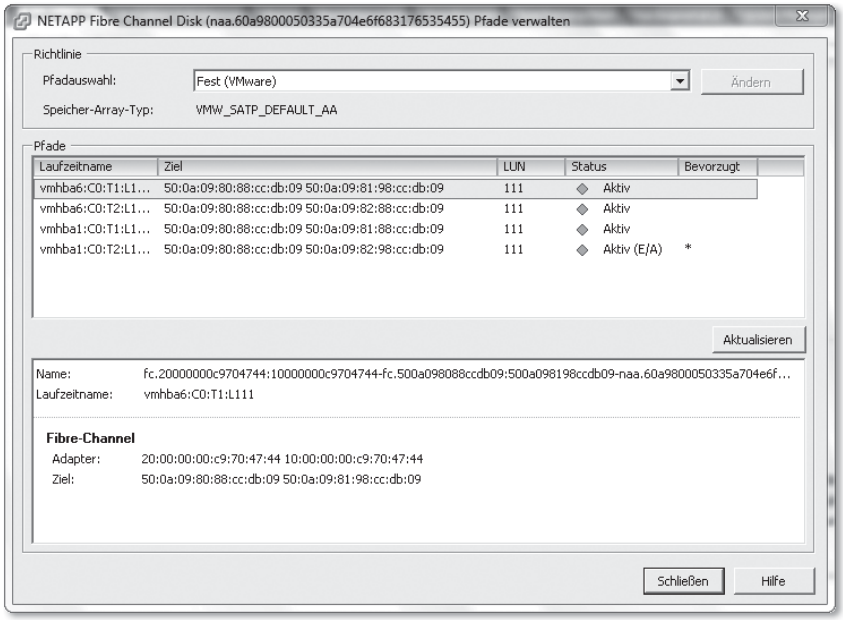


Abbildung 10.9 Kein »ALUA SATP«, nur »DEFAULT_AA«

Die Voraussetzung dafür ist, dass wir das Native-Multipathing-Plugin (NMP) von ESX informieren, welche Art von Path Selection Policy (PSP) durchgeführt werden soll. Einzelne LUNs können Sie im GUI in der Pfadverwaltung auf PSP: Round-Robin umkonfigurieren. Möchten Sie aber als Standardeinstellung festlegen, dass für ALUA generell Round-Robin-Load-Balancing durchgeführt wird, so müssen Sie dies auch in der aktuellen Version 5.0 weiterhin über die Kommandozeile im ESXi eingestellt werden:

```
[root@esx~]# esxcli storage nmp satp set
                    -s VMW_SATP_ALUA -P VMW_PSP_RR
Default PSP for VMW_SATP_ALUA is now VMW_PSP_RR
```

Anschließend sollte der ESX-Host beide direkten Pfade zur LUN parallel für I/Os benutzen – die I/Os werden gleichmäßig über beide Pfade verteilt. Die Troubleshooting-Software ESXTOP zeigt die Lastverteilung, siehe Abbildung 10.10.

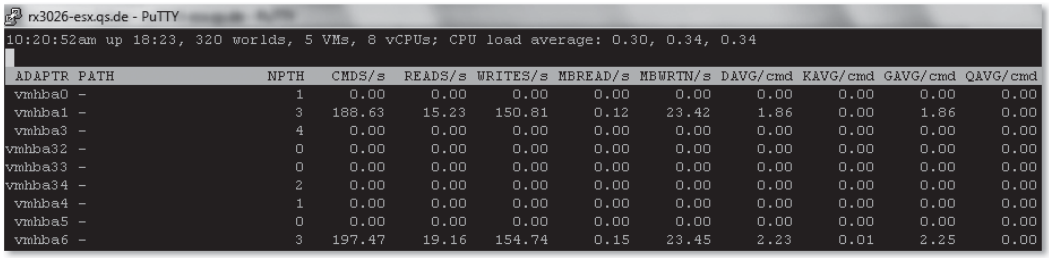


Abbildung 10.10 ESXTOP: gleichmäßige Lastverteilung auf vmhba1 und 6

Nachdem an diesem Punkt die LUNs erkannt wurden und Sie das Load-Balancing sowie gegebenenfalls die Nutzung der Pfade korrigiert haben, müssen Sie die LUNs mit VMFS-Dateisystem formatieren – dadurch erst werden sie zu einem Datastore.

Diesen Vorgang können Sie sowohl grafisch als auch auf der Kommandozeile erledigen. Hier die grafische Variante.

Abbildung 10.11 Speicher hinzufügen

Wählen Sie im Reiter KONFIGURATION den Menüpunkt SPEICHER, und klicken Sie auf den Knopf SPEICHER HINZUFÜGEN.

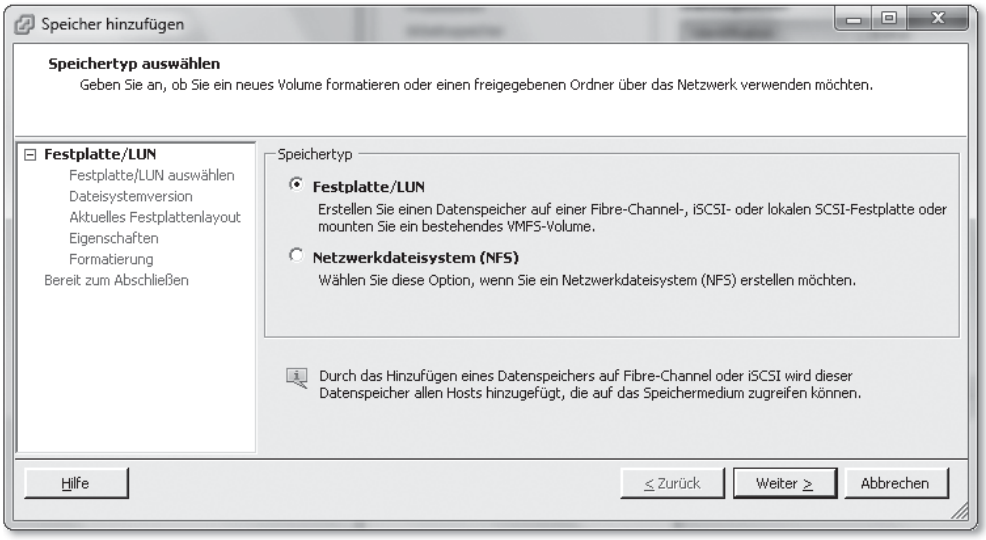


Abbildung 10.12 FC ist Blockspeicher, eine LUN.

Wählen Sie FESTPLATTE/LUN, da ein Blockspeicher formatiert werden soll. Der gleiche Vorgang wird übrigens auch für lokale Festplatten und RAIDs sowie für iSCSI durchgeführt. Die andere Auswahl, NETZWERKDATEISYSTEM (NFS), erklären wir in Abschnitt 10.2.3, »NFS-Datastores«.

Es werden alle gefundenen Geräte ohne Partitionstabelle angezeigt – da davon ausgegangen wird, dass sie leer sind – sowie Geräte mit freien, nicht partitionierten Bereichen. Wir wählen unsere leere LUN.

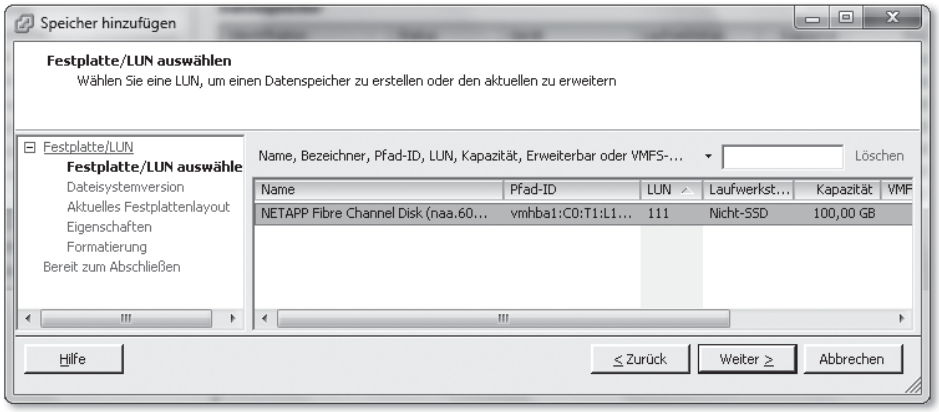


Abbildung 10.13 Wählen Sie die noch leere LUN aus.

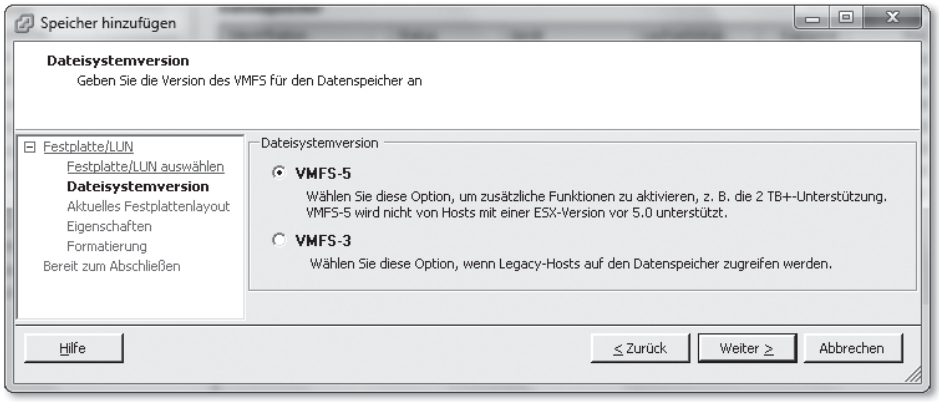


Abbildung 10.14 Auswahl: VMFS-5 oder das alte VMFS-3

Im nächsten Fenster wählen Sie, ob Sie das Dateisystem im aktuellen Format der Version 5 anlegen wollen oder ob Sie aus Gründen der Abwärtskompatibilität noch die Version 3 verwenden wollen. Generell ist aus Performance- und Platzgründen die aktuelle Version 5 immer vorzuziehen.

In diesem Schritt vergeben Sie einen sprechenden Namen für den Datastore. Die Empfehlung lautet, den Namen des beherbergenden Speichersystems, das Speicherprotokoll und eventuell die LUN-ID mit in den Namen aufzunehmen. Dadurch behalten Sie später, wenn mehrere LUNs vorhanden sind, einen besseren Überblick.

Im folgenden Dialogfeld können Sie noch die Größe des Datastores auf der LUN einstellen; die Empfehlung lautet, immer die gesamte LUN zu verwenden, also »Platz maximieren«. Eine LUN aufzuteilen ist nicht sinnvoll, da LUNs ja auf modernen Speichersystemen in beliebigen Größen erstellt werden können – wer also einen kleineren Datastore haben möchte, der sollte einfach eine kleinere LUN provisionieren.

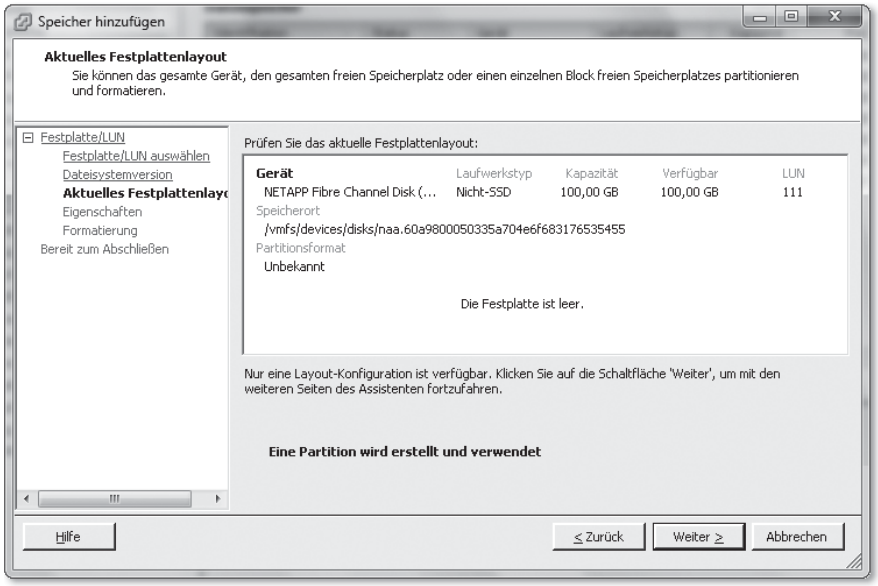


Abbildung 10.15 Informationen über den aktuellen Zustand der LUN (leer)

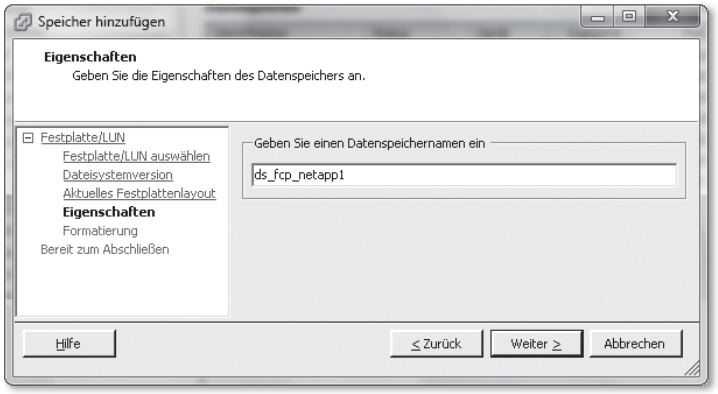


Abbildung 10.16 Namen für den Datastore wählen

Im alten VMFS-3 konnte zusätzlich die Blockgröße eingestellt werden, aus historischen Gründen sei dieser Parameter noch kurz erklärt: Von der Blockgröße des File-Systems leitet sich die maximale Größe einer einzelnen Datei innerhalb des VMFS ab. Die Standardauswahl von 1 MB Blocksize sollte für die meisten Anwendungen reichen, da hieraus eine Dateigröße von 256 GB resultiert, also eine VMDK-Datei nicht größer als 256 GB werden darf. Positive Auswirkungen auf die Performance sind bei verschiedenen Blockgrößen eher minimal (+1–3 %), dafür ist der Platzverschnitt bei sehr kleinen Dateien relativ groß. Die Empfehlung ist: Falls Sie nicht planen, VMDK-Dateien mit mehr als 256 GB Größe zu erstellen, sollten Sie den Wert von 1 MB beibehalten.

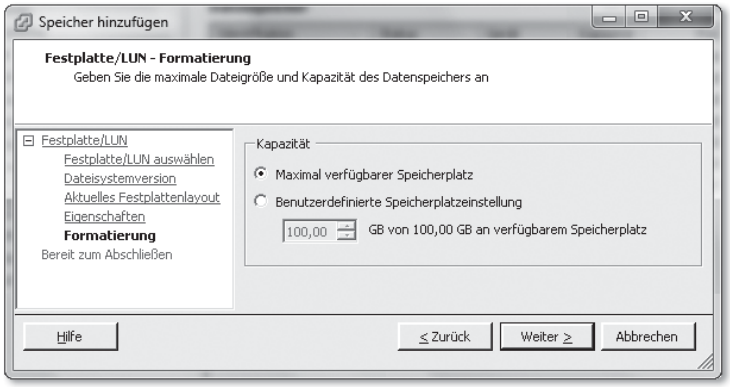


Abbildung 10.17 Kapazität maximieren, also LUN komplett verwenden

In VMFS-3 durften (unabhängig von der Blockgröße!) die Dateisysteme ohne Nutzung von Extents maximal 2 TB groß werden, durch die Nutzung der maximalen Anzahl von 32 Extents konnte das VMFS-3 dann 64 TB groß werden. Die 2-TB-Beschränkung rührte daher, dass LUNs in vSphere 4 nur 2 TB groß sein durften. In der aktuellen Version VMFS-5 ist die Beschränkung der LUN-Größe aufgehoben; eine LUN darf 64 TB groß werden, und das darin liegende VMFS-5 ebenfalls.

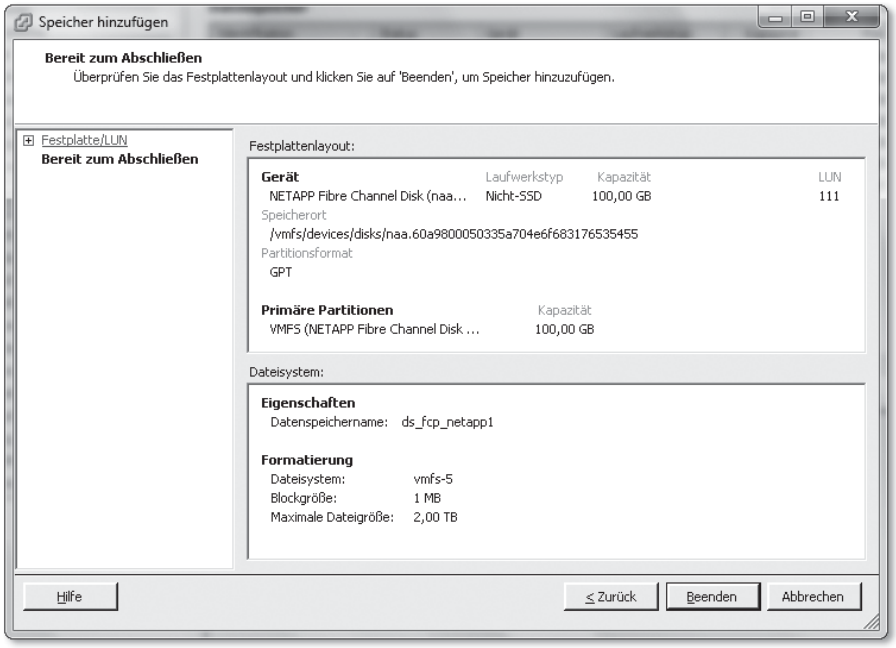


Abbildung 10.18 Zusammenfassung der Datastore-Einstellungen

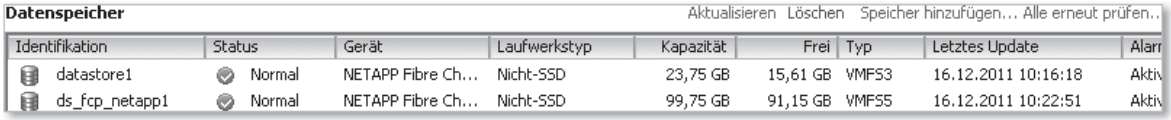


Abbildung 10.19 Der neue, 100 GB große VMFS-5-FC-Datastore ist fertig.

Abschließend werfen wir in Abbildung 10.20 noch einen kurzen Blick auf die EIGENSCHAFTEN des Datastores.

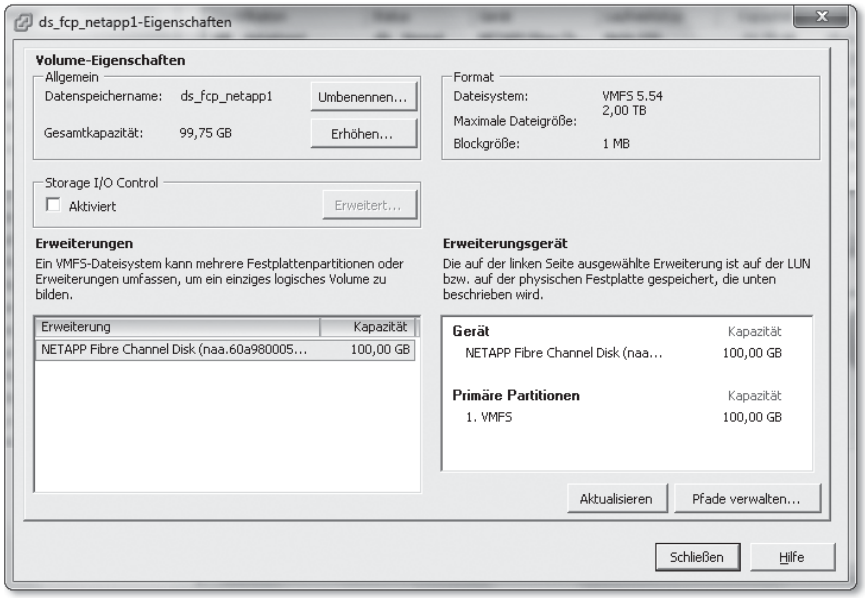


Abbildung 10.20 Datastore-Eigenschaften

Nachdem Sie nun erfolgreich den Datastore angelegt haben, können Sie ihn für virtuelle Maschinen oder ISO-Files verwenden.

10.2.2 iSCSI

Nach der »klassischen« Anbindung von ESX-Hosts an das Speichersystem über Fibre-Channel-Technologie betrachten wir nun eine Alternative: iSCSI. Wie der »SCSI«-Teil des Namens schon suggeriert, handelt es sich dabei um blockorientierten Storage, allerdings werden die SCSI-Kommandos und die Daten nicht über FC transportiert, sondern über IP. iSCSI erfreut sich steigender Beliebtheit, da viele Administratoren aus dem kleineren Mittelstand vor einer Investition in Fibre-Channel zurückschrecken, sowohl hinsichtlich Switches als auch, was das Erlernen von neuem Wissen angeht. iSCSI dagegen ist relativ schnell einsetzbar, weil oft Netzwerkkenntnisse vorhanden sind und die Netzwerk-/LAN-Infrastruktur sowieso.

Wo für FCP noch zwingend HBAs gekauft werden müssen, haben Sie bei iSCSI die Wahl: Kaufe ich einen iSCSI-HBA, oder nehme ich einen iSCSI-Softwaretreiber, der die vorhandene LAN-Karte verwendet? Beide haben Vor- und Nachteile: Die iSCSI-HBA-Karte belastet die Host-CPU weniger und erlaubt das Booten von iSCSI-LUNs, kostet aber Geld und einen PCI-Slot. Softwaretreiber belasten die CPU, sind nicht bootfähig – dafür aber sind sie meist kostenlos. Seit ESXi (Achtung: nur ESXi, nicht ESX Classic!) 4.1 ist es möglich, mit manchen normalen Netzwerkkarten auch über Software-iSCSI zu booten: Die Funktion nennt sich *iSCSI Boot Firmware Table*, kurz iBFT, und erfordert eine spezielle Firmware auf der Netzwerkkarte. Für die meisten gängigen Intel- und Broadcom-Karten ist eine solche Firmware aber kostenlos beim Hersteller verfügbar, viele Hersteller liefern ihre Server bereits heute mit einer solchen Firmware für die On-Board-LAN-Karten aus.

Diese Belastung der CPU durch Software-iSCSI können Sie selbst bei aktuellen Prozessoren nicht komplett außer Acht lassen. Die Erfahrung aus der Praxis zeigt, dass bei einem modernen Nehalem XEON 2 bis 3 Gigabit pro Sekunde iSCSI-Traffic die Rechenleistung eines gesamten Cores in Anspruch nimmt. Das sollten Sie beim Sizing des ESX-Hosts beachten.

Arbeiten an der Infrastruktur

Für iSCSI ist bei der Infrastruktur eigentlich nur das LAN wichtig, allerdings gibt es hier auch einiges zu beachten, um optimale Ergebnisse zu erzielen. Die LAN-Switches sollten auf keinen Fall überbucht sein, das heißt, Sie müssen auf allen Ports, die mit iSCSI zu tun haben, darauf achten, dass wirklich volle 1 GBit/s zur Verfügung stehen. Viele Switch-Hersteller überbuchen ihre Switches, es ist also nicht auf allen Ports die volle Bandbreite verfügbar – das kann zu erheblichen Performanceeinbußen führen. Sie sollten sich nicht von der Namhaftigkeit eines Switch-Herstellers blenden lassen, sondern am besten die technische Spezifikation zu Rate ziehen. Erfahrungen haben gezeigt, dass z. B. ein 48-Port-Einschub-Modul mit 1-GBit-Ports eines bekannten Switch-Herstellers nur über 8 GBit/s auf der Backplane verfügt, der Switch also um Faktor 1 : 6 überbucht ist.

In puncto Redundanz sei angemerkt, dass es bei iSCSI nicht sinnvoll ist, einen EtherChannel (oder LACP, je nach Hersteller) zu bauen – es steigt dadurch weder die Geschwindigkeit (IP-Hash-Verteilung funktioniert bei einer einzigen Quell- und einer einzigen Ziel-IP nicht) noch die Redundanz (wenn die Uplink-Ports des vSwitches auf den gleichen LAN-Switch verbunden sind). iSCSI bildet Redundanz durch das Feature Multiple Connections per Session (MCS) ab, dabei werden für eine iSCSI-Verbindung mehrere TCP-Connections zwischen Initiator und Target aufgebaut. Diese Verbindungen verhalten sich dann wie mehrere Pfade im Fibre-Channel-Umfeld: Es ist möglich, im Fehlerfall einen Failover zwischen Pfaden zu erreichen, und die I/Os können per Round-Robin über beide Links verteilt werden.

Für optimale Redundanz und Performance sollten Sie im Zusammenhang mit iSCSI einen eigenen vSwitch konfigurieren, der mit zwei Uplinks auf verschiedene physische Switches verbunden ist. An diesem vSwitch müssen Sie zwei Portgruppen erstellen, jeweils vom Typ »VMkernel«; diese werden die iSCSI-Connections bedienen (siehe Abbildung 10.23).

Sehr wichtig ist, dass jede dieser Portgruppen nur einen aktiven Uplink besitzt, der andere Port muss zwingend auf »UNUSED« stehen, *nicht* auf »STANDBY«, sonst kommt es später zu Fehlermeldungen. Die Fehler rühren daher, dass der VMKernel nicht mit »STANDBY«-Interfaces umgehen kann. Ein LAN Interface muss »AKTIV« sein oder eben »UNUSED«! Die korrekten Einstellungen entnehmen Sie Abbildung 10.21 und Abbildung 10.22.

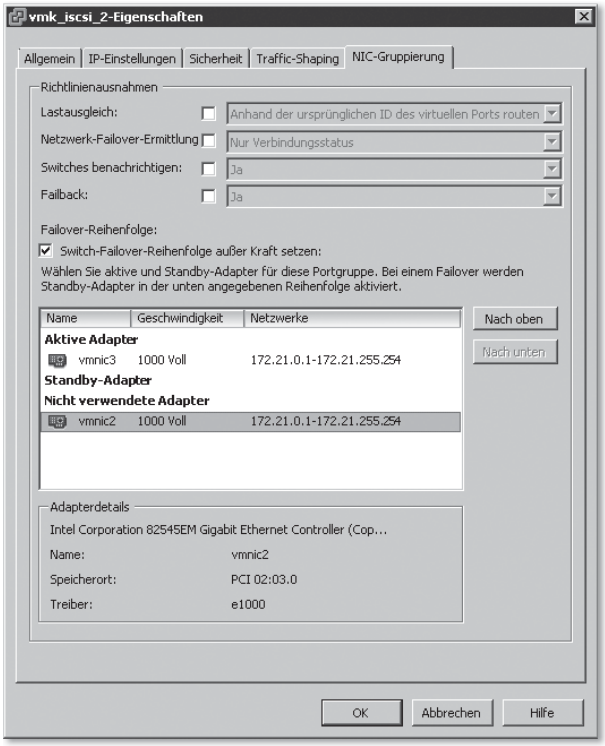


Abbildung 10.21 Pro Portgruppe: ein Adapter »active«, der andere »unused«

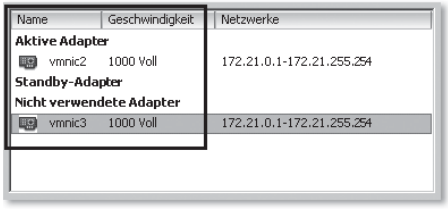


Abbildung 10.22 Bei der anderen Portgruppe genau umgekehrt

Die genauere Konfiguration der iSCSI-Software-HBAs und der Portgruppen zeigen wir in Abbildung 10.26 und in Abbildung 10.27, an dieser Stelle sind nur die Vorarbeiten im LAN-Umfeld wichtig.

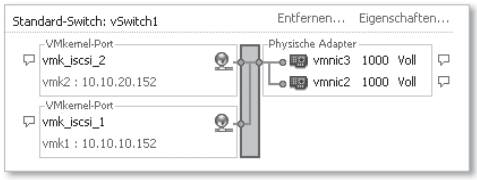


Abbildung 10.23 vSwitch mit zwei VMkernel-Portgruppen

Um iSCSI noch leistungsfähiger zu gestalten und die CPU-Auslastung auf dem ESX-Host möglichst niedrig zu halten, ist der Einsatz von Jumbo-Frames im Netzwerksegment möglich. Jumbo-Frames sind LAN-Frames mit einer Größe von 9 K (statt der normalen Maximum Transfer Unit von 1.500 Bytes). Da typische I/O-Größen von VMs zwischen 4 K und 8 K liegen, passen die meisten I/Os in einen einzigen LAN-Frame, die Latenz sinkt durch ausbleibende Segmentierung. Bei Jumbo-Frames ist zu beachten, dass *alle* Komponenten in diesem LAN-Segment oder VLAN eine MTU von 9.000 besitzen müssen! Sobald ein einziges Gerät in dem Jumbo-Layer-2-Segment eine kleinere MTU besitzt, wird es zu massiven Fehlern und Performanceproblemen wegen abgeschnittener Ethernet-Frames kommen!

Falls Sie sich für Jumbo-Frames entscheiden sollten, so müssen Sie zuerst den vSwitch auf MTU 9000 einstellen, anschließend beide VMkernel-Ports, siehe Abbildung 10.24 und Abbildung 10.25.

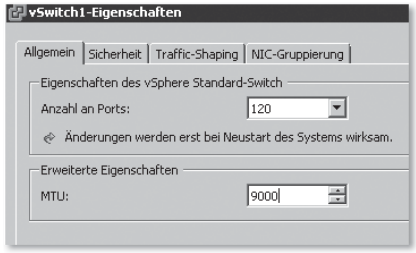


Abbildung 10.24 vSwitch MTU auf 9000 einstellen

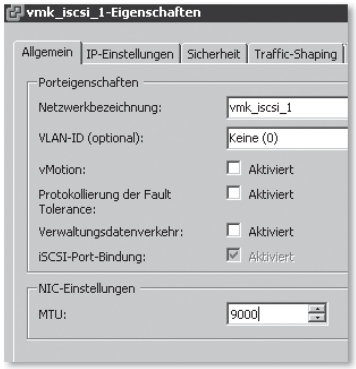


Abbildung 10.25 MTU der VMkernel-Ports auf 9000 einstellen

Jumbo-Frames können – wie oben erwähnt – auch eine Problemquelle sein. Deshalb sollten Sie das iSCSI-Netzwerk erstmals ohne diese einrichten und testen; für mehr Performance können Sie später immer noch umstellen. Testen Sie unbedingt ausführlich – die Praxis zeigt, dass die oft nur minimalen Performancevorteile die Risiken der Fehlkonfiguration häufig nicht wirklich aufwiegen.

Arbeiten am Storage-System

Der iSCSI-Dienst muss auf einem NetApp-System erst einmal gestartet werden, das geschieht mit dem Kommando `iscsi start`. Es handelt sich wie bei allen Protokollen auf NetApp um ein lizenzpflichtiges Feature, allerdings hat NetApp in den ersten Jahren die iSCSI-Lizenzen kostenlos an die Kunden vergeben, um möglichst schnell Marktanteile zu gewinnen. Seit November 2010 bekommt der Kunde von NetApp immer das erste Protokoll kostenlos mit seiner Maschine geliefert, jedes weitere ist kostenpflichtig. Dadurch sind viele Kunden freier geworden in der Wahl ihrer Storage-Anbindung.

Die Arbeiten für die Bereitstellung von iSCSI-LUNs sind auf NetApp-Seite sehr ähnlich wie die Konfiguration von Fibre-Channel. In beiden Fällen müssen Sie Volumes, LUNs und iGroups erstellen. Der wichtigste Unterschied liegt darin, dass es sich um eine iSCSI-iGroup handelt, die sogenannte IQNs enthält. Die FCP-iGroup enthielt dagegen die WWPNs.

IQN steht für iSCSI Qualified Name und bezeichnet einen iSCSI-Host (egal ob Initiator oder Target) eindeutig – unabhängig davon, wie viele LAN-Karten oder Host-Namen das Gerät hat. Ein Beispiel für einen solchen IQN-Namen ist: `iqn.1998-01.com.vmware:rx3023-esx-1ad9214f`. Er besteht aus dem umgedrehten Datum der Domain-Registrierung, dem umgedrehten Domain-Namen selbst und – durch einen Doppelpunkt getrennt – einem eindeutigen String, bei vSphere sind das der ESX-Host-Name und einige zufällig gewählte Zeichen.

Zum Erstellen und Anbinden der LUNs führen Sie nun mit Ausnahme der iGroup-Konfiguration den quasi gleichen Vorgang wie bei FCP durch, begonnen mit dem Anlegen eines Volumes:

```
na1> vol create esx_iscsi aggr0 200g
Creation of volume 'esx_iscsi' with size 200g on containing
aggregate 'aggr0' has completed.
```

Auf dem Volume sollten Sie auch wieder automatische Snapshots deaktivieren, für Backup-Zwecke legen Sie später skriptgesteuerte Snapshots an.

```
na1>  snap reserve esx_iscsi 0
na1>  vol options esx_iscsi nosnap on
```

Im nächsten Schritt erstellen Sie wieder eine LUN:

```
na1> lun create -s 150g -t vmware
              -o noreserve /vol/esx_iscsi/iscsi_ds01.lun
```

Nun legen Sie die iSCSI-iGroup an und nehmen die iSCSI-Initiator-IQNs in diese neue Gruppe auf. Allerdings verhält sich iSCSI an dieser Stelle deutlich anders als FCP – da wir in diesem Beispiel mit Software-iSCSI arbeiten, müssen Sie auf jedem ESX-Host

- den Software-iSCSI-HBA aktivieren, erst dann wird dessen IQN erstellt und angezeigt, anschließend
- den Software-HBA so konfigurieren, dass er sich bei der NetApp anmeldet.

Beide Schritte erfordern eine kurze Konfiguration am ESX-Host. Unter Konfiguration und dann Speicheradapter klicken Sie auf den iSCSI-Software-Initiator, anschließend schalten Sie den Adapter unter Eigenschaften und Konfigurieren durch das Setzen des Häkchens auf Aktiviert ein. Dies wird in Abbildung 10.26 gezeigt.

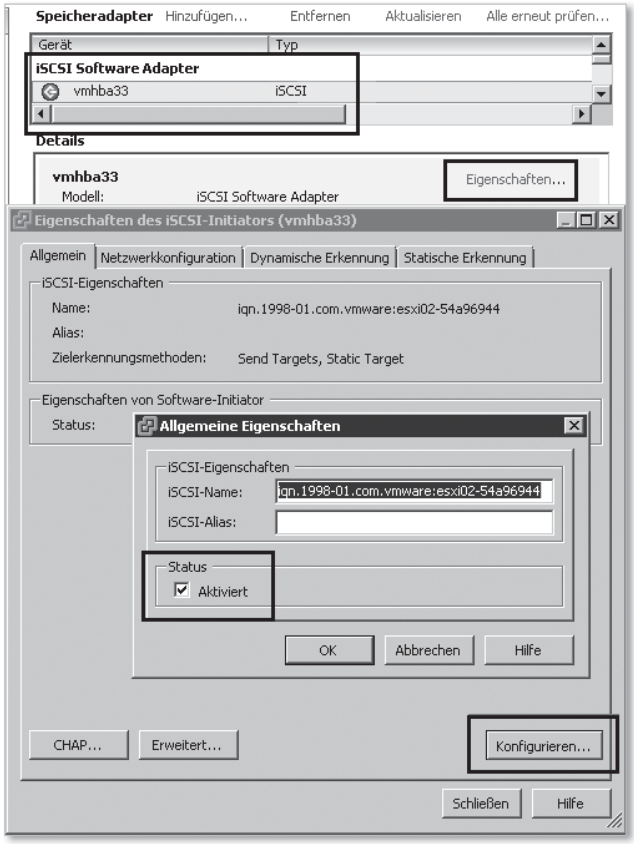


Abbildung 10.26 Den Software-iSCSI-HBA aktivieren

Nach dem Bestätigen ist der iSCSI-HBA aktiviert, und die IQN wird angezeigt. Diese IQN müssen Sie im nächsten Schritt in die iGroup übernehmen, am besten per Cut & Paste (Abbildung 10.27).

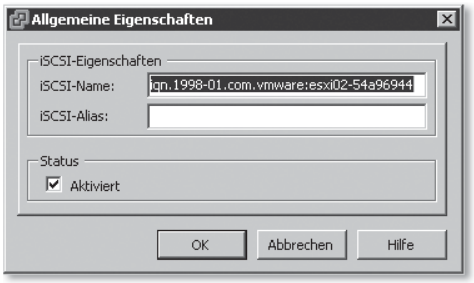


Abbildung 10.27 Aktivierter HBA

```
na1> igroup create -i -t vmware esx_iscsi_all
na1> igroup add esx_iscsi_all iqn.1998-01.com.vmware:esx02i-54a96944
```

(für alle ESX-Hosts wiederholen)

```
na1>  igroup show
         esx_iscsi_all (iSCSI):
         OS Type: vmware
         Member:  iqn.1998-01.com.vmware:esx02i-54a96944
         (logged in on: e0b,e0c)
```

Anders als bei FCP müssen Sie für iSCSI-Multipathing die iGroup nicht auf ALUA setzen, da das iSCSI-Protokoll das Multipathing anders implementiert, nämlich per MCS, also Multiple Connections per Session.

Falls iSCSI nur auf bestimmten LAN-Interfaces des NetApp-Speichersystems gesprochen werden soll, müssen Sie die unerwünschten Interfaces ausblenden. Das geschieht mit `iscsi interface disable <InterfaceName>`. Der Vorgang ist deshalb wichtig, weil im iSCSI-Login-Dialog zwischen Initiator und Target versucht wird, über *alle* aktiven Interfaces zu kommunizieren, leider auch über IP-Routing technisch nicht erreichbare Interfaces – das Phänomen tritt immer dann auf, wenn es eine Trennung zwischen Storage-Netz und anderen Netzen gibt. Es wird also empfohlen, auf dem NetApp-Speichersystem den iSCSI Dienst auf die wirklich verwendeten LAN-Ports zu beschränken. Dadurch wird vermieden, dass Sie ungewollten iSCSI-Datenverkehr im gleichen Netzwerk wie z. B. Ihre CIFS-Clients erzeugen. iSCSI kann mit dem `iscsi interface`-Befehl auf bestimmte Interfaces festgelegt werden. Falls Sie dabei vorhandene Verbindungen trennen, werden Sie gewarnt. Beispiel:

```
na01*> iscsi interface show
Interface e0a enabled
Interface e0b enabled
Interface e0c enabled
Interface e0d enabled
netapp02*> iscsi interface disable e0a
Disabling the specified network interface will result
in shutdown of one or more iSCSI sessions.
```

```
Do you wish to see a list of initiators affected? y
iqn.1998-01.com.vmware:esxi02-54a96944
iqn.1998-01.com.vmware:esxi01-7e7ce637
Shutdown sessions and continue? y
Disabling interface e0a
na01*> iscsi interface show
Interface e0a disabled
Interface e0b enabled
Interface e0c enabled
Interface e0d enabled
```

Der Rest des Vorgangs gestaltet sich auf NetApp-Seite wie auch bei FCP, Sie müssen die LUN an die iGroup mappen:

```
na1> lun map /vol/esx_iscsi/iscsi_ds01.lun esx_iscsi_all 1
Sun Dec 25 18:38:06 MET [na1: lun.map:info]: LUN /vol/esx_iscsi/iscsi_
ds01.lun was mapped to initiator group esx_iscsi_all=1
na1> lun show -m
LUN path                      Mapped to      LUN ID  Protocol
/vol/esx_iscsi/iscsi_ds1.lun  esx_iscsi_all   11      iSCSI
```

Die LUN sollte nun an den entsprechenden Hosts sichtbar sein, alle weiteren Arbeiten erledigen Sie am ESX-Host.

Arbeiten am ESX-Host

Damit die soeben erstellte LUN beim nächsten HBA-Rescan auf dem ESX-Host sichtbar wird, muss der Software-HBA am ESX-Host sich zunächst auf das iSCSI-Target verbinden. Sie müssen sich von jedem Host aus auf das Speichersystem verbinden; es handelt sich um eine Point-to-Point-Verbindung und nicht wie bei FCP um ein gemeinsam nutzbares (*shared*) Medium (die Zone), das durch das Zoning definiert wurde.

In den Eigenschaften des Software-HBAs definieren Sie das Target bei Dynamische Erkennung, siehe Abbildung 10.28.

Anschließend können Sie neu scannen; die LUN sollte auftauchen. Auf dem NetApp-System erscheint eine Meldung, dass sich ein iSCSI-Initiator neu verbunden hat:

```
[na1: iscsi.notice:notice]: ISCSI: New session from initiator
iqn.1998-01.com.vmware:esx02i-54a96944 at IP addr 10.10.10.152
```

In ESX-Versionen vor 4.0 musste neben dem VMkernel-Interface auch ein Service-Console-Interface im selben Subnetz definiert sein, da früher der Send Targets-Login-Dialog zwischen ESX und Storage noch in zwei Schritten definiert war. Beim ersten Schritt prüfte die Service Console die Verfügbarkeit der LUNs, im zweiten Schritt wurde dann die Datenverbindung vom VMkernel zum iSCSI-Storage hergestellt. Seit Version 4 ist das nicht mehr nötig, der VMkernel macht beides.

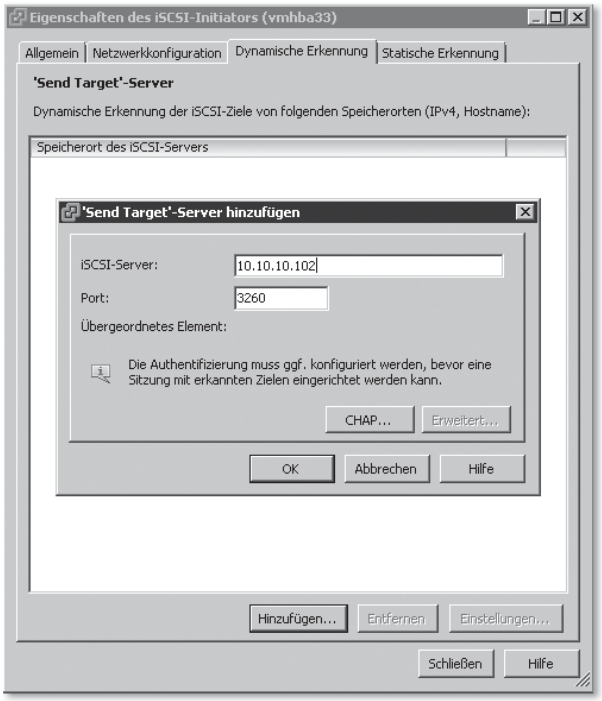


Abbildung 10.28 IP-Adresse des NetApp-Systems eintragen

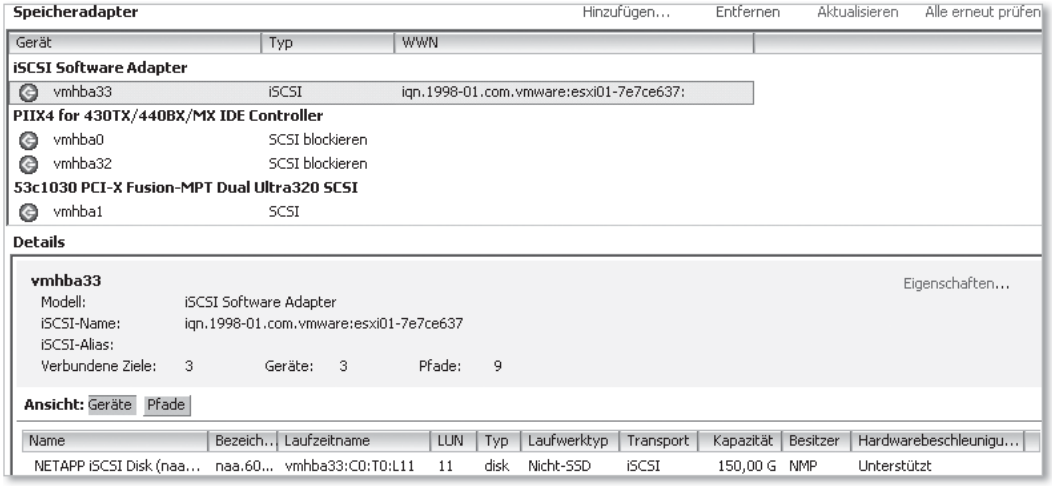


Abbildung 10.29 Nach dem Rescan wird die LUN angezeigt.

Nachdem die LUN sichtbar ist, können Sie nun ein VMFS-Dateisystem anlegen, der Vorgang ist der gleiche wie bei FCP: Unter SPEICHER klicken Sie SPEICHER HINZUFÜGEN an und wählen anschließend die noch leere iSCSI zum Erstellen des Datastores aus.

Abbildung 10.30 Die leere iSCSI-LUN auswählen

In den nächsten Schritten des Dialogs stellen Sie auch wieder die Blockgröße ein, klicken auf KAPAZITÄT MAXIMIEREN und bestätigen dann; die LUN wird benannt und somit zum nutzbaren Datastore (Abbildung 10.31).

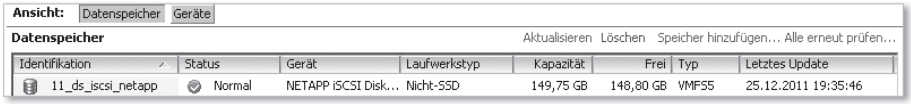


Abbildung 10.31 Der iSCSI-Datastore ist fertig.

Damit die gleiche Ausfallsicherheit wie bei FCP gewährleistet werden kann, müssen Sie nun noch dem Software-iSCSI-HBA das zweite VMkernel-Interface hinzufügen. Dieses haben Sie vorhin schon angelegt, allerdings konfigurieren Sie nun beide VMkernel-Interfaces zum Software-Initiator hinzu und zwar in den EIGENSCHAFTEN des VMHBA33 unter NETZWERKKONFIGURATION.

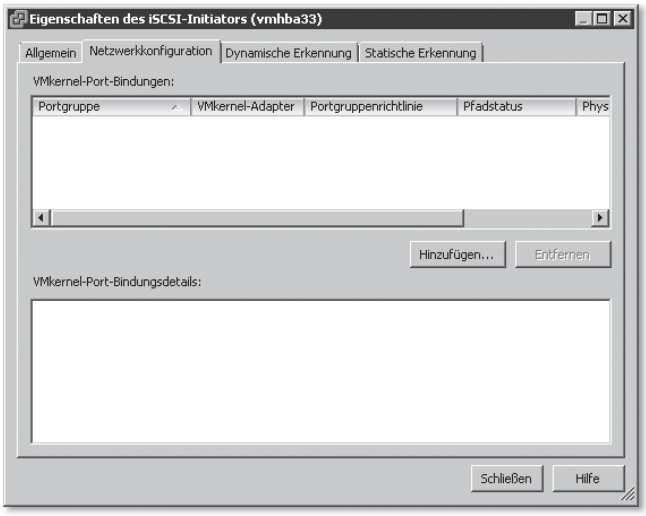


Abbildung 10.32 Die zwei VMKernel-Interfaces müssen gebunden werden.

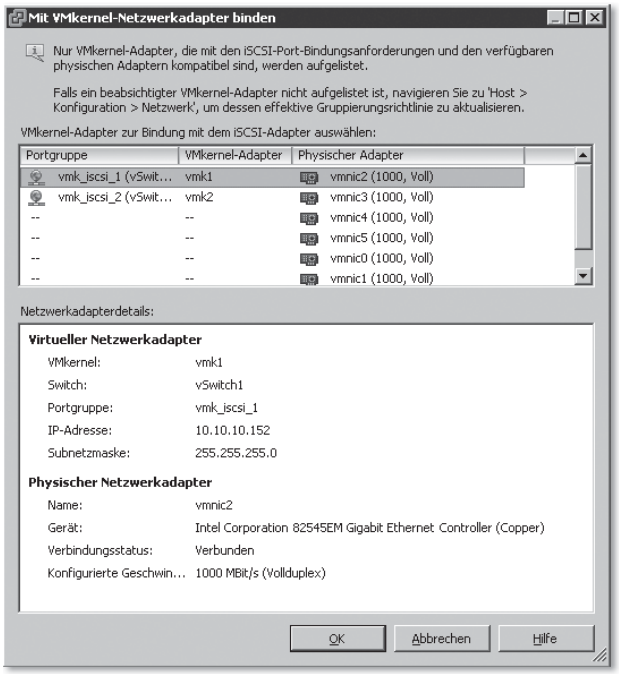


Abbildung 10.33 Jeder »vmk«-Adapter muss gebunden werden.

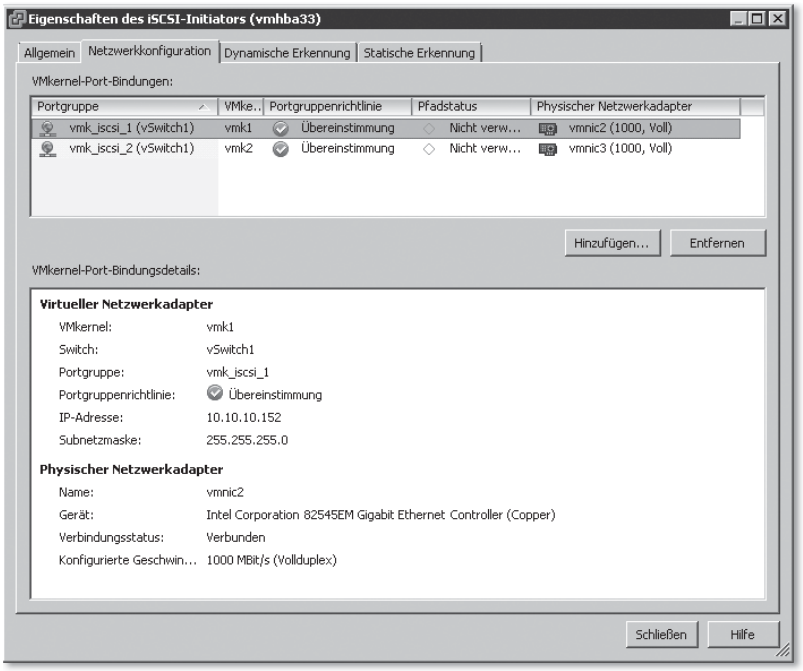


Abbildung 10.34 Ergebnis des Port-Bindings

Falls Sie lieber die Command-Line bevorzugen, können Sie diese Schritte auch schnell im ESXi-CLI durchführen:

```
[root@esx02 ~]# esxcli swiscsi nic add -n vmk_iscsi_1 -d vmhba33
[root@esx02 ~]# esxcli swiscsi nic add -n vmk_iscsi_2 -d vmhba33
```

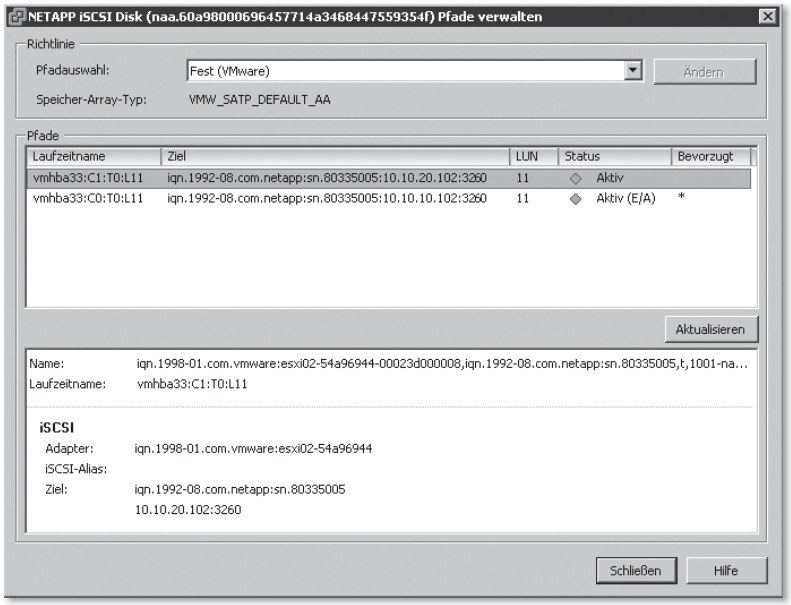


Abbildung 10.35 Zwei Pfade zur gleichen LUN, aber nur ein Pfad aktiv

Mit zwei Pfaden würde der Failover grundsätzlich schon einmal funktionieren, allerdings sollten Sie auch von Load-Balancing profitieren. Dafür stellen Sie die Pfadauswahl auf Round-Robin ein, ähnlich wie es bei FCP nötig war, nur ist im Falle von iSCSI kein spezielles SATP im Einsatz, sondern Sie verwenden das normale SATP_DEFAULT_AA.

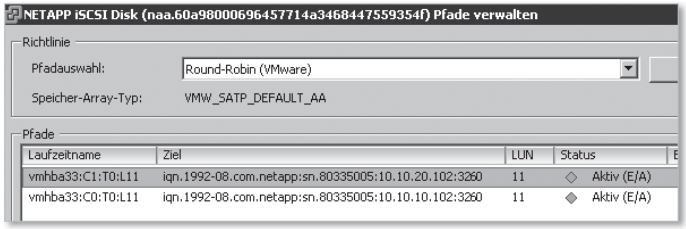


Abbildung 10.36 Active-Active mit Round-Robin-Load-Balancing mit iSCSI

Ein echtes iSCSI-Load-Balancing mit ESX 3 und 3.5 war nicht einfach möglich, es sei denn, man setzte einen Hardware-HBA ein. Dieser verfügt über zwei getrennte Ports und meldet sich auch als zwei HBAs gegenüber dem ESX-Host; die Konfiguration war dadurch fast identisch mit Fibre-Channel.

Jeweils mit ESX 4 und nochmals mit ESX 5 wurde die mögliche iSCSI-Performance drastisch verbessert. Durch den Einsatz von 10-Gigabit-Ethernet kann nun annähernd gleiche Geschwindigkeit wie mit Fibre-Channel erreicht werden – allerdings bei deutlich höherer CPU-Last und leicht schlechterer Latenz.

10.2.3 NFS-Datastores

Das Network File System (NFS) wurde in den 80er Jahren von Sun Microsystems veröffentlicht. Es war damals ein revolutionärer Ansatz, über das Netzwerk auf Dateien zuzugreifen, die auf einem anderen Rechner gespeichert waren.

Seit ESX-Version 3.0 erlaubt VMware auch die Verwendung des NAS-(Network-attached Storage-)Protokolls für die Ablage von virtuellen Maschinen. Das andere aus der Windows-Welt bekannte NAS-Protokoll namens CIFS wird für die Ablage von VMDK-Dateien hingegen aus Performancegründen nicht unterstützt. Microsoft hat diese Schwächen von CIFS in Bezug auf Geschwindigkeit erkannt und wird diese vorrausichtlich mit Version SMB 2.2 beseitigen – eventuell wird es dann in Zukunft auch Unterstützung dafür in vSphere geben. Bis dahin bleibt als einzige Variante des File-Zugriffs auf Datastores das Protokoll NFS.

Mit NFS greifen wir also das erste Mal dateiorientiert auf das Speichersystem zu – es ist kein VMFS-Cluster-File-System auf LUNs mehr nötig. Auf ein Share (deutsch: Netzlaufwerk) konnte schon immer parallel zugegriffen werden, es wurde schließlich genau dafür entwickelt.

Eingebaute Locking-Mechanismen im NFS-Protokoll verhindern den gleichzeitigen Zugriff auf dieselbe Datei von zwei verschiedenen Hosts aus.

Im Vergleich zu Fibre-Channel wird NFS oft nicht als ernstzunehmende Konkurrenz gesehen, wenn es um High-Performance-Storage geht. Doch dieses Vorurteil ist veraltet: NFS ist durchaus in der Lage, den beiden blockorientierten Speicherzugriffen Paroli zu bieten. Nicht umsonst hat der Datenbank-Hersteller Oracle für Oracle 11 einen sogenannten Direct-NFS-Client herausgebracht, der beweist, wie schnell Datenbanken auf NFS-Speicher laufen können.

Der Einsatz von 10-Gigabit-Ethernet bringt NFS-Durchsatz und Antwortzeiten auf ein vergleichbares Niveau mit Fibre-Channel und bietet bessere Leistungen als iSCSI. Ein relativ aktuelles Dokument, das die mögliche Geschwindigkeit in vSphere-Umgebungen vergleicht, finden Sie hier: *http://media.netapp.com/documents/tr-3916.pdf*. Dort wird auch auf aktuelle Technologien wie 8-GB-FC, 10-GB-Ethernet und FCoE eingegangen. Im vSphere-Umfeld hält NFS immer stärkeren Einzug; viele der neuen Implementierungen werden aufgrund von vereinfachter Verwaltung, weniger Infrastrukturkosten und sehr guter Skalierbarkeit mit NFS umgesetzt.

Arbeiten am Speichersystem

Die Konfiguration von NFS-Freigaben auf einem NetApp-Speichersystem ist relativ einfach und schnell zu erledigen – schließlich war NFS das erste Protokoll, das von NetApp unterstützt wurde. Ein weiterer Punkt, der zur einfachen Konfiguration beiträgt, ist die Tatsache, dass beim dateiorientierten Zugriff keinerlei LUNs nötig sind. Ein NetApp-Volume entspricht einem Dateisystem, das heißt, es kann direkt per NFS freigegeben werden. Allerdings müssen Sie durch diese Veränderung nun auf andere Dinge achten, zum Beispiel Zugriffsrechte auf das Share und die Dateien.

Bei einem NetApp-System ist NFS ein kostenpflichtiges Protokoll, das lizenziert werden muss. Erworbene Lizenzen spielen Sie mit dem Befehl `license add <licensecode>` ein. Gegebenenfalls müssen Sie den Dienst noch starten, und zwar mit `nfs on`. Zuerst erstellen Sie auf dem NetApp-System wieder ein Volume, diesmal zur direkten Ablage von VMs:

```
na1> vol create esx_nfs aggr0 200g
Creation of volume 'esx_nfs' with size 200g on containing
aggregate 'aggr0' has completed.
```

In einem NAS-Volume ist es sinnvoll, die Snapshot-Reserve nicht abzuschalten, da die NFS-Clients jeweils den echten Wert für freien Speicher in dem Volume angezeigt bekommen. Weil der Snapshot-Plattenplatzverbrauch bei einem Volume mit abgeschalteter Snapshot-Reserve als normalen Speicherverbrauch angezeigt wird, erhalten die Clients falsche oder verwirrende Informationen über den freien und belegten Speicher. In unserem Beispiel ist der Standardwert von 20 % für Snapshot-Reserve eingestellt. Sie könnten diesen Wert jederzeit verändern, solange noch genug Platz im Volume frei ist.

```
na1> df -h esx_nfs
Filesystem               total       used      avail capacity
/vol/esx_nfs/            160GB      104KB      159GB       0%
/vol/esx_nfs/.snapshot    40GB        0GB       40GB       0%
```

Ähnlich wie bei FCP oder iSCSI ergibt es keinen Sinn, vom NetApp-Speichersystem regelmäßig automatisch Snapshots erzeugen zu lassen – die VMs und deren enthaltene Applikationen wären nicht konsistent. Also schalten wir auch wieder den automatischen Scheduler für Snapshots auf NetApp-Seite aus, die Snapshots zur Datensicherung lösen wir später manuell oder per Skript aus.

```
na1> vol options esx_nfs nosnap on
```

Eine empfohlene Tuning-Option für NFS-Datastores ist das Ausschalten der Access-Time-Flags auf dem Volume. Dadurch werden bei reinen Leseanfragen auf die VMDK-Dateien keine unnötigen Metadaten-Schreibzugriffe ausgeführt, die die letzte Zugriffszeit auf das File (die *A-Time*) aktualisieren.

```
na1> vol options esx_nfs no_atime_update on
```

Sie sollten auf einem NetApp-Speichersystem auch dringend darauf achten, dass die Zugriffsrechte der Dateien in einem Volume nach Unix-Art verwaltet werden. Gerade wenn ein Kunde das System als Multiprotokoll-Gerät konfiguriert hat (also für NFS und CIFS gleichzeitig), kann es vorkommen, dass per Default CIFS-Rechte auf dem Volume verwaltet werden und keine Unix-Rechte. vSphere greift allerdings als Unix-Client über NFS auf das Volume zu, deshalb müssen die Rechte auch auf Unix eingestellt sein:

```
na1> qtree security /vol/esxnfs unix
```

Nachdem alle Einstellungen für das Volume durchgeführt wurden, so muss es noch für die Clients freigegeben werden. Der Vorgang ist auf jeder Art von NFS-Server sehr ähnlich: Meist gibt es eine Konfigurationsdatei namens */etc/exports* und einen dazu passenden Befehl `exportfs`.

Da der VMkernel von vSphere als User-ID 0 läuft, müssen Sie auch den Zugriff auf den Export als User »root« erlauben. Dafür dient die Option `root=<IP>`. Oder andersherum ausgedrückt: Falls Sie diese Option nicht setzen, so schaltet der NetApp NFS-Server den Zugriff von ESX als User »root« auf einen anonymen Zugriff um – und dieser anonyme User hat dann keine Rechte mehr, die Zugriffe werden fehlschlagen. Man spricht dabei auch von einem *Root-Squash*.

Außerdem braucht der ESX-Host logischerweise Lese- und Schreibrechte auf das Volume, was Sie durch die Option `rw=<IP>` konfigurieren. Entweder tragen Sie nun diese Einstellungen in die Datei */etc/exports* ein und lesen die Datei erneut mit dem Befehl `exportfs -a`, oder Sie erledigen beides mit einem einzigen Befehl:

```
na1> exportfs -p rw=192.168.123.1,root=192.168.123.1 /vol/esx_nfs
```

Weitere IP-Adressen von ESX-Hosts können Sie mit Doppelpunkt getrennt angeben.

Arbeiten am ESX-Host

Nun gilt es wieder, den soeben bereitgestellten Speicherplatz an dem ESX-Host anzubinden; diesmal wird ein NFS-Datastore verbunden. Da der VMkernel den NFS-Datastore über ein IP-Netzwerk verbindet, müssen Sie zuerst im Netzwerkbereich ein VMkernel-Interface für IP-Storage erstellen. Wie auch bei iSCSI empfiehlt sich eine Abtrennung dieses Netzes in ein eigenes VLAN oder noch besser auf eine eigene physische Infrastruktur, weil dadurch die Performance am wenigsten beeinträchtigt wird und Sie gegebenenfalls andere oder bessere Einstellungen wählen können, zum Beispiel Jumbo-Frames.

Load-Balancing und Failover sind mit NFS ebenso realisierbar wie mit den anderen beiden Storage-Protokollen, allerdings nur bedingt. Einen NFS-Datastore können Sie redundant anbinden, indem Sie den vSwitch mit mehreren Uplinks zum physischen Switch (pSwitch) binden. Möchten Sie allerdings eine redundante Active/Active-Anbindung, also einen Etherchannel oder Link Aggregation über mehrere Switches hinweg, so müssen Sie darauf achten, dass die Switches das Feature MLAG (Multichassis Link Aggregation) unterstützen oder aber dass die Switches gestackt werden, also für den ESX-Host wie ein einzelner Switch aussehen.

vSphere unterstützt nur statische EtherChannels, kein dynamisches LACP (Link Aggregation Control Protocol), also konfigurieren Sie bitte kein LACP auf Ihren Switches.

Um mehr Datendurchsatz zu erlangen, sollten Sie als Load-Balancing-Option auf der Portgruppe IP-Hash wählen. Das allein hat jedoch nicht den gewünschten Effekt, da der Hash-Algorithmus als Resultat immer denselben Link verwendet – schließlich wird die Verbindung ja nur von einer einzigen VMkernel-IP zu einer einzigen NFS-Server-IP hergestellt. Diesen Effekt können Sie vermeiden, indem Sie der Netzwerk-Karte auf NetApp-Seite einfach mehrere IP-Adressen (IP-Aliase) geben und verschiedene Datastores über die verschiedenen IPs verbinden. Das ist zwar kein echtes Round-Robin-Load-Balancing, jedoch wird die Last der verschiedenen Datastores über die verschiedenen Links verteilt.

Wir entscheiden uns für unser Konfigurationsbeispiel für die empfohlene Variante, in der der vSwitch ein IP-Hashing-Load-Balancing durchführt. Bitte bedenken Sie: Das funktioniert nur, wenn Sie entweder alle Uplinks auf den gleichen physischen Switch verbinden und dort eine Port-Channel-Link-Aggregation konfigurieren, oder wenn Sie die Uplinks auf mehrere Switches verteilen, die Multichassis Link Aggregation unterstützen. LAN-Switches ohne diese Features sollten Sie nur im Active/Passive-Modus verwenden.

Den vSwitch von iSCSI sollten Sie aus mehreren Gründen nicht gleichzeitig für NFS-Traffic nutzen. Einerseits sollte die verfügbare Bandbreite auch wirklich für jedes Protokoll zur Verfügung stehen, andererseits könnte die Uplink-Einstellung der VMkernel-Ports von iSCSI nicht zu den Empfehlungen für NFS passen.

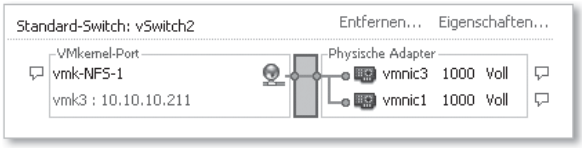


Abbildung 10.37 Dedizierte Uplinks für NFS und ein VMkernel-Port

Für Load-Balancing reicht in einem Etherchannel-Setup ein einziger VMkernel-Port, dessen beide Uplinks des vSwitches müssen aber aktiv sein, das Load-Balancing sollte nach IP-Hash passieren, siehe Abbildung 10.38.

Damit auch ein Load-Balancing über die verschiedenen Uplinks erzielt wird, ist es nötig, auf dem NetApp-Speichersystem mehrere IP-Aliasse zu konfigurieren und die Datastores später auch unter den verschieden IP-Adressen zu mounten. Bitte achten Sie darauf, dass jeder Datastore auf jedem Host immer konsistent gemountet wird, zum Beispiel: Datastore 1 von IP-Adresse .1, analog dazu Datastore 2 von IP Adresse .2 – und zwar auf jedem Host gleich. vSphere bildet nämlich eine UUID (Universally Unique Identifier – eine universell eindeutige Kennung) aus den verschiedenen Namen und IP-Adressen, um die Datastores eindeutig identifizieren zu können. Wären die IPs und Datastores inkonsistent zugeordnet, so würde vSphere oder der vCenter Server glauben, dass es sich dabei um verschiedene Datastores handelt.

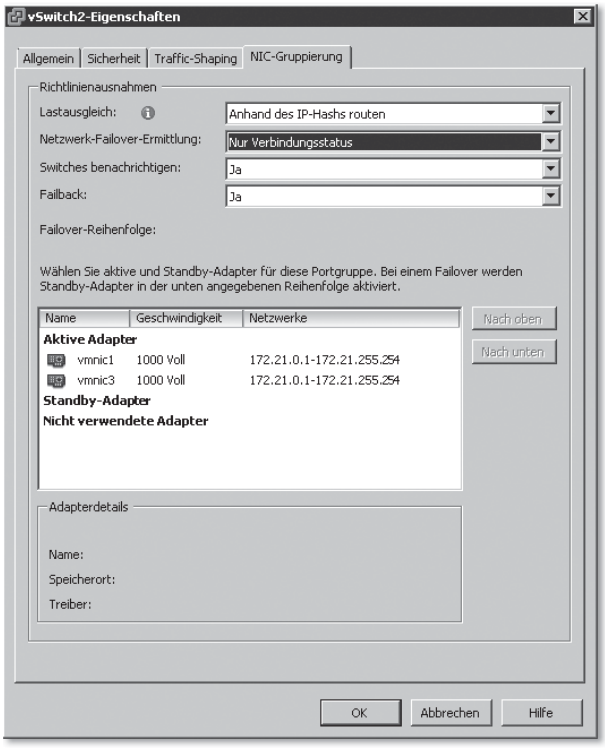


Abbildung 10.38 IP-Hash-Routing und beide Uplinks aktiv

Sind Ihre vSwitches und VMkernel-Ports erst einmal eingerichtet, dann ist die Anbindung des NFS-Datastores relativ schnell erledigt: Wählen Sie unter KONFIGURATION und SPEICHER nun SPEICHER HINZUFÜGEN, und klicken Sie diesmal NETZWERKDATEISYSTEM (NFS) an (Abbildung 10.39).

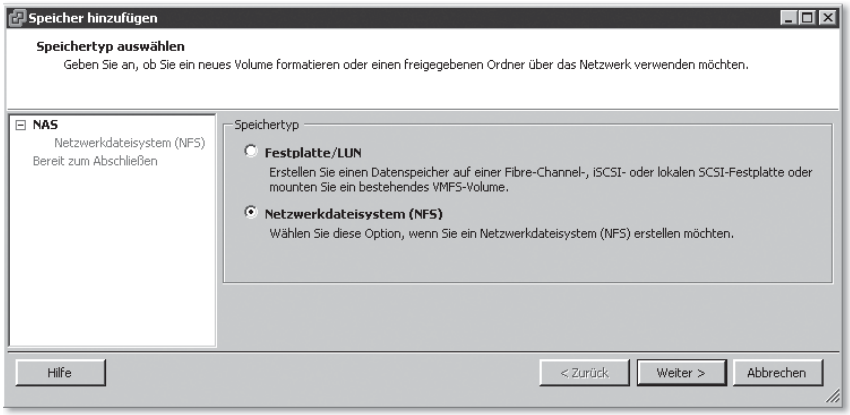


Abbildung 10.39 NFS auswählen

Im nächsten Dialog geben Sie an, zu welchem NFS-Server bzw. welcher IP-Adresse sich der ESX-Host (genauer: dessen VMkernel) verbinden soll und welches NFS-Share verbunden wird. Wir wählen für den ersten Datastore auch die erste IP-Adresse des NetApp-Systems (10.10.10.101).

Zusätzlich müssen Sie wie bei den anderen Datastores einen Namen vergeben. Stehen die ESX-Hosts unter der Verwaltung eines vCenter-Servers, so müssen Sie den NFS-Export trotzdem auf allen Hosts manuell verbinden, der Name des Datastores wird dann aber automatisch auf allen Hosts auf den gleichen Namen gesetzt, und zwar auf den zuerst vergebenen. Sie können jedoch später noch den Namen des Datastores ändern, indem Sie einfach einen Rechtsklick ausführen und UMBENENNEN wählen.

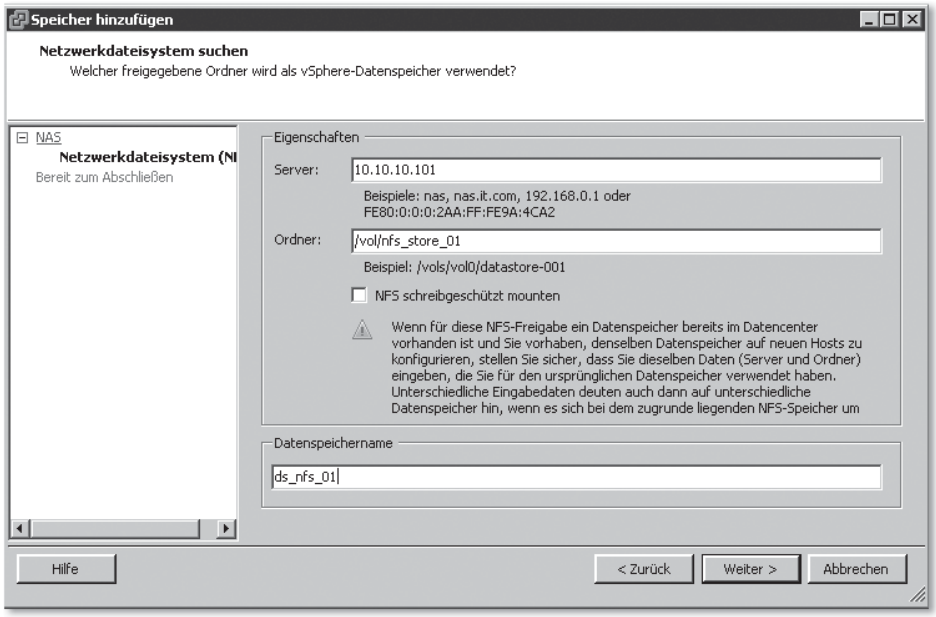


Abbildung 10.40 NFS-Server, Volume und Datastore-Name angeben

Da wir in unserem Beispiel die Variante mit Load-Balancing konfigurieren möchten, müssen wir dafür noch einen zweiten Datastore verbinden, und zwar vom anderen IP-Alias unseres NetApp-Systems (Adresse 10.10.10.111).

Ist der Datastore dann verbunden, so erscheint er in der Liste der Datastores (Abbildung 10.42).

Um NFS-Datastores zu vergrößern oder verkleinern, reicht es, auf NetApp-Seite das entsprechende flexible Volume anzupassen. Das kann im laufenden Betrieb geschehen.

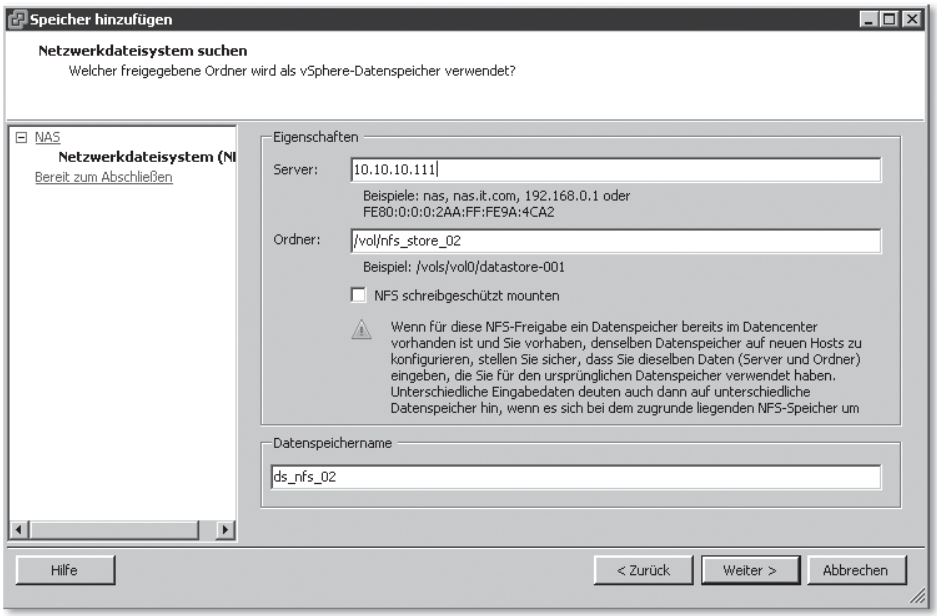


Abbildung 10.41 Zweiter Datastore von anderer NetApp-IP

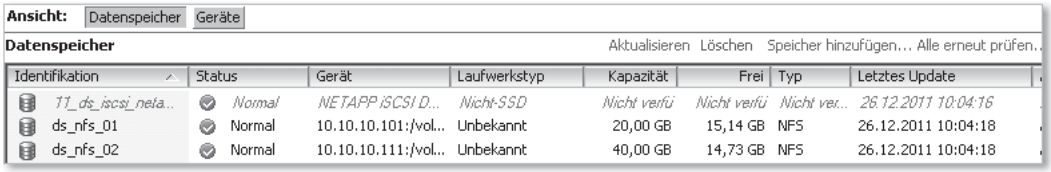


Abbildung 10.42 Ergebnis: Der NFS-Datastore ist sichtbar.

Anzahl der VMs pro NFS-Datastore

Es ist nicht leicht, genaue Aussagen über Maximalanzahl von VMs auf einem NFS-Datastore zu treffen, da dieser aufgrund der File-Locks wesentliche Vorteile in der Skalierung gegenüber den blockbasierten VMFS-Volumes hat, die mit SCSI-Locks arbeiten.

Grundlegend hängt die sinnvolle Anzahl der VMs auf einem NFS-Datastore natürlich von der darunterliegenden Speicherarchitektur ab und davon, welche Leistung diese liefern kann. So können Sie beispielsweise mit einem genügend ausgestatteten NetApp-Storage der Einstiegsklasse FAS2200 einige Dutzend VMs bis ca. 100 VMs mit entsprechenden I/O-Charakteristiken versorgen. Müssten Sie mehrere Hundert oder gar Tausend VMs versorgen, sollten Sie den Filer auch entsprechend auf Controller- und Festplattenseite ausbauen. Flash-Cache-Karten werden zur Beschleunigung explizit empfohlen; siehe dazu auf Seite 537 den Abschnitt »Flash-Cache-Karten«.

Im Standard nutzen Kunden die NFS-Datastores mit einer Belegung zwischen 100 und 200 VMs. Bis inklusive ONTAP 8.0 existiert bei NetApp allerdings aufgrund der Deduplizierung ein Soft-Limit, dass maximal 255 VMs auf einem NFS-Export (Datastore) betrieben werden sollen, da bei größerer Anzahl ein weniger optimaler Deduplizierungs-Effekt erzielt werden kann. Dieses Limit wurde in ONTAP 8.1 auf ca. 32000 angehoben.

Getestet wurden allerdings auch schon NFS-Datastores mit über 800 VMs, was auch problemlos funktionierte. Hier stellt sich aber dann die Frage der Sinnhaftigkeit wegen Redundanz und maximaler Cluster-Konfiguration auf VMware-Seite.

10.3 Umgang mit Datastores

Sind die Datastores einmal angelegt, so will man mit ihnen auch arbeiten. VMware hat in den letzten Jahren viel Zeit damit verbracht, die Bedienbarkeit über die grafische Oberfläche des vSphere-Clients und die WebAccess-Schnittstelle zu realisieren.

10.3.1 Rescan SAN

Ebenfalls mit vSphere wurde eine starke Vereinfachung beim SAN-Rescan eingeführt, die es ermöglicht, auf Datacenter- oder Cluster-Ebene im Kontextmenü Rescan SAN auszuwählen und gleich mehrere Hosts auf einmal zu scannen. Außerdem wird nun automatisch bei der Anlage eines neuen FC-/iSCSI-Datastores ein Rescan auf allen Hosts im Cluster ausgeführt.

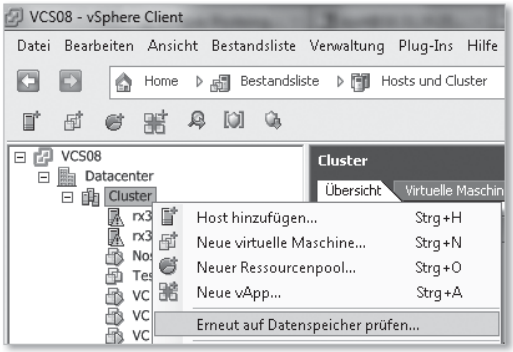


Abbildung 10.43 »Rescan Datastores« auf Cluster-Ebene

10.3.2 Speicheransichten

Neben dem Zugriff über den ESX-Host existiert im vCenter eine Datastore-Ansicht, in der Sie die Datastores zentral bedienen können.

Abbildung 10.44 Datastore-View

In dieser Ansicht sehen Sie auf einen Blick den Status der verschiedenen Datastores ein und erkennen, wie viele virtuelle Maschinen auf dem Datastore registriert sind, welche Hosts mit ihm verbunden sind oder welche Berechtigungen gesetzt sind.

Eine der interessantesten Ansichten ist allerdings unter dem LEISTUNG Tab zu finden.

Abbildung 10.45 Datastores im »Leistung«-View

Die wahrscheinlich nützlichste Funktion sind aber die SPEICHERANSICHTEN, die ideal sind für die schnelle Statuskontrolle sowie das Auslesen der WWPNs oder der Anzahl der Pfade.

Die SPEICHERANSICHTEN sind nicht nur unter dem Datastore-View, sondern auch in der Ansicht der ESX-Host-Systeme zu finden. Dabei ist der Zeitpunkt der letzten Aktualisierung, zu beachten. Im Zweifelsfall sollten Sie immer erst eine Aktualisierung durchführen, bevor Sie auf die Angaben vertrauen.

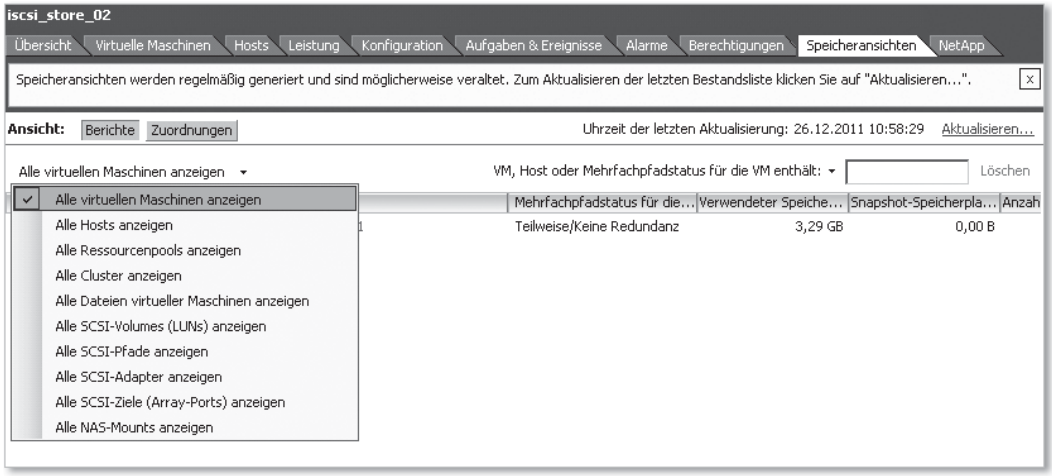


Abbildung 10.46 Datastores in den Speicheransichten

10.3.3 Datastore-Browser

Möchten Sie mit bestehenden Daten im Datastore arbeiten oder neue Daten importieren, so bietet sich der Datastore-Browser an. Diesen starten Sie aus dem vSphere-Client heraus oder in funktionsbeschränkter Form auch über die Browserschnittstelle von ESX oder vCenter (WebAccess).

Abbildung 10.47 WebAccess-Zugriff auf die Datastores

Der Datastore-Browser wird automatisch geöffnet, sobald Sie im Kontextmenü des Datastores »Datenspeicher durchsuchen« aufrufen.

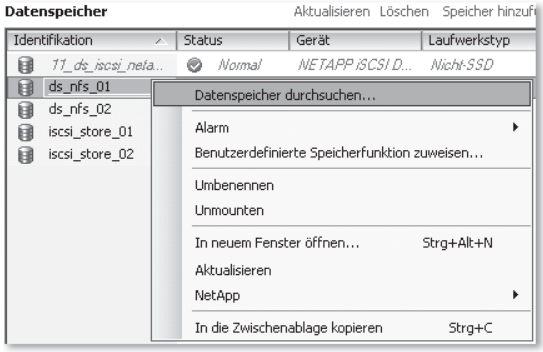


Abbildung 10.48 Datastore-Browser starten

Innerhalb des Datastore-Browsers können Sie nahezu beliebig agieren, da vom Umbenennen von Ordnern oder Dateien über Verschieben zwischen Datastores bis hin zur Registrierung neuer VMs alles möglich ist.

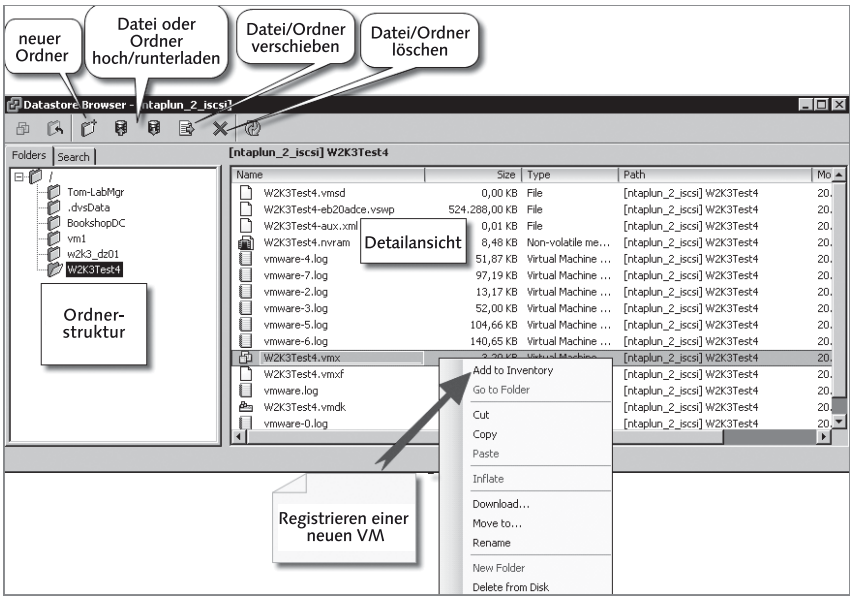


Abbildung 10.49 Datastore-Browser-Nutzung

10.3.4 Storage-Alarme

Viele Leser werden aufgeatmet haben, als die Storage-Alerts mit vSphere 4 Einzug hielten, um z. B. vor volllaufenden Datastores zu warnen oder natürlich den Füllstand bei Nutzung von Thin Provisioning im Auge zu behalten. Ebenso wichtig ist die Alarmierung bei Deduplizierung, falls es mit NFS verwendet wird, da die Effekte des Überbuchens sehr ähnlich wie bei Thin Provisioning sind.

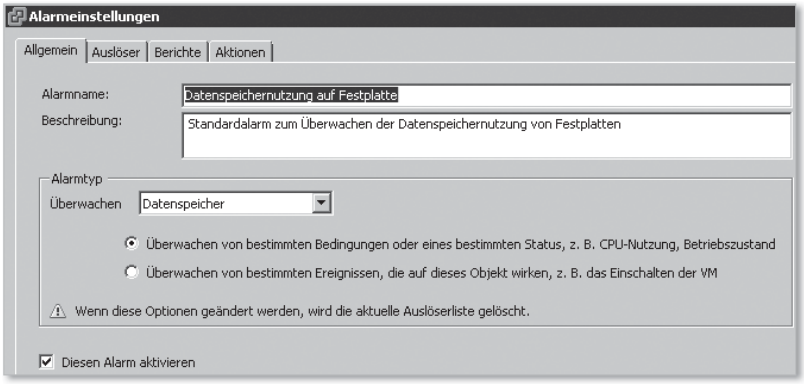


Abbildung 10.50 Storage-Alarme = Alarme, die Datastores überwachen

Innerhalb der Storage-Alarme unterscheiden wir zwischen zwei Zuständen des Alarmtyps: Bedingungen und Ereignisse.

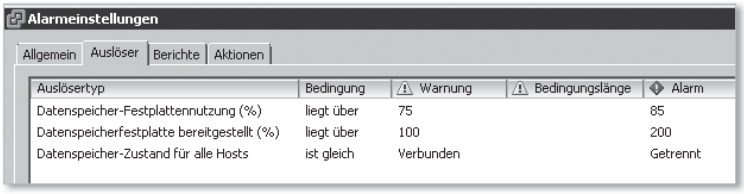


Abbildung 10.51 Statuskontrolle über Alarme

Mittels Bedingungskontrolle überwachen Sie die Nutzung der Datastores, den Status zu jedem verbundenen ESX-Host und die Überbuchung der Datastores (Thin Provisioning).

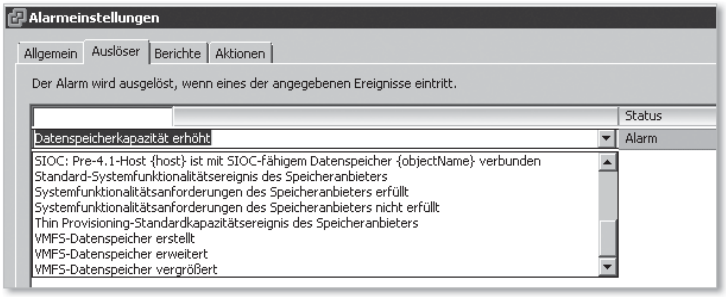


Abbildung 10.52 Ereigniskontrolle über Alarme

Die Ereigniskontrolle dient auf der anderen Seite dazu, Änderungen an den Datastores zu überwachen. Dies reicht von dem Hinzufügen oder Löschen des gesamten Datastores oder einzelner Dateien bis hin zur Überwachung, ob ein Datastore per »extend« oder »expand« vergrößert wurde. Hilfreich ist diese Art der Alarmierung, wenn mehrere Administratoren an einer vSphere-Farm arbeiten und besondere Veränderungen protokollieren möchten.

10.3.5 Datastore-Erweiterung

Eine weitere sehr wichtige Änderung von vSphere 4 bestand in der Möglichkeit, VMFS-Volumes zu erweitern. Bis dahin war dies nur mit Extents möglich gewesen, das heißt, mehrere VMFS-Partitionen auf mehreren LUNs wurden »zusammengeklebt«, sie waren also in ihrer Eigenschaft immer noch eigenständig (Größe, Plattennutzung etc.), wurden allerdings als ein einzelner Datastore angezeigt.

VMFS Volume Grow nennt sich die in vSphere 4 neu eingeführte Funktion, die einzelne VMFS-Partitionen auf dem Volume im laufenden Betrieb vergrößert. So ist es möglich, auf neue Gegebenheiten, z. B. das Datenwachstum von VMs, zu reagieren, ohne direkt die größtmöglichen LUNs nutzen zu müssen, um für den Fall der Fälle gerüstet zu sein.

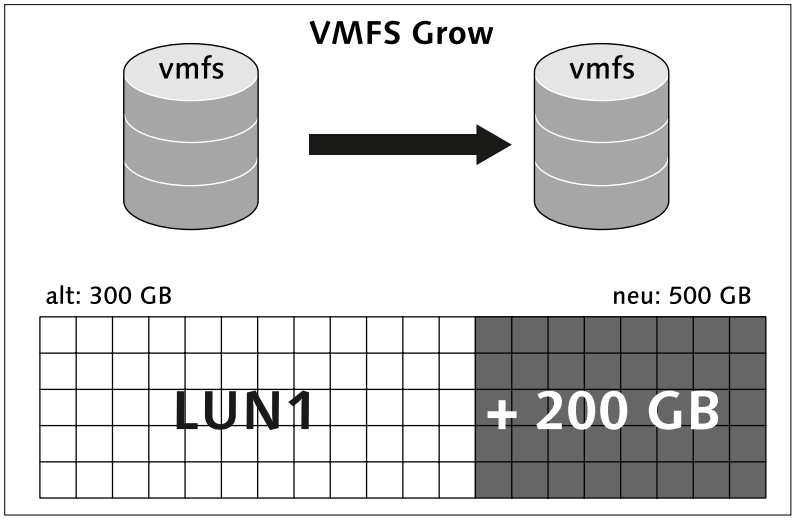


Abbildung 10.53 Vergrößerung der LUN von 300 GB auf 500 GB im Backend (LUN) und Frontend (VMFS)

Der erste Schritt besteht dabei im Vergrößern der LUN, die bereits mit VMFS formatiert und genutzt wird. Das geht so:

```
na1> lun resize /vol/iscsi_store_11/store_11.lun 500g
lun resize: resized to:  500.0g (536887689216)
```

Beim nächsten Rescan wird die Vergrößerung der LUN erkannt.

Ist der zusätzliche Speicherplatz erkannt, sehen Sie die Vergrößerung in der Ansicht Erweiterungen, da eine Größendifferenz zwischen Device und Partition vorliegt. Per Erhöhen rufen Sie den Dialog zur Auswahlerweiterung des Datastores auf.

Wählen Sie nun die gleiche LUN aus, so wird ein VMFS Volume Grow ausgeführt; wählen Sie eine andere LUN, so wird der Datastore mit einem Extent erweitert.

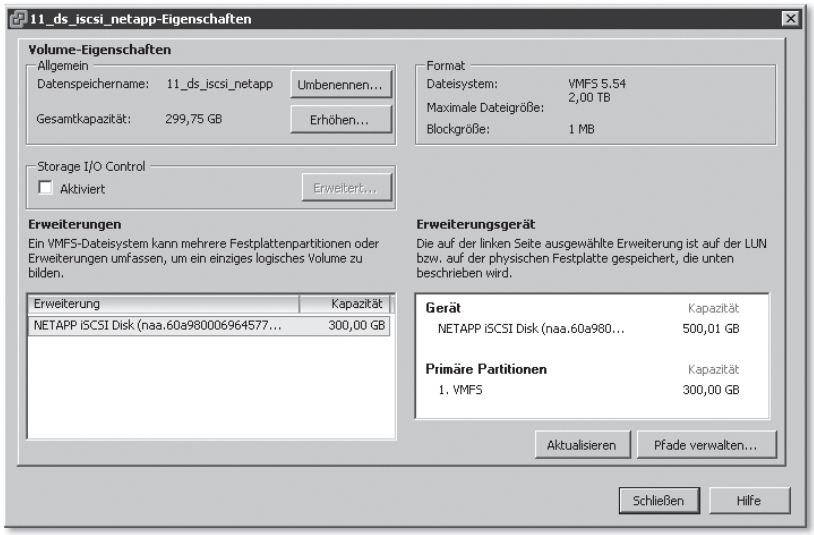


Abbildung 10.54 Einen Datastore vergrößern Sie in seinem »Eigenschaften«-Fenster.

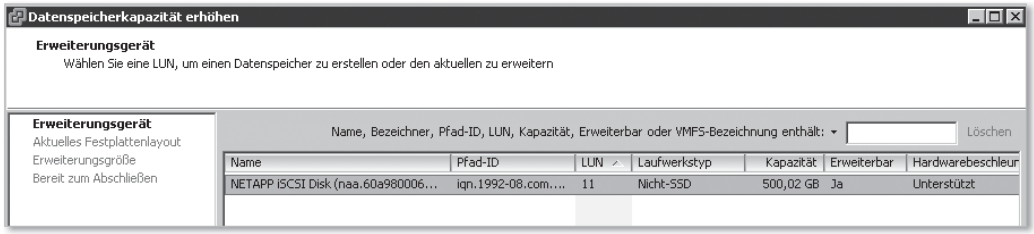


Abbildung 10.55 Erkennung der Kapazitätserweiterung

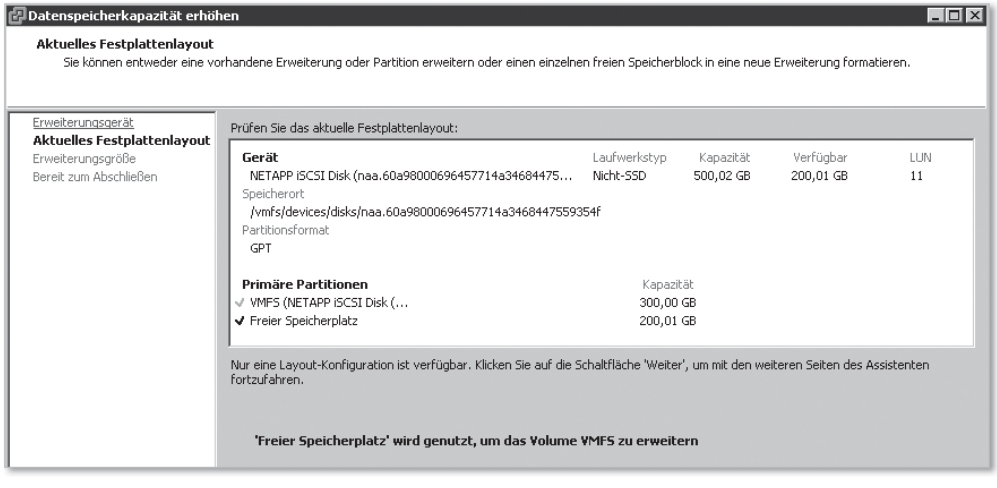


Abbildung 10.56 Um welche Kapazität soll der Datastore wachsen?

Der VMFS Grow wird empfohlen, die alte Variante mit Extent sollten Sie wenn möglich vermeiden. Eine Verkleinerung eines VMFS-Datastores ist weder online noch offline möglich, selbst wenn das darunterliegende Speichersystem eine LUN im laufenden Betrieb verkleinern könnte. Die einzige Möglichkeit, Datastores zu verkleinern, existiert mit NFS. vSphere beherrscht den Vorgang sogar im laufenden Betrieb, vorausgesetzt, das Speichersystem kann Volumes verkleinern.

10.4 NetApp-Spezialitäten

NetApp-Speichersysteme bieten viele fortgeschrittene Funktionen, die das Zusammenspiel mit Virtualisierungslösungen verbessern. Die meisten dieser Features gab es schon, bevor man an Server-Konsolidierung dachte. Da aber NetApp-Storages ja selbst schon eine Virtualisierungslösung darstellen – Storage-Virtualisierung –, passen ihre Features hervorragend zu den Funktionen von VMware. Im Folgenden gehen wir auf Cloning, Snapshots, Backup und Tuning von NetApp-Storage für VMware ein.

10.4.1 Cloning-Technologien

Virtuelle Maschinen liegen in Form von Dateien vor. Durch Kopieren dieser Dateien erstellen Sie auf einfache Weise Duplikate von VMs – virtuelle Maschinen müssen nicht immer frisch installiert werden. VMware bringt dafür im vCenter-Server das Feature *Templates*, also »Vorlagen«, mit. Dabei handelt es sich um VMs, die nicht einschaltbar sind, deren Konfigurations-Datei auf *.vmtx* endet und die Sie bei Bedarf kopieren und anpassen, um so eine neue VM zu erstellen.

Grundsätzlich gibt es verschiedenste Gründe, VMDK-Dateien zu kopieren:

- Ausrollen (Deployment) von VMs für neue Dienste
- Kopieren von aktiven VMs zu Testzwecken (z. B. Softwareupdate)
- Bedarf an neuen VMs für virtuelle Desktops
- Backup oder Recovery

Ein normaler Kopiervorgang sieht bei ESX immer so aus, dass die entsprechenden Blöcke vom ESX-Host gelesen und anschließend wieder neu in den Datastore geschrieben werden. Aufgrund der Datenbewegung stellt das eine Belastung für den ESX-Host, das Netzwerk und das Speichersystem dar. NetApp-Speichersysteme erlauben es, virtuelle Kopien von Daten anzulegen, indem nur Zeiger kopiert werden – ähnlich wie bei NetApp-Snapshots. Diese Kopien belegen extrem wenig Platz (nur Metadaten für die Zeiger) und sind sofort verfügbar.

In naher Zukunft werden die Hersteller VMware und NetApp die Integration der vStorage-API so weit fertigstellen, dass die Erstellung von VM-Kopien auf das effiziente Storage-System aus-

gelagert werden kann, was die Geschwindigkeit beim Kopieren steigern und den Platzverbrauch verringern wird.

Die vStorage API for Array Integration (VAAI) unterstützt die Verlagerung der Kopierarbeit auf das Storage, auch NetApp integriert diese Funktion seit Data ONTAP-Version 8.0.1. Ein VAAI-Copy-Offload ist auf dem NetApp-Speichersystem aber immer noch ein Kopiervorgang, kein echter Clone.

Wenn Sie von vSphere aus echte Clones auf NetApps durchführen wollen, so müssen Sie aktuell zur Virtual Storage Console (VSC) 2.1.2 greifen, dem vSphere-Plugin von NetApp. Von dort aus ist es möglich, größere Mengen von virtuellen Maschinen über eine grafische Oberfläche zur Verfügung zu stellen.

Die grundlegenden Cloning-Vorgänge und Befehle erklären wir hier zusätzlich auf der NetApp-Kommandozeile erklärt.

LUN-Clones

Kunden, die ein Blockprotokoll (egal ob iSCSI oder FCP) lizenziert haben, erhalten die kostenlose Funktionalität, mit der sie Clones von LUNs erstellen können. Anwendungsbeispiele für die Verwendung von LUN-Clones sind:

- Testzwecke: Clonen Sie einen gesamten Datastore, um die VMs noch einmal auf einem anderen, isolierten Host hochzufahren und ein Softwareupgrade durchzuführen, falls der produktive Datastore vielleicht kaputtgeht.
- Recovery-Zwecke: Falls Sie Backups mit Hilfe von NetApp-Snapshots machen, können Sie per LUN-Clone einen alten Snapshot-Zustand des Datastores an den ESX-Host mappen – von dort aus kopieren Sie die rückzusichernde VM dann wieder auf Ihren produktiven Datastore. Ihre Restore-Zeiten senken sich dadurch auf wenige Minuten, selbst für ganze VMs, unabhängig von deren Größe.

LUN-Clones basieren auf NetApp-Snapshots. Um also einen Clone einer LUN zu erstellen, muss mindestens ein Snapshot des Volumes mit der enthaltenen LUN vorhanden sein. Am besten stellen Sie sich vor, dass jede Stunde ein Snapshot des Volumes zu Backup-Zwecken erstellt wird. (Mehr zu Backups per Snapshot in Abschnitt 14.1.4, »Backup von vSphere-Umgebungen mit NetApp-Storage«, unter der Überschrift »SMVI«.)

Ein Snapshot ist ein eingefrorener Zustand des Volumes, der nicht mehr veränderbar ist, also read-only. Auf diesem Zustand können Sie nun eine Clone-LUN anlegen, indem Sie einfach eine neue LUN erstellen und so tun, als ob diese schon Daten enthielte – es werden einfach Zeiger auf die Originaldaten aus dem Snapshot erstellt.

Somit werden Lesezugriffe auf die Clone-LUN durch die Kopie der Zeiger in Wirklichkeit von den Originalblöcken bedient, die Schreibzugriffe werden im LUN-Clone direkt abgelegt. Das heißt: Ein LUN-Clone braucht initial fast keinen Platz, später, wenn mehr Daten in den Clone

geschrieben wurden, steigt der Platzverbrauch an. Die Verwendung von LUN-Clones auf der NetApp-Kommandozeile funktioniert wie folgt:

Zuerst muss ein Snapshot des Volumes existieren, in dem die LUN liegt; an dieser Stelle gehen wir davon aus, dass die VMs in unserem Snapshot in einem konsistenten Zustand vorliegen. Einen solchen Zustand erzielen Sie z. B. durch einen vorherigen VMware-Snapshot der VM.

```
na1> snap create esxfcp snap4backup
na1> snap list esxfcp
  %/used       %/total  date          name
----------  ----------  ------------  --------
   9% (9%)    0% ( 0%)  Nov 14 14:01  snap4backup
```

Nun erzeugen Sie den LUN-Clone:

```
na1> lun clone create
usage:
lun clone create <clone_lunpath> [-o noreserve]
              -b <parent_lunpath> <parent_snap>

na1> lun clone create /vol/esxfcp/datastore1-CLONE.lun
   -o noreserve -b /vol/esxfcp/datastore1.lun snap4backup
```

Daraufhin gibt es zwei LUNs im Volume, das Original und einen Clone – da der Clone auf dem Snapshot basiert und diesen als »Lebensgrundlage« benötigt, ändert sich der Zustand des Snapshots in BUSY und ist nicht mehr löschbar, solange der Clone existiert:

```
na1> lun show
   /vol/esxfcp/datastore1-CLONE.lun    5g   (r/w, online)
   /vol/esxfcp/datastore1.lun          5g   (r/w, online)
na1> lun show -v /vol/esxfcp/datastore1-CLONE.lun
   /vol/esxfcp/datastore1-CLONE.lun    5g   (r/w, online)
     Serial#: C4iACZT5GWDq
     Backed by:/vol/esxfcp/.snapshot/snap4backup/datastore1.lun
     Share: none
     Space Reservation: disabled
     Multiprotocol Type: vmware
na1> snap list esxfcp
  %/used       %/total  date          name
----------  ----------  ------------  --------
 12% (12%)    0% ( 0%)  Nov 14 14:01  snap4backup   (busy,LUNs)
```

Um den Clone dann auf ESX-Seite verwenden zu können, müssen Sie ihn noch an eine iGroup mappen, genau wie jede andere normale LUN auch. Taucht der geclonte Datastore nach dem HBA-Rescan am ESX-Host auf, so können Sie wählen, was im Anwendungsfall »Recovery einer defekten VM« geschehen soll: Entweder kopieren Sie die gewünschte VM aus dem Clone-Datastore in den Original-Datastore und schalten die so recoverte VM wieder ein, oder Sie

registrieren die VM direkt auf dem Clone-Datastore, starten sie dort und kopieren sie dann im laufenden Betrieb per Storage vMotion auf den produktiven Datastore.

In jedem Fall sollten Sie einen LUN-Clone nach erledigter Arbeit wieder zerstören, da er einen Snapshot blockiert und sonst das Datenwachstum im Volume im Laufe der Zeit zu viel Platz belegen würde.

VMFS-Resignatur

Eine geclonte LUN führt zu einem geclonten VMFS-Datastore. Der ESX-Host sieht die ID (oder Signatur) des Datastores doppelt, deshalb müssen Sie dem Host mitteilen, was er mit dieser ID tun soll. Die VMFS-Signatur (u. a. UUID) wird beim Anlegen der VMFS-Partition anhand der Storage-Daten vergeben und auf die LUN geschrieben. Diese Signatur ist einmalig und stimmt nur überein, wenn sich nichts an der LUN oder dem Storage-System ändert. Der ESX-Server berechnet die UUID beim Erkennen eines Datastores seinerseits und vergleicht sie mit der Signatur auf dem Datastore. Stimmen die berechneten Daten nicht mit den Metadaten überein, wird ein Datastore-Snapshot erkannt.

Unter ESX 3.x führte schon die Anpassung der LUN-ID noch zur Änderung der berechneten VMFS-Signatur, was seit 3.5 U3 nicht mehr der Fall ist. Aktuell hängt die Signatur hauptsächlich von der LUN-Seriennummer ab. Kopien von LUNs mit bestehendem VMFS werden von den ESX-Hosts aufgrund der veränderten Metadaten daher auch als aus Sicherheitsgründen als Snapshot erkannt und können nicht direkt genutzt werden.

Mappen Sie den Clone der LUN an dieselben ESX-Hosts wie den Original-Datastore, so müssen Sie bedenken, dass der ESX-Host bereits eine LUN kennt, die dieselbe VMFS-ID hat. Binden Sie den Clone an einen ESX-Host, der mit dem Original-Volume keinen Kontakt hat, so können Sie die Signatur beibehalten. Da der Clone nun mit der gleichen VMFS-ID kommt, jedoch eine andere LUN-ID und LUN-Seriennummer hat, erkennt der ESX-Host, dass es sich dabei um einen Snapshot handeln muss, und wird diesen Snapshot »re-signieren«, d. h. eine neue VMFS-ID für den geclonten Datastore vergeben. In ESX 3 und 3.5 musste für das Resignatur-Feature noch die Advanced Option LVM.Resignature auf 1 gesetzt werden.

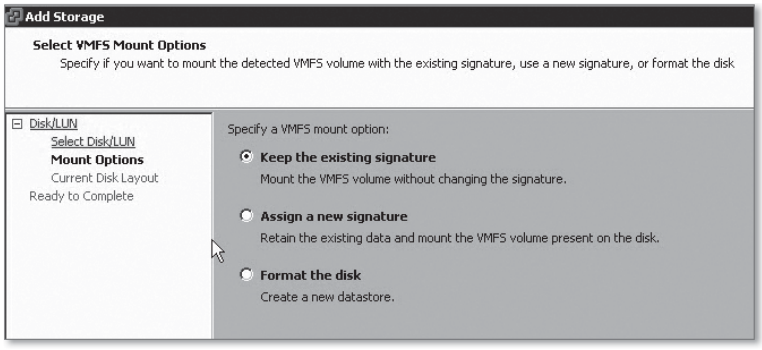


Abbildung 10.57 Was soll mit dem als Snapshot erkannten Datastore passieren?

Seit ESX 4 wählen Sie dies beim Hinzufügen eines neuen Datastores aus, also in diesem Fall ASSIGN A NEW SIGNATURE. Möchten Sie den Datastore einfach hinzufügen, ohne ihn zu resignieren, wählen Sie KEEP THE EXISTING SIGNATURE aus. Diese Unterscheidung ist wichtig, da bei einer Neusignatur die VMs auf diesem Datastore neu registriert werden müssen.

Möchten Sie über die die Kommandozeile vorgehen, so arbeiten Sie mit dem Befehl `esxcfg-volume`:

- `esxcfg-volume -l` = Auflisten aller als Snapshot erkannten Datastores
- `esxcfg-volume -r <VMFS UUID/Label>` = Resignatur des angegebenen Datastores
- `esxcfg-volume -M <VMFS UUID/Label>` = Beibehaltung der Signatur und Verbinden des als Snapshot erkannten Datastores

Für unseren Anwendungsfall eines schnellen Restores oder eines VMFS-Clones für Testzwecke ist in fast allen Fällen eine Resignatur sinnvoll und notwendig.

FlexClones

FlexClones haben eine sehr starke Ähnlichkeit mit LUN-Clones, allerdings ist dieses Feature bei NetApp kostenpflichtig. Mit FlexClones ist es möglich, ganze Volumes zu clonen und nicht nur Clones von einzelnen LUNs innerhalb eines Volumes anzulegen.

Möchten Sie ähnliche Vorgänge wie oben beschrieben (Tests oder Recovery usw.) mit NFS-Datastores durchführen, so müssen Sie eine FlexClone-Lizenz anschaffen – NFS-Datastores bringen keine LUNs mit sich, sondern stellen immer den Export eines gesamten FlexVols einer NetApp dar – deshalb muss auch das ganze Volume geclont werden.

Ist eine FlexClone-Lizenz auf dem NetApp-System eingespielt, so erzeugen Sie mit dem folgenden Befehl einen Clone:

```
na1> vol clone create
usage:
vol clone create <vol-name> [-s none | file | volume]
            -b <parent_flexvol> [<parent_snapshot>]

na1> vol clone create esxnfs_clone -s none -b esxnfs
Creation of clone volume 'esxnfs_clone' has completed.
```

Es gibt auch wieder die Möglichkeit, einen alten Snapshot-Zustand für den Clone zu verwenden – oder aber Sie geben beim VolClone keinen alten Snapshot an, dann wird ein neuer aktueller Snapshot erzeugt:

```
na3021> vol status esxnfs
         Volume State       Status                  Options
         esxnfs online      raid_dp, flex
                            redirect
```

```
         Volume has clones: esxnfs_clone
         Containing aggregate: 'aggr0'

na3021> vol status esxnfs_clone
         Volume State         Status            Options
   esxnfs_clone online        raid_dp, flex     guarantee=none

           Clone, backed by volume 'esxnfs',
                  snapshot 'clone_esxnfs_clone.1'
```

Das geclonte NFS-Volume muss nur per `exportfs` zur gemeinsamen Nutzung freigegeben und dann auf dem ESX-Host als neuer NAS-Datastore verbunden werden. Resignatur oder Ähnliches ist nicht nötig – es kann sofort verwendet werden.

File-Clones und Sub-LUN-Cloning

Die FlexClone-Lizenz bringt in Verbindung mit Deduplizierung (siehe Abschnitt 10.4.2, »Tuning und Optimierung«) einige nette Funktionen mit, die im Alltag noch nicht einfach verwendbar sind, sie werden erst durch die Integration von APIs oder die Bereitstellung von Tools wie dem Rapid Cloning Utility von NetApp interessant. Es wird mindestens ONTAP 7.3.2 benötigt. Ab ONTAP 8.1.1 arbeiten diese Cloning-Features noch schneller und effizienter, außerdem ist ab dieser Version auch die NFS-VAAI unterstützt, so können Sie direkt von vSphere aus Clones erzeugen ohne Verwendung von weiteren Hilfsmitteln oder Command-Line-Befehlen!

Der theoretische Hintergrund sei dennoch kurz erklärt: Für das Erstellen neuer VMs aus Templates helfen die beiden soeben vorgestellten Cloning-Funktionen noch relativ wenig, da beide Clones (egal ob LUN- oder Volume-Clones) immer als Resultat einen weiteren Datastore erstellen. Eigentlich möchte man ja aber im vorhandenen Datastore eine Datei kopieren, nur eben effizienter, also clonen. Genau dafür sind File- und LUN-Clones vorgesehen.

Ein File-Clone funktioniert so, dass – anstatt eine Datei in einem Volume zu kopieren – lediglich eine Kopie der Metadaten (Zeiger auf die Datenblöcke) erstellt wird mit einem neuen Dateinamen. So haben Sie zwei Dateien, die aber auf dieselben Blöcke zeigen. Dieser Vorgang ist sehr sinnvoll bei NAS-Datastores; Sie clonen einfach ganze VMs, indem Sie die VMDK-Dateien clonen.

Der Sub-LUN-Clone geht davon aus, dass innerhalb einer LUN ein VMFS-Datastore existiert und darin VMDK-Dateien liegen. Statt den gesamten Datastore zu clonen, bekommt das NetApp-Speichersystem über eine API eine Liste der Blöcke übermittelt, die die zu kopierende VMDK-Datei innerhalb der LUN belegt, und erzeugt auch wieder nur durch Kopieren der Zeiger auf diese Blöcke eine Kopie der VMDK-Datei innerhalb der LUN. Beide Funktionen können Sie manuell testen, wobei nur die File-Clones so wirklich sinnvoll realisierbar sind. Zum Testen arbeiten Sie mit dem Befehl `clone`:

```
na1> clone start /vol/esxfs/OK-test-flat.vmdk /vol/esxnfs/
          OK-test-flat2.vmdk
Clone operation started successfully. ID: 1.
```

Clones auf diese Weise zu erstellen, ist noch relativ mühsam, da Sie alle Dateien, die zu einer VM gehören, einzeln clonen müssen. Abhilfe schafft das Rapid Cloning Utility von NetApp, das Sie kostenlos über die *now.netapp.com*-Website erhalten. Es ist mittlerweile ein Teil der Virtual Storage Console (VSC), die seit Version 2.1.1 kompatibel mit vSphere 5 ist.

Sollte künftig die vStorage-API zwischen den beiden Herstellern NetApp und VMware noch besser integriert werden, so wird es möglich sein, aus dem vCenter-Server direkt Clones auf dem NetApp-Speicher zu erstellen – transparent mit den gleichen Klicks, wie Sie bisher Dateien kopieren, nur eben schneller und platzsparender. Sie werden ohne zusätzliche Software und ohne Änderung im Administrationsverhalten wesentlich effizientere Kopien seiner VMs erstellen.

10.4.2 Tuning und Optimierung

Flash-Cache-Karten

NetApp hat Storage-Beschleuniger-Karten im Portfolio, die sogenannten Flash-Cache-Karten. Der alte Name dieser Karte war Performance Accelerator Module (PAM). Damit deutlich wird, warum diese Karten sehr sinnvoll sind und wie genau sie funktionieren, müssen Sie zuerst verstehen, wann ein Speichersystem schnell ist.

Bei den meisten Storage-Systemen gilt die alte Regel »Viele Spindeln (also Festplatten) bedeuten viel Geschwindigkeit«. Aber wie schnell ist eine Festplatte eigentlich? Die Geschwindigkeit einer Festplatte wird – wie in Kapitel 9, »Storage-Architektur«, schon beschrieben – in der Anzahl der Input/Output-Operationen pro Sekunde (IOPS) gemessen. Die maximal mögliche Anzahl der IOPS hängt dabei stark von der mittleren Zugriffszeit der Disk ab, und diese ist wiederum von der Drehzahl abhängig. Als Beispiel wählen wir eine moderne FC- oder SAS-Platte mit 15.000 Umdrehungen pro Minute. Eine solche Platte hat eine Zugriffszeit von ca. 5 ms. Das bedeutet leicht vereinfacht, dass man ca. 200 Mal pro Sekunde den Plattenkopf umpositionieren kann und die Disk somit auch 200 I/Os pro Sekunde abarbeiten kann.

Der maximale Datendurchsatz ist bei einer Festplatte eine ebenso wichtige Kenngröße wie die Zugriffszeit bzw. die I/O-Leistung einer Platte – jedoch hängt der Datendurchsatz direkt von der Art des Zugriffsmusters ab. Lesen Sie beispielsweise in 4-K-Blöcken zufällige Daten von der Disk (Random-Read-Muster), so errechnen Sie den Durchsatz einfach mit:

200 IOPS × 4 KByte / IOP = 800 KByte/s

Das ist ein erschreckend niedriger Wert, der allerdings bei echtem Random-Workload nicht unrealistisch ist. Greifen Sie hingegen sequentiell auf eine Festplatte zu, so muss der Plattenkopf nicht umpositioniert werden, und Sie erhalten deutlich höhere Datentransferraten, die

meist bis an die physische Grenze des Festplattenbusses von mehreren Hundert Megabytes pro Sekunde heranreichen. In der Praxis zeigt sich jedoch sehr deutlich, dass die Zugriffsmuster gerade im VMware-Umfeld ziemlich zufällig sind und eine typische I/O-Größe von 4 bis 8 KBytes haben. Das ist nicht verwunderlich, weil typischerweise mehrere Hundert virtuelle Maschinen gleichzeitig auf einem zentralen Storage-Array lesen und schreiben. Für die Planung einer VMware-vSphere-Umgebung müssen Sie deshalb unbedingt auf die Anzahl der benötigten I/Os achten und nicht ausschließlich – wie leider sehr häufig fälschlich angenommen – auf die benötigte Speicherkapazität.

Stellen Sie beispielsweise eine Rechnung an, dass 300 VMs durchschnittlich 40 IOPS benötigen, so sind das in Summe 12.000 I/Os, zur Sicherheit rechnen Sie für Lastspitzen 25 % hinzu, also kommen Sie insgesamt auf 15.000 IOPS. Um diese gewünschte Anzahl an parallelen Zugriffen ohne zu hohe Latenz abzuwickeln, braucht unser Speichersystem ca. 75 Datenfestplatten in der RAID-Gruppe (15.000 geteilt durch 200 I/Os pro Disk). Im Falle eines NetApp-Speichersystems entspricht das ca. 6 Disk-Shelves, jedes Disk-Shelf enthält nämlich 14 Festplatten.

Bei einer Festplattengröße von 450 GB ergibt sich aus 75 Disks eine nutzbare Größe von ca. 25 TB (408.000 MB/Disk × 75 Disks minus 15 % Overhead). Rechnen Sie nun diese 25 TB herunter auf den möglichen Speicher pro VM, so kommen Sie eindeutig zu dem Schluss, dass ca. 85 GB pro VM deutlich zu viel Speicher ist! Die Erfahrung aus vielen Kundenprojekten zeigt, dass eine durchschnittliche VM deutlich weniger Platz benötigt, in den meisten Fällen belegt eine einzelne VM oft nicht mehr als 20 oder 30 GB.

An diesem Punkt sollte Folgendes klargeworden sein:

- Für ausreichende Performance benötigen Sie eine gewisse Anzahl Disks benötigt.
- Jede Disk bringt neben I/O-Leistung auch Kapazität mit.
- Korrektes Storage-Sizing sollte primär nach Performance erfolgen, danach erst nach Kapazität.
- Die meisten Kunden kaufen oft deutlich mehr Kapazität, als sie benötigen, weil sie die I/O-Leistung der vielen Platten brauchen.

Und genau an dieser Stelle greift die Flash-Cache-Karte von NetApp ein.

In der bisherigen Betrachtung der Geschwindigkeit von Storage-Systemen haben wir nämlich eine wichtige Kenngröße außer Acht gelassen: den *Cache*. Doch was ist ein Cache, und wie funktioniert er? Der Lesecache eines jeden Speichersystems merkt sich in einem sehr schnellen Speicher (meistens ein Teil des System-RAMs des Controllers) kürzlich von Festplatten gelesene Daten oder Daten, auf die sehr häufig zugegriffen wird. Sollte ein Client auf Daten zugreifen, die sich schon im Cache befinden, so kann auf einen langsamen Festplattenzugriff verzichtet werden, und die angefragten Daten kommen mit sehr hoher Geschwindigkeit aus dem Cache direkt zum Client. Je größer also der Cache, desto häufiger werden die Daten aus

dem Cache zum Client geliefert, und desto seltener muss auf die Festplatten zugegriffen werden – die Performance des Speichersystems steigt. Könnte man also den Cache eines Speichersystems erweitern, so wäre es möglich, die gewünschte Performance aus dem vergrößerten Cache zu gewinnen statt durch die Anschaffung vieler Festplatten.

Flash Cache von NetApp ist kurz gesagt eine Cache-Erweiterungskarte. Durch den Einsatz von Flash Cache können Sie auf den zusätzlichen Kauf von Festplatten verzichten, bei gleichzeitig sinkenden Betriebskosten. Schließlich brauchen Festplatten im Betrieb Strom, Kühlung, Platz und einen Wartungsvertrag.

Die meisten Storage-Hersteller begegnen der Problematik von extrem hohen I/O-Anforderungen ihrer Kunden mit dem Einsatz von Solid-State-Disks (SSDs), einer modernen Art von nicht flüchtigem Flash-Speicher. Bei Flash-Speicher entfällt die mechanische Umpositionierung der Festplattenköpfe, daher sind die Antwortzeiten von SSDs je nach Bauart um den Faktor 10–100 schneller als klassische Platten.

Da SSDs aktuell aber noch sehr teuer und leider nur mit relativ niedrigen Kapazitäten verfügbar sind, ist ihre Verwendung nur im sogenannten Tier-0-Einsatz rentabel, also bei Applikationen, die wirklich allerhöchste Anforderungen stellen. Der Kunde wählt also sehr genau aus, welche Art von Daten auf die teuren, aber schnellen Disks gelegt wird. NetApp verfolgt eine andere, effizientere Strategie: Anstatt den Kunden aktiv wählen zu lassen, welche Daten von Applikation es verdienen, auf den schnellen Platten zu lagern, nutzt NetApp die Flash- und SSD-Technologie einfach als Cache. Dadurch profitieren alle Daten, die auf dem Storage-System liegen – eben alle Daten, die am häufigsten abgerufen werden, wie beim normalen System-RAM-Cache. Der einzige Unterschied ist, dass der Cache um ein Vielfaches größer ist als das reguläre System-RAM, das in der Regel zwischen 2 und 32 GB groß ist.

Seit ONTAP 8.1.1 bietet NetApp im Cluster-Mode neben den Flash-Cache-Karten auch die Möglichkeit der Storage-Beschleunigung durch sogenannte Hybrid-Aggregate an. Dabei kann der Kunde die Größe des Caches pro Aggregat festlegen, indem er dem Aggregat neben klassischen Festplatten auch SSDs zur Beschleunigung hinzufügt. Diese dienen dann – anders als Flash Cache – dem Lese- und Schreibe-Cache.

Die Flash-Cache-Karten sind in drei Varianten verfügbar, in Größen von 256 GB, 512 GB und 1 TB. Je nach NetApp-Controller-Typ sind in den aktuellen Mittelklasse- und High-End-Systemen zwischen eine und fünf Karten nutzbar, was die Gesamtmenge des Cache deutlich erhöht.

Nachdem wir erklärt haben, wie diese Karten funktionieren, möchten wir jetzt ihre Konfiguration zeigen. Neben der Flash-Cache-Karte brauchen Sie eine Softwarelizenz für die NetApp, diese wird allerdings beim Kauf der Karte mitgeliefert.

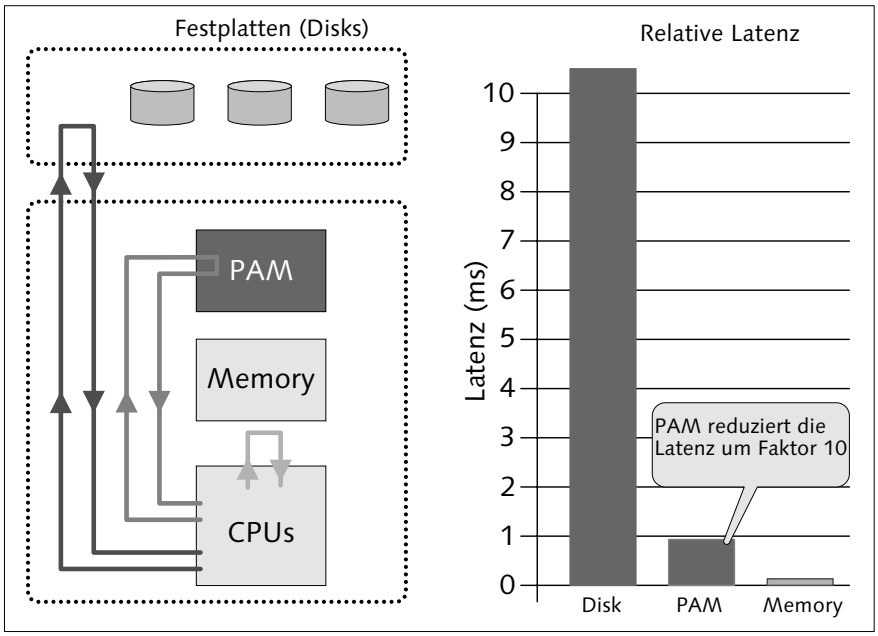


Abbildung 10.58 Arbeitslogik von Flash-Cache-Karten und ihre Latenzzeiten

Eine Karte wird aus Sicht des NetApp-Betriebssystems ONTAP so erkannt:

```
na1> sysconfig -v 3
      slot 3: Flash Cache 256 GB
                State:     Enabled
           Model Name:     X1937A-R5
        Serial Number:     5000246719
          Part Number:     111-00660
       Board Revision:     D0
         FPGA Release:     1.10
           FPGA Build:     201012200653
```

Die Konfiguration der Flash-Cache-Karte ist relativ einfach: Sie müssen sie lediglich aktivieren, später passen Sie gegebenenfalls auch noch Parameter an, je nachdem, welche Art von Daten im Cache der Karte landen soll.

Zum Einschalten verwenden Sie den folgenden Befehl:

```
na1> options flexscale.enable on
```

Weitere Parameter prüfen Sie mit:

```
na1> options flexscale
flexscale.enable            on
flexscale.lopri_blocks      off
flexscale.normal_data_blocks on
```

Diese Einstellungen sind ein sinnvoller Default. Generell werden Metadaten immer gecacht, die normalen Datenblöcke auch. Auf das Cachen von »Low-Prio-Blocks« sollten Sie in den meisten Anwendungsfällen verzichten, weil dadurch bei großen Lesevorgängen (z. B. Backups) sonst der gesamte Cache überschrieben wird und somit wertlos ist.

Anschließend sollten Sie das System einfach arbeiten lassen und nach einigen Stunden oder Tagen die Nutzung des Cache prüfen.

```
na1> stats show -i 5 -p flexscale-access
 Cache                                          Disk Reads
 Usage  Hit Meta Miss Hit Evict Inval Insert Replaced
     %   /s   /s   /s   %    /s    /s     /s       /s
    99   96   13  338  22    10     0      0       96
    99  146    6  451  24     0     0      0       27
    99  133   11  438  23     0     0      0       24
    99  110   18  487  18     0     0      0       46
    99  222   44  499  30     0     0      0      115
    99  141   11  327  30     0     0      0       27
    99  170   17  846  16     0     0      0       57
    99   43   12  382  10     0     0      0       24
```

Nach einer gewissen Aufwärmzeit füllt sich der Cache, in unserem Beispiel ist er zu 99 % voll. Dann steigt die Cache-Hit-Rate, hier ist sie aktuell nur bei ca. 20–30 % – unser System ist nicht sehr stark ausgelastet.

Gerade bei VMware- und VDI-Workloads (virtuelle Desktops) sind Flash-Cache-Karten extrem nützlich, da viele VMs gleichzeitig von den Platten lesen (Random-Workload), dabei sind die höchsten Beschleunigungsraten zu erzielen. Besonders die VDI-typischen »*Boot-Storms*« sind ohne intelligente und ausreichend große Caches nicht mehr performant abbildbar.

Flash-Cache-Karten funktionieren übrigens auch hervorragend mit der NetApp-Deduplizierung zusammen. Stellen Sie sich vor, dass in einem VDI-Szenario 200 Desktop-VMs die gleiche VMDK-Festplattendatei haben. Dieses wurde durch NetApp-Deduplizierung auf nur eine einzige Instanz reduziert, braucht also nur so viel Diskspeicher wie eine einzelne VM, alle doppelten Blöcke wurden eliminiert. Diese reduzierte Menge an Speicherplatz passt nun gut in den Cache der Flash-Cache-Karte. Selbst bei einer 256 GB großen Flash-Cache-Karte kann es durchaus vorkommen, dass ein großer Teil der Leseanfragen ausschließlich aus der Karte bedient wird und die Disks nur noch zum Schreiben benötigt werden. Die spürbare höhere Geschwindigkeit für die Clients ist dabei enorm, der eingesparte Plattenplatz ebenso.

Deduplication

Deduplizierung ist die Erkennung und Eliminierung von redundanten Daten. Netapp hat seit ONTAP 7.2 einen Mechanismus zur Deduplication in das Betriebssystem mit eingebaut. Die benötigte ONTAP-Lizenz heißt A-SIS, das Marketing bezeichnet die Funktionalität als Dedupe. Deduplizierung hilft dabei, weniger Speicherplatz zu verbrauchen, indem man doppelte Blöcke

mehrfach verlinkt (ähnlich wie klassische Unix-Hardlinks) und sie somit nicht mehr doppelt speichern muss. Nur arbeitet Dedupe nicht wie Unix-Hardlinks auf Dateiebene, sondern auf Blockebene – datei-übergreifend. Etwas Ähnliches kann ONTAP schon sehr lange, und zwar im Zusammenhang mit CIFS-File-Folding. Um es noch einmal ganz deutlich zu sagen: A-SIS hat *nichts* mit Komprimierung zu tun! Die Dateien werden weiterhin unkomprimiert auf den Platten abgelegt. Lediglich mehrfach vorhandene Datenblöcke desselben Inhalts werden eliminiert.

Das Feature ist kein Performance-Killer, da es sich um einen sogenannten Post-Processing-Mode handelt, die Daten werden also zuerst normal gespeichert – dedupliziert wird dann später; und zwar nur, wenn es explizit gestartet wird: entweder manuell oder per Scheduler. Das bedeutet, dass im Normalbetrieb keine Deduplizierung der gleichen Blöcke stattfindet, Sie also die normale Performance der Maschine erwarten können. Erst um Mitternacht (das ist der verstellbare Default) legt der A-SIS-Mechanismus los. A-SIS arbeitet wie folgt:

1. Das NetApp-System scannt alle Blöcke in einem Volume und erstellt Prüfsummen, die sogenannten *Fingerprints*.
2. Anschließend werden die Fingerprints sortiert und miteinander verglichen.
3. Gleiche Fingerprints kommen auf die Liste der genauer zu inspizierenden Blöcke.
4. Die Blöcke werden anschließend wirklich Byte für Byte verglichen, um sicherzustellen, dass es sich wirklich um ein Duplikat handelt und nicht nur zufällig die Prüfsumme der Blöcke gleich ist.
5. Jetzt erst beginnt der eigentliche Vorgang der Deduplizierung. Die identifizierten Dubletten werden erst neu verlinkt, anschließend die redundanten Blöcke als frei markiert.

Neben dem Nearline- und Backup-Storage-Markt gibt es besonders bei NetApp-Kunden auch eine starke Nachfrage aus dem Primärspeicher-Umfeld nach DeDupe. Die Erfahrungen zeigen, dass auch im normalen File-Serving-Umfeld relativ einfach Einsparungseffekte von 30 bis 40 % zu erzielen sind, aber auch im Block-Storage-Umfeld (erst ab ONTAP 7.2.2 unterstützt) gute Ergebnisse erreicht werden können, insbesondere wenn es sich um offensichtliche Dubletten handelt wie im VMware ESX-Umfeld … Dort hat schließlich jede virtuelle Maschine ein Betriebssystem installiert. Je mehr VMs also auf dem gleichen Volume bzw. innerhalb der gleichen LUN liegen, desto mehr Einsparungen ergeben sich, in einigen Kundenszenarien sogar mehr als 70 %.

Empfohlen wird der Einsatz von Deduplizierung auf dem NetApp-System in Zusammenhang mit VMware erst seit ONTAP 7.3.2, da seit dieser Version auch deduplizierte Blöcke aus verschiedenen Files (VMDK-Dateien!) optimal im RAM oder Flash-Cache verwaltet werden. Der Cache wird ebenfalls dedupliziert verwaltet, was auch dort zu einer besseren Platzausnutzung und somit zu einer weiteren Geschwindigkeitssteigerung führt. Bei all den Vorteilen wollen wir die Nachteile nicht verschweigen:

A-SIS funktioniert nur auf Volume-Ebene. Damit können Sie nur Einsparungen innerhalb eines flexiblen Volumes erzielen, jedoch leider noch nicht volumeübergreifend, also auf

Aggregatsebene. Sie müssen also beim Layout des Storage darauf achten, jene Daten in Volumes zusammenzufassen, die latent zu Dubletten neigen. Ein Deduplizierungsprozess wirkt sich auf den Snapshot-Platzverbrauch aus. Das ist kein wirklicher Nachteil per se, sondern nur ein »normaler technischer Vorgang», wird jedoch von einigen Kunden als leichter Nachteil empfunden: Deduplizierung bedeutet Datenveränderung, genau wie andere Löschvorgänge. Damit wird der Plattenplatz zwar freigegeben, aber die dedupizierten Blöcke werden immer noch im Snapshot festgehalten, bis dieser verschwindet.

Im Zusammenspiel mit Block-Storage (FCP und iSCSI) funktioniert DeDupe auch, allerdings muss zwingend auch Thin Provisioning aktiviert werden, sonst sind die Einsparungen vorhanden, aber leider nicht auf dem Storage-Array sichtbar. Das ist auch kein wirklicher Nachteil (Thin Provisioning ist sehr effizient!), nur schrecken einige Kunden davor zurück, weil sie durch die Überbuchung, die Thin Provisioning mit sich bringt, gezwungen sind, den Speicherplatzverbrauch genauer zu überwachen (Aufwand). Mehr dazu lesen Sie auf Seite 546 im folgenden Abschnitt »Thin Provisioning«.

Praxisbeispiel Konfiguration und Auswertung von DeDupe

Zuerst müssen Sie die beiden benötigten Lizenzen einspielen. Seit ONTAP 8.0 brauchen Sie keine Nearstore-Lizenz mehr für DeDupe, und seit 8.1 brauchen Sie gar keine Lizenz mehr!

```
na1> license add XXXXXXX
A nearstore_option site license has been installed.
        Data ONTAP is switching to NearStore mode.
        NearStore Option enabled.
Mon May 14 14:57:32 MEST [rc:notice]: nearstore_option licensed
na1> license add XXXXXXX
A a_sis site license has been installed.
        A-SIS enabled.
Mon May 14 14:58:08 MEST [rc:notice]: a_sis licensed
```

Schritt 1: Grund-Setup

Wir brauchen zuerst ein Aggregat und ein Volume, auf denen wir Platz sparen wollen. In vorhandenen Umgebungen können Sie diesen Schritt natürlich überspringen.

```
na1> aggr create aggr0 5
Creation of an aggregate with 5 disks has completed.
Mon May 14 14:58:34 MEST [wafl.vol.add:notice]: Aggregate aggr0 has been added
to the system.
na1>
na1> vol create asisdemo aggr0 10g
Creation of volume 'asisdemo' with size 10g on containing aggregate
'aggr0' has completed.
```

Anschließend müssen wir Daten auf unserem Volume erzeugen. Das machen wir am einfachsten und schnellsten mit dem versteckten Befehl `mkfile`. Ein Vorteil von `mkfile` ist, dass es lau-

ter Nullen in die erzeugte Dateien schreibt – welche Daten eignen sich besser für Deduplizierung als lauter Nullen?

```
na1> priv set -q diag
na1*> mkfile 1g /vol/asisdemo/f1
na1*> mkfile 1g /vol/asisdemo/f2
na1*> df -h asisdemo
Filesystem               total       used      avail capacity
/vol/asisdemo/          8192MB     2052MB     6139MB      25%
```

Nun liegen ca. 2 GB in zwei verschiedenen Dateien vor – fast alle Blöcke können theoretisch eliminiert werden. Aktivieren Sie A-SIS für das Volume aktivieren, und starten Sie danach den Deduplizierungsprozess:

Schritt 3: DeDupe aktivieren

```
na1*> sis on /vol/asisdemo
SIS for "/vol/asisdemo" is enabled.
Already existing data could be processed by running "sis start -s /vol/
asisdemo".
```

Schritt 4: Initialen DeDupe-Lauf starten

```
na1*> sis start -s /vol/asisdemo
The file system will be scanned to process existing data in
  /vol/asisdemo.
This operation may initialize related existing metafiles.
Are you sure you want to proceed with scan (y/n)? y
Mon May 14 15:00:37 MEST [wafl.scan.start:info]: Starting SIS volume scan on vo
lume asisdemo.
```

Den initialen Lauf müssen Sie nur einmal durchführen, später starten Sie die Deduplizierungsvorgänge entweder per Scheduler oder manuell.

Das NetApp-System erstellt nun im Hintergrund seine Fingerprint-Datenbank mit den Hashes aller Blöcke auf dem Volume. Dieser Vorgang braucht erstaunlich wenig CPU, wirkt sich aber negativ auf den Read-Cache aus. Das Cache-Age sinkt auf wenige Minuten.

Den Fortschritt der Indizierung prüfen Sie wie folgt:

Phase 1: Fingerprints sammeln

```
na1*> sis status /vol/asisdemo
Path                 State      Status     Progress
/vol/asisdemo        Enabled    Active     1949 MB Scanned
na1*>
na1*> sis status /vol/asisdemo
```

```
Path                State      Status     Progress
/vol/asisdemo       Enabled    Active     2048 MB Scanned
```

Phase 2: Doppelte Prüfsummen finden

Jetzt identifizieren Sie die doppelten Blöcke anhand des Indexes:

```
na1*> sis status /vol/asisdemo
Path           State      Status     Progress
/vol/asisdemo  Enabled    Active     372 MB Searched
```

Phase 3: Die Dubletten entfernen

```
na1*> sis status /vol/asisdemo
Path           State      Status     Progress
/vol/asisdemo  Enabled    Active     178 MB (8%) Done
na1*> sis status /vol/asisdemo
Path           State      Status     Progress
/vol/asisdemo  Enabled    Active     559 MB (27%) Done
```

Das Ergebnis ist wie folgt:

```
na1*> sis status
Path                    State      Status     Progress
/vol/asisdemo           Enabled    Idle       Idle for 00:07:31
na1*>
na1*> sis status -l
Path:                   /vol/asisdemo
State:                  Enabled
Status:                 Idle
Progress:               Idle for 00:07:33
Type:                   Regular
Schedule:               sun-sat@0
Last Operation Begin:   Mon May 14 15:00:37 MEST 2011
Last Operation End:     Mon May 14 15:02:42 MEST 2011
Last Operation Size:    2048 MB
Last Operation Error:   -
Stage:                  Done
Fingerprints Gathered:  524288
Gathering Begin:        Mon May 14 15:00:37 MEST 2011
Fingerprints Sorted:    524288
Duplicate Blocks Found: 524287
Sorting Begin:          Mon May 14 15:01:10 MEST 2011
Blocks De-duplicated:   522571
De-duping Begin:        Mon May 14 15:01:15 MEST 2011
Fingerprints Deleted:   0
Checking Begin:         -
```

```
na1*>
na1*> df -h asisdemo
Filesystem              total        used     avail capacity
/vol/asisdemo/          8192MB       30MB     8161MB       0%
```

Das Beispiel zeigt extreme Einsparungsraten: Von 524.288 Blöcken sind 524.287 Blöcke gleich! Das war zu erwarten, da nur Nullen in den Blöcken enthalten sind. Warum konnten aber nur 522.571 Blöcke dedupliziert werden? Das liegt an der Art und Weise, wie das WAFL-Dateisystem von NetApp funktioniert. Momentan sind »nur« 255 Zeiger auf den gleichen Block möglich. Dadurch ergibt sich eine maximale Einsparungsrate von 1 : 255. Seit ONTAP-Version 8.1 ist es wegen des verbesserten Dateisystems möglich, einen Deduplizierungsfaktor von 1 : 32767 zu erreichen. Schließlich können Sie sich anzeigen lassen, wie viel wirklich eingespart wurde:

```
na1*> sis stat -b
Path             Allocated      Saving          %Saved
/vol/asisdemo    13615 blocks   783345 blocks   98%
na1*> sis stat -v
Path             Allocated      Saving          %Saved
/vol/asisdemo    53 MB          3059 MB         98%
```

Es sei nochmals angemerkt, dass dies ein Extrembeispiel ist. Realistische Werte bewegen sich je nach Art der Daten zwischen 5 und 70 % Einsparung. Wer grob abschätzen möchte, wie viel er sparen könnte, dem sei die NetApp-(Marketing-)Website *www.itcalc.com* empfohlen.

Thin Provisioning

Thin Provisioning ermöglicht weitere Platzeinsparungen auf dem Speichersystem, da nur noch der Speicherplatz reserviert wird, der auch real belegt ist. Dadurch können Sie das Speichersystem überbuchen, also mehr Kapazität an die Hosts vergeben, als wirklich vorhanden ist. Das ist an vielen Stellen sehr sinnvoll, da die Platzausnutzung des Hosts oft sehr schlecht ist; insbesondere im Virtualisierungsumfeld ist ohne Thin Provisioning die Verschwendung von teurem Speicherplatz programmiert. Dies wollen wir anhand eines Beispiels aufzeigen.

Wir gehen davon aus, dass der ESX-Host einen FCP-Datastore (also eine LUN) benötigt, der 100 GB groß ist. Auf dem NetApp-System legen Sie ein Volume an, das ebenfalls 100 GB groß ist und das wiederum eine 100 GB große LUN enthält. Es sollen keine NetApp-Snapshots erstellt werden, deshalb reichen 100 GB Volume-Größe aus. Somit sind auf dem NetApp-Speichersystem 100 GB Platz verbraucht, obwohl der ESX-Host noch gar nichts in dem Datastore abgelegt hat. Die Planung ist, dass in diesem Datastore 7 VMs mit je einer 10-GB-VMDK-Datei abgelegt werden sollen, somit wären ca. 70 GB verbraucht; allerdings muss noch 30 GB Platz frei bleiben, da die VMs ja Delta-Dateien (für VM-Snapshots) und VSWP-Dateien für Memory-Overcommitment anlegen werden. Innerhalb einer jeden VMDK-Datei wird Windows XP installiert, die Installation ist ca. 4 GB groß, dazu kommen 2 GB pro VM an Applikationen.

Zusammengezählt wäre der reale Platzverbrauch 7 × 6 GB, in Summe 42 GB. Doch auf der NetApp-Seite wurden wegen der festen Provisionierung die vollen 100 GB belegt. Durch Thin Provisioning können Sie den nicht belegten Platz wieder frei machen.

Generell kann festgehalten werden, dass Thin Provisioning die einzig sinnvolle Art der Speichervergabe ist. Oft sind sich Administratoren oder Applikationsbetreuer nicht sicher, wie viel Speicher später wirklich benötigt wird. Deshalb buchen sie zur Sicherheit erst einmal deutlich mehr Speicherplatz, als sie vielleicht je belegen werden. Durch Thin Provisioning wird diese Platzverschwendung reduziert bzw. eliminiert.

Thin Provisioning auf NetApp-Seite ist nicht mit dem Thin-Format der VMDK-Platten zu verwechseln! Der Mechanismus ist zwar grundlegend der gleiche, allerdings spart eine Thin-VMDK-Datei auf NetApp nur Platz, wenn die LUN auch im Thin-Provisioning-Modus läuft oder die Thin-VMDK-Datei auf einem NFS-Datastore liegt. Auf NetApp-Seite gibt es mehrere logische Schichten, die überbucht werden können.

Thin Provisioning: Volumes überbuchen

Die wichtigste Schicht ist die LUN innerhalb eines Volumes. Ob eine LUN dünn provisioniert ist, hängt damit zusammen, ob die sogenannte LUN Space Reservation aktiviert ist. Das wählen Sie beim Anlegen der LUN aus (`lun create -o noreserve`) oder schalten es später an- und ab (`lun set reservation enable/disable`).

LUN Space Reservation *an* hat zwei Auswirkungen:

1. Die LUN belegt sofort den vollen Platz im Volume, auch wenn noch keine Blöcke in der LUN belegt wurden.
2. Sämtlicher Platz, der in der LUN belegt ist, wird im Falle eines Volume-Snapshots auf dem NetApp-Speichersystem noch einmal außerhalb der LUN im Volume belegt, man spricht von der Overwrite Reserve.

Punkt 1 ist an sich schon unschön, siehe die Kalkulation von gerade eben. Aber Punkt 2 wirkt sich sehr negativ auf die Platzbelegung aus, da im Falle einer vollen LUN die doppelte LUN-Größe im Volume an Platz belegt (eigentlich reserviert) wird. Es gibt eine Volume-Option namens *Fractional Reserve*, die per Default auf 100 % steht. Sie besagt, dass 100 % des in der LUN belegten Platzes nochmals außerhalb reserviert werden, falls ein Snapshot erstellt wurde. Sie können diese Option justieren und den Wert reduzieren (z. B. auf die reale Datenänderungsrate), aber dann ist nicht mehr gewährleistet, dass immer genug Platz im Volume zur Verfügung steht, um alle Schreibzugriffe erfolgreich durchzuführen.

Noch einmal ganz deutlich: Wer diese Reserve angeschaltet lässt, hat immer die Sicherheit, dass genug Platz für Schreibzugriffe in der LUN vorhanden ist – allerdings wird auch ziemlich viel Platz verschwendet.

LUN Space Reservation *aus* hat auch zwei Auswirkungen:

1. Die LUN belegt nur den Platz im Volume, der auch innerhalb der LUN belegt ist.
2. Im Falle von Snapshots des Volumes, in dem die LUN liegt, wird keinerlei Reserve abgebildet.

Dieser Zustand ist aus Gründen der Platzeinsparung optimal, da leerer Platz dann keinerlei Speicher im Volume auf dem NetApp-Storage belegt. Allerdings besteht hier die große Gefahr, dass das Volume sich so weit füllt, dass kein Platz mehr für Schreibzugriffe in der LUN zur Verfügung steht. In diesem Fall nimmt das Betriebssystem von NetApp aus Schutzgründen bezüglich der Datenkonsistenz die LUN offline: Das fatale Resultat für den ESX-Host ist, dass der Datastore verschwindet und alle VMs darin abstürzen werden.

Damit das nicht passieren kann, gibt es einen Schutzmechanismus, der sich *Volume Autosize* nennt. Sie können einstellen, dass im Volume automatisch bestimmte Snapshots gelöscht (`snap autodelete`) werden oder dass das Volume sich automatisch vergrößert (`vol autogrow`).

Im Falle von NFS-Datastores ist das Thin Provisioning wesentlich einfacher, da im Volume ja sowieso nur der Platz belegt ist, der real durch Daten im Datastore verwendet wird. Ein Container wie LUNs existiert bei NFS nicht. Zusätzliche Einsparungen sind einfach möglich, indem Sie die VMDK-Dateien als Thin-Files anlegen, neu angelegte VMDK-Dateien auf NFS-Datastores waren bei VMware ESX in der Standardeinstellung schon immer Thin-Files.

Deduplication von NetApp erzeugt den freien Platz im Volume. Diesen neuen Platzgewinn können Sie mit LUNs nur dann nutzen, wenn diese thin-provisioned sind. Wäre die Platzreserve dagegen nicht ausgeschaltet, so belegte die LUN immer ihre volle Größe – egal, ob Daten darin sind oder nicht. Einsparungen von DeDupe werden bei NFS-Datastores sofort sichtbar. Der durch DeDupe entstandene neue freie Platz im Volume ist nur auf Storage-Seite sichtbar (und zwar im Volume), nicht aber auf ESX-Seite. Möchten Sie den gewonnenen Platz dort auch nutzen, so provisionieren Sie einfach eine weitere LUN für einen weiteren Datastore. Bei NFS hingegen ist das nicht nötig, der freie Platz wird sofort im Datastore sichtbar.

Thin Provisioning: Aggregate überbuchen

Die Einsparungen, die im Volume durch Thin Provisioning oder DeDupe erzielt werden, sollten im Idealfall an das Aggregat weitergegeben werden, in dem das Volume liegt, nur dann können andere Volumes im selben Aggregat vom gewonnenen Speicher profitieren. Anstatt nur in einem einzelnen Volume Platz zu sparen, kann so das gesamte Speichersystem oder wenigstens das ganze Aggregat den freien Speicher für andere Zwecke nutzen.

Der dafür vorgesehene Mechanismus heißt *Volume Space Guarantee* und lässt sich in drei Stufen einstellen:

1. VOLUME: Der gesamte Volume-Platz wird im Aggregat abgezogen, egal, ob Daten darin liegen oder nicht, ähnlich der vollen LUN Space Reservation.
2. NONE: Im Aggregat wird nur der Plattenplatz belegt, der auch im Volume real verbraucht ist.
3. FILE: Das Aggregat reserviert für das Volume exakt so viel Platz, wie das Volume benötigt, um die LUN Space Reservation einzuhalten.

Somit wäre im Gesamtbild betrachtet die platzsparendste Variante:

1. LUN Space Reservation: aus
2. DeDuplizierung: an
3. Volume Space Reservation: auf NONE

Thin Provisioning: Überwachung

Die große Krux an Thin Provisioning ist, dass Sie gezwungen sind, die Platzverbräuche zu überwachen, um eine Überfüllung des gesamten Systems frühzeitig zu erkennen und zu verhindern.

Das Gefahrenpotential bei Thin Provisioning ist deutlich größer als bei klassischer fetter Provisionierung von Speicher. Im klassischen Modell füllt sich vielleicht ein einziger Speicherbereich, und eine einzige Applikation bekommt Platzprobleme. Bei Thin Provisioning hingegen bedeutet ein einziger vollgelaufener Speicherbereich immer, dass alle Applikationen gleichzeitig betroffen sind und Probleme bekommen werden. Durch kontinuierliche und automatische Überwachung müssen Sie also dafür sorgen, dass der Speicher nicht vollläuft und Sie rechtzeitig reagieren können. Das kostenlose Verwaltungsprodukt *OnCommand* (früher: »Operations Manager« oder »Data Fabric Manager«) von NetApp erlaubt dies. Wer lieber mit einer Open-Source-Lösung arbeiten möchte, dem sei das Nagios-Plugin *check_filer* (*check_naf*) der Firma Teamix GmbH aus Nürnberg empfohlen. Das Plugin ist Teil der Teamix Monitoring Plugins und kann unter *http://www.teamix.org/projects/monitoringplugins* heruntergeladen werden.

Neben der Überwachung hat sich ein einfacher Trick eingebürgert, mit dem Sie mehr Zeit zum Reagieren gewinnen: Ein sogenanntes *Platzhalter-Volume* (auch *Spacer-Volume* genannt). Die Idee ist einfach: Sie schalten Thin Provisioning für möglichst alle Ihre Daten-Volumes ein. Ein zusätzliches Volume namens »Platzhalter« wird aber nicht dünn provisioniert; es dient dazu, künstlich eine gewisse Menge Speicherplatz zu blockieren. Ich empfehle – abhängig vom Anwendungsfall –, ca. 20–25 % der Aggregatsgröße durch das Platzhalter-Volume zu blockieren. Sollte nun das Monitoring melden, dass der Platz zur Neige geht, so können Sie als erste Maßnahme Platz gewinnen, indem Sie das Platzhalter-Volume verkleinern. Das war die erste Warnung für Sie. Anschließend sollten Sie zügig die Kapazität Ihres Speichersystems erweitern – Sie müssen Festplatten nachkaufen. Das Spacer-Volume erkauft Ihnen vereinfacht gesprochen lediglich etwas Zeit. Noch einmal deutlich: Thin Provisioning ist eine tolle Sache, wer aber nicht überwacht, der handelt fahrlässig!

Thin Provisioning: Space-Reclamation

Wie gerade beschrieben bietet Thin Provision eine Methode, den Speicher nach Bedarf zu allokieren, also Speicherplatz erst dann auf dem Storage-System zu belegen, wenn er auf Host-Seite (ESX-Host) oder innerhalb der VM benötigt wird. Der dadurch gewonnene Platzvorteil hält aber nicht ewig an. Anfangs profitieren Sie mehr von Thin Provisioning als später. Ursächlich dafür ist die Art und Weise, wie die verschiedenen Speicher-Container miteinander kommunizieren. Die verschiedenen übereinanderliegenden Container sind:

- Dateisystem NTFS (innerhalb der VM)
- VMDK-Container
- Dateisystem VMFS
- LUN auf Speichersystem

Wenn eine darüberliegende Schicht Speicherblöcke allokiert, wird die darunterliegende Schicht über den Speicherbedarf informiert. Ein Beispiel: Eine neue Datei wird innerhalb einer VM erstellt. Diese Datei wird folglich Platz im NTFS der VMs verbrauchen. NTFS belegt mindestens einen Block (oder mehr). Daraufhin ist ein Block in der VMDK-Datei belegt, der wiederum einen Block im VMFS verbraucht. Das VMFS belegt den Block schließlich in der LUN. Damit ist ein Block innerhalb der LUN als verbraucht gekennzeichnet, auf unserem Speichersystem ist folglich weniger freier Platz verfügbar. Leider funktioniert der Vorgang beim Löschen von Daten aber nicht. Gelöschte Daten innerhalb einer VM (oberste Schicht) führen nicht dazu, dass innerhalb der LUN wieder Platz freigegeben wird (unterste Schicht). Das liegt daran, dass das NTFS dem VMDK-Container nicht meldet, dass ein Block nicht mehr benötigt wird. Auch ein VMDK-Container meldet dem VMFS nicht, wenn ein Block nicht mehr gebraucht wird. In anderen Worten bedeutet das: Thin Provisioning spart nur dann Platz, solange noch nicht alle Blöcke in unseren Container jemals als belegt markiert waren. Je länger also eine dünn provisionierte VM-Farm existiert, desto weniger Ersparnis haben Sie durch Thin Provisioning.

In vSphere 5 gab es dennoch gute Neuigkeiten: VMFS-5 kann jetzt in bestimmten Situationen freigewordene Blöcke doch auch an die LUN weiterkommunizieren; wenn eine gesamte Datei (z. B. VMDK oder VSWP) innerhalb eines VMFS-5-Dateisystems gelöscht wurde, so werden deren Blöcke auch in der LUN freigegeben. Ganze VMDK-Dateien werden z. B. beim Löschen einer VM freigegeben oder aber bei einem Storage-vMotion-Vorgang. Im Zusammenhang mit NFS-Datastores ist die Thematik der Space-Reclamation zwar auch wichtig, allerdings berührt sie nicht so viele Schichten. Sowohl der Container des VMFS-Dateisystems als auch der Container der LUN entfallen – das Speichersystem weiß direkt, welche VMDK-Dateien existieren und somit Platz belegen. Freie Blöcke innerhalb von dünn provisionierten VMDK-Dateien belegen ebenfalls keinen Platz auf dem NFS-Storage, solange dieses mit sogenannten Sparse-Files umgehen kann.

Zusammenfassend ist festzuhalten, dass Space-Reclamation eine wichtige Komponente für Thin Provisioning ist, durch die erst das Versprechen von Platzeinsparungen langfristig

einhaltbar ist. Für eine ganzheitliche Umsetzung der Space-Reclamation muss VMware auf zwei Ebenen nachbessern: Einerseits müssen innerhalb der VMDK-Datei die frei gewordenen Blöcke nach unten zum VMFS (oder NFS) weiterkommuniziert werden, andererseits muss ein VMFS freigewordene Blöcke direkt an die LUN weitergeben – und nicht erst beim vollständigen Löschen der VMDK-Datei.

NetApp hat schon länger einen Ansatz für Space-Reclamation innerhalb von NTFS-Dateisystemen auf LUNs; dieser Mechanismus funktioniert aber aktuell nur dann, wenn es sich um eine LUN direkt auf dem NetApp-System handelt und leider nicht bei einem NTFS innerhalb einer VMDK-Datei. Die Schnittstellen von VMware fehlen.

10.4.3 Best Practices

Zu Beginn dieses Kapitels haben wir die grundlegende Konfiguration und Einrichtung der Storage-Anbindung gezeigt, allerdings sind im Zusammenhang mit NetApp und Speichersystemen allgemein noch weitere Punkte für einen reibungslosen Betrieb zu beachten. All diese Punkte fassen wir hier unter »Best Practices« zusammen.

NetApp-vSphere-Integration

NetApp liefert für die automatische Implementierung aller empfohlenen vSphere- und NetApp-Einstellungen fertige Werkzeuge mit. Sie sollten diese Software unbedingt installieren und konfigurieren, da sonst Ihr ESX-Setup unter Umständen nicht optimal funktionieren wird. Die Auswirkung der fehlenden Software kann unterschiedlich schlimm sein. Im besten Fall laufen die Systeme lediglich suboptimal, also zu langsam. Im schlimmsten Fall glauben Sie, dass scheinbar alles funktioniert, da keine Fehler angezeigt werden, aber der Teufel steckt hier leider im Detail. Wenn zum Beispiel ein NetApp-Controller ausfällt, so passiert ein Cluster-Failover – der andere Controller übernimmt den Dienst. Dieser Vorgang kann aber bis zu drei Minuten dauern. Sowohl der vSphere Host als auch die darauf laufenden VMs müssen aber genauso lange warten, bevor sie ihren Storage (Datastore oder Disks) als verloren melden. Die Standardeinstellungen sind leider deutlich kürzer. Im Normalfall sieht es also aus, als wäre alles in Ordnung, bei einem Cluster-Schwenk hängen sich die VMs jedoch auf. Dies können Sie durch Erhöhen des Disk-Timeout-Wertes verhindern – die Host Utilities oder die VSC erledigen das automatisch.

Bei den Werkzeugen wird unterschieden, ob es sich dabei um Tools für ESX-Classic handelt oder um Software für ESXi. Die alte Version der Tools nennt sich *ESX Host Utilities* und muss in die Service Console des ESX Classic installiert werden. Die neue Variante nennt sich *Virtual Storage Console* (VSC) und wird auf einem Windows-Rechner installiert, der mit dem vCenter kommunizieren kann, oder eben direkt auf dem vCenter Server selbst. Für beide Varianten ist der Download der Software von *now.netapp.com* kostenlos, so Sie einen Login für diese Seite besitzen. Die Virtual Storage Console installiert aber auch andere Funktionen, die auf kostenpflichtige Features von NetApp zurückgreifen und extra Lizenzen benötigen. Damit sind

konkret das *Cloning Utility* und die Backup-Software *SnapManager for Virtual Infrastructure* gemeint.

Falls Sie noch ESX Classic in den Versionen 3.5, 4.0 oder 4.1 betreiben, können Sie die Host Utilities in Version 5.2.1 vom 21. März 2011 einsetzen. Haben Sie bereits auf ESXi oder betreiben vSphere 5, wo es bekanntlich ja nur ESXi gibt, steht Ihnen die Virtual Storage Console zur Verfügung. Sie brauchen für volle vSphere 5-Kompatibilität mindestens die Version 2.1.1.

Diese Utilities bzw. die VSC liefern Folgendes mit:

- optimierte Einstellungen für HBAs
- richtiges Setzen der Timeout-Werte für LUNs und NFS-Datastores
- richtige Timeouts für Gastbetriebssysteme
- Diagnosetools für HBAs, SAN-Switches und die NetApp
- Prüfen und Korrigieren von VMDK-Alignment-Fehlern (siehe Seite 554 unter der Überschrift, »Virtual Storage Console«)

NetApp Host Utilities

Aus Gründen der Rückwärtskompatibilität erklären wir hier noch, wie Sie die NetApp Host Utilities für ESX Classic installieren, obwohl davon auszugehen ist, dass Sie bereits ESXi betreiben. In diesem Fall überspringen Sie bitte diesen Abschnitt und lesen bei »Virtual Storage Console« weiter.

Damit der VMware-Betrieb im NetApp-Umfeld richtig funktioniert, ist es zwingend nötig, entweder alle empfohlenen Einstellungen durchzuführen oder die ESX Host Utilities (HU) zu installieren, sonst kommt es in einigen Fällen wie oben bereits erwähnt (z. B. Cluster-Takeover) zu Problemen, weil z. B. der ESX-Host seinen Datastore verliert. Die ESX Host Utilities installieren Sie in der Service Console. Die Host Utilities werden in Form eines TGZ-Paketes geliefert. Am einfachsten kopieren Sie das heruntergeladene Paket mit SCP in die Service Console. und installieren diese Tools nach dem Entpacken einfach mit dem Skript *./install* auf dem ESX-Host:

```
[root@esx ~]# tar xfz netapp_esx_host_utilities_5_2_1.tar.gz
[root@esx ~]# cd netapp_esx_host_utilities_5_2_1
[root@esx netapp_esx_host_utilities_5_2_1]# ./install
These tools require several ports to be open in the ESX firewall.
The following ports will need to be opened:
   20/tcp (incoming)
   21/tcp (outgoing)
   23/tcp (outgoing)
   80/tcp (incoming/outgoing)
   443/tcp (incoming)
Do you want to open the ports now (yes or no)?> yes
```

```
Installing VMware(R) ESX Host Utilities 5.1.......................
   Unpacking files to /opt/netapp/santools.................DONE
   Adding the ESX Host Utilities firewall rules............DONE
   Enabling the ESX Host Utilities firewall service........DONE
   Creating symbolic link for sanlun.......................DONE
   Creating symbolic link for config_nfs...................DONE
   Creating symbolic link for config_hba...................DONE
   Creating symbolic link for config_mpath.................DONE
   Creating symbolic links for MAN pages...................DONE
   Checking for installed HBAs.............................DONE
   Installing Emulex HBAAPI libraries.....................DONE
   Optimizing HBA settings.................................DONE
   Optimizing NFS Heartbeat settings.......................DONE
   Optimizing Preferred Paths.............................. DONE
```

Die Host Utilities sind nun installiert, Sie finden die Binaries unter */opt/netapp/santools*.

Die wichtigsten Tools für den Umgang mit Datastores und LUNs sind:

- `sanlun` (`sanlun lun show`)
  Zeigt eine Übersicht, welche LUNs von der NetApp welche Device-Namen auf dem ESX haben.
- `config_mpath` (`config_mpath -loadbalance -primary`)
  (Wird nur für ESX 3.5 gebraucht. Seit 4.0 gibt es ALUA, siehe oben.) Setzt die aktiven und passiven FCP-Pfade zur NetApp
- `config_hba` und `config_nfs`
  Setzen die Timeout- und Queue-Length-Variablen richtig.

Sind die Einstellungen für den ESX-Host nun korrekt ausgeführt, so müssen Sie auch noch zwingend *in jedem Gastsystem* den richtigen Wert für die Disk-Timeouts setzen. Dafür liefert NetApp ISO-Files mit, die Sie lediglich an die virtuellen Maschinen binden. Im Falle von Windows wird automatisch ein Registry-Key gesetzt, der den Disk-Timeout auf 190 Sekunden stellt; bei Linux passiert etwas Ähnliches, allerdings über `udev` und nicht über die Registry. Die GOS-ISO-Files werden bei der Host-Utilities-Installation unter */vmimages/gos_timeout-iso-images* abgelegt.

Die Werte können Sie auch manuell ohne Guest-OS-ISO setzen:

Windows:

Setzen Sie den folgenden Registry Key auf 190:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disk]
```

Linux:

Tragen Sie in die Datei */etc/udev/rules.d/z50_netapp.rules* folgende Zeile ein:

```
ACTION=="add", SUBSYSTEM=="scsi", SYSFS{type}=="0|7|14", RUN+="/bin/sh -c
'echo 190 > /sys/$$DEVPATH/timeout'"
```

ONTAP-Versionen vor 7.3 brauchen einen Timeout-Wert von 190 Sekunden, ab 7.3 reichen laut NetApp auch 130 Sekunden.

Virtual Storage Console

Die Virtual Storage Console (VSC) von NetApp ist ein Plugin für das ESX-vCenter bzw. für den vSphere-Client, das die Konfiguration und Prüfung der NetApp-Einstellungen für optimale Zusammenarbeit mit VMware erlaubt. Die VSC wird langfristig die Host Utilities ersetzen – momentan sind sie nur dann wirklich nötig, wenn Sie noch nicht auf ESXi setzen oder einen ESX-Host noch mit Version 3.5 betreiben; die aktuelle Version 4.0 der VSC unterstützt nur ESX und ESXi-Hosts ab Version 4.0.

Die VSC erfordert auf NetApp-Seite mindestens ONTAP-Version 7.3.1.1, für volle vSphere-Funktionalität mit VAAI-Integration ist aber mindestens ONTAP 8.0.1 nötig. Bei der Installation der VSC werden folgende Funktionen mit installiert:

- Monitoring and Host Configuration
  - Nachfolgeprodukt der Host Utilities
- Optimization and Migration
  - Ergänzung zu `mbrscan` und `mbralign`
  - Repariert Alignment-Probleme
- Provisioning and Cloning
  - Nachfolgeprodukt des Rapid Cloning Utilitys
  - erstellt Clones von VMs (z. B. für virtuelle Desktops) und erlaubt grafische Provisionierung von Datastores auf NetApp-Speicher vom vSphere-Client aus
- Backup/Recovery (optional)
  - Nachfolgeprodukt des SnapManagers for Virtual Infrastructure.; Ermöglicht schnelles, snapshot-basiertes Backup und Recovery von VMs

Wie Sie sehen, ist die VSC deutlich mehr als nur »Host Utilities für ESXi«. Die Auswahl des Installers sehen Sie in Abbildung 10.59.

Nach der sehr einfachen Installation durch Doppelklick auf die EXE-Datei und der Verbindung von der VSC zum vCenter (Abbildung 10.60) sehen Sie im vCenter-Client ein weiteres Konfigurationsfenster: Sie müssen noch die Login-Daten für das NetApp-Storagesystem eingeben (Abbildung 10.61). Es ist empfehlenswert, einen eigenen User mit eingeschränkten Permissions für die VSC anzulegen – mehr dazu finden Sie in der Betriebsanleitung der VSC.

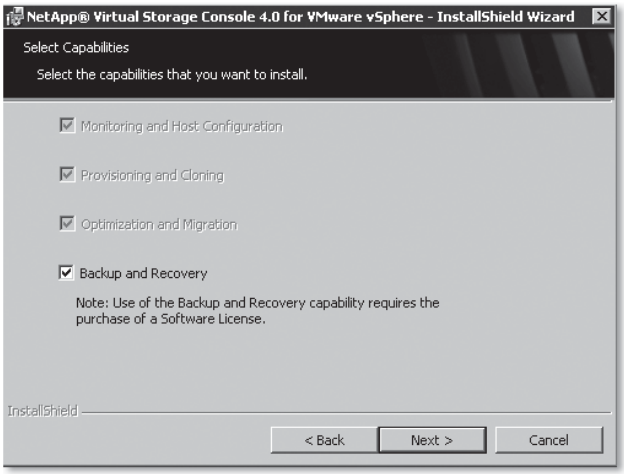


Abbildung 10.59 Die vier Teile der VSC

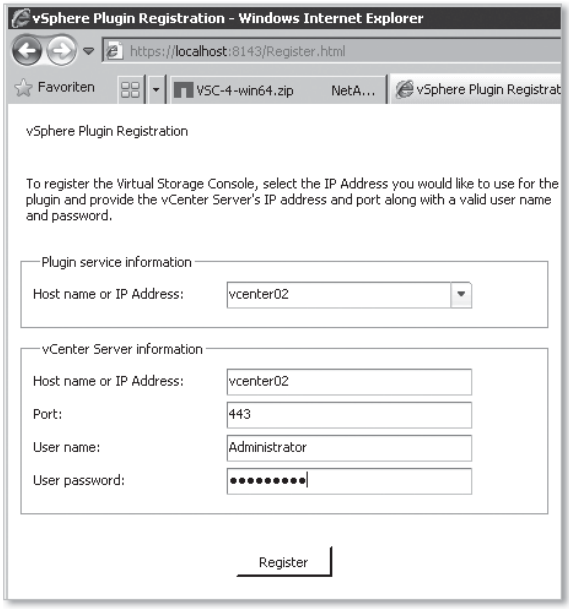


Abbildung 10.60 VSC wird am vCenter registriert.

Sofort nachdem Sie die Virtual Storage Console am vCenter registriert haben, tauchen auf allen verbundenen vSphere-Clients die neuen Funktionen und Schaltflächen der VSC auf, hauptsächlich sichtbar in der Menüleiste mit neuen Icons, im Bereich Applikationen und Lösungen sowie als NetApp-Reiterkärtchen ganz rechts im Bildschirm.

Zuerst müssen Sie der VSC mitteilen, welche NetApp-Systeme Sie verwalten möchten, und deren Zugangsdaten eingeben.

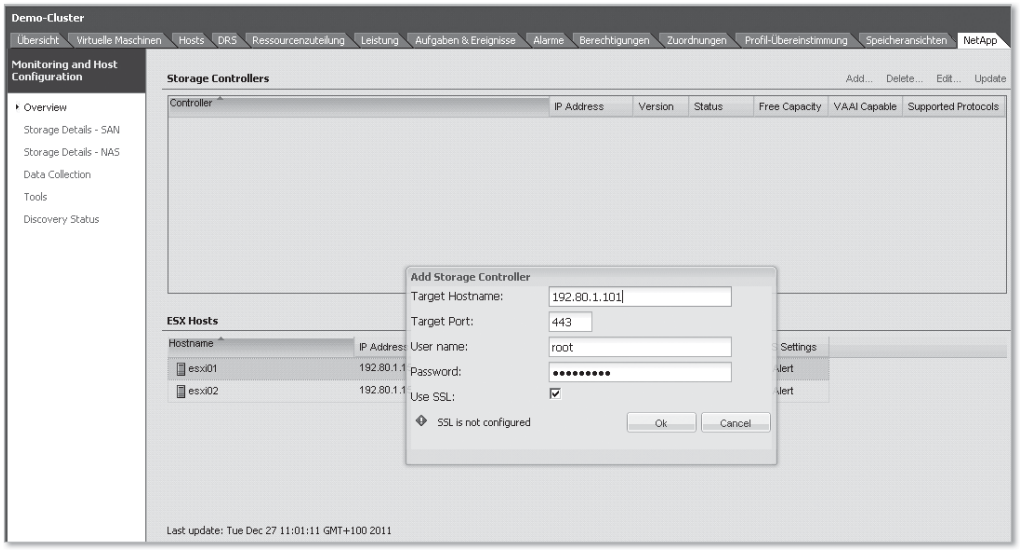


Abbildung 10.61 Hinzufügen von NetApp-Controllern

Anschließend erhalten Sie eine schöne Übersicht über die SAN-Komponenten (Abbildung 10.62).

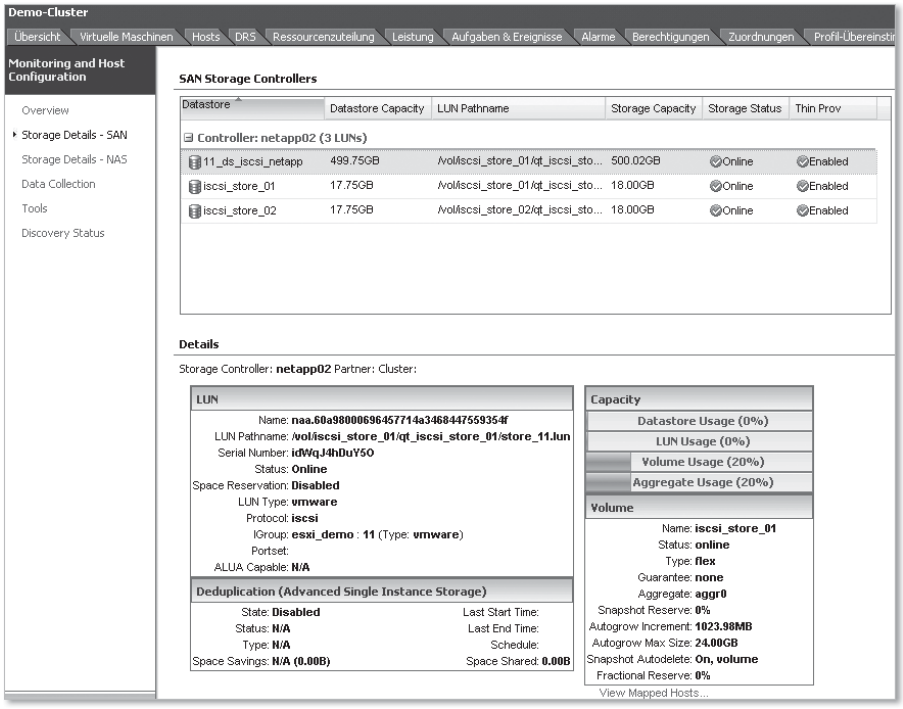


Abbildung 10.62 Ansicht des FCP-Datastores und einer freien LUN

Diese Übersicht gibt es auch für die NAS-Datastores, zu sehen in Abbildung 10.63.

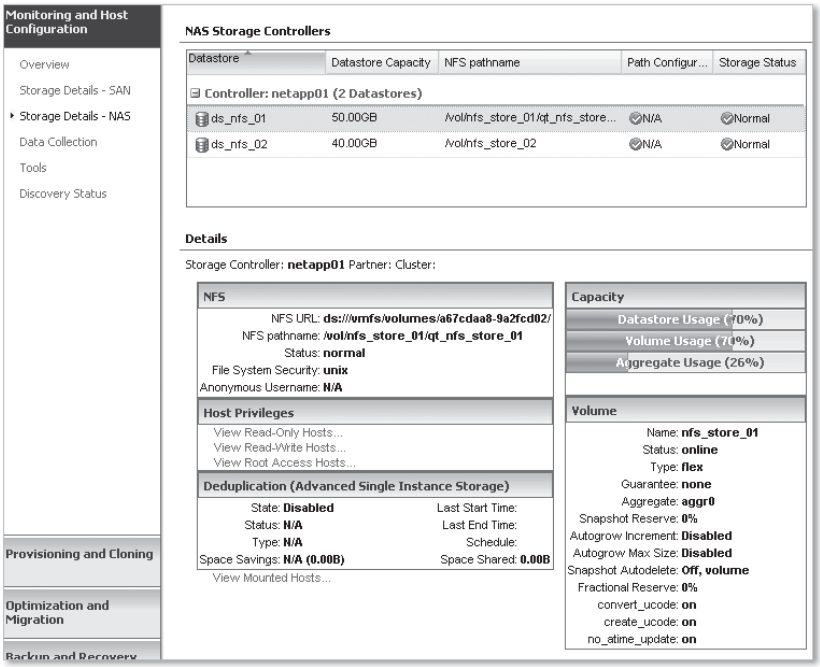


Abbildung 10.63 Ansicht eines NFS-Datastores

Die VSC erlaubt auch die Sammlung von Supportinformationen, ähnlich der Kommandos `switch_info`, `sanlun`, `esx_info` usw. aus den Host Utilities. Diese Log-Files können Sie dann im Supportfall an NetApp oder VMware hochladen (Abbildung 10.64).

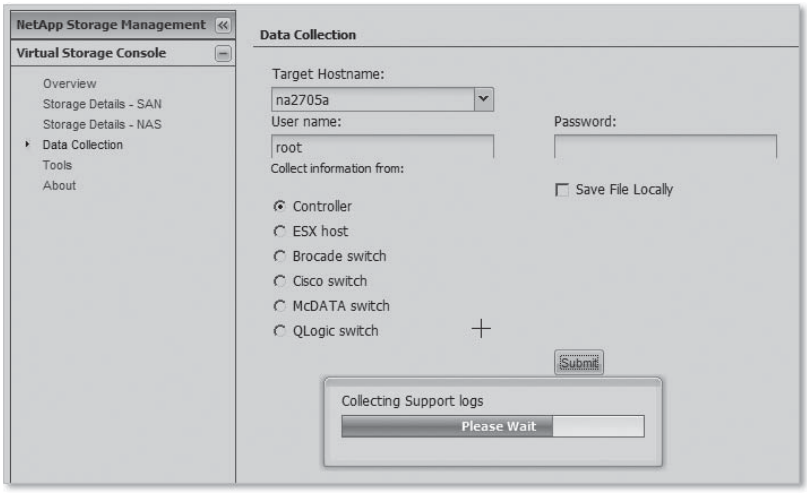


Abbildung 10.64 Informationssammler für Supportfälle

Neben den reinen Informationen lässt die VSC den Administrator auch per Klick die Best Practices wie Timeouts usw. anzeigen, kontrollieren und konfigurieren (Abbildung 10.65 und Abbildung 10.66).

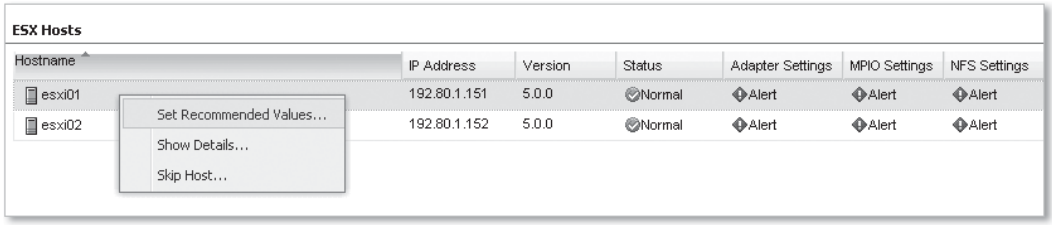


Abbildung 10.65 Matrix zur Prüfung der empfohlenen Einstellungen

Nachdem Sie die empfohlenen Parameter gesetzt haben, werden Sie gebeten, den Host neu zu starten – ohne Reboot greifen leider nicht alle eingestellten Werte.

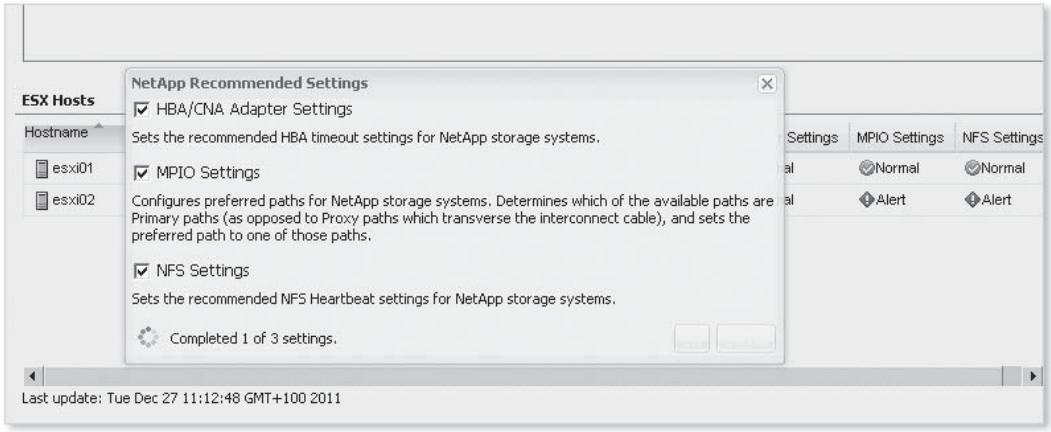


Abbildung 10.66 Automatische Konfiguration der empfohlenen Einstellungen

Genau wie auch die Host Utilities bringt die VSC die notwendigen ausführbaren Dateien wie `mbrscan` und `mbralign` mit, um die Alignment-Probleme von VMDK-Dateien zu reparieren. Auch die Timeout-Guest-OS-ISOs werden mitgeliefert (Abbildung 10.67).

Eine der wichtigeren Neuerungen der VSC sind die MBR-Tools für ESXi. Die herkömmlichen Varianten von *MBRScan* und *MBRAlign* aus den Host Utilities waren unter ESXi nämlich nicht lauffähig. Das bedeutete für den Administrator leider immer noch die Notwendigkeit, einen ESX-Classic-Host vorzuhalten, nur um die Alignments der VMDK-Datei korrigieren zu können. Ebenfalls neu ist das mitgelieferte ESXi-Plugin für VAAI-Unterstützung in Verbindung mit NFS und NetApp-Storage. Voraussetzung dafür ist Data ONTAP 8.1.1 im 7-Mode oder Data ONTAP 8.1.0 im Cluster-Mode. VMware liefert in vSphere 5 zwar die APIs für NAS-Plugins mit, die Plugins selbst müssen jedoch vom Hersteller bereitgestellt werden.

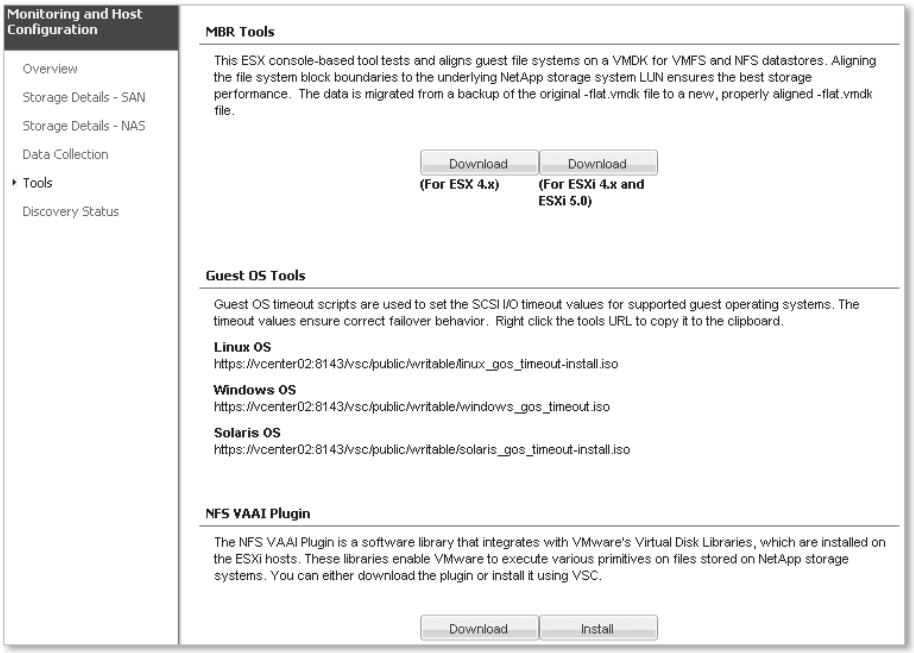


Abbildung 10.67 Download der mitgelieferten Tools

Die VAAI für NFS-Unterstützung liefert zwei neue Funktionen: Offloading von File-Clones und das Erstellen von Thick-VMDKs auf NFS. File-Clones sind der definitiv interessantere Aspekt, da NetApp seine Stärken hier voll ausspielen kann: Der FlexClone-Mechanismus (siehe »File-Clones und Sub-LUN-Cloning«, Seite 536) kann nun ganze VMDK-Dateien in Sekundenbruchteilen clonen – ein klassischer Kopierprozess entfällt. Besonders daran ist, dass Sie Ihr Arbeitsverhalten nicht mehr anpassen müssen, sondern einfach die normalen von VMware vorgegeben Menüpunkte zum Kopieren/Erstellen von virtuellen Maschinen verwenden. Die andere Funktion der NFS-VAAI-Plugins, die Thick-Files auf NFS, sind für einen speziellen Anwendungsfall gedacht: Kunden, die NFS-Speicher verwenden, aber eben kein Thin Provisioning einsetzen wollen, mussten bisher bei der Erstellung von VMDK-Dateien immer manuell eingreifen, um thick-provisioned VMDKs zu erhalten – per Default sind VMDK-Dateien auf NFS ja immer »dünn«.

Fazit: Die VSC ist ein würdiger Nachfolger der ESX Host Utilities; besonders positiv hervorzuheben ist die Übersichtlichkeit bei der Prüfung, ob die korrekten Werte eingestellt sind. Wichtig ist auch der neue Support von ESXi – bisher mussten die Kunden mit ESXi aufgrund des fehlenden Supports der Host Utilities alle Einstellungen manuell durchführen.

Die Backup- und Recovery-Funktionalität der VSC erklären wir in Abschnitt 14.1.4, »Backup von vSphere-Umgebungen mit NetApp-Storage«, noch ausführlicher; Informationen zur Funktion für die Korrektur des Misalignments erhalten Sie gleich im nächsten Abschnitt.

Alignment-Probleme: LUNs, VMFS, NFS und VMDK-Dateien

Bei Misalignment-Problemen handelt es sich um einen Hauptverursacher von Schwierigkeiten mit Storage-Performance. Gleichzeitig ist vielen Administratoren dieses Problem nicht bekannt, oder es wird bewusst ignoriert oder heruntergespielt. Vermeintlich existiert nämlich kein Problem, augenscheinlich funktioniert ja alles. Doch der Schein trügt: Alignment-Probleme führen oft zu stufenweisen Einbrüchen in der Performance. Das heißt, in der Praxis ist bis zu einer gewissen Anzahl an VMs alles in Ordnung, das Erstellen einer einzigen zusätzlichen VM lässt die Geschwindigkeit des Speichersystems jedoch stark absinken.

Ich möchte Sie an dieser Stelle ausdrücklich warnen: Nehmen Sie dieses Problem nicht auf die leichte Schulter!

Um die beste Performance für VMs auf einer NetApp zu erreichen, ist es notwendig, dass die File-System-Blöcke innerhalb eines Guest-OS direkt korrekt an den Blockgrenzen des NetApp-Speichersystems ausgerichtet (englisch: *alignment*) sind.

Typischerweise sind in einer vSphere-Umgebung mehrere verschiedene Schichten im Speicherumfeld vorhanden; wir betrachten die Schichten von der untersten bis zur obersten:

- NetApp-WAFL-File-System und die darin liegenden LUNs
- VMFS auf der LUN
- VMDK-Datei mit Partitionierung und File-System des Gast-OS

Durch diese verschiedenen involvierten Schichten kommt es zu einem unschönen Effekt: Jede Schicht bringt eigene Partitionstabellen mit, die den Anfang der Partition so verschieben, dass die Grenzen nicht mehr korrekt aneinander ausgerichtet sind, wie Abbildung 10.68 zeigt.

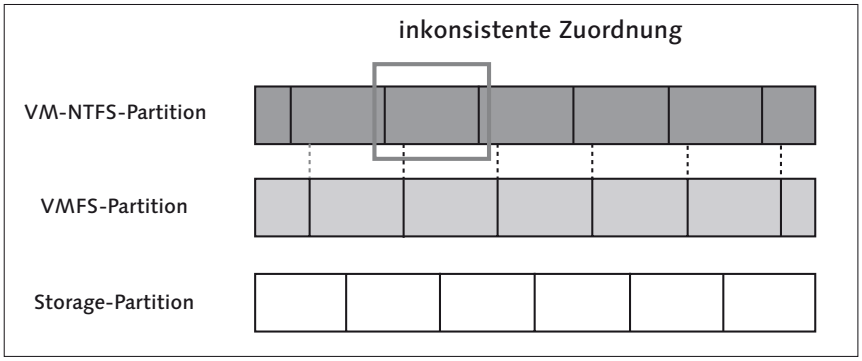


Abbildung 10.68 Inkonsistente Partitionsausrichtung

So kann es dazu kommen, dass ein Schreib- oder Lesezugriff auf einen Block im Guest-OS zu zwei oder gar drei Zugriffen auf dem NetApp-System führt. Das wirkt sich negativ auf die Antwortzeit und die Last des Speichersystems aus, die Performance der virtuellen Maschine verschlechtert sich.

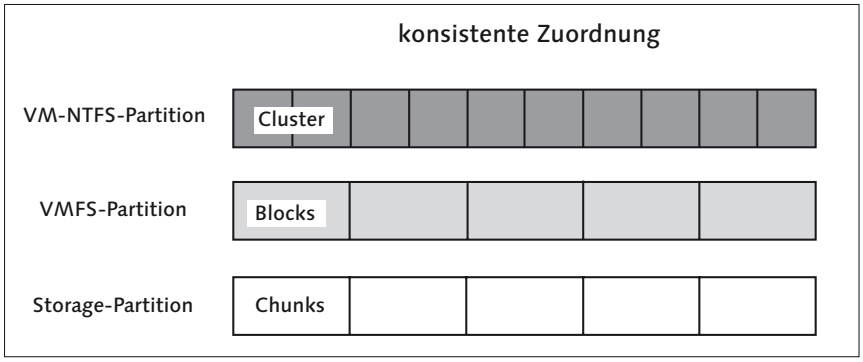


Abbildung 10.69 Konsistentes Partition-Alignment

Der eigentliche Haken am Thema Ausrichtung (*Alignment*) ist, dass die Defaulteinstellungen der Partitionierungstools `fdisk` (Linux) und `diskpart` (Windows) sowie die *vmkfstools* von VMware dieses Problem hervorrufen. Oder anders ausgedrückt: Die Defaulteinstellungen führen leider zum falschen Ergebnis.

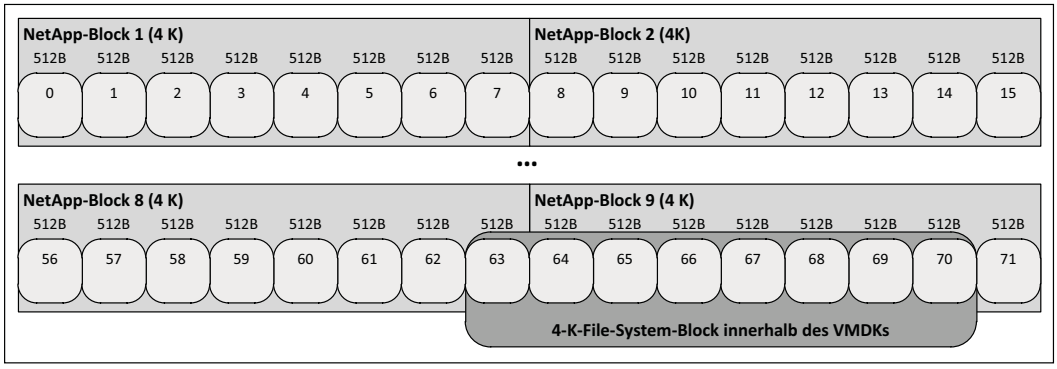


Abbildung 10.70 Misalignment, hier typisch an der LBA63-Grenze

Dieses allgemeine Problem tritt bei jedem Speicherhersteller auf; NetApp liefert aber zum Glück Lösungen, um die Alignment-Probleme zwischen allen Schichten zu korrigieren.

Allgemein kann gesagt werden, dass jene Betriebssysteme von dieser Problematik betroffen sind, die den Anfangssektor ihrer Partition nicht auf eine 4-K-Blockgrenze legen.

- Betroffen sind:Windows 95, 98, ME, Windows NT, 2000, 2003.
- Nicht betroffen sind:Windows Vista, 7, 2008.

Bei Linux sind so gut wie alle Varianten betroffen, mit Ausnahme derer, die schon auf das neue *fdisk* (mind. Version 2.17.1) setzen, wie zum Beispiel Ubuntu Linux ab Version 10.04 oder Red Hat Enterprise ab Version 6.

Aktuell zeichnet sich am Markt ab, dass die meisten OS-Hersteller (egal ob Linux oder Windows) sich auf ein Standard-Offset für den Partitionsbeginn von 1 Megabyte festlegen. Dieser Wert hat den Vorteil, dass er für fast alle Speichersysteme universell funktioniert und nirgendwo zu Alignment-Problemen führt. Schließlich lässt sich 1 Megabyte rund durch alle möglichen Blockgrößen (512, 1 K, 2 K, 4 K, 8 K) oder durch alle gängigen RAID-Stripeset-Größen (4 K, 8 K, 16 K, 32 K, 64 K, 128 K) teilen.

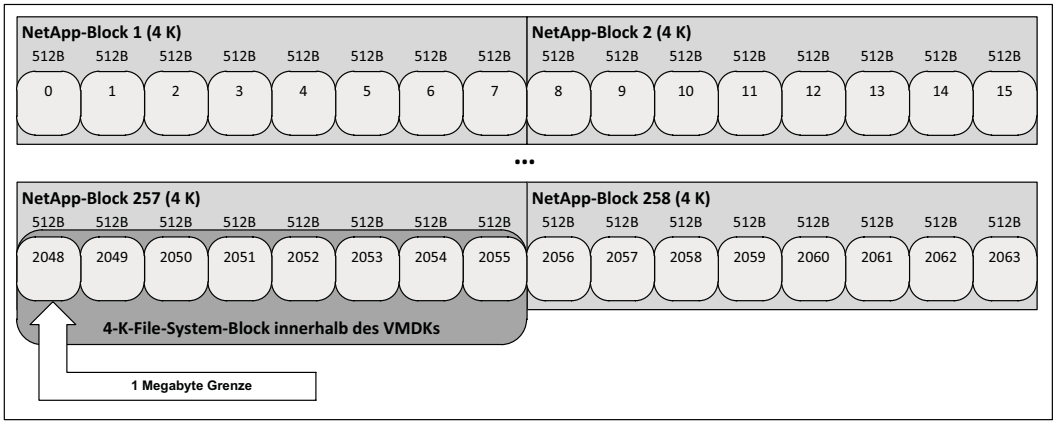


Abbildung 10.71 Korrektes Alignment, hier an der 1-MB-Grenze

LUN-Alignment korrigieren

Zuerst muss die Beziehung zwischen den LUN und dem VMFS betrachtet werden. Um die VMFS-Partition automatisch korrekt an der NetApp-Blockgrenze der LUN und des WAFL-Dateisystems auszurichten, ist nur sehr wenig Aufwand nötig. Im Prinzip erledigt NetApp die gesamte Arbeit für uns, vorausgesetzt, dass Sie beim Erstellen der LUN den richtigen LUN-Typ auswählen.

```
na3021> lun create -s 200g -t vmware ......
na3021> lun show -v
 /vol/esxfcp/fcp_ds01.lun     200g (r/w, online, mapped)
                Serial#: P3HwDJT0HNed
                Share: none
                Space Reservation: disabled
                Multiprotocol Type: vmware
                Maps: esx_fcp_all=1
```

Der `Multiprotocol Type` steht auf `vmware`, das heißt, NetApp rechnet einfach den entsprechenden Partition-Offset des VMFS-3-Dateisystems dazu, somit ist die Blockgrenze des VMFS-3 identisch mit der der NetApp-LUN. Bei NFS-Datastores ist ein LUN-Alignment nicht notwendig, schließlich gibt es in diesem Zusammenhang keine LUNs. Auf die korrekte Ausrichtung der VMDK-Dateien müssen Sie jedoch trotzdem achten, wie wir gleich im Anschluss erklären.

VMDK-Alignment korrigieren

Anschließend müssen Sie noch die Ausrichtung der Dateisystemblöcke innerhalb des VMDK-Disk-Files korrigieren, was sich leider als etwas aufwendiger erweist, da dieses Alignment direkt vom Gastbetriebssystem abhängt. Jedes Gastbetriebssystem hat eigene Partitionen, daher sind Sie auf die verschiedenen Partitionierungstools angewiesen.

Die generelle Regel ist: NetApp hat eine Blockgröße von 4 K (4.096 Bytes), also muss die Partition auch an einer 4-K-Grenze beginnen. Entweder legen Sie vor der Installation des Gastbetriebssystems manuell eine korrekt ausgerichtete Partition an (und erstellen darauf ein sauberes VM-Template), oder Sie korrigieren das Problem später mit dem Tool `mbralign` von NetApp aus den Host Utilities bzw. der Virtual Storage Console.

Möglichkeit 1: Manuelle Partitionierung

Windows-Partitionen haben per Default einen Partition-Offset von 32.256 Bytes (LBA 63), das wird sehr schön unter *msinfo32.exe* sichtbar (Abbildung 10.72).

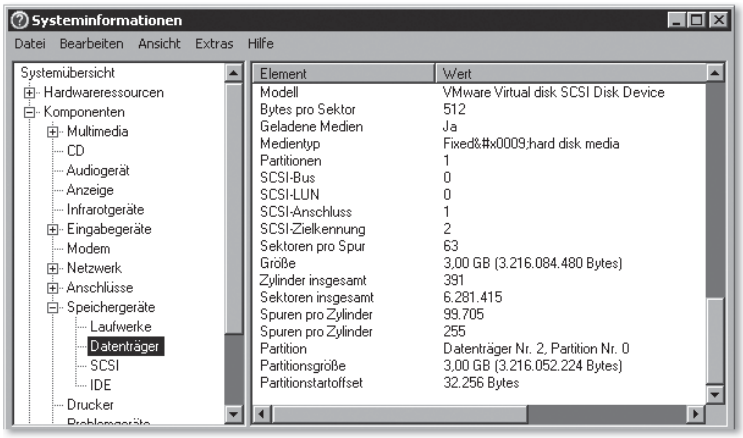


Abbildung 10.72 MSInfo32 zeigt den Partitionstartoffset an, der Maßgabe für die Alignment-Prüfung ist.

Allerdings ist 32.256 kein volles Vielfaches von 4.096, also stimmt das Alignment nicht. Die Lösung ist, eine leere virtuelle Festplatte an eine vorhandene VM anzuhängen und manuell mit *diskpart.exe* eine Partition anzulegen. Diese Festplatte hängen Sie anschließend an eine neue VM an und installieren darin dann Windows (Abbildung 10.73).

Das Ergebnis in *msinfo32.exe* zeigt danach, dass die Partition jetzt richtig ausgerichtet ist, da der neue Offset mit 32.768 Bytes durch 4.096 teilbar ist. Unter Linux müssen Sie die Partition in der VM auf einer leeren Disk mit dem Befehl `fdisk /dev/sda` anlegen (Abbildung 10.74).

Nachdem Sie wie im Screenshot dargestellt eine neue Partition mit [N] angelegt und die gesamte Platte ausgewählt haben, ändern Sie anschließend im Experten-Modus [X] den Beginn der Partition [B], und zwar auch wieder auf einen durch 4 .096 teilbaren Wert, z. B. 64 K; das Ergebnis sollte dann aussehen wie in (Abbildung 10.75).

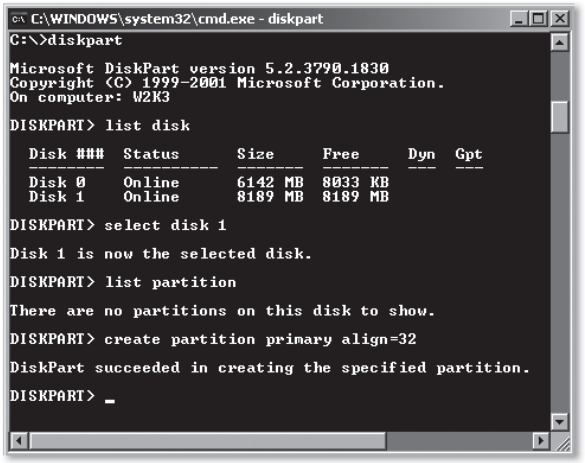


Abbildung 10.73 Erstellen einer richtig ausgerichteten Partition mit »diskpart«

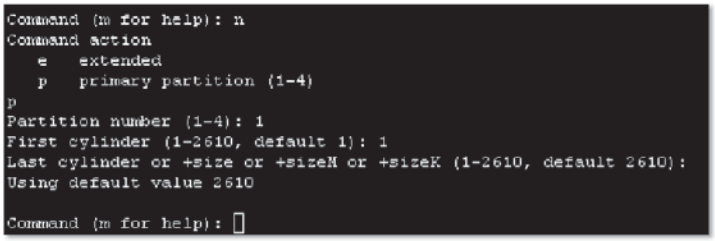


Abbildung 10.74 Partition mit »fdisk« unter Linux anlegen

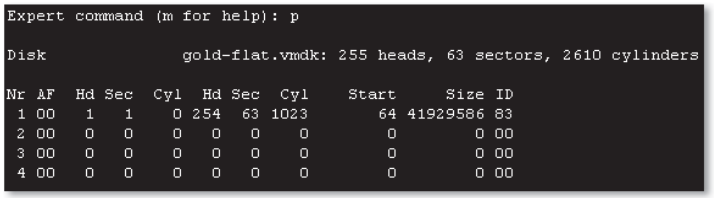


Abbildung 10.75 Mit »fdisk« unter Linux die Partition prüfen

Egal, ob Sie eine sauber ausgerichtete Linux- oder Windows-Platte angelegt haben, das Ergebnis sollten Sie auf jeden Fall nach der Betriebssysteminstallation als VM-Template festhalten, damit Sie diese Arbeit nicht für jede neue VM erledigen müssen.

Möglichkeit 2: Reparatur mit NetApp Tools

Für Administratoren, die mit richtigem Alignment bisher noch nicht allzu vertraut sind, gibt es auch eine Abhilfe: Die beiden kleinen Programme `mbrscan` und `mbralign` aus den Host Utilities oder der VSC von NetApp können falsch ausgerichtete VMDK-Dateien aufspüren und reparieren.

Die beiden Tools werden beim ESX Classic nach */opt/netapp/santools/* installiert, auf dem ESXi landen sie in */opt/ontap/*. Zuerst starten Sie das Programm `mbrscan` auf das entsprechende -FLAT.VMDK-File:

```
# /opt/netapp/santools/mbrscan OK-fcp-w2k3-1-flat.vmdk
--------------------
OK-fcp-w2k3-1-flat.vmdk p1 (NTFS) lba:63  offset:32256  aligned:No
--------------------
```

Sie können auch einen Massenlauf mit einfachen Shell-Wildcards auf sämtliche VMs im Datastore anstoßen, um einen schnellen Gesamtüberblick zu erhalten:

```
# /opt/netapp/santools/mbrscan /vmfs/volume/fcp_datastore1/*/*-flat.vmdk
```

Wichtig!

Um die betroffenen VMDK-Dateien zu reparieren, müssen Sie die VM ausschalten. Außerdem darf die VM keine Snapshots oder Linked Clones besitzen!

Anschließend starten Sie den Befehl `mbralign` auf die VMDK-Datei (**nicht** die -FLAT.VMDK-Datei):

```
# /opt/netapp/santools/mbralign OK-fcp-w2k3-1.vmdk
Part  Type  old LBA  New Start LBA  New End   LBA Length in KB
P1    07    63       64             12562831  6281383
Creating a backup of OK-fcp-w2k3-1.vmdk
Creating a backup of ./OK-fcp-w2k3-1-flat.vmdk
Creating a copy the Master Boot Record
Working on partition P1 (3): Starting to migrate blocks from 32256
to 32768.
12801 read ops in 1 sec.  99.29% read (99.31 mB/s).
  99.29% written (99.31 mB/s)
Working on space not in any partition: Starting to migrate blocks.
100.00 percent complete.  100.00 percent written.
Making adjustments to ./OK-fcp-w2k3-1-flat.vmdk.
Adjusting the descriptor file.
```

Das Tool erstellt zunächst ein Backup der Originaldatei und legt dann eine neue, konsistent zugeordnete VMDK-Festplattendatei an und kopiert die Blöcke aus dem Original in die neue Datei.

Dabei ist neben dem Aspekt der Plattenplatzbelegung (Aufräumen nicht vergessen!) zu beachten, dass nach der Reparatur eventuell der Bootloader der VM nicht mehr funktioniert; besonders Linux-VMs sind betroffen, Windows-VMs weniger. Die Abhilfe für einen kaputten Bootloader ist sehr einfach: Booten Sie eine Recovery-DVD, z. B. Knoppix oder die Distributions-CD, und schreiben Sie den Bootloader bzw. den Bootrecord neu. Im Falle von GRUB starten Sie nach dem Boot von der Rescue-CD den Befehl `grub`:

```
grub> root hd(0,0)
grub> setup (hd0)
grub> quit
```

Danach sollte die Linux-VM wieder problemlos booten.

Möglichkeit 3: Keine Reparatur, nur Workaround

Die VSC enthält seit Version 4 ein sehr raffiniertes Werkzeug namens *iAlign*, das das Alignment-Problem durch einen Workaround löst. Dieses Tool kann das Problem nicht nur im laufenden Betrieb erkennen (`mbrscan` hingegen erfordert Downtime der VM!), sondern den Workaround sogar ohne Downtime der VM schaffen. Die Funktionsweise ist relativ einfach erklärt: Anstatt die falsch ausgerichteten VMDK-Dateien zu reparieren, werden sie einfach per Storage vMotion auf einen speziell manipulierten Datastore umgezogen. Dieser spezielle Datastore liegt auf einer NetApp-LUN, die absichtlich ein falsches LUN-Offset besitzt – und zwar um genau so viele Blöcke falsch, wie die entsprechenden VMDK-Dateien falsch alignt sind – nur in die andere Richtung verschoben. So wird der Fehler innerhalb der VMDK-Datei durch einen zweiten – absichtlichen – Fehler in der VMFS-LUN wieder korrigiert.

Sie finden dieses neue Feature im Bereich Optimiziation und Migration der VSC. Zuerst müssen Sie alle Datastores »scannen«, Sie können neben einem manuellen Scan auch regelmäßig per Scheduler nach Fehlern suchen lassen.

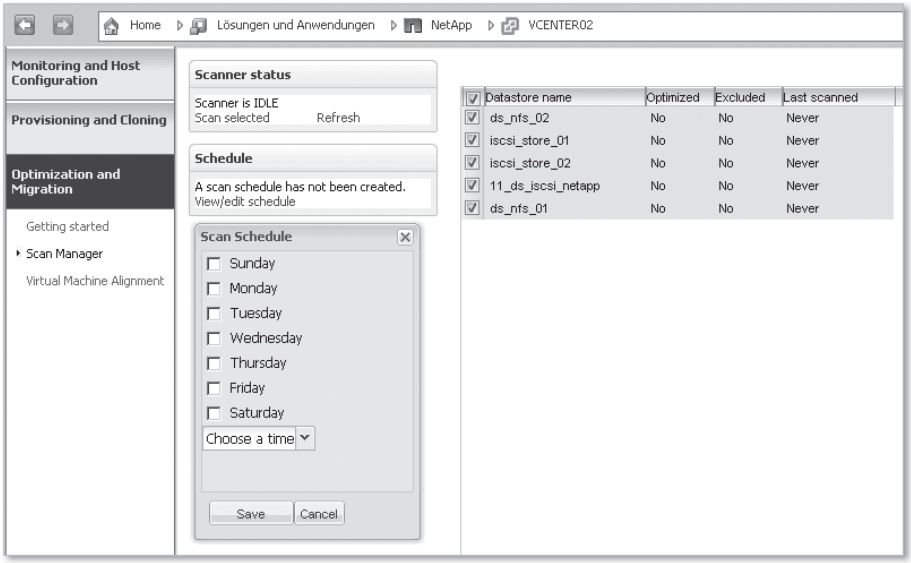


Abbildung 10.76 Scan nach misalignten VMs oder Datastores

Anschließend können Sie von der VSC ein oder mehrere manipulierte Datastores anlegen lassen und dann die betroffenen VMDK-Dateien dorthin per svMotion migrieren lassen. Die VMs tauchen dann im Ordner *Functionally aligned* auf.

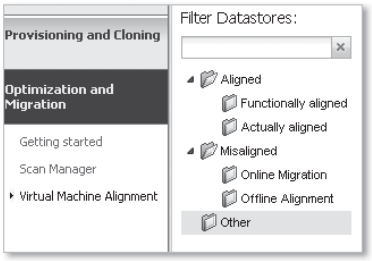


Abbildung 10.77 Einordnung der migrierten VMs mit Workaround

Auch wenn diese speziellen Datastores nicht für »normale« VMs gedacht sind, ist es an manchen Stellen nicht möglich, sich gegen andere Automatismen wie Storage DRS zu schützen, es sei denn, Sie deaktivieren diese Features für die betroffenen VMs.

Der Ansatz »doppelt falsch ist wieder richtig« ist aktuell sehr innovativ und wirklich noch einzigartig; ob er sich aber langfristig durchsetzen wird, ist aus zwei Gründen fraglich: Erstens ist es immer besser, ein Problem zu lösen, als nur einen Workaround zu schaffen. Zweitens wird das Problem des Misalignments langfristig verschwinden, weil alle modernen Betriebsysteme diese Problematik durch richtige Partitionierung vermeiden.

Generelle Empfehlung zum Umgang mit Misalignment

- **Empfehlung 1: Vermeiden Sie das Problem.**
  Versuchen Sie, die potentiellen Probleme mit Misalignment einfach zu vermeiden, indem Sie auf aktuelle Betriebssystemversionen setzen, die ihre Partitionen automatisch an richtigen Blockgrenzen erstellen. Beispielsweise spricht wahrscheinlich nicht viel dagegen, dass Sie für den neu angedachten Server-Dienst ein Windows 2008 verwenden statt ein Windows 2003. Außerdem ist der Umstieg auf Virtualisierung bei einigen Servern eine gute Gelegenheit, den schon zu lange vor sich hergeschobenen Aufräumjob anzugehen. Sie sollten vor einem P2V-Prozess nachdenken, ob Sie nicht viel besser den Server einfach als virtuelle Maschine frisch installieren und nur die Daten dorthin übernehmen. Frische VMs sind schlanker und dadurch schneller. Des Weiteren können Sie für verschiedene Dienste auch gleich mehrere VMs einrichten und dadurch Dienste voneinander trennen, die früher auf demselben Server liefen.
- **Empfehlung 2: Machen Sie es von Anfang an richtig!**
  Am besten bauen Sie sich sauber alignte Templates für alle zukünftigen VMs. Das sorgt dafür, dass nur noch richtig konfigurierte Partitionen existieren, selbst wenn andere Administratoren mit vSphere arbeiten, die nichts von Partition-Alignment wissen. Außerdem sorgen konsistent ausgerichtete VMs für einen wesentlich besseren Deduplizierungsgrad auf dem Speichersystem.
- **Empfehlung 3: Aufräumen**
  Korrigieren Sie die Fehler, wenn möglich. Beginnen Sie, um eine schnelle Schadensbegrenzung zu schaffen, mit jenen VMs, die am meisten unalignten I/O produzieren. Die restli-

chen VMs, die wenig Last auf dem Datastore erzeugen, können Sie dann später bei einer guten Gelegenheit (z. B. einer Downtime) reparieren. Falls Downtimes für *MBRAlign* komplett ausgeschlossen sind, so können Sie immer noch die »Workaround«-Methode der VSC mit *iAlign* wählen.

- **Empfehlung 4: Aufklärung**
  Erzählen Sie Ihren Kollegen von Misalignment und was man dagegen tun kann. Nur durch ausreichende Aufklärung wird das Problem langfristig verschwinden. Jeder Administrator sollte sich dessen bewusst sein. Als kleines Beispiel aus der Praxis möchte ich noch folgende Geschichte erzählen: Ein Administrator setzte alle Empfehlungen um, seine gesamte vSphere-Umgebung war sauber, es gab keinerlei Fälle von Misalignment mehr. Nach einigen Monaten bekam er von NetApp im Storage-Audit die Nachricht, dass er starkes Misalignment auf seinen VMware-LUNs hätte. Ungläubig untersuchte er die Situation und musste zugeben: NetApp hatte recht! Das Problem war mit Hilfe von mbrscan schnell gefunden: Im Laufe der Zeit hatten seine Kollegen immer mehr neue VMDK-Dateien erstellt, um diese als »Daten-Laufwerk« für ihre virtuellen Datenbank-Server zu verwenden. Dieses Laufwerk mit dem Buchstaben »D« wurde aber mit Standardeinstellungen von Windows 2003 partitioniert und war dadurch nicht richtig an der 4-K-Blockgrenze ausgerichtet. Hätte er vorher stolz von seinen erfolgreichen Alignment-Taktiken erzählt und seine Kollegen so auf die mögliche Problematik aufmerksam gemacht, so wäre es nie zu dem Problem gekommen.

Nach den theoretischen Grundlagen aus Kapitel 10 soll das Buch auch eine praktische Anleitung anhand echter Beispiele liefern. An dieser Stelle erhalten Sie neben den eigentlichen Erläuterungen für die Umsetzung der verschiedenen Speicheranbindungen von vSphere auch nützliche Tuning- und Optimierungstipps zu EMC-VNX-Speichersystemen.

11 Storage-Konfiguration des EMC-VNX-Speichersystems unter vSphere 5

Autor dieses Kapitels ist Marcel Brunner, EMC vSpecialist, zuständig für Global Accounts & Alliances EMEA, marcel.brunner@emc.com, Blog: cloujockey.me

Mit dem Erscheinen der vorliegenden Auflage werden erstmalig auch EMC²- Speichersysteme berücksichtigt. Die Lektüre des Kapitels 9, »Storage-Architektur«, ist empfohlen, da diese Konzepte aufzeigen, die auch für den Betrieb von EMC-Speichertechnologien Gültigkeit haben. Beispiele hierfür sind das grundsätzliche Verständnis zum Umgang mit den Speichermöglichkeiten und -eigenschaften von vSphere, die redundante Anbindung der Speichernetzwerke etc. EMC selbst bietet eine Vielzahl von Primärspeichersystemen an:

- EMC Atmos – objektbasiertes Speichersystem basierend auf einer Grid-Architektur, das Daten als Objekte darstellt und nach definierten Richtlinien speichert und verwaltet
- EMC Isilon – Scale-out-NAS-System mit der Skalierbarkeit eines einzigen Dateisystems von über zehn Petabytes basierend auf einer Grid-Architektur
- EMC Symmetrix VMAX und VMAXe – High-End-Speichersysteme basierend auf einer Director-Architektur namens Virtual Matrix Architecture
- EMC VNX und VNXe – Mid-Range-Speichersysteme, wobei die Konfiguration einer VNX Inhalt dieses Kapitels ist
- EMC VPLEX – Virtualisierungslösung für heterogene Speicherlandschaften basierend auf einer Scale-out-Cluster-Architektur für einen lokalen oder geografisch unabhängigen aktiven Zugriff auf dieselben Datenbestände

11.1 Einführung

Die VNX-Produktreihe eignet sich für alle Unternehmen und zeichnet sich als eine skalierbare und anwenderfreundliche Lösung zur Block-, Datei- und Objektspeicherung aus. Das System verfügt über zwei Storage-Processors für die Anbindung der Blockspeicherprotokolle Fibre-

Channel, FCoE und iSCSI. Zur dateibasierten Speicherung stehen ein bis maximal acht X-Blades zur Verfügung, die über 1- oder 10-Gigabit-Ethernet Zugriff via CIFS oder NFS ermöglichen. Mit dem Zusatz EMC Atmos Virtual Edition können Applikationen direkt via Atmos API oder REST-Protokoll auf das Speichersystem zugreifen.

Das System bietet seine umfangreiche Funktionalität in Form von insgesamt fünf Software-Suites an:

- FAST Suite – automatische Optimierung der Systemperformance beim Datenzugriff; bedingt den Einsatz unterschiedlicher Festplattentechnologien.
- Security and Compliance Suite – bietet Schutz der Daten vor Veränderung, Löschung und schädlichen Aktivitäten.
- Local Protection Suite – ermöglicht mit kontinuierlichen, abhängigen und unabhängigen Kopien (Continuous Data Protection, Snapshots und Clones) den lokalen Schutz von Daten.
- Remote Protection Suite – bietet RPO-basierten Datenschutz mittels kontinuierlicher, synchroner oder asynchroner Replikation (die zeitliche Einstellung bestimmt den maximal tolerierbaren Datenverlust von 0 Sekunden bis 24 Stunden).
- Application Protection Suite – ermöglicht applikations- oder VMware-VMFS-konsistente Sicherung Ihrer kritischen Applikationen oder der gesamtem VMware-Umgebung.

Sie erfahren in diesem Kapitel, wie Sie ein VNX-Speichersystem erfolgreich für den Betrieb von Cloud- und vSphere-basierten virtuellen Infrastrukturen in Ihrem Unternehmen einführen.

11.2 Planung und Konfiguration eines VNX-Systems

Die richtige Planung und Konfiguration einer VNX ist wichtig für den performanten Betrieb einer virtuellen Umgebung. Der folgende Abschnitt soll die Grundlagen vermitteln, um das Speichersystem optimal zu nutzen.

Grundsätzliches zu Soft- und Firmware-Versionen

Die in diesem Kapitel vorgestellten Eigenschaften der verwendeten Produkte beziehen sich auf folgende Release-Stände:

- VNX OE Block 31.5
- VNX OE File 7.0.40
- vSphere 5.0
- RM 5.4.1

Neuere Releases können Erweiterungen und Änderungen mit sich bringen, die in diesem Kapitel getroffene Aussagen überholt erscheinen lassen.

ESXi und VNX-Speichersysteme unterstützen die Protokolle FC, FCoE, iSCSI und NFS. Die VNX unterstützt im Weiteren CIFS für die Bereitstellung von Netzwerkverzeichnissen von virtuellen Maschinen mit Windows als Betriebssystem.

Konnektivität verschiedener Block-Technologien

ESXi und VNX unterstützen derzeit den Zugriff auf SCSI-Geräte mit einem SCSI-Transport-Typ. Das heißt, dass auf eine LUN über jeweils ein Protokoll zugegriffen wird. Es ist nicht möglich, dieselbe LUN mit iSCSI und gleichzeitig mit FC oder FCoE anzusprechen. Selbstverständlich unterstützen sowohl ESXi als auch VNX den Parallelbetrieb mehrerer Protokolle auf demselben Host bzw. Speichersystem.

Ein VNX-System bietet drei Möglichkeiten, Speicherkapazität zu konfigurieren und bereitzustellen:

- EMC Unisphere – eine web-basierte, zentrale und grafisch-unterstützte Oberfläche zum Verwalten mehrerer VNX-Speichersysteme
- Command Line Interface – skriptfähige, text-basierte Schnittstelle zur Verwaltung eines Systems
- EMC Virtual Storage Integrator – frei verfügbare Plugin-Suite für VMware vCenter (Version 4 und 5) zur Ansicht, Erstellung und Manipulation von Datastores und den VMDK-Dateien virtueller Maschinen

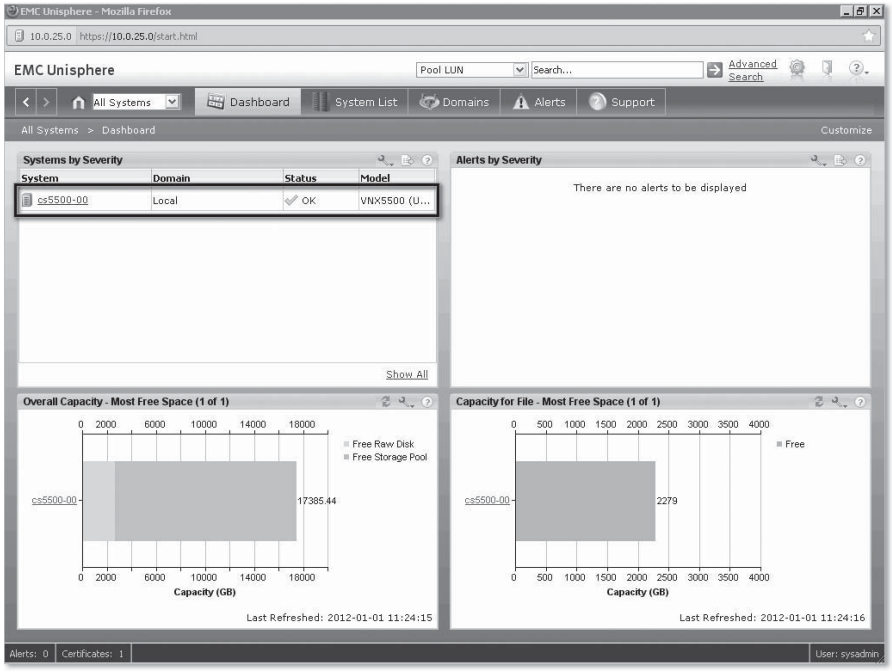


Abbildung 11.1 Dashboard-Ansicht von Unisphere

11.2.1 Einleitung zu VNX-blockbasierten Speicheroptionen

Festplattentypen

Ein VNX-System unterscheidet drei Festplattentypen, die im selben System betrieben werden können und sich durch unterschiedliche Eigenschaften auszeichnen (Tabelle 11.1).

Typ	Einsatzgebiet
Flash-Festplatten (SSD)	Applikationen mit Anforderungen zu niedrigen Antwortzeiten, beispielsweise Logs von Datenbanken oder VMware View Desktops
Serial Attached SCSI (SAS)	geschäftskritische, virtualisierte Applikationen mit hohen Performance- und Kapazitätsanforderungen, beispielsweise Microsoft Exchange
Nearline SAS	virtualisierte Applikationen mit einem Anforderungsprofil von geringem Durchsatz und mittlerer Zugriffszeit, beispielsweise Infrastrukturdienstleistungen wie DNS, AD; aber auch mit hohen Anforderungen an Kapazität wie VM-Templates, ISO-Images und Backups oder unveränderliche Daten

Tabelle 11.1 Festplattentypen

Jede Festplatte kann Teil einer RAID-Gruppe oder eines Pools sein sowie als Hot Spare eingesetzt werden.

VNX-Speichergruppen

VNX unterscheidet zwei Arten der Gruppierung von Festplatten: RAID-Groups und Storage-Pools. Sie bekleiden unterschiedliche Funktionen. Wichtige Eigenschaften einer RAID-Group sind, dass sie über ein fixes Reservationsmodell verfügt und einen einzigen LUN-Typ unterstützt, der die ganze bei seiner Erstellung zugewiesene verfügbare Kapazität allokiert. Gegenüber RAID-Groups präsentieren sich Storage-Pools flexibler und dynamischer. Deren LUN-Typen können thin oder thick sein. Eine LUN eines Storage-Pools wird segmentiert in 1-GB-Slices erstellt.

Speichergruppen

VNX unterstützt grundsätzlich den gleichzeitigen Betrieb von mehreren RAID-Levels (0,1, 1/0, 3, 5 und 6). Nur ein RAID-Level kann bei der Erstellung einer RAID-Group oder eines Storage-Pools eingestellt werden. RAID-Groups unterstützen sämtliche RAID-Level. Eine RAID-Group besteht immer aus einem Festplattentyp. Storage-Pools können mit RAID 1/0, 5 oder 6 konfiguriert werden. Wenn Sie diese mit FAST VP verwenden, dürfen Sie unterschiedliche Festplattentypen in denselben Storage-Pool aufnehmen. Verwenden Sie im Mischbetrieb Ihres Storage-Pool Flash-Drives, steht Ihnen mit der aktuellen Firmware VNX OE 31.5.x nur die Konfiguration mit RAID 5 zur Verfügung. VNX benötigt für Datenschutzmechanismen wie Snapshots eine oder mehrere RAID-Groups.

Eine Übersicht der Eigenschaften von RAID-Groups und Storage-Pools finden Sie in Tabelle 11.2.

Eigenschaften	RAID-Groups	Storage-Pools
Typ	RAID-Group-LUN	thin (TLU), thick (DLU)
Allokation	vollständig	TLU: keine, DLU: Reservation
maximale Festplatten	16	71–996 (abhängig von Systemtyp)
erweiterbar	ja	ja
komprimierbar	nein	ja
SCSI-Unmap	nein	ja
verkleinerbar	nein	ja

Tabelle 11.2 Eigenschaften von Speichergruppen (TLU = Thin LUN, DLU = Dense LUN)

FAST VP (Fully Automated Storage Tiering for Virtual Provisioning) bietet Ihnen eine automatische Verschiebung von Datensätzen (*Slice*) innerhalb eines Storage-Pools, der mit unterschiedlichen Festplattentypen konfiguriert ist. Es werden drei Festplattentypen voneinander unterschieden: Flash-Speicher, SAS und NL-SAS. Speichersysteme, die mehrere Festplattentechnologien in einem System vereinen, werden oft als *Tiered Storage Arrays* bezeichnet. Für die Konfiguration von FAST VP benötigt man mindestens zwei Festplattentypen. Das Speichersystem analysiert im Hintergrund, welche Datensätze oft im Zugriff sind und welche weniger. Slices werden manuell oder mittels eines automatischen Planers in der Größe von 1 GB entsprechend der Zugriffshäufigkeit innerhalb eines Storage-Pools und seiner Tiers migriert. So optimiert sich das System ständig selbst und bietet jederzeit eine gute Performance. FAST VP greift nicht ad hoc, sondern seine Vorzüge kommen erst nach einiger Betriebszeit richtig zum Tragen.

FAST-VP-Datenplatzierungs-Richtlinien

EMC empfiehlt, bei der Erstellung einer LUN aus einem FAST-VP-Storage-Pool von der Grundeinstellung Auto-Tier abzusehen und stattdessen die Priorität auf den höchsten verfügbaren Storage-Tier (Highest Available Tier) zu legen.

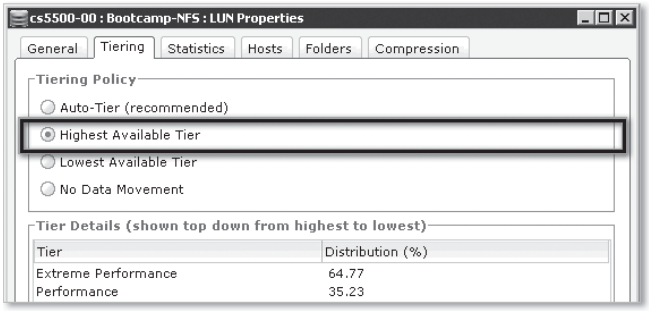


Abbildung 11.2 Einstellung der »Tiering Policy« einer individuellen Storage-Pool-LUN

VNX bietet die Möglichkeit, LUNs zu erstellen, die mehrere Tiers umfassen. FAST-VP passt das I/O-Profil eines Datastores über die unterschiedlichen Tiers eines Storage-Pools an. Die Resul-

tate dieser Optimierung sehen Sie jedoch erst nach einer gewissen Laufzeit und nicht schon bei der Inbetriebnahme.

Einrichten von Storage-Pools

Beim Einrichten eines Storage-Pools entscheiden Sie sich für einen RAID-Schutz (1/0, 5 oder 6). Bitte achten Sie darauf, dass in jedem Speicher-Tier die Gesamtzahl der Festplatten durch deren Anzahl im geplanten RAID-Verbund geteilt eine ganze Zahl ergibt.

Beispiel 1: Storage-Pool-Konfiguration mit zwei Tiers: 5 Flash-Festplatten, 50 NL-SAS-Festplatten. Wahl RAID 5. Resultat: 1 RAID-5-(4+1)-Verbund mit Flash-Festplatten und 10 RAID-5-(4+1)-Verbünde mit SAS-Festplatten.

Beispiel 2: Storage-Pool-Konfiguration mit drei Tiers: 5 Flash-Festplatten, 9 SAS-Festplatten, 25 NL-SAS-Festplatten. Wahl RAID 5. Resultat: 1 RAID-5-(4+1)-Verbund mit Flash-Festplatten, 1 RAID-5-(4+1)-Verbund mit SAS-Festplatten, 1 RAID-5-(3+1)-Verbund mit SAS-Festplatten, 5 RAID-5-(4+1)-Verbünde mit NL-SAS-Festplatten.

Beispiel 1 zeigt einen gleichmäßig konfigurierten Storage-Pool auf und Beispiel 2 einen ungleichmäßigen. Letzterer kann sich negativ auf die Performance auswirken.

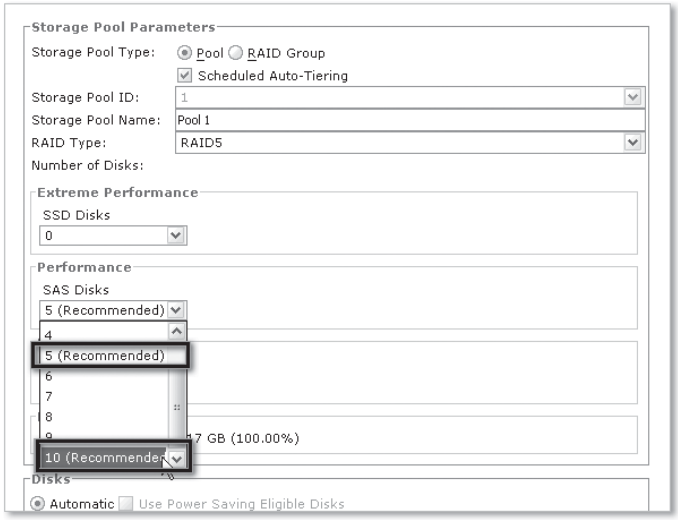


Abbildung 11.3 Empfohlene Einstellungen beim Erstellen eines Pools

Die attraktivste RAID-Konfiguration für VMFS- wie auch NFS-Datastores ist ein RAID-5-Verbund mit jeweils fünf Festplatten. Idealerweise erfolgt der Ausbau auch in der Granularität von minimal fünf Festplatten. Sie können den Ausbau auch mit einer durch fünf teilbaren Menge vornehmen (beispielsweise 20 oder 25 Festplatten). EMC empfiehlt beim Ausbau eines Storage-Pools eine gleichbleibende Anzahl an Festplatten (erfolgt zum Beispiel der erste Ausbau mit fünf Festplatten, so sollten es auch beim nächsten Ausbau fünf Festplatten sein). Ansonsten beeinträchtigen Sie die Performance des Storage Pools.

Alternativ konfigurieren Sie für erhöhte Ausfallsicherheit RAID 6. EMC empfiehlt den Einsatz von RAID-6-Gruppen bei Festplatten mit mehr als 1 TB Kapazität. Die optimale Konfiguration ist ein RAID-6-(8+2)-Festplattenverbund. Das ist ein Unterschied zur Storage-Pool-Konfiguration, die RAID 6 mit acht Festplatten konfiguriert.

Storage-Pool-Konfiguration mit RAID 6

Sie können eine Storage-Pool-Konfiguration mit RAID 6 (8+2) anstelle der Grundeinstellung von RAID 6 (6+2) erzwingen, indem Sie einen Storage-Pool mit initial zehn Festplatten einrichten und diesen um immer weitere zehn vergrößern. Nachteile:

1. Sie können keine Flash-Festplatten nutzen. Empfehlung: Richten Sie daher FAST Cache ein.
2. Die granulare Ausbaubarkeit ist ein wenig geringer (zehn anstelle von acht Festplatten).

VNX LUNs

Die Charakteristik von RAID-Group-LUNs (RG-LUNs) ist, dass sie den gesamten ihr zugewiesenen Speicherplatz allokieren. Eine 1-TB-LUN zum Beispiel konsumiert auf VNX 1 TB. Die LUN wird basierend auf direkt aneinanderliegenden Blöcken erstellt.

Ist es gewünscht, dass der I/O über mehrere RAID-Groups verteilt wird, so unterstützt VNX den Zusammenschluss mehrerer RG-LUNs zu einer einzigen riesigen LUN, genannt *MetaLUN*. In virtualisierten Umgebungen werden RG-LUNs und MetaLUNs eingesetzt, wenn eine Applikation explizit nach dedizierten Speicherressourcen verlangt. Das aktive Hot Sparing und die ständig im Hintergrund laufende Überwachung der Festplatten identifizieren potentielle Ausfälle frühzeitig und schützen so die RAID-Verbünde zusätzlich. Global Hot Spares werden separat konfiguriert.

Global Hot Spares

Sie benötigen pro Festplattentyp einen Hot Spare. Faustregel: Planen Sie pro 30 Festplatten eine Global-Hot-Spare-Festplatte ein.

Storage-Pools kennen zwei Typen von LUNs: Thin LUNs (TLU) und Thick LUNs (DLU – Dense LUNs). Eine DLU ist der Standardtyp, wenn Sie aus einem Storage-Pool eine LUN erstellen. Anders als bei einer RG-LUN ist die einer DLU zugeordnete Speicherkapazität nicht allokiert. Letztere unterscheidet sich von einer TLU darin, dass die ihr zugewiesene Speicherkapazität zu 100 % reserviert ist, d. h. von der Gesamtkapazität des Storage-Pools abgezogen wird. Eine Überprovisionierung der Gesamtkapazität des Speichersystems, wie sie bei TLUs möglich ist, können Sie mit DLUs nicht abbilden. Die maximale Kapazität einer TLU oder DLU ist 16 TB.

Wichtige Information zu TLUs

Beim Einsatz von TLUs empfiehlt sich eine regelmäßige Überwachung des Systems. Umso mehr, da VMware-Administratoren gerne mit Thin-Virtual-Disks (VMDK-Datei) arbeiten.

Eine Kombination der beiden Mechanismen nennt man *thin on thin*. In vSphere 5 gibt es die Funktion Thin-Provisioning-Stun, um der gefürchteten Out-of-Space-Kondition entgegenzuwirken, die sämtliche VMs eines betroffenen VMFS-Datastores beeinträchtigt. Blöcke, die einmal in einer TLU allokiert sind, bleiben bestehen, auch wenn das Gastsystem sie gelöscht hat. Wie Sie diese ungenutzte Kapazität wieder freigeben, erfahren Sie in Abschnitt 11.2.3, »Best Practices zu blockbasierten Speicheroptionen«.

VNX unterstützt LUN-Shrink (das Freigeben von ungenutzter Kapazität einer LUN) für alle LUN-Typen.

Systemcache und FAST Cache

VNX verfügt über einen Schreib- und Lesecache. Dessen Größe ist abhängig vom Systemtyp der VNX-Produktreihe. Sämtliche Schreibvorgänge werden innerhalb des Systems zwischen den beiden Storage-Processors gespiegelt.

Der Systemcache kann um Flash-Festplatten erweitert werden. Die Größe dieser als *FAST Cache* bezeichneten Technologie ist wiederum abhängig vom Systemtyp. Im Gegensatz zu FAST VP arbeitet FAST Cache in Echtzeit und nutzt 64-KB-Extents anstelle der 1-GB-Slices. Diese Extents werden basierend auf der Zugriffshäufigkeit der enthaltenen Blöcke in den FAST Cache promoviert. Folgezugriffe auf Blöcke eines promovierten Extents gestalten sich entsprechend schneller. Sollte der Zugriff auf ein Extent nachlassen oder ändern sich die Prioritäten von Blöcken, wird der entsprechende Extent von FAST Cache freigegeben. Je häufiger ein Lesezugriff auf ein Extent erfolgt, desto größer ist der Geschwindigkeitseffekt. Zum Beispiel profitieren VMware-View-Umgebungen enorm von dieser Funktionalität.

FAST Cache bringt nicht nur für Lesezugriff Vorteile, sondern hilft auch bei Schreibvorgängen und kann den Systemcache signifikant entlasten.

FAST Cache vs. Flash-Festplatten im Storage-Pool

FAST Cache agiert global für das System und lässt sich pro Storage-Pool und RG-LUN aktivieren. Flash-Festplatten im Storage-Pool bringen nur dem jeweiligen Pool einen Nutzen. Das heißt, nutzen Sie wertvolle Flash-Festplatten in erster Priorität für FAST Cache.

11.2.2 Konfiguration der VNX für blockbasierten Zugriff

Für den Einsatz einer VNX empfiehlt EMC, die Grundeinstellung nicht zu verändern, es sei denn, Sie wollen das System für Applikationen mit höchsten Performanceansprüchen optimieren. Sie finden in diesem Abschnitt Empfehlungen zur Leistungssteigerung im Betrieb mit virtuellen Umgebungen. Nach der Installation der VNX mit dem *VNX-Installation-Assistant-for-File/Unified* können Sie mit der Konfiguration des Speichersystems beginnen. Diese Routine erläutern wir hier nicht, da sie von EMC gut dokumentiert ist.

VNX Installation Assistant for File/Unified

Führen Sie bei einer Erstinstallation einer VNX unbedingt den *VNX-Installation-Assistant-for-File/Unified* aus. Dieses Programm überprüft das System auf fehlerhafte Komponenten und Verkabelung hin. Es bereitet eine Grundkonfiguration gemäß Ihren Angaben vor und führt diese aus. Verzichten Sie auf eine automatische Konfiguration der Speicherkapazität an dieser Stelle.

Verbindung zum vCenter

Sie benötigen eine Installation von Java, um die webbasierte Verwaltung zu starten. Öffnen Sie einen Browser, und verweisen Sie ihn zur IP-Adresse oder zum Fully Qualified Domain Name (FQDN). Beim Aufsetzen der VNX haben Sie diese Informationen bereits verwendet.

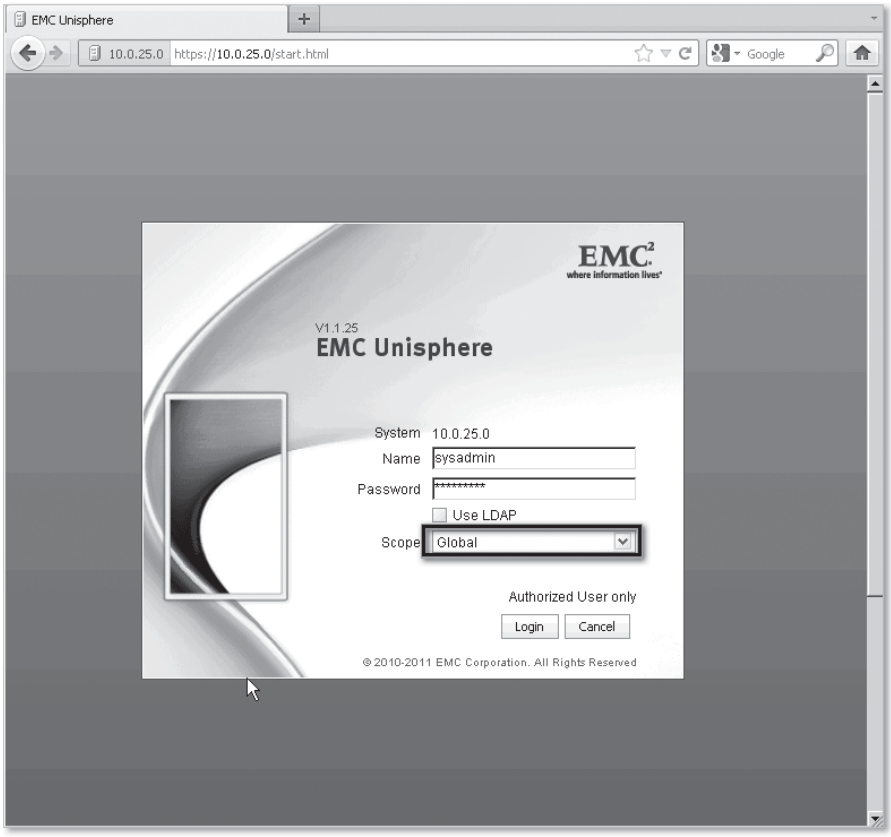


Abbildung 11.4 Einwahl in Unisphere zur Verwaltung der VNX

Achten Sie beim Login darauf, dass der SCOPE auf GLOBAL steht. Nach dem erfolgreichen Login können Sie die VNX mit *vCenter* und dem ESXi-Server verbinden. Navigieren Sie vom DASHBOARD zu SYSTEM LIST, und wählen Sie die neu installierte VNX aus der Liste aus. Unisphere erlaubt die zentrale Verwaltung mehrerer VNX-Systeme.

Wizards

Für die wichtigsten Aufgaben zur Verwaltung eines VNX-Systems steht Ihnen eine Vielzahl an Wizards zur Verfügung. Diese Helfer finden Sie am einfachsten über die Reiter der Hauptnavigationsleiste (System • Storage • Hosts • Data Protection • Settings). Tipp: Bedienen Sie sich wann immer möglich des Wizards.

Ein Anwendungsbeispiel mit einem Wizard sehen Sie beim Hinzufügen Ihres vCenters und der ESXi-Hosts. Ansonsten verzichten wir in diesem Kapitel auf den Einsatz von Wizards, um die Grundlagen besser zu vermitteln.

Wählen Sie dann Hosts • Virtualization, um ins Menü für die Verwaltung der ESXi-Server zu gelangen. Sie sehen auf der rechten Seite des Dropdown-Menüs eine Auswahl der Wizards, die Ihnen zur Verfügung stehen.

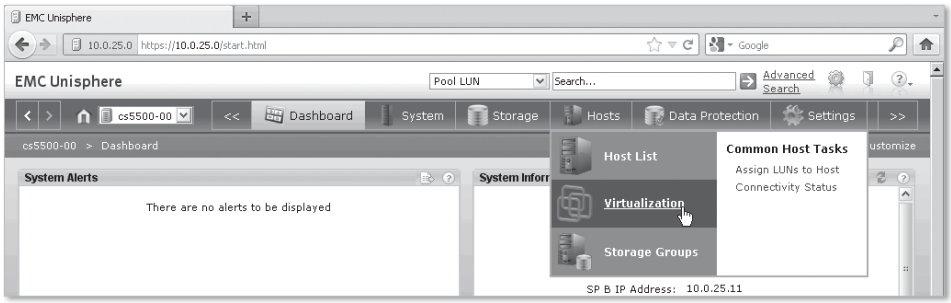


Abbildung 11.5 Menüführung der Verwaltungsoberfläche eines VNX-Systems

Mit einem Klick auf Add starten Sie den Hypervisor Information Configuration Wizard. Werden sämtliche ESXi-Server von vCenter verwaltet, dann entscheiden Sie sich für Configure my ESX Servers managed by vCenter und fahren fort.

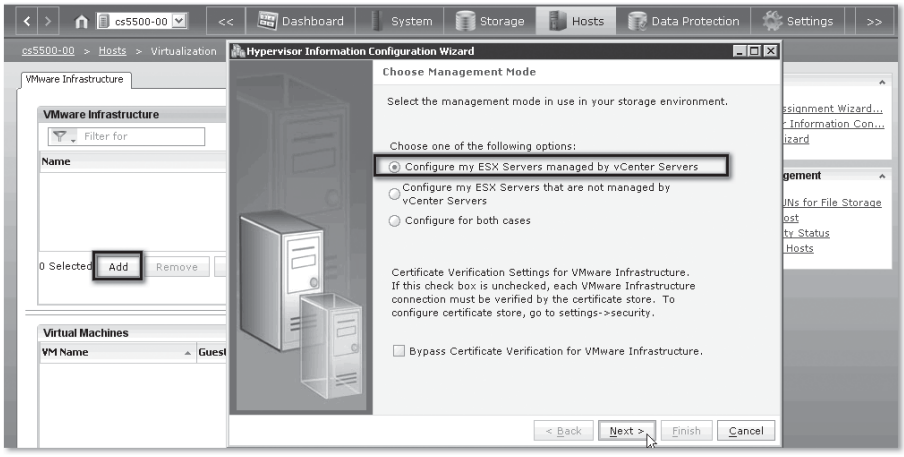


Abbildung 11.6 »Hypervisor Information Configuration«-Wizard

Sobald Sie im nächsten Fenster auf ADD klicken, erscheint ein Eingabefenster zur Angabe Ihrer vCenter. Füllen Sie diese Maske aus, und bestätigen Sie mit OK.

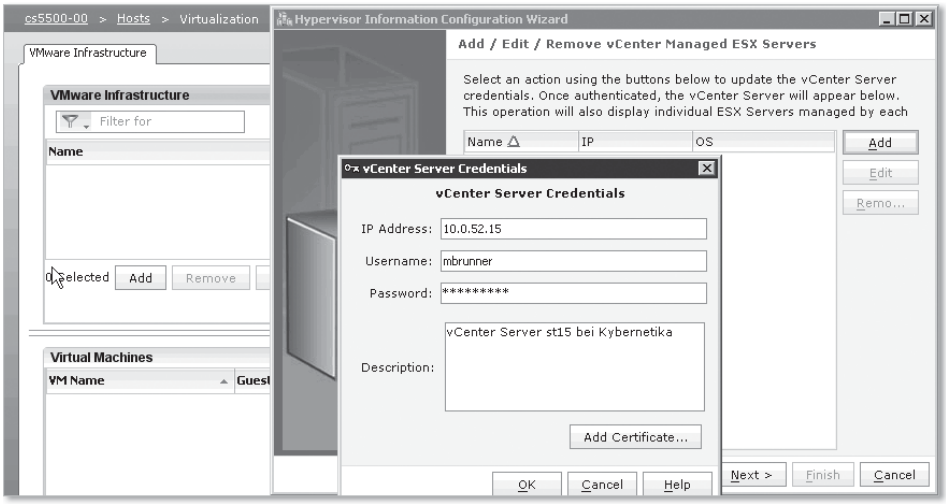


Abbildung 11.7 Anmelden der vCenter im Wizard

Importieren Sie das Sicherheitszertifikat. Sie finden die Datei auf Ihrem vCenter Server; sie heißt *rui.crt*.

- Windows Server 2008:
  C:\Program Data\VMware\VMware VirtualCenter\SSL
- Übrige Windows-Systeme:
  C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL

Abbildung 11.8 Erfolgreicher Import der vCenter

In der Übersicht HOSTS • HOST LIST finden Sie eine Auflistung sämtlicher Server.

Cache und FAST Cache

Die Kapazität des Hauptspeichers variiert bei den Systemtypen, ist aber nicht ausbaubar. Reservieren Sie für den Lese-Cache initial die Werte in Tabelle 11.3, und nutzen Sie die verbleibende Kapazität als Schreib-Cache. Sie sollten nie mehr als 1.024 MB für den Lese-Cache einsetzen.

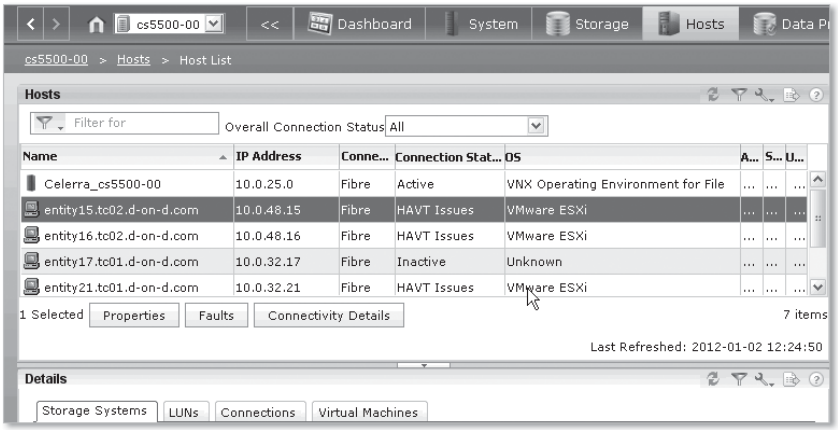


Abbildung 11.9 Gesamtübersicht der Unisphere bekannten Server

SP RAM	VNX5100	VNX5300	VNX5500	VNX5700	VNX7500
Lese-Cache	100 MB	400 MB	700 MB	1.024 MB	1.024 MB

Tabelle 11.3 Empfohlene Einstellungen für den Lese-Cache

Rufen Sie via SYSTEM • SYSTEM MANAGEMENT • MANAGE CACHE das Fenster zur Verwaltung des Cache auf. Im Reiter SP CACHE deaktivieren Sie sowohl den Write- als auch die Lese-Caches; klicken Sie dann auf APPLY.

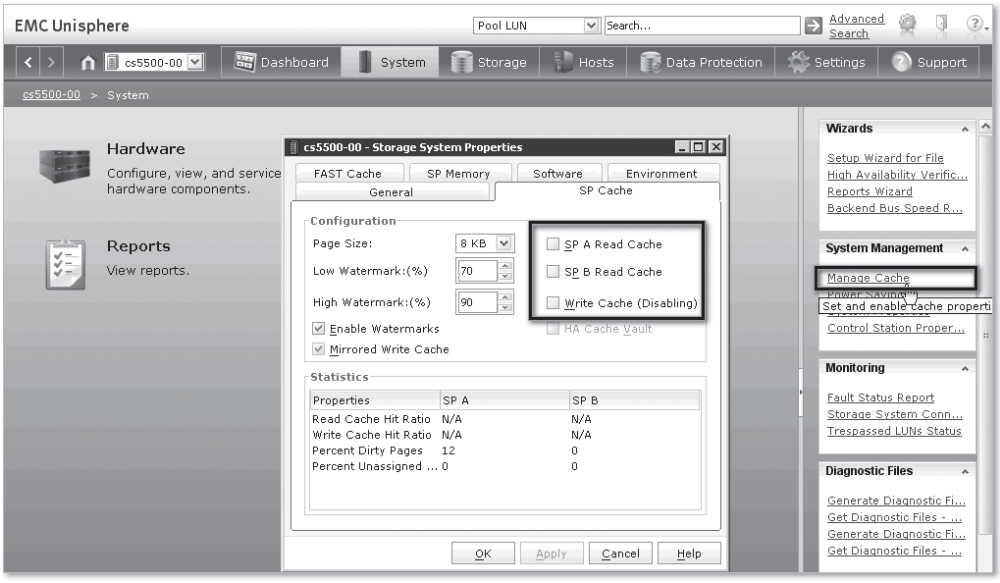


Abbildung 11.10 Aufrufen der Verwaltung des Cache

Wechseln Sie danach zum Reiter SP MEMORY, um den Hauptspeicher des Speichersystems gemäß den Empfehlungen von Tabelle 11.3 einzustellen. Das Beispiel bezieht sich auf eine VNX5500. Klicken Sie auf APPLY.

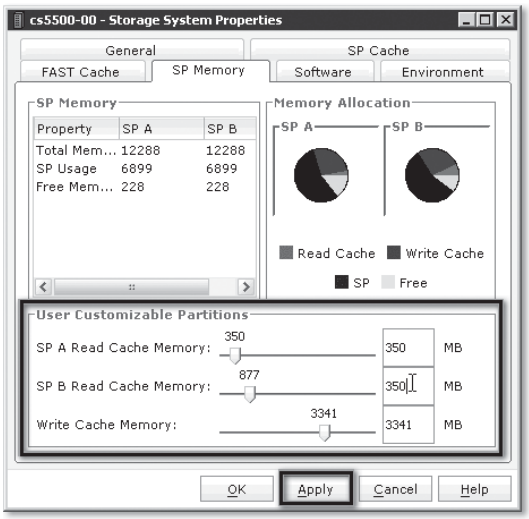


Abbildung 11.11 Einstellen der Werte für Lese- und Schreib-Cache

Gehen Sie wieder zurück zum Reiter SP CACHE, und aktivieren Sie die Schreib- und Lese-Caches erneut. Setzen Sie die PAGE SIZE auf 8 KB. Bestätigen Sie Ihre Eingaben mit APPLY.

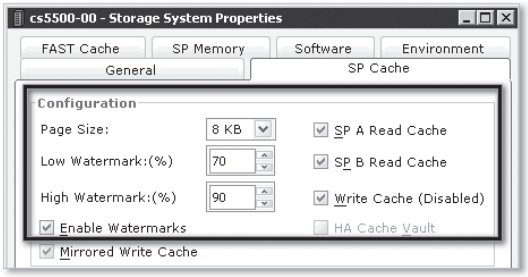


Abbildung 11.12 Aktivieren der Lese- und des Schreib-Caches

Wasserzeichen für den Cache

Sollte es zu Leistungsverzögerungen aufgrund eines zu kleinen Schreib-Caches kommen, verringern Sie die Werte WATERMARK-Werte (empfohlene Werte sind LOW = 60 % und HIGH = 80 %). Das erlaubt eine frühere Freigabe von I/Os im Cache.

Falls Ihr Speichersystem mit Flash-Festplatten ausgerüstet ist und Sie diese als Erweiterung des Hauptspeichers nutzen wollen, wählen Sie zur Konfiguration den Reiter FAST CACHE. Wollen Sie nicht alle Flash-Festplatten als FAST Cache nutzen, entscheiden Sie sich für die

Option MANUELL. Andernfalls können Sie die Grundeinstellung AUTOMATISCH beibehalten. Bestätigen Sie Ihre Auswahl mit OK.

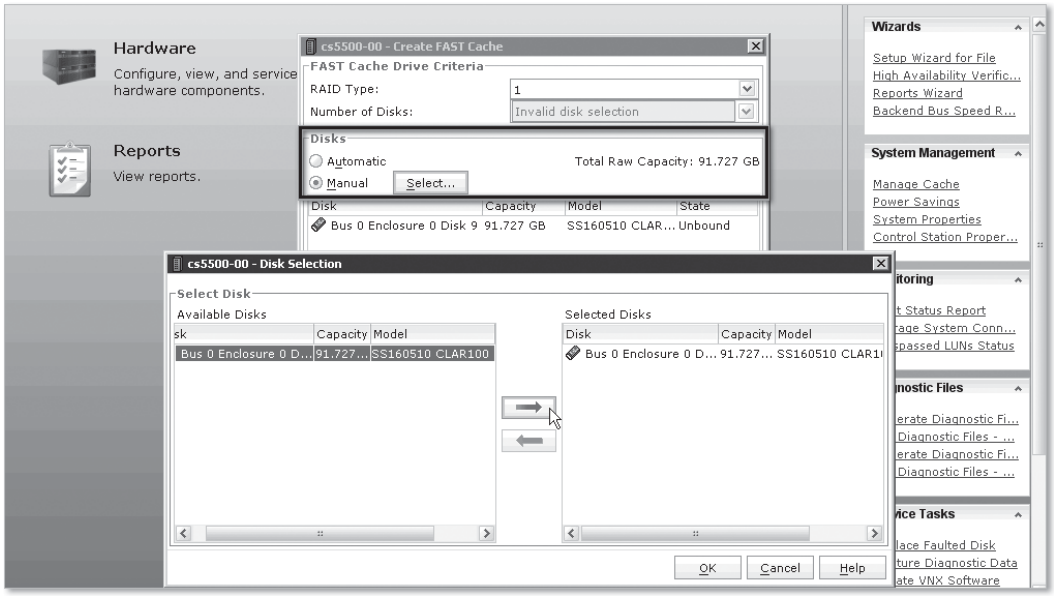


Abbildung 11.13 Manuelle Konfiguration des FAST Cache

Beim Einsatz von FAST Cache wird dieser pro Storage-Pool ein- oder ausgeschaltet. Nutzen Sie RAID-Gruppen, so müssen Sie den FAST Cache pro RG-LUN oder MetaLUN-Komponente aktivieren (Abbildung 11.14).

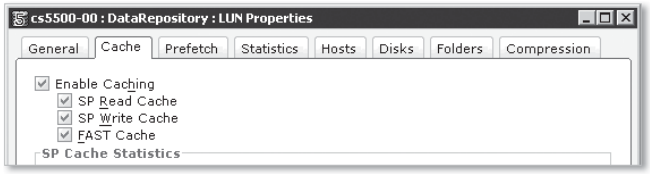


Abbildung 11.14 Konfiguration des Cache einer individuellen RG-LUN

RAID-Gruppen und Storage-Pools

Zur Konfiguration einer RAID-Gruppe gehen Sie auf STORAGE • STORAGE CONFIGURATION • STORAGE POOL und klicken auf CREATE. In der Eingabemaske wählen Sie beim STORAGE POOL TYPE den Typ RAID GROUP aus. Die Maske ändert sich je nachdem, ob Sie einen Storage-Pool oder eine RAID-Gruppe konfigurieren. Sie können eine STORAGE POOL ID vergeben und den RAID-Schutz bestimmen. Das Speichersystem unterbreitet Ihnen einen Vorschlag mit den Konfigurationsempfehlungen für die RAID-Gruppe. Dieser wiederum erfolgt anhand der Wahl des RAID-Schutzes sowie der Anzahl Festplatten, die Ihnen zur Verfügung stehen. Diese Auswahl ist je nach Konfigurationsstand unterschiedlich.

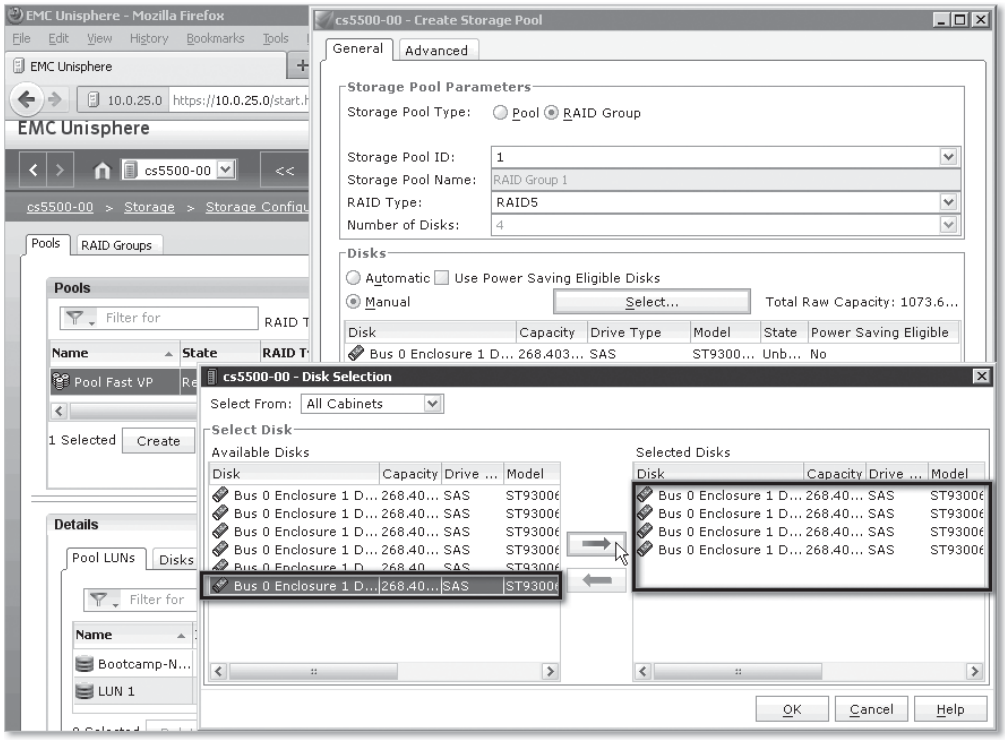


Abbildung 11.15 Manuelles Hinzufügen von Festplatten

Bei den Festplatten steht Ihnen nur ein Typ zur Verfügung. Sie dürfen wählen, ob Sie mit dem Vorschlag zur Konfiguration der RAID-Gruppe einverstanden sind oder ob Sie die Festplatten manuell hinzufügen möchten (Abbildung 11.15). Die manuelle Konfiguration der Festplatten steht Ihnen auch für das Erstellen eines Storage-Pools zur Verfügung.

Hinter dem Reiter ADVANCED verbergen sich interessante Konfigurationsmöglichkeiten. Das VNX-System übernimmt automatisch Aufgaben zur Defragmentierung von RG-LUNs und optimiert so die Performance.

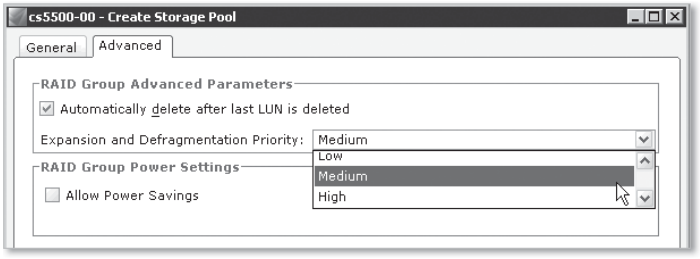


Abbildung 11.16 Erweiterte Konfigurationsmöglichkeiten einer RAID-Gruppe

Bestätigen Sie Einstellungen mit APPLY.

Eine Besonderheit bei der Festplattenkonfiguration ist, dass Sie für Nearline-SAS-Festplatten (NL-SAS) den Knopf User Power Saving Eligible Disks aktivieren können. Das ermöglicht das Herunterfahren von Festplatten, die nicht im alltäglichen Zugriff sind.

Prinzipiell gilt: »Go wide before going deep.« Das heißt, Sie sollten einzelne LUNs über möglichst viele Spindeln (physische Festplatten) verteilen. Für eine gutes Preis-/Leistungsverhältnis bietet sich RAID 5 (4 + 1) an. Das gilt für RAID-Gruppen wie für Storage-Pools. Alternativ bietet sich die Möglichkeit von RAID 6 (6 + 2). Storage-Pools arbeiten in der Grundkonfiguration mit 8 Festplatten.

Nach der Erstellung der genannten RAID-Verbünde bieten sich Ihnen folgende Möglichkeiten zur Konfiguration von VMFS-Datastores über mehr als 5 oder 8 Spindeln:

- Konfigurieren von Storage-Pools anstelle von RAID-Groups
- Bilden von MetaLUNs
- LUN-Growing von VMFS-Datastores
- Erstellen von VMFS-Datastores mit Extents

Zum Erstellen eines Storage-Pools gehen Sie auf Storage • Storage Configuration • Storage Pool und klicken auf Create. In der Eingabemaske aktivieren Sie Scheduled Auto-Tiering. Falls Sie beabsichtigen, Storage Dynamic Resource Scheduling (SDRS) oder Storage I/O Control (SIOC) einzusetzen, beachten Sie die Best Practices in Abschnitt 11.2.3, »Best Practices zu blockbasierten Speicheroptionen«. Wählen Sie den gewünschten RAID-Schutz. Sie erhalten dann eine Übersicht über die empfohlene Anzahl an Festplatten für den Storage-Pool. Diese Empfehlung steht Ihnen pro Festplattentyp Flash, SAS und NL-SAS zur Verfügung. Wählen Sie die gewünschte Anzahl an Festplatten pro Festplattentyp für Ihren Storage-Pool aus. Bei den Empfehlungen handelt es sich um Best Practices.

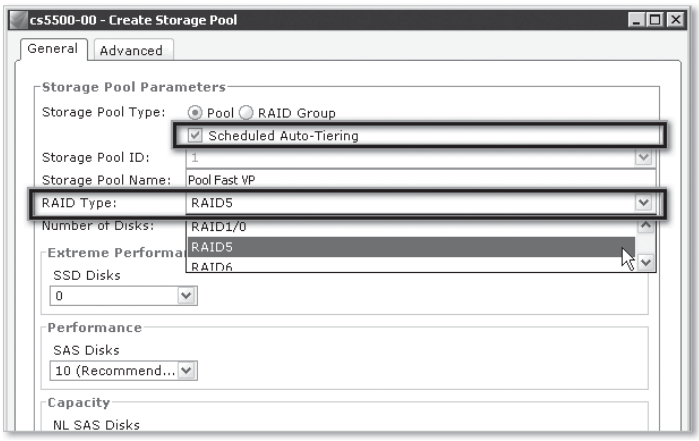


Abbildung 11.17 Eingabemaske zur Erstellung von Storage-Pools oder RAID-Gruppen

Belassen Sie die restlichen Konfigurationsparameter in ihrer Grundeinstellung, und klicken Sie auf den Reiter ADVANCED.

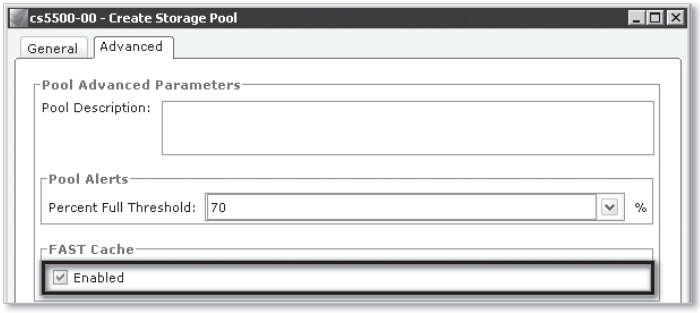


Abbildung 11.18 Fortgeschrittene Konfigurationsmöglichkeiten

Sie haben in den POOL ADVANCED PARAMETERS die Möglichkeit, FAST CACHE einzuschalten. Den Parameter SCHEDULED AUTO-TIERING können Sie gemäß Ihren Wünschen konfigurieren (Abbildung 11.19). Hierfür klicken Sie auf MANAGE AUTO-TIERING im Menü zur rechten Seite.

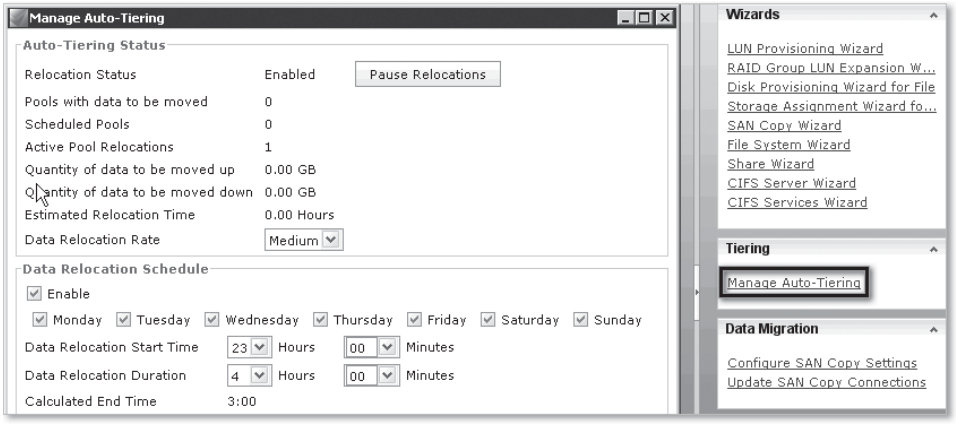


Abbildung 11.19 Planer für das Auto-Tiering

LUN-Konfiguration und ALUA

Das Speichersystem ist nun bereit, und Sie dürfen die erste LUN erstellen. Wählen Sie STORAGE • LUNS • LUNS, und klicken Sie im Fenster auf CREATE. Erstellen Sie eine LUN aus dem STORAGE POOL namens POOL FAST VP. Die LUN soll als TLU mit einer Kapazität von 4 TB konfiguriert werden. Wahlweise können Sie einen Namen vergeben und eine START LUN ID. Das ist nützlich, falls Sie mehrere LUNs erstellen und diese einfach identifizieren wollen, beispielsweise wenn Sie dem dateibasierten Speicherbereich des VNX-Systems LUNs zur Verfügung stellen.

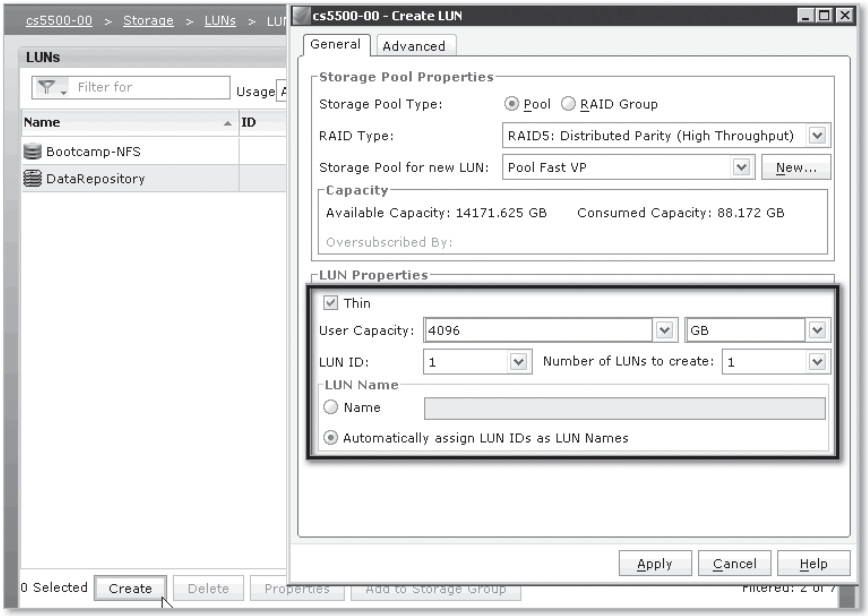


Abbildung 11.20 Maske zum Erstellen einer LUN

Gehen Sie zum Reiter ADVANCED. Wählen Sie die Erstplatzierung der Daten im HIGHEST AVAILABLE TIER.

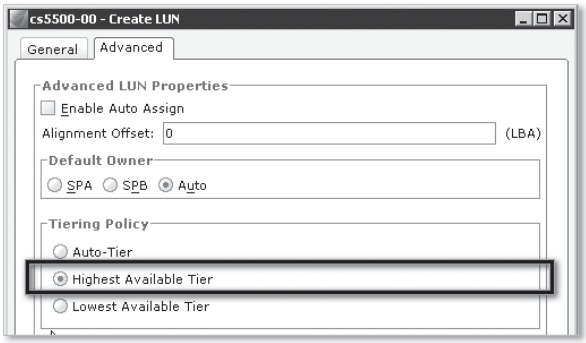


Abbildung 11.21 Wahl der »Tiering Policy«

Die übrigen Einstellungen der Eingabemaske können Sie in den Grundeinstellungen belassen. Bestätigen Sie Ihre Auswahl mit APPLY. Die Initialisierung des Storage-Pools nimmt wenige Minuten in Anspruch.

In einem nächsten Schritt soll die LUN dem ESX-Cluster zur Verfügung gestellt werden. Dafür müssen Sie das LUN-Masking konfigurieren. Dieses funktioniert bei einem VNX-System ein wenig anders. Es kennt das Prinzip der Storage-Groups. Mit Hilfe einer Storage-Group weisen

Sie Hosts und LUNs einander zu. Zur Konfiguration einer Storage-Group gehen Sie zu Hosts • Storage Groups und klicken auf Create.

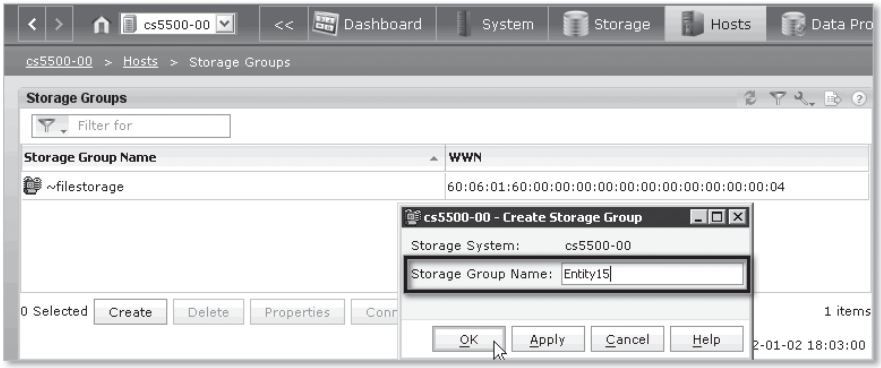


Abbildung 11.22 Namensgebung einer Storage-Group

Geben Sie der Storage-Group einen eindeutigen Namen. Bestätigen Sie die Eingabe mit OK. Folgen Sie den Anweisungen, um LUNs zur Storage-Group hinzuzufügen.

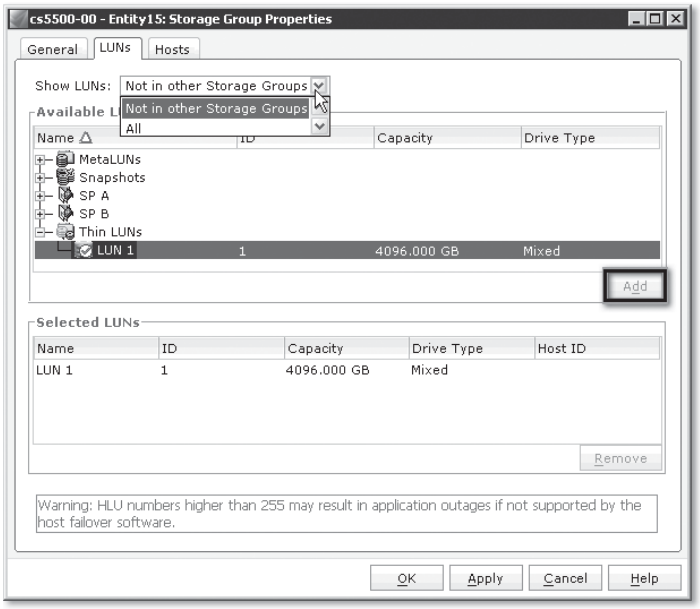


Abbildung 11.23 Auswahl der LUNs in den Eigenschaften einer Storage-Group

Suchen Sie sich die erstellte LUN in der Baumstruktur aus, und fügen Sie sie mit Add hinzu. Vergeben Sie für die LUN eine Host ID, und klicken Sie auf Apply.

Best Practices für Host-IDs

Vergeben Sie der Host-ID nach Möglichkeit dieselbe Zahl wie der LUN ID, die das VNX-Systeme zur internen Identifikation benutzt. Das vereinfacht das Troubleshooting. Ausnahme: Die Host-ID »LUN 0« verwenden Sie ausschließlich als Boot-LUN.

Wechseln Sie zum Reiter Hosts, und fügen Sie den gewünschten Host der Storage-Group hinzu. Suchen Sie sich den gewünschten ESXi-Server aus der Liste der verfügbaren Hosts aus, und fügen Sie ihn der Storage-Group hinzu. Bestätigen Sie Ihre Auswahl mit OK.

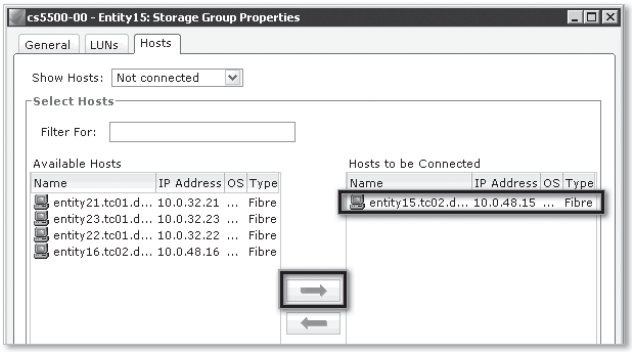


Abbildung 11.24 Auswahl der Hosts in den Eigenschaften einer Storage-Group

Wiederholen Sie den Vorgang, wenn Sie eine LUN einem ESX-Cluster zur Verfügung stellen wollen. Sie wählen dabei immer wieder dieselbe LUN aus.

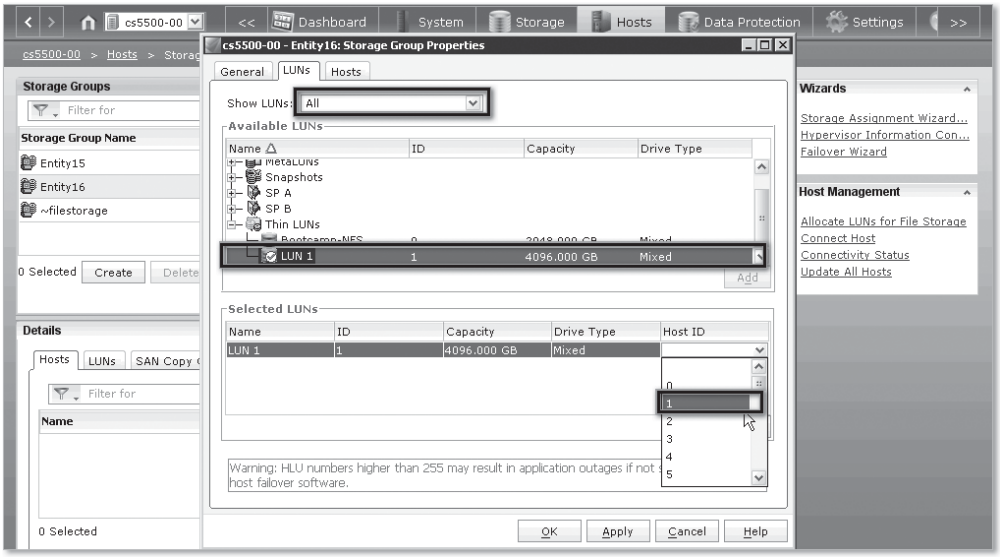


Abbildung 11.25 Vorgehen bei Zuweisen von LUNs zu einem ESX-Cluster

Best Practices für Storage-Groups

Es erscheint im ersten Augenblick logischer, einer Storage-Group mehrere ESXi-Hosts zu zuweisen, um Zugriff auf dieselbe LUN zu geben. Die korrekte Vorgehensweise ist aber genau umgekehrt. Das liegt zum einen darin begründet, dass Sie unter Umständen auch vom Host booten wollen und es somit zum Konflikt der Boot-Volumes käme. Zum anderen vertritt EMC die Philosophie des »des Single Initiator – Single Target-Zoning« im SAN.

Die LUN ist jetzt zur Anbindung an den ESX-Cluster vorbereitet. Wechseln Sie dazu auf Ihr vCenter. Gehen Sie zur Ansicht CONFIGURATION • STORAGE ADAPTERS der einzelnen ESXi-Server des Clusters. Führen Sie einen Rescan der HBAs durch, falls die Pfade zu den LUNs nicht angezeigt werden.

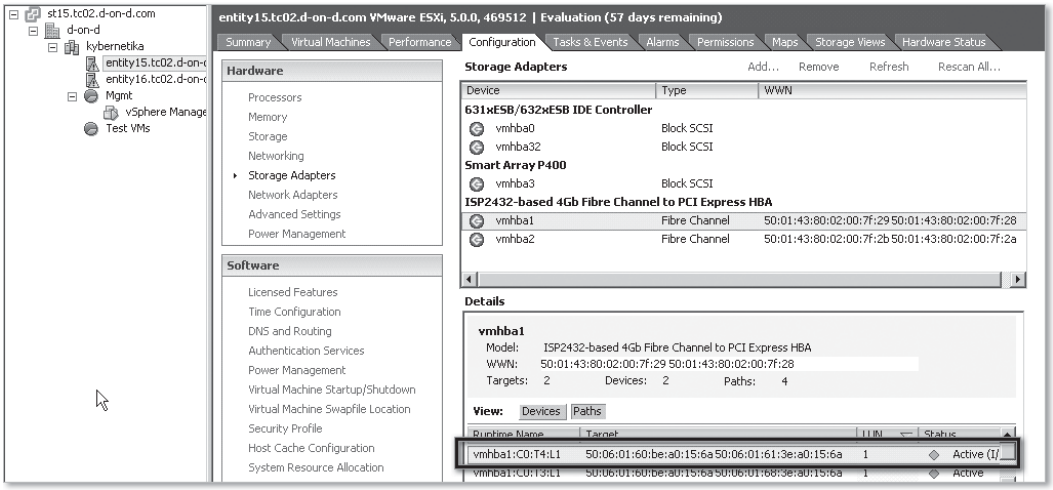


Abbildung 11.26 Präsentation der LUN im ESXi-Server

Fügen Sie dann die LUN mit dem Wizard ADD STORAGE... einem ESXi-Server hinzu. Wählen Sie unbedingt das VMFS-5-Dateisystem, da die neue LUN 4 TB Kapazität bietet.

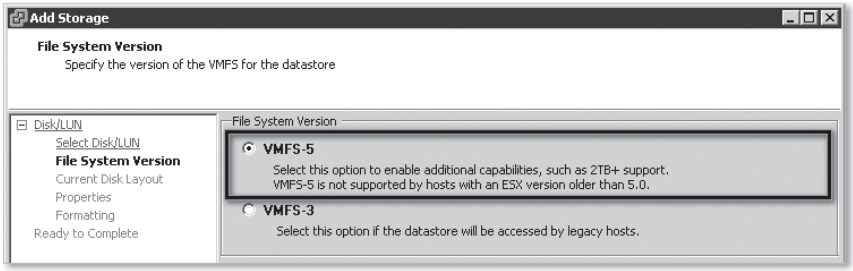


Abbildung 11.27 Erstellen eines VMFS-Datastores mit Hilfe des Wizards

Überprüfen Sie, ob auch dem zweiten ESXi-Server des Clusters Zugriff auf den neuen VMFS-Datastore gewährt ist. Testen Sie den Schreibzugriff, indem Sie ein Verzeichnis anlegen.

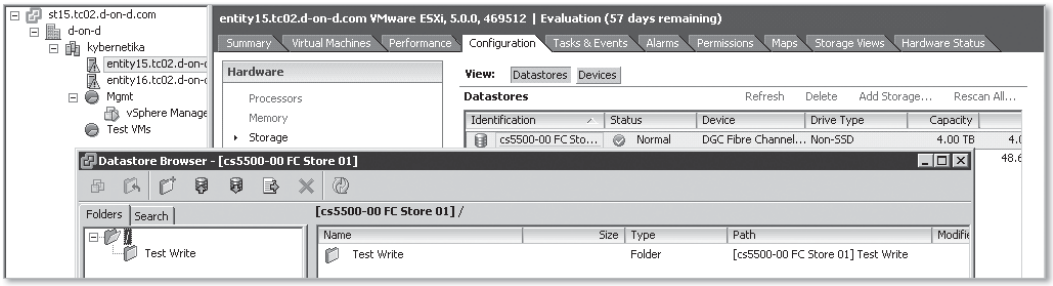


Abbildung 11.28 Zugriff auf den VMFS-Datastore

ALUA (*Asymmetric Logical Unit Access*) schützt eine LUN vor einem Pfadausfall im SAN, so dass ein solcher kein LUN-Trespassing (die LUN wird nicht mehr auf dem optimalen Pfad angesprochen) zur Folge hat. ALUA hat keinen Effekt auf die Performance des optimalen Pfades. Wird eine LUN jedoch nicht über ihren optimalen Pfad angesprochen, so sind die Folgen eine Einbuße von 10 bis 20 % in IOPS-Leistung und eine Verminderung der Bandbreite von bis zu 50 %.

Überprüfen Sie, dass Ihre ESXi-Server seitens des VNX-Systems für ALUA konfiguriert sind. Gehen Sie auf HOSTS • VIRTUALIZATION • HOST MANAGEMENT • CONNECTIVITY STATUS.

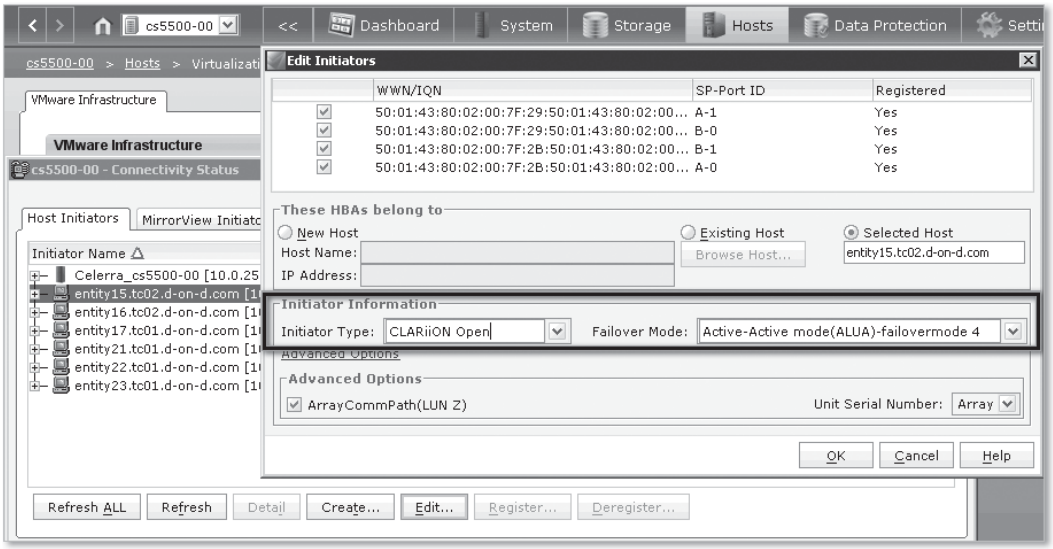


Abbildung 11.29 Überprüfen und Einstellen von ALUA

Wählen Sie den zu überprüfenden ESXi-Server aus der Host Initiator-Liste aus, und klicken Sie auf Edit. In der Eingabemaske stellen Sie den Wert Failover Mode auf Active – Active (failovermode 4). Bestätigen Sie Ihre Eingabe mit OK.

Hinweise zu den »Advanced Options«

Achten Sie im selben Fenster in Abbildung 11.29 bei Advanced Options auf die Option Array-CommPath (LUN Z). Das Aktivieren der Checkbox hilft im Falle einer Fehlersuche dabei, die Konnektivität vom ESXi-Host zur VNX festzustellen.

Nachdem die Einstellung von ALUA auf dem Speichersystem bestätigt ist, gilt es, diese auch für die ESXi-Hosts zu überprüfen. Diese Überprüfung müssen Sie für jeden Host einzeln vornehmen.

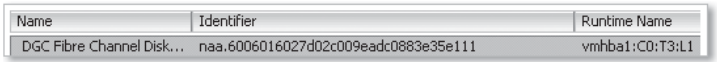


Abbildung 11.30 »Storage Adapter Devices«-Ansicht

Suchen Sie sich die Identifier der konfigurierten LUN aus. Der Name des Identifiers beginnt mit »naa«. Notieren Sie sich die ersten acht Zeichen, im Beispiel: »naa.6006«.

Verbinden Sie sich mit der vSphere Management Appliance (vMA), und wählen Sie einen ESXi-Host zur Konfiguration aus. Führen Sie dazu folgenden Befehl aus:

```
vi-admin@vcenter: ~> esxcli --server entity15.tc02.d-on-
d.com storage nmp device list |grep -A 7 -i naa.6006
naa.6006016027d02c009eadc0883e35e111
Device Display Name: DGC Fibre Channel Disk (naa.6006016027d02c009eadc0883e35e111)
Storage Array Type: VMW_SATP_ALUA_CX
Storage Array Type Device Config: {navireg=on, ipfilter=on}{implicit_
support=on;explicit_support=on; explicit_allow=on;alua_followover=on;{TPG_id=
  2,TPG_state=ANO}{TPG_id=1,TPG_state=AO}}
Path Selection Policy: VMW_PSP_FIXED
Path Selection Policy Device Config: {preferred=vmhba1:C0:T4:L1;current=
  vmhba1:C0:T4:L1}
Path Selection Policy Device Custom Config:
Working Paths: vmhba1:C0:T4:L1
```

Achten Sie auf die auf die Zeilen `Storage Array Type` und `Path Selection Policy`. Wenn diese auf `VMW_SATP_ALUA_CX` bzw. `VMW_PSP_FIXED` lauten, dann brauchen Sie keine weiteren Schritte zu unternehmen. Wie Sie Multipathing-Einstellungen verändern, erfahren Sie in Abschnitt 11.3.7.

Führen Sie diese Überprüfung bei sämtlichen Hosts durch, die Zugriff auf diese LUN haben.

11.2.3 Best Practices zu blockbasierten Speicheroptionen

Ein VNX-System kann für den Einsatz in virtuellen Umgebungen optimiert werden. Generell gelten die folgenden allgemeinen Best Practices:

- die Firmware auf den neuesten Stand bringen
- Kenntnis über die Arbeitslast der Applikationen
- die Grundeinstellungen des Systems nutzen
- auftretende Probleme sofort lösen

Das Anwenden der Best Practices erfolgt am besten »top-down«:

- Anwenden der Best Practices von Applikationen (viele Hersteller bieten für ihre Anwendungen und Datenbanken Tuning-Werkzeuge an)
- Befolgen der Best Practices für vSphere 5
- Durchführen von Best Practices im Netzwerk
- Ausüben von Best Practices am Speichersystem

Applikationen, Datenbanken, virtuelle Maschinen und vSphere 5

Blockbasierter Speicher wird in Form des VMFS, *In-Guest-iSCSI* oder von Raw Device Mappings (Virtual oder Physical RDM) zur Verfügung gestellt. EMC empfiehlt den Einsatz von VMFS-5. RDMs und In-Guest-iSCSI sollten nur in Spezialfällen Verwendung finden, die explizit danach verlangen, wie beispielsweise Microsoft Cluster Services (MSCS). Sie führen zu einer beträchtlichen Steigerung der Komplexität virtueller Umgebungen.

VNX-Systeme können blockbasierte Speicherkapazität mit den Protokollen Fibre-Channel over Ethernet (FCoE), Fibre-Channel (FC) oder iSCSI zur Verfügung stellen.

Wahl des Speicherprotokolls

EMC hat keine Präferenzen zur Nutzung von Speicherprotokollen. Vielmehr sollen Sie ein oder mehrere Protokolle passend zu ihren Applikationen zur Anbindung von Speicherkapazität einsetzen. Zu beachten ist, dass der Applikationshersteller unter Umständen ein Protokoll nicht unterstützt (beispielsweise unterstützt Microsoft für Exchange 2007 kein NFS). Ein anderes Beispiel ist, wenn Sie eine Multipathing-Lösung für eine Ihrer Applikationen benötigen. Diese Lösung gibt es nur für blockbasierten Speicher. Performance hingegen ist nur in seltenen Fällen ein Grund, blockbasierten Speicher einzusetzen. Dafür sind die Unterschiede zu marginal. Es ist empfehlenswert, dass Sie eine Matrix ihrer Applikationen nach den folgenden Kriterien erstellen, um die richtige Protokollwahl zu treffen: Unterstützung des Applikationsherstellers, tolerierte Latenz, benötigte Bandbreite, erforderlicher Durchsatz, Multipathing und Path-Failover. Falls Sie ein blockbasiertes Protokoll benötigen, bietet iSCSI eine preiswerte Alternative zu FC oder gar FCoE.

Die meisten Applikationen greifen auf ein Dateisystem des Gastbetriebssystems zu. Eine einfache Möglichkeit, die Performance zu steigern, verspricht die Defragmentierung der

Volumes (Virtual Disks) zu sein. Bevor Sie zu diesem Mittel greifen, klären Sie, auf welche Weise die Speicherkapazität zur Verfügung gestellt wird.

In folgenden Fällen ist von einer hostbasierten Defragmentierung abzuraten:

- TLUs und FAST-VP-LUNs aus einem Storage-Pool sowie komprimierte LUNs
- RG-LUNs, die auf RAID-Gruppen mit Flash-Festplatten liegen
- alle LUNs, die FAST Cache nutzen

Wenn Sie Thin Virtual Disks und Thin Provisioning gleichzeitig einsetzen, ist es ratsam, einen Alarm einzustellen. Gehen Sie im vCenter zu INVENTORY • DATASTORES AND DATASTORE CLUSTERS. Setzen Sie die Alarmwerte entsprechend dem Schwellenwert für den VNX-Storage-Pool. Sie finden letzteren Wert in Unisphere unter STORAGE • STORAGE POOLS • <POOL NAME> • PROPERTIES • ADVANCED • STORAGE POOL ALERT. Die Grundeinstellung ist 70 %.

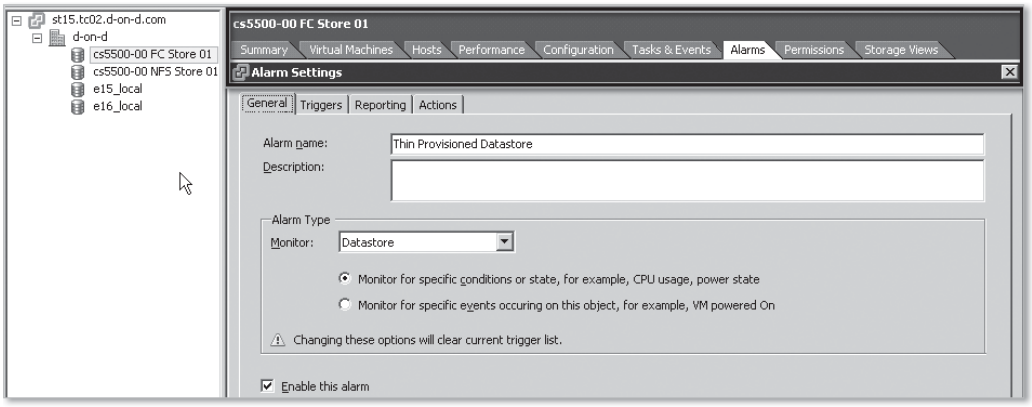


Abbildung 11.31 Konfiguration des Alarms

Im Reiter TRIGGER definieren Sie die Werte für einen Alarm im Falle eines Überprovisionierens und für den Fall, dass die effektive Nutzkapazität den Schwellenwert von 70 % respektive 75 % überschreitet.

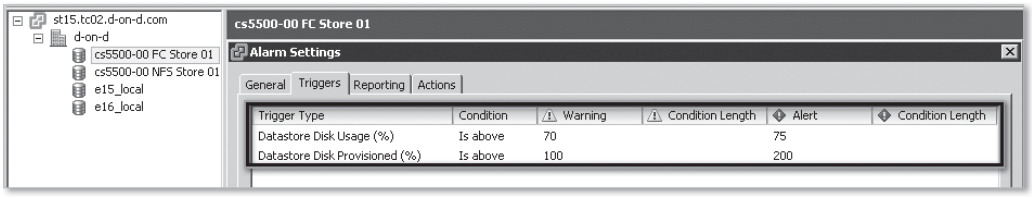


Abbildung 11.32 Definition der Trigger

Sie können sich Benachrichtigungen senden lassen, wenn ein Schwellenwert überschritten wird. Bestätigen Sie Ihre Auswahl mit OK.

Einige Worte zur Einstellung von VMs

Falls Sie iSCSI einsetzen, ist es wichtig, den Zeitüberschreitungswert des Gastbetriebssystems einzustellen Diese Einstellung muss für jedes System einzeln erfolgen. VMware Tools stellt für diesen Wert automatisch 60 Sekunden ein. EMC empfiehlt eine Erhöhung dieses Werts auf 120 Sekunden.

Prozedur für Windows-Betriebssysteme:

1. Gehen Sie auf Start • Ausführen. Tippen Sie »regedit« ein, und klicken Sie auf OK.
2. Suchen Sie in der Baumstruktur HKEY_LOCAL_MACHINE • System • CurrentControlSet • Services • disk.
3. Doppelklicken Sie auf auf TimeOutValue. Setzen Sie den Wert 120 (Decimal), und klicken Sie auf OK.
4. Booten Sie die virtuelle Maschine.

Performance-Charakteristik von virtuellen Umgebungen

Vor der großflächigen Einführung von virtuellen Umgebungen wurden hochkomplexe und inflexible Speichersystem-Layouts passend auf die Performance-Charakteristika der wichtigsten Applikationen vorgeschlagen. Solche Designs können in virtuellen Umgebungen auch abgebildet werden. Applikationen und Datenbanken können ein oder mehrere Threads nutzen. Aufgrund einer hohen Konsolidierung mit der virtuellen Abbildung von Serversystemen und ihren Applikationen ist das I/O-Profil für das Speichersystem randomisiert, und es müssen gleichzeitig mehrere Threads bedient werden.

VMFS-5 arbeitet mit einer Sub-Block-Größe von 8 KB und einer Blockgröße von 1 MB. Daher ist eine VNX für den Betrieb in einer virtuellen Umgebung auf »multiple threads, small block, random IO« zu optimieren.

Hintergrundwissen zur Blockgröße von VNX

Die Grundeinstellung der RAID-Group-Stripe-Block-Size ist 64 KB. Bei RAID 5 (4+1) nutzen Sie somit eine Stripe-Size von 256 KB. Vermeiden Sie RAID-Konfigurationen mit ungeraden Zahlen (beispielsweise RAID 1/0 [3+3]).

Anbindung der ESXi-Server

VNX ist ein Speichersystem mit zwei Storage-Processors (SP). Beide SPs sind aktiv. Aus Sicht einer VNX-LUN wird diese von nur einem SP aktiv bedient. Das wird als *optimierter Pfad und LUN-Ownership* bezeichnet. Daher spricht man von einem Active/Passive-System. Fällt der aktive Pfad von einem Host zu einer LUN aus, so hat dies einen systeminternen Pfad-Failover zur Folge. Man spricht von *LUN-Trespassing*. Ein *LUN-Trespassing* kann häufiger auftreten, als man denkt, beispielsweise bei Wartung am SAN und Ändern eines Zonesets. Um das LUN-

Trespassing in solchen Fällen zu verhindern, empfiehlt EMC, ALUA einzusetzen. ALUA wird seit vSphere 4.0 unterstützt.

VMware Native Multipathing Round-Robin (VMW_PSP_RR)

Stellen Sie sicher, dass NMP den SATP auf `VMW_SATP_ALUA` und den PSP auf `VMW_PSP_FIXED` gesetzt hat. Die heutige Implementation unterstützt derzeit keine automatisierte Wiederherstellung der Original-Pfade (*Auto-Restore*) der LUNs. Das heißt, falls ein LUN-Trespassing auftritt, wird die LUN nicht an den ursprünglichen SP (Default-Owner) zurückgegeben. Daher ist vom Einsatz von `VMW_PSP_RR` zur Lastverteilung mittels Round-Robin mit vSphere 5.0 abzuraten.

Sollten Ihre ESXi-Server über mehr als zwei Host-Bus-Adapter oder Netzwerkkarten für Datenverkehr verfügen, so empfiehlt EMC den Einsatz von PowerPath/Virtual Edition (PPVE). PPVE ist ein Third-Party-Multipath-Plugin und Path-Failover-Werkzeug. Es erlaubt die aktive Nutzung von bis zu 32 Pfaden. Sie können PPVE für alle Block-Protokolle nutzen.

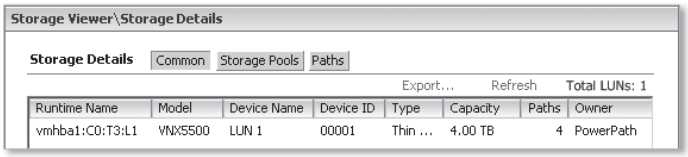


Abbildung 11.33 Informationen eines VMFS-Datastores mit PPVE

Eine Lastverteilung können Sie nicht nur mit dem Einsatz von Multipathing-Werkzeugen erreichen, sondern auch mit Storage Dynamic Resource Scheduling (SDRS). SDRS ist nicht mit einer FAST-Technologie gleichzusetzen. Es ist ein Mechanismus zur Lastverteilung basierend auf I/O und Kapazität. Wenn Sie SDRS nutzen wollen, empfiehlt EMC, dass Sie paarweise, symmetrische Datastores mit äquivalenten Kapazitäts- und Performance-Charakteristiken erstellen. Wählen Sie die LUNs von unterschiedlichen RAID-Gruppen oder Storage-Pools aus. Diese sollten regelmäßig über die beiden SPs verteilt sein. Das Ziel ist es, die I/O-Last der Datastores zu gleichmäßig zu verteilen.

Verwendung von SDRS I/O Metric

Verwenden Sie FAST-VP-Storage-Pools oder mehrere LUNs vom selben Storage-Pool, müssen Sie SIOC in den SDRS Runtime Rules deaktivieren. Genannte Storage-Pools verfügen über zwei oder mehr unterschiedliche Festplattentypen, die sich durch unterschiedliche Latenzzeiten auszeichnen. Das kann zu unnötigen Storage-vMotion-Tätigkeiten sowie zur unerwünschten Promotion von Slices in einen höheren Tier führen.

Belassen Sie die Migrations-Richtlinien von SDRS über einen gewissen Zeitraum im manuellen Modus, und beobachten Sie das Verhalten, um die beste Einstellung zu finden. Danach können Sie SDRS vollständig automatisieren. Verwenden Sie auf den LUNs mit SDRS eine LUN-basierte Replikation, dann empfiehlt es sich, die manuelle Einstellung beizubehalten.

Tabelle 11.4 bietet Ihnen eine Hilfestellung zum Einsatz mit SDRS:

VNX-Funktion	initiale Platzierung	Migrationsempfehlung
TLU	ja	unterstützt mit VASA
DLU, RG-LUN	ja	ja
FAST VP	ja	nein, manueller Modus[1]
FAST	ja	nein, manueller Modus[1]
Replikation	ja	nein, manueller Modus[1]
LUN-Snapshot	ja	nein
Deduplikation	ja	nein, führt zur Inflation

Tabelle 11.4 Einsatz von SDRS

Gehen Sie in Unisphere auf STORAGE • STORAGE POOLS, und klicken Sie auf PROPERTIES, um das Tiering-Verhalten des Storage-Pools einzustellen.

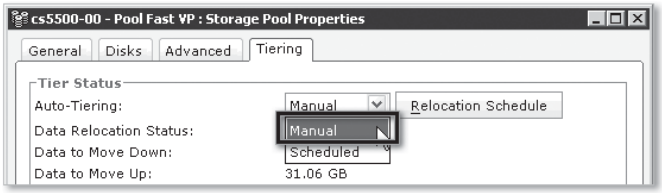


Abbildung 11.34 Umschalten des Tiering-Verhaltens

Sollten Sie gemäß Tabelle 11.4 eine VNX-Funktion mit der SDRS-Migrationsempfehlung »manuell« verwenden, können Sie die Relokation der Daten den Eigenschaften des entsprechenden Storage-Pools entnehmen. Passen Sie den Status gegebenenfalls wie in Abbildung 11.34 an.

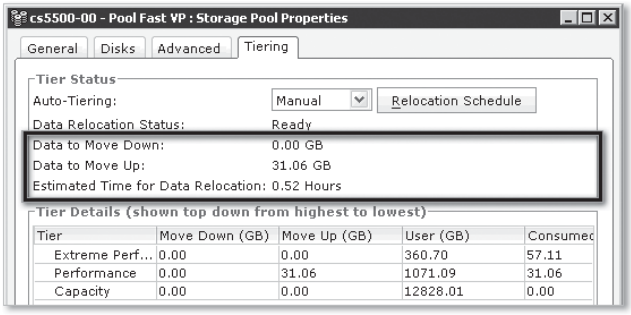


Abbildung 11.35 Empfohlene Relokation der Daten

1 Siehe auch VMware-Knowledge-Base-Artikel 1020651 zu Storage I/O Control. (*http://kb.vmware.com/kb/1020651*)

In Abbildung 11.35 sehen Sie die geschätzte Zeit für die Migration von Slices ab. Sie können die Datenrelokation manuell ansteuern. Klicken Sie mit der rechten Maustaste auf den gewünschten Storage-Pool, und wählen Sie Auto-Tiering • Start Data Relocation.

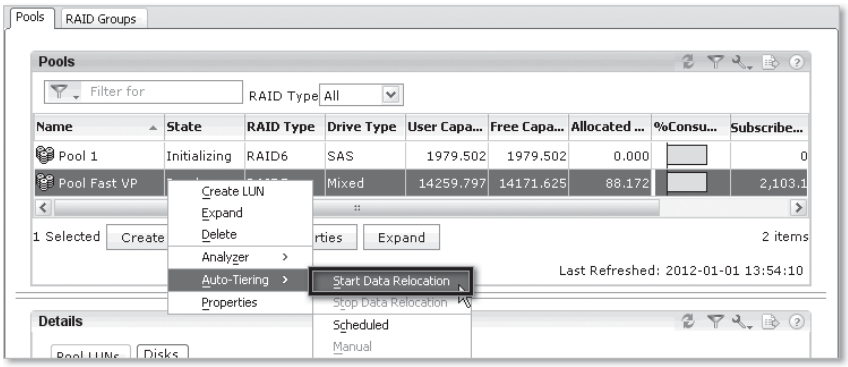


Abbildung 11.36 Starten der Relokation von Daten eines Storage-Pools

Für den Betrieb von SDRS mit TLUs ist es notwendig, vSphere API for Storage Awareness (VASA) einzusetzen. VASA gibt Auskunft über die Fähigkeiten von Speichersystemen. Entweder holt sich VASA Informationen vom Speichersystem, oder Sie nutzen die Möglichkeit, *VASA Storage Capabilities* selbst zu definieren. Die Implementation von VASA beruht auf dem SMI-S-Standard. SMI-S kann nicht zwischen unterschiedlichen Storage-Pools unterscheiden und klassifiziert diese als Tiered Storage. Auch NFS ist darin nicht definiert. In Fällen, wo VASA keine native Unterstützung bietet, ist es sinnvoll, eigene VASA Storage Capabilities zu hinterlegen. Sie erfahren in Abschnitt 11.4.2, »Installation von VASA«, wie Sie VASA installieren.

Tabelle 11.5 gibt Aufschluss über die Zuordnung, die VASA vornimmt:

VNX-LUN-Type	Anzeige im vCenter
LUN einer Flash-Festplatte	Extreme Performance
Storage-Pool-LUN	Tiered Storage
FAST	Tiered Storage
RG-LUN	Capacity
NFS	Unsupported

Tabelle 11.5 Zuordnung des Speichertyps in VASA

Gehen Sie über Home • Management • VM Storage Profiles, um Ihr erstes Speicherprofil zu erstellen. Klicken Sie auf Create VM Storage Profile. Benennen Sie das Speicherprofil, und wählen Sie Mixed aus den Möglichkeiten aus. Beenden Sie den Wizard mit Finish. Gehen Sie nun auf Enable VM Storage Profile, und aktivieren Sie dieses in Ihrem Cluster.

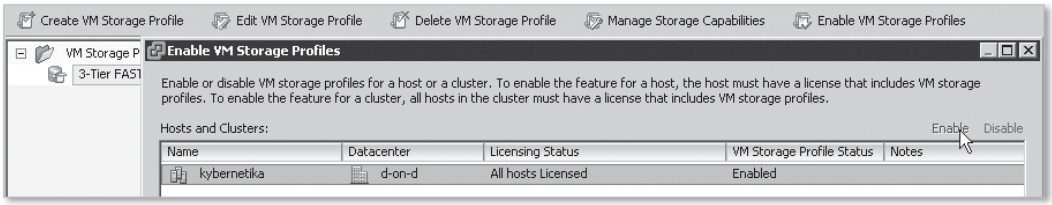


Abbildung 11.37 Aktivieren des Speicherprofils

Gehen Sie nun auf HOME • VMS AND TEMPLATES, und wählen Sie eine virtuelle Maschine, die auf den Storage-Pools mit FAST zugreift. Editieren Sie die Eigenschaften der virtuellen Maschine. Dazu klicken Sie auf den Reiter PROFILES und wählen das VM-Speicherprofil aus. Bestätigen Sie Ihre Wahl mit einem Klick auf PROPAGATE.

Wiederholen Sie diesen Vorgang für sämtliche virtuelle Maschinen Ihres ESX-Clusters. Achten Sie darauf, dass Sie nur VM-Speicherprofile mit virtuellen Maschinen assoziieren, die auf den passenden Datastore zugreifen. Die Angabe über die Storage-Characteristic eines VMFS-Datastores erfahren Sie am einfachsten über HOME • DATASTORES AND DATASTORE CLUSTERS.

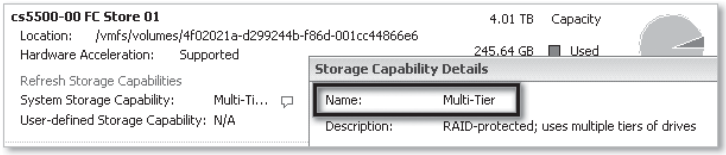


Abbildung 11.38 Charakteristik eines VMFS-Datastores

Speicherprofile und fehlerhafte Assoziationen

Sollten virtuelle Maschinen mit einem VM-Speicherprofil assoziiert sein, das nicht auf sie passt, so hat dies eine Statusmeldung zur Folge. Die virtuelle Maschine wird als »non-compliant« markiert. Sie können den Status jederzeit via CENTER • HOME • VM STORAGE PROFILES • »NAME: STORAGE PROFILE« • VIRTUAL MACHINES überprüfen.

Nun haben Sie zwei Optionen: Entweder Sie migrieren die VM mittels Storage vMotion, oder Sie editieren die Einstellungen der VM.

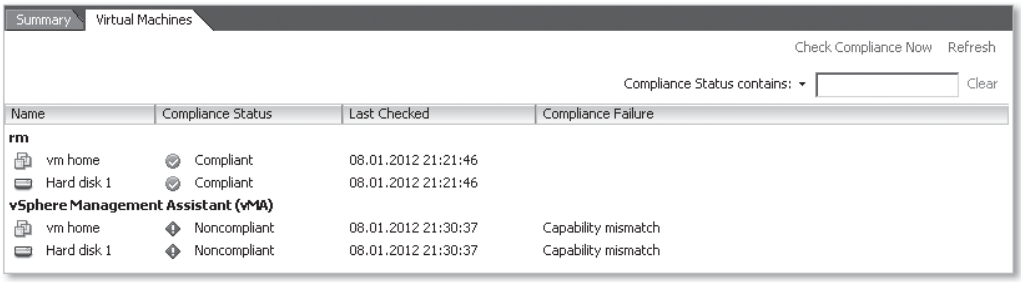


Abbildung 11.39 Compliance-Check von VASA

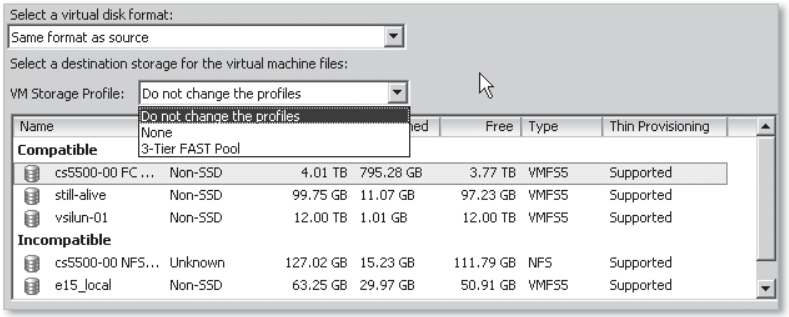


Abbildung 11.40 Optionen von Storage vMotion mit VASA

Wie erwähnt bietet VASA derzeit nicht für jeden Anwendungsfall ein Systemprofil. Deshalb haben Sie die Möglichkeit, eigene Profile zu erstellen. Dazu gehen Sie auf HOME • MANAGEMENT • VM STORAGE PROFILES • MANAGE STORAGE CAPABILITIES und klicken auf ADD, um eine eigene Storage-Capability zu definieren. Erstellen Sie das VM-Speicherprofil über CREATE VM STORAGE PROFILE. Nun steht das zweite VM-Speicherprofil zur Auswahl. Sie müssen die neu erstellte Storage-Capability noch den passenden Datastores zuweisen. Erst dann ist es sinnvoll, das VM-Speicherprofil mit den virtuellen Maschinen zu assoziieren.

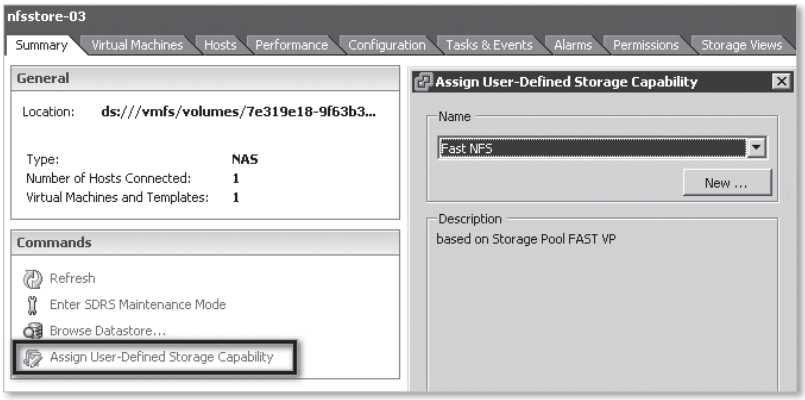


Abbildung 11.41 Zufügen einer Storage-Capability zu einem Datastore

Charakteristisch für das I/O-Verhalten virtueller Umgebungen ist, dass sie einen hohen Grad an gleichzeitigen I/O-Anfragen aufweisen. Das resultiert in einer stetig hohen Nutzlast der Systemressourcen (HBA, Schnittstellen zum SAN und LUN). Können diese I/O-Anfragen nicht sofort vom System (Host oder Speichersystem) abgearbeitet werden, landen sie in einer Warteschleife (*Queue*). Sie weist eine Obergrenze in Abhängigkeit auf. Ist diese erreicht, antwortet der HBA, die Schnittstelle vom Speichersystem oder die betroffene LUN mit »QFULL« (»queue full«). Normalerweise reagiert der Host mit einer Wartezeit von etwas mehr als einer Sekunde. Tritt dies häufiger auf, beeinträchtigt das die Performance.

»Queue-Depth eines ESXi-Hosts« – »Disk.SchedNumReqOutstanding«

In den ADVANCED CONFIGURATION eines ESXi-Hosts finden Sie den Parameter DISK.SCHEDNUMREQOUTSTANDING. Die Grundeinstellung ist 32. Sie können diesen Parameter auf den Maximalwert von 256 erhöhen. Verwenden Sie `resxtop` über einen längeren Zeitraum, um die benötigte Queue-Depth (maximale Anzahl der ausstehenden IOs) zu bestimmen. Vorsicht ist geboten, da eine Fehlmanipulation dieser Einstellung die Performance beeinträchtigen kann. Es ist empfehlenswert, nur dann die Grundeinstellung zu ändern, wenn sämtliche anderen Tuning-Möglichkeiten bereits ausgeschöpft sind.

Der VMware-Knowledge-Base-Artikel 1008205 gibt Auskunft zur Bedienung von *resxtop* zur Analyse der Storage-Performance (*http://kb.vmware.com/kb/1008205)*. Diesen Parameter können Sie in VCENTER • ESXI-SERVER • CONFIGURATION • ADVANCED SETTINGS anpassen.

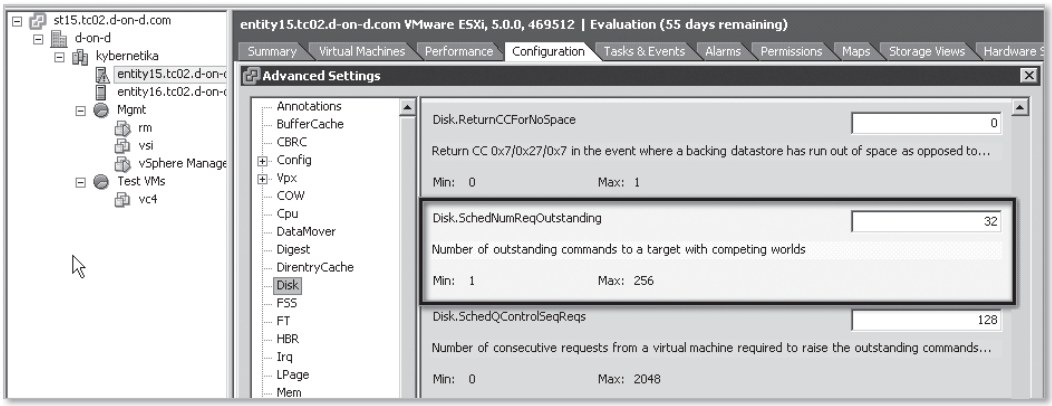


Abbildung 11.42 Anpassen des Parameters für die LUN-Queue-Depth

Um die richtige Queue-Depth-Einstellung Ihrer ESXi-Hosts zu setzen, müssen Sie nebst der Anzahl der Hosts, die vom Speichersystem bedient werden, auch die Limits des Speichersystems kennen. Jede Festplatte verfügt über dieselbe Queue-Depth. Der Frontend-Port-Treiber (Schnittstellentreiber zum SAN) wird ein QFULL rapportieren, wenn eine von zwei Konditionen eintritt:

- Das maximale Queue-Limit von 2.048 ist erreicht (planen Sie konservativ mit dem Wert 1.600).
- Das maximale Queue-Limit einer LUN ist erreicht. Sie errechnet sich aus:
  14 × (Anzahl Festplatten abzüglich Parität) + 32
  (Beispiel RAID 5 (4+1): 14 × 4 + 32 = 88)

Vor allem im ESX-Cluster-Betrieb, wo mehrere ESXi-Server auf dieselbe LUN zugreifen, kann eine Erhöhung des Parameters – DISK.SCHEDNUMREQOUTSTANDING negative Folgen haben. Mit dem Unisphere Analyzer, einem Werkzeug der VNX, können Sie Statistikwerte über Queues sammeln.

Den Unisphere Analyzer rufen Sie über System • Hardware • Storage Hardware • SPs • SPA • Analyzer • Performance Details auf.

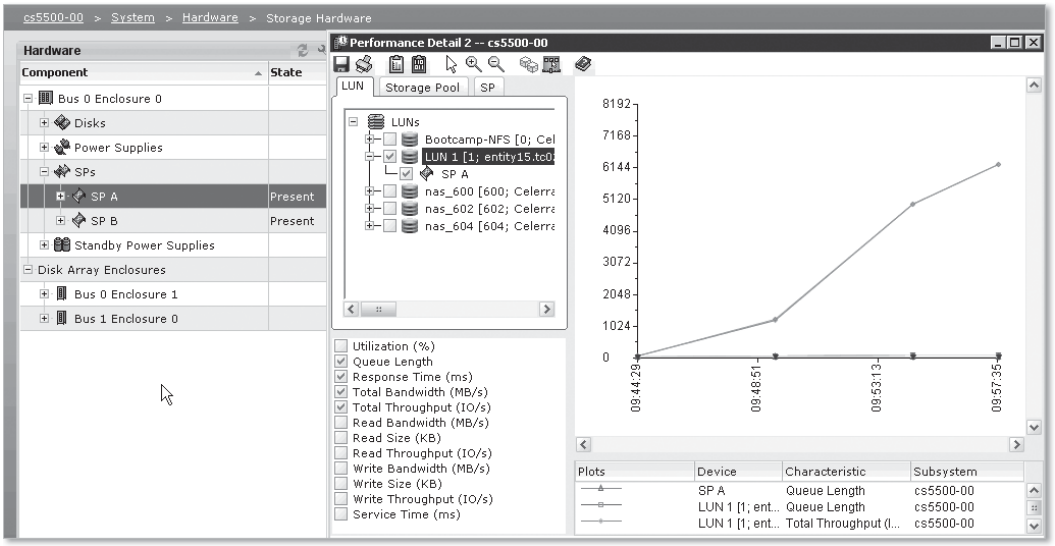


Abbildung 11.43 Unisphere Analyzer

Storage I/O Control (SIOC) gibt Ihnen ein dynamisches Werkzeug zur Kontrolle und Priorisierung der I/O-Anfragen Ihrer virtuellen Maschinen auf Host-Ebene an die Hand. SIOC arbeitet mit Schwellenwerten für die Latenz (Congestion Threshold). Wird ein solcher Schwellenwert übertreten, so wird SIOC die Zuweisung der I/O-Anforderungen einzelner virtueller Maschinen gemäß deren Shares in den I/O-Queues der NFS oder VMFS-Datastores priorisieren.

Tabelle 11.6 listet die von EMC empfohlenen Werte für den Congestion Threshold von SIOC auf.

Speichertyp	Congestion Threshold	Bemerkungen
Flash-Festplatten	10–20 ms	–
SAS-Festplatten	20–30 ms	–
FAST VP/Storage-Pool-LUNs (tiered)	35–50 ms	Der einzustellende Wert hängt von der Verteilung der Festplattentypen im Pool ab.
NFS	30 ms	Nutzen Sie im Netzwerk auch QoS und für den vDS NIOC. Wenden Sie Best Practices für NFS im Netzwerk an.

Tabelle 11.6 Empfehlungen für Storage-I/O-Control-Einstellungen

SIOC ist nicht unterstützt für folgende Konfigurationen:

- VMware RDM
- Datastores mit mehreren Extents

Für den Einsatz von SIOC ist es empfehlenswert, im Speichersystem RAID-Groups und Storage-Pools der virtuellen Umgebungen zu dedizieren. SIOC erkennt auch I/O-Lasten, die nicht vSphere betreffen. Für nähere Informationen konsultieren Sie den VMware-Knowledge-Base-Artikel 1020651 (*http://kb.vmware.com/kb/1020651*). Passen Sie den Congestion Threshold-Wert entsprechend den Eigenschaften des Datastores an (Abbildung 11.44).

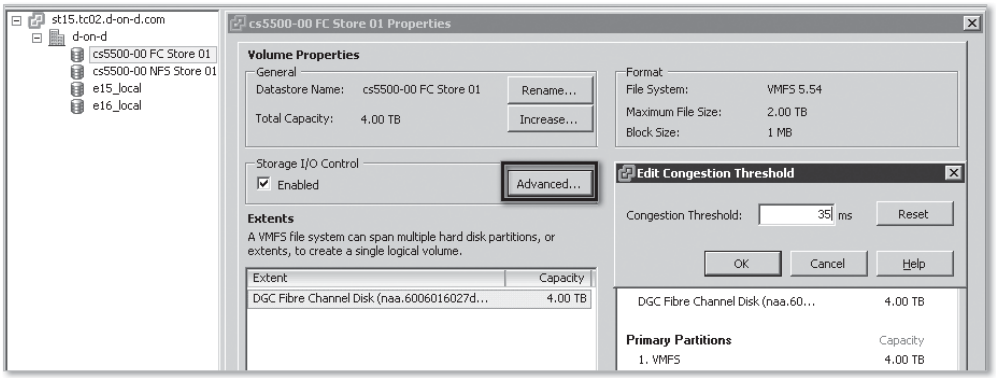


Abbildung 11.44 Ändern des Werts für »Congestion Threshold«

Das VNX-System unterstützt nebst VASA auch vSphere API for Array Integration (VAAI). Das Speichersystem unterstützt alle VAAI-Primitives sowohl für block- als auch für dateibasierten Speicher. Die Vorzüge von VAAI sind in Abschnitt 9.12 ausführlich erklärt. Darin behandeln wir die Advanced Settings behandelt, die pro ESXi-Server aktiviert sein müssen. Bevor Sie verifizieren, dass die VAAI-Primitives vom Speichersystem unterstützt sind, überprüfen Sie, ob die notwendigen Parameter in den Advanced Settings Ihrer ESXi-Server eingeschaltet sind.

Zur Überprüfung, dass die VAAI-Primitives eingeschaltet sind, wählen Sie sich in den vSphere Management Assistant (vMA) ein.

Mit `vifptarget` gestalten Sie die Befehlseingabe ein wenig leichter und ersparen sich Zeit:

```
vi-admin@vcenter:/[entity15.tc02.d-on-d.com]> vifptarget --set entity15
```

Tippen Sie folgende Befehlszeile ein, um zu sehen, ob das VNX-System über eine VAAI-Integration verfügt:

```
vi-admin@vcenter:/[entity15.tc02.d-on-d.com]> esxcli storage core plugin list
Plugin name   Plugin class
------------  ------------
VMW_VAAIP_CX  VAAI
```

```
VAAI_FILTER   Filter
NMP           MP
vi-admin@vcenter:/[entity15.tc02.d-on-d.com]>
```

Der folgende Befehl zeigt auf, ob ein Datastore VAAI unterstützt:

```
vi-admin@vcenter:/[entity15.tc02.d-on-d.com]> esxcli storage core device list
naa.6006016027d02c009eadc0883e35e111
Display Name: DGC Fibre Channel Disk (naa.6006016027d02c009eadc0883e35e111)
Has Settable Display Name: true
Size: 4194304
Device Type: Direct-Access
Multipath Plugin: NMP
Devfs Path: /vmfs/devices/disks/naa.6006016027d02c009eadc0883e35e111
Vendor: DGC
Model: VRAID
Revision: 0531
SCSI Level: 4
Is Pseudo: false
Status: on
Is RDM Capable: true
Is Local: false
Is Removable: false
Is SSD: false
Is Offline: false
Is Perennially Reserved: false
Thin Provisioning Status: yes
Attached Filters: VAAI_FILTER
VAAI Status: supported
Other UIDs: vml.0200010000006006016027d02c009eadc0883e35e111565241494420
```

Nutzen Sie den folgenden Befehl, um die unterstützten VAAI-Primitives pro Datastore anzuzeigen:

```
vi-admin@vcenter:/[entity15.tc02.d-on-d.com]> esxcli storage core devicevaai
  status get
naa.6006016027d02c009eadc0883e35e111
VAAI Plugin Name: VMW_VAAIP_CX
ATS Status: supported
Clone Status: supported
Zero Status: supported
Delete Status: supported
...
vi-admin@vcenter:/[entity15.tc02.d-on-d.com]>
```

Eine der interessanteren VAAI-Primitives ist mit Sicherheit *VAAI UNMAP*, da es verspricht, nicht genutzte Blöcke wieder freizugeben, was (vor allem) kommt bei Thin Provisioning zum Zug kommt.

Um den Effekt von VAAI UNMAP nachzuvollziehen, führen Sie das folgende kleine Beispiel durch:

1. Erstellen Sie einen VM-Snapshot einer virtuellen Maschine Ihrer Wahl. Im Beispiel verwenden wir Windows 2008.
2. Erstellen Sie eine 4 GB große Datei, beispielsweise mit `rktools createfil bulkdata 4194303`.
3. Beobachten Sie danach die Kapazitätsangaben der VM, des Datastores und der zugehörigen Thin-provisioned LUN.
4. Löschen Sie den VM-Snapshot.
5. Beobachten Sie die neuen Kapazitätsangaben.

Die folgende Bilderreihe dokumentiert den Effekt von VAAI UNMAP – wie Sie sehen, hält VAAI UNMAP, was es verspricht.

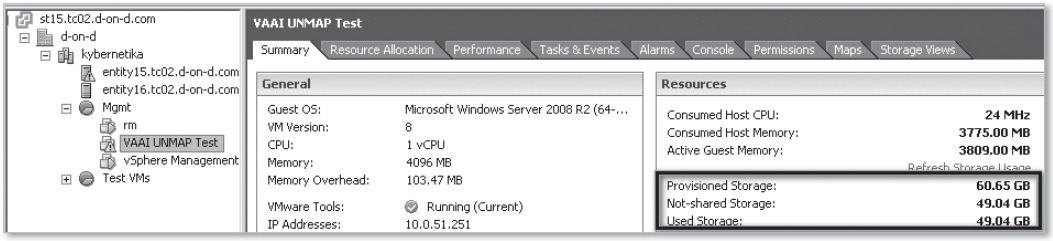


Abbildung 11.45 Kapazitätsangaben der VM vor UNMAP

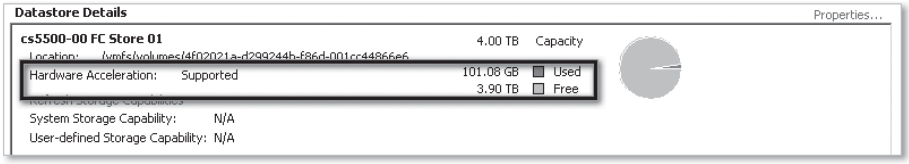


Abbildung 11.46 Kapazitätsangaben des VMFS-Datastores vor UNMAP

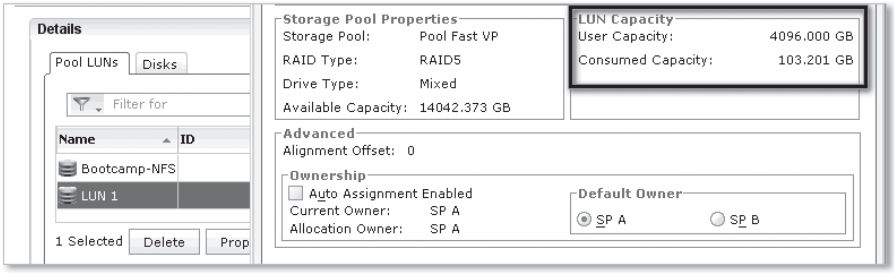


Abbildung 11.47 Kapazitätsangaben der TLU vor UNMAP

Abbildung 11.48 Kapazitätsangaben der VM nach UNMAP

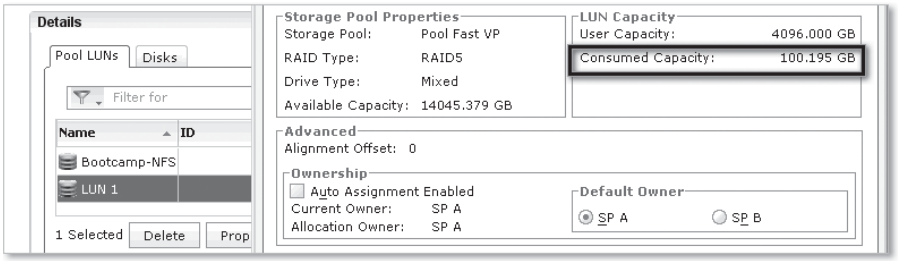


Abbildung 11.49 Kapazitätsangaben der TLU nach UNMAP

VAAI UNMAP im produktiven Einsatz

Zu diesem Zeitpunkt raten sowohl VMware als auch EMC von einem Einsatz von VAAI UNMAP in Produktionsumgebungen ab. In intensiven Tests wurden Performanceschwierigkeiten festgestellt. Dabei handelt es sich nicht um ein EMC-spezifisches Problem, sondern es betrifft alle Speichersysteme mit VAAI-Unterstützung. Im VMware-Knowledge-Base-Artikel 2007427 finden Sie nähere Informationen (*http://kb.vmware.com/kb/2007427*).

Nutzen Sie diesen Befehl in der vMA, um VAAI UNMAP zu deaktivieren:

```
vi-admin@vcenter:/[entity16.tc02.d-on-d.com]> esxcli system settings advanced set
--int-value 0 --option /VMFS3/EnableBlockDelete
```

Führen Sie diesen Befehl für jeden einzelnen ESXi-Host durch. Mit folgendem Befehl können Sie die Einstellung überprüfen:

```
vi-admin@vcenter:/[entity16.tc02.d-on-d.com]> esxcli system settings advanced
list --option /VMFS3/EnableBlockDelete

Path: /VMFS3/EnableBlockDelete
Type: integer
Int Value: 0
Default Int Value: 1
Min Value: 0
Max Value: 1
String Value:
Default String Value:
Valid Characters:
Description: Enable VMFS block delete
```

Netzwerkanbindung im FC-SAN

Die folgenden Faktoren beeinflussen die Performance im Netzwerk:

- Geschwindigkeit der Switch-Ports
- Überbuchung der Ports (abhängig vom Hersteller und Switch-Typ)
- Anzahl der Interswitch-Links
- IP-Verbindungen zwischen Switches (bei der Replikation über große Distanzen oder beim Einsatz von iSCSI)

EMC vertritt für die Anbindung von FC-SAN das Konzept zweier unabhängiger Fabrics (A und B). So können Sie problemlos Wartungsarbeiten am SAN vollziehen, ohne dass die Applikationen die Konnektivität zum Speichersystem verlieren und deswegen heruntergefahren werden müssten. Das Zoning des SAN sollte immer nach dem Schema »single Initiator, single Target« erfolgen.

Idealerweise verbinden Sie mindestens zwei Schnittstellen eines Storage-Processors mit dem SAN und schließen den einen an Fabric A und den anderen an Fabric B an. Verfahren Sie genauso mit dem zweiten Storage-Processor (siehe auch Abbildung 19.17 im Bonus-Kapitel auf der Website).

Performance im FC-SAN

Reduzieren Sie für die beste Performance im SAN die Anzahl der Hops vom Server zum Speichersystem. Unter Umständen müssen Sie beim Unterhalt größerer SANs die Anschlüsse eines Storage-Processors so verteilen, dass stark ausgelastete Verbindungen auf demselben Switch liegen. In SAN-Core-Edge-Architekturen werden Speichersysteme typischerweise direkt an den Core angeschlossen. Das garantiert immer gleich lange Wege zwischen Speichersystem und Server. Empfehlenswert ist es, die Anschlüsse des Speichersystems mit Switch-Ports ohne Überbuchung zu verbinden. Serversysteme sind im Normalfall weniger ausgelastet und können auf die übrigen Switch-Ports verteilt werden.

Netzwerkanbindung im IP-SAN

Die Ethernet-Infrastruktur sollte mindestens 1 GB unterstützen, und es ist empfehlenswert, zwei getrennte physische Netzwerke einzusetzen. Ist das nicht möglich, so isolieren Sie den iSCSI-Verkehr der Switches mit VLANs. Nutzen Sie immer redundante Anschlüsse für iSCSI (zwei Schnittstellen). Vermeiden Sie geroutete und Multi-Hop-Netzwerke. Verwenden Sie für 1-GB-Ethernet-Netzwerke ausschließlich Kabel des Typs CAT 5e oder CAT 6 mit möglichst geringer Kabellänge (die Latenz erhöht sich, je länger das Kabel). Schalten Sie die Auto-Negotiation-Einstellungen zu Pause-Frames aus, und setzen Sie eine fixe Geschwindigkeit der Schnittstelle. Konfigurieren Sie sämtliche beteiligte Geräte mit »full duplex«, und achten Sie darauf, dass »TCP Flow Control« eingestellt ist. Unicast und Spanning Tree Protocol (STP) sind auf den Switch Ports, die iSCSI-Verkehr (iSCSI Initiator und Target) handhaben, auszuschalten. Falls Ihre Ethernet-Infrastruktur Quality of Service (QoS) unterstützt, so ist es empfehlens-

wert, den iSCSI-Verkehr zu priorisieren. Sollten Sie Virtual Distributed Switches (vDS) verwenden, so aktivieren Sie Network I/O Control (NIOC), und stellen Sie einen hohen Wert für iSCSI-Traffic-Shares (beispielsweise 75) ein. Limitieren Sie bei einer Überlastung zusätzlich die Bandbreite von vMotion-Traffic.

Performance im IP-SAN

Wählen Sie Netzwerkkarten und Ethernet-Switches, die Jumbo-Frames unterstützen. Konfigurieren Sie die Maximal Transfer Unit (MTU) von 9.000 auf allen Geräten vom Speichersystem bis zum Gast (für »In-Guest-iSCSI«).

Deaktivieren Sie am ESXi-Host die Einstellung zu DelayedACK Sie benötigen dafür das Privileg: »Host.Configuration.Storage Partition Configuration«.

Prozedur für ESXi-Server:

1. Öffnen Sie die Dialogbox iSCSI Initiator Properties.
2. Wählen Sie den Reiter General, und klicken Sie auf Advanced. Um auf der Initiator-Ebene Einstellungen vorzunehmen, gehen Sie zu Schritt 6. Um auf der Target-Ebene Einstellungen vorzunehmen, gehen Sie zu Schritt 3.
3. Sie können auf der Target-Ebene die Advanced Parameters nur für software- und hardwareabhängige iSCSI-Adapter ändern.
4. Wählen Sie entweder den Reiter Dynamic Discovery oder Static Discovery (das hängt davon ab, wie Sie iSCSI in Ihrem Unternehmen einsetzen).
5. Wählen Sie eines der verfügbaren Targets aus der Liste, und klicken Sie auf Settings • Advanced.
6. Deaktivieren Sie den Advanced Parameter DelayedAck, und klicken Sie auf OK, um die Einstellung vorzunehmen.

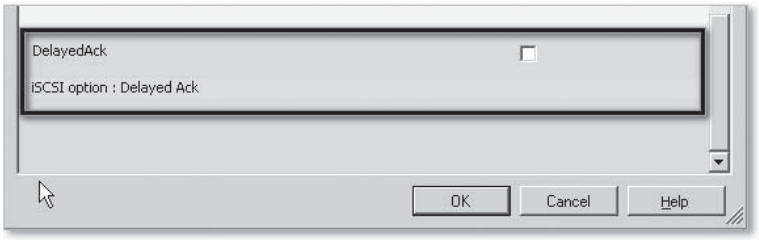


Abbildung 11.50 Deaktivieren von TCP Delayed Acknowledge

Wichtig ist es, zusätzlich die iSCSI-Timeouts von vSphere ESXi und der Gastbetriebssysteme einzustellen. Diese Einstellung muss für jedes System einzeln erfolgen.

Prozedur für Windows-Betriebssysteme (Timeout für 120s):

1. Gehen sie auf START • AUSFÜHREN. Tippen Sie »regedit« ein, und klicken Sie auf OK.
2. Suchen Sie in der Baumstruktur HKEY_LOCAL_MACHINE • SYSTEM • CURRENTCONTROLSET • SERVICES • DISK.
3. Doppelklicken Sie auf den TIMEOUTVALUE. Setzen Sie den Wert 120 (DECIMAL), und klicken Sie auf OK.
4. Booten Sie die virtuelle Maschine.
5. Alternativ: Schreiben Sie den Befehl: `reg.exe add \\%1\HKLM\SYSTEM\CurrentControlSet\Services\Disk /V TimeoutValue /t /REG_DWORD /d 120 /f".`

Mit der Virtual Port-Technologie stehen einem VNX-System maximal 32 Ports pro Storage-Processor zur Verfügung. VLAN-Tagging (IEE 802.1q) wird sowohl für iSCSI als auch für NFS unterstützt. Nutzen Sie niemals das Subnetz 192.168.0.0/16, da es für die Management-Kommunikation von VNX vorgesehen ist. Auf den iSCSI-Frontend-Port des VNX-Systems sollten keine Gateways definiert sein. Falls ein Routing nicht vermieden werden kann, müssen die Routen fest definiert werden. Definieren Sie eigene Subnetze für SP-Ports. Am besten verwenden Sie zwei Subnetze, die Sie wie in Abbildung 11.51 ersichtlich anschließen.

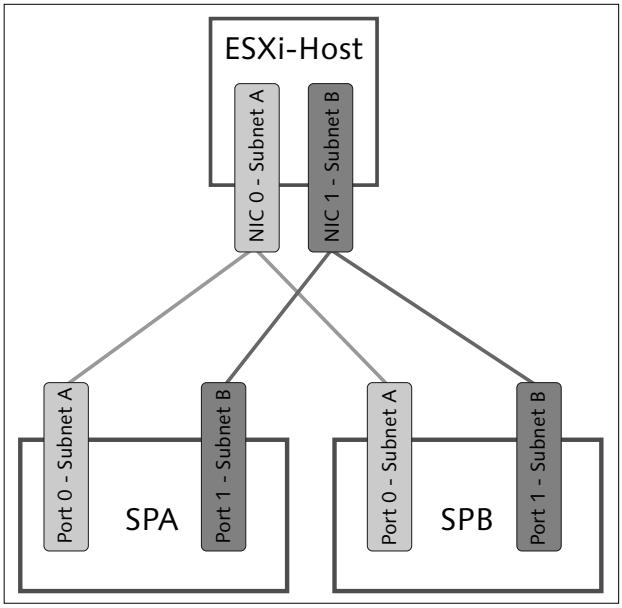


Abbildung 11.51 Ausgekreuzte Verbindungen mit unterschiedlichen Subnetzen

Verwenden Sie iSCSI als eine Alternative in den Fällen, wo Sie blockbasierten Zugriff benötigen, da die Applikation explizit *Fibre-Channel* verlangt. Die ESXi-Implementation von iSCSI hat die Eigenschaft, dass nur eine Datenverbindung zwischen einem ESXi Server und einem einzelnen Speicherziel (Initiator zu Target) aufgebaut wird. Im Gegensatz zu NFS können Sie

Multipathing-Lösungen (entweder NMP oder PPVE) einsetzen. Dafür benötigen Sie zwei VMkernel-Ports und zwei Ethernet-Schnittstellen. Letztere müssen als Uplink für je einen VMkernel-Port konfiguriert werden. Auf Seiten des Speichersystems sollten zwei iSCSI-Targets aufgetrennt auf die beiden SPs definiert sein. Idealerweise erfolgt der Anschluss über zwei physische Ethernet-Switches. Verbinden Sie Ihr VNX-System so, dass sich ein Initiator auf zwei Targets einwählt. Dem Initiator sind zwei iSCSI-Ports zugewiesen.

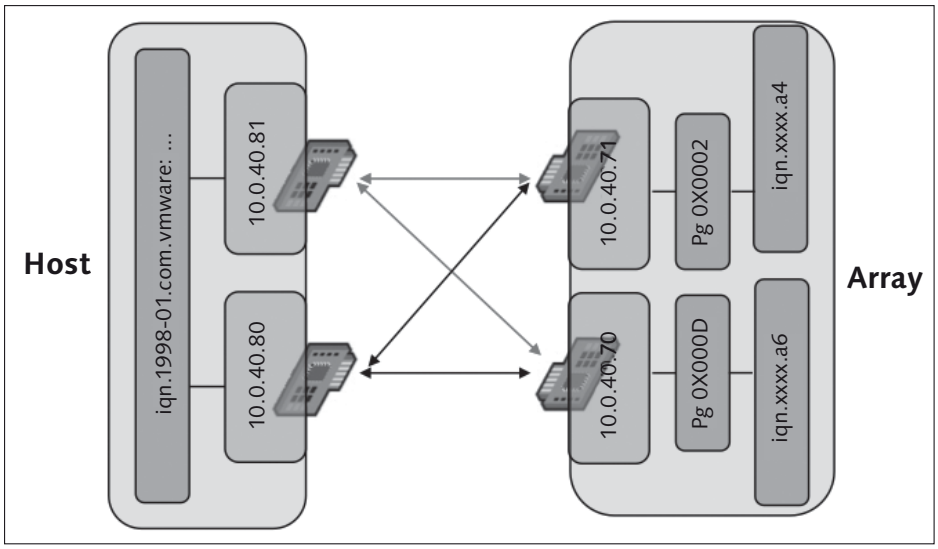


Abbildung 11.52 Beziehung zwischen Initiator und Target

11.2.4 Einleitung zu VNX-dateibasierten Speicheroptionen

Mit Hilfe der dateibasierten Speicheroption können Sie nebst der blockbasierten Anbindung auch NFS-Datastores in ihrer virtuellen Umgebung betreiben. Die dateibasierte Anbindung von Datastores gewinnt zusehends an Popularität. Deshalb ist es wichtig zu verstehen, wie Sie eine VNX optimal auf diesen Einsatz vorbereiten.

Um den Verwaltungsaufwand der dateisystembasierten Speicheranbindung einfach zu halten, gibt es im VNX Operating Environment for File (OE) einen Volume-Manager. Dieser kann mit RG-LUNs, TLUs und DLUs umgehen. Wenn Sie Dateisysteme möglichst effizient nutzen wollen, gilt es, Best Practices zur Konfiguration einzuhalten.

Der Volume Manager führt neue Begriffe ein, um zwischen block- und dateibasierten Speicherkapazitäten zu unterscheiden:

- **Disk Volume** (»dvol«) – physische, blockbasierte Speichereinheit, bezeichnet eine LUN
- **Stripe-Volume** – eine Anordnung von Volumes, die als ein einzelnes Volume wiedergegeben werden
- **Slice-Volume** – eine logische Einheit oder spezifizierte Zone eines Volumes, um kleinere, besser verwaltbare Speichereinheiten zu bilden

11.2.5 Konfiguration der Volumes für Dateisysteme

Um ein Dateisystem auf einer VNX bereitzustellen, bedarf es einiger Schritte im Voraus:

1. Konfiguration des Netzwerks
2. Erstellen einer RAID-Group oder eines Storage-Pools
3. Bereitstellen von LUNs
4. Hinzufügen der LUNs zur Storage-Group ~filestorage
5. Bekanntgabe der Kapazität mit Volume-Management

Wählen Sie sich über Unisphere, der web-basierten Verwaltungsoberfläche, ein, um mit der Konfiguration zu beginnen.

Netzwerkkonfiguration

Gehen Sie zu Settings • Network • Settings for File, wählen Sie den Reiter DNS, und klicken Sie auf Create. Füllen Sie die Maske entsprechend der DNS-Server in Ihrer Infrastruktur aus. Wenn Sie mehr als einen DNS-Server angeben wollen, so trennen Sie die IP-Adressen mit einem Komma.

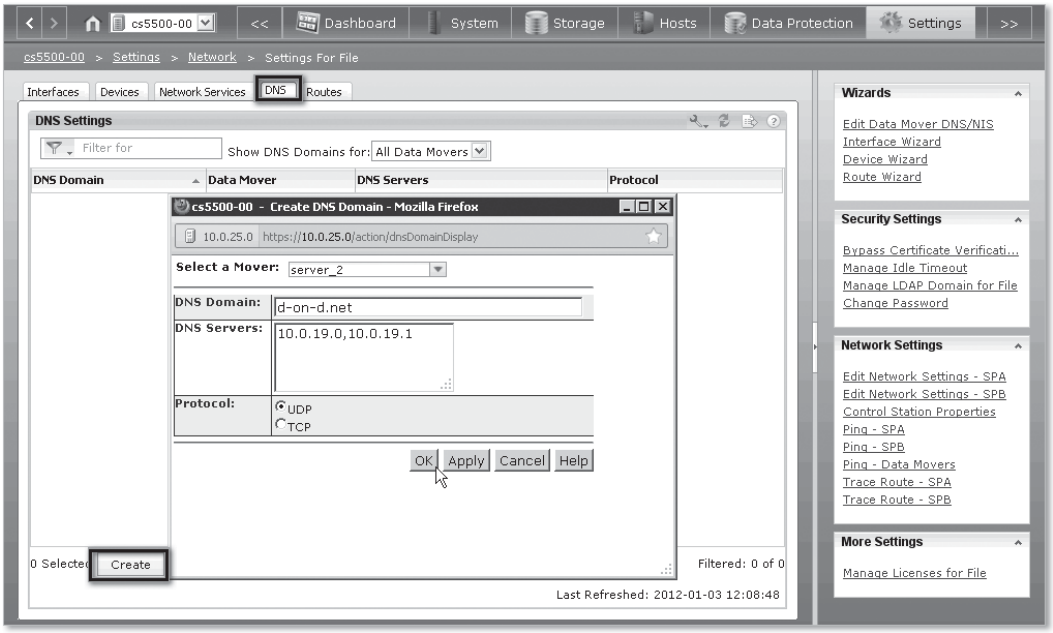


Abbildung 11.53 Konfiguration der DNS-Server

Gehen Sie dann auf den Reiter Network Services, und verifizieren Sie, dass NFS für den Node »server_2« im State Enabled ist (Abbildung 11.54). Sollte das nicht der Fall sein, wählen Sie den entsprechenden Service aus und klicken auf Enable.

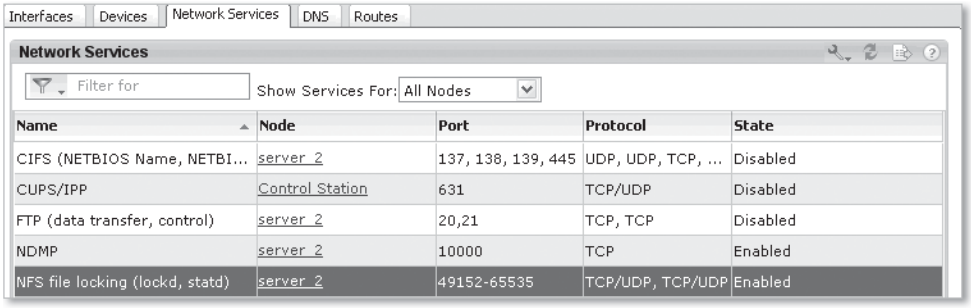


Abbildung 11.54 Verifikation der Netzwerkdienste

Im Reiter DEVICES können Sie das Netzwerk konfigurieren. Diese Konfiguration ist stark von den Möglichkeiten abhängig, die Ihr Netzwerk zulässt. Abschnitt 11.2.6 gibt einige Anregungen zur Konfiguration. Klicken Sie auf CREATE. In der Eingabemaske aus Abbildung 11.55 wählen Sie die primären DATA MOVER (NAS-Header) aus, auf denen das Netzwerkgerät konfiguriert werden soll. Wenn Sie über mehrere primäre Data Mover verfügen (bis maximal 7), haben Sie die Möglichkeit, die Netzwerkgeräte überall gleich zu konfigurieren. Bestimmen Sie dann den TYPE des Netzwerks. Beachten Sie, dass Ihre Infrastruktur EtherChannel oder Link Aggregation unterstützen muss. Sonst bleibt Ihnen nur die Möglichkeit von Fail Safe Networking (FSN) zur redundanten Anbindung. Im Rahmen dieses Kapitels erstellen wir ein 10-GB-Ethernet-Netzwerk mit FSN. Wählen Sie hierfür eine Schnittstelle als primäre und eine zweite als sekundäre Schnittstelle aus. Tragen Sie den gewünschten Netzwerkgerätenamen ein. Bestätigen Sie Ihre Eingaben mit OK.

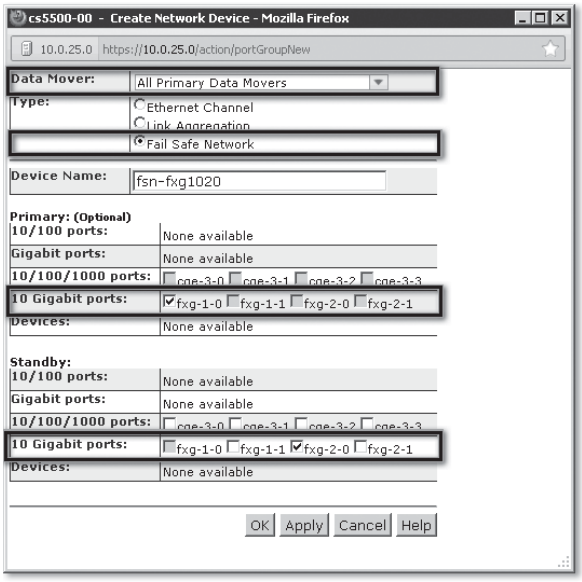


Abbildung 11.55 Konfiguration eines FSN

Wechseln Sie zum Reiter Interfaces, um ein Netzwerkgerät mit ein oder mehreren Schnittstellen zu konfigurieren. Achten Sie vor allem auf die Wahl des richtigen Data Movers und des neu erstellten Netzwerkgerätes. Füllen Sie die restliche Eingabemaske mit Ihren Werten aus. Sie brauchen der Netzwerkschnittstelle nicht unbedingt einen Namen zu geben, das ist für die Verwaltung aber sehr hilfreich.

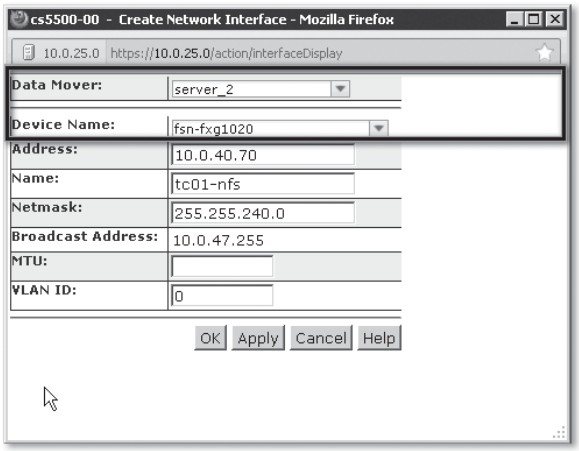


Abbildung 11.56 Konfiguration einer Netzwerkschnittstelle

Zuweisung von Speicherkapazität

Vor der effektiven Erstellung von Dateisystemen benötigt das VNX-System Speicherkapazität. Am einfachsten geht das mit dem Wizard Disk Provisioning for File. Sie finden ihn in der Übersichtsansicht des Reiters Storage. In diesem Abschnitt zeigen wir das manuelle Vorgehen.

Das Vorgehen ist nahezu identisch mit dem Erstellen von Storage-Pools und LUNs für den blockbasierten Speicherbereich. Detaillierte Informationen finden Sie in Abschnitt 11.2.2. Die folgenden Schritte bis zur Konfiguration des ersten Dateisystems müssen Sie nur vornehmen, falls Sie bei der Inbetriebnahme des VNX-Systems durch den VNX-Installation-Assistant-for-File/Unified keine Kapazität provisioniert haben (Ausgangslage dieses Kapitels).

Gehen Sie zu Hosts • Storage Groups, und klicken Sie auf Create, um eine Storage-Group zu erstellen. Im vorliegenden Beispiel von Abbildung 11.57 werden die im System noch freien verbleibenden fünf Festplatten konfiguriert. Im Reiter Advanced ist FAST Cache eingeschaltet, und der Storage Pool Alert ist auf den Schwellenwert von 70 % gesetzt.

Für den nächsten Schritt wählen Sie Storage • LUNs • LUNs und klicken im Fenster auf Create. Erstellen Sie fünf LUNs aus dem Storage Pool namens Pool NAS. Die LUNs sollen als DLU mit einer Kapazität von 200 GB (maximal 16 TB) konfiguriert werden. Vergeben Sie als Namen »nas« und eine Starting-ID mit der Zahl 600 (Abbildung 11.58).

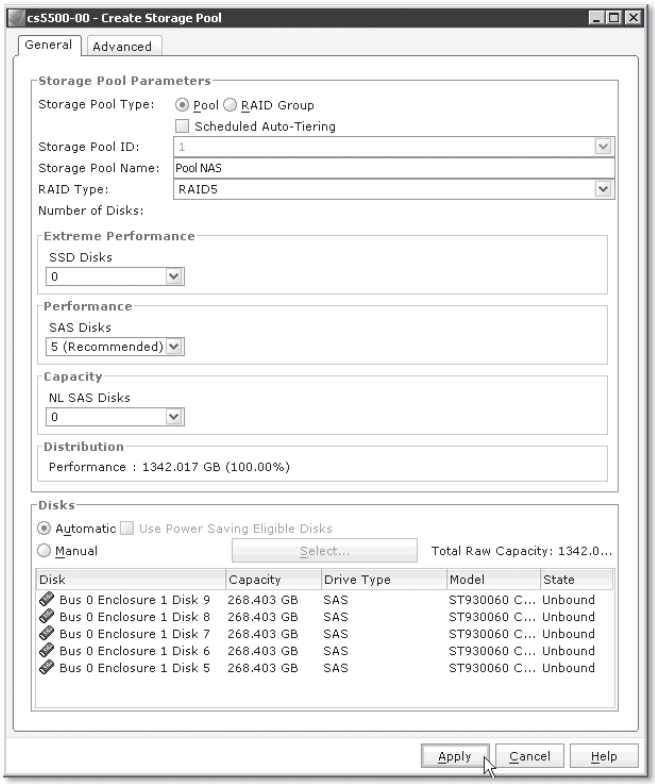


Abbildung 11.57 Konfiguration des Storage-Pools für Dateisysteme

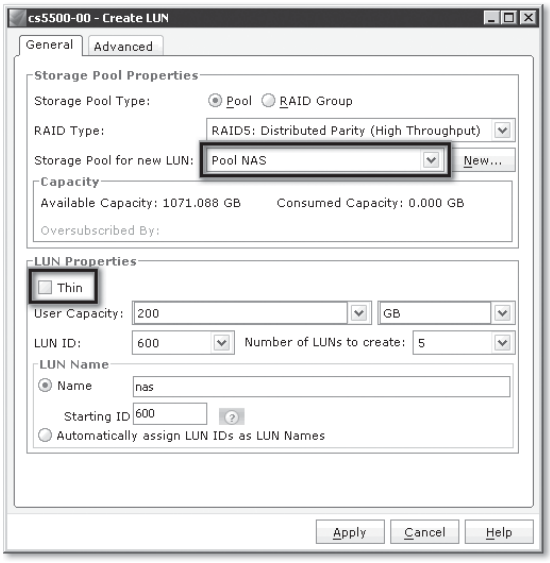


Abbildung 11.58 Konfiguration der LUNs für Dateisysteme

Achten Sie bei den Einstellungen im Reiter ADVANCED darauf, dass Sie immer dieselbe TIERING POLICY für sämtliche LUNs dieses Storage-Pools wählen. Deaktivieren Sie in den ADVANCED LUN PROPERTIES das Kästchen ENABLE AUTO ASSIGN.

Abbildung 11.59 Einstellungen zur »Tiering Policy«

Überprüfen Sie nun, ob die neu erstellten LUNs einen alternierenden Storage-Processor als DEFAULT OWNER haben. Am einfachsten wählen Sie die zu prüfende LUN aus und klicken auf PROPERTIES. In der Anzeige finden Sie den Rahmen OWNERSHIP.

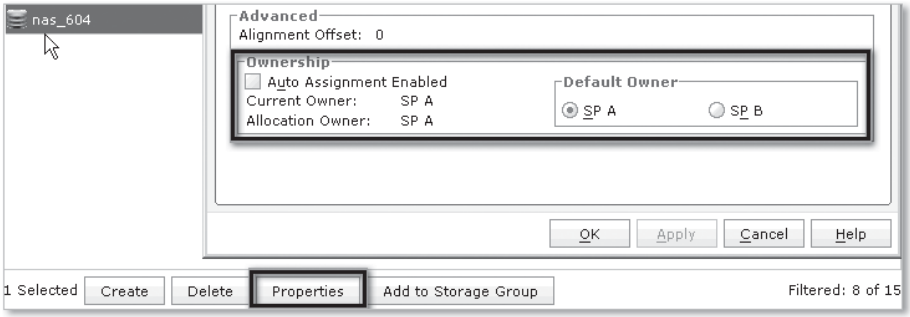


Abbildung 11.60 Überprüfen des Default-Owners

Aus Sicht eines VNX-Systems ist der dateibasierte Speicherbereich ein Spezialfall einer Server-Plattform. Daher müssen die neu erstellten LUNs einer Storage-Group hinzugefügt werden. Die Storage-Group für den dateibasierten Speicherbereich besteht bereits. Sie ist mit dem Namen ~FILESTORAGE gekennzeichnet. Zum Hinzufügen der neu erstellten LUNs zur Storage-Group ~FILESTORAGE klicken Sie auf ADD TO STORAGE GROUP.

Wie bei einem Server üblich muss die zusätzliche Kapazität im dateibasierten Bereich initialisiert werden. Wählen Sie auf der rechten Seite im Bereich FILE STORAGE den Befehl RESCAN STORAGE SYSTEMS aus.

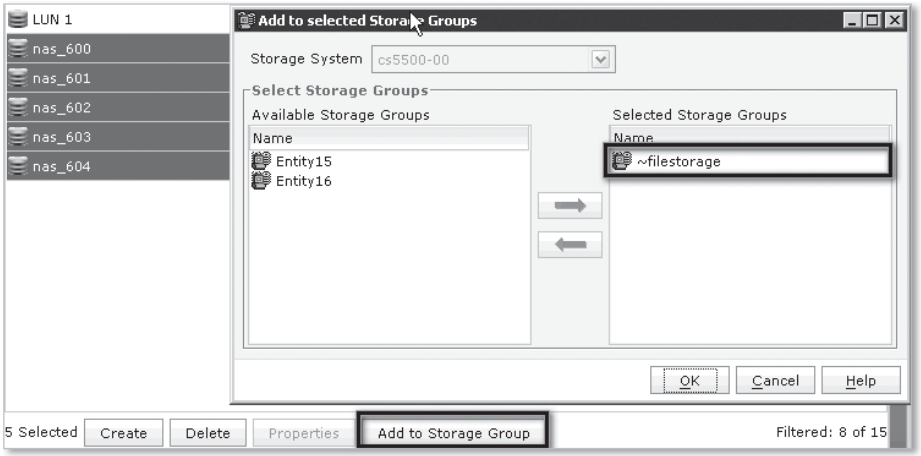


Abbildung 11.61 Hinzufügen von LUNs zu einer Storage-Group

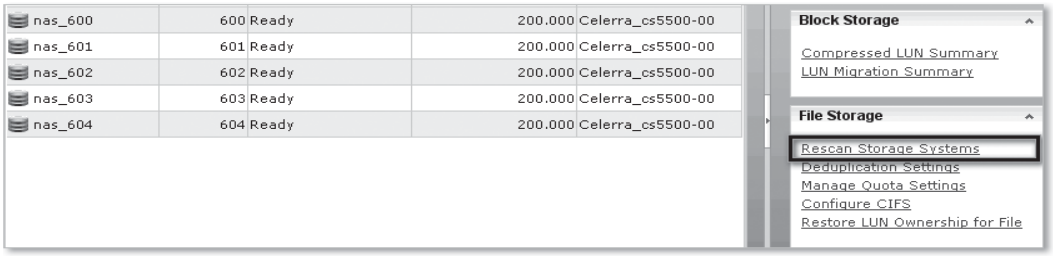


Abbildung 11.62 Initialisierung der neuen LUNs

Loggen Sie sich in das CLI ein. Wie das geht, erfahren Sie in Abschnitt 11.4.1, »Command-Line Interfaces (CLIs)«. Sie lernen den Umgang mit den Befehlen `export`, `nas_disk`, `nas_volume` und `nas_pool`. Mit diesen Befehlen erstellen Sie einen *Storage-Pool-for-File*.

Am besten setzen Sie als Erstes die Umgebungsvariablen mit dem Befehl `export`:

```
[nasadmin@cs5500-00 ~]$ export NAS_DB=/nas
[nasadmin@cs5500-00 ~]$ export PATH=$PATH:/nas/bin
```

Der Rescan der neuen LUNs sollte zwischenzeitlich durchgelaufen sein. Überprüfen Sie, ob die neuen LUNs auch angezeigt werden. Achten Sie auf die Spalte `inuse`, und merken Sie sich den Namen der LUNs (»d*nn*).

```
[nasadmin@cs5500-00 ~]$ nas_disk -list
id   inuse   sizeMB    storageID-devID        type     name         servers
1    y       11260     CKM00112000670-2007    CLSTD    root_disk    1,2
2    y       11260     CKM00112000670-2008    CLSTD    root_ldisk   1,2
3    y       2038      CKM00112000670-2009    CLSTD    d3           1,2
4    y       2038      CKM00112000670-200A    CLSTD    d4           1,2
5    y       2044      CKM00112000670-200B    CLSTD    d5           1,2
```

```
6    y       65526     CKM00112000670-200C    CLSTD    d6          1,2
7    y       257023    CKM00112000670-0006    CLSAS    d7          1,2
12   n       204799    CKM00112000670-0258    PERF     d12         1,2
13   n       204799    CKM00112000670-025A    PERF     d13         1,2
14   n       204799    CKM00112000670-025C    PERF     d14         1,2
15   n       204799    CKM00112000670-0259    PERF     d15         1,2
16   n       204799    CKM00112000670-025B    PERF     d16         1,2
[nasadmin@cs5500-00 ~]$
```

Nun beginnt die Konfiguration der neuen LUNs. Mit dem Befehl `nas_volume` erstellen Sie ein *Stripe-Volume*. Zur Erstellung eines Stripe-Volumes benötigen Sie mindestens zwei LUNs. Ein Stripe-Volumes verteilt die Daten optimal über die beiden LUNs (analog zu einem RAID-0-Stripe). Die Größe des Stripes muss 256 KB sein.

```
[nasadmin@cs5500-00 ~]$ nas_volume -name stripevol-01 -create
  -Stripe 262144 d12,d13,d14,d15,d16
id          = 494
name        = stripevol-01
acl         = 0
in_use      = False
type        = stripe
stripe_size = 262144
volume_set  = d12,d13,d14,d15,d16
disks       = d12,d13,d14,d15,d16

Warning 17716815759: truncating volume
    total = 1023995 avail = 1023998 ( 100% ) (sizes in MB)
[nasadmin@cs5500-00 ~]$
```

Aus dem neu gebildeten Striped Volume erstellen Sie einen Pool. Mit den Optionen `-default_slice_flag` und `is_greedy` bestimmen Sie das Verhalten bei der Erstellung eines Dateisystems. Konkret darf sich das Dateisystem über den ganzen Storage-Pool ausbreiten, und der Volume Manager legt es im größten Bereich des Storage-Pools an.

```
[nasadmin@cs5500-00 ~]$ nas_pool -create -name slicepool-01 -volumes stripevol-
01 -default_slice_flag y -is_greedy y
id                  = 45
name                = slicepool-01
description         =
acl                 = 0
in_use              = False
clients             =
members             = stripevol-01
storage_system(s)   = CKM00112000670
default_slice_flag  = True
is_user_defined     = True
```

```
thin                 = False
tiering_policy       = Auto-Tier/Optimize Pool
compressed           = False
mirrored             = False
disk_type            = Performance
server_visibility    = server_2,server_3
is_greedy            = True
template_pool        = Pool NAS
num_stripe_members   = 5
stripe_size          = 262144
```

Erstellen und Exportieren eines Dateisystems

Nun ist das VNX-System bereit für die Erstellung des ersten Dateisystems. Dazu nutzen Sie den Befehl `nas_fs`. Im Beispiel erstellen wir ein Dateisystem über den gesamten Storage-Pool mit Thin Provisioning. Der Schwellenwert zur automatischen Erweiterung ist auf 75 % eingestellt. Außerdem stellen wir Ihnen die Befehle `server_mountpoint` und `server_mount` vor.

```
[nasadmin@cs5500-00 ~]$ nas_fs -name nfsstore-01 -create size=64G
  pool=slicepool-01 -auto_extend yes -thin yes -hwm 75% -max_size 128G
  -option slice=y  mover=server_2 id=600
id        = 130
name      = nfsstore-01
acl       = 0
in_use    = False
type      = uxfs
worm      = off
volume    = v497
pool      = slicepool-01
member_of = root_avm_fs_group_45
rw_servers=
ro_servers=
rw_vdms   =
ro_vdms   =
auto_ext  = hwm=75%,max_size=131072M,thin=yes
deduplication   = unavailable
thin_storage    = False
tiering_policy  = Auto-Tier/Optimize Pool
compressed      = False
mirrored        = False
stor_devs    =    CKM00112000670-0258,CKM00112000670-025A,CKM00112000670-
025C,CKM00112000670-0259,CKM00112000670-025B
disks     = d12,d13,d14,d15,d16
```

Das neue Dateisystem benötigt ein Verzeichnis, um sich der Außenwelt zu präsentieren.

```
[nasadmin@cs5500-00 ~]$ server_mountpoint server_2 -create /vmw-vols/nfs-01
server_2 : done
```

Nach diesen beiden Schritten können Sie das Dateisystem dem Verzeichnis zuweisen. Zusätzlich optimieren Sie das Schreib- und Leseverhalten für VMware-Umgebungen mit den beiden Mount-Optionen `noprefetch` und `uncached`.

```
[nasadmin@cs5500-00 ~]$ server_mount server_2 -option rw,noprefetch,uncached,
  nonotify,noscan nfsstore-01 /vmw-vols/nfs-01
server_2 : done
```

Provisionieren eines Dateisystems

Nun müssen Sie das Verzeichnis via NFS exportieren, damit Sie es unter vSphere hinzufügen können. Vergeben Sie die entsprechenden Zugriffsberechtigungen für Ihre ESXi-Server. Im untenstehenden Beispiel dürfen sämtliche Server des Netzwerks 10.0.32.0/20 auf den Export zugreifen. Schränken Sie den Zugriff auf die VMkernel-Ports Ihrer Server ein. Einzelne IP-Adressen trennen Sie mit einem Doppelpunkt voneinander.

```
[nasadmin@cs5500-00 ~]$ server_export server_2 -Protocol nfs -name nfsstore-01
  -option rw=10.0.32.20/20:10.0.32.21/20,root=10.0.32.20/20:10.0.32.21/20
  /vmw-vols/nfs-01

server_2 : done
```

- Eine Performanceverbesserung erreichen Sie durch die Erhöhung der Anzahl Threads pro Data Mover:
  ```
  [nasadmin@cs5500-00 ~]$ server_param server_2 -facility nfs -modify nthreads
    -value 2048
  ```
- Die Aktivierung des Wertes erfordert einen Reboot des jeweiligen Data Mover:
  ```
  [nasadmin@cs5500-00 ~]$ server_cpu server_2 -reboot now
  ```
- Überprüfen können Sie den Erfolg Ihrer Einstellung mit dem folgenden Befehl:
  ```
  [nasadmin@cs5500-00 ~]$ server_param server_2 -facility nfs -info nthreads
  ```

Damit ist das Dateisystem bereit, den EXSi-Hosts zur Verfügung gestellt zu werden. Gehen Sie ins vCenter, und wählen Sie den ersten ESXi-Host aus, dem Sie Zugriff gewähren wollen. Wechseln Sie auf den Reiter Configuration, und klicken Sie auf Add Storage... Füllen Sie die Maske mit den Angaben zum NFS-Server (die Schnittstelle, die Sie eingangs dieses Abschnitts erstellt haben) sowie zum konfigurierten Verzeichnis (den *Mountpoint*) aus, und geben Sie dem Datastore einen Namen.

Diesen Vorgang müssen Sie für jeden ESXi-Server wiederholen.

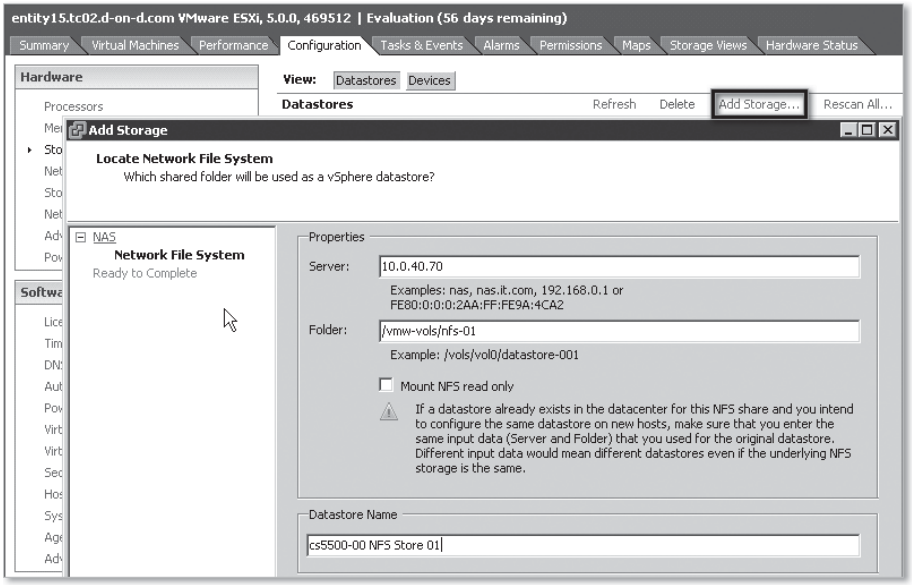


Abbildung 11.63 Provisionieren des NFS-Datastores

11.2.6 Best Practices der dateibasierten Speicheroption

Im Allgemeinen gelten die Best Practices für das VNX-System auch für die dateibasierten Speicheroptionen. Diese finden Sie in Abschnitt 11.2.3, »Best Practices zu blockbasierten Speicheroptionen«.

Applikationen, Datenbanken, virtuelle Maschinen und vSphere 5

VNX-Systeme können dateibasierte Speicherkapazität für VMware-Umgebungen mit dem NFS-Protokoll zur Verfügung stellen.

Wahl des Speicherprotokolls

Falls Sie nicht über ein FC-SAN- oder eine FCoE-Infrastruktur verfügen, ist NFS sicherlich das Protokoll erster Wahl. Es gibt Applikationen, die explizit nach einem Blockprotokoll verlangen. Ein Bespiel hierfür ist Microsoft Exchange (und zwar alle Versionen). In diesem Fall steht Ihnen mit iSCSI eine gute Alternative zur Verfügung. Ein weiteres Anwendungsbeispiel für iSCSI ist, falls Sie für Ihre unternehmenskritischen Applikationen eine Multipathing-Lösung suchen.

Einige Worte zur Einstellung von VMs

Auch beim Einsatz von NFS ist es wichtig, den Zeitüberschreitungswert des Gastbetriebssystems zu setzen. Das Vorgehen zeigen wir Ihnen in Abschnitt 11.2.3, »Best Practices zu blockbasierten Speicheroptionen«, auf.

Anbindung der ESXi-Server

Pro NFS-Datastore baut ESXi eine Datenverbindungen zwischen einem ESXi-Server und einem einzelnen Speicherziel (*Target-LUN* oder *Mountpoint*) auf. Das liegt darin begründet, dass die Implementation des NFSv3-Protokolls auf eine TCP-Session pro Netzwerkverbindung limitiert ist. Die Bandbreite eines einzelnen Datastores ist auf die der Datenverbindung beschränkt. Die einzige Möglichkeit, diese Bandbreite zu erhöhen, ist ein Technologiewechsel (z. B. von 1-GB-Ethernet auf 10-GB-Ethernet).

Grundeinstellung der Anzahl NFS-Datastores ändern

ESXi erlaubt bis zu 256 NFS-Datastores und zieht damit mit der Anzahl unterstützter LUNs gleich. Die Grundeinstellung weist jedoch nur maximal acht NFS-Datastores auf. Erhöhen Sie diesen Wert auf die von Ihnen benötigte Anzahl. Der zu ändernde Parameter heißt NFS.Max.Volumes. Siehe auch VMware KB-Artikel 2239 (*kb.vmware.com/kb/2239*).

Diesen Parameter können Sie in vCenter • ESXi-Server • Configuration • Advanced Settings • NFS anpassen (Abbildung 11.64). EMC empfiehlt auch eine Änderung folgender Parameter pro ESXi-Host, wenn Sie die Anzahl der NFS-Datastores erhöhen. Sie ändern die Größe des Heap Memorys vom TCP/IP-Stack des Servers. Die Parameter finden Sie unter vCenter • ESXi-Server • Configuration • Advanced Settings • Net.

- Net.TcpIpHeapSize auf maximal 32. Erhöhung des Wertes auf 32 MB.
- Net.TcpIpHeapMax auf maximal 128. Erhöhung des Wertes auf 128 MB.

Obenstehende Änderungen verlangen einen Reboot des ESXi-Servers. Gemäß VMware KB Artikel 1007909 (*kb.vmware.com/kb/1007909*) errechnen Sie die TCP/IP-Heap, indem Sie die gegebene Anzahl der NFS-Datastores linear zu den Grundwerten skalieren. Beispiel: Die Grundeinstellung ist 8 NFS-Datastores, Heapsize 6 MB, Heapmax 30 MB (8/6/30). Erhöhen Sie die Anzahl NFS-Datastores auf 16, so lauten Ihre neuen Werte (16/12/60). Das VMkernel-Log gibt Auskunft über zu geringe Werte der TCP/IP-Heap (*kb.vmware.com/kb/1007332*).

Desweiteren sollten Sie folgende Einstellungen an den Parametern unter vCenter • ESXi-Server • Configuration • Advanced Settings • NFS vornehmen:

- NFS:HeartbeatFrequency auf 12 Sekunden.
- NFS.HeartbeatTimeout auf 5 Sekunden.
- NFS.HearbeatDelta auf 5 Sekunden.
- NFS.HeartbeatMaxFailures auf 10.

Diese Einstellungen erfolgen manuell pro ESXi-Server und müssen für sämtliche ESXi-Server, die auf den NFS-Datastore zugreifen, identisch sein.

Abbildung 11.64 Anpassung der Anzahl zugelassener NFS-Datastores

Das NIC-Binding mittels Route-based on IP-Hash von vSphere ermöglicht wohl einen Port-Failover, aber kein Load-Balancing eines einzelnen NFS-Datastores. Bei gesättigter Bandbreite können Sie eine Lastverteilung einzelner VMs erreichen, indem Sie mehrere Netzwerkverbindungen zu einem NFS-Datastore einsetzen. Das bedingt, dass Sie mindestens zwei physische Schnittstellen der VNX und ebenso viele des ESXI-Servers nutzen. Auf Seiten des VNX-Systems konfigurieren Sie am besten einen Trunk mit LACP oder EtherChannel über vier 1-GB-Ethernet-Schnittstellen. Verbinden Sie zwei Schnittstellen mit Switch A und zwei mit Switch B.

Eine automatisierte Möglichkeit, dass verschiedene NFS-Datastores auch unterschiedliche Pfade nutzen, bietet Round-Robin-DNS. Der FQDN des Datastores muss auf mindestens zwei IP-Adressen verweisen. Die DNS-Auflösung geschieht pro Datastore, und sein DNS-Name wird in der vCenter-Datenbank eingetragen. Von Round-Robin-DNS profitieren nicht nur mehrere NFS-Datastores, die auf einen ESXi-Server über potenziell mehrere Schnittstellen verbinden, sondern auch weitere ESXi-Server, da der Mechanismus auch hier zum Tragen kommt. Sie benötigen mehr als einen VMkernel-Port für die Anbindung von NFS-Datastores mit Round-Robin-DNS an einen einzelnen ESXi-Host. Ist ein ESXi-Server einmal über einen Pfad mit dem NFS-Datastore verbunden, so versucht er bei einer Unterbrechung, für den Neuaufbau der Verbindung dieselbe IP-Adresse zu verwenden. Erst der Reboot eines Servers hat eine DNS-Abfrage des FQDNs zur Folge und damit die erneute Zuweisung einer IP-Adresse nach dem Round-Robin-Verfahren. EMC empfiehlt den Einsatz von Round-Robin-DNS.

Eine Priorisierung der Last oder I/O-Anforderungen erreichen Sie mit SIOC. Stellen Sie den Wert Congestions Threshold auf 30 ms ein. Datastores mit aktivierter SIOC müssen explizit einem vCenter zugewiesen sein. Sie können SIOC in vCenter • Inventory • Datastores and Datastore Clusters • <NFS-Datastore> • Configuration • Advanced Settings • Properties anpassen.

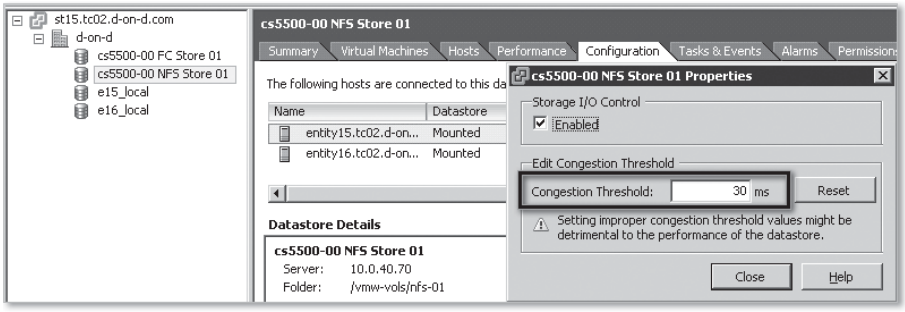


Abbildung 11.65 »Congestion Threshold« für NFS-Datastores

SIOC für NFS-Datastores eignet sich nicht für die folgenden Einsatzgebiete

- Dateiablage
- Mischbetrieb (nebst NFS werden die Festplatten noch für FC-LUNs gebraucht)

Eine beliebte Möglichkeit, NFS-Datastores einzusetzen, ist, sie als Dateiablage für Templates, ISO-Dateien etc. zu verwenden und den Zugriff auf dasselbe Dateisystem via CIFS zu gewähren.

Oftmals werden die gleichen Festplatten nicht nur für NFS-Datastores, sondern auch für andere Zwecke gebraucht. Das hat höhere Latenzzeiten für den betroffenen NFS-Datastore zur Folge und damit Einfluss auf das Verhalten von SIOC oder SDRS mit I/O Metric.

SDRS hilft, die Lastverteilung von virtuellen Maschinen zu automatisieren. Erstellen Sie eine gerade Anzahl an NFS-Datastores derselben Größe (beispielsweise vier NFS Datastores). Exportieren Sie sie über unterschiedliche Ethernet-Schnittstellen. Sie müssen darauf achten, dass die ESXi-Server unterschiedliche Pfade für die Anbindung verwenden. Konfigurieren Sie Round-Robin-DNS für den Einsatz mit SDRS. Zur Konfiguration von SDRS wählen Sie eine I/O-Latency von 30 ms (Congestion Threshold). Diese sollten Sie bei Dateisystemen, die auf FAST-Technologie beruhen, nicht verwenden.

Mit vSphere 5 erhielten die VAAI-Primitives nicht nur im blockbasierten Bereich Zuwachs, sondern sie wurden auch um NFS-Funktionalitäten ergänzt. Wie Sie VAAI-Primitives für NFS aktivieren, erfahren Sie in Abschnitt 11.4.3. Die Unterstützung von VAAI for NFS sehen Sie in der vMA nach Eingabe der folgenden Befehlszeile:

```
vi-admin@vcenter:~[entity15.tc02.d-on-d.com]> esxcli storage nfs list
```

```
vi-admin@vcenter:~[entity15.tc02.d-on-d.com]> esxcli storage nfs list
Volume Name             Host        Share             Accessible  Mounted  Hardware Acceleration
----------------------  ----------  ----------------  ----------  -------  ---------------------
cs5500-00 NFS Store 01  10.0.40.70  /vmw-vols/nfs-01        true     true  Supported
vi-admin@vcenter:~[entity15.tc02.d-on-d.com]>
```

Abbildung 11.66 VAAI für NFS

Nach erfolgreicher Installation können Sie seit vSphere 5 auch Thick Virtual Disks via NFS-Datastores provisionieren. Diese werden oft für virtuelle Maschinen mit hohen Performanceansprüchen hilfreich eingesetzt.

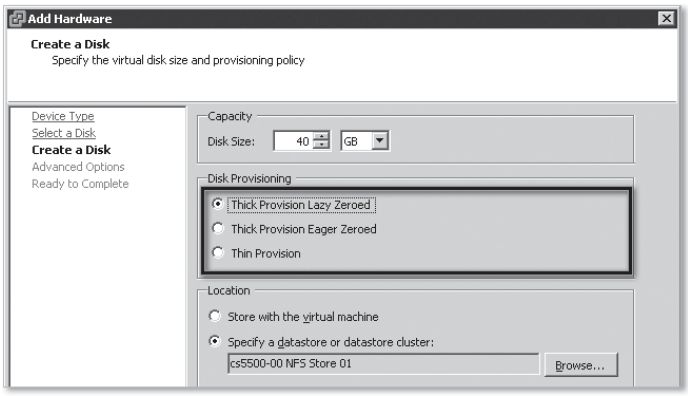


Abbildung 11.67 Disk Provisioning für VAAI NFS

Eine weitere interessante VAAI-Primitive ist das Erstellen eines Fast Clones. Starten Sie den SSH-Dienst eines ESXi-Servers über vCenter • <ESXi-Server> • Configuration • Security Profile • Services • Properties • Options. Loggen Sie sich in den ESXi-Server ein.

```
~ # cd /vmfs/volumes/c8ed541d-1f86d2d4/vc4/
/vmfs/volumes/c8ed541d-1f86d2d4/vc4 # vmkfstools -I vc4.vmdk vc4-fc01.vmdk
/vmfs/volumes/c8ed541d-1f86d2d4/vc4 # vmkfstools --extendedstat vc4.vmdk
Capacity bytes: 42949672960
Used bytes: 11625676800
Unshared bytes: 11625676800
/vmfs/volumes/c8ed541d-1f86d2d4/vc4 # vmkfstools --extendedstat vc4-fc01.vmdk
Capacity bytes: 42949672960
Used bytes: 11625676800
Unshared bytes: 0
```

Mit dem Befehl `vmkfstools -extendedstat <vol.vmdk>` erfahren Sie, welche Kapazität die Virtual Disk im Datastore belegt. Die Anzeige Unshared bytes ist für Fast Clones von hohem Interesse. Sie zeigt die effektiv vom Fast Clone konsumierte Kapazität an.

Wie Sie effizient mit VASA arbeiten und benutzerdefinierte Profile erstellen, erfahren Sie in Abschnitt 11.2.2, »Konfiguration der VNX für blockbasierten Zugriff«.

Netzwerkanbindung für NFS

Zur redundanten Anbindung von Netzwerken verwenden Sie Network Link Aggregation. Das ermöglicht eine Ausfallsicherheit von NFS-Datastores. Sie haben die Wahl zwischen zwei Protokollen: Link Aggregation Control Protocol (IEEE 802.3ad, LACP) oder EtherChannel (nur für Cisco-Switches). Falls Sie EtherChannel einsetzen, so können Sie von der Funktion »Cross-Stack-EtherChannel« profitieren. Cisco bezeichnet diese Technologie als *Virtual Port Channel* (vPC). Das erlaubt Ihnen, eine Aggregation der Netzwerkschnittstellen über zwei physische Switches zu verteilen, was die Verfügbarkeit erhöht. Sollten Ihre Switches diese Möglichkeit nicht bieten, empfiehlt es sich, bei einer VNX Fail-Safe Networking (FSN) zu konfigurieren.

Die Ethernet-Infrastruktur sollte mindestens 1 GB unterstützen, und es ist empfehlenswert, zwei getrennte physische Netzwerke einzusetzen. Ist das nicht möglich, so isolieren Sie den NFS-Datenverkehr der Switches mit VLANs. Vermeiden Sie geroutete und Multi-Hop-Netzwerke. Verwenden Sie für 1-GB-Ethernet-Netzwerke ausschließlich Kabel des Typs CAT 5e oder CAT 6. Schalten Sie die Auto-Negotiation-Einstellungen zu Pause-Frames aus, und setzen Sie eine fixe Geschwindigkeit der Schnittstelle. Konfigurieren Sie sämtliche beteiligte Geräte mit Full Duplex, und achten Sie darauf, dass die TCP Flow Control eingestellt ist. Deaktivieren Sie das Spanning Tree Protocol (STP). Falls Ihre Ethernet-Infrastruktur Quality of Service (QoS) unterstützt, ist es empfehlenswert, die Schnittstellen mit NFS-Verkehr zu priorisieren. Sollten Sie überdies Virtual Distributed Switches einsetzen, dann verwenden Sie zusätzlich NIOC (beispielsweise mit dem Wert 75 für NFS-Traffic), um dem NFS-Datenfluss Ihrer ESX-Cluster eine feste Bandbreite zu garantieren. Vor allem beim Einsatz weniger Ethernet-Schnittstellen ist es

ratsam, NIOC einzusetzen, wo verschiedene Services (vMotion, VM-Verkehr, FT-Logging etc.) um Bandbreite konkurrieren. Limitieren Sie bei einer Überlastung zusätzlich die Bandbreite von vMotion-Traffic.

Konfiguration der Speicherkapazität zur Nutzung für Dateisysteme

Planen Sie, die Dateisysteme auf Basis eines Storage-Pools zu erstellen, bedienen Sie sich ausschließlich Thick LUNs (DLU). Das Verwenden von Thin LUNs (TLU) kann zu beträchtlichen Effizienz- und Performanceeinbußen führen. Dateisysteme allokieren ihren Speicher nach Zylindergruppen. Diese Methode schluckt sehr schnell die gesamte Kapazität einer TLU.

Sie können für das Thin Provisioning (EMC nennt diese Funktion auch *Virtual Provisioning*) von Dateisystemen sowohl RG-LUNs als auch DLUs verwenden. In diesem Abschnitt beschreiben wir die Best Practices für »Storage Pools for File« basierend auf DLUs.

Best Practices zum Provisionieren von Kapazität für Dateisysteme

Prinzipiell ist es empfohlen, dem dateibasierten Bereich eines VNX-Systems mit Hilfe von RG-LUNs Kapazität zur Verfügung zu stellen. Der Vorteil liegt in einer einfacheren Verwaltung dieses Bereichs und einer optimalen Performance begründet.

VNX-Systeme können Thin-provisioned Dateisysteme automatisch erweitern. Das spart administrativen Aufwand. Dabei bestimmen Sie die maximale Erweiterbarkeit des Dateisystems (bis 16 TB) und einen Schwellenwert, der festlegt, bei welchem Füllstand eine Erweiterung durchgeführt wird. Ist der Schwellenwert erreicht, wird das Dateisystem automatisch erweitert. Die Grundeinstellung für diesen Schwellenwert ist 90 %. In virtuellen Infrastrukturen, wo mehrheitlich mit großen Dateien gearbeitet wird, empfiehlt sich eine etwas konservativere Einstellung von 75 %. Damit verhindern Sie potenzielle Out-of-Space-Konditionen beim Ausrollen großer virtueller Maschinen. vCenter kennt nur die Kapazitätsobergrenze bei virtuell provisionierten Dateisystemen mit zugeschalteter, selbstständiger Erweiterung.

Verhalten bei einer Erweiterung mit ungenügend freier Storage-Pool-for-File-Kapazität

Sollte bei einer anstehenden Erweiterung nicht genügend freie Kapazität vorhanden sein, so beansprucht das betroffene Dateisystem den gesamten restlichen Speicher für sich.

Sie dürfen auch FAST VP für Storage-Pools von Dateisystemen verwenden. Die Tiering Policy von Slices (1-GB-Datensätze) wird pro DLU festgelegt. Daher empfiehlt EMC die Verwendung derselben Tiering Policy für sämtliche LUNs innerhalb eines Storage-Pools. Nur so können die gewünschten Volume-Slices erstellt werden.

Wollen Sie einen Storage-Pool für die Erstellung von Dateisystemen verwenden, dann provisionieren Sie die gesamte Kapazität dieses Pools bei seiner Erstellung oder Erweiterung. Konfigurieren Sie sämtliche DLUs, und weisen Sie sie der Storage-Group ~filestorage zu.

Best Practices der Konfiguration von Storage-Pools für Dateisysteme

Dedizieren Sie einen Storage-Pool nur für Dateisysteme. Nutzen Sie die gesamte vorhandene Kapazität. Erstellen Sie pro physische Festplatte ungefähr eine DLU im Storage-Pool. Die Größe der TLUs muss identisch sein. Weisen Sie eine Hälfte der TLUs dem ersten (SPA) und die andere dem zweiten Storage-Processor (SPB) zu. Versuchen Sie, eine Anzahl LUNs zu konfigurieren, die sich durch die Zahl 5 teilen lässt. Beispiel: Falls Ihr Storage-Pool 24 Festplatten enthält, wählen Sie 20 oder 25 TLUs.

Beim Erstellen der TLUs wird die eine Hälfte dem *SPA* und die andere dem *SPB* zugewiesen. Dieser Vorgang wird *SP-Ownership* genannt. Dabei müssen Sie darauf achten, dass der Allocation-Owner gleich dem Default-Owner ist.

Für das Aggregieren von Storage-Pool-TLUs kombinieren Sie mehrere TLUs miteinander, um ein oder mehrere Dateisysteme daraufzulegen. So optimieren Sie die Performance, da so mehrere *dvol*-Queues genutzt werden können. Nutzen Sie eine Stripe-Size von 262.144 Bytes (256 KB) für das empfohlene Striping über 5 TLUs. Sollten Sie weniger als fünf TLUs zur Verfügung haben, so nehmen Sie so viele, wie Sie können.

Dateisysteme können in ihrer Größe nicht schrumpfen. Diese Funktion wird auf Pool-Ebene zur Verfügung gestellt.

Optimale Balance der SP-Ownership ist wichtig

Achten Sie darauf, dass Sie innerhalb eines Stripe-Volumes die SP-Ownership abwechselnd für aufeinanderfolgende DLUs einsetzen. Über Stripe-Volumes hinweg ist es empfehlenswert, die ersten DLUs mit alternierender SP-Ownership konfigurieren. Beispiel: Stripe-Volume 1: A-B-A-B-A, gefolgt von Stripe-Volume 2: B-A-B-A-B.

Da der Algorithmus des *Automatic Volume Management* Storage-Pool-for-File nicht automatisch mit Slice- und Stripe-Volumes arbeitet, müssen Sie wie folgt verfahren:

1. Manual Volume Management (MVM): Erstellen Sie das Stripe-Volume mit dem Befehl `nas_volume`.
2. User-defined File-Pools: Fügen Sie die Stripe-Volumes mit dem Befehl `nas_pool` hinzu. Mit einem Parameter bei der Erstellung des Dateisystems bestimmen Sie die Nutzung von Slices. So kann sich das Dateisystem über den ganzen Storage-Pool-for-File erstrecken.

Das Vorgehen entspricht exakt dem, wie Sie es in Abschnitt 11.2.5 praktisch durchgeführt haben. Allerdings haben Sie entgegen den Best Practices zur Erstellung des Storage Pools for File nur fünf Festplatten anstelle der 20 oder 25 verwendet.

11.3 Effizientes Arbeiten mit vSphere ESXi und VNX

Beim Einsatz von VNX profitieren Sie von folgenden Eigenschaften des Systems:

- Thin Provisioning: Steigert die Effizienz der Nutzung von Speicherressourcen, indem keine Allokation der Blöcke stattfindet.
- Dateikomprimierung: Einzelne, nicht leistungskritische virtuelle Maschinen können komprimiert werden.
- LUN-Komprimierung: Um die Gesamtkapazität des Systems zu optimieren, können einzelne LUNs komprimiert werden. Da sämtliche virtuelle Maschinen (VM) eines VMFS-Datastores von der Komprimierung betroffen sind, müssen Sie sicherstellen, dass sich keine performancekritischen VMs darin befinden. Des Weiteren sollten Sie auf den Einsatz von VMFS-Extents verzichten, wenn Sie diese Funktion nutzen.
- FAST VP und FAST Cache: Erlaubt Ihnen, Slices im häufigen Zugriff automatisch im schnellen Zugriff zu haben. FAST VP optimiert über einen bestimmten Zeitraum und FAST Cache ad hoc.
- Unterstützt VAAI und VASA.
- EMC Replication Manager: Erlaubt Ihnen eine VMFS-konsistente Replikation, Clone oder Point-in-Time-Kopie der virtuellen Maschinen.

Voraussetzungen

Folgende Bedingungen müssen in ihrer Umgebung erfüllt bzw. folgende Softwarepakete müssen installiert sein, um die Techniken dieses Abschnitts anzuwenden:

- Konfiguration eines Storage-Pools und eines Storage Pools for File
- EMC Virtual Storage Integrator (VSI)
- VASA und VAAI
- EMC Replication Manager

11.3.1 Erstellen eines VMFS-Datastores

Starten Sie Ihren vSphere-Client. Zur Manipulation mit Speicherobjekten werden Sie sich in diesem und den folgenden Abschnitten häufig der Menüstruktur vCenter • <ESXi-Cluster> • EMC bedienen.

Klicken Sie mit der rechten Maustaste auf Ihren ESXi-Cluster, und wählen Sie EMC • Unified Storage • Provision Storage. Entscheiden Sie sich im Wizard für die Erstellung einer Disk/LUN. Markieren Sie Ihr VNX-System. Selektieren Sie den Storage-Pool Pool Fast VP. Erstellen Sie ein VMFS-5-Dateisystem. Benennen Sie den VMFS-Datastore, und akzeptieren Sie die vorgeschlagene LUN-ID. Ändern Sie den Default Owner in SPB. Sie haben schon eine FC-LUN erstellt, und EMC empfiehlt, die LUN-Ownership der SPs alternierend einzusetzen. Erstellen Sie

eine Thin LUN mit einer Kapazität von 4 TB. Klicken Sie auf FINISH, um den Auftrag ausführen zu lassen. Kurze Zeit später erscheint Ihr neuer Datastore in der Ansicht der DATASTORES AND DATASTORE CLUSTERS. Der neu erstellte VMFS-Datastore steht dem gesamten ESX-Cluster zur Verfügung. Wollen Sie nur einem ESXi-Server Speicherkapazität zur Verfügung stellen, dann wählen Sie anstelle Ihres ESX-Clusters einen ESXi-Server.

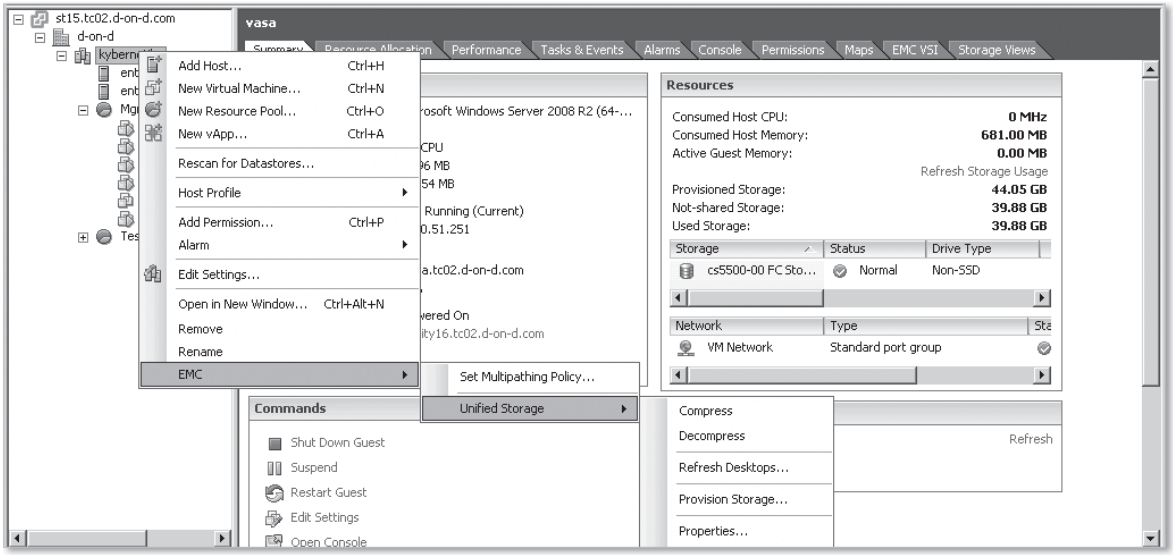


Abbildung 11.68 Möglichkeiten von Virtual Storage Integrator (VSI)

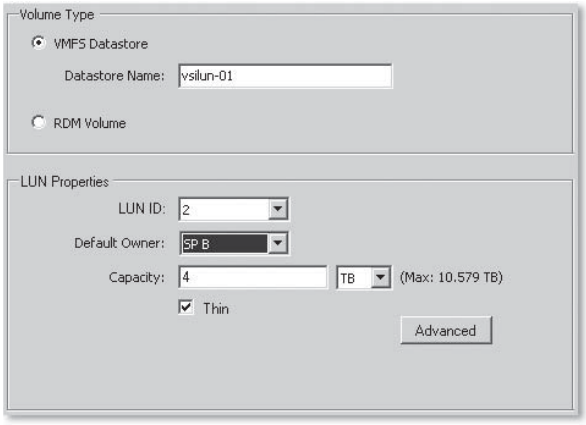


Abbildung 11.69 Einstellungen des VMFS-Datastores

Hinter dem Knopf ADVANCED verbirgt sich die Einstellung des Auto-Tierings (EMC-FAST-Technologie). Diese Einstellung können Sie nur vornehmen, wenn Sie die FAST-Technologie für den gewählten Storage-Pool einsetzen.

Überprüfen der LUN-Ownership

Sie haben mit VSI derzeit weder die Möglichkeit sich die LUN-Ownership anzeigen zu lassen, noch schlägt Ihnen das Plugin die LUN-Ownership vor.

Am einfachsten überprüfen Sie die LUN-Ownership mit folgendem Befehl:

```
naviseccli.exe -h 10.0.25.10 -user sysadmin -password password -scope 0 getlun
  -default
```

11.3.2 Erstellen eines Raw Device Mappings

Klicken Sie mit der rechten Maustaste auf Ihren ESXi-Cluster, und wählen Sie EMC • Unified Storage • Provision Storage. Entscheiden Sie sich im Wizard für die Erstellung einer Disk/LUN. Markieren Sie Ihr VNX-System. Selektieren Sie den Storage-Pool Pool Fast VP. Erstellen Sie ein VMFS-5-Dateisystem. Aktivieren Sie den Knopf RDM Volume, und akzeptieren Sie die vorgeschlagene LUN-ID. Belassen Sie den Default Owner auf SPA. Erstellen Sie eine Thick LUN (Haken bei Thin nicht setzen) mit einer Kapazität 80 GB. Klicken Sie auf Finish, um den Auftrag ausführen zu lassen. Gehen Sie über Home • Inventory VMs and Templates. Wählen Sie einen Windows 2008 R2-Server aus, und fügen Sie das neu erstellte RDM hinzu. Die neue Disk steht Ihnen in der virtuellen Maschine sofort zur Verfügung und kann mit `diskmgmt.msc` manipuliert werden.

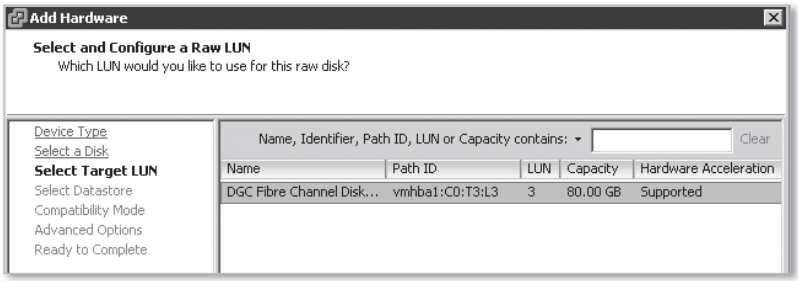


Abbildung 11.70 Raw Device Mapping

11.3.3 Erstellen eines NFS-Datastores

Klicken Sie mit der rechten Maustaste auf Ihren ESXi-Cluster, und wählen Sie EMC • Unified Storage • Provision Storage. Entscheiden Sie sich im Wizard für die Erstellung eines Network File Systems. Markieren Sie Ihr VNX-System. Benennen Sie den Datastore. Wählen Sie einen Data Mover und das Data Mover Interface, über das Sie den NFS-Datastore verbinden wollen. Drücken Sie den Knopf Create New NFS Export. Selektieren Sie den Storage-Pool Pool slicepool-01. Erstellen Sie ein Dateisystem mit einer initialen Kapazität von 64 GB und einer maximalen von 128 GB. Nutzen Sie die Option Thin. Klicken Sie auf Advanced. Korrigieren Sie den Wert der Highwater Mark auf 75 %. Setzen Sie die Parameter No Prefetch, Direct Writes Enabled und Set Timeout Settings. Bestätigen Sie Ihre Wahl mit

Finish, um den Auftrag ausführen zu lassen. Kurze Zeit später erscheint Ihr neuer Datastore in der Ansicht Datastores and Datastore Clusters. Der neu erstellte NFS-Datastore steht dem gesamten ESX-Cluster zur Verfügung. Wollen Sie nur einem ESXi-Server Speicherkapazität zur Verfügung stellen, dann wählen Sie anstelle Ihres ESX-Clusters einen ESXi-Server.

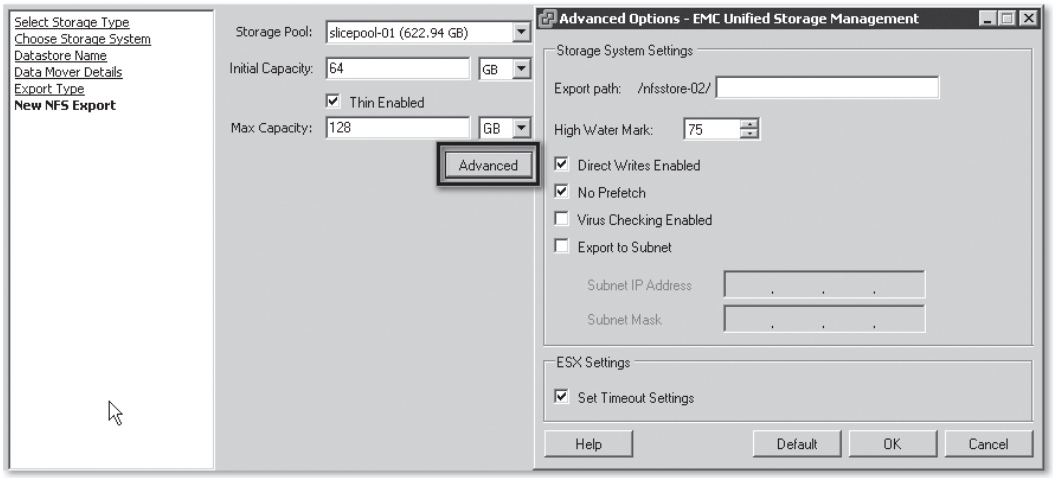


Abbildung 11.71 Advanced Settings von VSI

Wahl des Data-Mover-Interfaces

Für das Load-Balancing von NFS-Datastores ist die alternierende Wahl der IP-Schnittstelle wichtig. Nähere Informationen finden Sie in Abschnitt 11.2.6.

Sie können das Data-Mover-Interface sämtlicher an einen ESXi-Server präsentierten NFS-Datastores überprüfen. Wählen Sie einen ESXi-Host. Gehen Sie auf den Reiter EMC VSI, und sortieren Sie die Datastores nach Device.

11.3.4 Erweitern von Datastores

Erweiterung eines VMFS-Datastores

Wechseln Sie zur Ansicht Datastores and Datastore Clusters. Rufen Sie mit einem rechten Mausklick auf einen VMFS-Datastore Ihrer Wahl den Menüpunkt EMC • Unified Storage • Extend Storage auf. In der Eingabemaske wählen Sie eine Erweiterung um 4 TB. Wenige Sekunden später wird die neue Kapazität dargestellt.

Erweiterung eines NFS-Datastores

Wechseln Sie zur Ansicht Datastores and Datastore Clusters. Rufen Sie mit einem rechten Mausklick auf einen NFS-Datastore Ihrer Wahl den Menüpunkt EMC • Unified Storage • Extend Storage auf. In der Eingabemaske wählen Sie eine Erweiterung um 64 GB. Wenige Sekunden später wird die neue Kapazität dargestellt.

11.3.5 Snaps und Clones

VSI-basiert

Wechseln Sie zur Ansicht VMs and Templates. Rufen Sie mit einem rechten Mausklick auf eine virtuelle Maschine den Menüpunkt EMC • Unified Storage • Fast Clone auf. Bestimmen Sie, zu welchem Resource-Pool die virtuellen Maschinen gehören sollen. In der Eingabemaske bestimmen Sie die Anzahl zu erstellender Fast Clones, deren Name und das Startverhalten inklusive Customization Specification. Wenige Sekunden später stehen Ihnen drei weitere virtuelle Maschinen zur Verfügung.

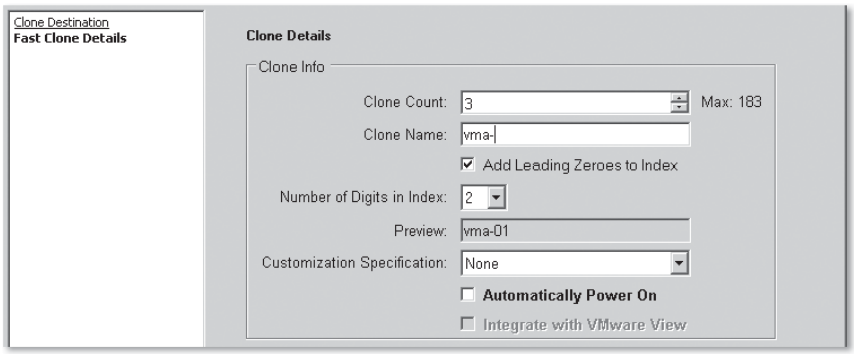


Abbildung 11.72 Erstellung eines Fast Clones

Zur Erstellung eines Full Clones gehen Sie analog vor. Rufen Sie anstelle des Menüpunkts für Fast Clone den Menüpunkt EMC • Unified Storage • Full Clone auf. Die Eingabemaske führt zusätzlich den Parameter Destination NFS Datastore.

Fast und Full Clone

Die virtuelle Maschine muss auf einem NFS-Datastore liegen, sonst steht diese Funktion nicht zur Verfügung. Fast Clones belegen nach Erstellung wenige Bytes. Bei einem Full Clone handelt es sich um eine 1:1-Kopie. Fast und Full Clones können Quelle für Storage vMotion sein.

Auf Basis des Replication Managers

VSI erlaubt es Ihnen, Snaps und Clones virtueller Maschinen zu erstellen. Es bietet Ihnen nicht die Wiederherstellungsmöglichkeit, wie Sie sie von Speichersystemen kennen. Diesen Zweck erfüllt der Replication Manager. Dieses Paket bietet Ihnen die Möglichkeit datastore-konsistenter Snapshots.

Sie brauchen ein Application-Set und einen Replication-Job, um einen erfolgreichen Snapshot durchzuführen. Nach dem Login in die Konsole des Replication Managers finden Sie zu Ihrer rechten Seite den Menüpunkt, mit dem Sie den Wizard zur Erstellung eines Application Sets aufrufen. Benennen Sie das Application-Set, suchen Sie sich einen NFS- oder VMFS-Datastore aus, und beenden Sie den Wizard mit Finish.

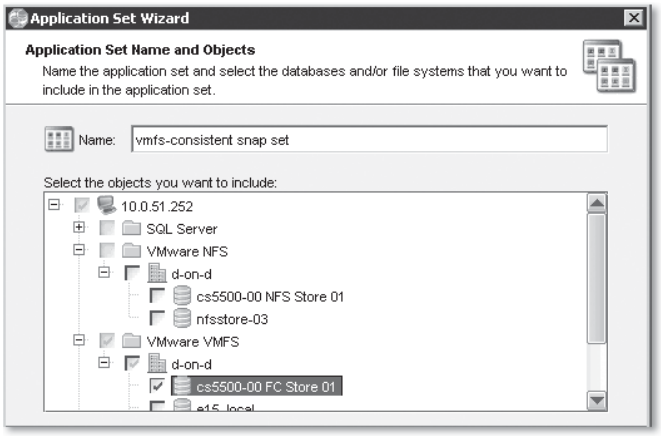


Abbildung 11.73 Replication Manager Application Set Wizard

Nun müssen Sie für dieses Application-Set einen Replication-Job definieren. Der Job Wizard wird automatisch nach Beendigung des Application Set Wizards aufgerufen. Verbinden Sie im Wizard das erstellte Application-Set mit dem Replication-Job. Wählen Sie SnapView Snap aus der Liste Replication Topology aus. Klicken Sie auf Next. Die nun präsentierten Mount Options brauchen Sie nicht auszufüllen. Wählen Sie die manuelle Methode aus, um den Replication-Job zu starten. Beenden Sie den Wizard mit Klick auf Next und Finish.

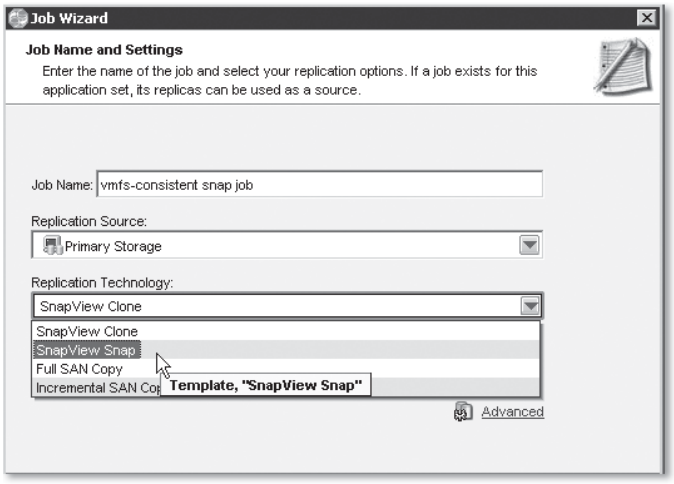


Abbildung 11.74 Replication Job Wizard

Den Replication-Job starten Sie mit einem rechten Mausklick auf das Application-Set in der Baumstruktur zur linken Seite über Application Set • <Name des Application Sets> • Run a job. Die Dauer des Snapshots ist abhängig von der Anzahl virtueller Maschinen im VMFS-Datastore. vCenter versetzt diese in einen konsistenten Zustand, bevor der Snapshot auf

Ihrem VNX-System durchgeführt wird. Snapshots eines NFS-Datastores erstellen Sie analog zu VMFS-Datastores.

Wenn Sie auf Ihr Application-Set klicken, sehen Sie Ihren erfolgreichen ersten Snapshot. Nach einem Rechtsklick auf den Snapshot können Sie unter Restore einen Wizard zur Wiederherstellung des VMFS-Datastores, einer einzelnen virtuellen Maschine oder einer Datei innerhalb einer virtuellen Maschine aufrufen. Der Wizard ist selbsterklärend. Als Mount Host müssen Sie den Replication-Manager-Server selbst angeben. Er fungiert im Beispiel auch als Proxy-Host.

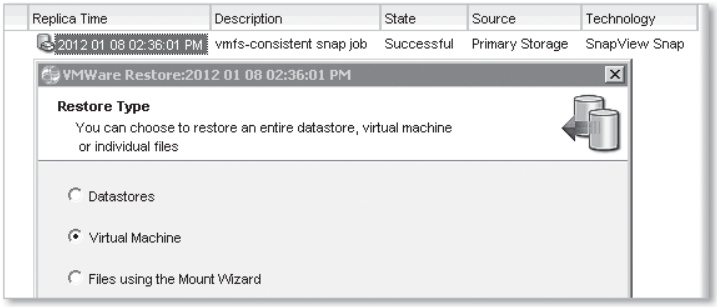


Abbildung 11.75 Auswahlmöglichkeiten einer Wiederherstellung

Die Wiederherstellung eines Datastores erfordert, dass keine virtuelle Maschine läuft. Sie beabsichtigen, den Datastore selbst wiederherzustellen. Beim Restore einer virtuellen Maschine darf diese wiederum nicht in Betrieb sein. Das Wiederherstellen von einzelnen Dateien innerhalb einer virtuellen Maschine kann auch in deren laufenden Betrieb erfolgen.

11.3.6 Komprimierung

Sie haben mit VSI die Möglichkeit, NFS-Datastore oder einzelne virtuelle Maschinen zu komprimieren und zu dekomprimieren. Rufen Sie nach einem rechten Mausklick auf eine virtuelle Maschine oder einen NFS-Datastore den Menüpunkt EMC • Unified Storage • Compress auf. Wenn Sie die Komprimierung auf Datastore-Ebene durchführen, werden sämtliche sich darin befindlichen VMs komprimiert. Sie können auch einzelne virtuelle Maschinen oder den NFS-Datastore wieder dekomprimieren.

Den Effekt der Komprimierung können Sie über den Menüpunkt EMC • Unified Storage • Properties einsehen. Das können Sie ab virtueller Maschine oder ab Datastore durchführen.

Komprimieren von VMFS-Datastores

VSI unterstützt derzeit die Komprimierung von VMFS-Datastores nicht. Zu diesem Zweck gehen Sie in Unisphere über den Reiter Storage • LUNs • LUNs. Wählen Sie die zu komprimierende LUN mit einem Rechtsklick auf Properties aus.

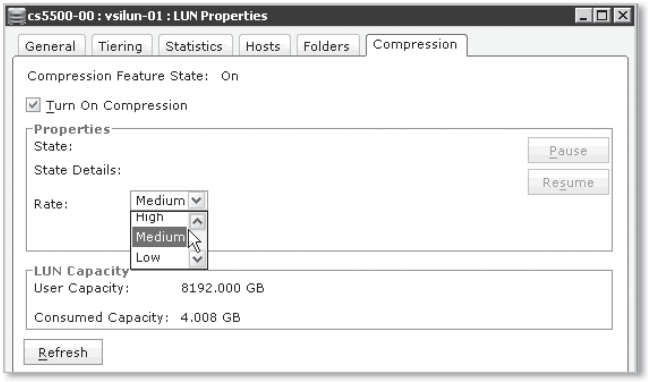


Abbildung 11.76 Einschalten der Komprimierung eines VMFS-Datastores

11.3.7 Einstellungen von Multipathing ändern

Wenn Sie Anpassungen an der Multipathing-Policy vornehmen, so können Sie das einfach über VSI bewerkstelligen. Falls Sie PowerPath/VE installiert haben, dürfen Sie auch das Load-Balancing-Verhalten dieser Multipathing-Technologie steuern. Wechseln Sie zur Ansicht HOSTS AND CLUSTERS. Rufen Sie mit einem rechten Mausklick auf einen ESXi-Server Ihrer Wahl den Menüpunkt EMC • SET MULTIPATHING POLICY auf. Treffen Sie Ihre Auswahl, und bestätigen Sie mit FINISH.

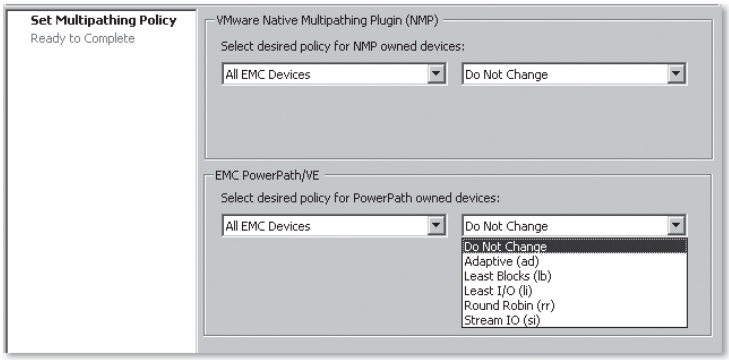


Abbildung 11.77 Setzen der Multipathing-Policy

11.3.8 VAAI und Speicherprofile

Während Sie von den VAAI-Primitives durch Ihre alltägliche Routinearbeit profitieren, offenbaren sich die Vorteile von VASA nicht zwingend auf den ersten Blick. Für die Verwaltung von SLA auf virtuellen Maschinen bringt es entscheidende Vorzüge und beschleunigt den Arbeitsfluss. So sind schnell virtuelle Maschinen ausfindig gemacht, die NON-COMPLIANT sind, oder Sie können via Storage vMotion das passende Profil aussuchen und bekommen die Datastores als COMPLIANT angezeigt, die darauf passen.

Wie Sie VAAI und VASA konfigurieren, anwenden und installieren, entnehmen Sie den Abschnitten 11.2.2 und 11.2.5, respektive 11.4.3 sowie 11.4.2.

Wenn Sie neu eine VM über Deploy from Template erstellen, präsentiert sich die Eingabemaske wie in Abbildung 11.78.

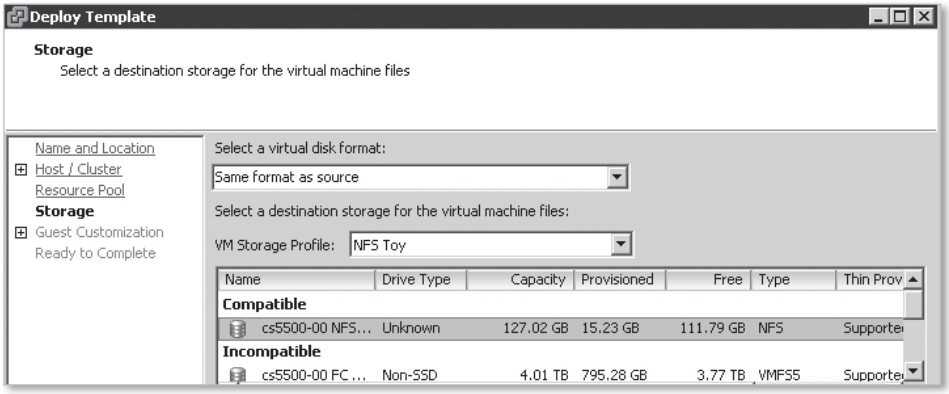


Abbildung 11.78 »Deploy from Template« mit VASA

11.4 Fortgeschrittene Techniken und Anwendungen

Dieser Abschnitt widmet sich fortgeschrittenen Techniken, wie sie auch in diesem Kapitel zur Anwendung kommen. Außerdem finden Sie nützliche Anleitungen zur Installation zusätzlicher EMC-spezifischer Software.

11.4.1 Command-Line Interfaces (CLIs)

VNX-Systeme verfügen über Command-Line Interfaces (CLI). Diese sind nützlich, wenn es darum geht, sich wiederholende Arbeiten mit Scripting durchzuführen, oder um Zugriff auf weitere Funktionen zu erhalten.

CLI für blockbasierten Speicher

Im Folgenden erfahren Sie, wie Sie anhand des Beispiels einer Windows-basierten Installation *Navisphere CLI* aufsetzen. Navisphere ist auch für die Plattformen Linux, Solaris, AIX, HP-UX und VMware erhältlich. Alternativ können Sie auch via CLI für dateibasierten Speicher auf den blockbasierten Bereich zugreifen. Wie das funktioniert, erfahren Sie im nächsten Abschnitt.

Die Software ist im Lieferumfang Ihres Speichersystems enthalten. Die aktuellste Version können Sie von Powerlink (*http://powerlink.emc.com*) beziehen. Sie finden Sie unter Home • Support • Software Downloads and Licensing • Downloads J-O • Navisphere Server

Software. Starten Sie das Installationsprogramm von Navisphere CLI. Bei der Installation gilt es ein paar Dinge zu beachten. Lassen Sie die Umgebungsvariable vom Installationsprogramm setzen.

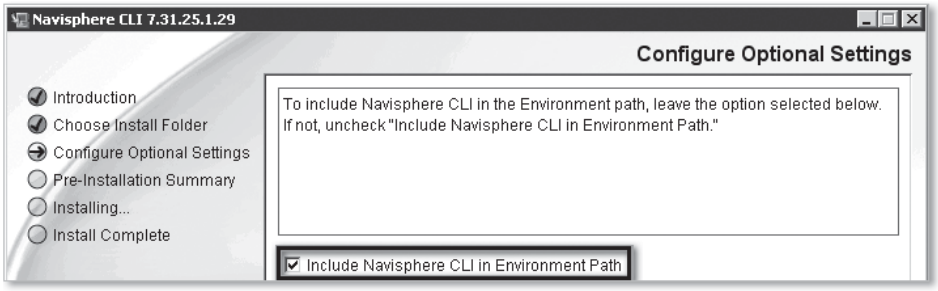


Abbildung 11.79 Umgebungsvariable bei der Installation

Wählen Sie die Erstellung des Security Files, und geben Sie den Benutzernamen und das Passwort des Systemadministratoren bekannt (Grundeinstellung: »nasadmin«). Achten Sie darauf, dass die Scope-Einstellung GLOBAL lautet.

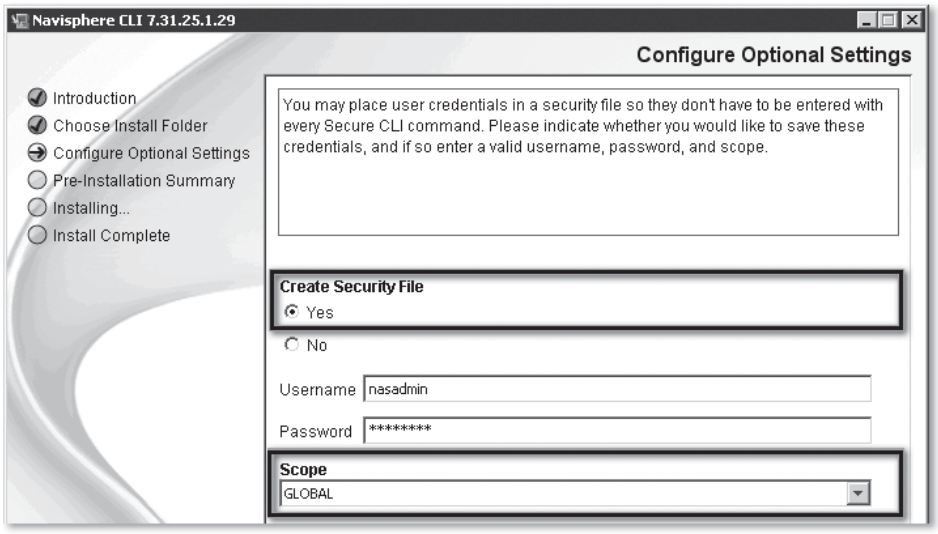


Abbildung 11.80 Erstellen eines sicheren Einwahlverfahrens

Selektieren Sie beim Verification Level zur Überprüfung des Zertifikats den Wert Medium. Damit stellen Sie sicher, dass dieses auch überprüft wird.

Beenden Sie die Installation, indem Sie die folgenden Eingabeaufforderungen mit Next und Finish bestätigen. Nach wenigen Minuten ist die Installation beendet, und Sie können über Start • Run... und Eingabe von »cmd« die Eingabeaufforderung von Windows aufrufen.

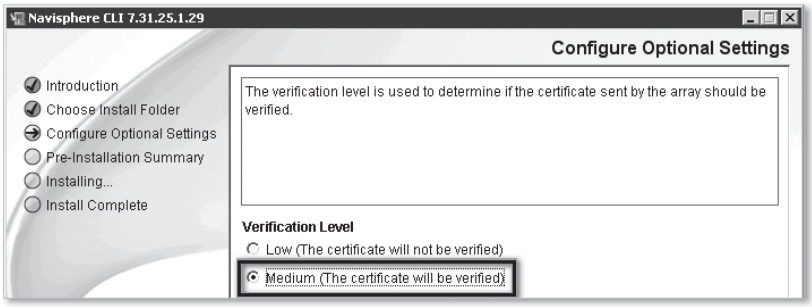


Abbildung 11.81 Überprüfung des Zertifikats

Zum Testen der Verbindungsherstellung zum Speichersystem oder zu einem der beiden Storage-Processors verwenden Sie folgenden Befehl:

```
C:\> naviseccli -User nasadmin -Password <Benutzer-Passwort> -Scope 0 -Address
  <IP-Adresse SPA oder SPB> arrayname

Array Name: <Hostname Ihres Speichersystems>

C:\> _
```

Wenn der Befehl korrekt ausgeführt und die Verbindung hergestellt wurde, erscheint der Name des Speichersystems.

CLI für dateibasierten Speicher

Der Zugriff auf das CLI erfolgt mittels Secure Shell. Für Windows-Systeme nutzen Sie für den Verbindungsaufbau am besten das Programm PuTTY. Geben Sie dafür dem Programm die IP-Adresse oder den FQDN für den Zugriff auf die webbasierte Oberfläche bekannt. Wählen Sie sich als Systemadministrator ein (Abbildung 11.82).

Das CLI für den dateibasierten Speicher enthält beispielsweise die Steuerungsparameter für den optimierten Zugriff auf Dateisystemen. Die meisten Befehle sind in den Verzeichnissen */nas/bin*, */nas/sbin* und */nasmcd/bin* abgelegt.

Sie können von dem CLI für dateibasierten Speicher ebenfalls direkt auf die Storage-Processors zugreifen und blockbasierte Befehle ausführen. Sie finden wichtige Befehle in den Verzeichnissen */nasmcd/sbin* sowie */nas/sbin/setup_backend*. Anbei sehen Sie ein Beispiel, wie Sie auf die blockbasierte Speicherumgebung zugreifen. Dazu bedienen Sie sich des Befehls, der im vorherigen Abschnitt beschrieben ist.

```
[nasadmin@cs5500-00 /]$ /nasmcd/sbin/naviseccli -User nasadmin -Password nasadmin
  -Scope 0 -Address 10.0.25.10 arrayname
Array Name: cs5500-00
```

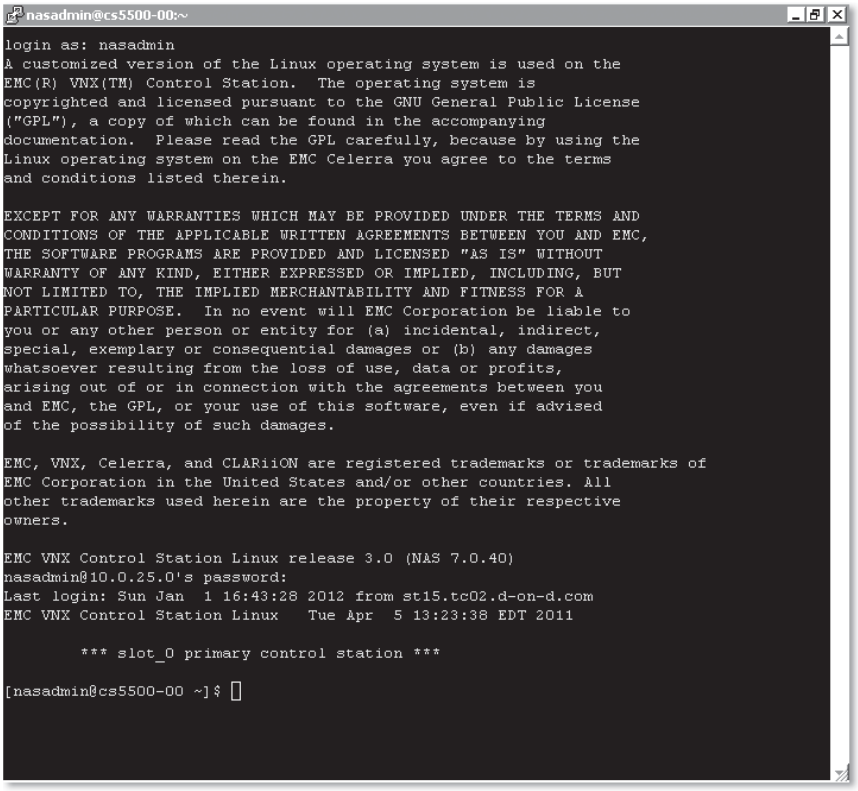


Abbildung 11.82 Einwahl in das CLI

11.4.2 Installation von VASA

Zur Implementation von VASA benötigen Sie den SMI-S-Provider. Sie finden ihn auf Powerlink (Home • Support • Software Downloads and Licensing • Downloads S • SMI-S Provider).

Die Installationsanleitung bezieht sich auf Windows-Server. Achten Sie bei der Installation des Pakets *se7314-WINDOWS-x64-SMI.msi* darauf, dass Sie nur den Array Provider auswählen.

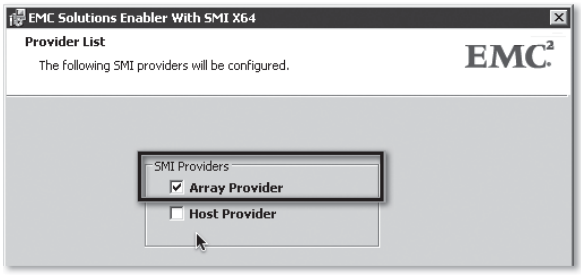


Abbildung 11.83 Installation des EMC Solutions Enablers (SMI)

Konfiguration des SMI-S-Providers

Erweitern Sie als Erstes die Umgebungsvariable `Path` Ihres Windows-Servers im System Variable Path um den Pfad `;c:\Program Files\EMC\SYMCLI\bin`.

Editieren Sie im nächsten Schritt die Datei *C:\Program Files\EMC\ECIM\ECOM\conf\Security_settings.xml*. Suchen Sie nach dem String `value="100"`. Ersetzen Sie den Wert `100` durch den Wert `1200`.

```
<!--
**************************************************************************************
*ExternalConnectionLimit:
* The maximum number of active client connections allowed by ECOM.
* Once this limit is reached, subsequent connections will be rejected.
* A value of zero implies the default value (100).
**************************************************************************************
-->
<ECOMSetting Name="ExternalConnectionLimit" Type="uint32" Value="1200"/>

</ECOMSettings>
```

Abbildung 11.84 Editieren der Datei »Security_settings.xml«

Starten Sie in `services.msc` den Dienst ECOM neu.

Öffnen Sie die Windows-Kommandozeile. Führen Sie die Befehlszeile `C:\Program Files\EMC\ECIM\ECOM\bin\TestSmiProvider.exe` aus. Bestätigen Sie alle Eingaben mit dem Grundwert. Notieren Sie sich folgende Werte:

- Benutzername »admin«
- Passwort »#1Password«
- https://<IP SMI-Provider Server>:5989/vasa/services/vasaService«

Sie können Benutzername, Passwort und Port Ihren Richtlinien anpassen.

Nun gelangen Sie zum SMI-Provider-Test-Programm. Mit dem Befehl `dv` prüfen Sie die Funktionstüchtigkeit des SMI Providers.

```
++++ Display version information ++++
CIM ObjectManager Name: EMC:10.0.51.251
CIMOM Version: EMC CIM Server Version 2.6.6.2.0.6
SMI-S spec version: 1.5.0
SMI-S Provider version: V4.3.1.1
SMI-S Provider Location: Proxy
SMI-S Provider Server:
Windows_NT vsi 6.1.7600 x86_64 VM Guest OS (64bit Libraries)
Solutions Enabler version: V7.3-1305 1.4
```

Abbildung 11.85 Ausgabe einer erfolgreichen Prüfung

Bei erfolgreicher Verifikation können Sie Ihr VNX-System mit dem SMI Provider verknüpfen, indem Sie `addsys` eingeben. Der `ArrayType` ist `Clar` (`1`). Als IP-Adressen verwenden Sie SPA und SPB. Das Benutzerkonto Ihres VNX-Systems muss Administrationsrechte mit *Scope Global* haben. In diesem Beispiel ist das »sysadmin«, der bislang immer verwendet wurde.

```
(localhost:5988) ? addsys
Add System (y|n) [n]: y

ArrayType (1=Clar, 2=Symm) [1]: 1
One or more IP address or Hostname or Array ID

Elements for Addresses
IP address or hostname or array id 0 (blank to quit): 10.0.25.10
IP address or hostname or array id 1 (blank to quit): 10.0.25.11
IP address or hostname or array id 2 (blank to quit):
Address types corresponding to addresses specified above.
(1=URL, 2=IP/Nodename, 3=Array ID)
Address Type (0) [default=2]: 2
Address Type (1) [default=2]: 2
User [null]: sysadmin
Password [null]:
++++ EMCAddSystem ++++
```

Abbildung 11.86 Eingabemaske des SMI Providers

Überprüfen Sie die erfolgreiche Anmeldung des Speichersystems mit `dv`.

```
SMI-S Provider Server:
Windows_NT vsi 6.1.7600 x86_64 VM Guest OS (64bit Libraries)

Solutions Enabler version: V7.3-1305 1.4

Firmware version information:
(Remote) CLARiiON Array CKM00112000670 (Rack Mounted VNX5500) : 5.31.0.5.509
```

Abbildung 11.87 Erfolgreiche Anmeldung am SMI Provider

Starten Sie Ihren vSphere-Client, und gehen Sie auf ADMINISTRATION • STORAGE PROVIDERS.

Abbildung 11.88 Storage-Provider im vCenter

Klicken Sie auf ADD..., um einen neuen Provider anzumelden. Füllen Sie die Maske entsprechend den vorher notierten Angaben aus.

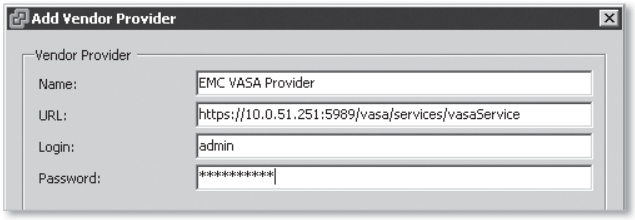


Abbildung 11.89 Eingabemaske von vSphere-VASA

Bei erfolgreicher Anmeldung sehen Sie Ihr VNX-System im unteren Fenster.

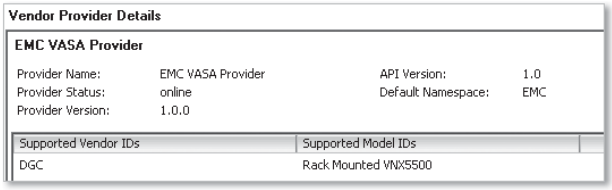


Abbildung 11.90 VASA für das VNX-System

11.4.3 Einrichten VAAI for File

Für das Einrichten der VAAI-Primitives für den dateibasierten Bereich benötigen Sie den VMware Update Manager (VUM) und die entsprechende Erweiterung von EMC. Diese können Sie von Powerlink beziehen (Home • Support • Software Downloads and Licensing • Downloads A-B • Adapters for Third-Party Applications). In diesem Buch benutzen wir die Version *EMC Nas Plugin 1.0-10*.

Nach dem Download müssen Sie prüfen, ob die Version des VNX-Systems den Anforderungen genügt. VAAI für NFS ist ab Version 7.0.35.x unterstützt. Öffnen Sie eine SSH-Verbindung auf das VNX-System. Eine Anleitung finden Sie in Abschnitt 11.4.1, »Command-Line Interfaces (CLIs)«. Geben Sie den Befehl `nas_version` ein.

```
[nasadmin@cs5500-00 ~]$ nas_version
7.0.40-1
```

Die angegebene Version entspricht den Anforderungen.

Starten Sie VUM über vCenter • Home • update manager. Gehen Sie zum Reiter Patch Management • Import Patches. Browsen Sie nach der Datei *EMCNasPlugin-1.0-10.zip*.

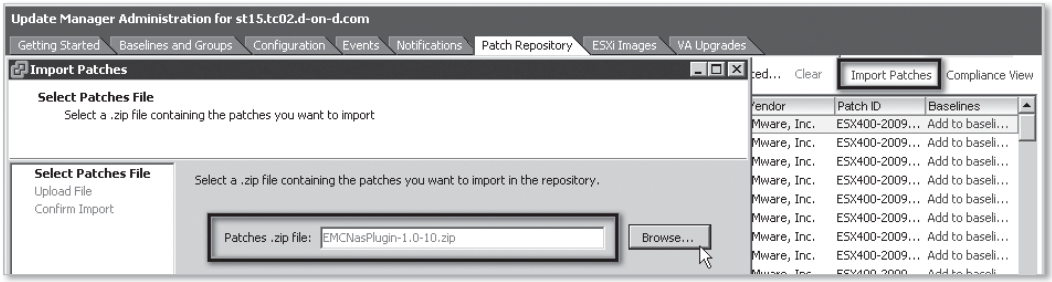


Abbildung 11.91 Bekanntgabe des Patches

Klicken Sie auf Next, um zum nächsten Fenster zu gelangen.

Bestätigen Sie Ihre Eingaben mit einem Klick auf Finish. Nun müssen Sie eine Baseline erstellen. Dafür klicken Sie auf Baselines and Groups • Create..., um den Wizard zur Erstellung einer neuen Baseline aufzurufen. Benennen Sie die neue Baseline, und deklarieren Sie sie als Host Extension.

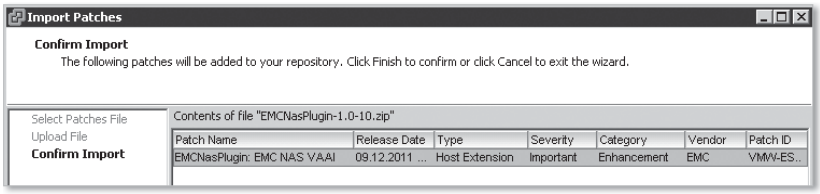


Abbildung 11.92 Verifikation des Patches

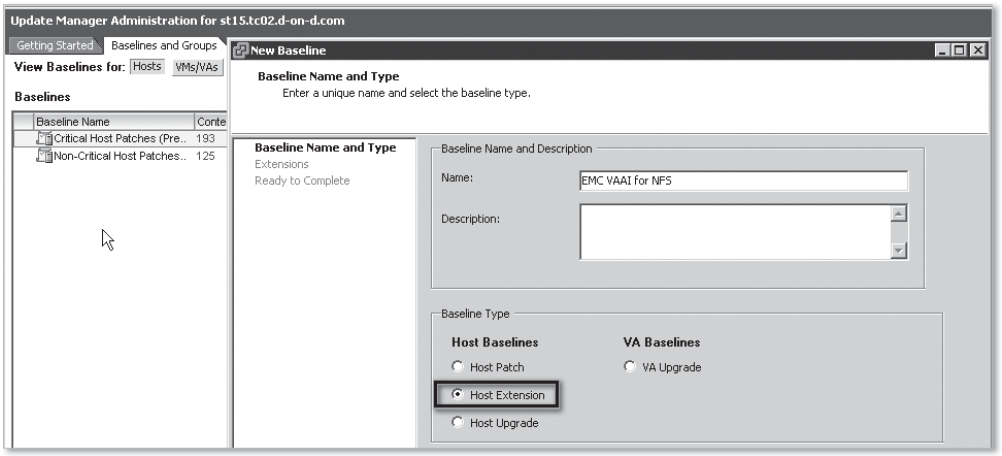


Abbildung 11.93 Der Baseline-Wizard

Suchen Sie nach dem Begriff »EMCNasPlugin EMC NAS VAAI«, und fügen sie dieses Plugin der Auswahl hinzu. Verifizieren Sie Ihre Angaben, und schließen Sie den Wizard mit Klick auf FINISH.

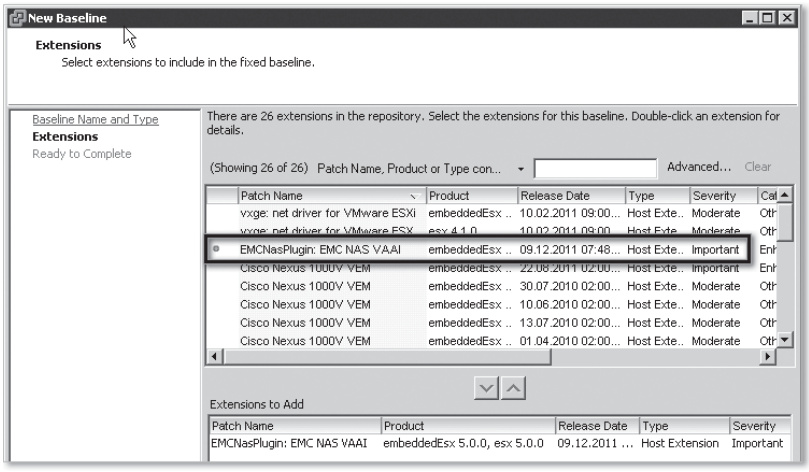


Abbildung 11.94 Auswahl des Patches

Gehen Sie anschließend über vCenter • Hosts and Clusters • <your cluster> • Update Manager • Attach..., um die neu erstellte Baseline auszuwählen und Ihrem ESX-Cluster hinzuzufügen.

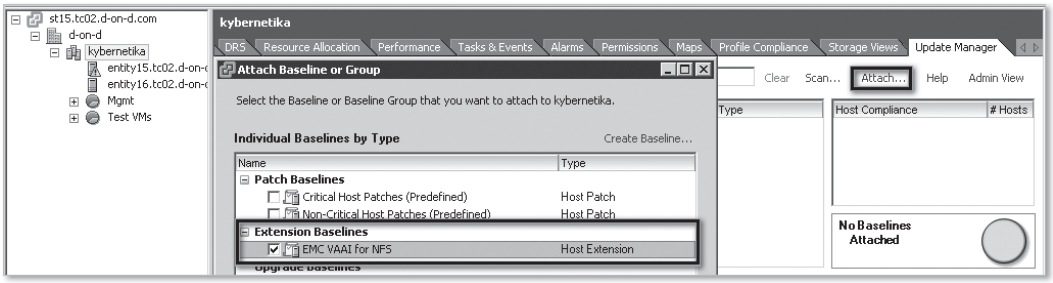


Abbildung 11.95 Auswahl einer Baseline

Klicken Sie auf Scan... für das Durchforsten der Patches and Extensions. Nun ist der Patch bereit, eingespielt zu werden.

Versetzen Sie Ihre ESXi-Hosts in den Maintenance-Modus. Applizieren Sie den Patch mit einem Klick auf Remediate... und Ausfüllen der Masken im Wizard. Normalerweise genügt es, die Grundeinstellung im Wizard zu akzeptieren. Gegebenenfalls müssen Sie die Richtlinie *VMware-High-Availability Admission-Control* übersteuern. Der Vorgang erfordert einen Reboot.

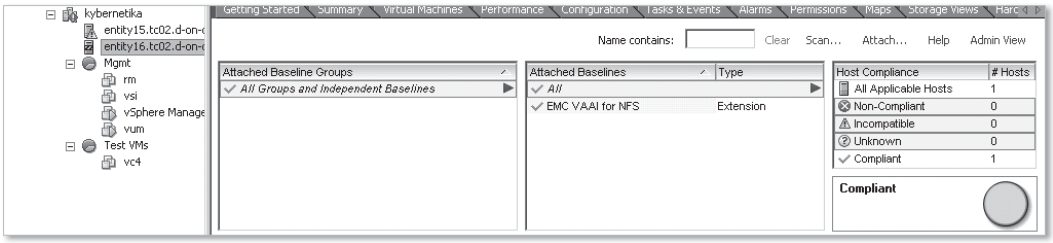


Abbildung 11.96 Erfolgreiche Installation von VAAI-Primitives für NFS

Wiederholen Sie diesen Vorgang für sämtliche Hosts Ihres ESX-Clusters.

11.4.4 Installation EMC PowerPath/VE

EMC empfiehlt, die *PowerPath Virtual Edition* (PPVE) über den VUM zu installieren. Das Vorgehen gleicht entsprechend dem bei den VAAI-Primitives in Abschnitt 11.4.3. PPVE können Sie von Powerlink beziehen (Home • Support • Software Downloads and Licensing • Downloads P-R • PowerPath for VMware). Extrahieren Sie das Paket *PowerPath_VE_5_7_for_VMWARE_vSphere_Install_SW_Bundle.zip*. Sie finden darin das Paket *EMCPower.VMWARE.5.7.b173.zip*, das Sie für VUM benötigen. Importieren Sie das Paket in VUM wie in Abschnitt 11.4.3 beschrieben.

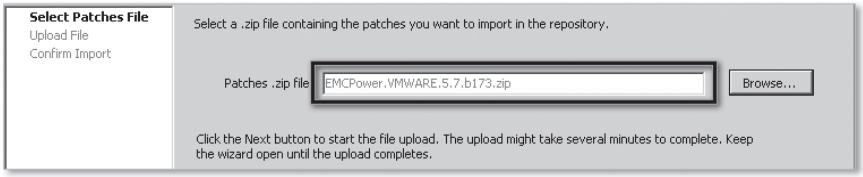


Abbildung 11.97 PowerPath-VE-Software

Überprüfen Sie die Angaben zum Paket.

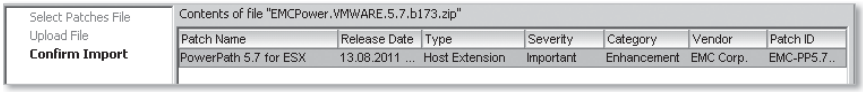


Abbildung 11.98 Verifikation des Pakets

Erstellen Sie eine Baseline für HOST EXTENSIONS.

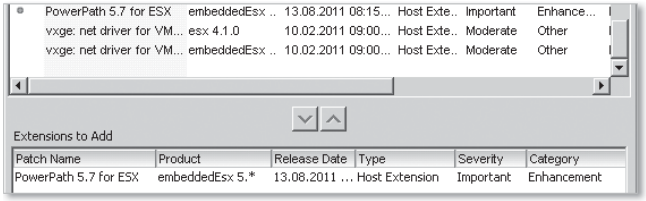


Abbildung 11.99 Konfiguration der Host-Extension-Baseline

Verknüpfen Sie die Baseline mit Ihrem *ESX-Cluster*.

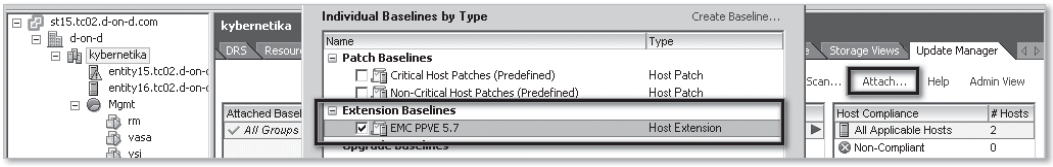


Abbildung 11.100 Anbindung der Baseline an den ESX-Cluster

Danach klicken auf STAGE..., um PPVE auf sämtlichen Hosts Ihres ESX-Clusters zu spielen.

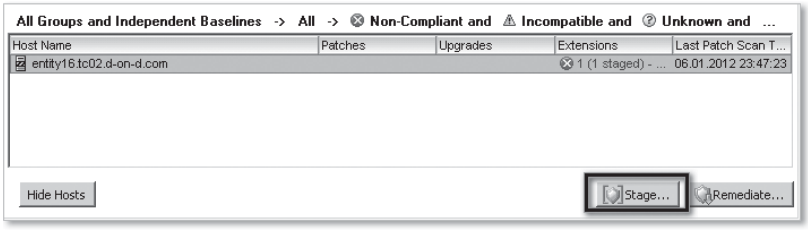


Abbildung 11.101 Staging der PPVE-Host-Extension

Nun versetzen Sie die Hosts gemäß Ihrer *VMware High Availability Admission Control Policy* in den Maintenance Mode. Rufen Sie nach einem Rechtsklick auf diese ESXi-Hosts den Befehl Remediate... auf.

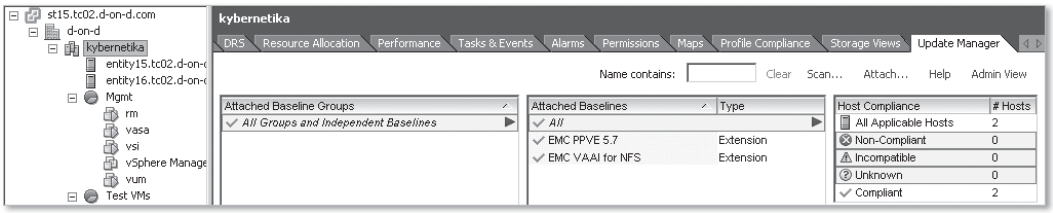


Abbildung 11.102 Erfolgreiche Applikation der PPVE-Host-Extension

Jetzt müssen Sie das PowerPath-Paket `rpowermt` auf einem Windows- oder Linux-Server installieren, um die Installation abzuschließen. In der zuvor extrahierten ZIP-Datei finden Sie das Verzeichnis *RTOOLS_Windows*. Dekomprimieren Sie die sich darin befindliche Datei *EMCPower.RTOOLS.Windows.x86_32.5.7.b173.zip*. Installieren Sie das Paket *EMCPower.RTOOLS.Net32.5.7.b173.exe*. Befolgen Sie die Instruktionen am Bildschirm, und beenden Sie die Installation mit Finish. Überprüfen Sie, ob die Umgebungsvariable für PPVE richtig gesetzt ist; sie lautet: `C:\Program Files (x86)\EMC\PowerPath\rpowermt\`.

Lizenzierung von PPVE

Die Lizenzierung von PPVE ist pro CPU Socket. EMC unterscheidet zwischen zwei Verfahren: *Served* und *Unserved Licensing*. Die erste Variante bedingt die Installation eines Lizenzservers, die zweite nicht. Die Verwaltung der Lizenzen mit einem Lizenzserver ist einfacher und besser geeignet für größere Umgebungen.

11.4.5 Blockbasierte Snapshots und Clones

Im blockbasierten Bereich eines VNX-Systems ist das Konzept von Snapshots anders als im dateibasierten Bereich. In ersterem müssen Sie LUNs als Snapshot-LUN erstellen. In letzterem ist der Snapshot eines Dateisystems selbst ein Dateisystem. Die Snapshot-LUNs stehen in einer 1:1-Beziehung zu ihrer Quell-LUN. Die Snapshot-LUNs werden im Reserved-LUN-Pool verwaltet. Sie können beliebig Snapshots einer Quell-LUN oder einer Clone-LUN erstellen; erst wenn Sie eine SnapView-Session starten, bedient sich das VNX-System des Reserved-LUN-Pools. Eine SnapView-Session kann *persistent* oder *persistent, consistent* sein.

Wenn Sie einen Snapshot aktivieren wollen, wählen Sie eine inaktive SnapView-Session aus. Der aktive Snapshot kann auf die gewohnte Weise über die Storage-Group als LUN dem ESXi-Server oder ESX-Cluster präsentiert werden. Sie können auf diese Weise maximal acht Snapshots beziehungsweise zeitlich unterschiedliche Datenbestände Ihrer Quell-LUN gleichzeitig zeigen.

Wählen Sie sich in Unisphere ein. Erstellen Sie eine LUN für jede Quell-LUN, von der Sie Snapshots erzeugen wollen. Wie Sie das machen, haben wir in Abschnitt 11.2.2 gezeigt. Wenn Sie Snapshot-LUNs aus einem Storage-Pool erstellen, können Sie zusätzlich im Reiter ADVANCED die TIERING POLICY Ihren Bedürfnissen anpassen. Die Größe dieser LUNs sollte 30 % der Gesamtkapazität der Quell-LUN betragen. Das erscheint anfänglich hoch, es wird aber dadurch relativiert, dass sämtliche Snapshot-Daten in der Snapshot-LUN gespeichert werden. Da Sie eine Snapshot-LUN auch aus einem Pool als DLU konfigurieren dürfen, wird diese Speicherkapazität zwar reserviert, nicht jedoch allokiert.

Nachdem Sie die gewünschte Anzahl an Snapshot-LUNs erstellt haben, greifen Sie über den Reiter DATA PROTECTION auf den RESERVED LUN POOL zu. Klicken Sie auf den Knopf CONFIGURE, und fügen Sie die Snapshot-LUNs mit ADD LUN dem Global Pool hinzu.

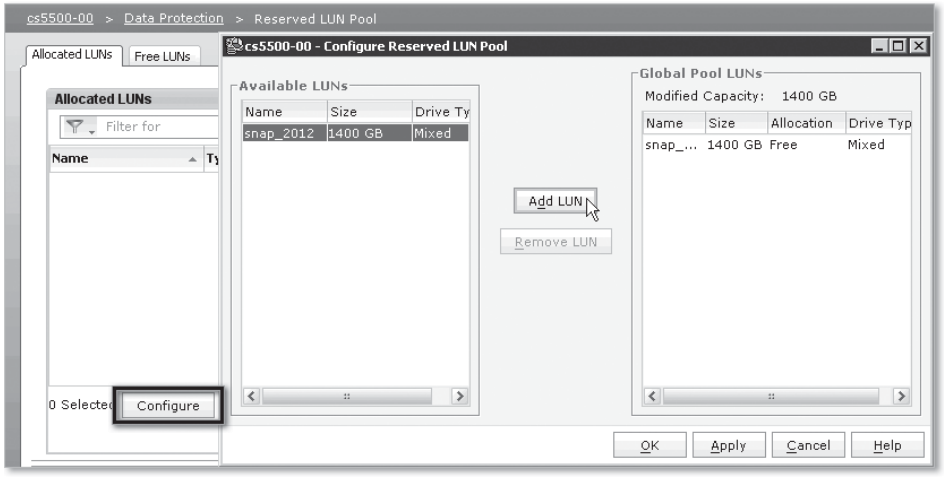


Abbildung 11.103 Hinzufügen der LUNs zum Reserved-LUN-Pool

Das VNX-System verwaltet die LUNs des Reserved-LUN-Pools automatisch. Wenn Sie den Replication Manager einsetzen, übernimmt er die Kontrolle über die SnapView-Sessions. Wollen Sie einen Snapshot erstellen, gehen Sie über STORAGE • LUNS • LUNS und wählen nach einem Rechtsklick auf die gewünschte LUN den Menüpunkt SNAPVIEW • CREATE SNAPS. Geben Sie dem Snapshot einen Namen. Auf Wunsch weisen Sie ihn einer Storage-Group zu.

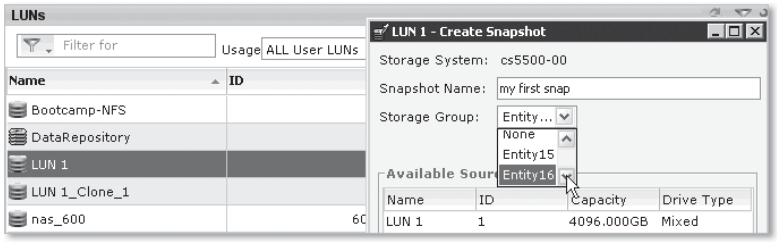


Abbildung 11.104 Erstellen eines Snapshots

Danach wählen Sie aus demselben Menü SnapView • Start SnapView Session. Benennen Sie die SnapView-Session. Ihre gewünschte LUN ist schon aufgelistet. Aktivieren Sie den Mode Consistent, können dieser SnapView-Session zu einem späteren Zeitpunkt keine weiteren Quell-LUNs oder Clones hinzugefügt werden.

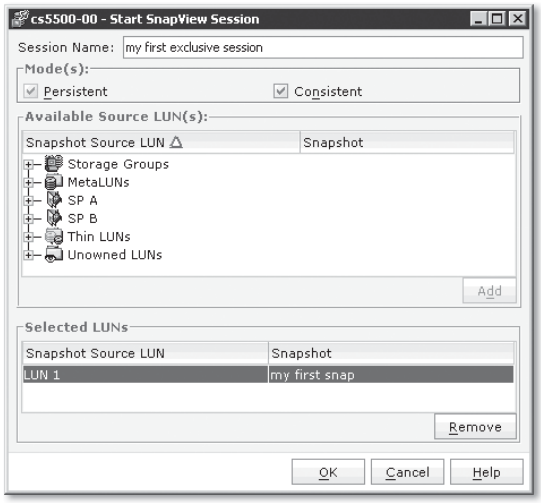


Abbildung 11.105 Konfigurieren einer SnapView-Session

Wenn Sie den Snapshot einem Host präsentieren wollen, gehen Sie über den Reiter Data Protection auf Snapshots • LUN Snapshots • Snapshot LUNs. Selektieren Sie Ihre SnapView-Session. Klicken Sie auf Activate. Wählen Sie die neu erstellte Session aus.

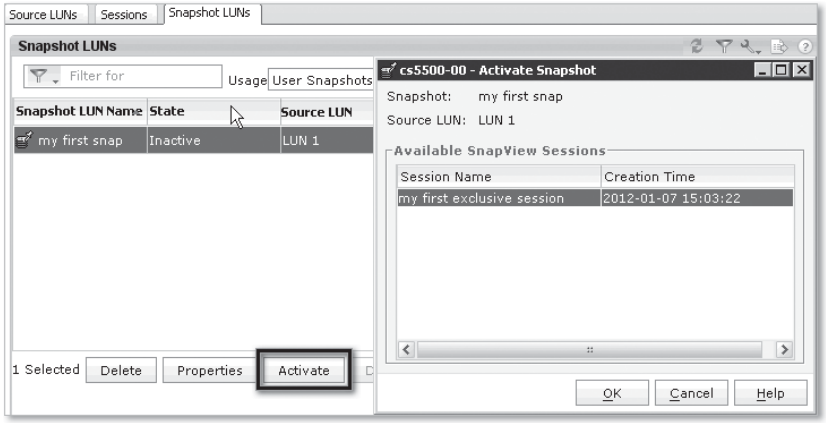


Abbildung 11.106 Aktivieren eines Snapshots

Sie können den Snapshot auf die gewohnte Weise über Add Storage... in vCenter importieren. Achten Sie darauf, dass Sie die VMFS-Mount-Option Assign a new signature wählen.

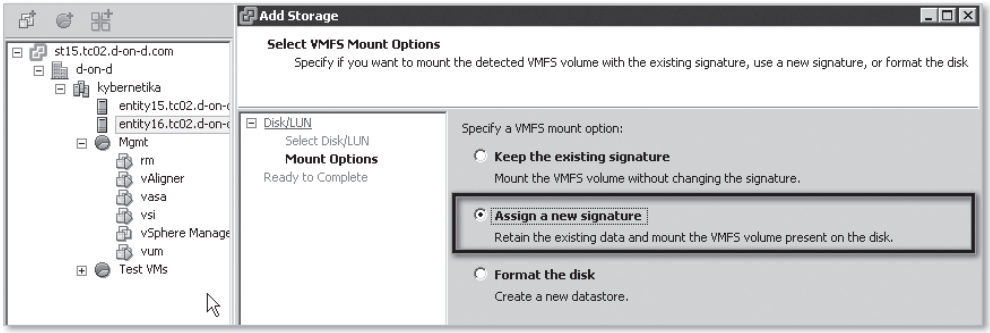


Abbildung 11.107 Zuweisen einer neuen Signatur

Nun können Sie auf Ihren Snapshot zugreifen und gewünschte Daten über den Datastore-Browser vom Snapshot in einen anderen Datastore verschieben.

Clones sind Kopien, die mit der Quell-LUN identisch sind. Sie erstellen sie am einfachsten über den Wizard. Sie finden ihn unter DATA PROTECTION • COMMON DATA PROTECTION TASKS • CREATE CLONE.

Wissenswertes zu Clones und Snapshots

Tipp: Falls Sie performance-kritische Aktionen mit Clones planen, erstellen Sie einen dedizierten Storage-Pool oder RAID-Gruppe für diesen Zweck. Ein VNX-System bietet Ihnen diese Möglichkeit. Snapshots sind abhängige Kopien und eignen sich daher nicht für performance-kritische Anwendungen. Deshalb benötigen Sie nicht zwingend einen dedizierten Storage-Pool.

11.4.6 Dateibasierte Snapshots und Clones

Im Gegensatz zur blockbasierten Methode müssen Sie keine Vorkehrungen treffen, um einen Snapshot zu erstellen. Im Umgang mit dateibasierten Snapshots, die zur Unterscheidung *File-System-Checkpoints* genannt werden, haben Sie die Möglichkeit, einen Planer aufzurufen. Mit diesem können Sie zu gewünschten Tageszeiten automatisiert File-System-Checkpoints erstellen.

Loggen Sie sich in Unisphere ein. Um einen File-System-Checkpoint zu erstellen, gehen Sie über den Reiter DATA PROTECTION auf SNAPSHOTS • FILE SYSTEM CHECKPOINTS • CHECKPOINTS. Klicken Sie auf CREATE. Wählen Sie in der Eingabemaske das gewünschte Dateisystem aus. Bestimmen Sie, ob der File-System-Checkpoint nur les- oder auch beschreibbar sein soll. Einmalig pro Dateisystem dürfen Sie auch bestimmen, aus welchem Storage-Pool-for-File sich das VNX-System für den File-System-Checkpoint bedienen soll.

Wollen Sie die Erstellung der File-System-Checkpoints automatisieren, klicken Sie über den Reiter SCHEDULES im selben Menü auf CREATE. Füllen Sie die selbsterklärende Eingabemaske aus. Bestätigen Sie Ihre Auswahl mit OK.

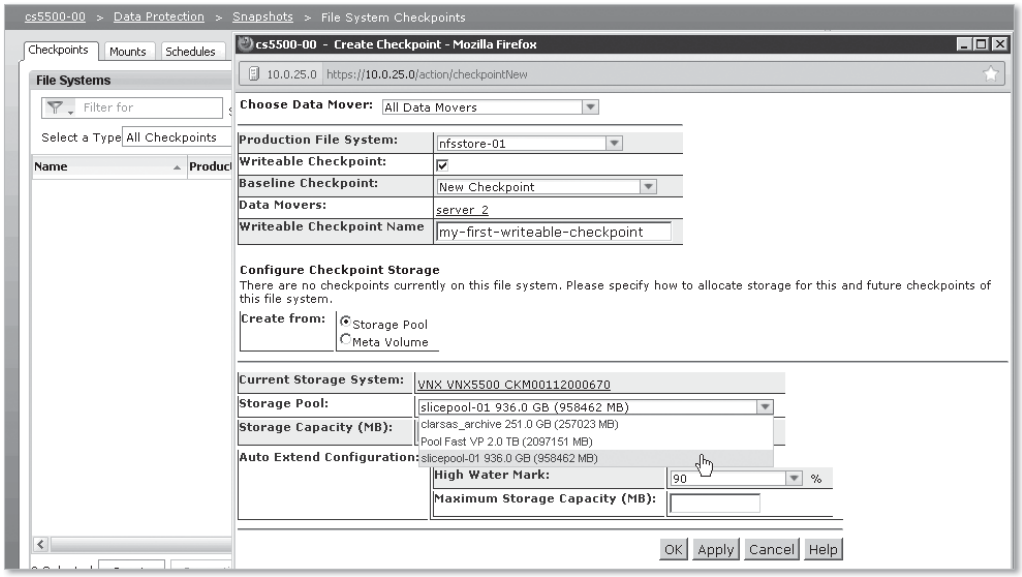


Abbildung 11.108 Erstellen eines File-System-Checkpoints

Gehen Sie auf STORAGE • SHARED FOLDERS • NFS, um den neu erstellten File-System-Checkpoint einem ESXi-Host oder ESX-Cluster zu präsentieren. Klicken Sie auf CREATE. Akzeptieren Sie den vorgeschlagenen Pfad. Sie können auch einen anderen wählen, aber dann müssen Sie den File-System-Checkpoint auch dahin neu verknüpfen. Tragen Sie die IP-Adressen Ihrer ESXi-Server, denen Sie Zugriff auf den File-System-Checkpoint geben wollen, in die Eingabeflächen von READ/WRITE HOSTS und ROOT HOSTS ein.

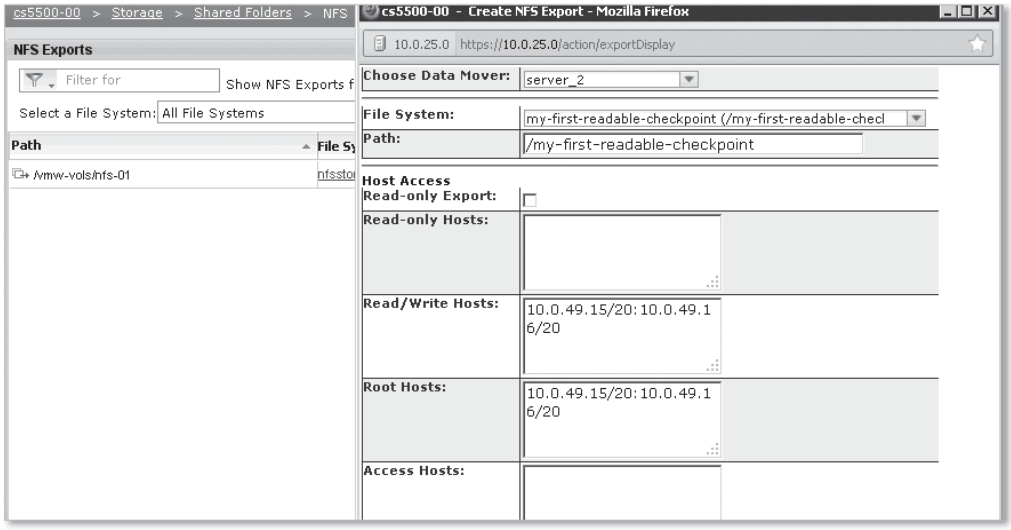


Abbildung 11.109 Konfigurieren eine File-System-Exports

Der File-System-Checkpoint ist jetzt bereit, auf die gewohnte Weise über Add Storage... in vCenter importiert zu werden.

Lese- und Schreibzugriff von File-System-Checkpoints

Ein File-System-Checkpoint kann als les- und beschreibbar markiert werden. Falls Sie ihn nur als lesbar erstellt haben, so können Sie ihn auch dann nicht beschreiben, wenn Sie ihn les- und beschreibbar exportieren.

Erstellen eines Clones

Clones entsprechen im dateibasierten Bereich Ihres VNX-Systems einer Replikation und werden dementsprechend als *Replication* bezeichnet. Replications können ein lokales oder ein fernes Ziel eines Quelldateisystems sein. Für ein Fernziel benötigen Sie ein zweites VNX-System. Replications benötigen eine fixe Verbindung von Quelle und Ziel. Diese Verbindung nennt sich *Data Mover Interconnect*. Für die Erstellung einer lokalen Replication besteht dieser schon; er heißt *Loopback*.

Sie erstellen eine Replication am einfachsten über den Wizard. Sie finden ihn unter Data Protection • Common Data Protection Tasks • Create Replication for File.

11.4.7 VMFS Volumen erweitern mit VNX

Erstellen eines Extents

Erstellen Sie eine neue LUN, und fügen Sie sie Ihrer Storage-Group hinzu wie in Abschnitt 11.2.2, »Konfiguration der VNX für blockbasierten Zugriff«, beschrieben. Bei einem ESX-Cluster müssen Sie die LUN für jeden Node der entsprechenden Storage-Group hinzufügen. Das erledigen Sie mit Add to Storage Group in einem Schritt. Danach gehen Sie auf vCenter, und wählen Sie den zu erweiternden VMFS-Datastore aus. Klicken Sie auf Properties am rechten unteren Bildschirmrand. Im geöffneten Fenster rufen Sie über Increase das Kontextmenü auf, um einen Extent hinzuzufügen.

VMFS-Datastore-LUN-Growing

Gehen Sie in Unisphere über den Reiter Storage • LUNs • LUNs. Rechtsklicken Sie auf eine LUN Ihrer Wahl. Im Kontextmenü rufen Sie Expand auf. Geben Sie hier die gewünschte Größe an. Gehen Sie dann auf vCenter, und wählen Sie den zu erweiternden VMFS-Datastore aus. Klicken Sie auf Properties am rechten unteren Bildschirmrand. Im geöffneten Fenster lassen Sie sich zuerst die neue Kapazität mit Refresh anzeigen. Klicken Sie dann auf Increase, um den VMFS-Datastore zu erweitern. Wählen Sie die zu erweiternde LUN aus.

Migration eines VMFS-Datastores auf eine größere LUN

Ein Spezialfall, einen Datastore wachsen zu lassen, ist die *LUN-Migration* auf eine größere LUN. Dieser Fall kommt beispielsweise bei Performance-Engpässen zum Tragen, das heißt, wenn Sie Ihre LUN über mehr Spindeln verteilen wollen. Eine solche Migration können Sie im laufenden Betrieb vollziehen.

Erstellen Sie in einem Testszenario mit VSI einen 50 GB großen VMFS-Datastore aus einer RAID-Gruppe. Wie das geht, haben wir in Abschnitt 11.3.1, »Erstellen eines VMFS-Datastores«, beschrieben. Migrieren Sie eine laufende VM in den neu erstellten VMFS-Datastore. Das ist die Ausgangslage. Legen Sie in Unisphere eine LUN von 100 GB aus einem Storage-Pool an, ohne diese einer Storage-Group zuzuweisen. Dieser Vorgang ist in Abschnitt 11.2.2, »Konfiguration der VNX für blockbasierten Zugriff«, beschrieben. Über den Reiter STORAGE • LUNs • LUNs wählen Sie nun die zu migrierende Quell-LUN mit einem Rechtsklick auf den Menüpunkt MIGRATE aus. Suchen Sie sich die Ziel-LUN aus, und bestätigen Sie Ihre Auswahl. Einige Zeit später ist die Migration beendet. Ihre Ziel-LUN besteht nun nicht mehr.

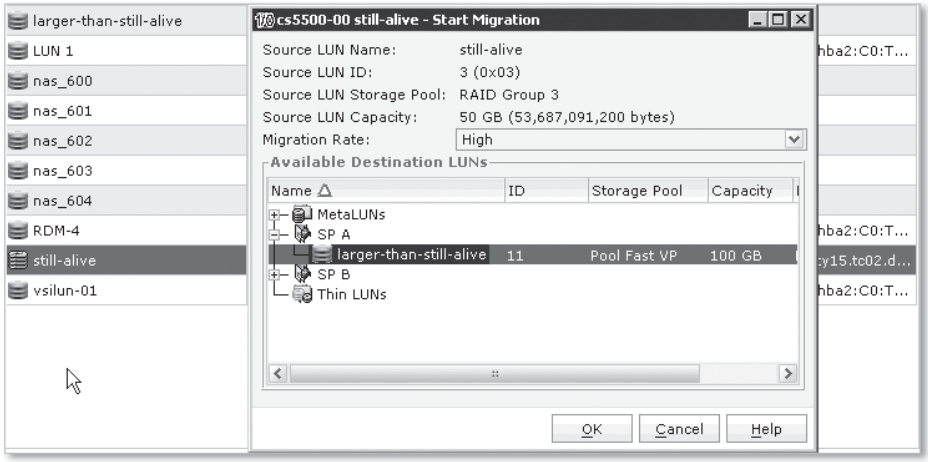


Abbildung 11.110 LUN-Migration in Unisphere

Gehen Sie dann auf vCENTER, und wählen Sie den zu erweiternden VMFS-Datastore aus. Klicken Sie auf PROPERTIES am rechten unteren Bildschirmrand. Im geöffneten Fenster lassen Sie sich als Erstes die neue Kapazität mit REFRESH anzeigen. Klicken Sie dann auf INCREASE, um den VMFS-Datastore zu erweitern. Wählen Sie die zu erweiternde LUN aus.

11.4.8 Erweitern eines NFS-Datastores mit VNX

Die Erweiterung eines NFS-Datastores ist automatisiert. Sie erfahren in Abschnitt 11.2.5, »Konfiguration der Volumes für Dateisysteme«, welche Einstellungen Sie tätigen müssen.

Loggen Sie sich in Unisphere ein. Klicken Sie auf Storage • Storage Configuration • File Systems. Wählen Sie das zu erweiternde Dateisystem aus, und klicken Sie auf Extend. In der Eingabemaske finden Sie den Parameter Extend Size. Geben Sie die gewünschte Erweiterungskapazität ein, und bestätigen Sie Ihre Eingabe.

Mechanismen zur Erweiterung von Dateisystemen

Es wird zwischen zwei Mechanismen zur automatischen Erweiterung unterschieden: *thin* und *auto-extend*. Thin kennt ein obligatorisches Limit, das nicht überschritten werden kann. Der Vorteil ist, dass diese Obergrenze einem ESXi-Host bekannt ist. Im Falle von *auto-extend* ist dieses Limit optional. Geben Sie keine Obergrenze an, kann das Dateisystem bis zur maximalen Größe des Storage Pools for File oder 16 TB anwachsen. Der ESXi-Host kennt nur die ursprüngliche Kapazität.

Falls Sie beabsichtigen, ein Thin-provisioned Dateisystem zu erweitern, müssen Sie Thin Provisioning deaktivieren. Danach können Sie das Dateisystem erweitern und Thin Provisioning wieder aktivieren. Das geht am schnellsten mit dem CLI.

Lesen Sie den Namen des zu erweiternden Dateisystems mit `nas_fs -list` aus:

```
[nasadmin@cs5500-00 ~]$ nas_fs -list
```

Schalten Sie Thin Provisioning mit `nas_fs -modify` kurzzeitig aus:

```
[nasadmin@cs5500-00 ~]$ nas_fs -modify nfsstore-01 -auto_extend no -thin no
```

Erweitern Sie das Dateisystem mit `nas_fs -xtend`:

```
[nasadmin@cs5500-00 ~]$ nas_fs -xtend nfsstore-01 size=10G
```

Schalten Sie Thin Provisioning wieder ein, und geben Sie neue Limits mit:

```
[nasadmin@cs5500-00 ~]$ nas_fs -modify nfsstore-02 -auto_extend yes -thin yes
  -hwm 75% -max_size 280G
```

11.4.9 Alignment von Volumes

Wenn Sie ein Tool zum einfachen Alignment diverser Betriebssysteme suchen, besuchen Sie den Hyperlink *http://nickapedia.com/2011/11/03/straighten-up-with-a-new-uber-tool-presenting-uberalign/*. Das Werkzeug kommt in zwei Paketen:

- ÜBERAlign Console 1.1 (für Windows mit dotnet4)
- ÜBERAlign vAligner (OVA-Datei)

Das Werkzeug erlaubt es zum einen, misaligned VMS zu erkennen und entsprechend zu korrigieren. Zum anderen erlaubt es auch einen Space-Reclaim von ungenutzter Speicherkapazität von Thin VMs von Windows- und Linux-Betriebssystemen. Das ist kein offizielles EMC-Werkzeug. Die Überprüfungen des Alignments sind es wert, dieses Werkzeug auszuprobieren. Eine ausführliche Anleitung finden Sie ebenfalls unter dem angegebenen Link.

11.4.10 Installation VSI

Der *EMC Virtual Storage Integrator (VSI)* ist ein vCenter-Plugin-Framework. Das heißt, EMC vereint viele Funktionalitäten unterschiedlichster Produkte unter einem Hut. Dementsprechend variabel ist auch die Installation. Sie finden die benötigten Programme in Powerlink unter HOME • SUPPORT • SOFTWARE DOWNLOADS AND LICENSING. Für ein VNX-System mit Multipathing-Fähigkeit benötigen Sie deshalb die folgenden Installationspakete des Frameworks:

1. *VSI for VMware vSphere Storage Viewer*
   (*emc-vsi-sv-5.0.0-vmware-vsphere-WINDOWS-x86.exe*)
2. *VSI for VMware vSphere Path Management*
   (*emc-vsi-pm-5.0.0-vmware-vsphere-WINDOWS-x86.exe*)
3. *Navisphere CLI*
   (Installationsanweisung siehe Abschnitt 11.4.1, »Command-Line Interfaces«)
4. *Unisphere CLI*
   (VNXe-CLI-Windows-32-x86-english-1.5.1.1.0001)
5. *VSI for VMware vSphere Unified Storage Management*
   (*emc-vsi-usm-5.0.0.86-vmware-vsphere-WINDOWS-x86*)

Installieren Sie die Pakete in der aufgelisteten Reihenfolge. Akzeptieren Sie die Installation des Solution Enablers mit dem ersten Paket. Beim nächsten Paket lassen Sie die Installation einfach durchlaufen.

VSI for VMware vSphere Path Management

Falls Sie PPVE einsetzen, müssen Sie das PPVE-Paket *rpowermt* zusätzlich auf dem System installieren, auf dem VSI läuft. Die Installationsanleitung finden Sie in Abschnitt 11.4.4, »Installation EMC PowerPath/VE«.

Danach gilt es, das Navisphere CLI einzuspielen. Der nächste Schritt ist die Installation des Unisphere CLI. Akzeptieren Sie die Grundeinstellung. Extrahieren Sie dann das Paket für *Unified-Storage-Management* (USM). Es enthält weitere drei Pakete:

1. *USM* (*emc-vsi-usm-5.0.0.86-vmware-vsphere-WINDOWS-x86.exe*)
2. *Access Control Utility* (*emc-acu-2.0.0.158-WINDOWS-x86.exe*)

Die Pflichtinstallation ist nur das USM-Paket selbst. Die anderen beiden optionalen Pakete ermöglichen eine Zugriffskontrolle bzw. erleichtern das Einrichten für die Manipulation der dateibasierten Speicherkapazität. Die Installation des USM umfasst lediglich das Einspielen des Pakets. Dasselbe gilt für das Access Control Utility (ACU).

VSI und Netzwerke

VSI benötigt zur Nutzung sämtlicher Funktionen Zugriff auf vCenter und das Speichernetzwerk Ihrer NFS-Datastores.

Konfigurieren der VSI-Module

Starten Sie als Erstes das Paket ACU, um sich eine Zugriffsdatei für Ihr VNX-System zu erstellen. Mit dieser gewähren Sie sich Zugriff auf das VNX-System über das vCenter.

Starten Sie das ACU, und klicken Sie auf ADD, um eine neue Zugriffsdatei zu erstellen. ACU bezeichnet das als *Access-Profile*. Benennen Sie das Access-Profile, und klicken Sie auf NEXT. Mit einem Klick auf ADD rufen Sie einen Wizard auf, um Ihr VNX-System hinzuzufügen. Wählen Sie als SYSTEM TYPE VNX aus. Bei der Eingabemaske zur VNX ACCESS METHOD müssen Sie beides, FILE und BLOCK, aktivieren. Danach fügen Sie als Erstes die VNX BLOCK CREDENTIALS ein. Ihre STORAGE PROCESSOR IP ist die des SPA. Den SCOPE definieren Sie mit GLOBAL. Sobald der blockbasierte Bereich der VNX authentifiziert ist, werden Sie aufgefordert, die gleiche Prozedur für den dateibasierten Bereich zu wiederholen. Der Hostname ist die IP-Adresse von Unisphere Ihres VNX-Systems. Aktivieren Sie in dieser Maske auch DHSM. Es ermöglicht die Erstellung eines Systembenutzers, der über Berechtigungen verfügt, Snaps und Clones zu erstellen. In der nächsten Maske legen Sie diesen Benutzer an und verteilen Zugriffsberechtigungen an die Server, die auf VSI zugreifen. In DHSM HOST ACCESS wählen Sie ALLOW ACCESS FROM SPECIFIC HOSTS. ACU schlägt Ihnen die virtuelle Maschine, von der aus Sie konfigurieren, vor. Tragen Sie die IP-Adressen sämtlicher vSphere-Clients ein, auf denen Sie VSI nutzen wollen.

Wichtige Informationen zu DHSM

Diesen Benutzer müssen Sie für sämtliche aktiven Data Mover anlegen. Achten Sie darauf, dass Benutzer sowie das Passwort immer gleich lauten. Sie können das im CLI mit dem Befehl `server_http server_2 -info` überprüfen.

Nun werden Sie aufgefordert, die Zugriffsprivilegien einzugeben. Wählen Sie SELECTED STORAGE POOLS aus der Liste aus. Nun erscheint eine Maske mit allen zur Verfügung stehenden Storage-Pools. Selektieren Sie diejenigen, die Sie unter Zugriff von VSI haben wollen.

Beenden Sie den Wizard mit einem Klick auf FINISH. Sie können den erstellten Eintrag jederzeit anpassen. Wählen Sie nun Ihr neu erstelltes Access-Profile aus, und exportieren Sie es. Speichern Sie die Datei mit einem Passwort an einem Ort Ihrer Wahl, und beenden Sie das ACU.

Starten Sie Ihren vSphere-Client. VSI ist bereits korrekt eingeschaltet. Klicken Sie auf das Icon VSI, das Sie über HOME • SOLUTIONS AND APPLICATIONS finden. In der Menüstruktur zur linken Seite finden Sie die installierten Plugins von VSI. Klicken Sie dazu auf SETTINGS • GENERAL • FEATURE MANAGER. Weiter unten sehen Sie den STORAGE VIEWER. Verbinden Sie sich mit dem SOLUTIONS ENABLER, indem sie FEATURES • SOLUTIONS ENABLER • TEST CONNECTION anwählen. Lassen Sie sich eine erfolgreiche Verbindung bestätigen. Wählen Sie danach FEATURES • STORAGE VIEWER • VNX SYSTEMS aus, füllen Sie die Eingabemaske aus, und beenden Sie diese mit DISCOVER NEW VNX unterhalb der Mitte am rechten Bildschirmrand.

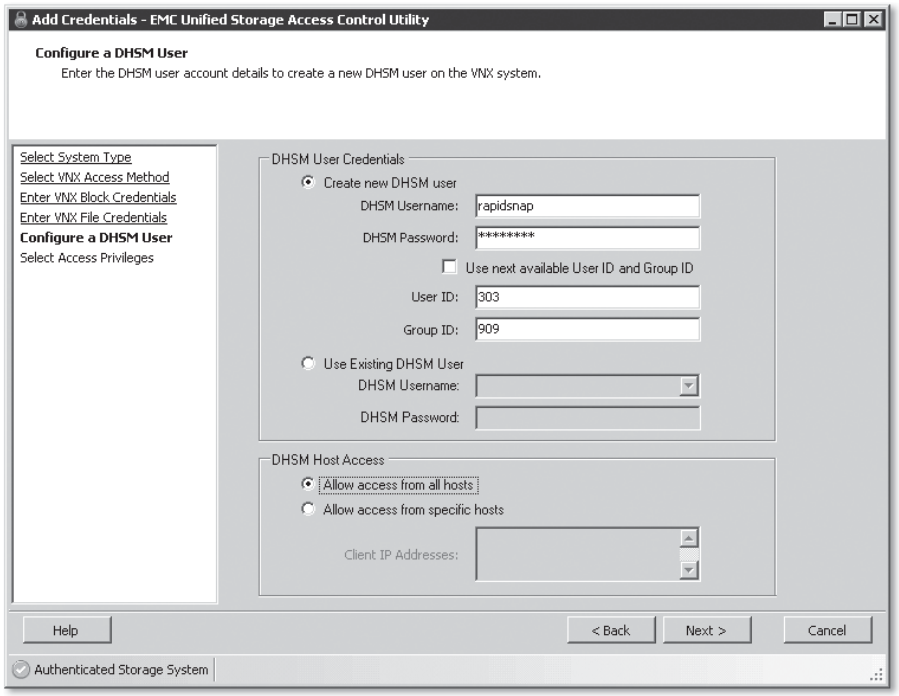


Abbildung 11.111 Erstellen eines VNX-Systembenutzers

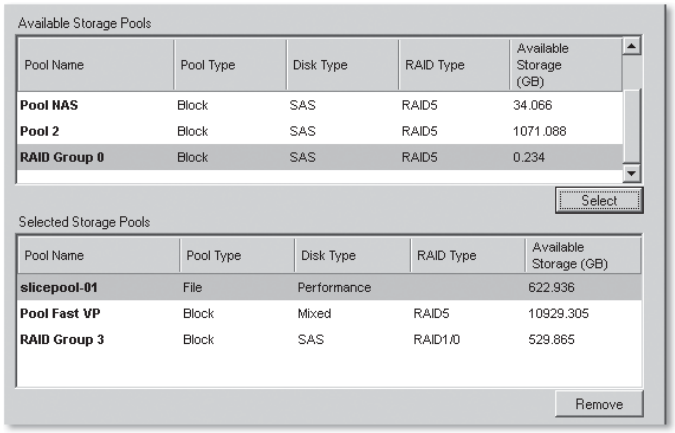


Abbildung 11.112 Privilegien von VSI auf Storage-Pools

Klicken Sie im Menü zur linken Seite auf Features • Unified Storage Management und darin auf Add. Wählen Sie aus der Maske Import Access Profile aus. Klicken Sie auf Next. Geben Sie den Ablageort Ihrer soeben erstellten Zugriffsdatei und das Passwort ein. Beenden Sie den Wizard. Ihr VNX-System wird mit den definierten Privilegien VSI bekanntgegeben.

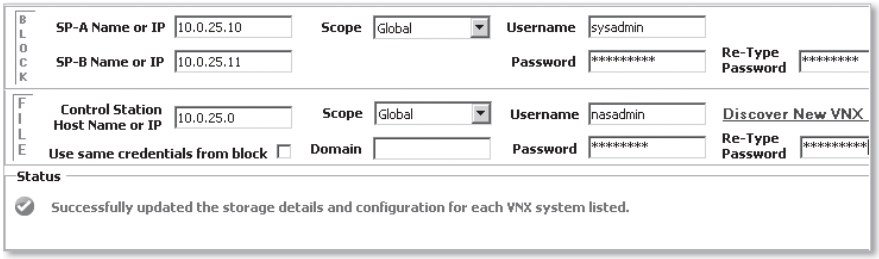


Abbildung 11.113 Registrierung des VNX-Systems in VSI

11.4.11 Installation des EMC Replication Managers

Der Einsatz des Replication Managers, einer zentralen Snapshot-, Clone- und Replikations-Suite, setzt voraus, dass Sie für Ihr VNX-System über entsprechende Lizenzen verfügen. Den Replication Manager können Sie 90 Tage testen und in einer virtuellen Maschine aufsetzen.Nebst Windows werden auch Unix- und Linux-Systeme unterstützt. Die Installation gestaltet sich einfach, obwohl sie auf fünf Pakete verteilt ist.

Die Pakete können Sie von Powerlink oder von EMC beziehen. AdmSnap finden Sie unter Home • Support • Software Downloads and Licensing • Downloads S • SnapView. Den Replication Manager können Sie von Home • Support • Software Downloads and Licensing • Downloads P-R • Replication Manager beziehen.

Installieren Sie in dieser Reihenfolge:

1. *SMI-S-Provider*: Siehe die Anleitung in Abschnitt 11.4.2, »Installation von VASA«.
2. *Navisphere Secure CLI*: Siehe Abschnitt 11.4.1, »Command-Line Interfaces«.
3. *AdmSnap*: Rufen Sie das Installationspaket auf. Bestätigen Sie am Ende der Installation mit Done.
4. *Replication Manager 5.4.0*: Akzeptieren Sie die Grundeinstellungen, und installieren Sie den Server, die Console und deb SQL-Agent. Der Replication Manager erlaubt individuelle Anpassungen von Ports und Protokollen. Die Installation im Beispiel beruht auf Grundeinstellungen.
5. *Replication Manager Service Pack 5.4.1*: Bestätigen Sie sämtlichee Aufforderungen. Beenden Sie die Installation mit Klick auf Finish.

Tipp: Installation unter Windows

Die virtuelle Maschine sollte noch nicht Teil einer Windows-Domäne sein, es sei denn, Sie sind Domain-Administrator mit dem Namen »Administrator«. Geben Sie in Folge bei der Eingabemaske nur den Username »Administrator« und das Password des lokalen Administrators ein. Nach der Erstanmeldung in Replication Manager erstellen Sie sich einen Local User. Danach können Sie die Domänenanbindung vollziehen und die virtuelle Maschine durchstarten.

Abbildung 11.114 Eingabemaske zur Benutzerauthentifizierung

Einrichten des Replication Managers

Da der Replication Manager ein zentrales Administrations-Werkzeug ist, müssen Sie ihm nebst einem Benutzer (rollenbasierte Verwaltung ist möglich) noch mindestens einen Server und ein Speichersystem bekanntgeben. Dafür finden Sie zur rechten Seite Wizards. Klicken Sie auf REGISTER PRODUCTION AND MOUNT HOST. Wählen Sie einen Windows-Server als Proxy-Host. Hier werden später zur Wiederherstellung einzelner Dateien Windows-Laufwerke bereitgestellt. Melden Sie sich zusätzlich in dieser Eingabemaske am vCenter an.

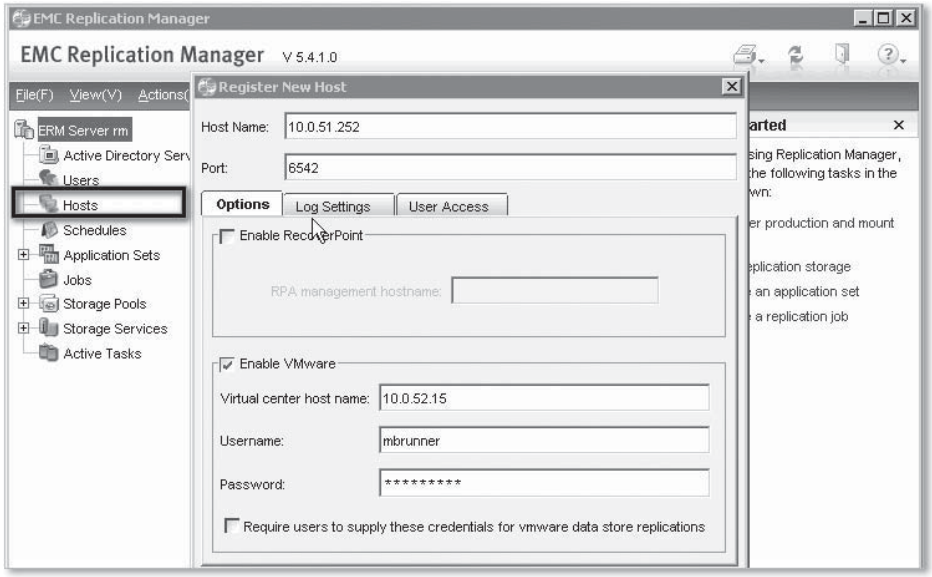


Abbildung 11.115 Replication Manager: Server hinzufügen

Bevor Sie fortfahren, stellen Sie sicher, dass Sie das VNX-System auf den Umgang mit Snapshots eingerichtet haben. Falls nicht, führen Sie jetzt die Schritte in Abschnitt 11.4.5, »Blockbasierte Snapshots und Clones«, durch. Nachdem der erste Server erfolgreich registriert wurde, starten Sie den Wizard ADD REPLICATION STORAGE. Klicken Sie auf ADD VNX FILE-BASED STORAGE ARRAY TO THIS LIST, und füllen Sie die Eingabemaske aus.

Nun wiederholen Sie diesen Schritt im Wizard, indem Sie dieses Mal auf die Seriennummer Ihrer VNX klicken. Wenn Sie dieses Formular ausgefüllt haben, klicken Sie auf NEXT.

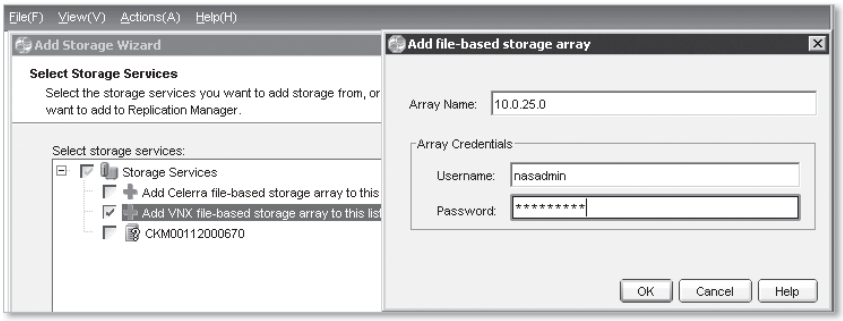


Abbildung 11.116 Registrieren des dateibasierten Bereichs der VNX

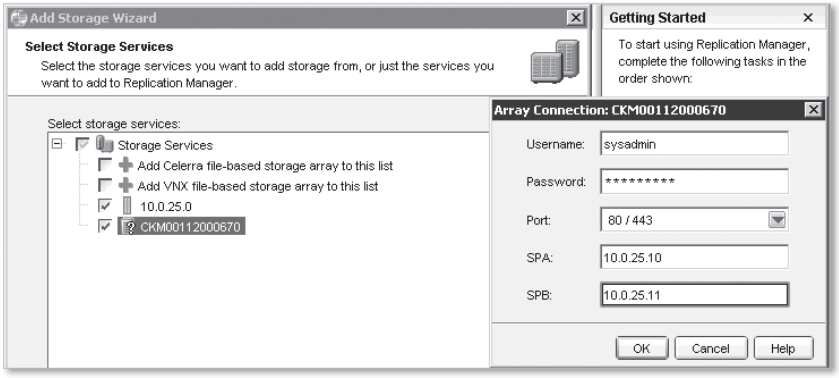


Abbildung 11.117 Registrieren des blockbasierten Bereichs der VNX

Nach einer kurzen Überprüfung werden Sie aufgefordert, ein Replikationsziel anzugeben. Wählen Sie es aus.

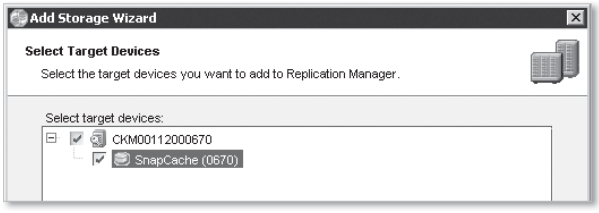


Abbildung 11.118 Auswählen des Replikationsziels

Nach einer weiteren Verifikation ist Ihr VNX-System vollständig registriert.

11.4.12 Installation von vSphere ESXi 5.0

Generell ist es einfacher, ESXi-SErver direkt auf den internen Festplatten des physischen Servers zu installieren oder ab USB-Drive zu booten. Verwenden Sie jedoch Blade-Systeme, bietet sich das Booten über SAN an.

Boot-LUNs in der Größe von 20 GB bieten mehr als ausreichend Kapazität. Weisen Sie die Boot-LUN der entsprechenden Storage-Group des Hosts zu, und verwenden Sie dabei als HOST LUN ID die Zahl 0. Das erlaubt Ihnen, auf einfachste Weise die Boot-LUN von anderen zu unterscheiden. Es gibt Blade-Systeme, die explizit nach einer Boot-LUN 0 verlangen.

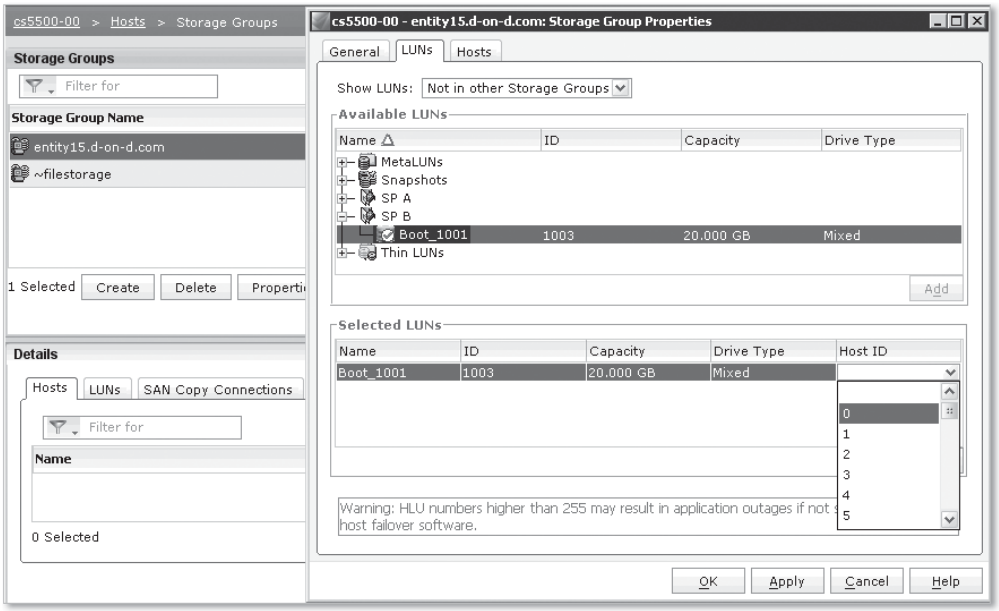


Abbildung 11.119 Zuweisung der Host-ID (LUN 0)

Wenn Sie die Host-ID einer LUN explizit vergeben wollen, müssen Sie die Properties der gewünschten Storage-Group aufrufen und die hinzuzufügende LUN auswählen. Dann können Sie sich die HOST ID, wie in Abbildung 11.119 ersichtlich, aussuchen. Nähere Informationen zur Erstellung einer LUN entnehmen Sie Abschnitt 11.2.2.

11.4.13 VNX Virtual Storage Appliance

Für den Fall, dass Sie Tests an einem VNX-System durchführen wollen und dazu nicht Ihr produktives Speichersystem missbrauchen wollen, stellt Ihnen EMC eine *VNX Virtual Storage Appliance* (VSA) zur Verfügung. Diese VSA ist allerdings auf den dateibasierten Bereich zugeschnitten, bietet abgesehen von dieser Einschränkung sämtliche Möglichkeiten. Sie können die VNX VSA von EMC direkt beziehen. Einfacher und schneller geht es, indem Sie den *ÜBER VNX (NFS) v1* von *nickapedia.com* herunterladen. Sie finden die VSA hier: *http://nickapedia.com/2011/04/08/new-uber-model-uber-vnx-nfs-v1/.*

Wichtiger Hinweis zum Einsatz der VSA

Die VNX VSA ist nicht für den produktiven Einsatz geeignet!

11.5 Troubleshooting – Erste Hilfe

Dieser Abschnitt vermittelt Ihnen nützliche Tipps im Umgang mit einem VNX-System. Es zeigt Ihnen Symptome und die Behebung des Fehlers auf.

11.5.1 Der ESXi-Host sieht keine FC-LUN

Obwohl das Zoning des SAN korrekt ist, können Sie dem ESXi-Server die LUN nicht hinzufügen.

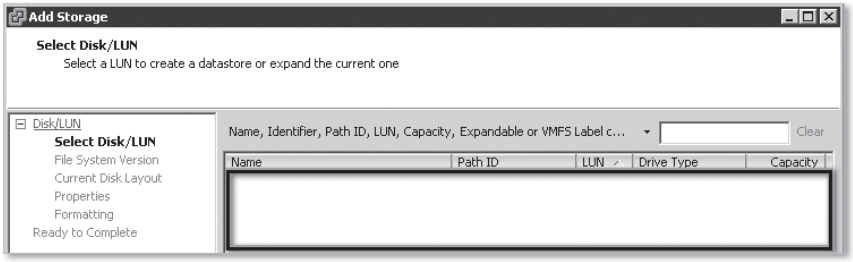


Abbildung 11.120 Auswahl der LUNs

Ein Rescan der HBAs zeigt ebenfalls nicht den gewünschten Erfolg. Sie sehen im vCenter folgendes Bild, und die LUN scheint verfügbar.

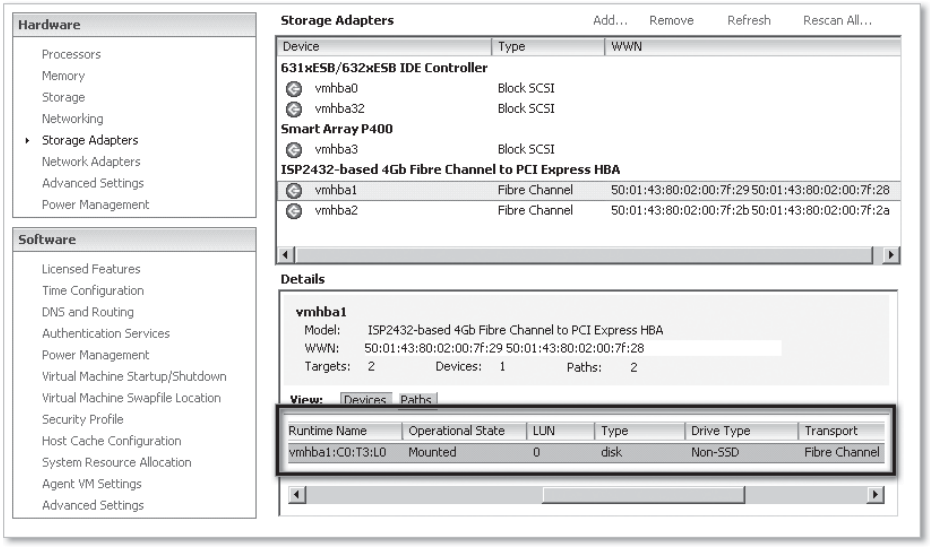


Abbildung 11.121 Sicht des Storage-Adapters

Wählen Sie sich über Unisphere in das VNX-System ein, und überprüfen Sie, ob in der Storage-Group die gewünschte LUN hinzugefügt wurde.

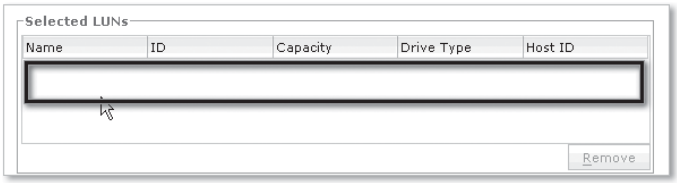


Abbildung 11.122 Auszug aus den Eigenschaften einer Storage-Group

Die LUN wird im Fenster SELECTED LUNS nicht angezeigt. Weisen Sie die LUN der Storage-Group zu, und bestätigen Sie Ihre Auswahl mit OK. Sie erfahren in Abschnitt 11.2.2 wie Sie vorgehen müssen.

Führen Sie einen RESCAN der STORAGE ADAPTERS durch. Verfahren Sie zur Erstellung eines VMFS-Datastores wie gewohnt.

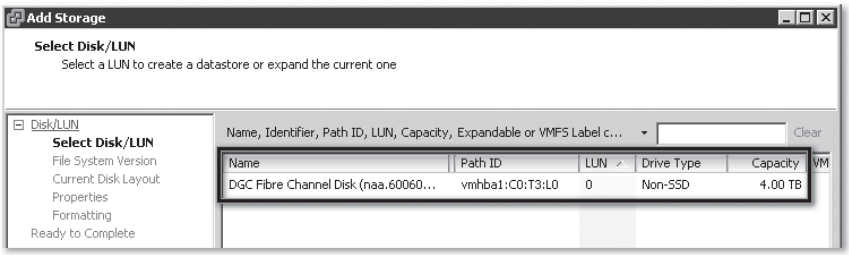


Abbildung 11.123 Auszug aus dem VMware-Wizard »Add Storage«

Die LUN ist nun sichtbar und wird mit den korrekten Werten dargestellt.

11.5.2 Der ESXi-Host hat keinen Schreibzugriff-Zugriff auf den NFS-Datastore

Obwohl Sie den NFS-Datastore an Ihren ESXi-Server anbinden können und er sich auch öffnen lässt, können Sie nicht darauf schreiben.

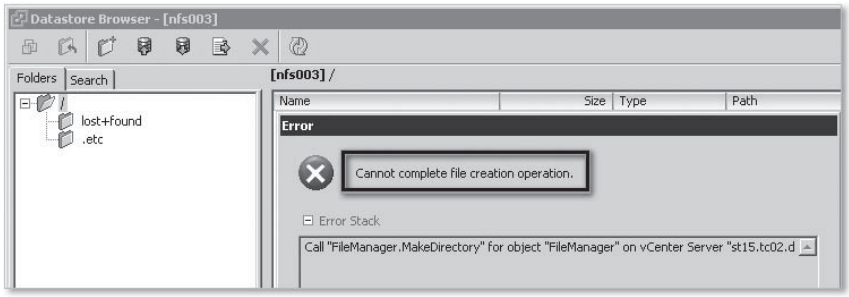


Abbildung 11.124 Kein Schreibzugriff

Loggen Sie sich via SSH in den dateibasierten Bereich des VNX-Systems ein. Setzen Sie die Umgebungsvariable, und geben Sie den Befehl `server_export` ein, um zu sehen, welche Dateisysteme exportiert sind.

```
[nasadmin@cs5500-00 ~]$ export NAS_DB=/nas
[nasadmin@cs5500-00 ~]$ server_export server_2
server_2 :
export "/vmw-vols/nfs-01" name="/nfsstore-01" rw=10.0.32.20/20:10.0.32.21/
20 root=10.0.32.21/20
...
```

Achten Sie sich dabei auf die Zugriffsrechte `root` und `rw` des Ziel-Dateisystems. Sollte die IP-Adresse Ihres ESXi-Servers nicht in den beiden Parametern `rw` und `root` vorkommen, müssen Sie die Rechte des Exports ändern. Benutzen Sie den Befehl `server_export`, um Ihrem ESXi-Host den Schreibzugriff zu ermöglichen.

```
[nasadmin@cs5500-00 ~]$ server_export server_2 -Protocol nfs -name nfsstore-
01 -option rw=10.0.32.20/20,root=10.0.32.20/20 /vmw-vols/nfs-01
server_2 : done
```

Handhabung von File-System-Checkpoints

Falls sich herausstellt, dass ein File-System-Checkpoint nur Schreibzugriff zulässt, müssen Sie einen neuen, beschreibbaren File-System-Checkpoint erstellen. Die Anleitung hierfür entnehmen Sie Abschnitt 11.4.6.

11.5.3 Ein Snapshot lässt sich nicht in ESXi präsentieren

Sie machen die seltene Erfahrung einer korrupten Virtual Disk. Gut ist es, wenn Sie einen Snapshot haben, auf den Sie zurückgreifen können. Sie fügen den Snapshot zur Storage-Group hinzu und gehen in das vCenter, um den Snapshot mit einem Rescan der HBAs sichtbar zu machen. Sie sehen das Bild aus Abbildung 11.125.

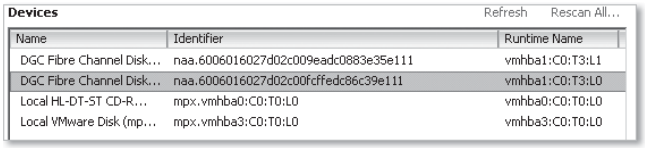


Abbildung 11.125 Die LUN ist sichtbar.

Wenn Sie nun den Snapshot zur Verfügung stellen wollen, präsentiert Ihnen der ADD STORAGE-Wizard die Anzeige aus Abbildung 11.126.

Sie wissen, dass Sie dem Snapshot eine neue Signatur geben müssen. Brechen Sie den Vorgang ab. Überprüfen Sie die SnapView-Session über DATA PROTECTION • LUN SNAPSHOTS • SNAPSHOT LUNs. Aktivieren Sie die Ziel-Snapshot-LUN. Führen Sie erneut einen RESCAN ALL... durch.

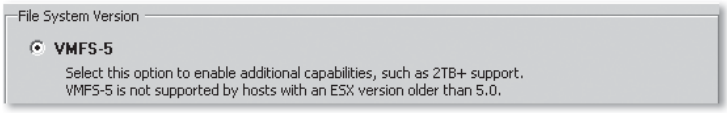


Abbildung 11.126 »Add Storage«

Rufen Sie den ADD STORAGE-Wizard wieder auf. Wählen Sie ASSIGN A NEW SIGNATURE von der Auswahl.

11.5.4 Sie haben Trespassed LUNs

Trespassed LUNs im blockbasierten Bereich

Sie stellen fest, dass die Performance Ihrer VMFS-Datastores nachgelassen hat. Sie wissen, dass einer der Indikatoren *Trespassed LUNs* sind. Das heißt, die Ownership einer LUN passt nicht auf die Zuweisung der LUN an den Storage-Processor.

Öffnen Sie das Kommandozeilenprogramm eines virtuellen Servers, der Navisphere CLI installiert hat. Geben Sie folgende Befehlszeile ein:

```
naviseccli.exe -h 10.0.25.10 -user sysadmin -password password
-scope 0 getlun -trespass
```

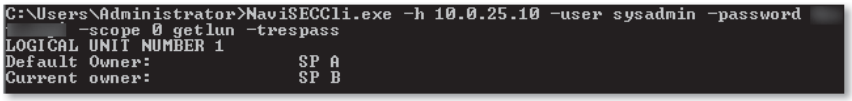


Abbildung 11.127 Ausgabe von »naviseccli«

Führen Sie danach die folgenden beiden Befehlszeilen aus:

```
naviseccli.exe -h 10.0.25.10 -user sysadmin -password password
  -scope 0 trespass mine
naviseccli.exe -h 10.0.25.11 -user sysadmin -password password
  -scope 0 trespass mine
```

Überprüfen Sie den Erfolg mit einer erneuten Eingabe des Befehls:

```
naviseccli.exe 10.0.25.10 -user sysadmin -password password -scope 0 getlun
  -trespass
```

Trespass-Befehl
Dieser Befehl funktioniert nicht für Private LUNs.

Trespassed LUNs im dateibasierten Bereich

Sie stellen fest, dass die Performance Ihrer NFS-Datastores nachgelassen hat. Sie wissen, dass einer der Indikatoren Trespassed LUNs sind. Das heißt, die Ownership einer LUN passt nicht auf die Zuweisung der LUN an den Storage-Processor.

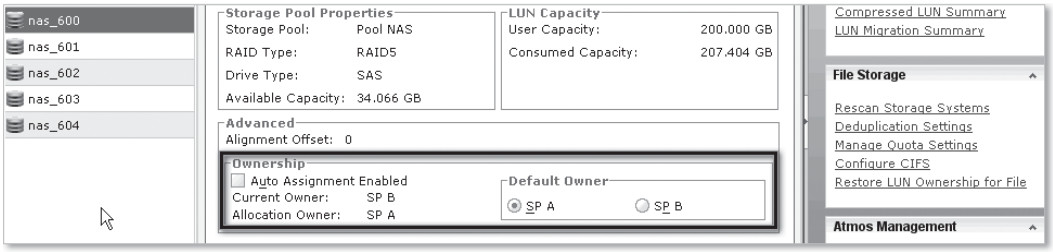


Abbildung 11.128 Beispiel einer Trespassed LUN

In UNISPHERE • STORAGE • LUNS • LUNS sehen Sie, dass Sie Trespassed LUNs haben, die dem Storage-Pool-for-File angehören. Wählen Sie zur Behebung des Zustands vom Menü zur rechten Seite im Bereich FILE STORAGE • RESTORE OWNERSHIP FOR FILE aus.

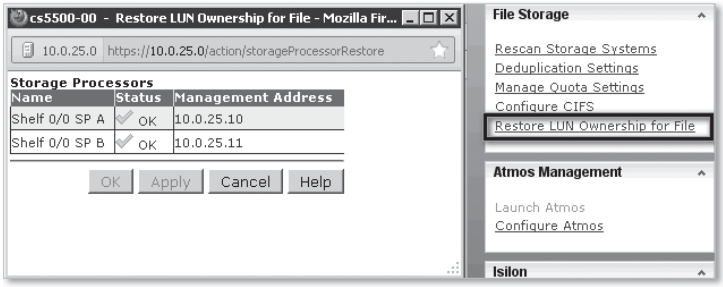


Abbildung 11.129 Wiederherstellen der Default-LUN-Ownership

Nach der Durchführung dieses Prozesses sind die LUNs wieder korrekt zugeordnet.

Die Konfiguration der Virtual Infrastructure 5 kann sehr umfassend und komplex sein. Es gibt viele Punkte, die Sie konfigurieren können oder müssen, um einen reibungslosen Betrieb zu gewährleisten. Auf diese Punkte gehen wir in diesem Kapitel ein.

12 Konfiguration von ESXi und vCenter

Autor dieses Kapitels ist Bertram Wöhrmann, Ligarion, bwoehrmann@ligarion.de

Die gesamte Infrastruktur umfasst nicht nur den vSphere-Host und den vCenter-Server, sondern auch zusätzliche Komponenten. Bei der Konfiguration müssen Sie auch andere Komponenten wie zum Beispiel den Lizenz-Server oder den NTP-Server beachten. Auf den folgenden Seiten gehen wir näher auf die verschiedenen Komponenten sowie die Konfiguration der Virtual Infrastructure 5 ein.

Für die eigentlichen Konfigurationsarbeiten können Sie entweder den Webclient oder den vSphere-Client nutzen. Nicht immer stehen unterschiedliche Möglichkeiten für ein und dieselbe Konfiguration zur Verfügung. Bei der Nutzung des vSphere-Clients kann die Verbindung direkt zum Host oder zum vCenter erfolgen.

An dieser Stelle möchten wir nicht alle Konfigurationsmöglichkeiten abarbeiten, sondern das Ganze themenorientiert durchführen.

Die Themen Storage und Netzwerk beschreiben wir in eigenen Kapiteln.

12.1 Hostprofile

Mit Version 4 der VMware Virtual Infrastructure führte VMware ein neues Feature, und zwar die *Hostprofile*. Diese Funktion hat weiterhin Bestand und ist mit der Version 5 noch leicht erweitert worden. Hostprofile erleichtern die Konfiguration einer Farm von vSphere-Servern. Dadurch ist es möglich, die Konfiguration eines Hosts auf verschiedene andere Hosts zu übertragen und somit identische Systeme zu erhalten.

Es ist nicht mehr nötig, die Konfiguration auf jedem Host einzeln und manuell vorzunehmen. Das spart Zeit, und die Fehleranfälligkeit sinkt. In der Vorgängerversion von vSphere musste bei der Konfiguration von zehn Hosts jeder einzelne Host angefasst werden. Dabei kam es schnell einmal zu Fehlern, wenn z. B. »mal eben« ein neues virtuelles Netzwerk eingerichtet werden musste. Dies störte nicht nur den Betrieb erheblich, sondern konnte auch dazu führen, dass nicht alle Funktionen in der virtuellen Infrastruktur zur Verfügung standen.

Achtung

Hostprofile können nur mit vSphere-Servern genutzt werden, die mindestens mit der Version 4.x installiert sind. Ältere Versionen sind nicht unterstützt.

Durch das einmalige Erstellen eines Hostprofils und das Verteilen auf die einzelnen Server ist eine schnelle und sichere Konfiguration einer vSphere-Farm möglich. Das Erstellen und Verteilen dieser Hostprofile beschreiben wir im Folgenden näher. Als Erstes legen Sie ein Hostprofil von einem fertig konfigurierten Host im System an oder importieren ein bestehendes. Auf der MANAGEMENT-Seite des vSphere-Clients oder über das Menü rufen Sie das Fenster für die HOST PROFILES auf (Abbildung 12.1). Im Fenster der Hostprofile können Sie Profile erstellen, duplizieren, löschen und editieren. Außerdem ist es möglich, vorhandene Cluster und ESXi-Hosts mit einem Profil zu verknüpfen.

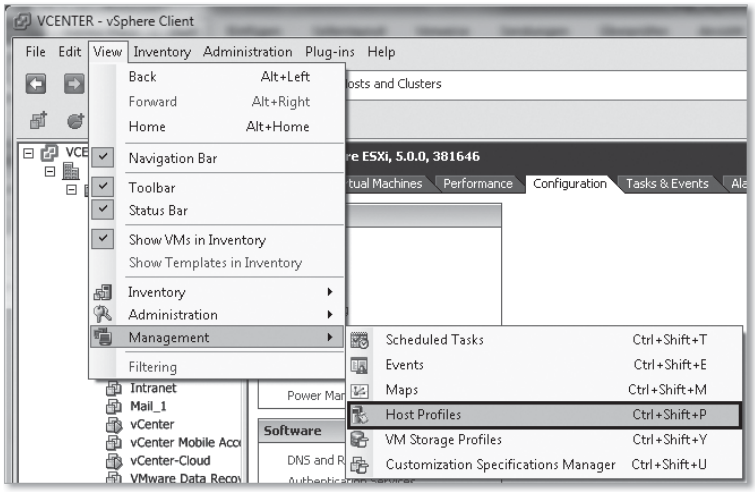


Abbildung 12.1 Aufruf der Hostprofil-Konfigurationsseite

Das Verknüpfen der Cluster oder vSphere-Hosts mit einem Hostprofil ähnelt dem Verbinden mit Policies für den VMware Update Manager. Sind Hosts mit einem Profil verbunden, können Sie die Hosts auf Konformität prüfen und die Profile auf die Hosts übertragen. Auch wenn Hostprofile die Konfiguration eines Hosts sehr erleichtern, kommen Sie um die eigentliche Konfiguration eines Hosts nicht herum. Auf den nächsten Seiten nehmen wir die Konfigurationen vor.

Wichtig

Die administrativen Passwörter der Hosts und die UUID werden nicht übernommen.

12.1.1 Erstellen eines Hostprofils

Das Erstellen eines Hostprofils ist denkbar einfach. Es werden keine Einstellungen oder Ähnliches in einer Konfigurationsdatei editiert. Zuerst konfigurieren Sie einen vSphere-Host komplett so durch, wie er produktiv zum Einsatz kommen soll. So parametrieren Sie zum Beispiel die Einstellungen für das Netzwerk. Als Beispiel werden drei virtuelle Switches erstellt und mit physischen Netzwerkkarten verbunden und Service Console, Fault Tolerance und vMotion konfiguriert. Damit diese Einstellungen auch auf die anderen Hosts übertragen werden, muss lediglich ein Profil von diesem Host erstellt werden.

Ebenso ist es möglich, ein Profil zu importieren. Dateien mit der Endung *.vpf* sind die beschriebenen Profildateien für VMware-Hosts. Die Profile werden automatisch in der Datenbank gespeichert. Über den Weg des Exports erhalten Sie eine Datei. So ist es zum Beispiel möglich, eine Datei zu erstellen, um diese dann beim Kunden zu nutzen oder dem Kunden zu schicken. Das Einzige, was Sie nach dem Einspielen noch anpassen müssen, ist die IP-Adresse. Sieht der Inhalt der Datei in der Oberfläche des vCenters noch recht lesbar aus (Abbildung 12.2), so ist der Inhalt der abgespeicherten XML-Datei aufgrund fehlender Umbrüche sehr schwer lesbar.

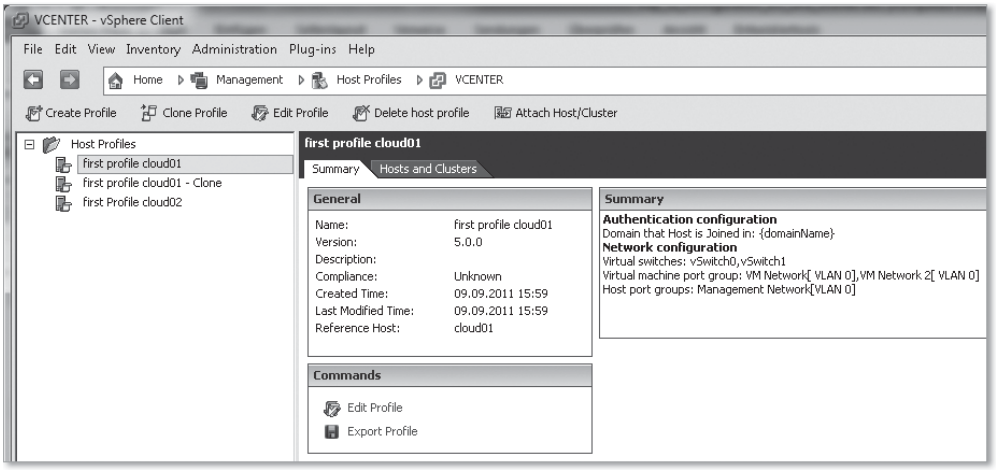


Abbildung 12.2 Profildatei eines vSphere-Hosts

Neben den Daten zu der Profildatei finden sich im SUMMARY im Klartext einige Konfigurationsteile. An dieser Stelle lässt sich das Profil exportieren oder auch editieren.

12.1.2 Anpassen eines Hostprofils

Haben Sie ein Profil einmal mit einem primären Host erstellt, ist es auch nachträglich möglich, das Profil Ihren Bedürfnissen anzupassen. Dazu starten Sie den Editiermodus über das Kontextmenü des entsprechenden Profils. Es öffnet sich ein Fenster, das wesentlich mehr offenbart als das SUMMARY-Fenster (Abbildung 12.3).

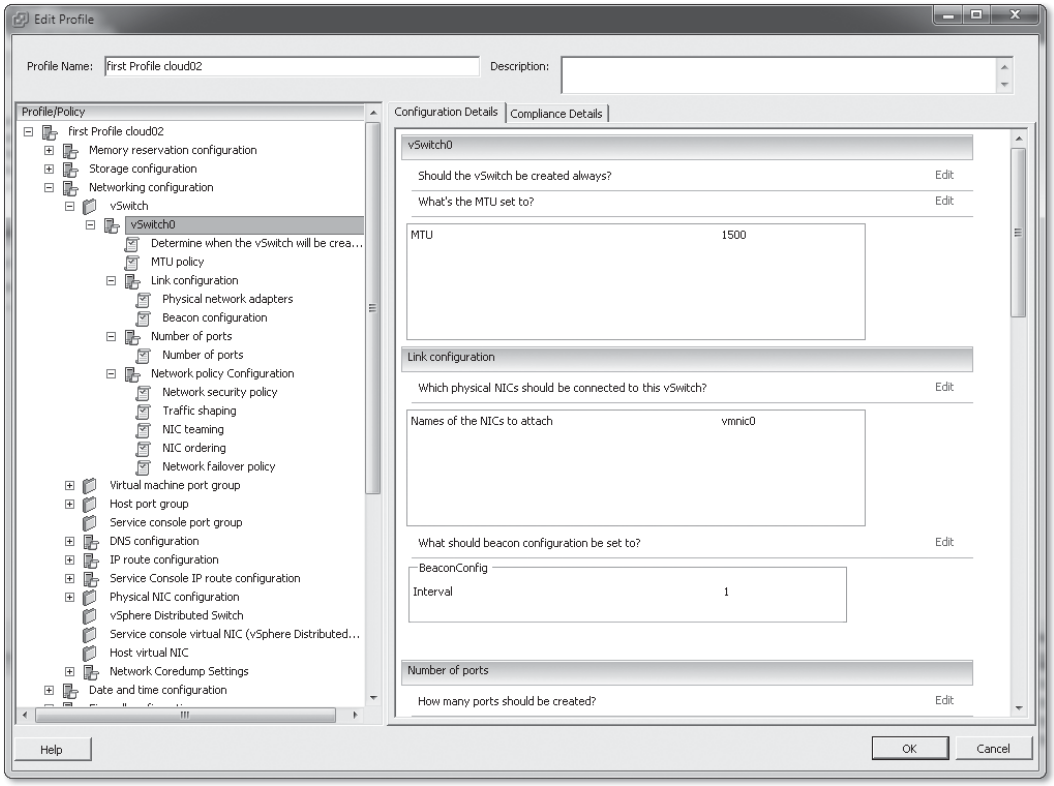


Abbildung 12.3 Editor für Hostprofile

Auch können Sie hier angeben, welche Einstellungen hostindividuell sind und damit beim Verteilen des Profils auf einen neuen Host via Aufforderung angepasst werden müssen. Sind die Anpassungsarbeiten beendet, schließen Sie das Fenster mit OK und können mit dem Profil arbeiten.

12.1.3 Host/Cluster mit Profil assoziieren

Nachdem Sie ein Hostprofil erstellt haben, können Sie es noch nicht mit einem Host assoziieren. Dafür müssen Sie als Erstes den Cluster oder den Host mit dem Profil verbinden. Wählen Sie im Fenster das Profil aus, um über den Button Attach Host/Cluster Maschinen mit dem Profil zu assoziieren (Abbildung 12.4).

Wenn Sie alle Maschinen hinzugefügt haben, erscheinen sie im Profil unter dem Reiter Hosts and Clusters. Hier ist es ebenfalls möglich, die Hostprofile auf die Maschinen zu übertragen und die nötigen Einstellungen vorzunehmen.

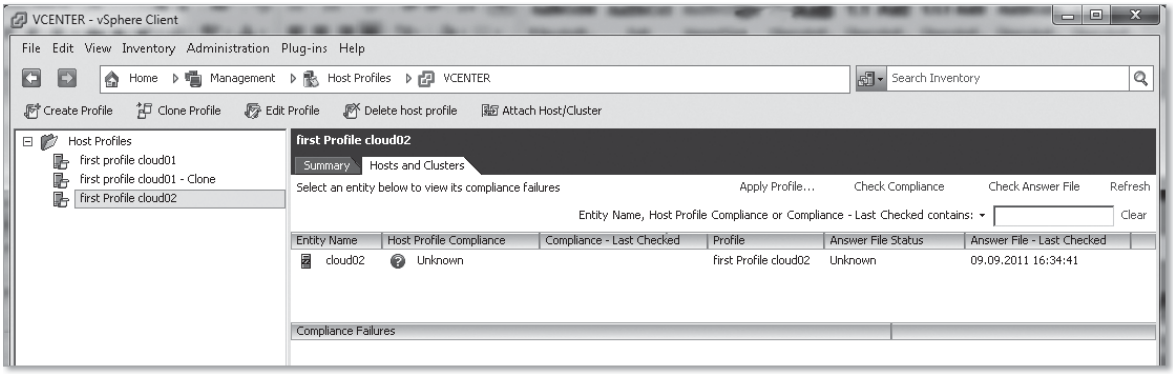


Abbildung 12.4 Binden von vSphere-Servern an ein Profil

Durch das Auswählen eines Servers in diesem Menü können Sie prüfen, ob der Host nach den Vorgaben des Hostprofils richtig konfiguriert ist. In diesem Fall hat noch kein Test der Host-Konfiguration stattgefunden. Dies erfolgt erst durch die Aktivierung von CHECK COMPLIANCE NOW.

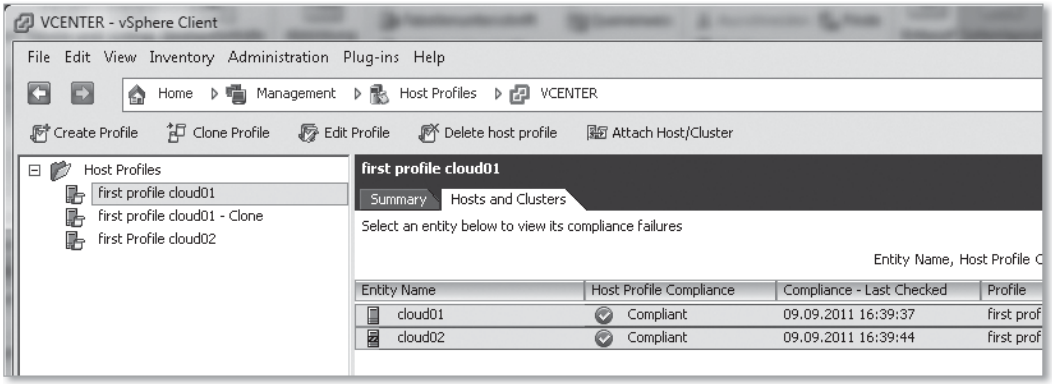


Abbildung 12.5 Ergebnis der Compliance-Prüfung

Sollte der Host nicht compliant sein (Abbildung 12.5), fahren Sie ihn in den Maintenance-Modus und wenden das Profil an.

12.1.4 Anwenden eines Hostprofils

Das Anwenden eines Hostprofils auf einen Host ist nur dann möglich, wenn dieser im Maintenance-Modus ist.

Ist ein geprüfter Host nicht compliant, können Sie ein Profil anwenden. Dafür müssen Sie, wie bereits erwähnt, den Host in den Maintenance-Modus fahren.

Ist ein Host zu sehen, der nicht richtig konfiguriert ist, wird der Host markiert und als nicht compliant angezeigt. Das darunterliegende Fenster zeigt an, welche Fehlkonfiguration vorliegt. So sehen Sie, welche Änderungen an der Host-Konfiguration vorgenommen werden.

Jetzt binden Sie das Profil auf den zweiten Host. Ist dieser nicht im Maintenance-Modus, erscheint direkt eine Fehlermeldung. Über das Kontextmenü können Sie den Host in den Maintenance-Modus fahren, um im folgenden Schritt das Profil zuzuweisen.

Je nachdem, welche Probleme beim Konfigurationscheck aufgetreten sind, öffnet sich entweder ein Fenster, das anzeigt, welche Änderungen durchgeführt werden (Abbildung 12.6), und Sie können den Vorgang starten, oder Sie erhalten die Möglichkeit, Konfigurationsfehler zu beheben. Bestünde z. B. die Gefahr, dass zwei Systeme mit identischer IP-Adresse im Netzwerk stehen, könnten Sie in dem Dialog aus Abbildung 12.6 die Adresse ändern.

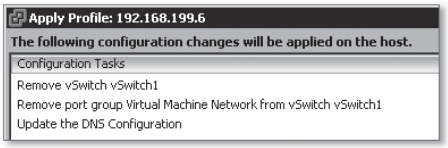


Abbildung 12.6 Zusammenfassung vor Änderungen

Sobald Sie alle Einstellungen vorgenommen haben, wird die Konfiguration aktualisiert. In den Recent Tasks des vCenters erkennen Sie nun den jeweiligen Task dazu. Durch das Verwenden von Hostprofilen wird das Durchführen und Prüfen von Konfigurationsänderungen in großen Umgebungen nicht nur sehr viel einfacher, sondern auch wesentlich weniger fehleranfällig.

Wenn Sie nicht ein gesamtes Profil auf einen Host anwenden möchten, so können Sie Optionen in einem vorhandenen Profil temporär aktivieren/deaktivieren. Öffnen Sie das Kontextmenü auf dem Hostprofil, und rufen Sie können dann den Menüpunkt Enable/Disable Profile Configuration… auf.

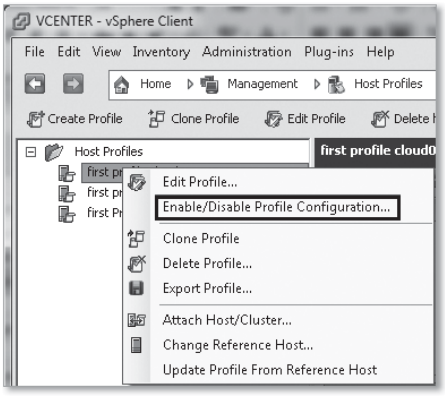


Abbildung 12.7 Aufruf »Enable/Disable Profile Configuration…«

Sie sehen nach dem Aufruf ein Fenster, in dem Sie die Aktivierung bzw. Deaktivierung vornehmen können.

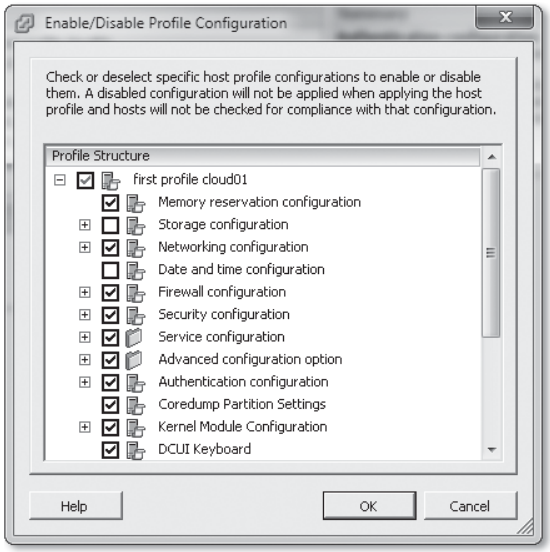


Abbildung 12.8 (De-)Aktivierungsauswahl

Die abgemeldeten Einstellungen werden nicht aus dem Profil gelöscht, Sie können sie können ohne Probleme auch wieder aktivieren. Ein möglicher Anwendungsfall: Wenn Sie z. B. Server im Einsatz haben, die unterschiedliche Netzwerkkarten haben oder bei denen die Reihenfolge der NICs eine andere ist, so können Sie ein vorhandenes Profil nutzen. Deaktivieren Sie die Karten, und wenden Sie das Profil an. Im Nachgang können Sie dann die Netzwerkkarten per Hand mit den Switches verbinden.

12.1.5 Profile-Compliance

Mit der Einführung der Hostprofile mit vSphere 4.x tat VMware einen großen Schritt im Sinne einer schnellen Möglichkeit, Hosts zu vereinheitlichen. Aus unserer Sicht fehlten aber noch die passenden Ansichten, um die Host-Compliance übersichtlich darzustellen. Dieses hat sich mit der Version 5.x geändert. Auf dem Host-Objekt gibt es einen neuen Reiter mit der Bezeichnung Profile Compliance. Hier können Sie direkt in der Host and Clusters-Ansicht sehen, wie der Compliance-Status der Server ist.

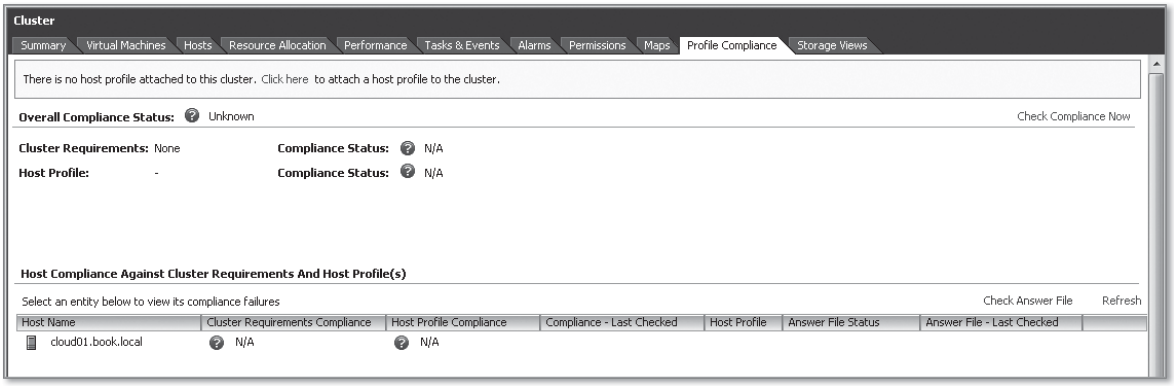


Abbildung 12.9 Übersicht der Compliance aller Hosts eines Clusters

12.2 NTP

Das Network Time Protocol (NTP) ist ein Standard zur Synchronisierung der Uhrzeit über das Netzwerk. Diese simpel klingende, aber sehr kritische Funktion sollten Sie unter allen Umständen konfigurieren. Eine Uhrzeit, die über alle Systeme im Netzwerk identisch ist, ist für den korrekten und reibungslosen Betrieb einer virtuellen Umgebung absolut notwendig! Probleme handelt man sich schnell ein, wenn man das Prinzip der Bereitstellung der Zeitfunktion nicht kennt. Das System hat eine hierarchische Struktur.

Die einzelnen Hierarchieebenen tragen die Bezeichnung *Stratum* mit einer laufenden Nummer. Je kleiner die Nummer ist, desto genauer ist die Uhrzeit bzw. geringer ist die Abweichung. Dabei ist *Stratum 0* die eigentliche Zeitquelle. Diese Zeitquelle wird direkt, nicht über das Netzwerk sondern per Schnittstelle, mit einem Computer verbunden. Dieser Computer ist Mitglied der *Stratum-1*-Ebene. Systeme, die sich die Zeit von der *Stratum-1*-Ebene abgreifen bilden die *Stratum-2*-Ebene und so fort. Je tiefer die Zeit abgefragt wird, desto größer kann die Zeitabweichung von der Ursprungsquelle sein. Beachten Sie die Besonderheit, dass ab der Ebene 1 jedes Gerät nicht nur Server, sondern auch Client ist.

Versuchen Sie, die Zeit mit einer möglichst hohen Ebene abzugleichen, und Sie sollten keine Probleme mit der Zeit in der virtuellen Landschaft bekommen

Sie haben verschiedene Möglichkeiten, NTP auf einem vSphere-Server zu konfigurieren. Für die Synchronisierung der Zeit der virtuellen Maschinen mit dem vSphere-Host können Sie die VMware Tools des Gastes verwenden. Dieses Thema behandeln wir in Abschnitt 15.4.6.

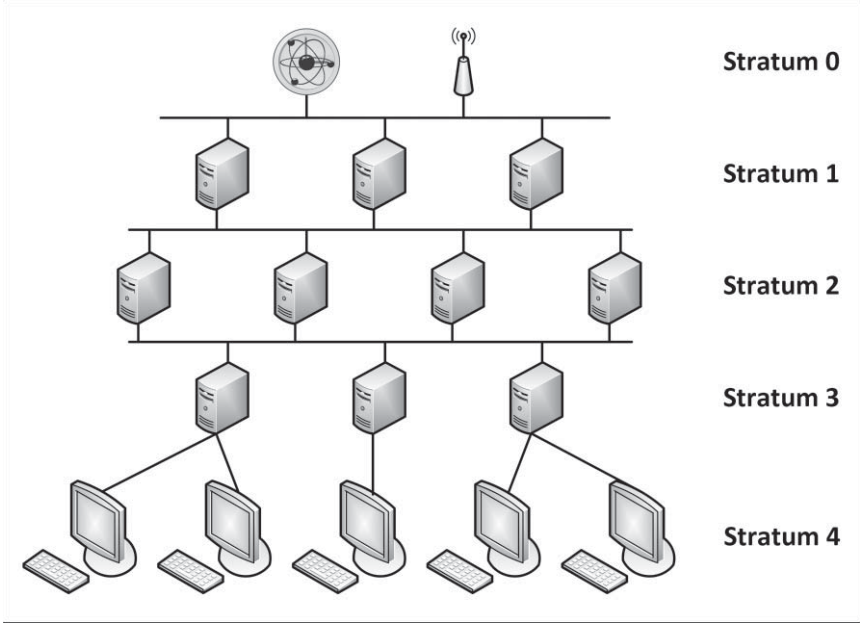


Abbildung 12.10 NTP-Hierarchie

12.2.1 NTP unter ESXi

Unter ESXi konfigurieren Sie NTP mit dem Befehl `vicfg-ntp.pl` des Remote Command Line Interfaces. Der Befehl `vicfg-ntp.pl` hat verschiedene Optionen, die in Tabelle 12.1 näher erläutert werden.

Optionen	Beschreibung
`-a|--add`	Name oder IP-Adresse des NTP-Servers, der hinzugefügt werden soll
`-d|--delete`	Name oder IP-Adresse des NTP-Servers, der entfernt werden soll
`-l|--list`	Zeigt alle verwendeten NTP-Server an.
`-h|--vihost`	der zu benutzende Host

Tabelle 12.1 Optionen des Befehls »vicfg-ntp.pl«

Bedenken Sie bitte, dass das Security Profile des Hosts so angepasst werden muss, dass die NTP-Ports zur Zeitquelle auch zugänglich sind.

NTP-Konfiguration mit dem vSphere-Client

Über den vSphere-Client gibt es ebenfalls eine Option, die NTP-Server zu konfigurieren. Es ist dabei unerheblich, ob Sie sich mit dem vCenter-Server oder mit dem Host direkt verbinden. Über den Reiter Configuration • Time Configuration rufen Sie das Konfigurationsfenster auf (Abbildung 12.11).

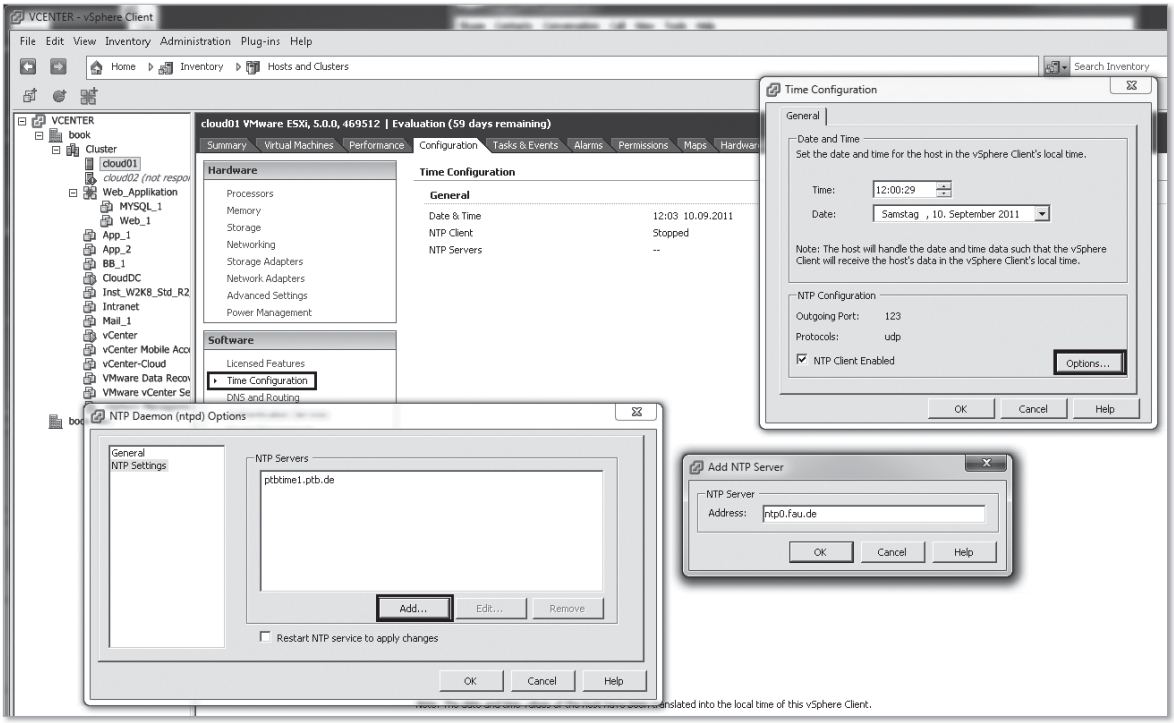


Abbildung 12.11 NTP-Konfiguration über den vSphere-Client

Hier rufen Sie mit dem Link Properties ein Fenster auf, in dem Sie alle Einstellungen vornehmen können. Über Options gelangen Sie in das Konfigurationsfenster, wo Sie wiederum über NTP Settings auf der linken Seite des Dialogfensters eine Eingabebox öffnen. Mit Add erreichen Sie einen Eingabedialog für den NTP-Server. Sind die Server eingetragen, können Sie alle Dialogfenster schließen. Zu guter Letzt ist noch die Startart des NTP-Dienstes festzulegen. Dabei haben Sie drei Optionen.

Startparameter	Bemerkung
Start automatically if any ports are open, and stop when all ports are closed	Der Dienst wird automatisch gestartet, wenn die Ports in der Firewall freigeschaltet sind. Im Gegenzug dazu wird der Dienst gestoppt, wenn die Ports geschlossen sind.
Start and stop with host	Der Dienst wird gestartet und gestoppt mit dem Host.
Start and stop manually	Der Dienst muss vom Administrator gestoppt und gestartet werden.

Tabelle 12.2 NTP-Startparameter

Legen Sie den NTP-Server auf diese Art an, müssen Sie auch nicht mehr die Firewall anpassen – dies geschieht automatisch.

Vergessen Sie aber nicht, dass natürlich auch die Firewalls im Netzwerk Ihre NTP-Anfrage durchlassen müssen. Sollte es Probleme geben, liegt es also nicht zwangsläufig am ESXi-Server.

12.2.2 NTP in der virtuellen Maschine mittels VMware Tools

Es ist möglich, die Zeit des virtuellen Gastes mit der Zeit des VMware-vSphere-Hosts zu synchronisieren (Abbildung 12.12). Dabei spielen die VMware Tools im virtuellen Gastsystem eine entscheidende Rolle, sie müssen also installiert sein.

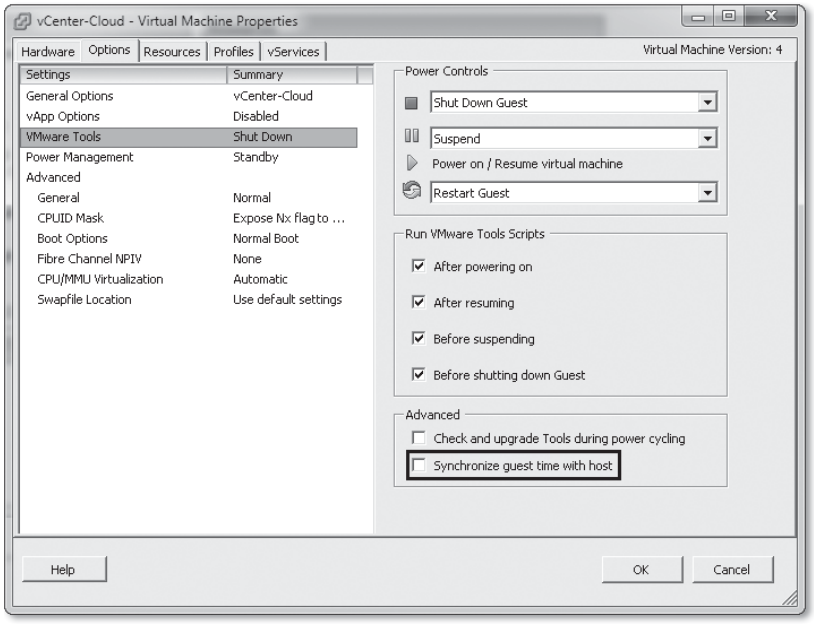


Abbildung 12.12 Aktivierung der Zeitsynchronisation für den Gast

Setzen Sie dazu in den Einstellungen einer virtuellen Maschine (Kontextmenü der VM • Edit Settings) unter dem Reiter Optionen einen Haken an der Option Synchronize guest time with host. Nach dem Setzen des Hakens in der Checkbox werden die VMware Tools die Zeit mit dem vSphere-Host abgleichen und die Zeit des Gastes anpassen.

Wichtig

Die Gastzeitsynchronisation der VMware Tools ist nur dafür ausgelegt, eine zu langsam laufende Uhr zur Zeitanpassung schneller laufen zu lassen. Die Tools können die Zeit nicht langsamer laufen lassen!

Verwenden Sie nicht parallel mehrere Möglichkeiten der Zeitsynchronisation. Gibt es bereits eine globale Unternehmenslösung zur Synchronisierung der Zeit, sollten Sie die virtuellen Maschinen ebenfalls entsprechend konfigurieren; in diesem Fall ist der Haken zu deaktivie-

ren. Achten Sie auch darauf, dass Mitglieder einer Domäne ihre Zeit automatisch mit dem AD-Controller (Active Directory Server) synchronisieren. Auch in diesem Fall ist von einer Aktivierung der Checkbox Synchronize guest time with host abzusehen.

Gerade in großen Umgebungen ist darauf zu achten, dass es einen definierten Prozess gibt, der beschreibt, wie mit dem Thema verfahren wird. Oft wird die Konfiguration der Gäste und der Hosts von unterschiedlichen Teams vorgenommen, was Fehlern Tür und Tor öffnet, wenn kein einheitliches Verfahren für die Zeitsynchronisation existiert.

12.2.3 Zeitsynchronisationsprobleme

So schön diese Funktionen sind und so simpel sich das Thema Zeitsynchronisation auch anhört, es gibt einige Tücken und Fallen, auf die Sie aufpassen müssen. Das Thema Zeit ist ein sehr wichtiges Thema in allen Netzwerken, aber vor allem bei der Verwendung von Verzeichnisdiensten.

Warum soll die Zeit überhaupt synchronisiert werden, und worin liegt die Ursache, dass die Zeit aus dem Ruder laufen kann? Die Mechanismen, die VMware nutzt, um Ressourcen in der virtuellen Umgebung zu sparen, wirken sich auf die Timer im Gast aus. Benötigt der virtuelle Server keine Rechenzeit, erhält er auch keine. Damit bekommt auch der Zeitgeber keine Rechenzeit, und so läuft die Uhr im Gast unregelmäßig. Aber nicht nur bei hohen Idle-Zyklen gibt es Probleme, auch wenn ein Host am oberen Limit läuft, kann es problematisch werden, jeder VM genug CPU-Rechenzeit zu geben, damit der Timer richtig läuft. Der Timer kann sowohl zu schnell als auch zu langsam laufen. Ganz kritisch ist das Zurückstellen der Uhrzeit besonders dann, wenn Sie auf dem System Datenbanken betreiben. Die einzelnen Transaktionen verlieren ihre Reihenfolge, wenn die Zeit zurückgestellt wird. Das ist dann der Beginn aller Probleme.

Allgemeines

Die Firma VMware hat die Probleme erkannt, die im Rahmen der Zeitsynchronisierung auftreten können. Aus diesem Grund gibt es eine zentrale Einstiegsseite auf der VMware-Website, die zu allen bekannten Artikeln zum Thema Zeitsynchronisation verzweigt. Sie finden den Link unter *http://blogs.vmware.com/kb/2009/02/new-timekeeping-articles.html*. Auch wenn die Seite schon etwas älter ist, so finden sich doch hier die interessanten Links zu dem Thema. Schlagen Sie hier nach, wenn Sie unsicher sind oder Probleme mit der Zeit in Ihrer Infrastruktur haben.

Außerdem beschäftigen sich zwei Knowledge-Base-Artikel mit dem Zeitthema für die Betriebssysteme Linux und Windows.

KB-Artikel URL	Bemerkungen
http://kb.vmware.com/kb/1006427	Timekeeping für Linux-Systeme
http://kb.vmware.com/kb/1318	Timekeeping für Windows-Systeme
http://www.vmware.com/files/pdf/Timekeeping-In-VirtualMachines.pdf	technisches Papier zu dem Thema

Tabelle 12.3 Knowledge-Base-Artikel zum Thema Zeitsynchronisation

Je nach eingesetztem Linux-Derivat und verwendetem Kernel haben Sie verschiedene Optionen, das Problem anzugehen. Dieser Linux-Artikel beschreibt, wie Sie bei welchem System mit welchem Kernel verfahren müssen, damit die Zeitsynchronisation einwandfrei funktioniert. Wir verzichten an dieser Stelle darauf, die Informationen direkt anzugeben; bei der Drucklegung des Buches wären Teile davon schon wieder überholt.

Zeitsynchronisation im Active Directory

Der Verzeichnisdienst Active Directory ist, was die Uhrzeit angeht, hochkritisch. Die AD-Implementierung von Microsoft erlaubt standardmäßig eine maximale Zeitdifferenz von 5 Minuten für das Kerberos-Protokoll. Fast alle Dienste und Policies arbeiten mit sogenannten *Timestamps*. Bei der Migration von physischen Maschinen zu virtuellen Maschinen werden auch oft die Active-Directory-Server (DCs = Domänen-Controller) migriert. Da diese Server das Herz eines Microsoft-Active-Directory-Netzwerks sind, ist für diese Maschinen meist ein NTP-Server konfiguriert. Sollte dies der Fall sein, müssen Sie darauf achten, dass entweder die Active-Directory-Server die Zeitsynchronisation bestimmen oder die vSphere-Hosts die aktuelle Zeit holen und per VMware Tools an die Gäste geben. Sie dürfen auf keinen Fall beide Möglichkeiten verwenden.

Das Zeitthema bei AD-Controllern können Sie aber mit einigen einfachen Kniffen entschärfen.

Zuerst sollten Sie den Time-Service auf dem AD-Controller anpassen. Rufen Sie dazu den Registry Editor auf. Dazu tippen Sie den Befehl `regedit` über Start • Ausführen in das Befehlsfenster ein. Ändern Sie nun im Registry Editor den Wert `HKLM\System\CurrentControlSet\W32Time\Parameters\Type` von `NT5DS` auf `NTP`. Als Timeserver geben Sie einen anderen Stratum-1-NTP-Server an.

Den Wert des Keys `HKLM\System\CurrentControlSet\W32Time\Config\AnnounceFlags` passen Sie von `10` auf `5` an. Hiermit weisen Sie dem Domänen-Controller fest die Funktion eines Zeit-Servers zu. Mit `net stop w32time` und `net start w32time` starten Sie den Zeitdienst nach der Neukonfiguration neu. Abschließend stoßen Sie in der Kommandozeile manuell eine Synchronisation mit dem neuen Stratum-1-Server mit dem Befehl `w32tm /resync /rediscover` an.

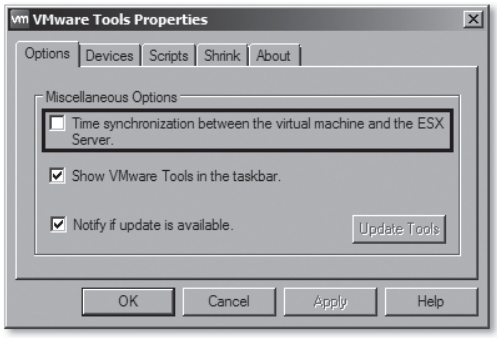


Abbildung 12.13 Deaktivierung der Zeitsynchronisation der VMware Tools

Nach dieser Konfiguration liegt für die gesamte Domäne eine stabile Zeitquelle vor. Entscheidend ist aber, dass Sie auf allen Servern der Domäne die Zeitsynchronisation über die VMware Tools deaktivieren (Abbildung 12.13)! Es gibt zwei Möglichkeiten, den Dialog zu öffnen: entweder über das Startmenü oder durch einen Doppelklick auf das VMware-Symbol in der Statusleiste.

12.3 SNMP

Das Simple Network Management Protocol (SNMP) ist ein Standard-Netzwerkprotokoll, das Sie zur Überwachung von Hardware verwenden können. Diese Informationen werden auf einem zentralen System gesammelt. Die Kommunikation mit dem zentralen Managementsystem erfolgt über zwei Wege: Entweder sendet das Managementsystem eine Anforderung von Informationen an ein zu überwachendes System, oder das zu überwachende System stellt die Überwachungsinformationen selbständig dem Managementsystem zur Verfügung.

12.3.1 SNMP unter VMware

Das SNMP-Protokoll wird auch von VMware unterstützt. Unter Zuhilfenahme des Netzwerkprotokolls können Sie den vSphere-Server überwachen. Auch hier holt entweder das Managementsystem die Informationen ab, oder der vSphere-Host sendet Informationen bei einem speziellen Event an das zentrale Management. Alle Enterprise-Produkte von VMware (vCenter, vSphere und ESXi) unterstützen das SNMP-Protokoll.

Der SNMP-Agent, der vom VMware-vSphere-Host verwendet wird, ist von Haus aus direkt im System installiert. Der Agent lässt sich mit jeglicher Software nutzen, die mit der Management Information Base (MIB) umgehen kann.

Die MIBs sind eine Art Adresse für die zu überwachenden Objekte. Mit Hilfe dieser Adresse können die Zustandsinformationen des zugehörigen Objekts abgefragt werden. Der Vollständigkeit halber sei noch erwähnt, dass MIBs Zahlenketten sind, die durch Punkte getrennt werden,

z. B. `1.3.6.1.4.1`. VMware unterstützt dabei nur Traps. Traps sind die Informationen, die unaufgefordert an das Management geschickt werden. Die SNMP GETs werden ausgelöst, wenn das zentrale Managementsystem gezielte Nachrichten von einem SNMP sprechenden Gerät benötigt. SNMP Gets werden von ESXi aber nicht unterstützt.

12.3.2 SNMP unter ESXi

Der SNMP-Agent unter ESXi unterscheidet sich von dem SNMP-Agent der vSphere. Durch die fehlende Service Console ist natürlich auch die Konfiguration von SNMP unter ESXi eine andere.

Der SNMP-Agent unter ESXi unterstützt im Moment nur SNMP-Traps und keine GETs. Um den Agent zu verwenden, müssen Sie den SNMP-Service aktivieren und eine Community sowie ein Ziel konfigurieren. Diese Arbeit erledigen Sie im Falle des ESXi mit dem VMware Remote Command Line Interface (Remote CLI). Der dazugehörige Befehl lautet `vicfg-snmp`. Tabelle 12.4 listet alle Optionen des Befehls `vicfg-snmp` auf.

Optionen	Beschreibung
`-c|--communities`	Setzt die SNMP-Communities; mehrere durch Kommas trennen.
`-D|--disable`	Stoppt den SNMP-Service.
`-E|--enable`	Startet den SNMP-Service.
`-y|--hwsrc`	Mit den Parametern `sensors` bzw. `indicators` legen Sie fest, ob die IPMI-Sensoren oder die CIM-Indikatoren als Quelle für die Hardwaremeldungen dienen.
`-n|--notraps`	Mit einer kommagetrennten Liste geben Sie die Traps an, die nicht gesendet werden sollen. Die Werte werden mit der Option `-reset` wieder zurückgesetzt.
`-p|--port`	Setzt den Port des SNMP-Agents. Standard ist `udp/162`.
`-r|--reset`	Löscht alle Communities.
`-s|--show`	Zeigt die SNMP-Agent-Konfiguration an.
`-t|--targets`	Setzt den Host für die die Benachrichtigungen. `hostname[@port][/community][,...]`
`-T|--test`	Sendet eine Testbenachrichtigung.
`-h|--vihost`	Der zu benutzende Host

Tabelle 12.4 Optionen des Befehls »vicfg-snmp«

Mit dem Befehl `vicfg-snmp -T` wird der ESXi einen Test-Trap schicken. So überprüfen Sie die Konfiguration und die Einstellungen.

12.3.3 SNMP in Gastbetriebssystemen

Natürlich können Sie das SNMP-Protokoll auch in den verschiedenen Gastbetriebssystemen verwenden. Auf Seite der Virtual Infrastructure sind dafür kein weiteres Eingreifen und keine weitere Konfiguration nötig. Je nach Gastbetriebssystem und Applikation lassen sich SNMP-

Einstellungen vornehmen. Zu den nötigen Konfigurationsschritten können Sie sich bei dem Hersteller des entsprechenden Betriebssystems informieren.

12.4 DNS

Eine sauber funktionierende Namensauflösung ist Grundvoraussetzung für eine einwandfrei arbeitende virtuelle Infrastruktur. Aus diesem Grund sollten Sie in der gesamten Umgebung DNS einsetzen. Ein falsch konfigurierter DNS kann zu viele Problembilder haben, die oftmals nicht direkt dem eigentlichen Problem zuzuordnen sind.

Die DNS-Konfiguration eines vSphere-Hosts können Sie über den vSphere-Client vornehmen. Dafür müssen Sie sich direkt am Host oder am vCenter-Server anmelden. Über den Tab CONFIGURATION gelangen Sie zur Einstellung DNS AND ROUTING, mit dem Link PROPERTIES erreichen Sie die Eingabemaske. In dieser Maske machen Sie alle nötigen Eingaben, um den Namensdienst zu konfigurieren (Abbildung 12.14).

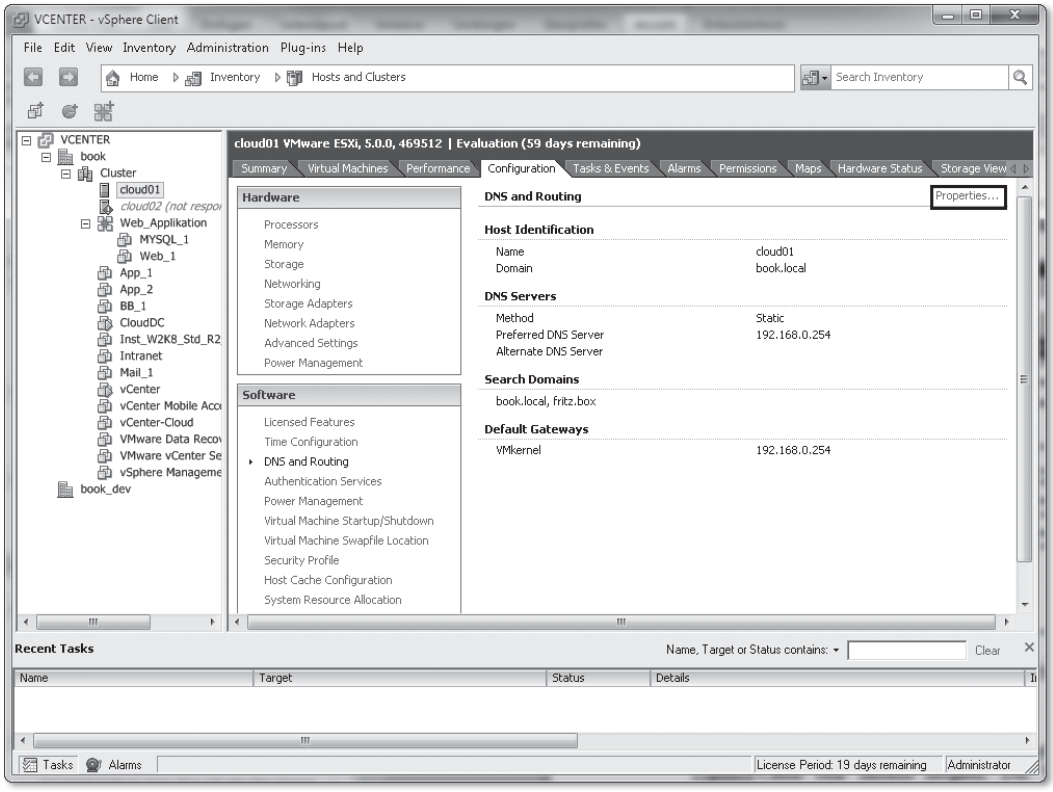


Abbildung 12.14 DNS-Konfiguration der vSphere-Hosts

Routing/Gateway

Eine Änderung am Gateway ist ebenfalls über den vSphere-Client sehr einfach möglich. Der Weg ist identisch mit der Anpassung der DNS-Einstellungen. Rufen Sie einfach den Reiter Routing auf. Hier verbirgt sich die Möglichkeit, Gateways für die Service Console sowie den VMkernel einzugeben. Beachten Sie – aber das ist keine vSphere-Eigenart –, dass das Gateway in Ihrem Netzwerksegment liegen muss.

12.5 Einrichtung von Resource-Pools

Nicht nur in großen Umgebungen kann es sinnvoll sein, mit Resource-Pools zu arbeiten, sondern auch in kleineren Umgebungen. Dabei lassen sich die Resource-Pools für andere Funktionen zweckentfremden; dazu aber später mehr in Abschnitt 12.12, »vCenter-Berechtigungen«.

Lassen Sie uns vorn beginnen und kurz in die Thematik einsteigen. Was sind *Resource-Pools* überhaupt? In Resource-Pools werden Teile von CPU- und Memory-Ressourcen eines Hosts zusammengefasst. Dabei ist es möglich, die Parameter des Pools variabel zu gestalten. Aber Pools fassen nicht nur Ressourcen zusammen, sie bieten auch die Möglichkeit der Rechtebündelung. Somit kann es ein Mittel der Wahl sein, Anwendern in »ihren« Resource-Pools mehr Rechte zu geben als auf den anderen Objekten der virtuellen Infrastruktur.

Die Resource-Pools werden in der Hosts and Clusters-Ansicht mit einem eigenen Symbol dargestellt – mit einer Ausnahme: Es gibt einen Resource-Pool, der in keiner Ansicht des vCenter Servers angezeigt wird. Dabei handelt es sich um den Root-Resource-Pool. In diesem Pool werden alle Ressourcen eines Hosts bzw. DRS-Clusters zusammengefasst. Hier sehen Sie auch, warum der Pool nicht angezeigt wird: Die Ressourcen von Host bzw. Cluster sind identisch. Alle in einem Pool liegenden virtuellen Maschinen gruppieren sich unter dem Resource-Pool, dem sie angehören.

In Resource-Pools ist es Ihnen möglich, Ressourcen aufzuteilen, bereitzustellen und zu reservieren. Sie können aber auch Resource-Pools ineinander verschachteln.

Erstellung eines Resource-Pools

Das Kontextmenü des Hosts oder Clusters führt zu dem Punkt New Resource Pool zur Erstellung von Resource-Pools (Abbildung 12.15).

Anschließend erscheint ein Fenster, in dem Sie verschiedene Einstellungen vornehmen können, um den Resource-Pool anzulegen (Abbildung 12.16).

In dem Feld Name geben Sie einen Name für diesen neuen Resource-Pool ein. Hier legen wir einen Pool für die Entwicklungsabteilung an. In den anderen Feldern konfigurieren Sie die zu verwendeten CPU- und RAM-Ressourcen.

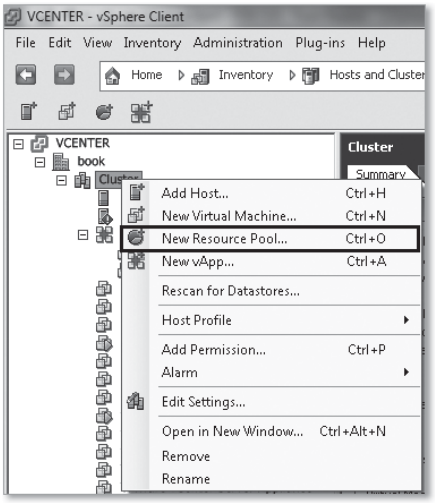


Abbildung 12.15 Neuen Resource-Pool erstellen

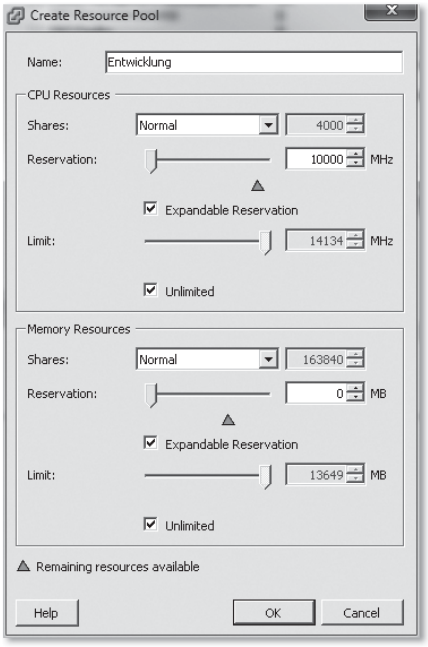


Abbildung 12.16 Konfiguration von Resource-Pools

Beachten Sie bitte, dass beim Anlegen von Resource-Pools das System eine Plausibilitätsprüfung durchführt, ob die vorhandenen und jetzt zugewiesenen Ressourcen auch zur Verfügung stehen. Optimal wäre es, vor dem Anlegen des Pools zu kontrollieren, ob die noch zur Verfügung stehenden Ressourcen für den Pool ausreichen. Es gibt im vCenter aber leider keine

Übersicht, die die zugewiesene Menge an Ressourcen anzeigt. Sie können nur die Gesamtressourcen des Clusters bzw. Hosts einsehen.

Eine Hilfe gibt Ihnen aber VMware im vSphere-Client doch mit: In Abbildung 12.16 sehen Sie zwei kleine orangefarbene Dreiecke; diese markieren die maximal nutzbaren Ressourcen bei der Einrichtung eines Pools.

Reservation

Bei dem Teil Reservation nehmen Sie auf Wunsch eine Reservierung für den Pool vor. Bei einer Reservierung werden die hier angegebenen Ressourcen dem Pool immer garantiert zugewiesen, wenn diese benötigt werden. Im Falle der CPU-Ressourcen in Abbildung 12.16 werden immer 10.000 MHz zugewiesen, bei den Memory-Ressourcen geben Sie durch den Wert 0 alle Speicherressourcen frei, wenn sie nicht benötigt werden.

Limit

Die Einstellung für Limit ist ähnlich wie eine Reservierung. Stellen Sie ein Limit ein, kann dieser Pool maximal diese Ressourcen anfordern und verwenden. Damit ist garantiert, dass virtuelle Maschinen, die in einem Resource-Pool liegen, nicht den Ressourcenbedarf von anderen VMs außerhalb des Pools beeinflussen.

Expandable

Haben Sie bei Expandable Reservation einen Haken gesetzt, können sich Kinder (virtuelle Maschinen und Pools) eines Vater-Objektes an dessen Ressourcen bedienen. Wenn Sie den Haken nicht gesetzt haben, können Kinder (virtuelle Maschinen und Pools) nur von diesem Pool Ressourcen beziehen, auch wenn der darüberstehende Vater-Pool freie Ressourcen zur Verfügung hat.

Lassen Sie uns das an einem Beispiel verdeutlichen. In Abbildung 12.17 sehen Sie verschachtelte Pools.

Sie sehen in dieser Konfiguration zwei Resource-Pools direkt im Wurzelverzeichnis des vCenters, zum einen die Produktion und zum anderen die Entwicklung. Die »Produktion« ist ein einfacher Resource-Pool, der Ressourcen gemäß seiner Konfiguration bereitstellt und sie für die enthaltenen VMs bereitstellt. Der Pool »Entwicklung« enthält noch mehrere untergliederte Resource-Pools, wobei der Pool »Mobile_Applikation« ebenfalls in zwei weitere Pools verzweigt. Als Beispiel haben Sie nun dem Pool »Mobile_Applikation« 10.000 MB Memory-Ressourcen und den Pools »Android« und »IOS« jeweils 2.000 MB Memory-Ressourcen zugewiesen. Ist nun bei den Pools »IOS« und »Android« die Option Expandable Reservation aktiviert, dann können die virtuellen Maschinen aus den beiden Pools »Android« und »IOS« bei Bedarf jeweils unabhängig voneinander Memory-Ressourcen beim Vater-Pool anfragen und auch bekommen. Benötigen die Maschinen in dem darüberliegenden Pool wieder mehr Ressourcen, werden diese den Tochter-Pools wieder entzogen.

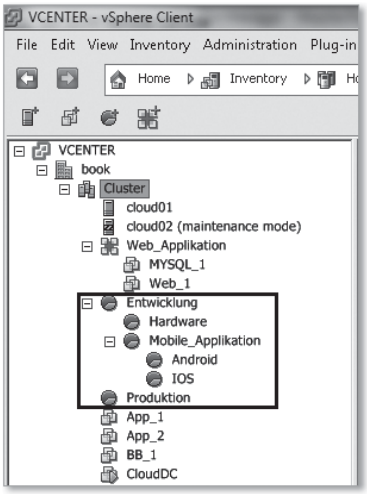


Abbildung 12.17 Verschachtelte Resource-Pools

Sie sehen also, dass das Anlegen eines solchen Pools sehr einfach und schnell erledigt ist. Bei großen und komplexen Umgebungen sollten Sie allerdings auf jeden Fall ein grundlegendes Konzept erstellen. Oft entstehen Ressourcen- oder Performanceprobleme aufgrund einer falschen Konfiguration von Resource-Pools in Zusammenhang mit einer großen Infrastruktur.

Shares

Die sogenannten *Shares* greifen immer dann, wenn keine freien Ressourcen mehr zur Verfügung stehen und die virtuellen Maschinen weitere Ressourcen anfordern. In diesem Fall priorisieren die Shares die Ressourcen der virtuellen Maschine anhand eines sharebasierten Modells. Wie viel Zeit das Objekt auf der eingestellten Ressource erhält, hängt immer von den eigenen Shares im Vergleich zu den vorhandenen Gesamt-Shares ab. Hat zum Beispiel eine virtuelle Maschine (VM1) 2.000 CPU-Shares und eine zweite virtuelle Maschine (VM2) 4.000 CPU-Shares, dann bekommt VM1 33 % und VM2 66 % der zur Verfügung stehenden CPU-Ressourcen. Die Aufteilungsgrundlage der CPU-Ressourcen bildet die Gesamtsumme aller Shares, das sind in diesem Fall 6.000 Shares (2.000 [VM1] + 4.000 [VM2]). VMware nutzt drei Standardwerte, die zum Einsatz kommen können. Natürlich ist es auch möglich, eigene Werte zu vergeben. In Tabelle 12.5 sind die Share-Werte aufgelistet.

Shares	CPU-Wert	Memory-Wert	Disk-Wert
Low	500	5 Shares pro MB Speicher	500
Normal	1.000	10 Shares pro MB Speicher	1.000
High	2.000	20 Shares pro MB Speicher	2.000
Custom	variabel	variabel	variabel

Tabelle 12.5 Standardwerte der Shares

Beachten Sie bitte, dass die Shares für die CPU immer pro CPU vergeben werden. Lassen Sie uns das anhand eines Beispiels erklären. Eine VM mit vier CPUs und dem SHARES-Wert NORMAL erhält vom System 4.000 Shares. Das errechnet sich aus dem SHARES-Wert selbst multipliziert mit der Anzahl der CPUs. Shares sind zwar ein Mittel der Priorisierung von Ressourcen, aber weniger ist hier definitiv mehr. Bedenken Sie: Je komplexer die Struktur ist, desto schwieriger ist es im Falle von Problemen, die Fehlerursache zu finden. Arbeiten Sie aus diesem Grund nie ohne Konzept, wenn Sie diese Mechanismen nutzen. Wichtig ist ebenfalls eine genaue Dokumentation solcher Konfigurationen, damit bei Problemen alle nötigen Informationen für die Fehlerbehebung vorliegen.

12.6 VMware vApp

Bieten Resource-Pools die Möglichkeit, unterschiedliche virtuelle Maschinen zu gruppieren, so haben Sie die Option, mit VMware-vApp-Server zusammenzufassen, die funktionell zusammengehören. Nicht nur das – es ist sogar möglich, die Abhängigkeiten der Systeme untereinander zu hinterlegen. Soll heißen: Der vCenter-Server weiß genau, in welcher Reihenfolge die Systeme gebootet werden müssen.

Lassen Sie uns das Ganze an einem Beispiel verdeutlichen. Wir nehmen dazu einen Webserver, der als Backend einen Datenbank-Server benötigt. Aus diesen beiden Systemen erzeugen wir nun eine vApp. Doch bevor die Arbeiten beginnen können, benötigen Sie einen DRS-Cluster oder einen VMware-Host mit mindestens Version 3.x.

12.6.1 Erstellen einer vApp

Zum Erstellen einer neuen vApp rufen Sie den entsprechenden Menüpunkt aus dem Kontextmenü des Hosts bzw. des Clusters auf (Abbildung 12.18).

Es startet – wie sollte es auch anders sein – ein Wizard, der Sie durch das Anlegen der vApp führt. Zuallererst geben Sie der Applikation einen Namen. Der Name muss eindeutig sein und darf nicht mit anderen Namen in der virtuellen Infrastruktur kollidieren. Beachten Sie, dass die Länge auf 80 Zeichen beschränkt ist. Es folgt die Angabe des Ablageorts in der Infrastruktur. Das kann ein Host oder ein Cluster sein. Es ist aber auch möglich, die vApp in einen Resource-Pool oder in eine bereits vorhandene vApp zu legen. Handelt es sich bei dem Zielort um einen nicht automatischen DRS-Cluster, dann ist die vApp direkt auf einem Host in diesem Cluster-Verbund abzulegen.

Machen Sie sich Ihre eigenen Gedanken, was für Sie am sinnvollsten ist. Auch hier sollten Sie darauf achten, dass eine Einheitlichkeit vorhanden ist und dass Sie alles so übersichtlich wie möglich halten.

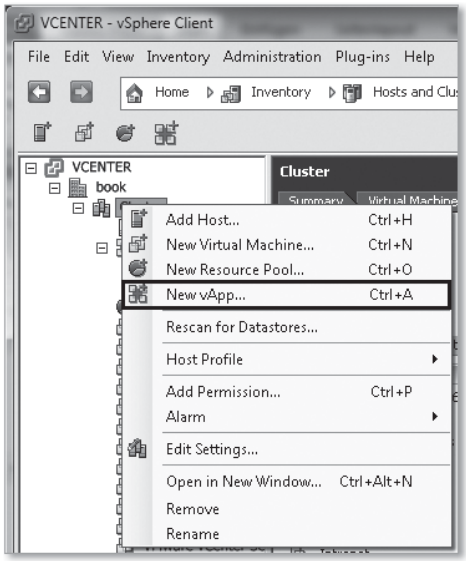


Abbildung 12.18 Erstellen einer vApp über das Kontextmenü

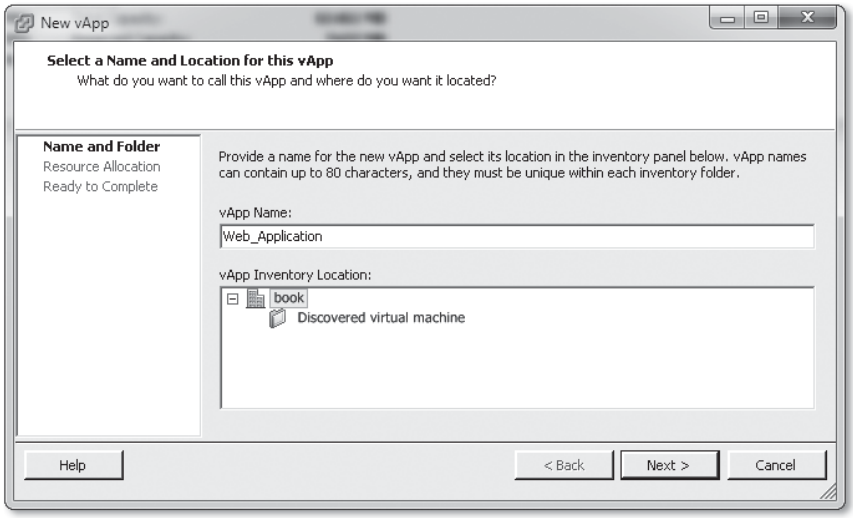


Abbildung 12.19 Anlage einer vApp und Namensvergabe

Wie schon bei der Anlage eines Resource-Pools können Sie der vApp nun auf Wunsch Ressourcen zuweisen (Abbildung 12.20).

Damit sind die Arbeiten für die Anlage der vApp schon erledigt. Nach der Zusammenfassung schließen Sie einfach den Dialog.

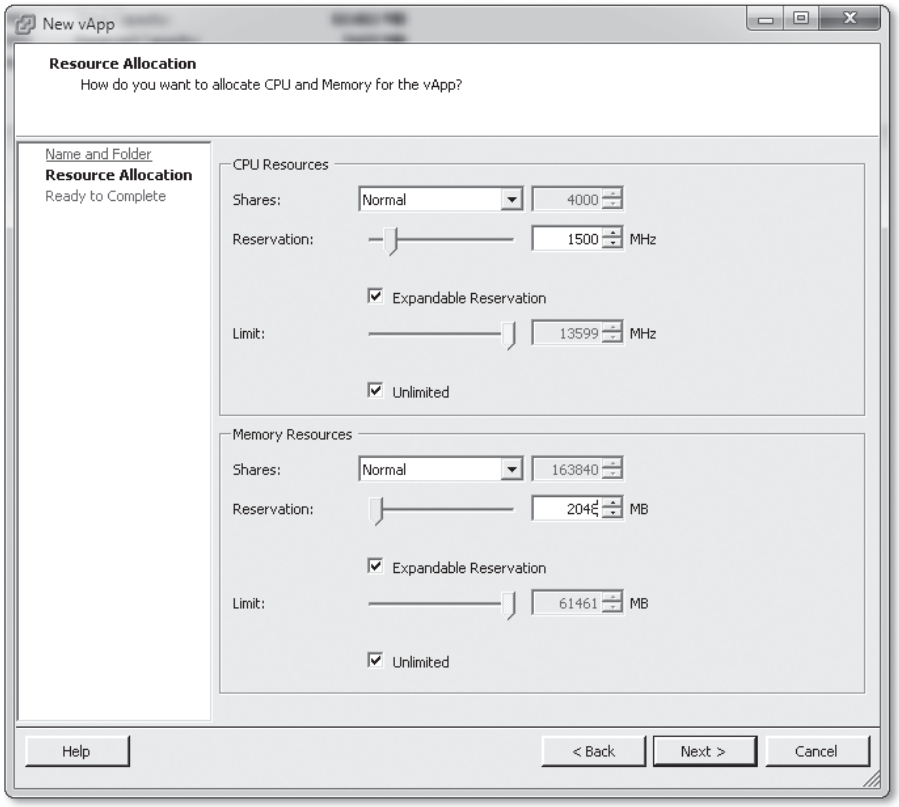


Abbildung 12.20 Ressourcenzuweisung für die vApp

12.6.2 Verknüpfung einer vApp mit virtuellen Servern

Ist die Hülle für eine vApp komplett angelegt, folgt im nächsten Schritt die Verknüpfung mit anderen vApps oder mit vorhandenen VMs. Die Verknüpfung von bereits vorhandenen VMs mit der vApp erfolgt durch einfaches Drag & Drop (Abbildung 12.21). Der Zustand der virtuellen Maschinen ist für den Aufnahmevorgang unerheblich. Die Aufnahme funktioniert sowohl im ausgeschalteten als auch im eingeschalteten Zustand.

Neue virtuelle Maschinen können Sie aber auch direkt in der vApp anlegen. Die Vorgehensweise entspricht der Ihnen bereits bekannten für die Erstellung einer VM.

Wenn Sie die beiden virtuellen Maschinen MYSQL_1 und WEB_1 der vApp WEB_APPLIKATION hinzugefügt haben, dann stellt sich das so dar wie in Abbildung 12.22.

Ist die vApp eingeschaltet, befindet sich, wie bei den VMs auch, ein grüner Pfeil in dem Anzeige-Icon.

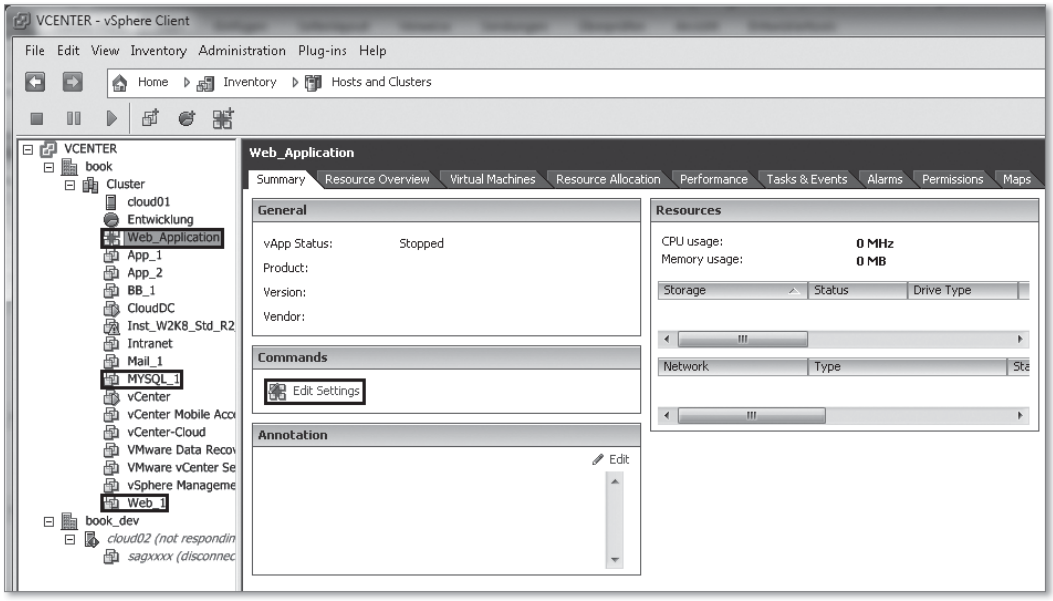


Abbildung 12.21 Erstellte vApp mit ihren zukünftigen VMs

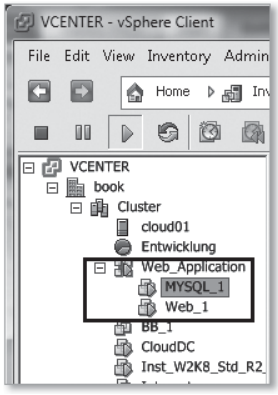


Abbildung 12.22 Fertig erstellte vApp »Bookshop_vApp«

Jetzt haben Sie die vApp »Web_Application« erstellt. In dieser vApp liegen ein Datenbank-Server und der dazugehörige Webserver.

Wie Sie in Abbildung 12.23 sehen, ist die vApp kein starres Gebilde. Sie können vApps in vApps erstellen oder dort sogar Resource-Pools anlegen. In der Ressourcenübersicht der vApp sehen Sie dann in der Übersicht genau, welche Elemente Bestandteil der vApp sind und wie viele dieser Elemente Teil des Konglomerats sind.

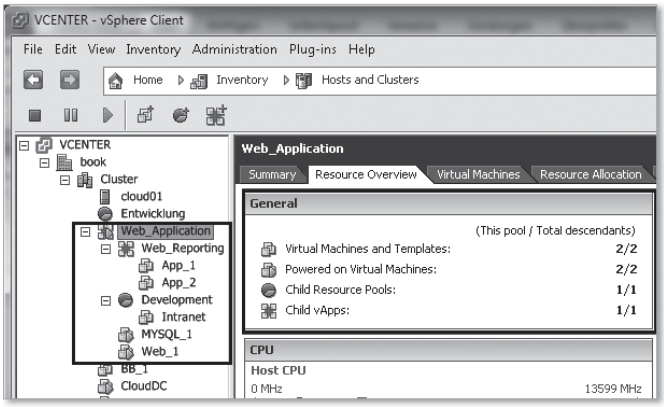


Abbildung 12.23 vApp-Verschachtelungen

12.6.3 vApp-Einstellungen

Über das Kontextmenü Edit Settings können Sie die Einstellungen der vApp weiter bearbeiten. Wählen Sie den Link Edit Settings aus, dann können Sie nur die Ressourcen der vApp bearbeiten. Das sich öffnende Fenster bietet drei Reiter: Optionen, Start Order und vServices (Abbildung 12.24). Der nach dem erstmaligen Aufruf angezeigte Dialog sollte Ihnen von der Anlage der vApp her bekannt vorkommen. Es handelt sich um die Ressourceneinstellungen der vApp.

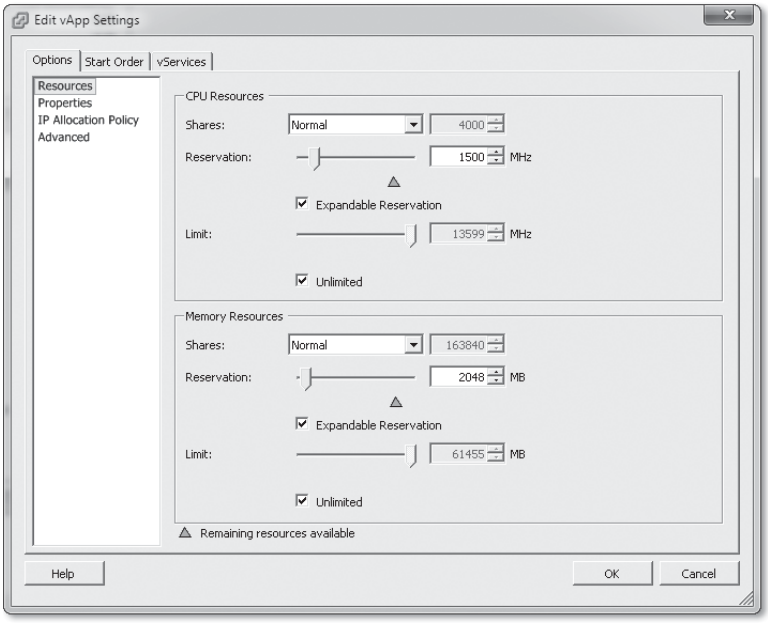


Abbildung 12.24 Anpassung der Ressourcen

Im Properties-Fenster finden sich derzeit keine weiteren Einstellmöglichkeiten. Die hier angezeigten Werte hängen mit den Einträgen im Fenster Advanced • Properties zusammen. Nur wenn die Optionen in dem Properties-Fenster aktiv sind, werden in diesem Fenster Einträge angezeigt.

Die IP Allocation Policy legt fest, in welcher Art und Weise die vApp ihre IP-Parameter erhält (Abbildung 12.25).

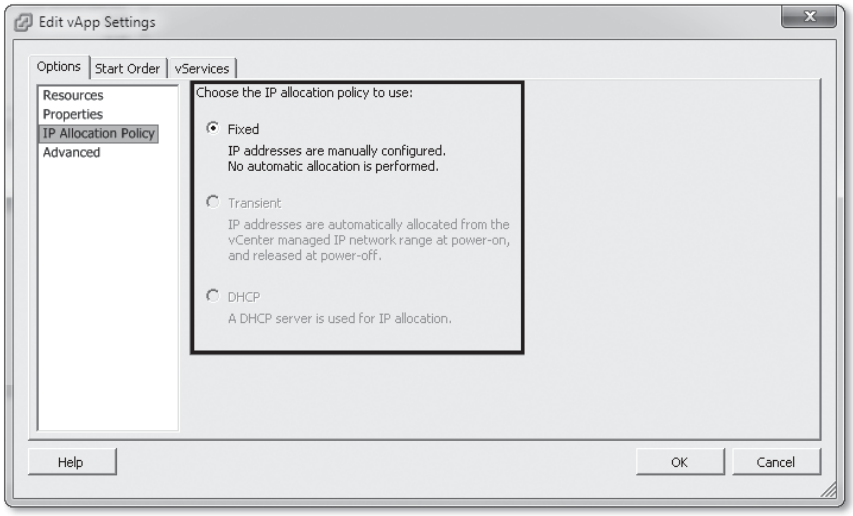


Abbildung 12.25 IP-Versorgung der vApp

Die Einträge in diesem Fenster korrelieren mit den Einträgen im Fenster Advanced • IP Allocation. Nur wenn die Optionen im IP Allocation-Fenster aktiv sind, ist es möglich, in dieser Policy andere Einstellungen als fixed auszuwählen. Bei fixed wird mit statischen IP-Adressen gearbeitet, bei DHCP wird der vApp automatisch eine Adresse zugewiesen, und bei transient wird die IP-Adresse aus einem Pool bezogen, der auf dem HA-Cluster unter IP Pool eingerichtet wird.

In der Advanced-Auswahl können Sie die vApp personalisieren (Abbildung 12.26). Die Felder in diesem Dialog sind selbsterklärend.

Zusätzlich finden Sie hier die beiden Buttons, die die weiter oben beschriebenen Konfigurationsfenster bereitstellen. Es handelt sich dabei um die Konfiguration der IP-Bereitstellung (Abbildung 12.27).

Die Einstellung DHCP an dieser Stelle aktiviert die DHCP-Option in der IP Allocation Policy. Die Option OVF Environment hängt mit der Transient-Option in der Allocation Policy zusammen. Bei der Auswahl können Sie noch festlegen, mit welcher IP-Version gearbeitet werden soll – IPv4, IPv6 oder mit beiden IP-Versionen.

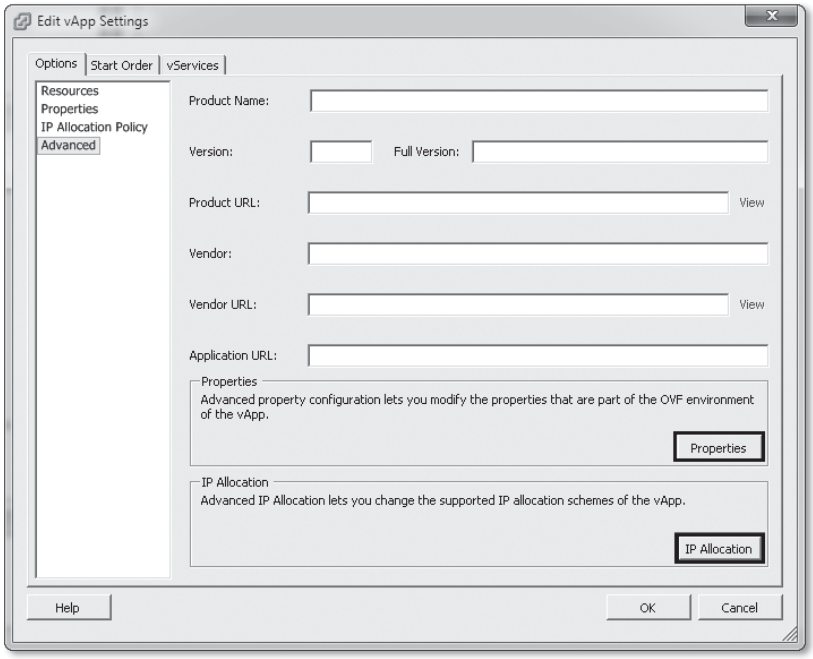


Abbildung 12.26 Personalisierung der vApp

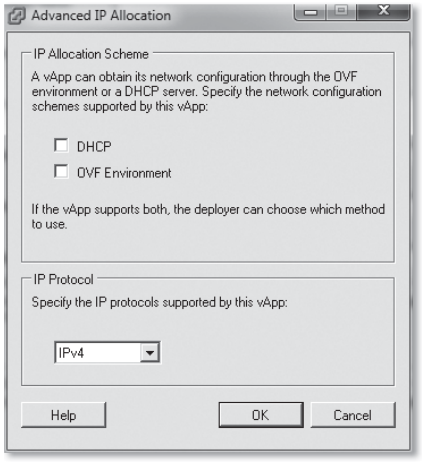


Abbildung 12.27 Konfiguration der IP-Bereitstellung

Zum Schluss bleibt noch die Konfiguration der START ORDER (Abbildung 12.28). Aus unserer Sicht ist dieser Punkt ein sehr wichtiger Baustein für die einwandfreie Funktion einer vApp, wenn diese nur zur Gruppierung von VMs dient und zur Abbildung von deren Abhängigkeiten untereinander.

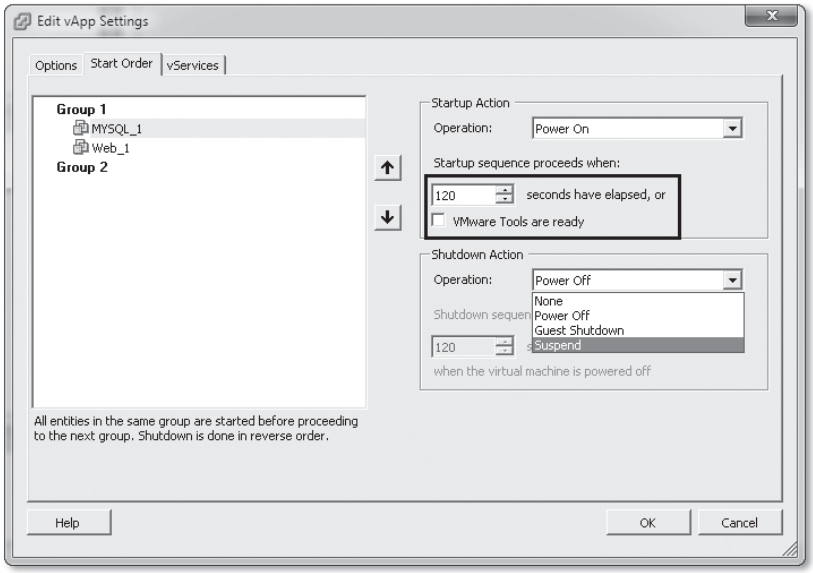


Abbildung 12.28 Startreihenfolge für die vApp

Für jeden Server können Sie eine eigene Aktion für den Start bzw. für den Shutdown festlegen. Beim Start gibt es, außer dem POWER ON, nur die Option, keine Aktion ausführen zu lassen. Zusätzlich können Sie angeben, welche Aktion der Startschuss für die folgende Gruppe ist. Entweder arbeiten Sie mit einem Timer, oder der abgeschlossene Start der VMware Tools ist der Trigger für die Aktivierung der nächsten Gruppe.

NONE, POWER OFF, GUEST SHUTDOWN und SUSPEND stehen als Optionen für das Beenden der Applikation zur Verfügung. Die Abarbeitungsreihenfolge erfolgt von oben nach unten für das Starten und von unten nach oben für das Stoppen der Applikation. Über die Pfeiltasten verschieben Sie beteiligte VMs zwischen den unterschiedlichen Gruppen, um so die Reihenfolge korrekt abzubilden.

Wichtig

Wenn Sie mit vApps arbeiten, dann denken Sie bitte daran, die Ein- und Ausschaltbefehle nur über das Kontextmenü der vApp zu nutzen. Anderenfalls wird die Startreihenfolge unter Umständen nicht eingehalten. Wurde über die vApp eine Aktion gestartet, sind die Befehle im Kontextmenü der VM ausgeblendet.

Wenn Sie tiefer in das Thema einsteigen und komplexere vApps und auch eigene OVFs (Open Virtualization Format) erstellen wollen, sollten Sie sich mit dem VMware Studio auseinandersetzen. Dieses Entwicklertool von VMware ermöglicht Ihnen, komplett eigene VMs zu kreieren. Nähere Informationen zu dem Thema finden Sie auf der Webseite von VMware unter *http://www.vmware.com/appliances/learn/vmware_studio.html.*

12.7 Automatisches Starten und Stoppen der VMs mit dem Host

Mit dem Start des vSphere-Hosts gibt es die Möglichkeit, virtuelle Maschinen automatisch zu starten. Speziell dafür bietet der Reiter CONFIGURATION auf einem vSphere-Host eine entsprechende Option. Unter dem Link SOFTWARE • VIRTUAL MACHINE STARTUP/SHUTDOWN können Sie dies konfigurieren und einschalten (Abbildung 12.29).

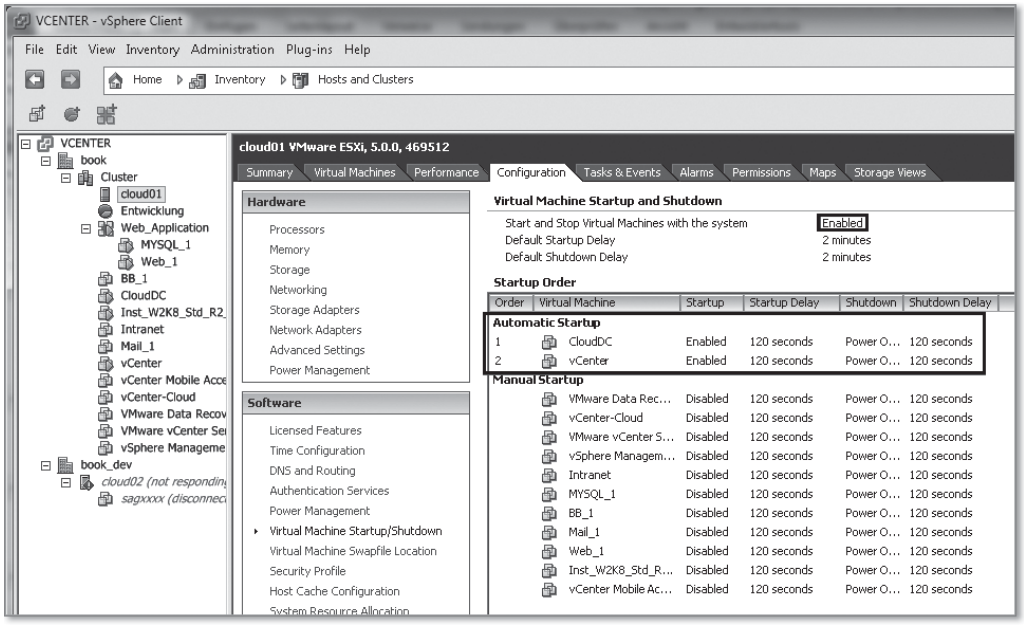


Abbildung 12.29 Automatisches Starten und Stoppen von virtuellen Maschinen

Im oberen Teil des Fensters wird der Status dieses Features angezeigt. In der Abbildung ist die Funktion bereits aktiviert. Dadurch besteht die Möglichkeit, die virtuellen Maschinen automatisch zu stoppen oder zu starten. Über den PROPERTIES-Link lässt sich die Funktion global für den Host aktivieren oder deaktivieren.

Rufen Sie mit dem Link PROPERTIES im rechten Teil des Fensters das in Abbildung 12.30 angezeigte Fenster auf. in dem Sie das automatische Starten und Stoppen der virtuellen Maschinen konfigurieren.

Sie müssen die Checkbox ALLOW VIRTUAL MACHINES TO START AND STOP AUTOMATICALLY WITH THE SYSTEM aktivieren, damit alle anderen Funktionen freigeschaltet werden. Anschließend können Sie das Verhalten der VMs nach einem Neustart des Hosts einstellen.

Für beide Optionen, das Starten und Stoppen, ist es möglich, eine Delay-Zeit anzugeben. Diese Zeit wird noch verstreichen, bevor die Aktionen durchgeführt werden. Bei den Verzögerungszeiten handelt es sich um eine globale Einstellung, die automatisch für alle VMs auf dem Host angewendet wird.

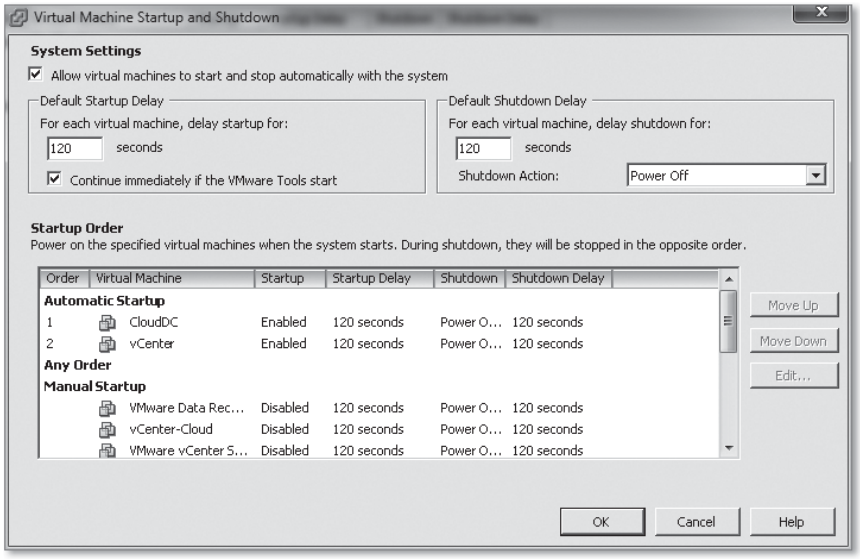


Abbildung 12.30 Automatisches Starten und Stoppen von virtuellen Maschinen aktivieren

Im unteren Teil des Fensters positionieren Sie über die Buttons Move Up und Move Down gegebenenfalls die virtuellen Maschinen in einer bestimmten Reihenfolge. Die Reihenfolge gibt an, in welcher Abfolge die virtuellen Maschinen gestartet werden. In derselben Reihenfolge, aber rückwärts, werden die virtuellen Maschinen heruntergefahren.

Im Beispiel in Abbildung 12.30 sehen Sie eine unserer Testumgebungen. Nach dem Start des Hosts wird automatisch der Domänen-Controller gestartet und anschließend der vCenter-Server. Virtuelle Maschinen unter dem Bereich Manual Startup werden nicht automatisch gestartet, sondern bleiben abgeschaltet, bis ein anderer Task oder eine manuelle Aktion die Maschinen bootet. Maschinen unter dem Punkt Any Order werden automatisch vom System gebootet, genau wie die Maschinen unter Automatic Startup.

12.8 vSphere-Security

Der VMware-vSphere-Host ist mit einer Firewall ausgestattet, die den vSphere-Host schützt. Die Firewall ist nach der Installation eingeschaltet und konfiguriert. Auch hier hat sich eine Änderung ergeben: Das vSphere-Security-Fenster teilt sich in zwei Abschnitte; im oberen finden sich nun die Dienste wieder, und im unteren werden die Ports angezeigt. Standardmäßig werden alle Ports erst einmal geschlossen, abgesehen von denjenigen, die für die Standardkommunikation notwendig sind. In unserem Fall sind nach der Installation alle Ports freigeschaltet, die in Tabelle 12.6 aufgelistet sind. Dabei haben wir die Ports in eingehende und den ausgehende aufgeteilt.

Dienste	Port	Protokoll	erlaubte IP-Adressen
SNMP-Server	161	UDP	alle
NFC	902	TCP	alle
CIM Secure Server	5989	TCP	alle
vSphere-Client	902, 443	TCP	alle
CIM SLP	427	UDP, TCP	alle
vMotion	800	TCP	alle
DNS-Client	63	UDP	alle
vSphere WebAccess	80	TCP	alle
DHCP-Client	68	UDP	alle
Fault Tolerance	8100, 8200	UDP, TCP	alle
CIM-Server	5988	TCP	alle
SSH-Server	22	TCP	alle

Tabelle 12.6 vSphere-Firewall: eingehende Verbindungen

Dienst	Port	Protokoll	erlaubte IP-Adressen
NFC	902	TCP	alle
CIM SLP	427	UDP, TCP	alle
vMotion	8000	TCP	alle
DNS-Client	53	UDP	alle
DHCP-Client	68	UDP	alle
Fault Tolerance	80, 8100, 8200	UDP, TCP	alle
WOL	9	UDP	alle
VMware vCenter Agent	902	UDP	alle
NTP	123	UDP	alle
HBR	31031, 44046	TCP	alle

Tabelle 12.7 vSphere-Firewall: ausgehende Verbindungen

Zusätzlich finden Sie im oberen Teil dieses Fensters (Abbildung 12.31) die Dienste des ESXi-Hosts. Ganz unten in der Ansicht können Sie den Lockdown-Modus aktivieren. Damit wird der Zugriff auf den ESXi-Host eingeschränkt. Ein Zugriff kann dann nur noch über die lokale Konsole erfolgen.

Die Dienste finden sich jetzt auch in diesem Fenster wieder. In Tabelle 12.8 zeigen wir Ihnen, welche Dienste beim vSphere-Host dabei sind und welche Startart sie haben.

Dienste	Startart
I/O Redirector (Active Directory Service)	stopped
Network Login Server (Active Directory Service)	stopped

Tabelle 12.8 Diensteübersicht ESXi-Host

Dienste	Startart
lbtd	running
vpxa	running
TSM	stopped
Local Security Authentication Server (Active Directory Server)	stopped
NTP Daemon	stopped
TSM-SSH	stopped
Direct Console UI	running
CIM Server	running

Tabelle 12.8 Diensteübersicht ESXi-Host (Forts.)

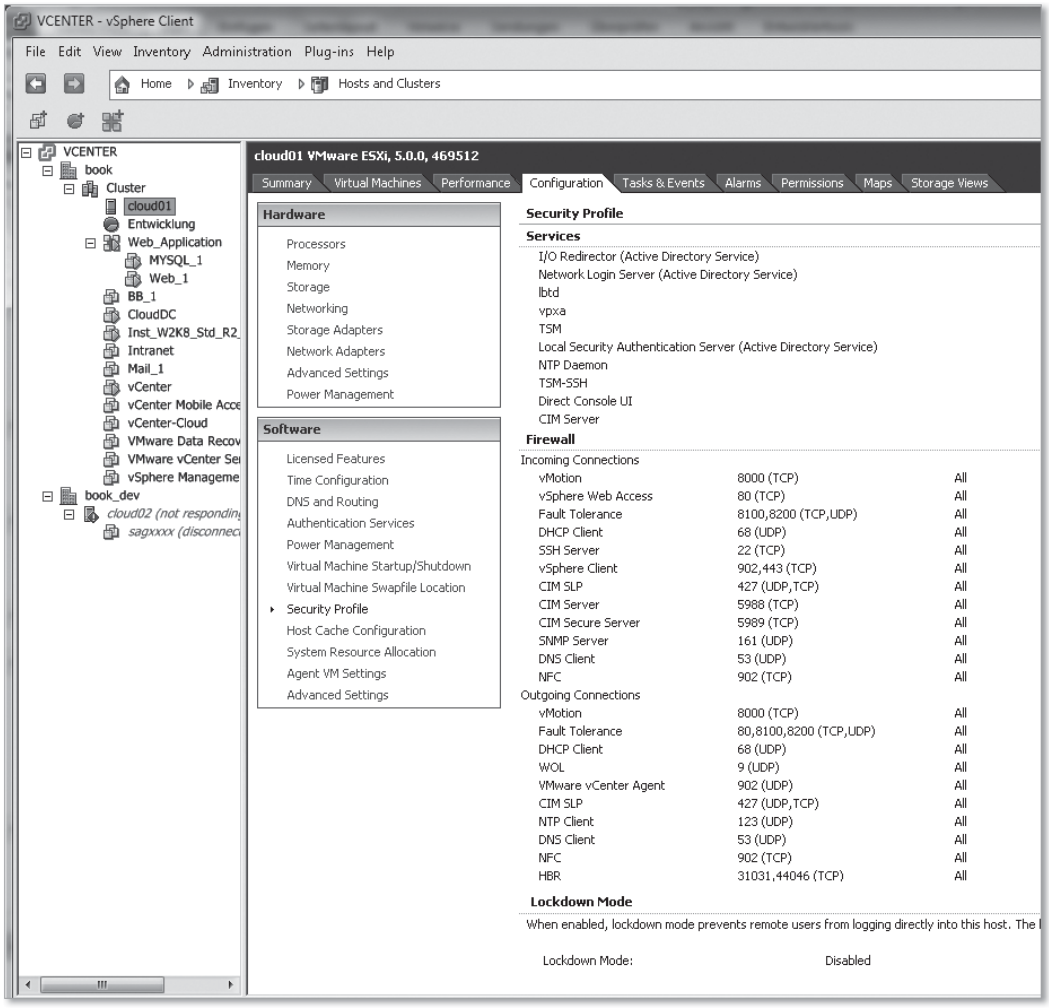


Abbildung 12.31 Security-Einstellungen des ESXi-Hosts

Einige Einstellungsanpassungen an den Diensten können Sie sofort sehen, wenn Sie sich auf der lokalen Konsole anmelden, so z. B. die ESXi-Shell.

Wird die Startart eines Dienstes geändert, werden im Hintergrund automatisch die Ports in der Firewall aktiviert. Damit ist gewährleistet, dass auch alle Ports geöffnet werden, die der Service benötigt.

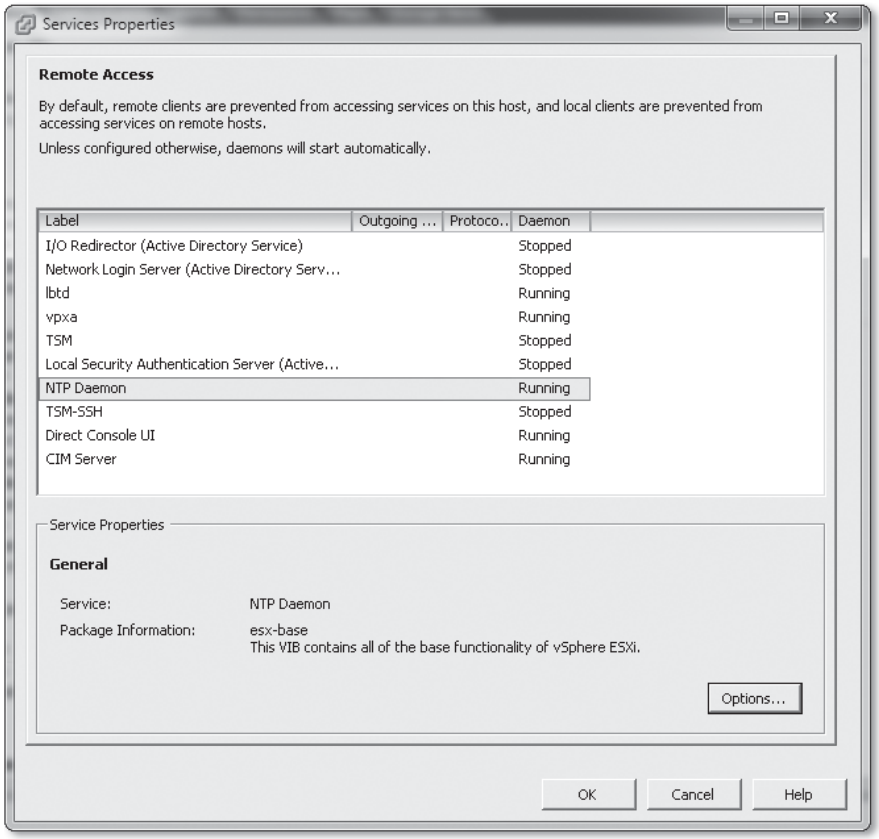


Abbildung 12.32 Dienste-Einstellungen des ESXi-Hosts

Die Startart können Sie einfach über die Eigenschaften des Dienstes ändern und für Ihre Zwecke anpassen.

12.8.1 Öffnen und Schließen eines Ports mit dem vSphere-Client

Um einen Port mit dem vSphere-Client zu öffnen oder zu schließen, müssen Sie sich direkt mit dem vSphere-Host oder mit einem vCenter verbinden und auf den CONFIGURATION-Reiter des VMware-Hosts zugreifen. Dort finden Sie einen Link mit dem Namen SECURITY PROFILE. Man vermutet nicht direkt die Firewall-Einstellungen dahinter, allerdings sind diese genau dort zu finden (Abbildung 12.33).

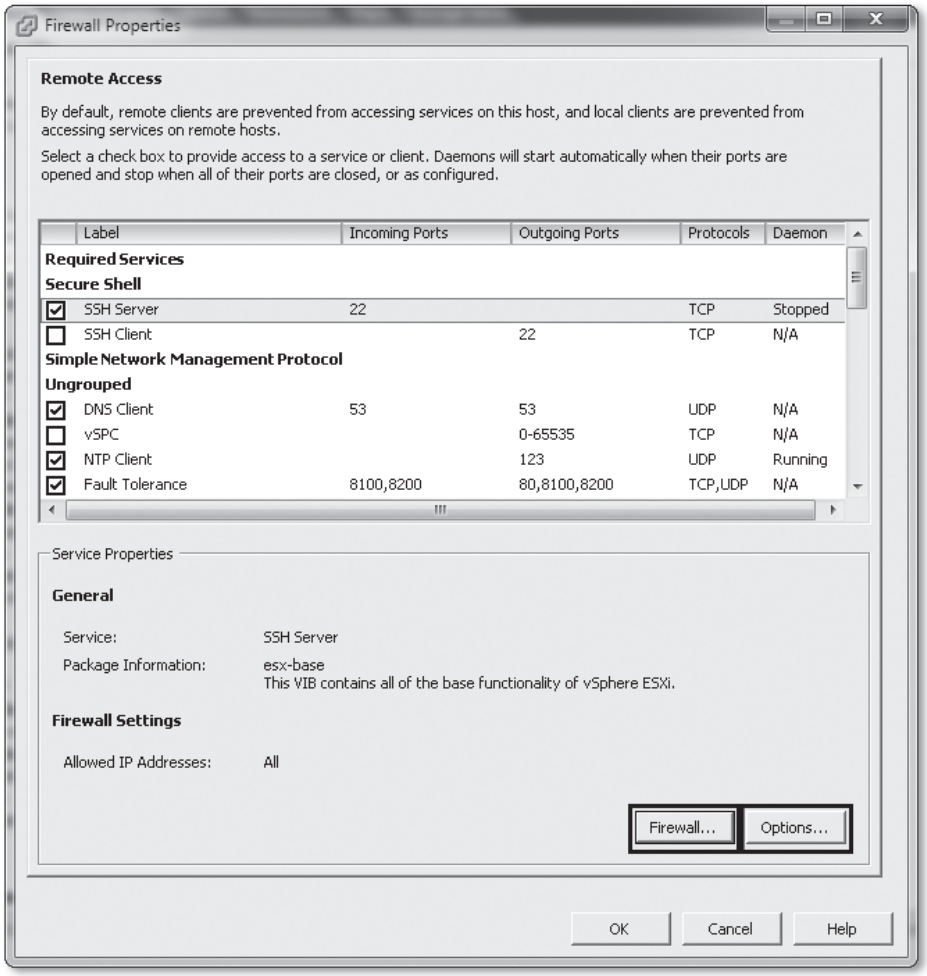


Abbildung 12.33 Portfreischaltungen der vSphere-Firewall

Es wird eine komplette Übersicht angezeigt, welche Ports mit welchen Parametern freigeschaltet sind. Diese können Sie auch hier über den Link PROPERTIES ändern. Folgen Sie dem Link, öffnet sich ein Fenster mit gängigen vorkonfigurierten Ports, die freigeschaltet werden können.

In dem Auswahlfenster bestehen zwei Schaltflächen, die weitergehende Konfigurationen erlauben. Über die Bedienfläche FIREWALL... können Sie die IP-Zugriffseinschränkungen konfigurieren.

Das Startverhalten der eingerichteten Freischaltung oder Sperrung von Ports lässt sich individuell konfigurieren. Sie haben drei Optionen für das Startverhalten der Portfreischaltung (Abbildung 12.34).

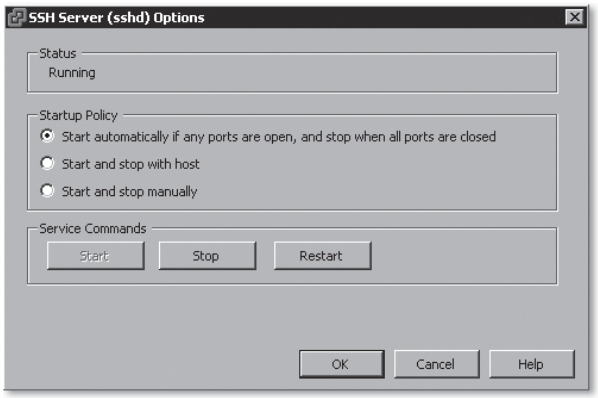


Abbildung 12.34 Startarten für Portfreischaltungen

START AUTOMATICALLY IF ANY PORTS ARE OPEN, AND STOP WHEN ALL PORTS ARE CLOSED ist die Standardoption für alle Ports. Wenn der Port geöffnet wurde, wird der Dienst automatisch gestartet. Mit der Option START AND STOP WITH THE HOST werden die Dienste direkt mit dem Host gestartet oder beendet. Bei Aktivierung von START AND STOP MANUALLY startet keine Freischaltung automatisch; der Dienst muss manuell gestartet werden. Wird der Dienst mit dieser Option manuell gestartet und später der Host neu gebootet, ist der Dienst nach dem Neustart nicht mehr verfügbar.

Vorsicht

Wird ein Port auf der Firewall, der bisher geöffnet war, geschlossen, werden bereits aktive Verbindungen nicht beendet. Die laufende Kommunikation über einen bestimmten nachträglich geschlossenen Port funktioniert noch so lange weiter, bis die Verbindung getrennt wird.

Sollen Ports freigeschaltet werden, die in dieser Liste nicht auftauchen, bleibt nur der Weg über die Kommandozeilen-Tools oder die vMA, um die Freischaltungen hinzuzufügen.

12.9 Lizenz-Server

Mit der Einführung der Version vSphere 4.x hat sich das Thema Lizenz-Server grundlegend geändert. Bei der Einführung der Virtual Infrastructure 3 gliederte VMware – warum auch immer, verstanden haben das viele Anwender nicht wirklich – den Lizenz-Server aus dem Virtual Center-Server aus. Es wurde ein externes Produkt zugekauft, das die Lizenzen verwaltete. Wie Sie wissen, hat sich das mit der letzten Version wieder geändert, es hat quasi ein »back to the Roots« stattgefunden – der Lizenz-Server hat wieder den Weg zurück ins zentrale Management gefunden. Die Freude war groß, und es ist anzunehmen, dass die Anzahl der Umgebungen, die noch den alten Lizenz-Server benötigen, weiter stark abnimmt. Nennen Sie eine Mischumgebung Ihr Eigen, dann müssen Sie *beide* Lizenz-Server einsetzen – den alten Lizenz-

Server für alle VI3.x-Systeme und den neuen, integrierten für die vSphere-Hosts ab der Version 4.x. Deshalb gehen wir auch auf beide Produkte ein.

Der Lizenz-Server ist integraler Bestandteil des vCenter-Servers und wird automatisch mit installiert. Er verwaltet alle Lizenzen und stellt sie dem vCenter selbst und den vSphere-Hosts zur Verfügung.

12.9.1 Konfiguration des vCenter-Lizenz-Servers

Der Lizenz-Server der Virtual Infrastructure seit der Version 4.x ist nicht separat zu installieren. Er integriert sich direkt in den vCenter-Server. Der Aufruf erfolgt einfach über die MANAGEMENT-Homepage des vCenters (Abbildung 12.35).

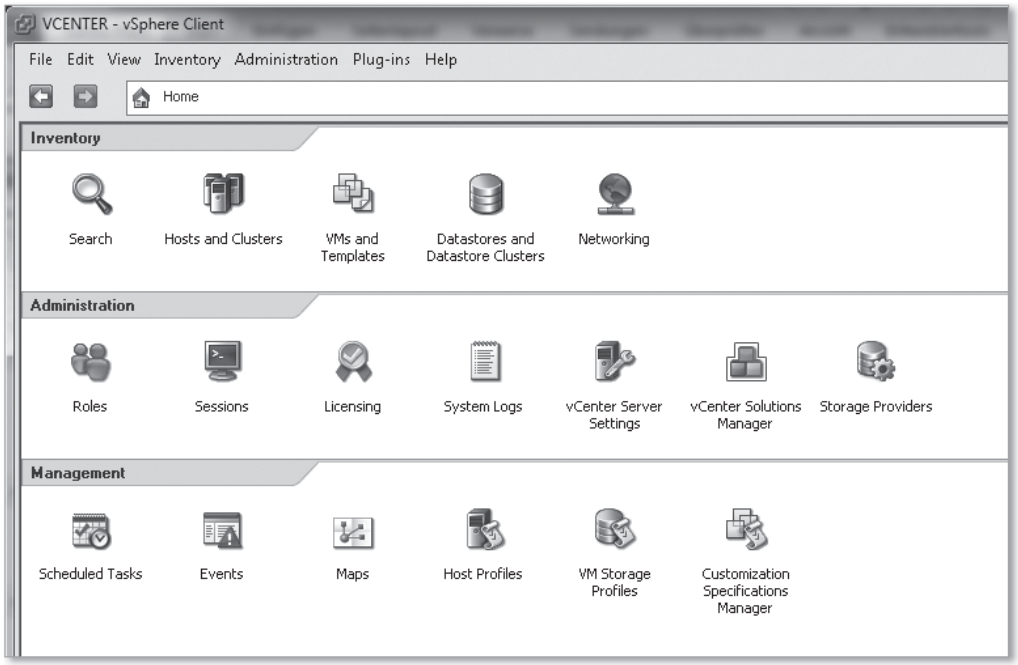


Abbildung 12.35 Aufruf des integrierten Lizenz-Servers

Haben Sie den Lizenz-Server aufgerufen, dann zeigt sich ein Übersichtsfenster mit den bereits installierten Lizenzen (Abbildung 12.36). Die Ansicht können Sie ändern, indem Sie nach Produkten, Lizenz-Keys und Asset-Daten sortieren. Die angezeigte Liste lässt sich auch exportieren; dabei stehen die Dateiformate CSV, XML, XLS, Standard-HTML und External CSS-HTML zur Verfügung.

Über den Link MANAGE VSPHERE LICENSES gelangen Sie in den eigentlichen Lizenzmanager des vCenters, wo Sie die Lizenzen verwalten (Abbildung 12.36).

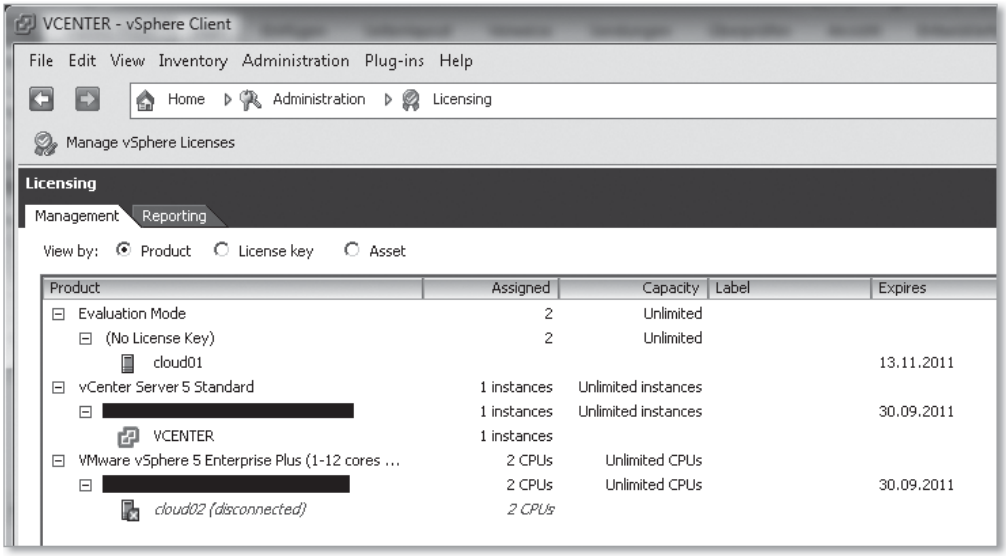


Abbildung 12.36 Übersicht des Lizenz-Servers

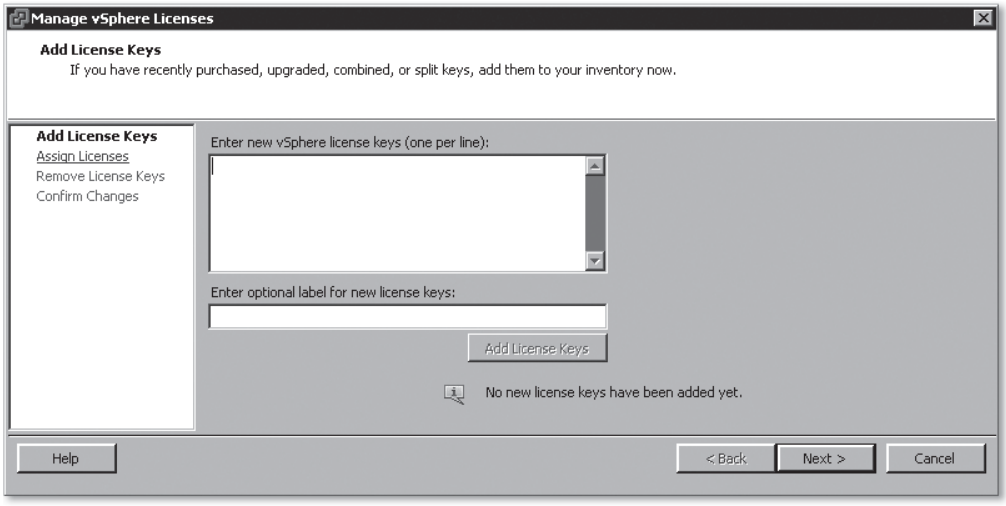


Abbildung 12.37 Hinzufügen von Lizenzen

Das Einpflegen von Lizenzen gliedert sich in mehrere Schritte. Als Erstes tragen Sie den Schlüssel ein. Optional fügen Sie zusätzlich eine Bezeichnung der Lizenz hinzu. Im zweiten Schritt weisen Sie den Key einem Asset-Satz zu (Abbildung 12.37). Haben Sie keine Angst, wenn Sie größere Umgebungen haben, Sie müssen nicht für jeden Server ein eigenes Lizenzpaket schnüren. Machen Sie es sich einfach, indem Sie einen großen Pool mit Lizenzen bilden und diesem Pool mehrere Server zuweisen. Auch an dieser Stelle können Sie Ihre Arbeit optimieren und erleichtern.

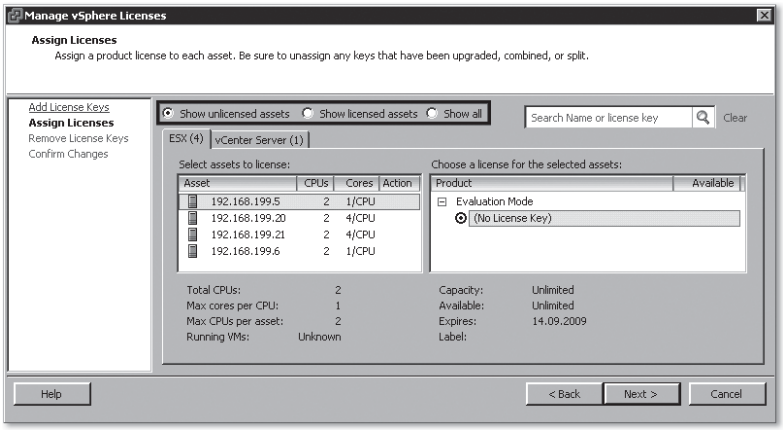


Abbildung 12.38 Zuweisen der Lizenzen zum Asset

Verschiedene Sortieroptionen ermöglichen eine Auflistung nach lizenzierten, unlizenzierten oder aller Assets. Zwei Reiter separieren die Lizenzen zwischen vCenter Server und vSphere-Hosts. Genauere Informationen über den Asset-Satz finden Sie im unteren Teil des Fensters. Im folgenden Fenster können Sie nicht zugewiesene Lizenzen vom Server entfernen.

Ihnen steht noch ein weiterer Weg zum Einpflegen von Lizenzen zur Verfügung, und zwar unter Administration • vCenter Server Settings… • Licensing (Abbildung 12.39).

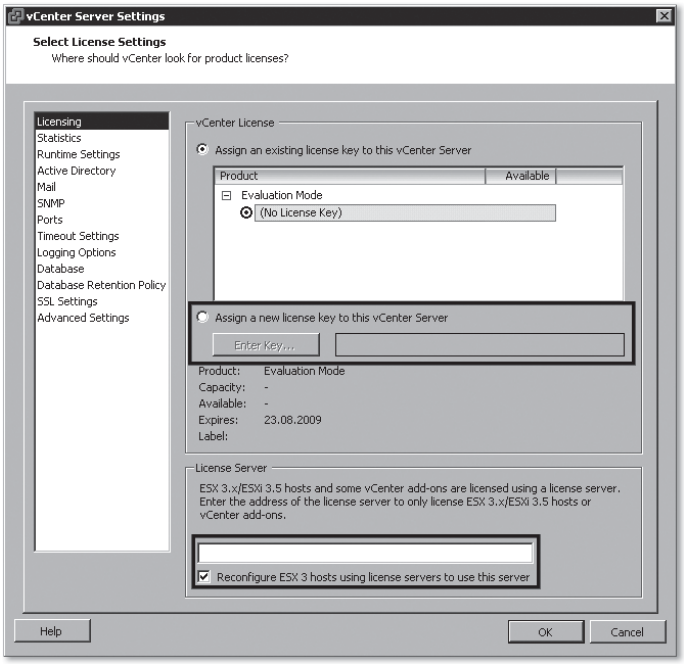


Abbildung 12.39 Lizenzpflege über die »vCenter Server Settings«

Die Vorgehensweise entspricht im Wesentlichen der bereits weiter oben beschriebenen.

12.9.2 Konfiguration des Lizenz-Servers für VI3.x-Systeme

Benötigen Sie weiterhin – ob temporär oder auf Dauer – einen Lizenz-Server für eine Virtual Infrastructure 3.x, dann ist dieser nach der Installation dem vCenter-Server bekanntzugeben. Setzen Sie keine VI3-Systeme mehr ein, können Sie diesen Abschnitt komplett überspringen.

Die Anmeldung der VI3.x-Lizenz-Servers erfolgt ebenfalls unter ADMINISTRATION • VCENTER SERVER SETTINGS… • LICENSING. Im unteren Teil des Fensters (siehe Abbildung 12.39) geben Sie den Lizenz-Server bekannt.

Den Lizenz-Server selbst können Sie über das vCenter nicht administrieren. Diesen Lizenz Server müssen Sie über das Startmenü den VMWARE LIZENZ SERVER aufrufen. Die beiden Einträge im Startmenü sind die Tools, mit denen Sie den VMware-Lizenz-Server konfigurieren und administrieren (Abbildung 12.40). Eine entsprechende Dokumentation finden Sie dort ebenfalls.

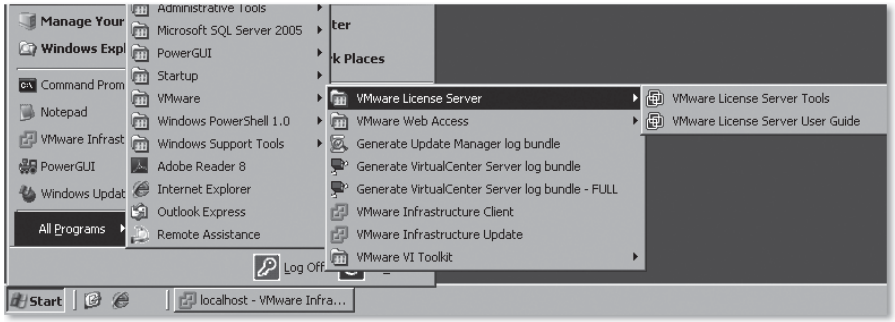


Abbildung 12.40 Start-Menü-Eintrag »VMware License Server«

Nach dem Aufruf der VMware-Lizenz-Server-Tools startet das GUI, mit dem Sie den VMware-Lizenz-Server konfigurieren (Abbildung 12.41). Die wichtigsten Reiter für die Administration sind SYSTEM SETTINGS, START/STOP/REREAD, SERVER DIAGS und CONFIG SERVICES. Mit diesen Reitern konfigurieren und analysieren Sie den VMware-Lizenz-Server.

Unter dem Reiter SYSTEM SETTINGS werden wichtige Informationen angezeigt (Abbildung 12.42). Diese sollten Sie in einer Datei speichern. Für ein eventuelles Wiederherstellen des Lizenz-Servers sind diese Dateien möglicherweise entscheidend.

Mit den Funktionen unter dem Reiter START/STOP/REREAD halten Sie den Lizenz-Server an, starten ihn und lesen die Lizenzdatei neu ein (Abbildung 12.43). Bei Problemen mit dem Lizenz-Server bringt ein einfaches Neustarten oder ein Einlesen der Lizenzdatei oft die gewünschte Funktion wieder online.

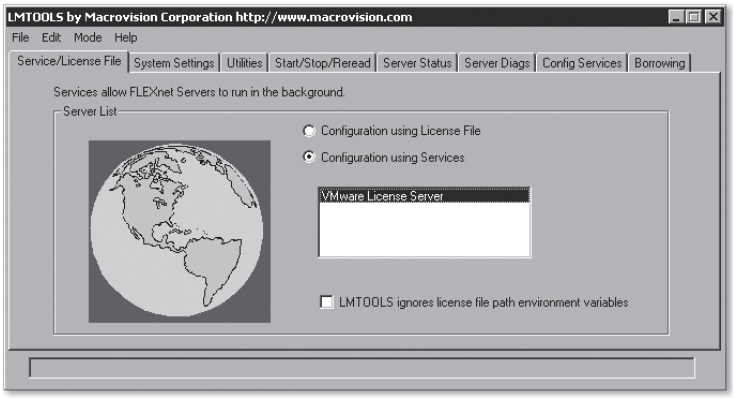


Abbildung 12.41 Konfigurationsfenster VMware-Lizenz-Server

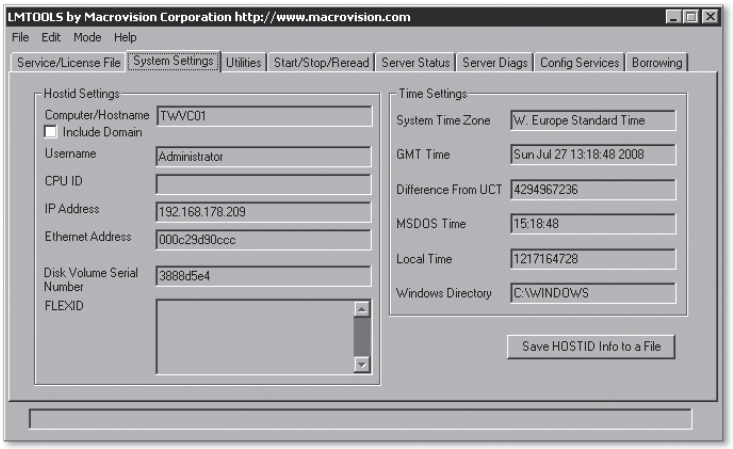


Abbildung 12.42 VMware-Lizenz-Server »System Settings«

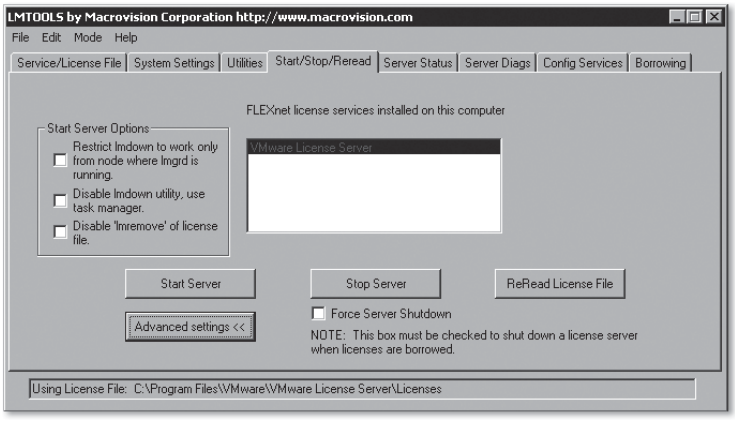


Abbildung 12.43 VMware-Lizenz-Server »Start/Stop/Reread«

Sollten Probleme mit dem Lizenz-Server auftreten, ist es möglich, unter dem Reiter SERVER DIAGS eine Diagnose durchzuführen (Abbildung 12.44).

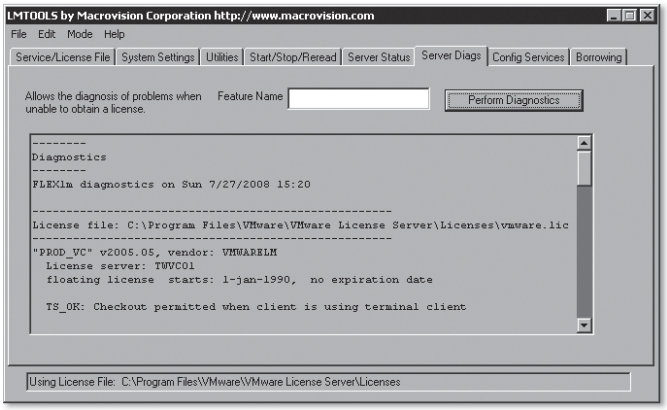


Abbildung 12.44 VMware-Lizenz-Server »Server Diags«

Die eigentliche Konfiguration erfolgt unter dem Reiter CONFIG SERVICES. Hier geben Sie die Pfade an, die das System benötigt, damit es einwandfrei läuft. Die Angaben beziehen sich auf das Log-Verzeichnis, den Ort der Lizenzdateien und den Pfad der EXE-Datei (Abbildung 12.45).

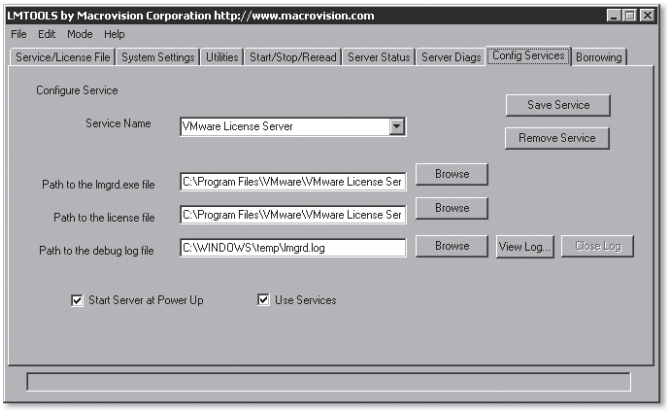


Abbildung 12.45 VMware-Lizenz-Server »Config Services«

Einbindung der Lizenzdateien in den Lizenz-Server vereinfachen

Viele Anwender kopieren alle Lizenzschlüssel in einer Datei zusammen, damit sie in den Lizenz-Server eingebunden werden können. Es ist auch möglich, alle Dateien in ein Verzeichnis zu kopieren und beim PATH TO THE LICENSE FILE nicht, wie oft beschrieben, die Lizenzdatei, sondern nur den Pfad anzugeben. In diesem Fall werden alle Lizenz-Files eingelesen, die in diesem Verzeichnis gefunden werden.

12.9.3 DNS-Name für Lizenz-Server

Es gibt einen relativ einfachen Weg, damit Umzüge des Lizenz-Servers nicht zu arbeitsintensiv sind: Der Administrator lässt sich von den DNS-Verantwortlichen ein Alias für den Lizenz-Server einrichten.

Das Problem des Lizenz-Servers ist aber, dass er sich trotz Alias auf den Host-Namen referenziert und auf dem ESXi 3.x-Host das Alias gegen den Server-Namen tauscht. Diese Problem umgehen Sie, indem Sie nach dem Umzug des Servers dem System das Alias als Server-Namen geben und den eigentlichen Server-Namen als Alias im DNS einrichten. Bei dieser Vorgehensweise müssen Sie weder auf dem vCenter-Server noch auf den VI3.x-Hosts nach dem Umzug eine Anpassung vornehmen.

12.9.4 Umzug eines Lizenz-Servers

Nachdem Sie einen Lizenz-Server für die VMware Virtual Infrastructure installiert und konfiguriert haben, arbeitet er in den meisten Fällen ohne Probleme und wird so schnell nicht mehr angefasst. Es gibt allerdings nicht wenige Fälle, bei denen der Lizenz-Server umziehen muss. Dies kann verschiedene Gründe haben, wie zum Beispiel den Austausch der Hardware oder die Erweiterung der Infrastruktur.

Der Vorgang als solcher ist eigentlich relativ unproblematisch: Sie installieren den Lizenz-Server auf einem anderen System neu und stellen ihn zur Verfügung. Sie kopieren die Lizenzen in das entsprechende Verzeichnis, testen die Funktion und geben den neuen Server allen Systemen bekannt. Zum einen müssen Sie auf den VI3.x-Hosts den neuen Server eintragen und zum anderen im vCenter-Lizenzmanager das neue Ziel angeben (siehe Abbildung 12.39).

12.10 Erweiterte Hardwarekonfiguration

Die Einträge HARDWARE auf dem Konfigurationsreiter möchten wir Ihnen nun näherbringen. In diesem Abschnitt finden sich unterschiedliche Einstellungen, die direkt im Zusammenhang mit der Server-Hardware stehen. Die Auswahl PROCESSORS ermöglicht die Aktivierung des Hyperthreadings bei Hosts mit Intel-CPUs.

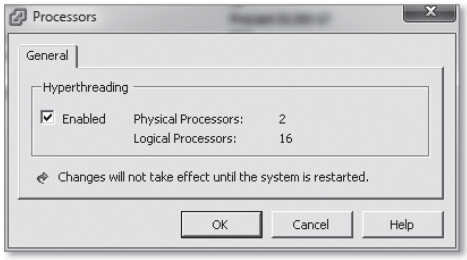


Abbildung 12.46 Aktivierung des Hyperthreadings

Der Punkt Memory ist eine reine Anzeige, hier können Sie keine Einstellungen anpassen. Sie sehen hier den Gesamtspeicher des Systems und wie viel Speicher dem Host selbst bzw. den virtuelle Maschinen zur Verfügung steht. Die Auswahl Storage gibt Ihnen zwei verschiedene Ansichten.

Abbildung 12.47 zeigt die Ansichten für den Storage-Auswahlpunkt. Dabei ist das Gesamtbild die Devices-Ansicht, und das rot Umrandete zeigt die Ansicht für den Punkt Datastores. Nähere Angaben finden Sie in Kapitel 9. Die Auswahl Storage Adapters zeigt die im Host verbauten Storage-Controller an. Auch hierzu erläutert Kapitel 9 weitere Details.

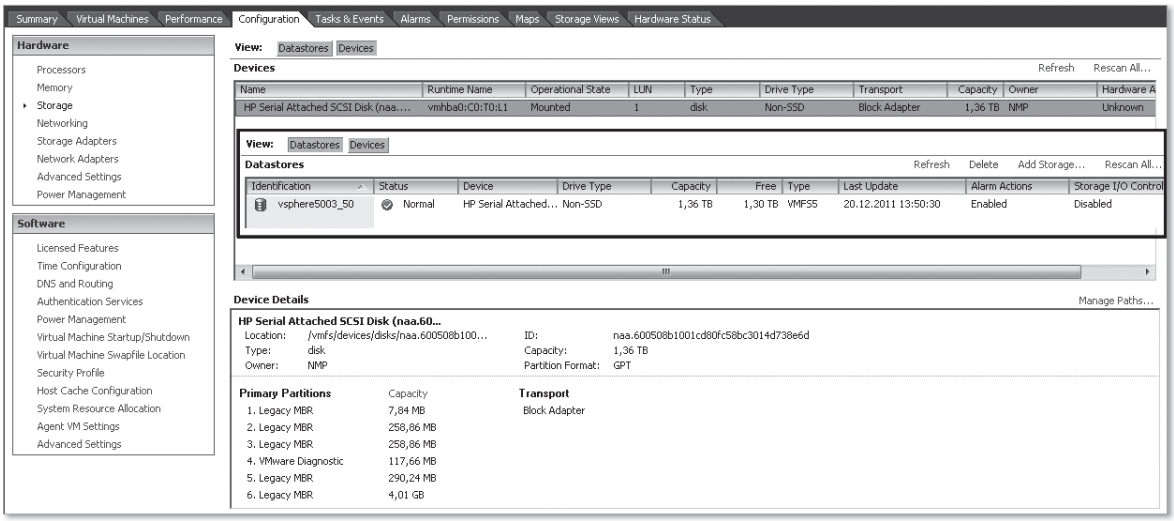


Abbildung 12.47 Ansichten in der Storage-Konfiguration

Auch bei den beiden Links für die Netzwerkkomponenten dient einer für die eigentliche Netzwerkkonfiguration, und hinter dem anderen Link verbirgt sich die Anzeige der im Host verbauten Netzwerkadapter. Weitergehende Informationen finden Sie in Kapitel 8.

Eine sehr interessante Funktion bietet der Link Advanced Settings. Hier gibt Ihnen das System die Option, Host-Hardware direkt in eine virtuelle Maschine zu binden. Rufen Sie den Link auf, dann befinden Sie sich zuerst in einem leeren Fenster, gelangen aber über den Link Configure Passthrough in eine Auswahl.

Hier finden Sie alle Geräte des Hosts, die Sie an eine virtuelle Maschine weiterreichen können. Im unteren Abschnitt des Fensters sehen Sie die Eigenschaften des ausgewählten Gerätes. Haben Sie ein Gerät an dieser Stelle aktiviert, dann können Sie es später in der VM einhängen. Alle Konfigurationsänderungen, die Sie hier am Host vornehmen, erfordern aber einen Reboot des Hosts.

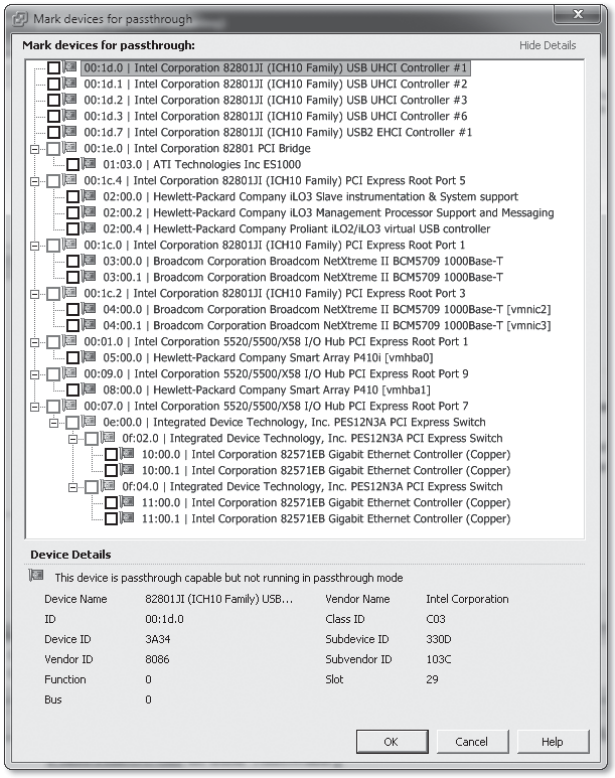


Abbildung 12.48 Passthrough-Hardware

Lassen Sie uns Ihnen nun zeigen, wie Sie ein solches Gerät in die VM einbinden. Dazu fahren Sie zuerst die VM herunterfahren und gehen dann in die Eigenschaften der Maschine zum Hinzufügen von Hardware. Wählen Sie dazu ein PCI-Device aus.

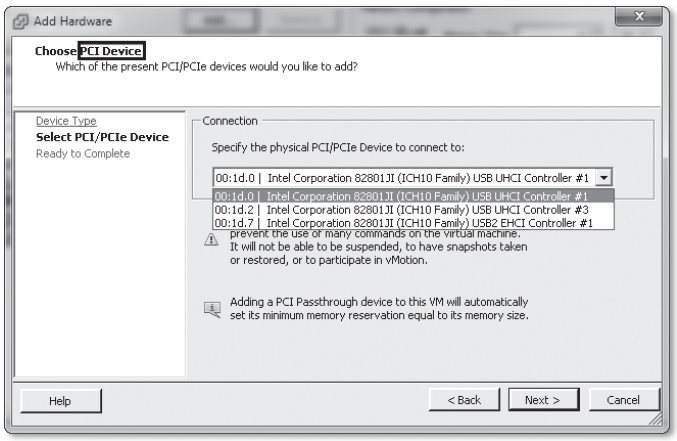


Abbildung 12.49 Einbinden eines Hardware-Devices in eine VM

Wählen Sie nun das Gerät aus. In diesem Fall gibt es drei USB-Controller, die eingebunden werden können. Sie binden hier kein Gerät ein, sondern den Controller. Bedenken Sie bitte, dass es die folgenden Einschränkungen für eine VM gibt, wenn Sie auf diese Art und Weise Geräte hinzufügen:

- kein Suspenden der VM
- kein vMotion
- kein Snapshot-Handling möglich,
- minimale Speicherreservierung wird auf den konfigurierten Arbeitsspeicher gesetzt.

Nach dem Start der virtuellen Maschine erkennen Sie im Gerätemanager, dass die Hardware ordnungsgemäß eingebunden wurde.

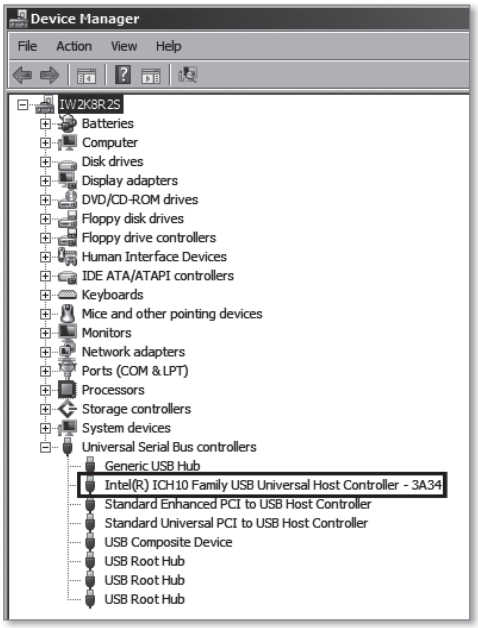


Abbildung 12.50 Passthrough-Hardware in einer virtuellen Maschine

Sollten Sie nun auf der VM ein USB-Gerät aufstecken, so können Sie es direkt in der VM nutzen.

Der letzte Menüpunkt unter Configuration • Hardware ist Power Management. An dieser Stelle können Sie für den einzelnen Host hinterlegen, wie stromsparend er agieren soll.

Vier unterschiedliche Einstellungen unterschiedlicher Abstufungen finden sich hier. Drei fest vordefinierte Rollen können Sie auswählen und eine Rolle, die frei konfigurierbar ist. Die konfigurierbaren Parameter für die frei einstellbare Power-Management-Rolle finden sich auf dem Configuration-Reiter unter Software • Advanced Settings • Power.

Hier können Sie dann die Anpassungen an Ihre Landschaft vornehmen.

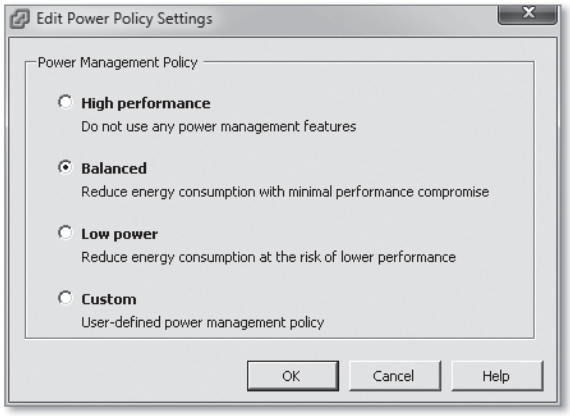


Abbildung 12.51 Host-Power-Management

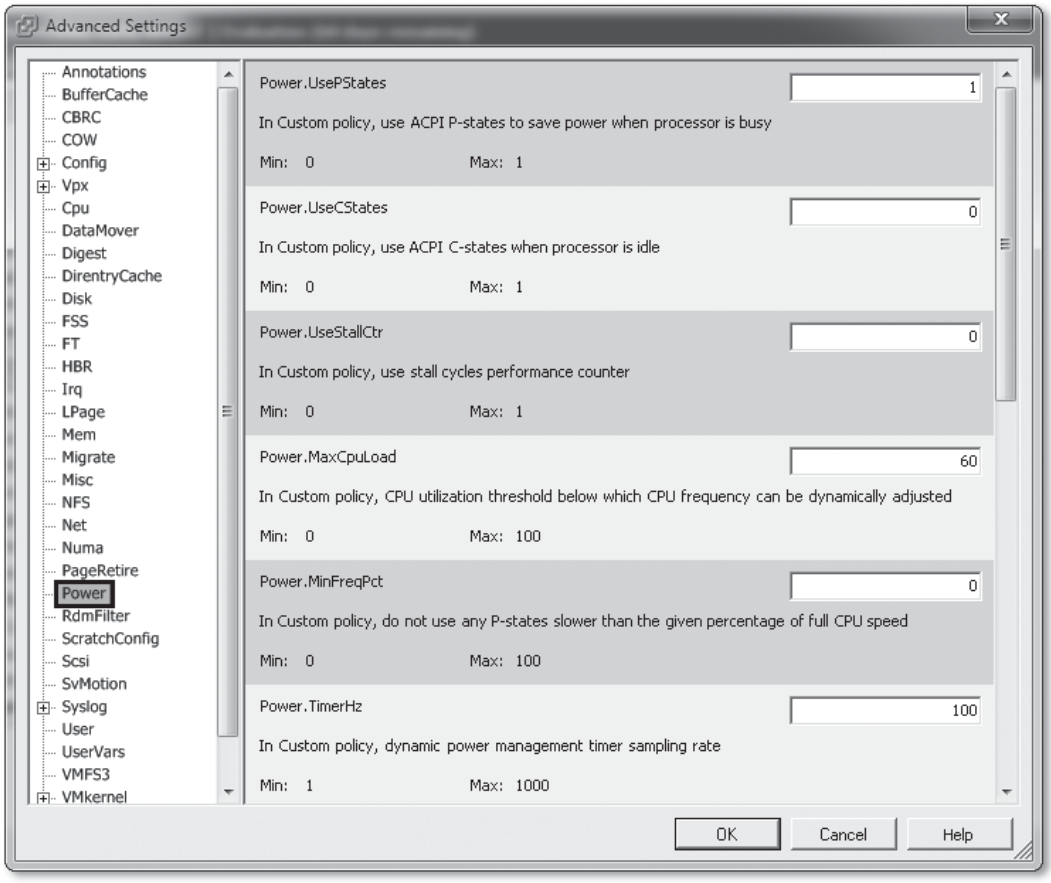


Abbildung 12.52 Anpassung der Power-Management-Parameter

12.11 Erweiterte Softwarekonfiguration

Lassen Sie uns nun auf die Einstellungen eingehen, die Sie am Host noch vornehmen können, die wir aber bis jetzt noch nicht angesprochen haben. Es handelt sich um insgesamt drei Punkte.

12.11.1 Ablage der VM-Swapfiles

VMware setzt bei seiner virtuellen Infrastruktur Mechanismen ein, die es ermöglichen, den virtuellen Maschinen mehr Arbeitsspeicher zuzuweisen, als tatsächlich in dem Host-System vorhanden ist. Das sogenannte Memory-Overcommitment bedingt aber, dass der Host nicht aktiv genutzten Arbeitsspeicher der einzelnen virtuellen Maschine auslagert. Diese Auslagerung findet, wie bei anderen Systemen auch, ins File-System statt. An dieser Stelle gibt es nun die Möglichkeit, festzulegen, an welchem Speicherort der Arbeitsspeicher ausgelagert werden soll.

Bei der Version vSphere 5.0 hat sich eine entscheidende Änderung in diesem Punkt ergeben. Findet das System eine SSD-Festplatte im ESXi-Host, dann wird dem Administrator angeboten, diese Platte als Swap-Location zu nutzen. Der Vorteil liegt auf der Hand: Eine bessere Ablage für ein Swapfile gibt es wohl nicht. Dieses Feature können Sie aber nur auf dem Host konfigurieren. Sie finden diese Einstellung unter dem Link Software • Host Cache Configuration. Wie mit dem Swappen umgegangen wird, lässt sich an zwei Stellen festlegen – entweder lokal an jeder virtuellen Maschine oder global am Cluster. Am Cluster können Sie das Swapfile im Verzeichnis der virtuellen Maschine ablegen oder in dem am Host konfigurierten Pfad.

Die gleichen Einstellungen können Sie in den Eigenschaften der virtuellen Maschinen unter dem Punkt Options • Swapfile Location vornehmen. Bedenken Sie bitte: Wenn Sie das Memory-Swapfile einer virtuellen Maschine auf einen lokalen Datastore ablegen, erhöhen sich die Zeiten beim vMotion, wenn der Host der VM sich ändert. In diesem Fall muss nämlich das gesamte Swapfile mit auf den neuen Host verschoben werden. Sie sehen also, dass es genau überlegt sein will, wie Sie diese Funktion konfigurieren. Wägen Sie alle Vor- und Nachteile gegeneinander ab, bevor Sie Ihr System passend konfigurieren. Auch an dieser Stelle ist es sehr wichtig, auf eine Einheitlichkeit der Konfiguration zu achten. Es bringt nichts, wenn Sie bei einer großen Anzahl von virtuellen Maschinen mit einem zu hohen Individualisierungsgrad arbeiten. Ist es trotz alledem erforderlich, dann dokumentieren Sie diese Schritte genau, damit im späteren Betrieb keine Probleme auftreten.

12.11.2 Host-Systemressourcen

Wählen Sie den Punkt Software/System Ressource Allocation aus. An dieser Stelle lassen sich die Systemressourcen des Host-Systems sehr granular einstellen. Es geht dabei nicht um die Service Console, sondern um die Zuweisungen von Ressourcen für den Hypervisor. Die

Einstellungen gruppieren sich in zwei Abschnitte. Im ersten Abschnitt weisen Sie den einzelnen Softwarekomponenten die Prioritäten und Ressourcen zu, im zweiten Abschnitt dem Hypervisor die Hardwareressourcen. Sie finden die Einstellungen im CONFIGURATION-Bereich (Abbildung 12.53).

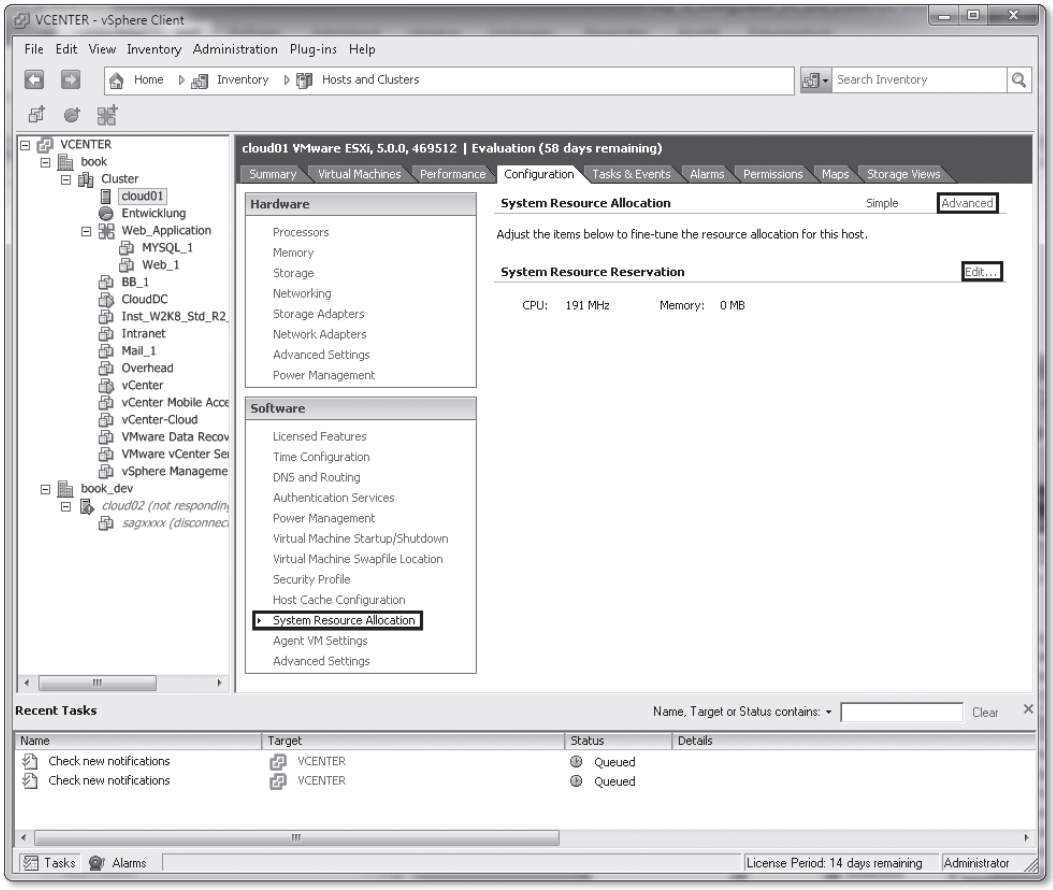


Abbildung 12.53 Einstellung der Hypervisor-Ressourcen

An die Einstellungen für die Hardwareressourcen gelangen Sie über den EDIT-Button. Die standardmäßigen Einstellungen für diesen Punkt sind in Abbildung 12.54 dargestellt.

Im Dialog fallen drei Dinge sofort auf: Zum einen liegen die SHARES-Werte weit unter den standardmäßigen LOW-Werten, zum Zweiten liegt für den Arbeitsspeicher keine Reservierung vor, und als Drittes ist für die Reservierung der CPU ein Wert eingetragen, der je nach gewähltem Host unterschiedlich ist. Woher kommt dieser krumme Wert? Die Erklärung ist ganz einfach: Das System reserviert automatisch 10 % der Taktfrequenz der CPU. In diesem Beispiel hat der Host also eine oder mehrere CPUs mit 1,91 GHz Taktfrequenz. Die Anzahl der Cores pro CPU spielt an dieser Stelle keine Rolle.

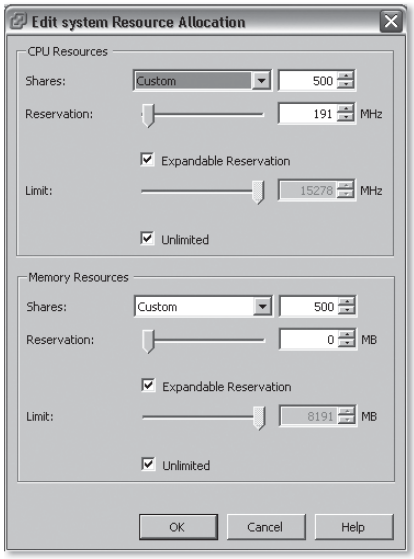


Abbildung 12.54 Ressourcenzuweisung für den Hypervisor

Kommen wir zum Thema Priorisierung von Systemressourcen. Über die beiden Links oben rechts lässt sich die Ansicht variieren. Mit der Auswahl von SIMPLE werden keine zusätzlichen Einstellmöglichkeiten dargestellt. Wechseln Sie dagegen in den ADVANCED-Modus, können Sie für jede der gelisteten System-Resource-Pool-Einträge die Konfiguration anpassen.

Hier eine eindringliche Warnung von unserer Seite: Überlegen Sie sich genau, ob Sie an dieser Stelle Änderungen vornehmen, ohne dass der VMware-Support Sie dazu auffordert. Gehen Sie einfach davon aus, dass sich VMware bei der Festlegung der Standardwerte Gedanken gemacht hat. Sie hebeln hier unter Umständen das System aus. Überlassen Sie den Spieltrieb anderen, und bewahren Sie Ihr System vor selbstverursachten Problemen.

12.11.3 Erweiterte Einstellungen

Jetzt kommen wir zu einem großen Abschnitt mit sehr vielen Unbekannten. Unter SOFTWARE • ADVANCED SETTINGS erreichen Sie das Fenster aus Abbildung 12.55.

Dieser Dialog bietet die Möglichkeit, viele Parameter des vSphere-Hosts anzupassen. Hier ändern Sie Einstellungen, wenn z. B. der Hardwarehersteller des Storages Sie dazu auffordert. Auch der VMware-Support verlangt von Ihnen hier möglicherweise eine Anpassung von Einstellungen, wenn es Probleme gibt. Viel mehr können wir Ihnen zu diesem Fenster aber nicht berichten, denn für die Funktion der einzelnen Parameter gibt es nur eine Kurzbeschreibung in der rechten Fensterhälfte. Mehr ist nirgends dokumentiert. Nur einige wenige Werte sind in unterschiedlichen Internetforen beschrieben. Auch hier gilt das, was wir schon im vorhergehenden Abschnitt geschrieben haben: Ändern Sie nur Werte, wenn der Hardware- oder Software-Support Sie dazu auffordert. Weniger ist auch hier mehr.

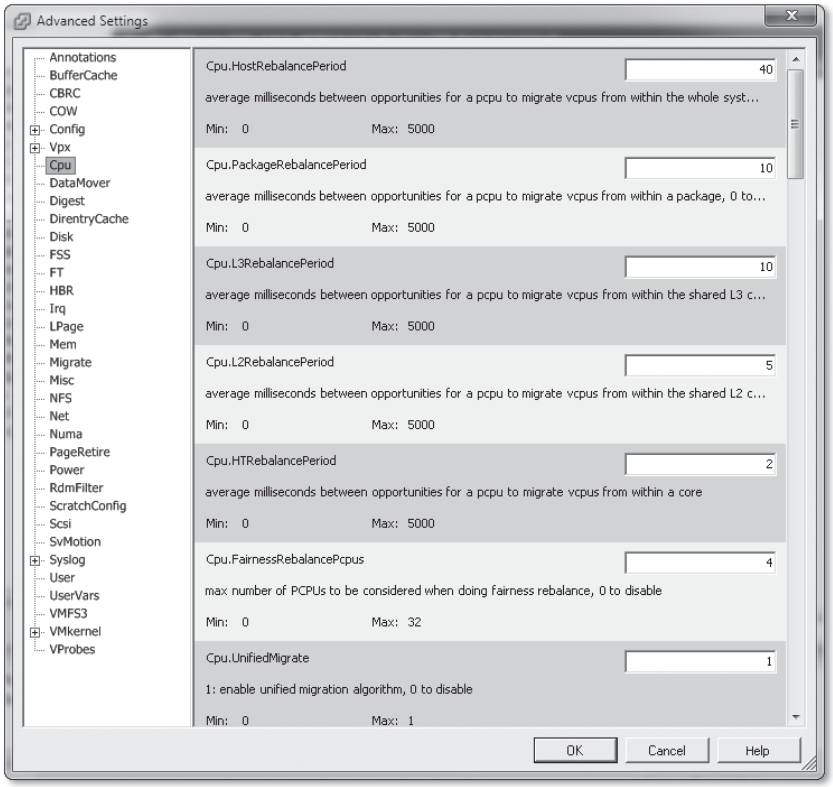


Abbildung 12.55 Fenster der »Advanced Settings«

12.12 vCenter-Berechtigungen

Wir haben uns bis jetzt wie selbstverständlich im vCenter bewegt. Aber wie ist das möglich? Woher kennt der vCenter-Server den Benutzer-Account aus dem Betriebssystem? Diese Fragen möchten wir in diesem Abschnitt klären.

VMware integriert den vCenter-Server nahtlos in das Benutzer-Gruppen-System des Windows-Betriebssystems. Ist der Server Mitglied eines Active Directorys (ADS), dann können auch Benutzer und Gruppen des ADS im vCenter berechtigt werden. Dass diese nahtlose Integration auch Probleme aufwirft, zeigen wir Ihnen in Abschnitt 11.3. Lesen Sie jetzt, wie VMware mit den Berechtigungen im vCenter umgeht.

Berechtigungssysteme führen immer zwei Komponenten zusammen: zum einen die Anwender, das können sowohl Benutzer als auch Gruppen sein (wir werden, der Einfachheit halber, nur noch von den »Benutzern« sprechen), zum anderen die Rechte. Beides wird in der Managementoberfläche zusammengeführt und bildet so ein Netzwerk für die Administration der gesamten Infrastruktur mit unterschiedlichen Rechteebenen.

Keine Angst, Sie müssen bei der Installation keine Benutzer anlegen. Das vCenter sucht sich automatisch die Gruppe »Administrators« und verbindet sie mit der Administratorengruppe des vCenters. Dieser Mechanismus funktioniert übrigens auch, wenn die Administratorengruppe umbenannt wurde. Die Gruppe der lokalen Administratoren ist damit auch automatisch die Hauptadministratoren-Gruppe im vCenter-Server.

Rechte können an alle Objekte des vCenters gebunden werden. Wenn die Möglichkeit besteht, aktiv Rechte zu vergeben, dann ist auf der rechten Seite im vCenter ein Reiter Permissions zu sehen. Hier führen Sie dann die entsprechenden Arbeiten durch (Abbildung 12.56).

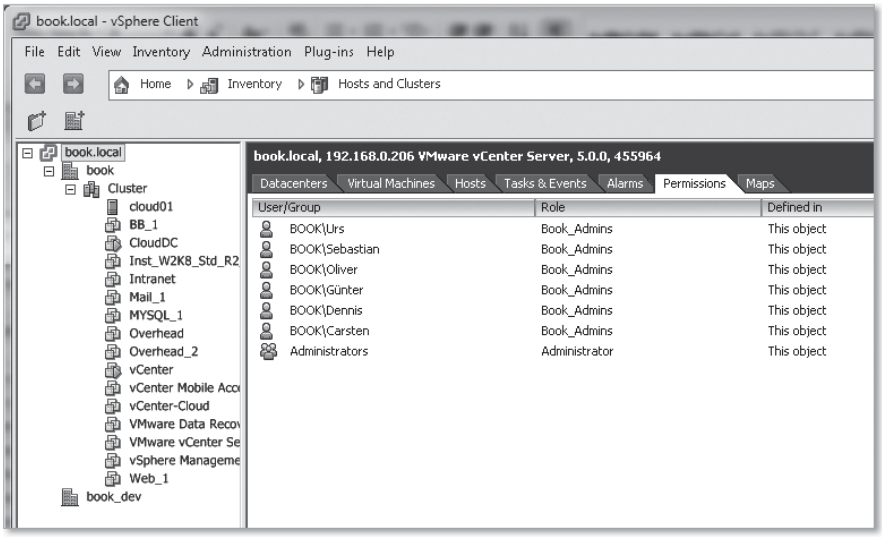


Abbildung 12.56 Rechtevergabe im vCenter

Unsere Empfehlung ist, dass Sie Rollen – so nennt VMware die Berechtigungen – für alle benötigten Zwecke erstellen und passend benennen. Lassen Sie in der Domäne ebenfalls passende Gruppen erstellen. Diese beiden Elemente fügen Sie dann im vCenter zusammen. Alle Anwender, die Berechtigungen benötigen, müssen dann nur in die passende ADS-Gruppe geschoben werden, und schon stehen die Berechtigungen. Mit dieser Strategie lassen sich die Benutzer und Rechte sehr einfach einpflegen.

Wie so oft kann man auch hier sagen: Weniger ist mehr. Vergeben Sie nur Rechte für Anwender, die Berechtigungen benötigen, und berechtigen Sie Mitarbeiter nicht schon im voreilenden Gehorsam.

12.12.1 Rollen

Nach der Neuinstallation stellt das System eine Reihe von Rollen zur Verfügung. Über den Menüpunkt Ansicht • Verwaltung • Rollen gelangen Sie in die Verwaltung der Benutzerrechte (Abbildung 12.57).

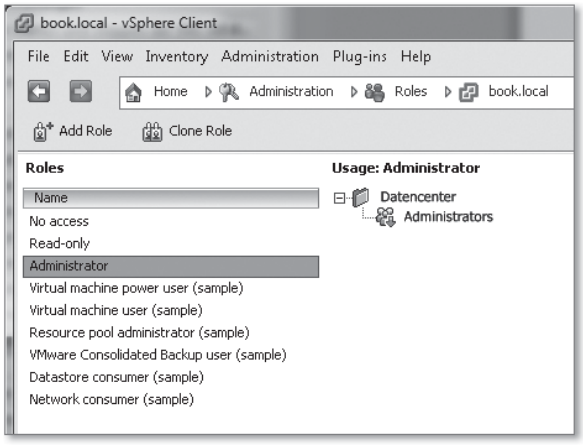


Abbildung 12.57 Management der Benutzerrechte

Wie Sie sehen, stellt das System schon einige Benutzerrollen zur Verfügung. Tabelle 12.9 listet diese auf und beschreibt ihre Funktion.

Rolle	Rollentyp	Bemerkungen
No access	System	Das Objekt ist nicht sichtbar, und es können keine Änderungen vorgenommen werden.
Read-only	System	Alle Objekte und Reiter sind sichtbar, mit Ausnahme der Console.
Administrator	System	Diese Rolle stellt den Benutzern alle Rechte zur Verfügung, es gibt keinerlei Einschränkungen.
Virtual achine power user	Beispiel	Administrative Rechte für die Arbeiten mit virtuellen Maschinen vergibt diese Rolle. Das schließt Hardwareänderungen und das Erstellen von Snapshots ein.
Virtual machine user	Beispiel	Entspricht den Rechten des Virtual machine power user ohne die Rechte, Hardwareänderungen vorzunehmen und Snapshots zu erstellen.
Resource pool administrator	Beispiel	Gibt das Recht, untergeordnete Resource-Pools anzulegen und zu manipulieren.
VMware Consolidated Backup-user	Beispiel	Rechte für die Verwendung von VMware VCB (Vmware Consolidated Backup)
datastore consumer	Beispiel	Erlaubt das Erstellen von virtuellen Festplatten oder Snapshots.
network consumer	Beispiel	Erlaubt die Manipulation der Netzwerkeinstellungen von VMs und Hosts.

Tabelle 12.9 Beschreibung der Rollentypen

Alle Rollen ab der vierten Position werden mit (SAMPLE) gekennzeichnet. Nutzen Sie diese Rollen als Basis für Ihre eigenen Definitionen. Die drei System-Rollen lassen sich nicht ändern, Sie können aber eine Rolle kopieren und anschließend für Ihre Zwecke anpassen. Die Beispielrollen sind manipulierbar. Trotzdem sollten Sie diese Rollen nicht ändern. Über das Kontextmenü erstellen Sie einfach einen Clone der Musterrolle, passen ihn mit dem EDIT-Befehl an Ihre Bedürfnisse an und benennen ihn sprechend (Abbildung 12.58).

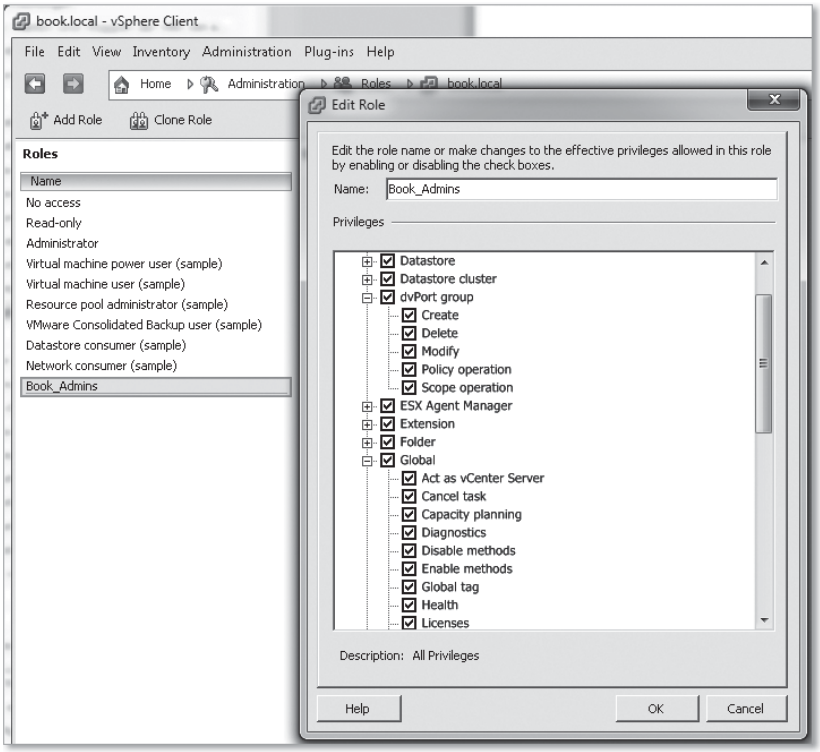


Abbildung 12.58 Anpassen einer Rolle

Selbstverständlich können Sie Rollen auch komplett neu erstellen. Über ADD ROLE legen Sie eine neue Rolle ohne jegliche Rechte an. Diese müssen Sie nur für Ihre Zwecke anpassen. Die Rechte werden immer hierarchisch vererbt. Die Vererbungsreihenfolge zeigt Abbildung 12.59.

Wie Sie sehen, übernehmen die meisten Objekte ihre Rechte von einem Vorgänger; einzig die virtuelle Maschine wird von mehreren übergeordneten Objekten beeinflusst. Das müssen Sie berücksichtigen, wenn Sie auf virtuellen Maschinen Rechte vergeben wollen. Außerdem ist es wichtig zu wissen, dass für die Freischaltung von detaillierten Funktionen, wie z. B. das Anhängen einer ISO-Datei, auch auf dem Host und dem Datastore Rechte vorhanden sein müssen.

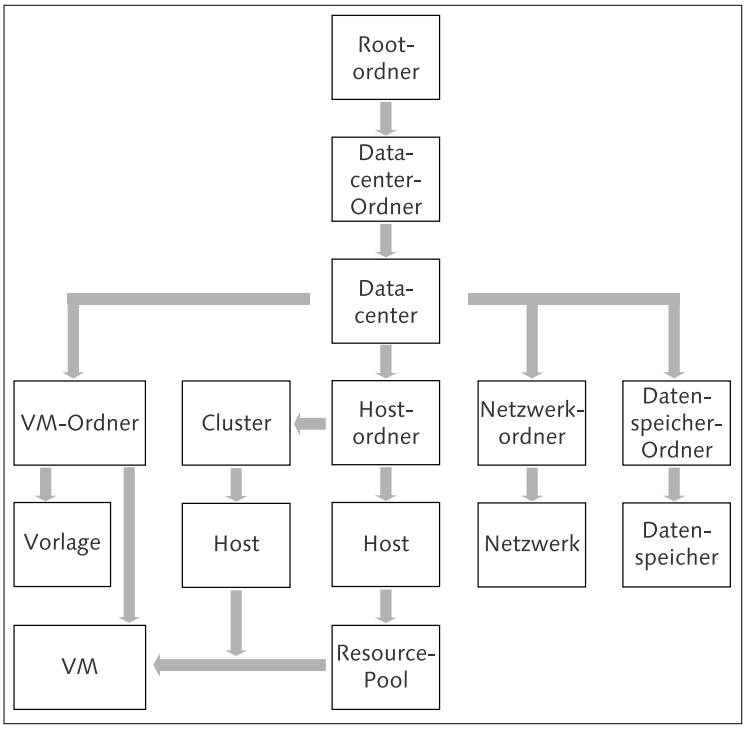


Abbildung 12.59 Form der Rechtevererbung

12.12.2 Benutzer einrichten

Wie oben bereits gesagt, werden im vCenter keine Benutzer erstellt. Der vCenter-Server referenziert sich auf die Benutzerdatenbank des Betriebssystems oder des ADS. Bevor Sie Benutzern Rollen zuweisen, sollten Sie diese Rollen einrichten. Die Verbindung zwischen dem User und den Rollen erfolgt im vCenter unter dem Reiter Permissions eines Objekts (Abbildung 12.60).

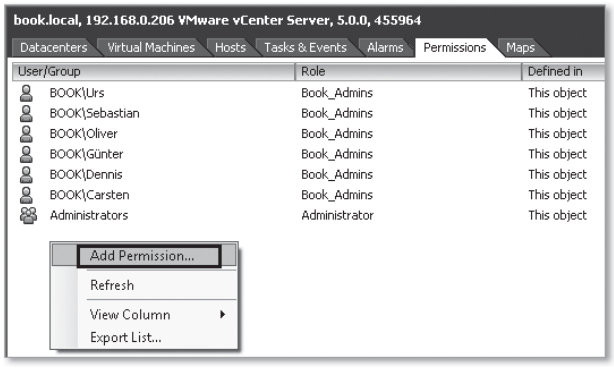


Abbildung 12.60 Neue Rechte verlinken

Nach Aufruf des Dialogs öffnet sich ein Fenster, in dem Sie zuerst auf der rechten Seite die Nutzerrechte auswählen (Abbildung 12.61). Zur Kontrolle können Sie sich unterhalb der Auswahl die zugewiesenen Rechte noch einmal genau anschauen. Änderungen der Zugriffsrechte sind hier nicht mehr möglich.

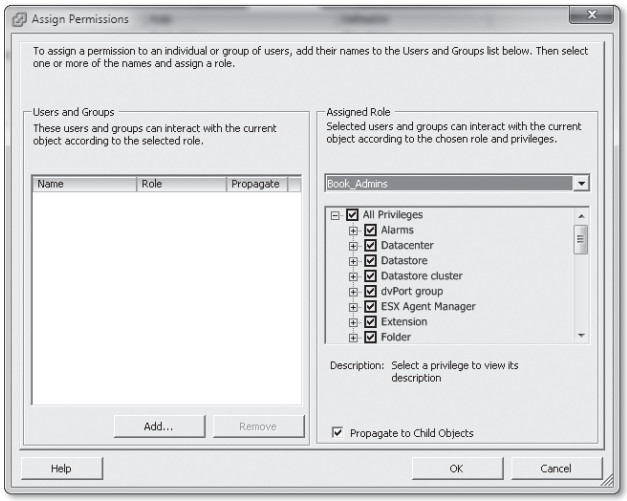


Abbildung 12.61 Einstellen der Rolle

Über den ADD-Button ordnen Sie dem ausgewählten Recht nun die Nutzer oder besser die Gruppen zu (Abbildung 12.62). Im Dropdown-Menü DOMAIN bestimmen Sie die Benutzerdatenbank, entweder die lokale Benutzerdatenbank des vCenters oder das ADS. In diesem Beispiel füge ich meinen Benutzer-Account dem vCenter hinzu.

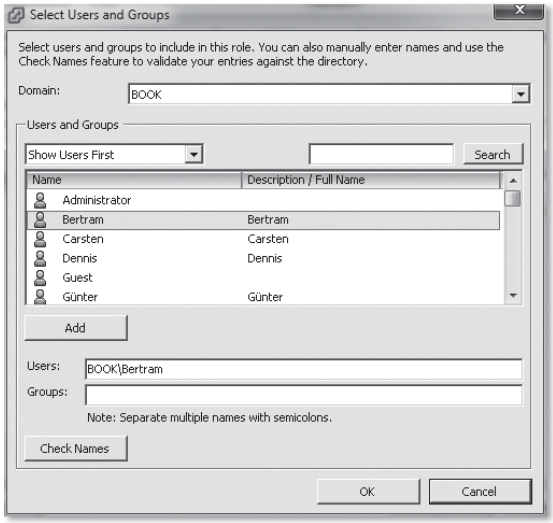


Abbildung 12.62 Auswahl eines Users

Mit dem Abschluss des Dialogs wird der Zusammenhang im Hauptfenster dargestellt (Abbildung 12.63). Selbstverständlich können Sie auch mehrere Objekte hinzufügen und mit dem ausgewählten Recht verbinden.

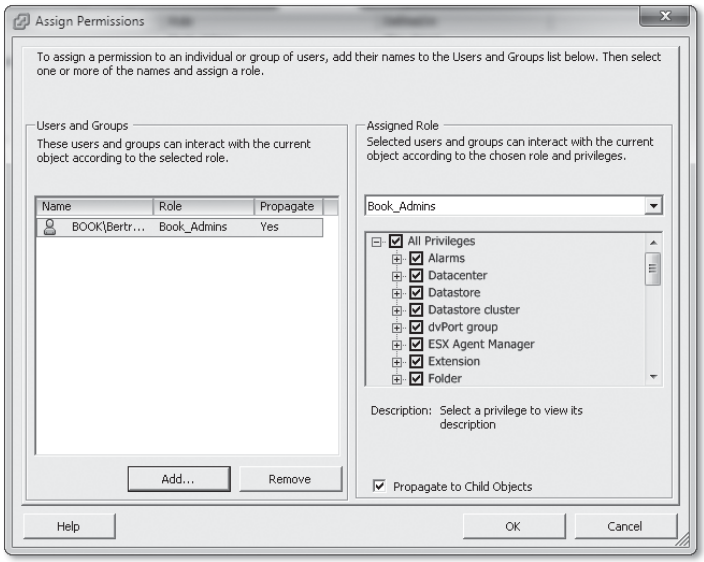


Abbildung 12.63 Verknüpfung von Gruppen bzw. Benutzern mit den Rollen

Achten Sie auf die Auswahl unten rechts im Fenster. Über die Aktivierung von PROPAGATE TO CHILD OBJECTS werden die Rechte in sämtliche untergeordnete Objekte weitergereicht.

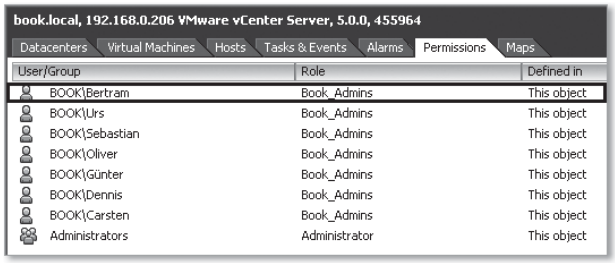


Abbildung 12.64 Neu eingerichtete Rechte für den User »Bertram« aus der Domäne »BOOK«

Das neu angelegte Recht ist nun in der Oberfläche sichtbar. Eine große Hilfe ist, dass in der rechten Spalte angezeigt wird, an welcher Stelle der Ursprung des Rechtes liegt.

Rechtekonkurrenz

Die Rechte eines einzelnen Users überschreiben die Rechte einer Gruppe. Ebenso haben die Rechte, die weiter unten in der Struktur vergeben werden, eine höhere Priorität als diejenigen, welche darüber liegen.

Ein User ist Mitglied in zwei Gruppen, Admin im Datacenter und User (Read-only-Rechte) in einem Ordner *Entwicklung* unterhalb des DCs. Geht der User in den Ordner *Entwicklung*, werden die Admin-Rechte ausgeblendet, und er hat nur Read-only-Rechte.

Benutzerrechte werden regelmäßig vom System validiert. Im vCenter können Sie das Zeitintervall einstellen. In den Standardeinstellungen werden die Accounts einmal am Tag (Abbildung 12.65) und selbstverständlich bei einem Neustart des Management-Servers überprüft.

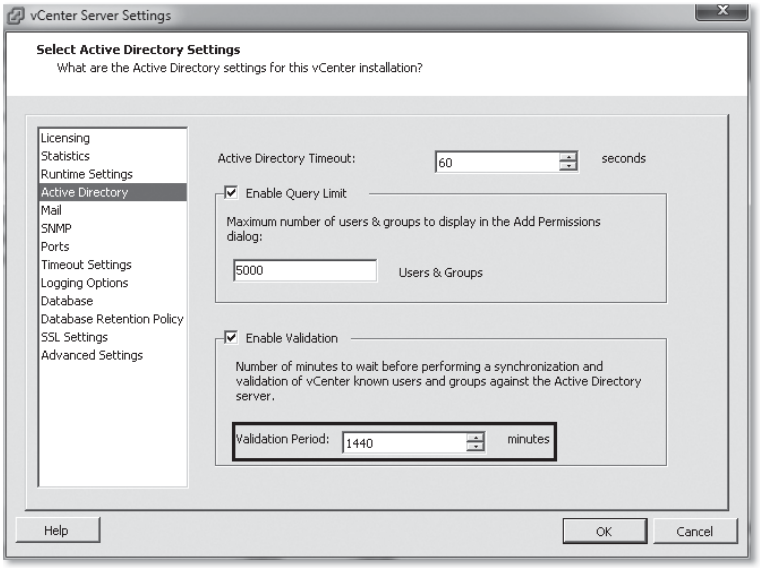


Abbildung 12.65 Berechtigungsvalidierungsintervall

Lassen Sie uns näher darauf eingehen, wie die Überprüfung der Accounts funktioniert. Wird ein vorhandener User »Meier« umbenannt in »Meier-Schmitz«, dann werden bei der nächsten Validierung die Rechte von »Meier« gelöscht, weil es den User nicht mehr gibt.

Verlässt eben dieser Herr »Meier« das Unternehmen und wird sein Account gelöscht, dann werden nach der nächsten Synchronisierung mit der Domäne alle Rechte von Herrn Meier gelöscht. Wird aber vor der nächsten Überprüfung ein Benutzer mit demselben Namen, also wieder »Meier«, neu angelegt, dann erhält der neue User die Rechte im vCenter, die der alte Benutzer schon hatte. Die Ursache für diesen Umstand liegt darin, dass das vCenter nicht die SID (Security Identifier) des ADS auswertet. Aus diesem Grund sollten Sie das Refresh-Intervall zum AD verkürzen. Ein Zeitfenster von zwei Stunden ist empfehlenswert.

12.12.3 Absicherung gegenüber dem Betriebssystem

Wie schon am Anfang des Abschnitts angedeutet, kann es ein Problem sein, dass automatisch die lokalen Administratoren auch die Administratoren im vCenter sind. Es hängt nicht unbe-

dingt von der Größe eines Unternehmens ab, wie die Betriebsaufgaben aufgeteilt werden. Die Administratoren des Betriebssystems sind nicht unbedingt auch die Personen, die die virtuelle Landschaft administrieren. Nicht selten werden die Betriebssystemadministratoren in Gruppen zusammengefasst und diese Gruppen in die lokale Gruppe der Administratoren eines jeden Servers aufgenommen. Folgerichtig sind jetzt alle Mitglieder der Gruppe auch Administratoren im vCenter.

Dieses Problem lässt sich nicht umgehen, indem Sie die Administratorengruppe vor der Installation umbenennen. Die Installationsroutine stellt das selbständig fest und verlinkt die umbenannte Gruppe mit den vCenter-Administratoren. Es gibt aber einen Weg, diesen Sachverhalt zu umgehen.

Installieren Sie zuerst das vCenter normal auf einem unterstützten System. Anschließend legen Sie nach einem Neustart des Systems eine neue Gruppe auf Betriebssystemebene an; nennen wir die Gruppe »VC-Admins«. In diese Gruppe nehmen Sie nun einen vorhandenen oder neu angelegten lokalen User auf. Alternativ wählen Sie eine Gruppe von vCenter-Administratoren aus dem Active Directory aus. Melden Sie sich jetzt mit einem User an, der Mitglied der lokalen Administratorengruppe ist.

In der Wurzel des vCenters berechtigen Sie die Gruppe »VC-Admins« mit der Rolle der Administratoren. Achten Sie darauf, dass Sie die Rechte durchpropagieren. Anschließend melden Sie sich wieder ab und melden sich neu am vCenter mit einem Benutzer aus der Gruppe der »VC-Admins« an.

Auf der obersten Ebene löschen Sie die Gruppe der Administratoren. In der Übersicht sehen Sie jetzt nur noch die neu angelegte Gruppe der »VC-Admins«.

Abbildung 12.66 Anpassung der administrativen Rechte

Es sind jetzt nur noch Anwender im vCenter berechtigt, die auch – über Gruppen oder direkt – Mitglied in der Gruppe »VC-Admins« sind. Für alle anderen Rechteebenen können Sie ebenfalls Gruppen anlegen und diese mit angemessenen Rechen versorgen.

12.13 Performancedaten des Hosts im vCenter

In der virtuellen Umgebung ist es wichtig, die Leistungsdaten der Landschaft im Auge zu behalten. Zur Überwachung der Leistungsdaten gibt es im vSphere-Client den Reiter Performance.

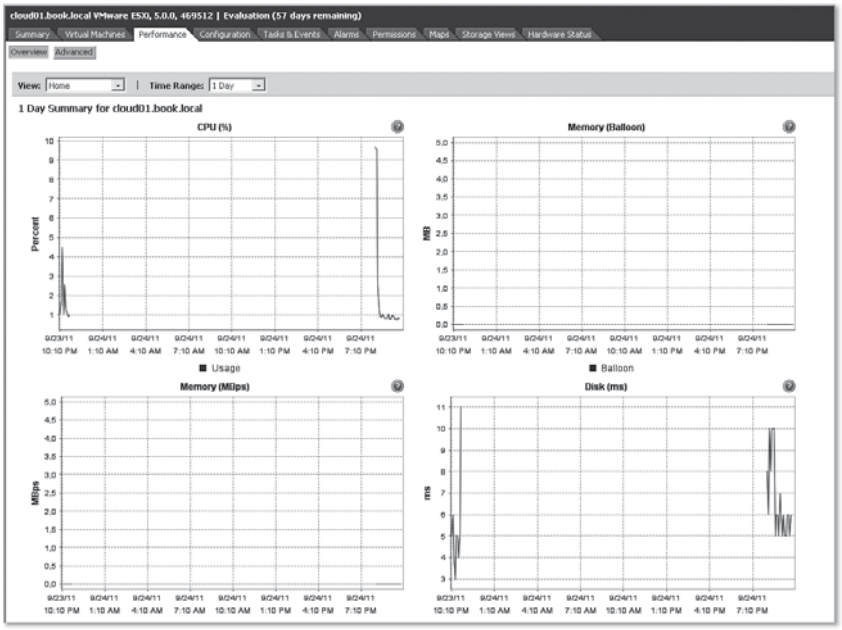


Abbildung 12.67 Performancedaten für CPU (%), Memory (MBps), Ballooning und Disk (ms)

Außer den hier dargestellten Werten gibt es noch weitere.

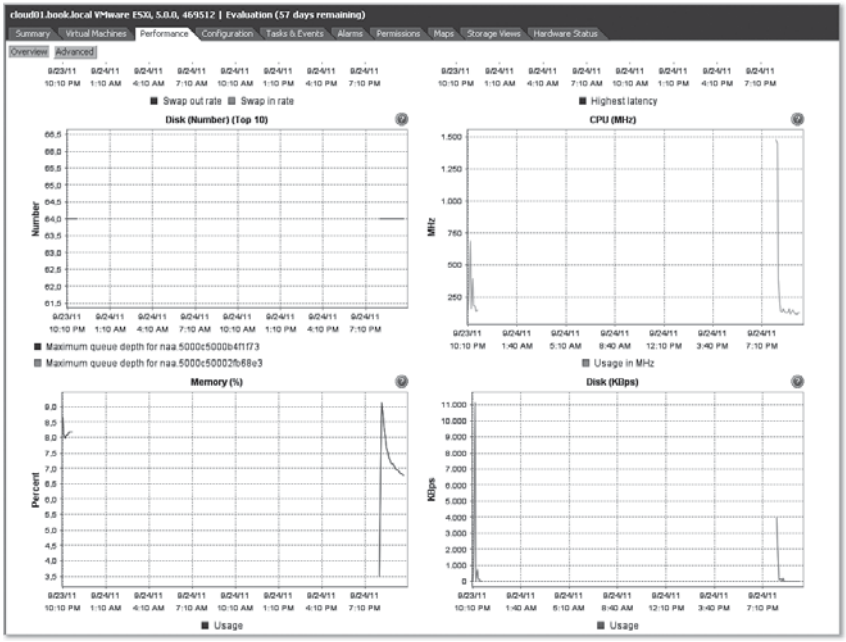


Abbildung 12.68 Performancedaten für Disk (Number), CPU (MHz), Memory (%) und Disk (KBps)

Als Letztes können Sie den Durchsatz des Netzwerks begutachten.

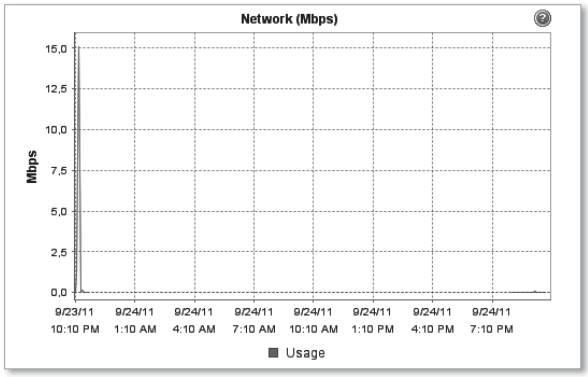


Abbildung 12.69 Performancedaten Netzwerk (MBps)

Sie können sich Leistungsdaten anzeigen lassen für das Datacenter, den Cluster, den Host, den Resource-Pool, die vApp und die virtuelle Maschine. In Tabelle 12.10 zeigen wir Ihnen, welche Diagrammoptionen wo angezeigt werden können.

Die Diagrammoptionen für die virtuelle Maschine listen wir an dieser Stelle der Vollständigkeit halber mit auf. Auf die Daten der VM gehen wir aber im Kapitel für die virtuelle Maschine (Kapitel 15, »Virtuelle Maschinen«) mit ein. Nur bei der VM sehen Sie am unteren Rand des Fensters noch eine Zusammenfassung der Diagramme in einer Zeile.

Auch hier haben sich Änderungen ergeben. Sie können sich nicht nur die Daten eines Objekts anzeigen lassen, sondern auch die Daten einiger unterliegender Objekte. Diese alternativen Objekte wählen Sie über ein Dropdown-Menü aus. Wir denken, dass an dieser Stelle die Tabelle 12.10 die übersichtlichste Form der Darstellung ist.

Ausgewähltes Objekt	Mögliche Anzeigen
Datacenter	Cluster
	Storage
Cluster	Cluster
	Resource-Pools & Virtual Machines
	Hosts
Hosts	Hosts
	Virtual Machines
vApp	vApp
Resource-Pools	Resource-Pools
Virtual Machine	Virtual Machine
	Storage

Tabelle 12.10 Performanceansichten

Sie müssen an dieser Stelle unterscheiden, ob Sie eine Echtzeitdarstellung möchten oder ob Sie ein längerfristiges Intervall betrachten wollen. Echtzeitdarstellungen sind nur beim Host und bei der VM möglich. Tabelle 12.11 zeigt die Optionen für die Echtzeitbeobachtung.

Diagrammoptionen	Beschreibung
Host	CPU (%)
	CPU (MHz)
	Memory (MB)
	Memory (MBps)
	Memory (%)
	Disk (ms)
	Disk (number) (Top 10)
	Disk Rate (KBps) (Top 10)
	Disk Requests (number) (Top 10)
	Network Rate (MBps) (Top 10)
	Network Packets (MBps) (Top 10)
VM	CPU (%)
	CPU Usage (MHz)
	Memory (MB)
	Memory (MBps)
	Memory (%)
	Disk (KBps)
	Network (MBps)

Tabelle 12.11 Echtzeit-Performancedaten

In Tabelle 12.12 finden Sie die Werte für die Langzeitüberwachung, die Sie in der Performancebetrachtung einsehen können.

Diagrammoptionen	Beschreibung
Datacenter	CPU (MHz) (Top 10)
	Memory (MB) (Top 10)
Cluster	CPU (MHz)
	Memory (MB)
Host	CPU (%)
	CPU (MHz)
	Memory (MB)
	Memory (MBps)
	Memory (%)

Tabelle 12.12 Langzeit-Performancedaten

Diagrammoptionen	Beschreibung
Host (Forts.)	Disk (ms)
	Disk (number) (Top 10)
	Disk Rate (KBps) (Top 10)
	Disk Requests (number) (Top 10)
	Network Rate (MBps) (Top 10)
	Network Packets (MBps) (Top 10)
VM	CPU (%)
	CPU Usage (Mhz)
	Memory (MB)
	Memory (MBps)
	Memory (%)
	Disk (KBps)
	Network (MBps)

Tabelle 12.12 Langzeit-Performancedaten (Forts.)

Bevor wir uns der Advanced-Ansicht zuwenden, möchten wir Ihnen noch zeigen, wie Sie die Overview-Ansicht noch beeinflussen können. Im zweiten Dropdown-Menü können Sie den zu betrachtenden Zeitraum auswählen. Neben den vorbesetzten Werten Realtime, 1 Day, 2 Days, 3 Days und 4 Days können Sie eine Custom-Ansicht wählen, bei der das Intervall frei einstellbar ist.

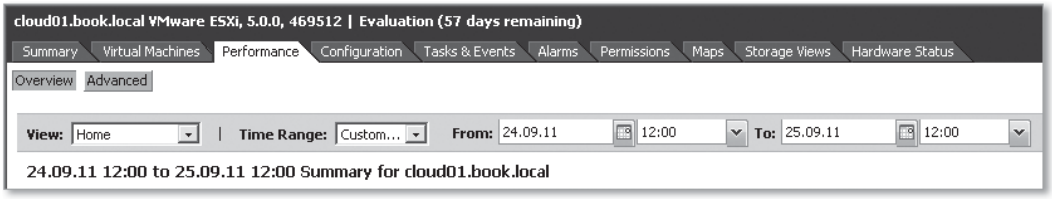


Abbildung 12.70 Einstellung des Betrachtungszeitraums

Wechseln wir nun zu der Advanced-Ansicht. An dieser Stelle können Sie weitere Metriken anzeigen lassen, um die globalen Werte besser beurteilen zu können.

Für jede aufgelistete Diagrammoption gibt es weitere Unterpunkte. So können Sie die zu beobachteten Objekte auswählen und die passenden Leistungsindikatoren aktivieren. Es wäre müßig, alle Permutationen für alle Punkte aufzuzählen. Sollten Sie die nötigen Informationen benötigen, möchten wir an dieser Stelle auf die VMware-Dokumentationen verweisen.

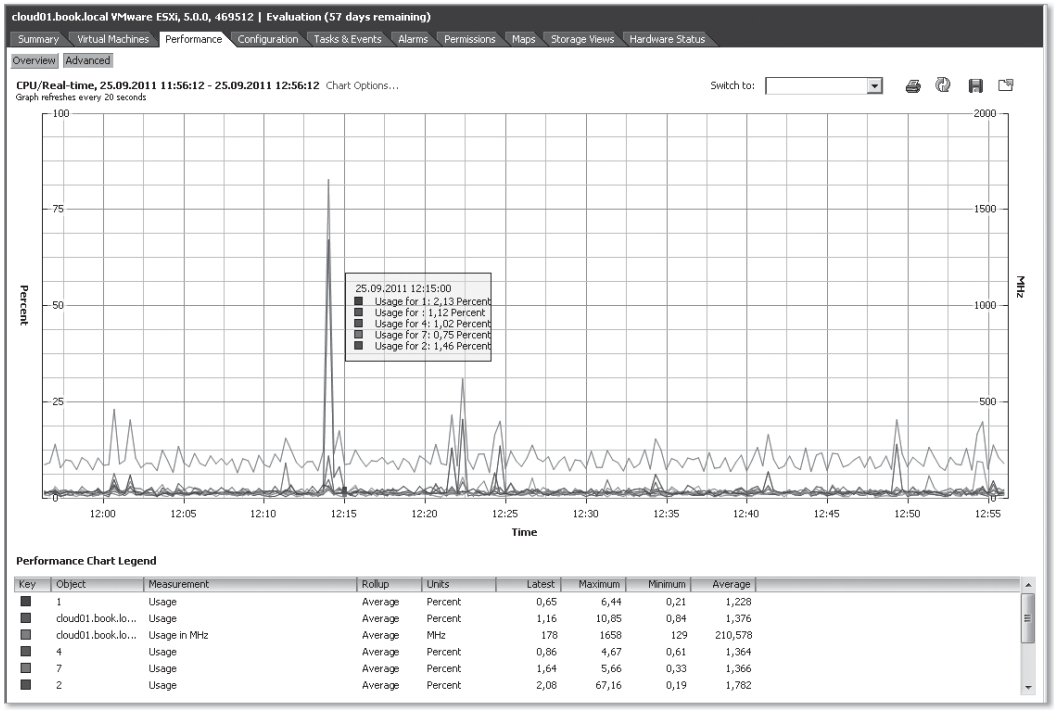


Abbildung 12.71 Übersicht des »Performance«-Views

Das Fenster gliedert sich in zwei große Abschnitte. Im oberen Abschnitt sehen Sie die grafische Darstellung der ausgewerteten Performancedaten. In dem unteren Drittel wird Ihnen angezeigt, welche Daten zur Darstellung kommen. Jedem Parameter ist ein farbiges Kästchen vorangestellt, das die Farbe des zugehörigen Diagrammelements zeigt. Wandern Sie mit der Maus über das Diagramm. Es wird ein kleines Übersichtsfenster eingeblendet, das Ihnen nähere Informationen über den ausgewählten Zeitpunkt gibt. Außer Datum und Uhrzeit sehen Sie die Werte des Zeitpunkts. Dabei werden der Farbcode des Parameters, die Beschreibung und der absolute Wert angezeigt.

Oben auf der rechten Seite haben Sie fünf Auswahlmöglichkeiten. Im Dropdown-Menü wählen Sie eines von mehreren Diagrammen aus. Die folgenden drei Symbole sprechen für sich selbst – Ausdrucken, Aktualisieren und Abspeichern des Diagramms ist dort möglich. Durch Klick auf das Symbol ganz rechts in der Zeile wird die Anzeige in einem eigenständigen Fenster geöffnet. Bis hier wurden die Auswertungen genutzt, die VMware in der Standardeinstellung zur Verfügung stellt. Sind für Sie auch andere Kombinationen von Messwerten interessant, gelangen Sie über den Link Chart Options in ein Fenster zur Anpassung der Anzeige (Abbildung 12.72).

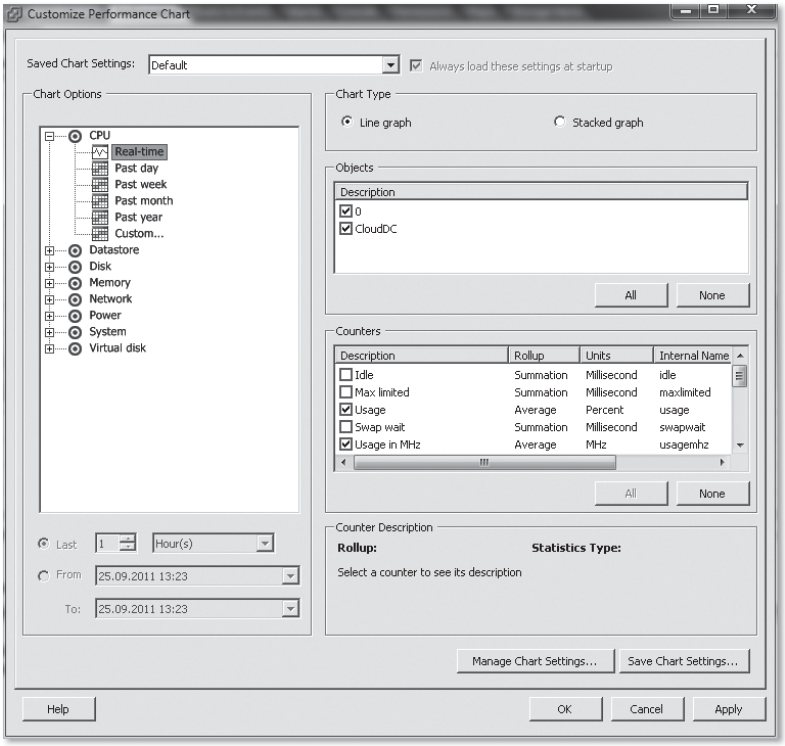


Abbildung 12.72 Anpassung der Diagrammanzeige

Auf der linken Seite des Fensters wählen Sie den anzuzeigenden Parameter und das gewünschte Zeitintervall aus. Die Beschriftung der Auswahl ist eigentlich eindeutig. Nutzen Sie die CUSTOM-Auswahl, dann ist unten links das Zeitintervall individuell einstellbar.

Auf der rechten Seite setzen Sie dann die Objekte und die zugehörigen Counter. Ihre selbsterstellten Ansichten lassen sich über den Button unten rechts abspeichern und anschließend über MANAGE CHART SETTINGS anzeigen oder löschen. Alle gespeicherten Einstellungen können Sie später unter ihrem Namen auch direkt im PERFORMANCE-Fenster aufrufen.

Performance-Messwerte

Wie Sie sich die verschiedenen Messwerte anzeigen lassen, haben wir erläutert. Nun stellt sich die Frage, wie Sie mit den angezeigten Messwerten umgehen. In diesem Abschnitt wollen wir nur auf einige Werte, die den Host betreffen, eingehen. In Kapitel 15, »Virtuelle Maschinen«, werden wir die Auswertung der VM-Performancedaten gesondert erläutern.

CPU-Performance

Als Erstes betrachten wir die Messwerte für die durchschnittliche CPU-Last des Hosts. Liegt diese im Durchschnitt nicht über 75 % und treten nicht häufig Spitzen von über 90 % auf,

dann müssen Sie sich keine Gedanken machen. Falls die Schwellenwerte überschritten werden, müssen Sie kontrollieren, ob die Host-CPU in die Sättigung geht. Dazu überprüfen Sie die CPU Ready-Werte aller auf dem betroffenen Host liegenden virtuellen Maschinen. Überschreitet ein Wert 20.000 ms, dann läuft die CPU zeitweise in der Sättigung. Dadurch werden durchaus auch andere VMs beeinflusst. Können Sie das Problem durch die Performanceauswertung mit einer VM assoziieren, dann sollten Sie sich näher mit dieser VM beschäftigen. Ein einfacher Weg ist an dieser Stelle, die Anzahl der Host-CPUs zu erweitern oder die Anzahl der virtuellen Maschinen zu verringern. Alternativ machen Sie den Host zum Mitglied eines DRS-Clusters; so kann die VM bei höherem Ressourcenbedarf verschoben werden.

Der bessere Weg ist aber, sich mit den VMs näher zu beschäftigen, die die Probleme verursachen.

Memory-Performance

Welches sind nun die Punkte, die Sie beim Arbeitsspeicher berücksichtigen müssen? Wie schon in Kapitel 2, »vSphere-Architektur«, beschrieben, erlaubt VMware, mehr Arbeitsspeicher an virtuelle Maschinen zu vergeben, als physisch verbaut ist. Mit dem Ballooning wird dieser Speicher zurückgefordert. Kann nicht genügend Speicher akquiriert werden, muss geswappt werden. Das sind die Werte, die auch bei den Performanceauswertungen wichtig sind. Hinzu kommt der Wert Shared bzw. Shared Common. Der letztere Wert zeigt die Größe des Bereichs an, in dem alle virtuellen Maschinen ihre gemeinsamen Speicherseiten ablegen. In Shared findet sich die Summe an Speicher wieder, die durch das Page-Sharing eingespart wurde.

Der Wert swap used deklariert die Speichermenge, die ins File-System des Hosts geswappt wird. Je stärker das System Speicher auf die Festplatte auslagert, desto stärker leidet die Performance. Balloon zeigt an, wie viel Speicher aktuell von dem `vmmemctl`-Treiber aus den VMware Tools genutzt wird. Hier sehen Sie nur dann Daten, wenn Sie mit Memory-Overcommitment arbeiten.

Storage-Performance

Die Punkte, die Sie berücksichtigen müssen, damit die Anbindung an den Storage performant ist, und was Sie tun müssen, damit das auch so bleibt, lesen Sie in Kapitel 9, 10 und 11.

Die Performancewerte des Storages können Sie am besten über die Auswertetools des Storages anzeigen und messen. Diese Werte zeigen aber die Gesamtperformance an aller angeschlossenen Server an, nicht nur von den VMware-Systemen.

Über das Performance-Chart und die Werte Read Latency und Write Latency wird sichtbar, wie lange die Abarbeitung der Lese- bzw. Schreibzyklen dauert. Der Usage-Wert ist bei System mit mehreren unterschiedlichen Storage-Anbindungen nicht ganz so aussagekräftig. Die Anzeige erfolgt nur für den gesamten Host und nicht für die einzelne LUN oder den einzelnen Storage.

Network-Performance

Hier sehen Sie, wie der Durchsatz auf den Netzwerkschnittstellen ist. Über USAGE wird angezeigt, welche Datenmengen über die einzelnen Adapter fließen. Dieser Wert hilft zu erkennen, ob die Anbindung der Komponenten ausreichend ist oder ob die Bandbreite erhöht werden muss. Sollte der Durchsatz an die Grenze gehen – das ist schön dadurch zu sehen, dass sich im oberen Bereich eine gerade Linie zeigt –, dann ist zu kontrollieren, ob und wann dieses Phänomen auftritt. Erst nach einer solchen Analyse sind Gegenmaßnahmen möglich, z. B. eine Erhöhung der Bandbreite. Solche Werte können aber auch entstehen, weil gerade besondere einmalige Aktionen im Netzwerk durchgeführt werden.

Bei der Auswertung der Datenbandbreite müssen Sie berücksichtigen, dass der praktische maximale Durchsatz nie die theoretische Grenze erreicht. Über die Parameter DROPPEDRX und DROPPEDTX lassen sich die verlorenen Pakete darstellen. Diese Werte sind bei öfter auftretenden Übertragungsfehlern hilfreich.

12.14 Weitere Funktionen des vCenters

In diesem Abschnitt möchten wir die vCenter-Funktionen erläutern, auf die wir bis jetzt noch nicht eingegangen sind.

Lassen Sie uns Ihnen noch einen kleinen Hinweis geben: Die Suchfunktion, die immer oben rechts im vCenter-Fenster zu sehen ist, ist sehr umfangreich und komplex, bringt Sie aber sehr schnell ans Ziel.

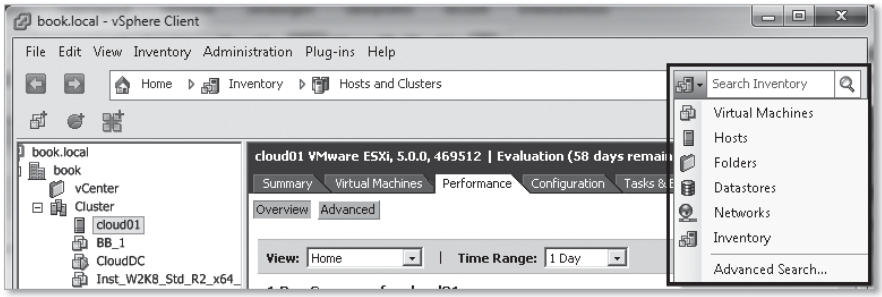


Abbildung 12.73 Suche im vCenter-Server

Sie können direkt angeben, in welchen Ansichten gesucht werden soll. Die Suche lässt sich sehr granular durchführen, wenn Sie die ADVANCED SEARCH…-Auswahl nutzen.

Es lassen sich verschiedenste Verschachtelungen bei der Suche durchführen, um das gewünschte Ergebnis zu erhalten. Diese Funktion wird aus unserer Sicht aber erst bei größeren Umgebungen oder verlinkten vCenter-Servern interessant.

Kommen wir zu den offenen Anzeige- und Konfigurationsmöglichkeiten beim vCenter-Server.

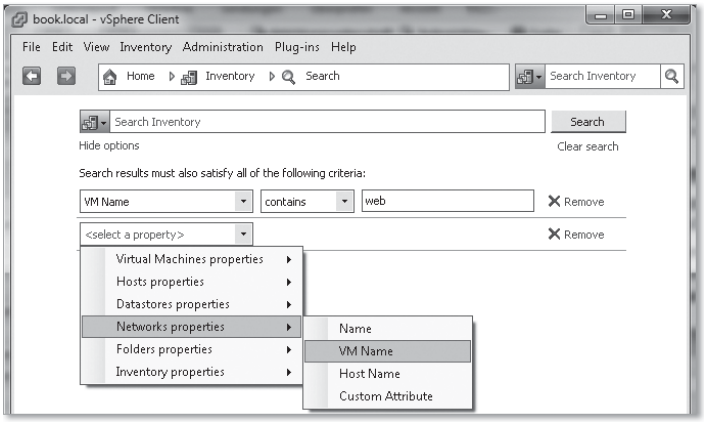


Abbildung 12.74 Detaillierte Suche im vCenter

12.14.1 IP-Pools

Das Datacenter-Objekt bietet einen neuen Reiter; er ist mit IP Pools bezeichnet. In diesem Konfigurationsfenster können Sie IP-Bereiche anlegen, die genutzt werden, um vApps mit passenden Adressen zu versorgen.

Wichtig

Es handelt sich nicht um einen integrierten DHCP-Server, sondern lediglich um eine Reservierung von Adressen für vApps.

Betätigen Sie einfach den Link Add oben am.

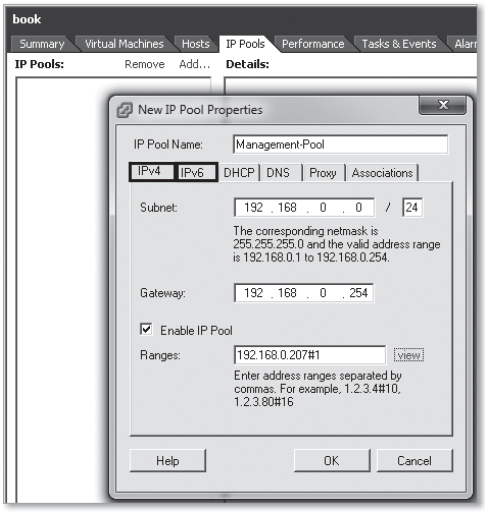


Abbildung 12.75 Anlegen von IP-Pools

Dieser Dialog gibt Ihnen die Möglichkeit, IP-Pools anzulegen. Dabei werden sowohl IPv4- als auch IPv6-Adressen unterstützt. Geben Sie das Subnetz, die Netzmaske (steht neben dem Subnetz), das Gateway und den Adressbereich (RANGES) ein. Unter RANGES geben Sie die Adressen an, die für vApps genutzt werden sollen. Hinter dem Reiter DHCP können Sie dem System einen vorhandenen DHCP-Server melden. Es folgt die Angabe der DNS-Parameter.

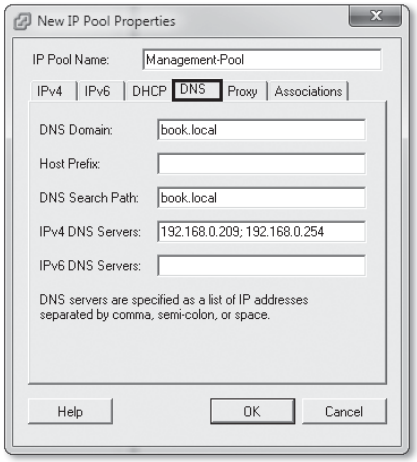


Abbildung 12.76 DNS Parameter des IP-Pools

Auch hier sehen Sie, dass zwischen IPv4 und IPv6 unterschieden wird. Der nächste Reiter nimmt die PROXY-Konfiguration auf in der Form <PROXY-SERVER>:<IP-PORT>. Abgeschlossen wird das Anlegen des IP-Pools mit der Zuweisung eines LAN zum Pool.

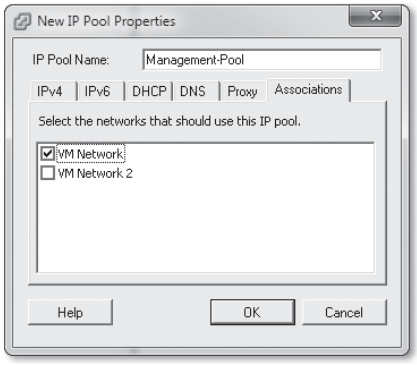


Abbildung 12.77 Verbinden des Pools mit dem Netzwerk

Nach dem Abschluss der Arbeiten können Sie mit virtuellen Apps und Appliances arbeiten, die IP-Pool-Funktion nutzen.

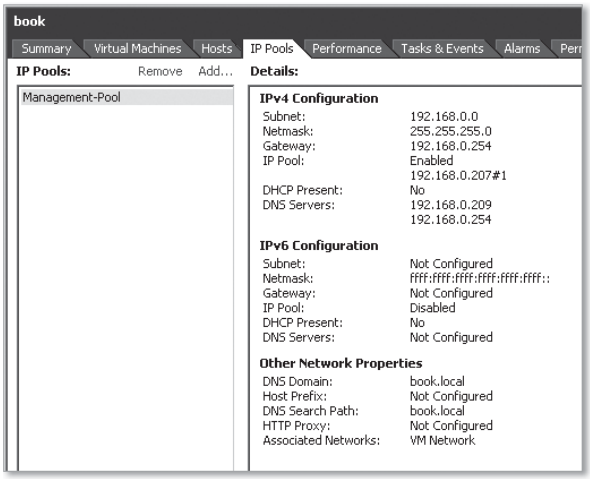


Abbildung 12.78 IP-Pool-Zusammenfassung

12.14.2 Storage Views

Der Reiter Storage Views (Speicheransichten) gibt Ihnen ausführlich Auskunft über – wie sollte es anders sein – den Storage, aber nicht nur. Es werden die Zusammenhänge der Komponenten untereinander angezeigt. Der Reiter steht Ihnen zur Verfügung bei den Objekten Datacenter, Cluster, Host und VM. Sie können sich aber nicht nur grafisch die Zusammenhänge darstellen lassen; der Button Report gibt Ihnen die Informationen in Listenform aus.

In Abbildung 12.79 sehen Sie, dass alle Informationen angezeigt werden, die den Administrator interessieren. Der freie und belegte Plattenplatz wird genauso gelistet wie die Belegung durch Snapshots und die Anzahl der virtuellen Festplatten-Files. Abbildung 12.80 zeigt, welche zusätzlichen Anzeigemöglichkeiten Sie haben.

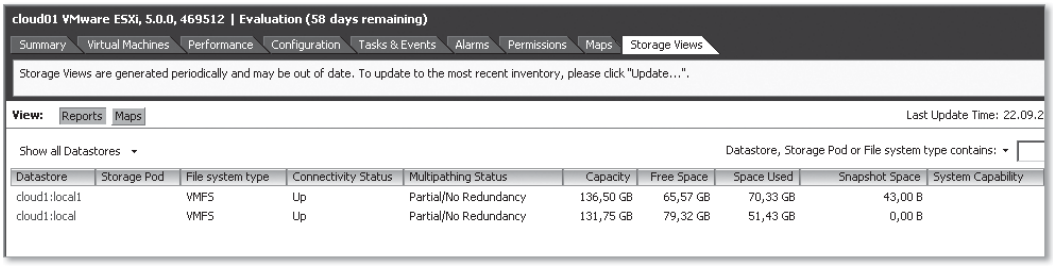


Abbildung 12.79 Auflistung der Datastores eines Hosts

Genügen Ihnen diese Informationen nicht, dann passen Sie die Ansicht für Ihren Informationsgrad an, indem Sie einfach die Ausgabe entsprechend ändern (Abbildung 12.81).

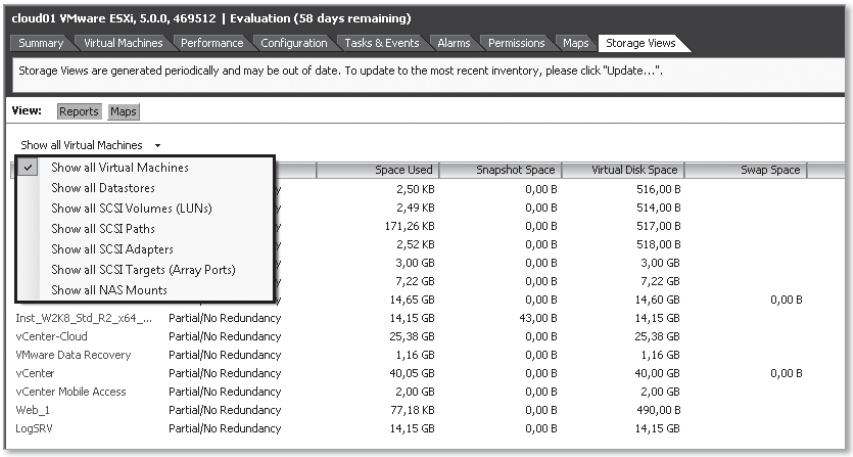


Abbildung 12.80 Anzeigemöglichkeiten

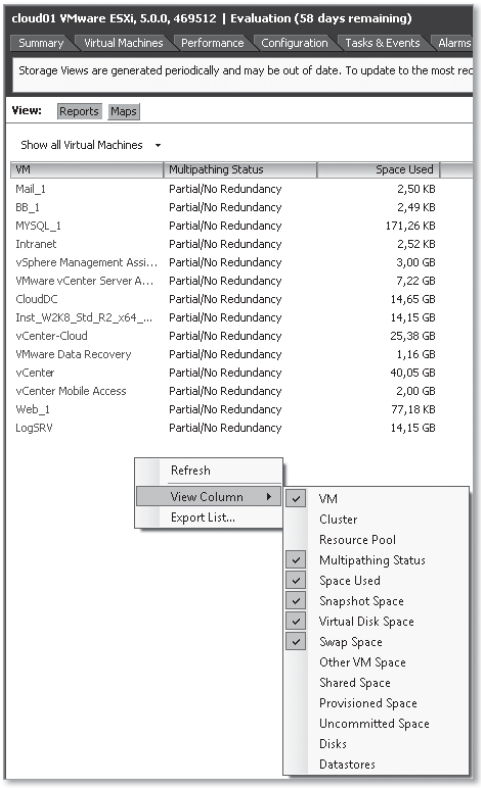
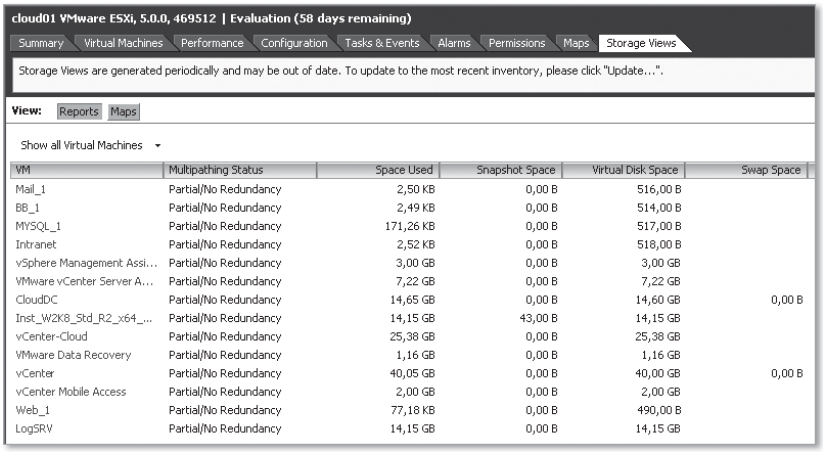


Abbildung 12.81 Anpassung der Ansichten

Alternativ können Sie aber auch andere Sichtweisen, wie z. B. aus der virtuellen Maschine, wählen und so sehen, wie der Storage dort angebunden ist (Abbildung 12.82).



VM	Multipathing Status	Space Used	Snapshot Space	Virtual Disk Space	Swap Space
Mail_1	Partial/No Redundancy	2,50 KB	0,00 B	516,00 B	
BB_1	Partial/No Redundancy	2,49 KB	0,00 B	514,00 B	
MYSQL_1	Partial/No Redundancy	171,26 KB	0,00 B	517,00 B	
Intranet	Partial/No Redundancy	2,52 KB	0,00 B	518,00 B	
vSphere Management Assi...	Partial/No Redundancy	3,00 GB	0,00 B	3,00 GB	
VMware vCenter Server A...	Partial/No Redundancy	7,22 GB	0,00 B	7,22 GB	
CloudDC	Partial/No Redundancy	14,65 GB	0,00 B	14,60 GB	0,00 B
Inst_W2K8_Std_R2_x64_...	Partial/No Redundancy	14,15 GB	43,00 B	14,15 GB	
vCenter-Cloud	Partial/No Redundancy	25,38 GB	0,00 B	25,38 GB	
VMware Data Recovery	Partial/No Redundancy	1,16 GB	0,00 B	1,16 GB	
vCenter	Partial/No Redundancy	40,05 GB	0,00 B	40,00 GB	0,00 B
vCenter Mobile Access	Partial/No Redundancy	2,00 GB	0,00 B	2,00 GB	
Web_1	Partial/No Redundancy	77,18 KB	0,00 B	490,00 B	
LogSRV	Partial/No Redundancy	14,15 GB	0,00 B	14,15 GB	

Abbildung 12.82 Storage-Ansicht der virtuellen Maschinen

Auch hier finden Sie alle Informationen, die mit dem Storage und der Anbindung der VM zu tun haben. Sollten Ihnen aber Tabellen nicht gefallen oder benötigen Sie eine management-ähnliche Ansicht, kein Problem – nutzen Sie doch einfach die Kartenansicht der Daten.

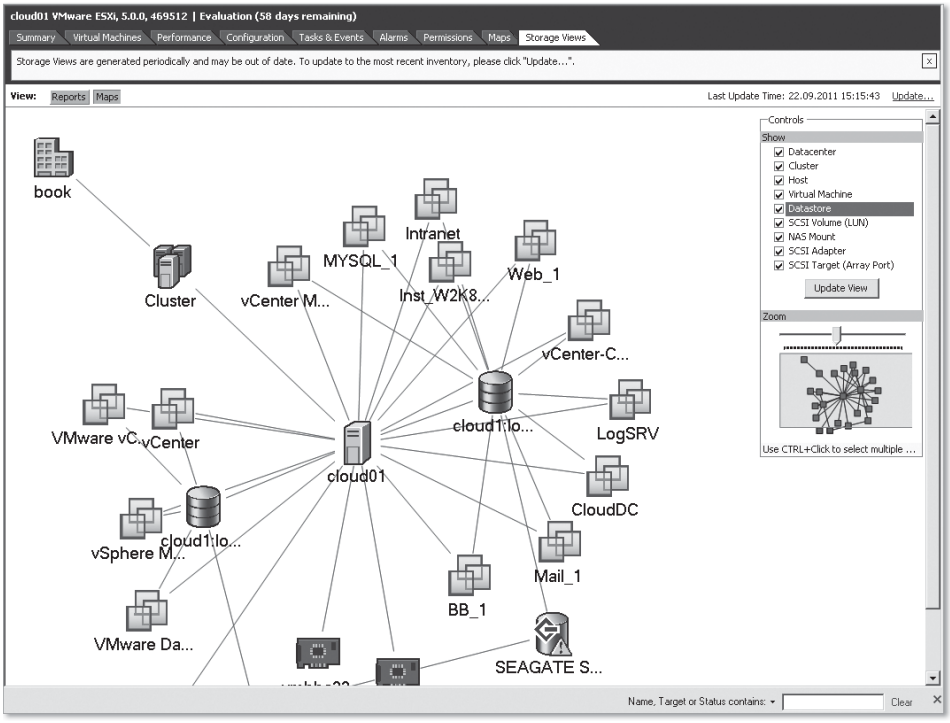


Abbildung 12.83 Grafische Ansicht der Anbindung

Alternativ füllen Sie mit den Daten eine Grafik, die Ihnen eine globale Übersicht der Zusammenhänge darstellt. Die anzuzeigenden Komponenten wählen Sie oben rechts aus. In dem Fenstersegment unterhalb stellen Sie den Zoom-Faktor ein. Die Darstellung umfasst den gesamten Weg, vom Host bis zum Storage. Die Anzahl der Pfade ist genauso sichtbar wie die Netzwerkkarte, über die der iSCSI-Storage angesprochen wird. Die Adressen sind ebenfalls eingeblendet. Auch wenn hier die Karte aus Sicht des Hosts dargestellt wird, ist es selbstverständlich auch möglich, den Standpunkt zu wechseln und die Sicht der VM einzunehmen.

12.14.3 Maps

Im Gegensatz zu den Storage Views ist die Auswahl des Reiters Maps an allen Objekten möglich. Sehen Sie eine solche Übersicht, fällt Ihnen sofort die Ähnlichkeit zu den Storage Views auf. Einen Unterschied gibt es schon: Das Zoom-Fenster und die Auswahl sind vertauscht. Sonst ist die gesamte Funktionalität identisch, zeigt aber zusätzliche Komponenten an.

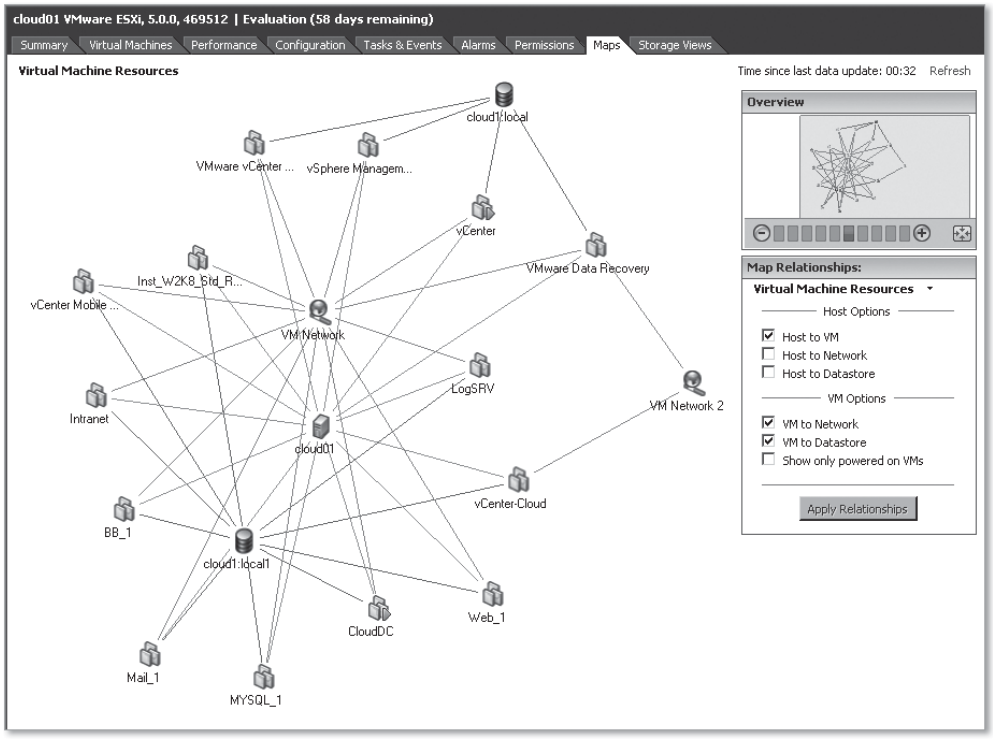


Abbildung 12.84 Die grafische Übersicht der virtuellen Landschaft

Bei unserer relativ kleinen Testlandschaft ist das Bild schon sehr unübersichtlich, wenn man alle Verbindungen anzeigen lässt. Weniger ist auch an dieser Stelle mehr. Überlegen Sie genau, auf welchem Objekt Sie die Ansichten wählen und welche Objekte Sie anzeigen lassen wollen.

12.14.4 Events

Besteht die Notwendigkeit, einmal zu einem späteren Zeitpunkt nachzuvollziehen, wann welche Aktion lief und wie sie abgeschlossen wurde, dann finden Sie die Information unter dem Menüpunkt VIEW • MANAGEMENT • EVENT.

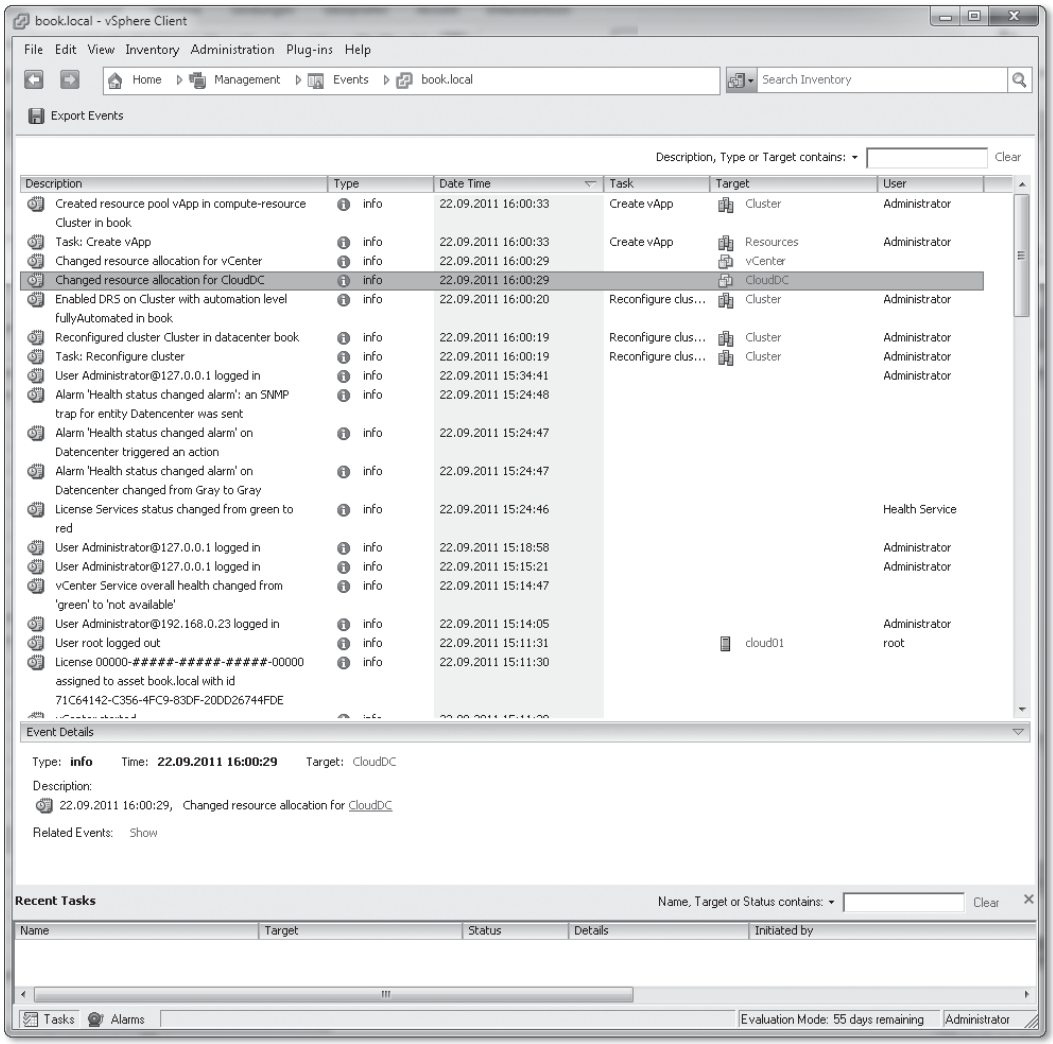


Abbildung 12.85 Anzeige der Events im vCenter

Im Hauptfenster des Clients werden zwar alle Ereignisse angezeigt, doch die Anzeige wird nach relativ kurzer Zeit wieder gelöscht. Damit sind die Informationen aber nicht verloren – im Eventfenster können Sie sich alles noch einmal anschauen. Damit bei der Menge der Ereignisse die Forschungen zeitlich nicht ausufern, ist oben eine Suchfunktion implementiert, über die Sie detailliert das Log durchsuchen können.

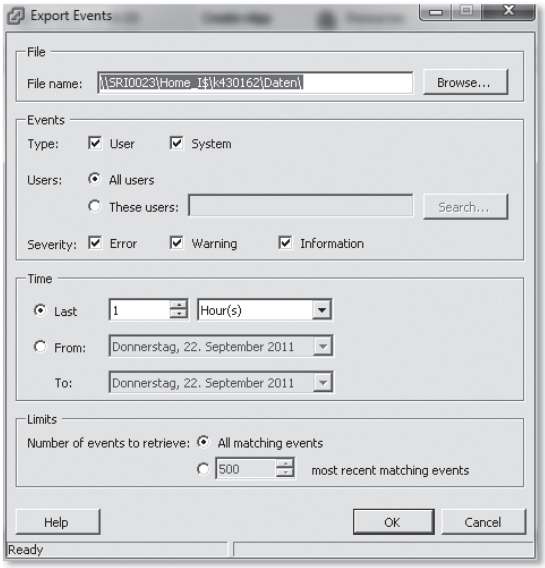


Abbildung 12.86 Export von Ereignissen

Bei Bedarf exportieren Sie über Export Events eine definierte Menge von Ereignissen. Die Auswahlmöglichkeiten sind sehr granular: Die Daten lassen sich getrennt nach System oder. Anwender und aufgeschlüsselt nach Fehlern, Informationen und Warnungen speichern. Dabei ist es sowohl möglich, nur die Daten aus einem bestimmten Zeitintervall zu inkludieren, als auch eine definierte Anzahl von Ereignissen auszuwählen.

12.14.5 Scheduled Tasks

Über den Menüpunkt View • Management • Scheduled Task gelangen Sie zu einer Liste mit allen Aktionen, die automatisch in der virtuellen Infrastruktur ablaufen. Als zusätzliche Information werden die letzte Ausführung und die nächste Fälligkeit der entsprechenden Aktion angezeigt.

In diesem Fenster können Sie auch neue Tasks anlegen. Mit den Buttons New, Properties und Remove manipulieren Sie die Tasks in diesem Fenster. Die Bezeichnung der einzelnen Schaltflächen lassen keine Fragen offen, deshalb möchten wir nur auf den New-Button eingehen. Klicken Sie darauf, öffnet sich ein Eingabefenster, über das Sie einen neuen Task erstellen.

VMware gibt eine Reihe von Möglichkeiten für die Neuerstellung von Tasks vor. Eigene Tasks können Sie nicht kreieren.

Hier die Liste der möglichen Tasks:

- Change the power state of a virtual machine
- Clone a virtual machine

- Deploy a virtual machine
- Migrate a virtual machine
- Create a virtual machine
- Create a snapshot of a virtual machine
- Add a host
- Change Cluster Power Settings
- Change Resource Pool or VM Resource Settings
- Check compliance of a profile

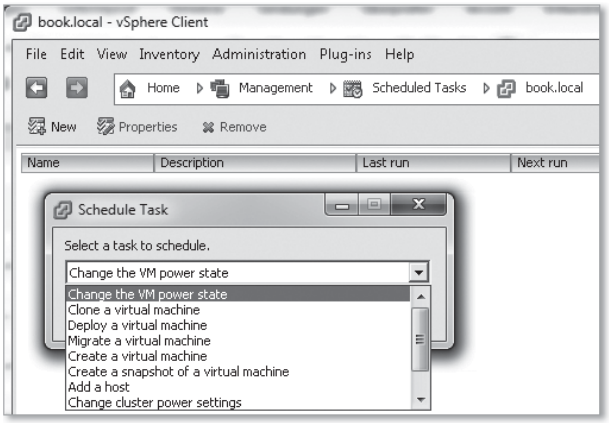


Abbildung 12.87 Erstellen eines neuen Tasks

Je nach Auswahl des Tasks öffnet sich ein entsprechendes Fenster, das die benötigten Informationen zur späteren Ausführung sammelt.

12.14.6 System-Logs

Ein weiterer sehr wichtiger Punkt ist die Auswertung von Log-Dateien beim vCenter-Server. Auf diese Funktion sind Sie angewiesen, wenn es Unregelmäßigkeiten gibt. Dabei ist es unerheblich, ob Sie selbst nähere Informationen suchen oder ob ein Supporter Informationen aus der virtuellen Landschaft benötigt. Zu dem Fenster gelangen Sie über View • Administration • System Logs. Abbildung 12.88 zeigt Ihnen die Ansicht.

Hier können Sie das zu betrachtende Log auswählen. Die Schaltflächen in der oberen Reihe sprechen für sich. Auch hier gibt es eine Suchfunktion, die sehr hilfreich ist, wenn Sie größere Log-Dateien durchsuchen müssen. Ist es notwendig, für eine Fehlerauswertung ein aktuelles definiertes Log zu ziehen, dann stoßen Sie den Vorgang über den Link oben links an (Abbildung 12.89).

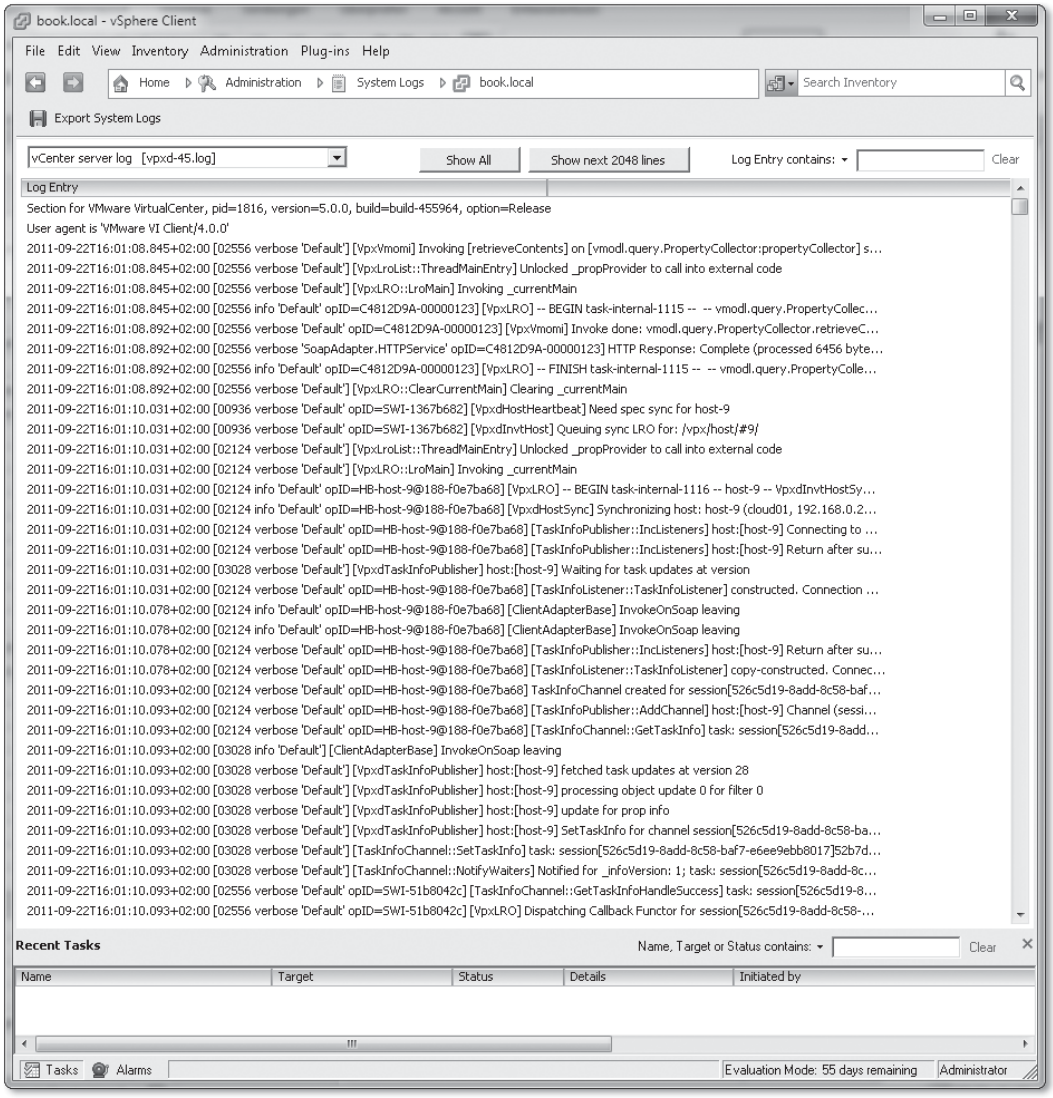


Abbildung 12.88 Anzeige der Log-Dateien

Haben Sie im ersten Schritt das Datacenter, den Cluster und/oder die passenden Hosts ausgewählt, so können Sie im zweiten Schritt die gewünschten Daten näher spezifizieren. Vergessen Sie aber nicht, die entsprechende Option Include information from vCenter Server and vSphere Client zu aktivieren, wenn das vCenter und der Client einbezogen werden sollen.

Auch die Performancedaten können Sie einbeziehen. Im letzten Schritt wählen Sie den Speicherort für das exportierte Log. Die Datei können Sie direkt auswerten oder dem Support übermitteln.

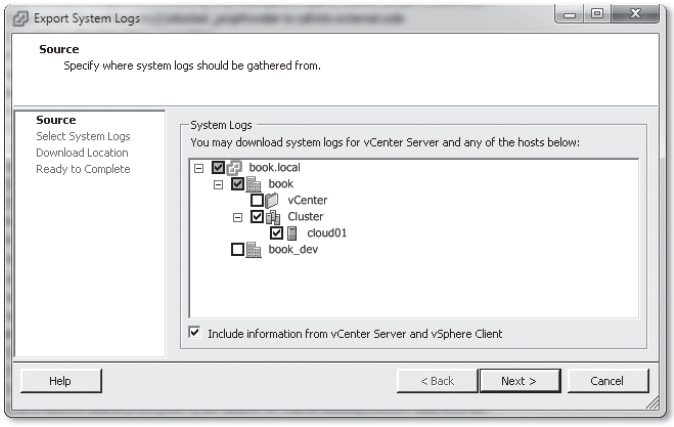


Abbildung 12.89 Export von Log-Dateien

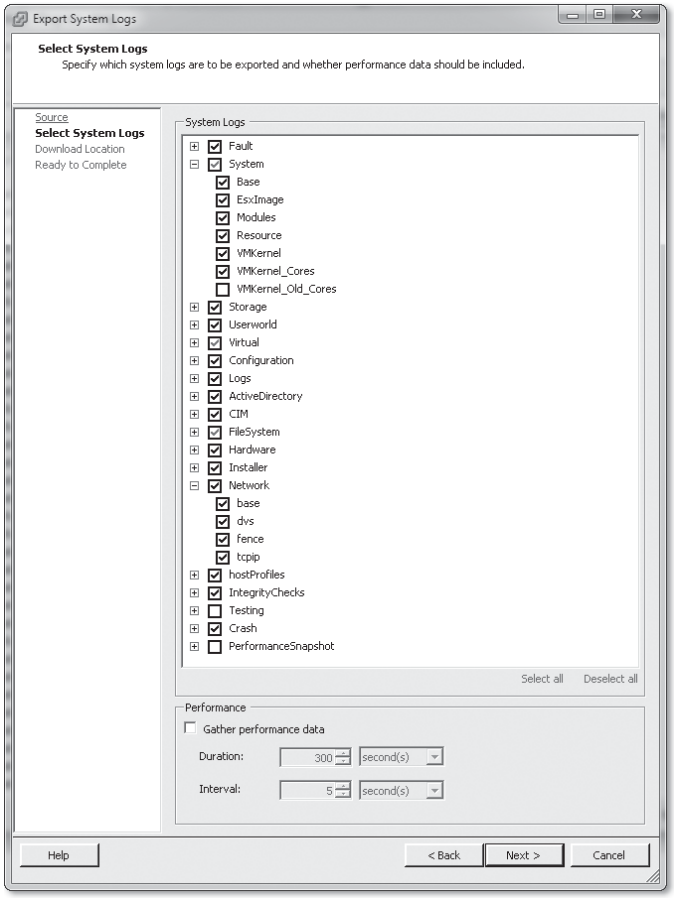


Abbildung 12.90 Auswahl der zu sammelnden Log-Dateien

12.14.7 Sessions

Für den vCenter-Administrator ist es wichtig zu sehen, welche User sich am vCenter angemeldet haben. Die Frage, wie lange einzelne Anwender angemeldet sind, ohne etwas gemacht zu haben, wird ebenfalls beantwortet. Über VIEW • ADMINISTRATION • SESSIONS gelangen Sie zum Ziel (Abbildung 12.91).

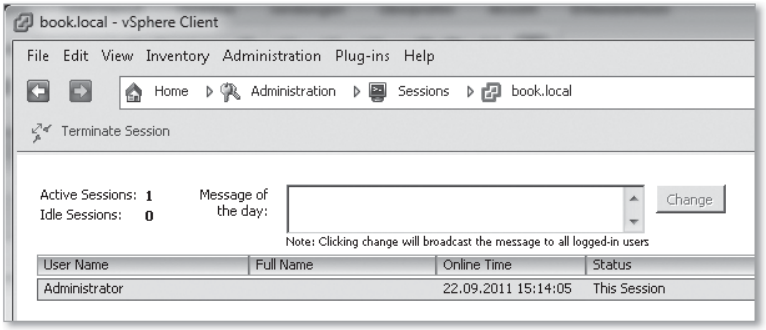


Abbildung 12.91 Verbindungen der Anwender zum vCenter

Außerdem sehen Sie sofort, wenn User doppelt angemeldet sind. Zur Ansicht kommen der Anwendername, die Anmeldezeit und der Status der Sitzung. Zusätzlich gibt es die Möglichkeit, einen »Tip of the Day« einzustellen. Dieser eignet sich besonders dafür, Wartungsarbeiten anzukündigen oder Ähnliches. Erstellen können Sie diese Nachricht über den Menüpunkt ADMINISTRATION • EDIT • MESSAGE OF THE DAY ...

12.14.8 vCenter Server Settings

In die Einstellungen des vCenter-Servers gelangen Sie auf zwei mögliche Arten: Entweder gehen Sie über die Homepage und rufen das Icon • VCENTER SERVER SETTINGS auf, oder Sie gehen den Weg über das Menü ADMINISTRATION • VCENTER SERVER SETTINGS Zu den verschiedenen Einstellungen selbst kommen wir in Abschnitt 12.15.

12.14.9 vCenter Solutions Manager

Der vCenter Solutions Manager ist eine neue Funktion, die mit vSphere 5 dazu gekommen. Es ist ja weithin bekannt, dass es die Option gibt, das vCenter um Funktionen zu erweitern. VMware macht es letztendlich auch mit einigen seiner Zusatzprodukte, wie z. B. dem Update Manager. Die installierte Applikation bindet sich direkt in das vCenter ein und stellt weitere Funktionen zur Verfügung. Unter Umständen wird das Kontextmenü um Funktionen erweitert, es tauschen neue Reiter in der Übersicht auf oder Ähnliches. Im Solutions Manager wird diese Verbindung von Applikationen mit dem vCenter nun sichtbar.

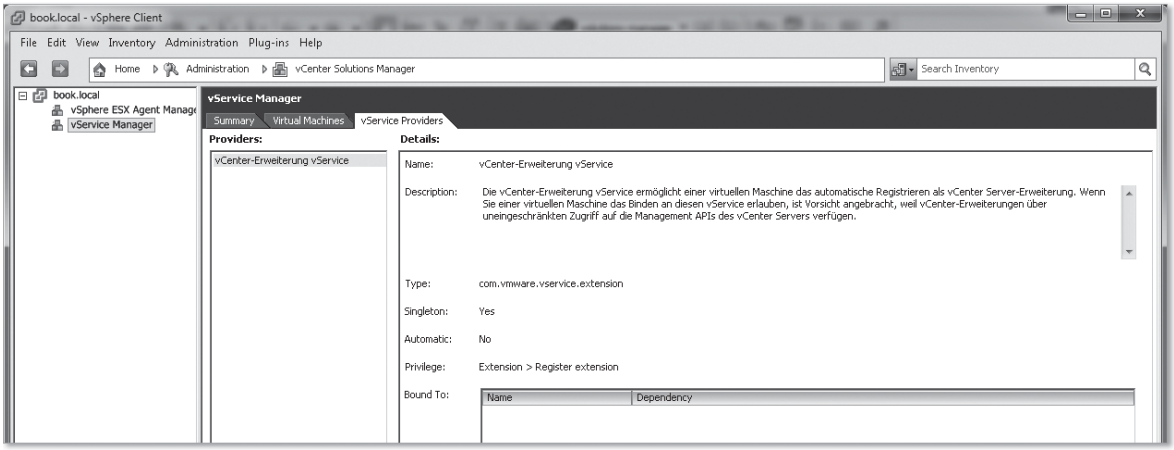


Abbildung 12.92 vCenter Solutions Manager

In Abbildung 12.92 sehen Sie die zwei Standard-Solutions, die in jedem vCenter zu finden sind: Das sind der vSphere ESX Agent Manager, der sich um das Handling der Host-Agents kümmert, und der vService Manager, der für das Management der Verbindungen zwischen einer VM und einer vCenter Erweiterung zuständig ist. Die VMs, die solche Dienste zur Verfügung stellen, finden Sie unter dem Reiter VIRTUAL MACHINES.

Sollten Sie Interesse daran haben, Software zu entwickeln, die sich über den Solutions Manager einbinden lässt, so empfehlen wir Ihnen die Dokumentation *vsphere-ext-solutions-50.PDF* von VMware. Sie finden die Datei unter *http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-ext-solutions-50.pdf*.

12.14.10 Storage-Providers

Bereits mit vSphere 4.x hat VMware eine Schnittstelle implementiert, über die Storage-Hersteller APIs einbinden können, um Operationen zwischen den VMware-Komponenten und dem Storage zu optimieren. Nehmen wir als Beispiel das Storage vMotion: Beim Wechseln des Datastores einer aktiven virtuellen Maschine stößt das Management die Operation an und kontrolliert sie, bis sie abgeschlossen ist. Binden Sie eine API ihres Storage-Herstellers ein, übergibt das Management die Aufgabe in deren Hände, entlastet sich somit von der Arbeit und hat Ressourcen für andere Aufgaben frei. Der Storage meldet dann nach Abschluss der Arbeiten den Vollzug der gestellten Aufgabe zurück ans vCenter.

In unserer Testlandschaft sind keine Storage-APIs zu finden. Wir haben keinen Storage, der diese Funktion unterstützt.

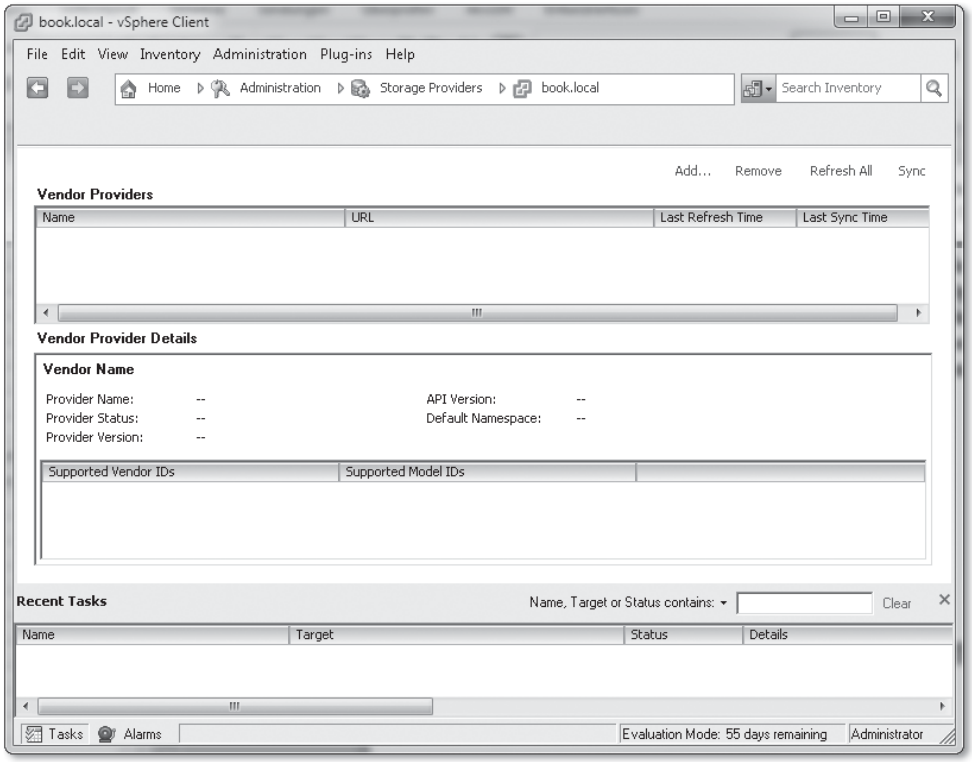


Abbildung 12.93 Übersicht der installierten Storage-APIs

12.14.11 VM-Speicherprofile

Die Speicherprofile sind eine weitere Neuerung, die VMware mit vSphere 5 eingeführt hat. Welche Philosophie steht dahinter, und was möchte VMware mit dieser neuen Funktion bezwecken? Schauen wir uns einmal den Prozess der Bereitstellung einer virtuellen Maschine an. Sind die Grunddaten – wie CPU, RAM, Netzwerk und Plattenanzahl sowie deren Größe – festgelegt, müssen Sie entscheiden, welche Leistungsdaten der Storage erfüllen muss. Nehmen wir einmal die klassische Variante von drei Storage-Wertigkeiten Gold, Silber und Bronze, die zum einen die Schnelligkeit und zum anderen die Verfügbarkeit des Storages widerspiegeln. Sie legen also drei Profile an, die dieser Einteilung gerecht werden, wozu Sie auf der Homepage den Punkt Storage Profiles wählen und den Link Create VM Storage Profile aufrufen.

Zusätzlich sind über Manage Storage Capabilities Wertigkeiten für den Storage festzulegen.

Diese verbinden Sie später mit dem Storage und den Speicherprofilen. Zuvor müssen Sie die Speicherprofile über Enable VM Storage Profile aktivieren, und über das Editieren der Profile stellen Sie eine Verknüpfung zwischen Profil und Wertigkeit her.

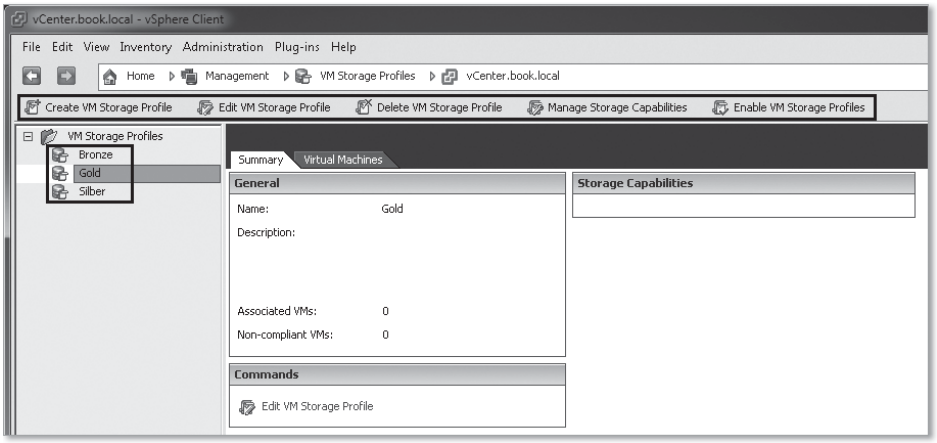


Abbildung 12.94 VM-Speicherprofile

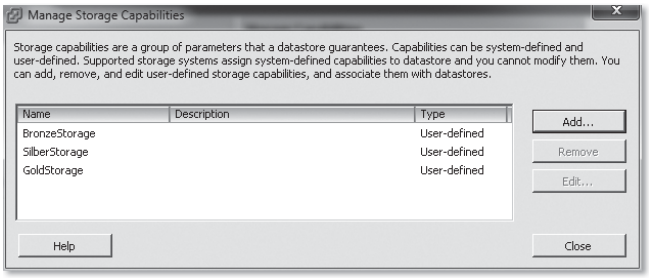


Abbildung 12.95 Festlegen von Storage-Wertigkeiten

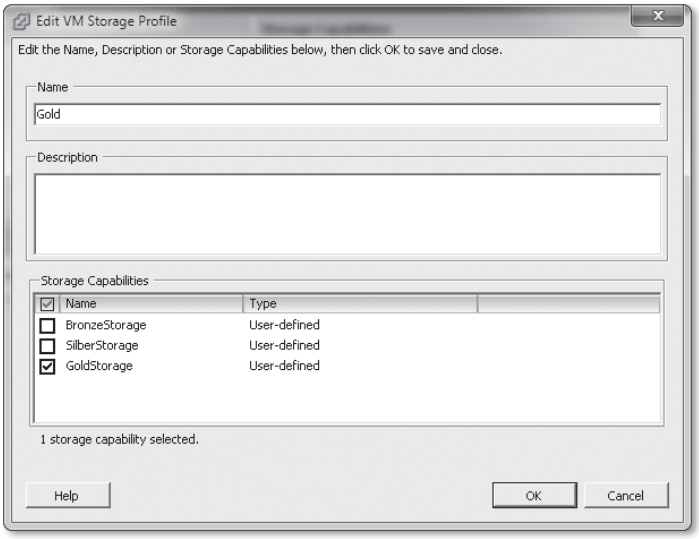


Abbildung 12.96 Profil und Wertigkeitsverknüpfung

Gehen Sie nun zu dem Datastore, dem Sie das Wertigkeitsprofil zuweisen wollen. Über den Link Assign User-Defined Storage Capability erfolgt die Verknüpfung.

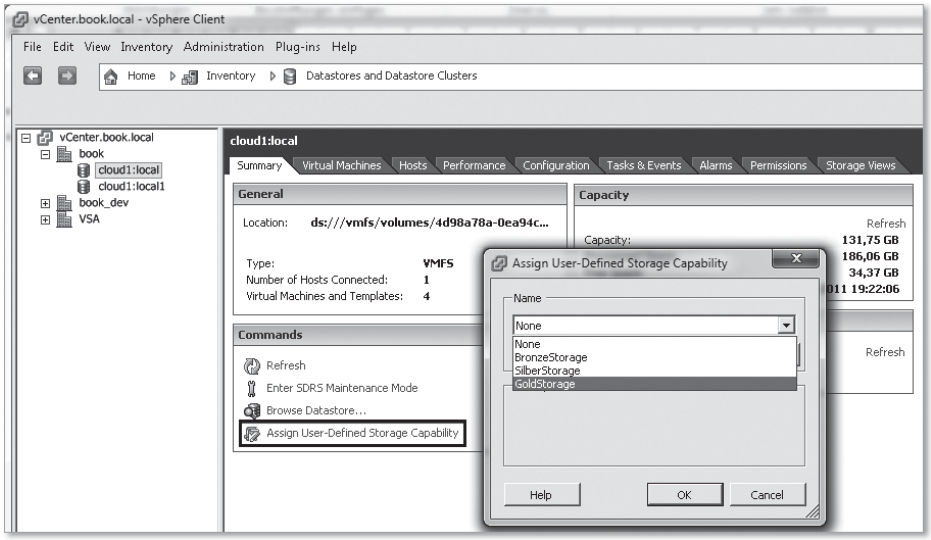


Abbildung 12.97 Verknüpfung von Datastores und Wertigkeiten

Erstellen Sie nun eine neue virtuelle Maschine, können Sie den Ziel-Storage nach den festgelegten Wertigkeitsprofilen aussuchen.

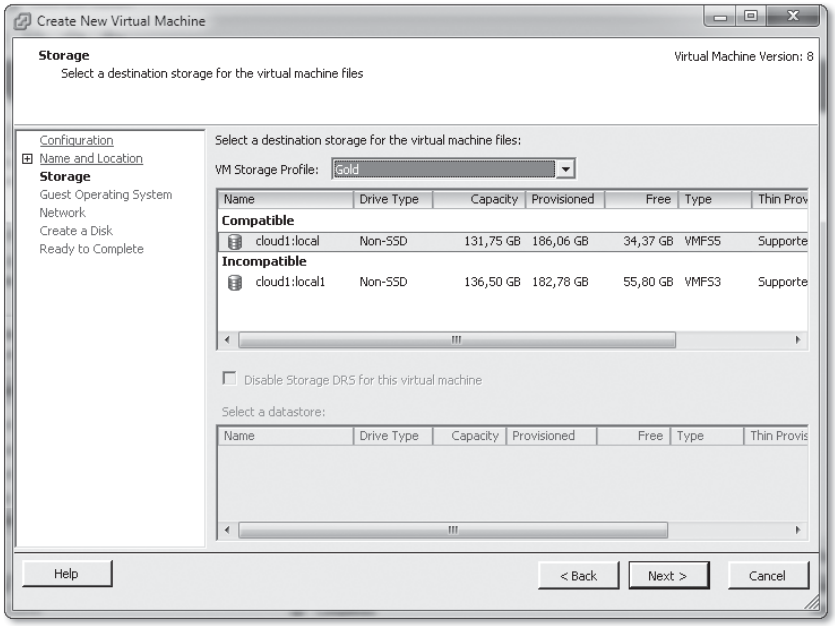


Abbildung 12.98 Anlegen einer VM mit dem Speicherprofil

Es werden Ihnen nun die kompatiblen Zielplatten angezeigt, auf denen Sie die VM anlegen können. Die Installation kann aber trotzdem auch auf nicht kompatiblen Platten erfolgen.

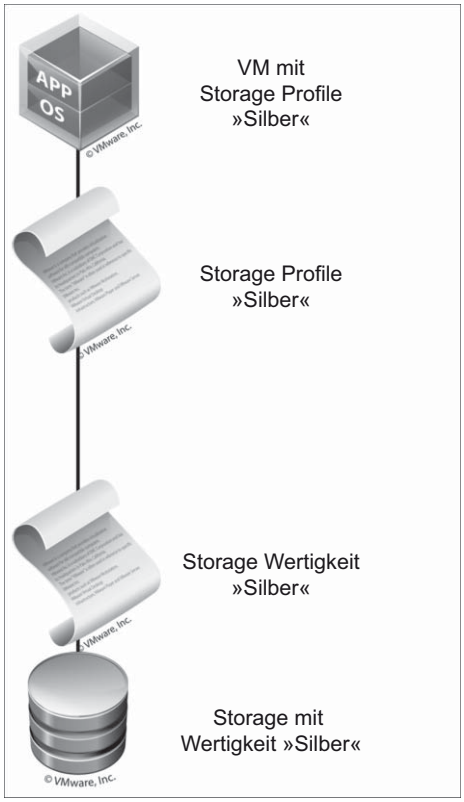


Abbildung 12.99 Virtuelle Maschine mit angehängtem Speicherprofil

So ist gewährleistet, dass die VM den Durchsatz zum Storage bekommt, den sie laut Anforderungen auch benötigt.

12.14.12 Customization Specification Manager

Beim Anpassen einer virtuellen Maschine oder wenn Sie eine VM klonen, können Sie ein Profil erstellen, das Sie auch später beim erneuten Klonen wieder benutzen können. Alle diese Profile werden an einer zentralen Stelle verwaltet: Wählen Sie auf der Homepage im vSphere-Client den Punkt Customization Specification Manager aus.

Sie haben hier verschiedene Möglichkeiten, mit den Optionen zu arbeiten. Sie lassen sich erstellen, exportieren, duplizieren, editieren oder löschen. Oder Sie importieren bereits vorhandene Profile. Das geschieht über den Link im oberen Bereich und nicht über das Kontextmenü. Mit diesen Profilen können Sie sich die Arbeit extrem erleichtern und müssen nicht bei jedem Vorgang alle benötigten Parameter per Hand eingeben.

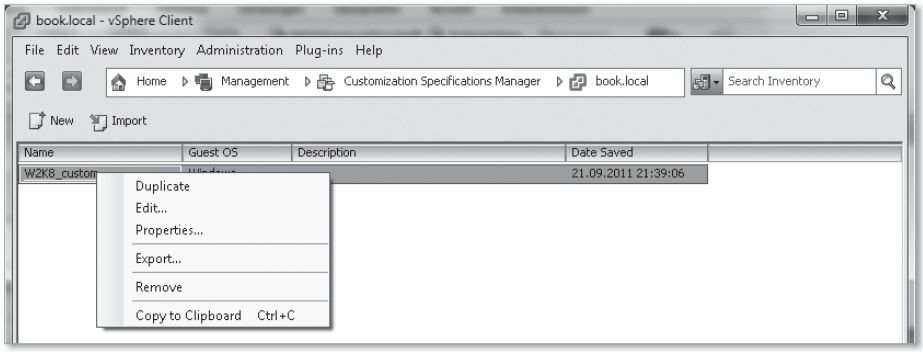


Abbildung 12.100 Profile für die Anpassung von zu klonenden VMs

12.14.13 Hardware-Status

Der HARDWARE STATUS befindet sich auf einem eigenen Reiter, der nach der Auswahl eines Hosts sichtbar ist. Dieses Fenster zeigt den »Gesundheitsstatus« der Hardware an (Abbildung 12.101). Die Informationen holt sich das vCenter über den Open-IPMI-Standard (Intelligent Platform Management Interface).

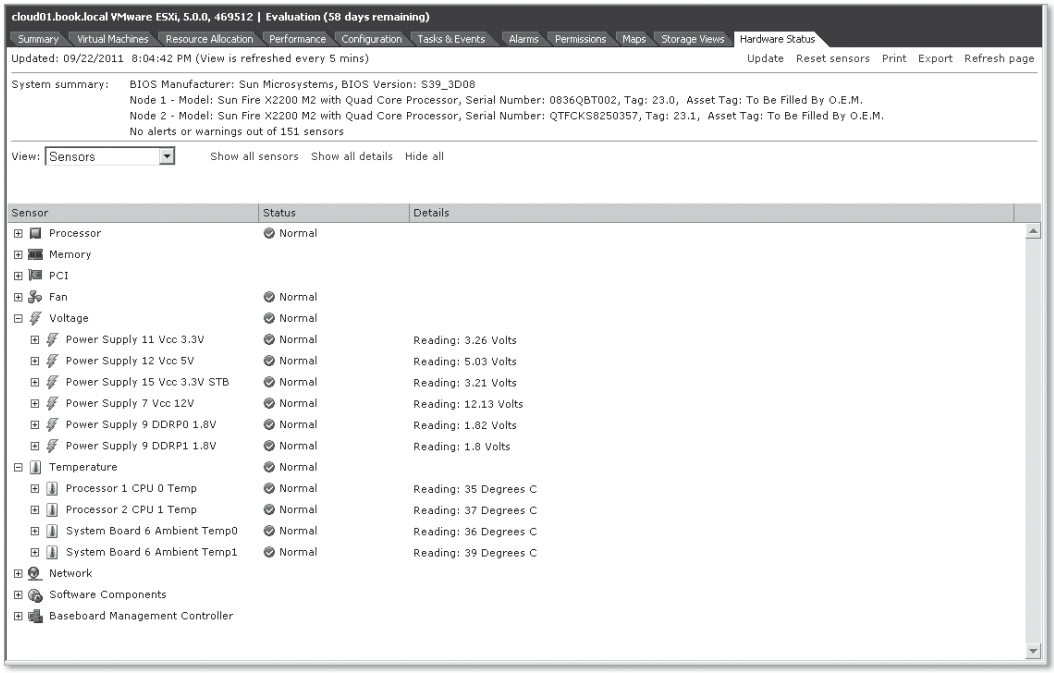


Abbildung 12.101 Hardware-Status des vSphere-Hosts

Jetzt werden Sie sich vielleicht darüber wundern, dass bei unterschiedlichen Hardwareherstellern auch unterschiedliche Daten angezeigt werden. Das hängt damit zusammen, wie der

Hardwarehersteller das IPMI implementiert hat. Bei einer reinen Open-IPMI-Implementierung sehen Sie nicht nur die Angaben, wie sie in Abbildung 12.101 dargestellt sind, sondern auch den RAID-Controller, die Festplatten und weitere Angaben. Der Vorteil bei dieser Implementierung ist, dass keine hardwarespezifischen Tools installiert werden müssen, damit alle Status angezeigt werden. Der Hersteller HP hat z. B. eine eigene Implementierung von IPMI, weswegen nicht alle Hardwareinformationen angezeigt werden, wenn die HP-SIM-Treiber nicht installiert sind.

12.14.14 Dienste anzeigen

Mit dem vCenter der Version 4 führte VMware eine zusätzliche Funktion ein, die es dem Administrator erleichtert, im Fehlerfall die Suche besser einzugrenzen. Über VIEW • ADMINISTRATION • VCENTER SERVICE STATUS erreichen Sie diese Übersicht.

Hier wird der Status aller vom vCenter genutzten Diensten angezeigt. Der unterschiedliche Status der Meldungen wird mit verschiedenen Farben und unterschiedlichen Symbolen markiert.

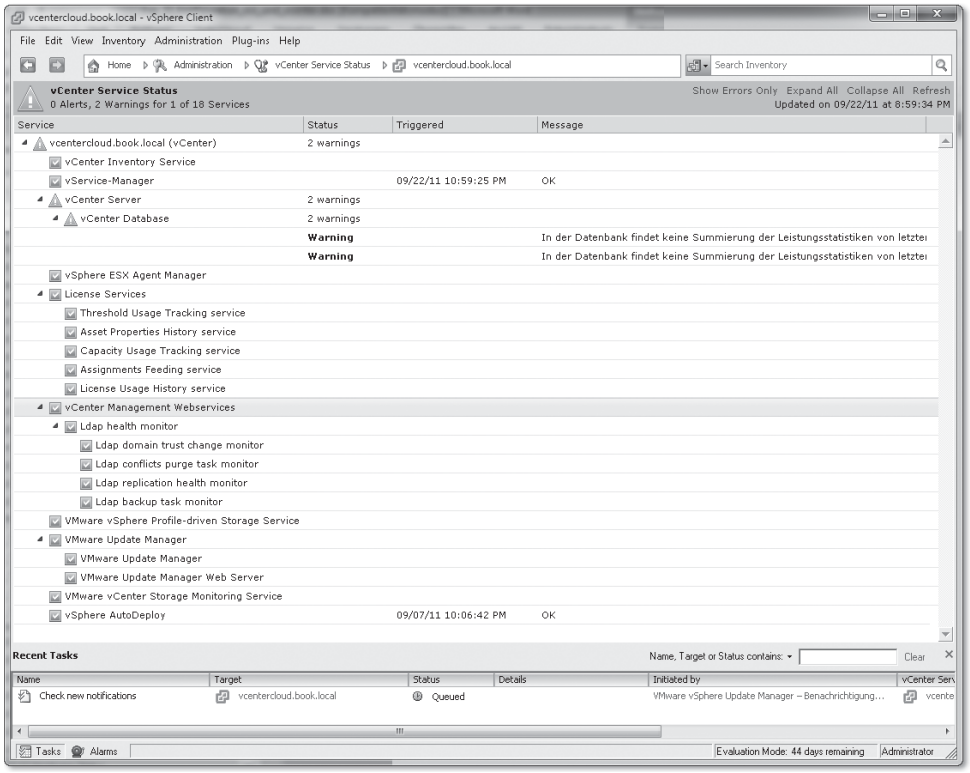


Abbildung 12.102 Status der vCenter-Dienste

Sie sehen, unsere Testumgebung hat lediglich ein paar kleine Wehwehchen.

12.15 vCenter-Konfigurationseinstellungen

Jetzt möchten wir noch auf die restlichen Konfigurationseinstellungen des vCenter-Servers eingehen, die wir bis jetzt noch nicht angesprochen haben. Dazu gehen wir das Konfigurationsmenü von oben nach unten durch. Der Aufruf erfolgt über den Menüpunkt VIEW • ADMINISTRATION • SERVER SETTINGS.

Achten Sie bitte auf die Anzeigen im Konfigurationsfenster. Ist nach einer Anpassung von Konfigurationsparametern ein Reboot nötig, dann wird dies im Fenster angezeigt.

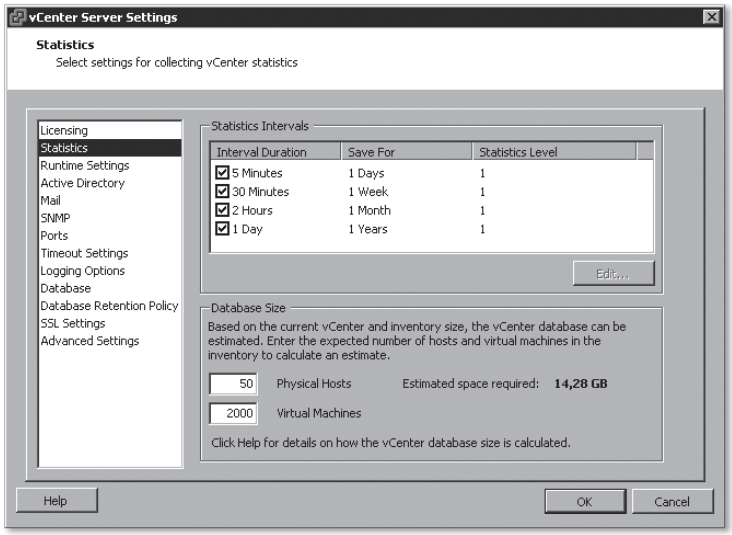


Abbildung 12.103 Einstellen der Intervalle für das Sammeln der Auswertungsdaten

Die Einstellungen betreffen das Sammeln der Performancedaten. Die Standardeinstellungen sind im Fenster sichtbar. Es gibt an dieser Stelle vier unterschiedliche Regeln, um die Daten zu sammeln und vorzuhalten. Über den EDIT-Button können Sie die Einstellungen manipulieren. Denken Sie daran, dass ein Ändern der Werte die Größe der vCenter-Datenbank direkt beeinflusst. Dabei ist es sehr hilfreich, dass in dem Fenster sofort angezeigt wird, wie sich die Größe der Datenbank ändert, wenn Sie Parameter anpassen.

Sie können nicht nur das Intervall und die Aufbewahrungszeit einstellen, sondern auch die Sammeltiefe der Daten. In Tabelle 12.13 zeigen wir, welche Informationen wann gesammelt werden.

Statistics-Level	Informationen
1	Die Grundmetriken werden über dieses Level gesammelt. Das sind die durchschnittliche Nutzung von CPU, Arbeitsspeicher, Festplatte und Netzwerk. Zusätzlich werden Systemlaufzeit, Systemtakt und DRS-Metriken protokolliert. Geräte werden in diesem Level nicht geloggt.
2	Level 2 enthält Level 1, wobei zu den Metriken CPU, Arbeitsspeicher, Festplatte und Netzwerk alle Informationen gesammelt werden, einschließlich des letzten Rollup-Typs. Einzige Ausnahme sind die Min- und Max-Werte des Rollup-Typs.
3	Hier ist ebenfalls Level 2 komplett inkludiert, einschließlich der Geräte. Auch hier bilden die Min- und Max-Werte der Rollup-Typen die Ausnahme.
4	Dieses Level sammelt alle Metriken, die das vCenter zur Verfügung stellt.

Tabelle 12.13 Liste der Statistics-Level

Es folgt die Konfiguration der Runtime Settings. Hier ist die ID des vCenters hinterlegt; den Namen und die IP-Adresse können Sie eintragen.

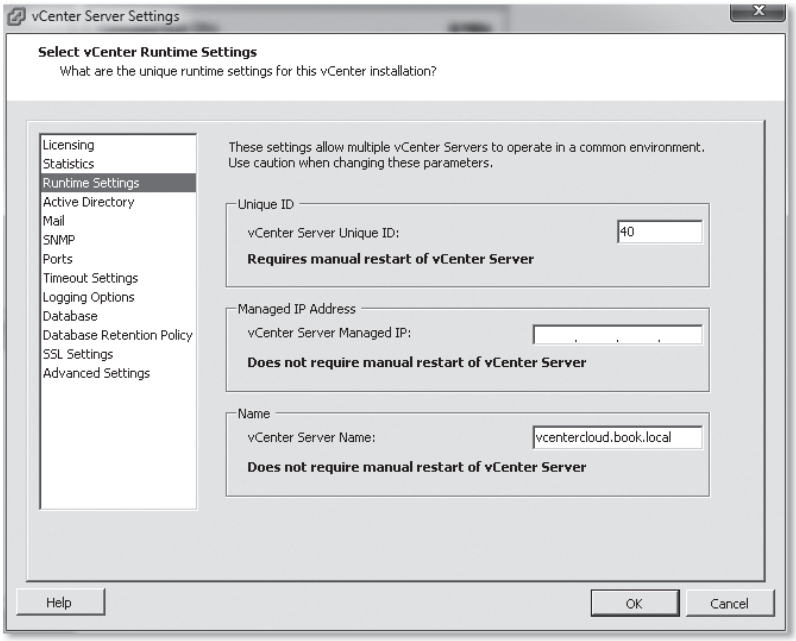


Abbildung 12.104 Einstellungen für die »Runtime Settings«

Die Unique ID muss einen Wert zwischen 0 und 63 haben. Dieser Wert wird bei der Installation zufällig vergeben. Die beiden anderen Einträge sprechen für sich.

Vergessen Sie nicht, die Mail-Einträge im vCenter-Server vorzunehmen. Neben dem Mailserver tragen Sie eine E-Mail-Adresse, besser noch eine Verteilerliste ein (Abbildung 12.105).

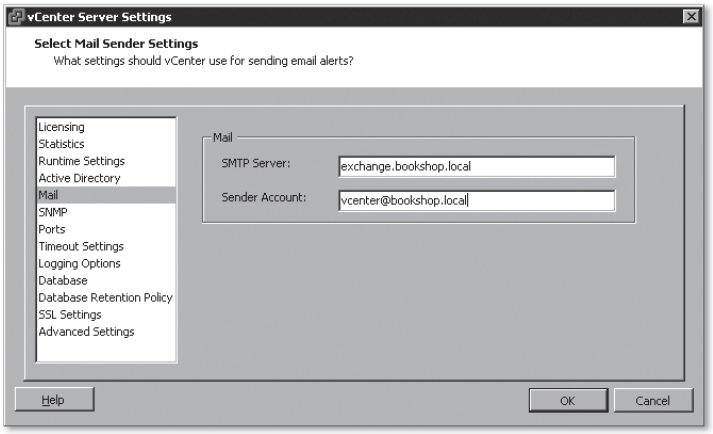


Abbildung 12.105 Einstellung der Mail-Benachrichtigung

An diesen Empfänger werden die Benachrichtigungen gesendet, die das System verschickt. Sollen die vom vCenter generierten SNMP-Nachrichten auf einem zentralen Managementsystem ausgewertet werden, dann sind die Parameter passend zu wählen.

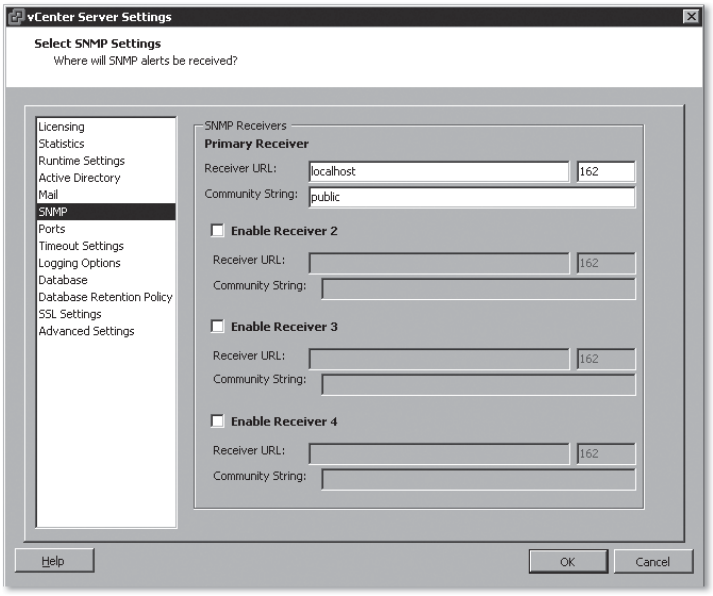


Abbildung 12.106 Konfiguration der SNMP-Empfänger

Es ist dabei nicht nur möglich, ein Ziel zu konfigurieren. Das vCenter unterstützt bis zu vier unterschiedliche Ziele für SNMP-Traps.

Die Zugriffsports für den vCenter-Server lassen sich ebenfalls anpassen. Als Standard sind für HTTP Port 80 und für HTTPS Port 443 festgelegt.

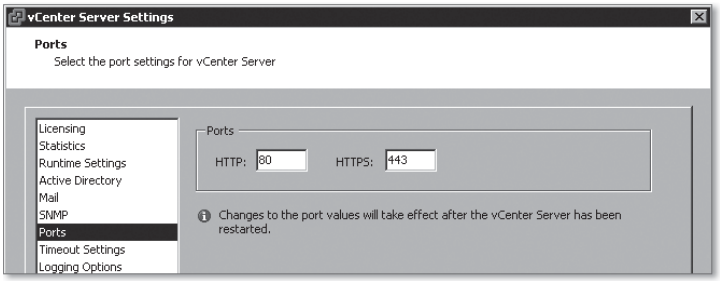


Abbildung 12.107 Kommunikationsports des vCenters

Denken Sie daran, eine Änderung in der Zugriffsmetrik zu dokumentieren, damit auch die Kollegen wissen, was zu tun ist, wenn der Installateur bei Anpassungen nicht dabei ist. Für die Kommunikation mit den Objekten in der virtuellen Infrastruktur werden im vCenter Timeout-Werte gesetzt.

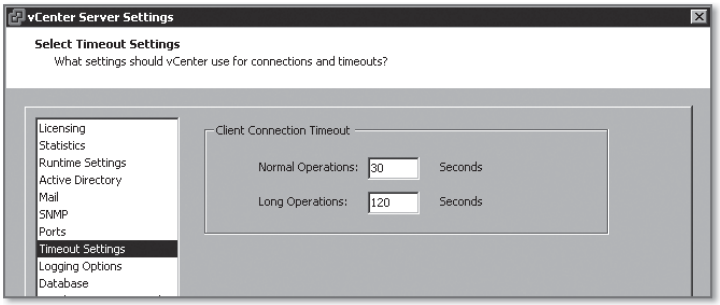


Abbildung 12.108 Zeitüberschreitungseinstellungen

Es werden zwei Vorgänge parametriert: der normale Vorgang und der lange Vorgang. Beide Werte sollten logischerweise nicht auf null gesetzt werden. Wichtig ist die Einstellung im Dialog für das Log-Level. An dieser Stelle bietet das vCenter sechs Optionen (Abbildung 12.109).

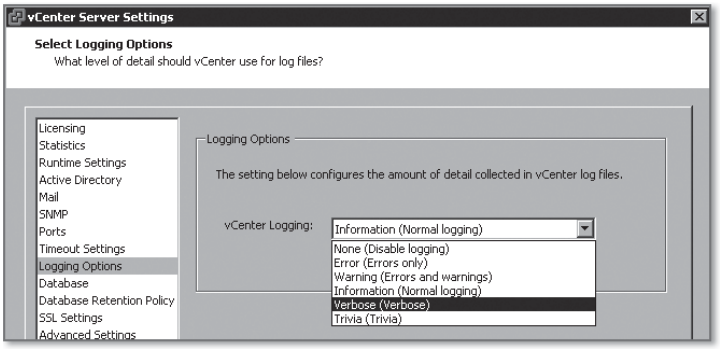


Abbildung 12.109 Einstellung des Log-Levels

Je nach ausgewähltem Level werden mehr oder weniger Daten gesammelt. Tabelle 12.14 listet die unterschiedlichen Level auf.

Log-Level	Informationen
None	Mit dieser Auswahl schalten Sie das Logging komplett ab.
Error	Diese Option loggt nur Fehlereinträge.
Warning	Wählen Sie diesen Punkt, wenn Sie nur Warnungen und Fehler sehen wollen.
Information	Es werden Informationen, Warnungen und Fehler angezeigt. Das ist das Standard-Log-Level.
Verbose	Dieses Level entspricht dem der Information, aber mit ausführlicherem Inhalt.
Trivia	In diesem Level wird der Informationsinhalt gegenüber dem Verbose-Level noch weiter erhöht.

Tabelle 12.14 Auflistung der möglichen Log-Level

Passen Sie das Level nur an, wenn es notwendig ist; die Datenmengen nehmen sonst einen enormen Umfang an. Die Anzahl der Datenbankverbindungen ist nach der Installation des vCenter-Servers auf 10 gesetzt. Der Dialog aus Abbildung 12.110 bietet an, den Wert zu ändern.

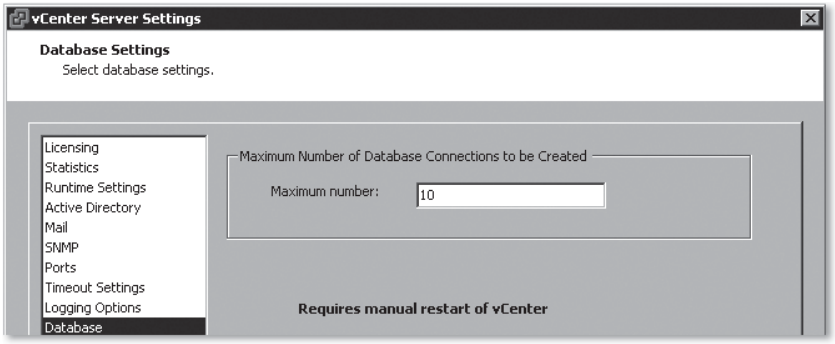


Abbildung 12.110 Anzahl von parallelen Datenbankverbindungen

Erhöhen Sie den Wert, wenn viele zeitkritische Aktionen laufen, was die Kommunikation zwischen vCenter und Datenbank verbessert. Natürlich ist es auch möglich, die Anzahl der Verbindungen zu reduzieren, etwa wenn diese Verbindungen hausintern verrechnet werden. Wünschen Sie, dass die Datenbankgröße nicht zu stark anwächst, begrenzen Sie über die Database Retention Policy das Wachstum der Datenbank. Hier können Sie das Speichern der Events und Tasks einschränken (Abbildung 12.111).

Berücksichtigen Sie, dass nach der Aktivierung der Retention Policy nicht mehr alle Aktionen in der virtuellen Landschaft nachvollzogen werden können. Es ist also abzuwägen, was wichtiger ist – eine Nachvollziehbarkeit aller Aktionen oder das Einsparen von Festplattenplatz.

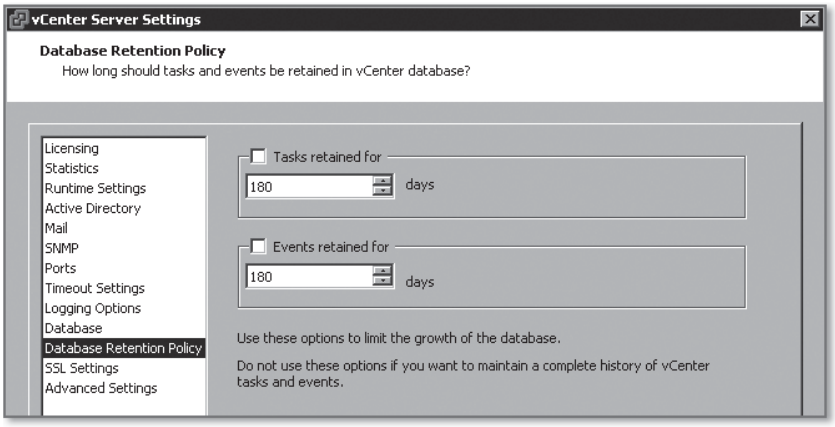


Abbildung 12.111 Beschränkung der Datenbankgröße

Unter SSL Settings ist manipulierbar, wie das vCenter mit den vSphere-Hosts kommuniziert. Vorkonfiguriert ist eine Verbindung mit der Nutzung von SSL-Zertifikaten. Es ist nicht empfehlenswert, diese Einstellung zu ändern (Abbildung 12.112).

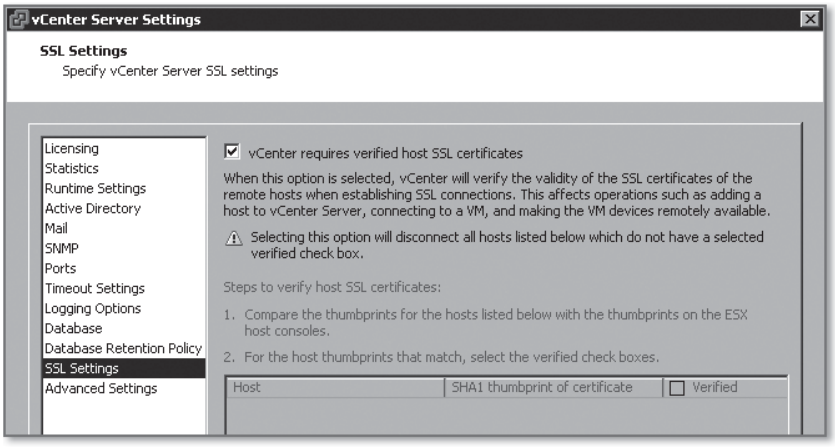


Abbildung 12.112 Aktivierung von SSL-Zertifikaten

Zu guter Letzt bietet VMware mit den Advanced Settings eine Option, zusätzlich Parameter einzufügen, die Sie nicht direkt über eine GUI einpflegen können (Abbildung 12.113). Trotzdem werden hier auch die Parameter angezeigt, die Sie über die GUI ändern können und die wir bis zu dieser Stelle besprochen haben. Alle Werte können Sie in den Advanced Settings einsehen, aber nicht manipulieren. Es besteht nur die Option, neue Werte einzutragen und über Add hinzuzufügen.

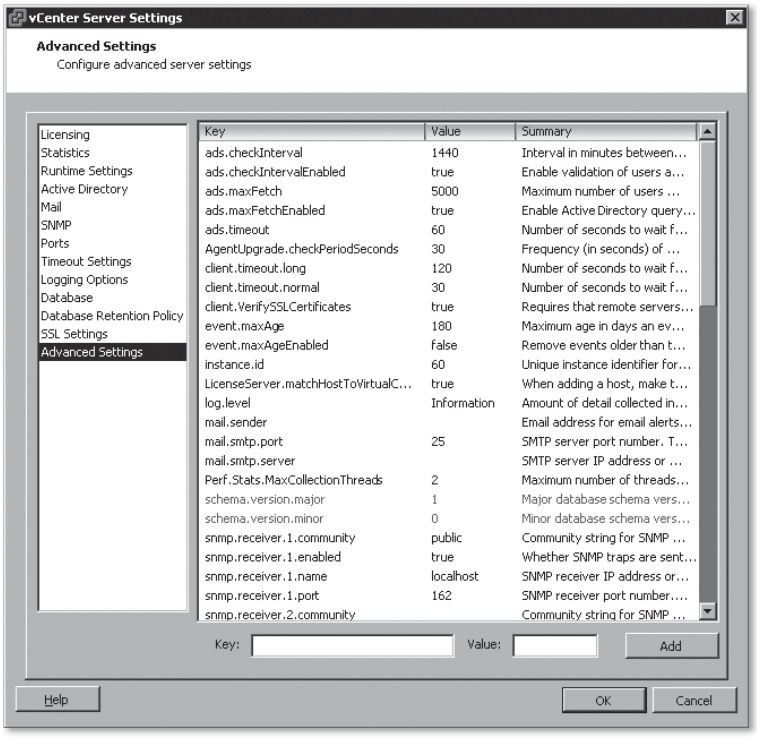


Abbildung 12.113 »Advanced Settings« des vCenters

12.16 Einrichten von Alarmen

Abschließend möchten wir in diesem Abschnitt auf die Alarmierungsfunktionen im vCenter-Server eingehen. Beim Vergleich mit der mit der Vorgängerversion, fällt auf, dass sich die Anzahl der möglichen Alarme in vCenter 5.x stark erhöht hat. Des Weiteren besteht auch die Möglichkeit, eigene Alarme zu kreieren und so die Alarmierung an die eigenen Bedürfnisse anzupassen.

Alarme können Sie mit fast jedem Objekt in der Infrastruktur verbinden, als da wären:

- Datacenter
- Cluster
- Host
- Datastore
- Datastore-Cluster
- Network
- Distributed Virtual Switch

- Distributed Virtual Switch Portgroup
- Virtual Machine
- vCenter Server

Dabei stehen Ihnen insgesamt 57 vordefinierte Alarme zur Verfügung. Es hängt nur vom Objekt ab, welche Alarme Sie nutzen können. Unterschieden wird dabei zwischen den Definitions, die im rechten Fensterabschnitt zu sehen sind, und den Triggered Alarms. Der letzte Punkt zeigt an, welche Alarme an dem betreffenden Objekt auch aktiv sind.

Bevor wir darauf eingehen, wie Sie Alarme erstellen, sollten wir uns anschauen, wie VMware die Struktur der Alarme angelegt hat. Auch wenn Alarme nur an bestimmte Objekte gebunden werden können, so wurden sie doch alle auf der Wurzelebene des vCenters definiert. Das ist auch schön in Abbildung 12.114 zu erkennen. In der mittleren Spalte ist leicht zu sehen, wo ein Alarm definiert wurde. Nur an diesem Definitionsort kann ein einmal definierter Alarm manipuliert werden. Dies gilt auch für die vordefinierten Alarme. Unsere Empfehlung ist, bei vordefinierten Alarmen nur die Schwellenwerte anzupassen. Bei weitergehenden Änderungen sollten Sie immer neue Alarme anlegen.

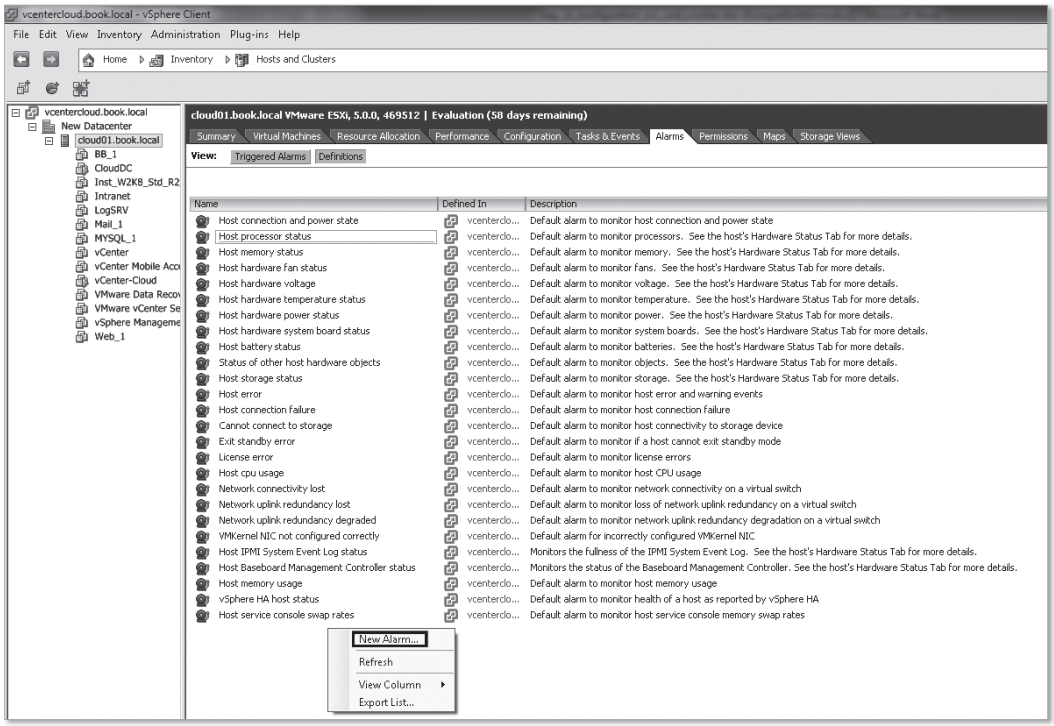


Abbildung 12.114 Übersicht der Alarmdefinitionen

Am einfachsten ist es, die Definitionen immer in der vCenter-Wurzel anzulegen und dann passend weiter unten mit den Objekten zu verbinden. Alarme werden erst in der Ansicht

Triggered Alarms sichtbar, wenn sie aktiviert wurden. Neu erstellt werden Alarme über das Kontextmenü der Definitions-Ansicht. Es öffnet sich ein Dialog, in dem Sie die weiteren Parameter eingeben (Abbildung 12.115). Legen Sie einen neuen Alarm an, sind diverse Grundeinstellungen vorzunehmen.

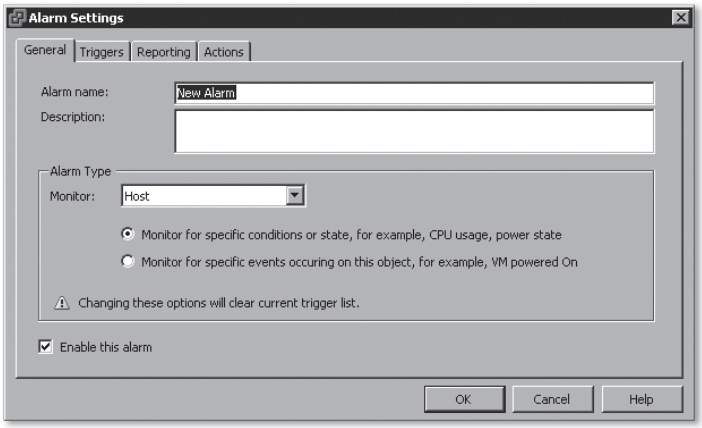


Abbildung 12.115 Grundparameter eines Alarms

Neben einem eindeutigen Namen ist festzulegen, für welches Objekt Sie den Alarm generieren. Was soll überwacht werden – ein Ereignis oder bestimmte Zustände? In diesem ersten Fenster können Sie den Alarm auch direkt aktivieren. Jetzt definieren Sie die Zustände, die überwacht werden sollen. Es steht eine lange Liste von Optionen zur Verfügung. Wählen Sie die passende aus, und markieren Sie den Status, der für den Trigger wichtig ist. Abschließend hinterlegen Sie in diesem Fenster die Konditionen für den Alarm.

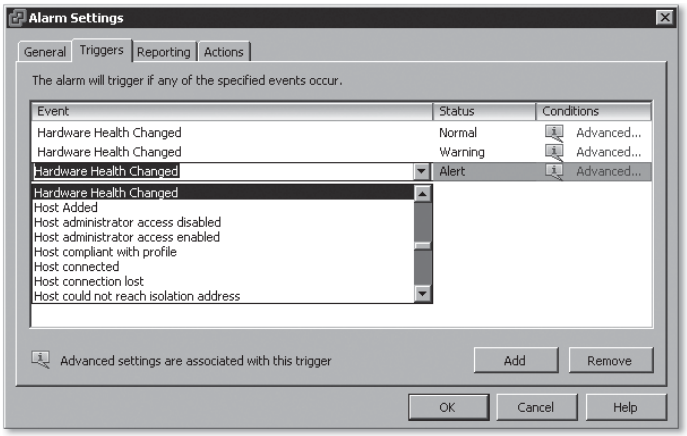


Abbildung 12.116 Trigger des Alarms

Sie können im Alarm auch mehrere Events hinterlegen.

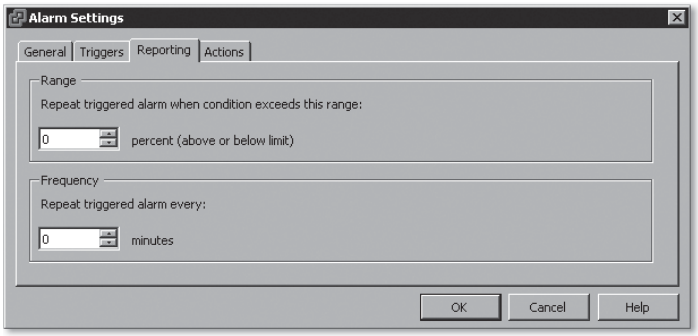


Abbildung 12.117 Wiederholungsintervall für den Alarm

Beim REPORTING legen Sie fest, unter welcher Bedingung ein ausgelöster Alarm wiederholt werden soll. Dabei stellen Sie einen Abweichungswert in Prozent ein und eine Frequenz, wie oft ein einmal ausgelöster Alarm wiederholt werden soll. Abschließend wählen Sie im Dropdown-Menü die bei einem Alarm auszuführende Aktion.

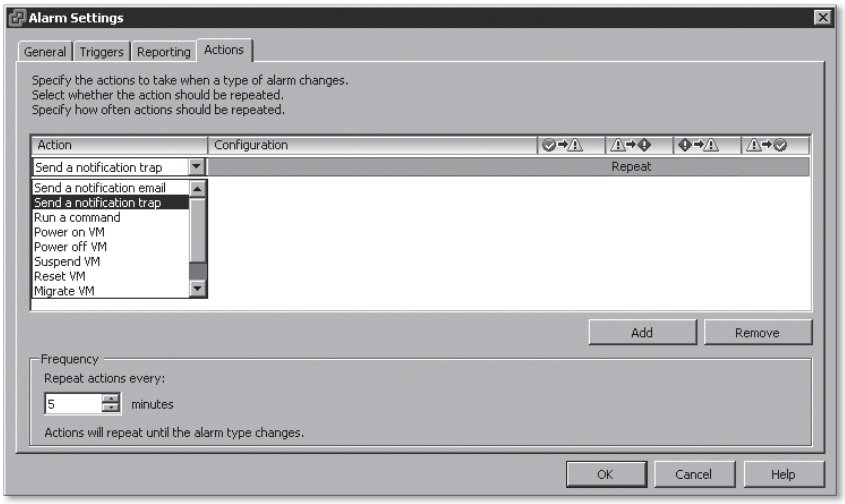


Abbildung 12.118 Parametrierung der Alarmaktion

Je nach Auswahl können Sie unter CONFIGURATION auch noch einen Eintrag vornehmen. In den rechten vier Spalten parametrieren Sie, bei welchem Statuswechsel die Aktion durchgeführt werden soll. Die Symbole repräsentieren dabei den Übergang zwischen den einzelnen Schwellenwerten. Die Aktion kann entweder einmal oder jedes Mal beim Erreichen der Grenze ausgeführt werden.

Die Alarmfunktion bietet eine Fülle von Möglichkeiten. Nutzen Sie sie, aber achten Sie darauf, nicht so viele Alarme zu erstellen, dass Ihr Postfach geflutet wird. Die Anzahl sollten Sie so wählen, dass Sie die Menge der Benachrichtigungen noch bewältigen können.

12.17 VMware vCenter Server-Appliance

Ist die Appliance importiert, können Sie sie einfach einschalten. Die Konsole stellt sich dar wie in Abbildung 12.119. Sie könnten an dieser Stelle auch die Konfiguration vornehmen, aber wesentlich komfortabler gestaltet sich das über den Webbrowser.

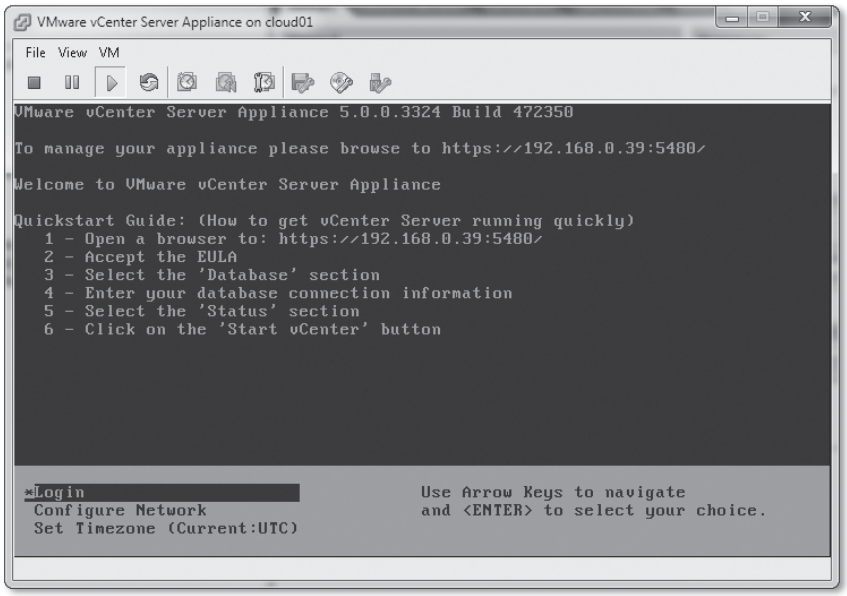


Abbildung 12.119 Konsole der VCVA (VMware vCenter Server Appliance)

Der Zugriff erfolgt dann über den Web-Browser. Die Anmeldedaten sind:

- User: »root«
- Passwort: »vmware«

Nach der Anmeldung ist das EULA zu bestätigen, anschließend erfolgt die eigentliche Konfiguration. Dabei gliedert sich die Oberfläche in mehrere Abschnitte.

Da ist zum einen die Leiste mit den Hauptmenüpunkten, die immer sichtbar ist. Das Aussehen der unteren Leiste ist individuell und hängt vom ausgewählten Hauptmenüpunkt ab. Wir möchten nicht allzu viel wertvollen Platz mit Screenshots bedrucken, aus diesem Grund werden wir zwar alle Punkte ansprechen, die zu konfigurieren sind, aber nur zu den wichtigen Punkten Abbildungen liefern.

Unter dem Hauptpunkt vCenter Server finden sich das EULA und der Status des vCenter Servers mit den Optionen, ihn zu starten oder zu stoppen. Für die Einrichtung der Datenbank erreichen Sie unter dem Hauptpunkt ein dediziertes Menü.

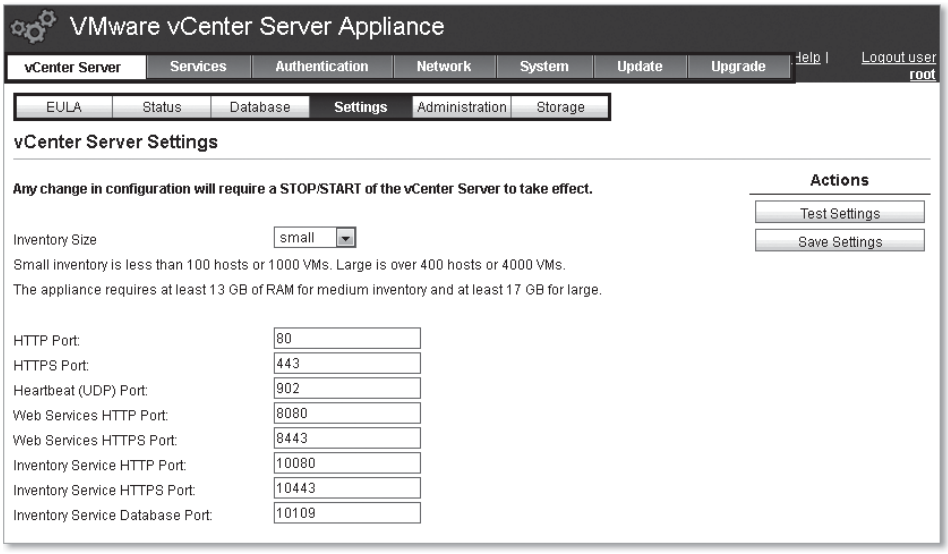


Abbildung 12.120 Konfigurationsoberfläche VCVA

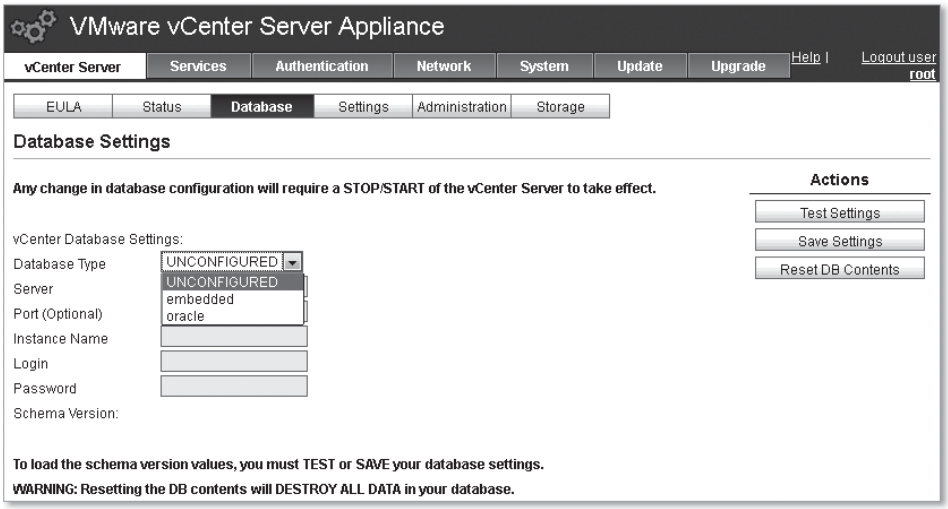


Abbildung 12.121 Auswahl der Datenbank

Damit Sie bei einer entfernten Datenbank das Schema angezeigt bekommen, müssen Sie zuerst die Einstellungen testen. In unserem Fall haben wir die EMBEDDED-Datenbank ausgewählt. Unter SETTINGS können Sie die IP-Ports der Appliance anpassen. Unsere Empfehlung ist: Nutzen Sie die Original-Ports, dass bereitet am wenigsten Schwierigkeiten und ist bei der VCVA auch grundsätzlich kein Problem, denn auf dem Server laufen ja keine weiteren anderen Applikationen. In diesem Konfigurationsfenster können Sie auch angeben, wie groß die zu verwaltende Landschaft sein soll. Dazu gibt es drei mögliche Auswahlpunkte.

Auswahl	Beschreibung
SMALL	für bis zu 100 Hosts und 1.000 VMs
MEDIUM	für 100 bis 400 Hosts und 1.000 bis 4.000 VMs
LARGE	für über 400 Hosts und über 4.000 VMs

Tabelle 12.15 VCVA-Sizing für das Inventory

Das ist aber nicht die einzige Stellschraube, an der Sie drehen müssen: Zusätzlich müssen Sie den Arbeitsspeicher der Appliance anheben. Richtwerte entnehmen Sie bitte Tabelle 12.16.

Arbeitsspeicher	Beschreibung
4 GB	für bis zu 10 Hosts und 100 VMs
8 GB	für bis zu 100 Hosts und bis zu 1.000 VMs
13 GB	für 100 bis 400 Hosts und 1.000 bis 4.000 VMs
17 GB	für über 400 Hosts und über 4.000 VMs

Tabelle 12.16 VCAC-Sizing für das Inventory

Zur Anpassung des Administratorkennworts wählen Sie den Menüpunkt ADMINISTRATION aus. Nach der Eingabe des derzeitigen Passworts vergeben Sie Ihr neues, nach Unternehmensvorgaben festgelegtes Kennwort. Im letzten Menüunterpunkt stellen Sie ein, auf welchem NFS-Share die Core- bzw. Log-Dateien abgelegt werden sollen. Hinter der Auswahl SERVICES verbergen sich die Port-Einstellungen für den Auto-Deploy-Service, den Syslog-Service und den Netdump-Service. Außerdem lassen sich an dieser Stelle die Dienste für den WebClient und für den ESXi-Dienst neu starten.

Soll das System in einen Verzeichnisdienst eingebunden werden, werden Sie unter dem Menüpunkt AUTHENTICATION fündig. Mögliche Optionen sind die Einbindung in ein Microsoft Active Directory oder in einen Unix-NIS-Dienst.

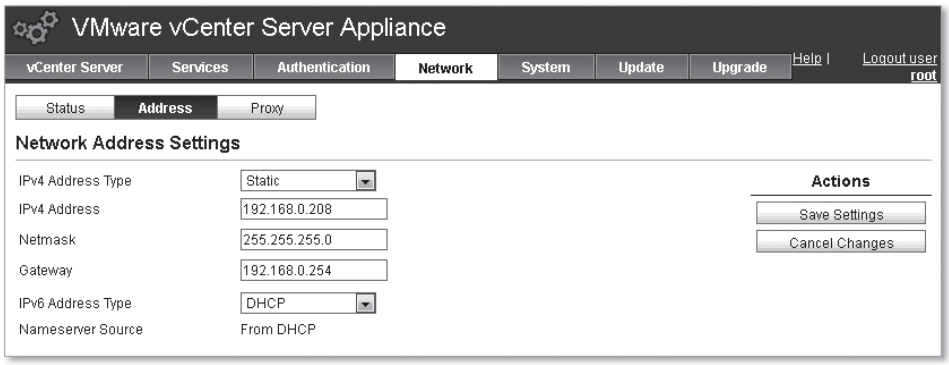


Abbildung 12.122 Netzwerkeinstellungen der VCVA

Für den Zugriff über das Netzwerk sind die Einstellungen unter Network vorzunehmen. Dabei werden sowohl IPV4- als auch IPV6-Adressen unterstützt. Unter Proxy hinterlegen Sie die Einstellungen, die benötigt werden, damit die Appliance aktualisiert werden kann. Mit den Parametern unter dem Punkt System stellen Sie außer dem Reboot und dem Shutdown die Zeitzone des Servers ein.

Aktualisierung der VMware vCenter Server-Appliance

Die beiden letzten Punkte sind Update und Upgrade. Hier findet das gesamte Handling für die Aktualisierung der Appliance statt. Über einen Scheduler wird im Internet bei VMware nach Updates für die vCenter-Appliance gesucht. Das Verhalten bezüglich Aktualisierungen bestimmen Sie mit den drei Optionen unter Automatic Updates: keine Updateverwaltung, die automatische Suche nach Updates und die Suche nach Updates und deren automatische Installation. Standardmäßig wird dabei auf das VMware-Repository im Internet zugegriffen, alternativ können Sie aber auch andere Quellen angeben. Das ist sehr sinnvoll, wenn Sie etwa laut Firmen-Policy mit dem Server nicht ins Internet dürfen. Auch beim Einsatz von mehreren VCVA-Servern kann es sinnvoll sein, die Aktualisierungen zentral zur Verfügung zu stellen.

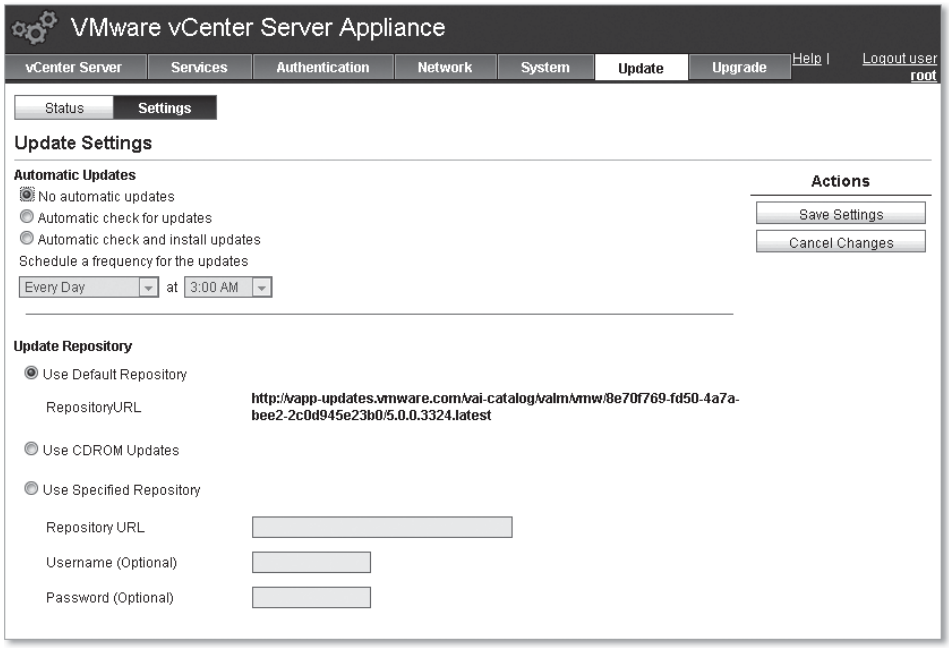


Abbildung 12.123 Update-Einstellungen der VCVA

Als letzter Einstellungspunkt bleibt Upgrade. Hier hat VMware eine Möglichkeit implementiert, parallel zu einer bereits vorhandenen Appliance eine neuere aufzubauen. Zuerst legen Sie fest, welche VCVA die Quelldaten liefert und welche die Konfiguration entgegennimmt. Nach der Auswahl der Rollen wird auf beiden Systemen ein Schlüssel erzeugt, den Sie auf der

jeweils anderen einspielen. Am einfachsten können Sie das über Cut & Paste durchführen, sonst sind Tippfehler wohl programmiert.

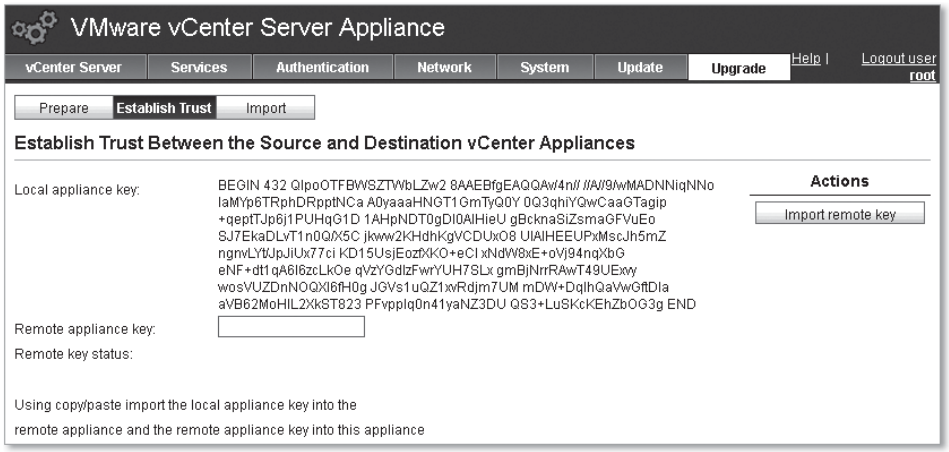


Abbildung 12.124 Upgrade Austausch-Key VCVA

Nach dem Starten des Abgleichs wird die Konfiguration auf die neue Appliance übernommen und die alte wird offline gesetzt. So können Sie ohne großen Aufwand eine neue VCVA aktivieren, ohne die gesamte Konfiguration per Hand übernehmen zu müssen.

Haben wir uns in dem vorhergehenden Kapitel mit der Konfiguration des vCenters und des Hosts beschäftigt, so wollen wir in diesem Kapitel näher auf die Konfiguration der vCenter-Add-ons eingehen.

13 Konfiguration von vCenter-Add-ons

Autor dieses Kapitels ist Bertram Wöhrmann, Ligarion, bwoehrmann@ligarion.de

Im vorhergehenden Kapitel lag der Schwerpunkt auf den Basisfunktionen des vCenter Servers; jetzt kommen wir zu zusätzlichen Optionen, die Ihnen als Administrator das Leben sehr erleichtern.

So besteht die Möglichkeit, Host-Systeme zu patchen. Danach beschäftigen wir uns mit der Verlinkung von vCenter Servern, bevor wir uns mit den neuen Funktionen des Sammelns von Logs und Dumps auseinandersetzen. Der Authentication Proxy steht als Nächstes auf der Liste. Einen recht großen Abschnitt werden die Installationsfunktionen für Hosts einnehmen. Der VMware Converter wird zwar nicht mehr direkt ins vCenter eingebunden, aber dennoch sollte er hier nicht fehlen. Zu guter Letzt möchten wir Ihnen die Datensicherungslösung von VMware näherbringen.

13.1 Einsatz des vCenter Update Managers

Der VMware vCenter Update Manager wurde mit Version 3.5 der VMware Virtual Infrastructure eingeführt. Er ist ein eigenständiges kostenloses Produkt zur Aktualisierung der VMware-Hosts. Das Patchen der Betriebssysteme von virtuellen Maschinen wird *nicht* mehr unterstützt, wohl aber die Aktualisierung der virtuellen Hardware und der VMware Tools. Zur Durchführung dieser Arbeiten müssen Sie eigene Mechanismen oder den VMware Configuration Manager einsetzen oder Software von Drittherstellern.

Der Update Manager wird nicht während der Installation des VMware vCenter Servers installiert. Wie bereits in Kapitel 6, »Installation«, beschrieben, installiert sich der Update Manager separat und wird später als Plugin im vCenter sowie in den zugehörenden Clients hinzugefügt.

In diesem Abschnitt werden wir näher auf den VMware Update Manager eingehen und alle wichtigen Punkte und Themen behandeln.

Exemplarisch zeigen wir Ihnen die vorbereitenden Arbeiten, die Sie durchführen müssen, um die Software effektiv nutzen zu können. Beachten Sie bitte dabei, dass die Anwendung von Updates auf die ESXi-Hosts unter Hosts And Clusters durchgeführt werden muss.

13.1.1 Installation

Die Installation des Update Managers haben wir bereits ausführlich in Kapitel 6, »Installation«, beschrieben.

Installation des Plugins

Bei der ersten Anmeldung am vCenter nach der Installation des vCenter Update Managers sehen Sie im Menü unter Plug-ins • manage plug-ins im Plug-in Manager ein neues Modul unter Available Plug-ins. Ein Klick auf den Link Download and Install installiert die Client-Komponente des Update Managers. Anschließend wird das Plugin automatisch aktiviert.

Der Client findet sich dann auf der vCenter-Homepage unter Solutions and Applications (Abbildung 13.1).

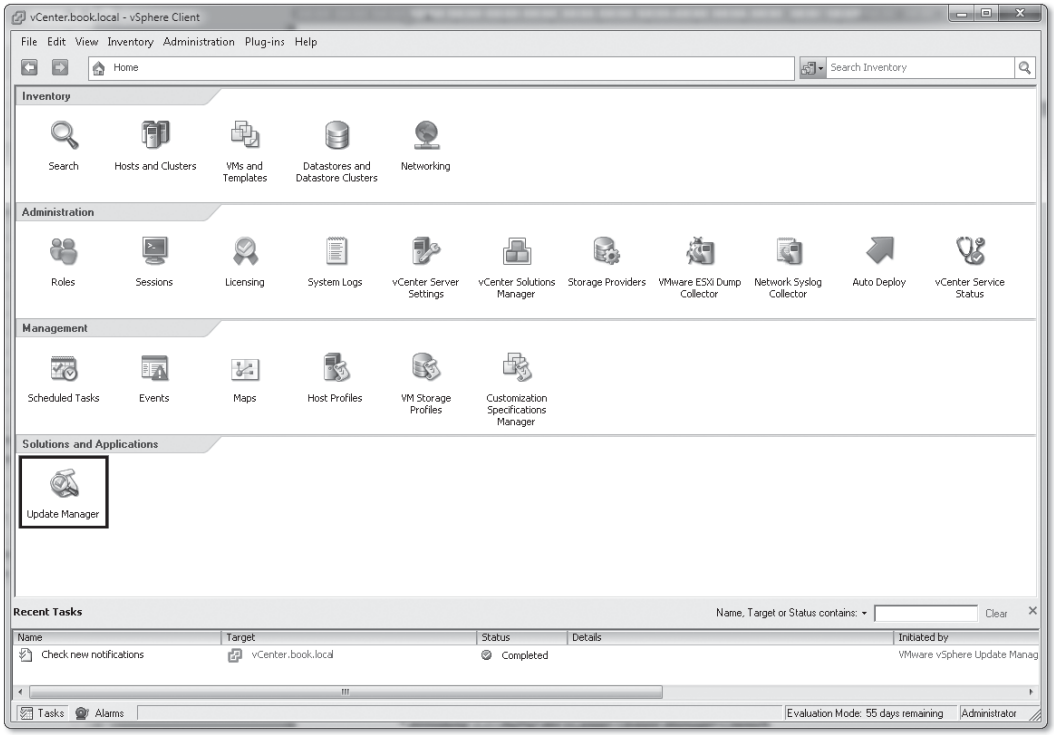


Abbildung 13.1 Aufruf des vCenter-Update-Manager-Clients

Damit ist die Installation des Update Managers abgeschlossen, und er ist nun bereit zur Konfiguration. Über den Button Update Manager gelangen Sie in das Hauptfenster des Plugins (Abbildung 13.2).

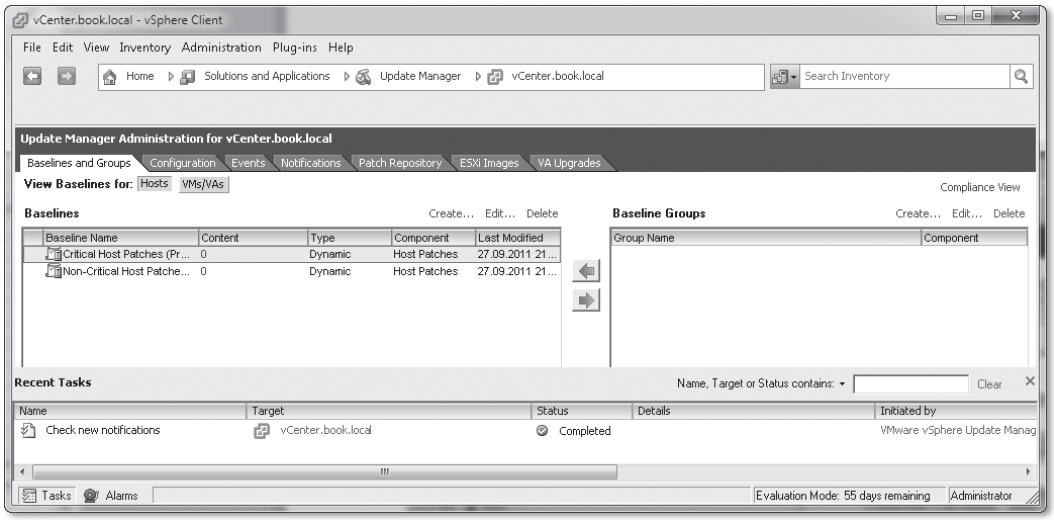


Abbildung 13.2 vCenter Update Manager: »Baselines and Groups«

Das Managementfenster hat sieben Reiter: Baselines and Groups, Configuration, Events, Notifications, Patch Repository, ESXi Images und VA Upgrades. Im oberen Drittel des Fensters lassen sich Baselines erstellen und verwalten, getrennt nach Hosts und VMs und VAs. Im mittleren Drittel erstellen Sie Baseline-Gruppen, in denen Sie wiederum Patch-Baselines zusammenfassen können. Im unteren Teil des Fensters werden die abgearbeiteten Tasks angezeigt. Im Folgenden werden wir einzeln auf die Konfigurationsfenster eingehen.

13.1.2 Konfiguration

Als Erstes müssen Sie den Update Manager konfigurieren. Die entsprechenden Einstellungen nehmen Sie im Reiter Configuration im Update-Manager-Hauptfenster vor (Abbildung 13.3).

Netzwerkkonfiguration

Über den Link Network Connectivity gelangen Sie in das Konfigurationsfenster, in dem Sie die Kommunikationsports der Applikation einstellen. Dabei handelt es sich um die Verbindung von Client und Applikation und den Port für den Zugriff auf das Patch-Repository sowie um die Ziel-IP oder den DNS-Namen des Repositorys.

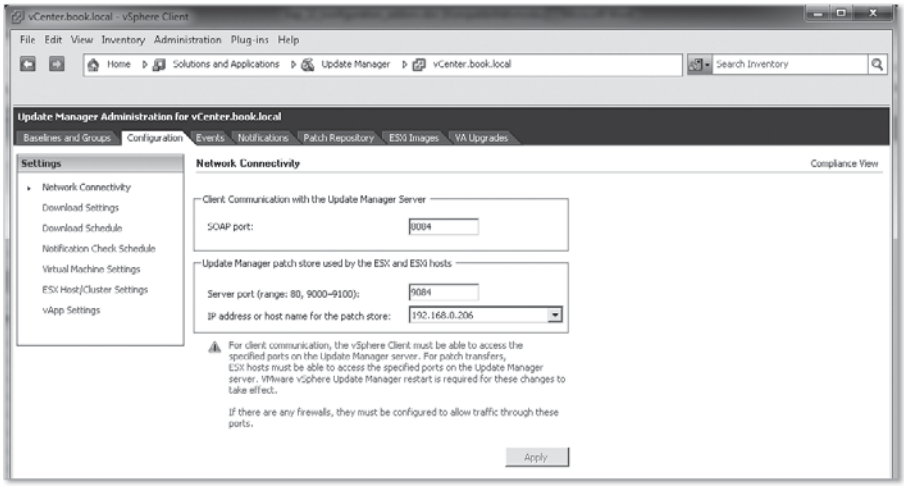


Abbildung 13.3 Netzwerkkonfiguration des Update Managers

Download-Einstellungen

In diesem Konfigurationsabschnitt konfigurieren Sie das Netzwerk der Server-Komponente. Bereiten Sie den Server dafür vor, die gewünschten Patches in das Repository zu laden (Abbildung 13.4). Wichtig an der Stelle ist, dass der Speicherplatz auf der Festplatte, auf der das Repository liegt, ausreicht (siehe auch Kapitel 6, »Installation«).

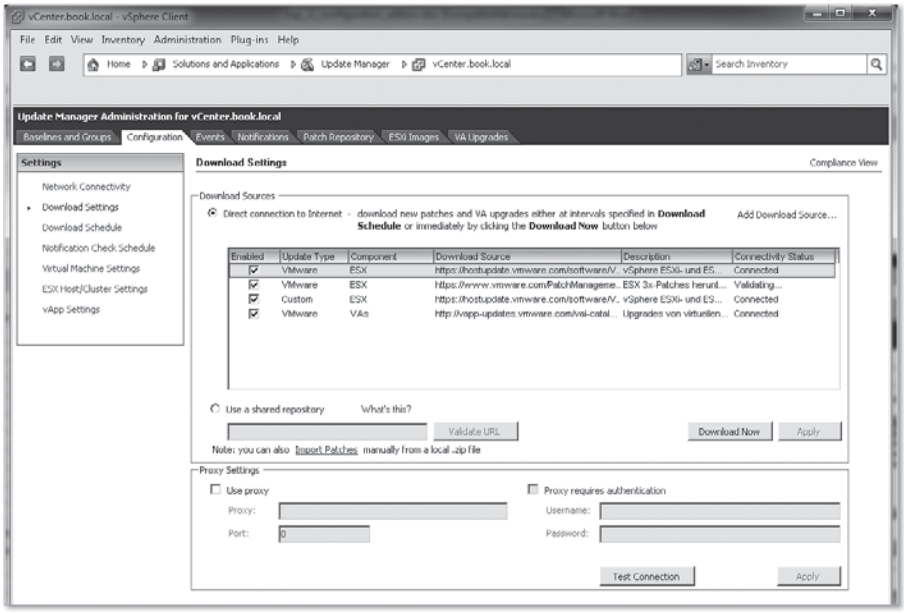


Abbildung 13.4 Download-Einstellungen des Update Managers

Die erste Konfiguration betrifft die Patches, die mit dem Update Manager verteilt werden sollen. Die Auswahl gliedert sich in Patches für ESX 3.x, ESX 4.x, ESX 5.x und Virtual Appliances. Wird das vCenter nur als Client ohne Download-Funktion genutzt und liegen dadurch die Patches in einem Repository auf einem anderen Server, dann können Sie unter Use shared repository den Zielpfad angeben. Erlaubt sind hier aber nur die Angabe einer lokalen Festplatte oder einer HTTP-basierten Quelle.

Ist das Herunterladen der Patches nur über einen Proxy-Server möglich, können Sie in diesem Fenster die passenden Parameter eintragen. Der Verbindungstest zeigt sofort, ob die Einstellungen korrekt sind oder modifiziert werden müssen.

Einen Download der Patches stoßen Sie direkt über den entsprechenden Button Download Now an. Zu Beginn werden nur die Informationen zu den Patches heruntergeladen, die Sie dann unter dem Reiter Patch Repository einsehen und weiterverarbeiten können.

Download-Zeitplaner

Der Update Manager enthält einen Zeitplaner für das Herunterladen von Patches. Dieser Prozess lässt sich in diesem Fenster automatisieren. Nach dem Aufruf werden Ihnen wie in Abbildung 13.5 die derzeitigen Einstellungen gezeigt.

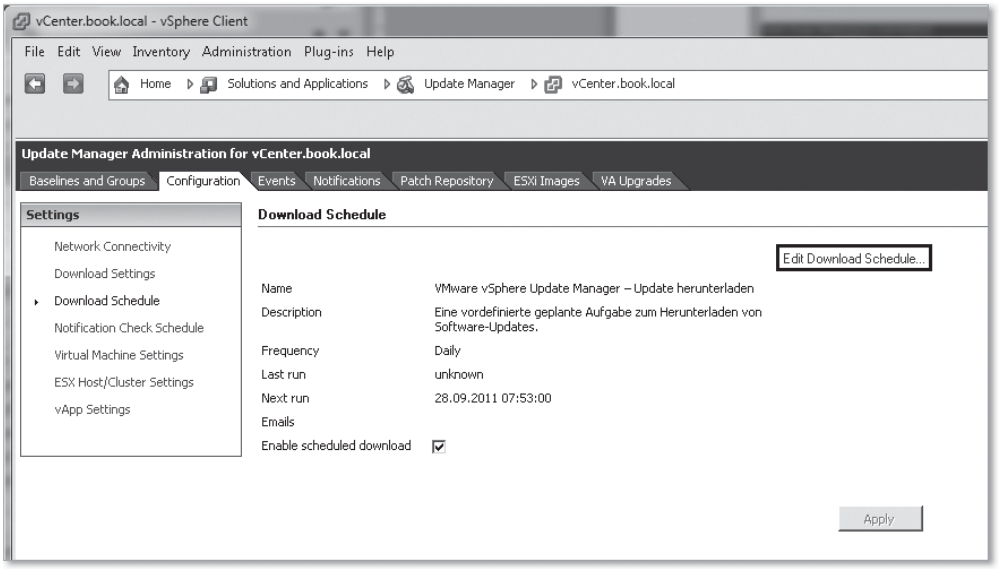


Abbildung 13.5 Download-Zeitplaner des Update Managers

Möchten Sie den Job anpassen, öffnen Sie über den Link Edit Download Schedule... eine Dialogbox zum Einstellen der Parameter (Abbildung 13.6).

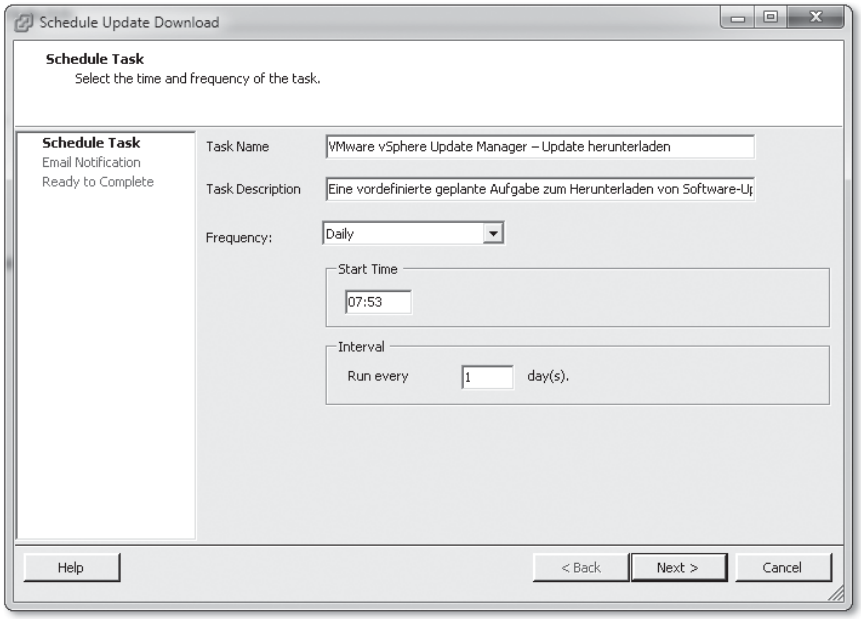


Abbildung 13.6 Parametrierung des Download-Tasks

An sich ist das Fenster selbsterklärend. Je nach ausgewählter Download-Frequenz ergeben sich unterschiedliche Konfigurationsoptionen. Zur Verfügung stehen die Download-Frequenzen ONCE, HOURLY, DAILY, WEEKLY und MONTHLY. Die Frequenz des Downloads sollten Sie davon abhängig machen, welche Systeme gepatcht werden sollen. Wir sind der Meinung, dass der Wochenrhythmus empfehlenswert ist. Ein stündlicher oder täglicher Rhythmus scheint nicht sonderlich sinnvoll. Aber auch hier spielen die Sicherheitsrichtlinien im Unternehmen eine große Rolle.

Ist der Job eingerichtet, besteht noch die Möglichkeit, eine E-Mail-Adresse anzugeben, die den Administrator benachrichtigt, wenn neue Patches heruntergeladen wurden.

Benachrichtigungsintervall

Unter SCHEDULE TASK konfigurieren Sie den Benachrichtigungsintervall. Wie oft soll das System nach Benachrichtigungen schauen, damit Sie immer rechtzeitig über neue Patches informiert sind?

Gast-Einstellungen

Eine sehr interessante Option geben Ihnen die VIRTUAL MACHINE SETTINGS an die Hand: Sie können die Patch-Arbeiten mit Unterstützung der Snapshot-Funktionalität durchführen (Abbildung 13.7). Wie funktioniert das Ganze? Bevor der Patch-Vorgang im Gast angestoßen wird, initiiert der Update Manager einen Snapshot. Ist der Snapshot erstellt, werden die Patch-Arbeiten durchgeführt.

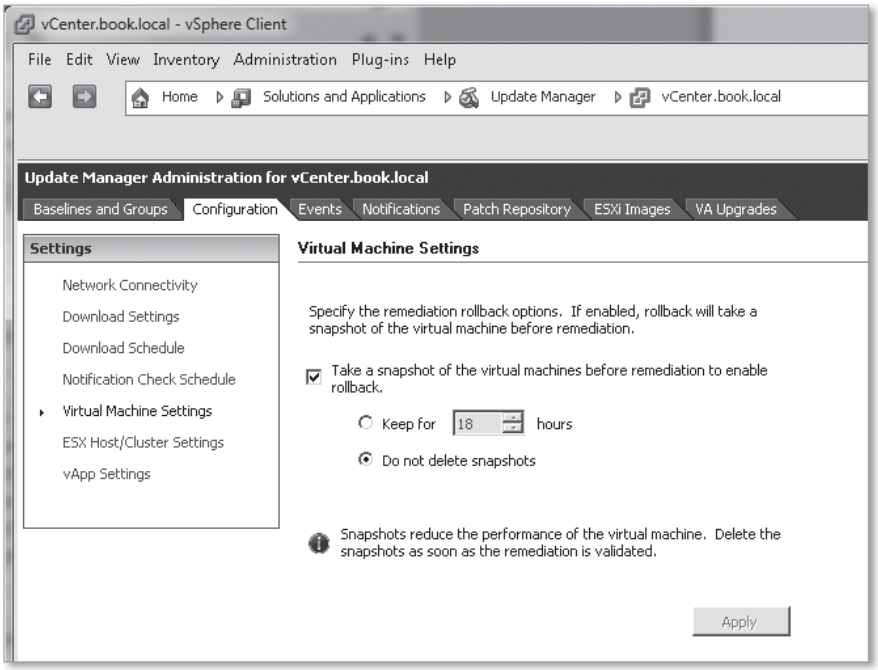


Abbildung 13.7 Einstellungen für den Gast

Im Konfigurationsfenster ist nun einstellbar, was mit dem Snapshot passieren soll. Entweder er wird angelegt und bleibt weiter aktiv, oder Sie geben ein Zeitfenster vor, nach dem er zurückgeschrieben wird. Ist das Zeitfenster optimal gewählt, dann bleibt genug Zeit, den Gast und seine Applikation zu testen und zu entscheiden, ob das Patchen erfolgreich war oder ob der Ursprungszustand wiederhergestellt werden muss.

ESX-Host-/Cluster-Einstellungen

Das Verhalten des Hosts beim Patchen parametrieren Sie unter ESX Host/Cluster Settings (Abbildung 13.8). Startet der Patch-Vorgang für einen Host, wird als Erstes versucht, den vSphere-Host in den Maintenance-Modus zu fahren. Ist das nicht möglich, kommen die Einstellungen zum Tragen, die in diesem Fenster vorgegeben wurden.

Zum Ersten ist festzulegen, was passieren soll, wenn der Host nicht in den Maintenance-Modus gefahren werden kann. Konfigurieren Sie das Wiederholintervall und die Anzahl der Wiederholungen. Andere Möglichkeiten sind, die virtuellen Maschinen in den Suspend-Modus zu versetzen (Suspend virtual Machines) oder sie herunterzufahren (Power off virtual Machines); in beiden Fällen wird danach erneut versucht, den Host zu patchen. Eine wichtige neue Funktion ist, entfernbare Geräte, die ein vMotion verhindern, temporär zu deaktivieren, damit die Arbeiten durchgeführt werden können.

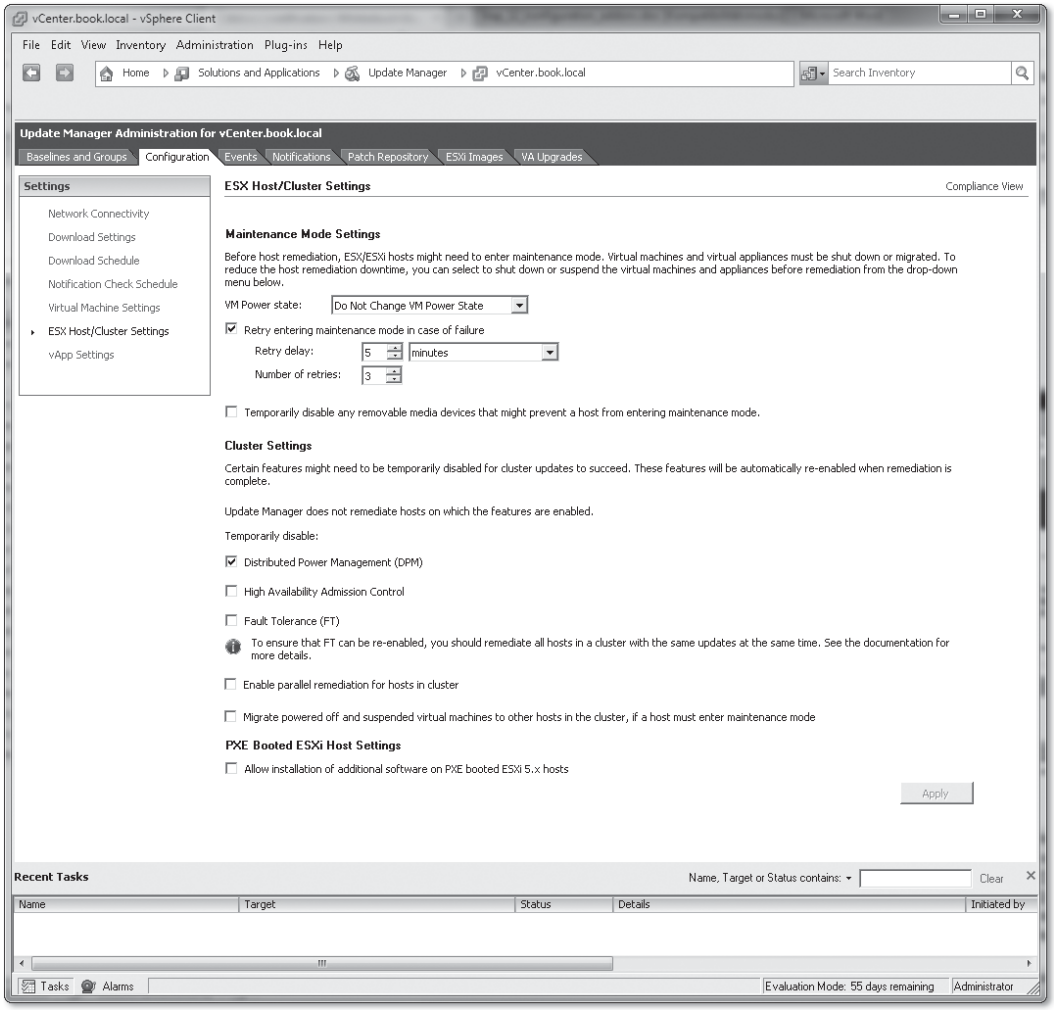


Abbildung 13.8 Konfiguration des Hosts im Update Manager

Neu hinzugekommen sind die Einstellungen für Cluster, mit denen Sie vorgeben, welche Funktionen für den Patch-Zeitraum im Cluster deaktiviert werden. Dazu zählen Distributed Power Management, High Availability Admission Control und Fault Tolerance. Das Verhalten von ausgeschalteten virtuellen Maschinen im Suspend-Modus können Sie genauso bestimmen wie das parallele Einspielen von Patches. Zusätzliche Software kann auch auf den Hosts eingespielt werden, aber nur auf solchen, die per PXE gebootet werden.

vApp-Konfiguration

Im Konfigurationsabschnitt vApp Settings bestimmen Sie, wie sich eine vApp nach dem Patchen verhält (Abbildung 13.9).

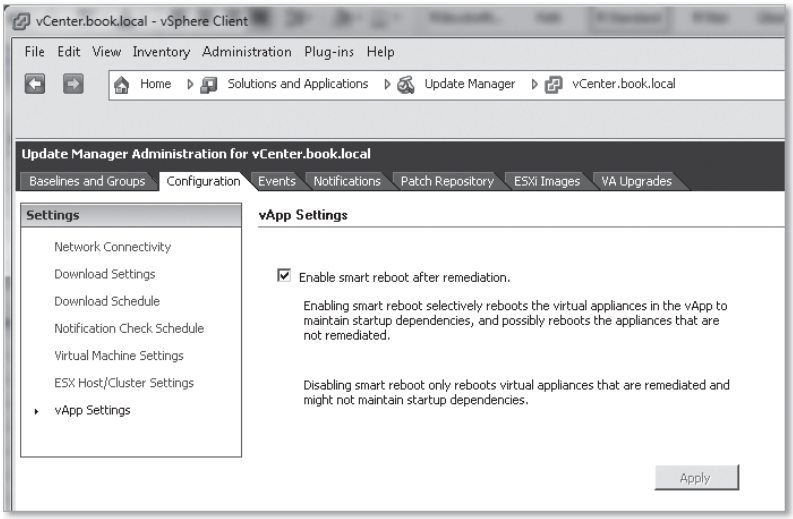


Abbildung 13.9 Verhalten einer vApp im Update Manager konfigurieren

Ist die Option ENABLE SMART REBOOT AFTER REMEDIATION aktiviert, sorgt der Update Manager dafür, dass alle von einer vApp betroffenen Appliances und VMs selektiv neu gestartet werden. Damit erreichen Sie, dass die Abhängigkeiten der Systeme untereinander eingehalten werden. Deaktivieren Sie diese Option, bleiben die Abhängigkeiten der VMs untereinander unberücksichtigt, und die VMs werden in der Reihenfolge des Patchens neu gestartet. Das kann abschließend aber dazu führen, dass die vApp nicht funktioniert, weil die Boot-Reihenfolge nicht eingehalten wurde.

13.1.3 Events

In einer großen Übersicht werden unter EVENTS alle Ereignisse aufgelistet, die mit dem Update Manager zu tun haben.

13.1.4 Notifications

Eine Liste der erzeugten Benachrichtigungen finden Sie in der Ansicht NOTIFICATIONS. Hier können Sie auch nachträglich noch einmal nachschauen, was gemeldet wurde.

13.1.5 Patch Repository

Alle Patches sehen Sie in der Anzeige PATCH REPOSITORY, und das mit verschiedenen zusätzlichen Informationen, wie z. B. die Wichtigkeit, für welche Version die einzelnen Patches sind und wann sie erschienen sind. Über das Kontextmenü können Sie sich die Eigenschaften eines Patches anzeigen lassen. Interessant ist auch die Information, welche weitergehenden Aktionen beim Einspielen diese Patches notwendig sind.

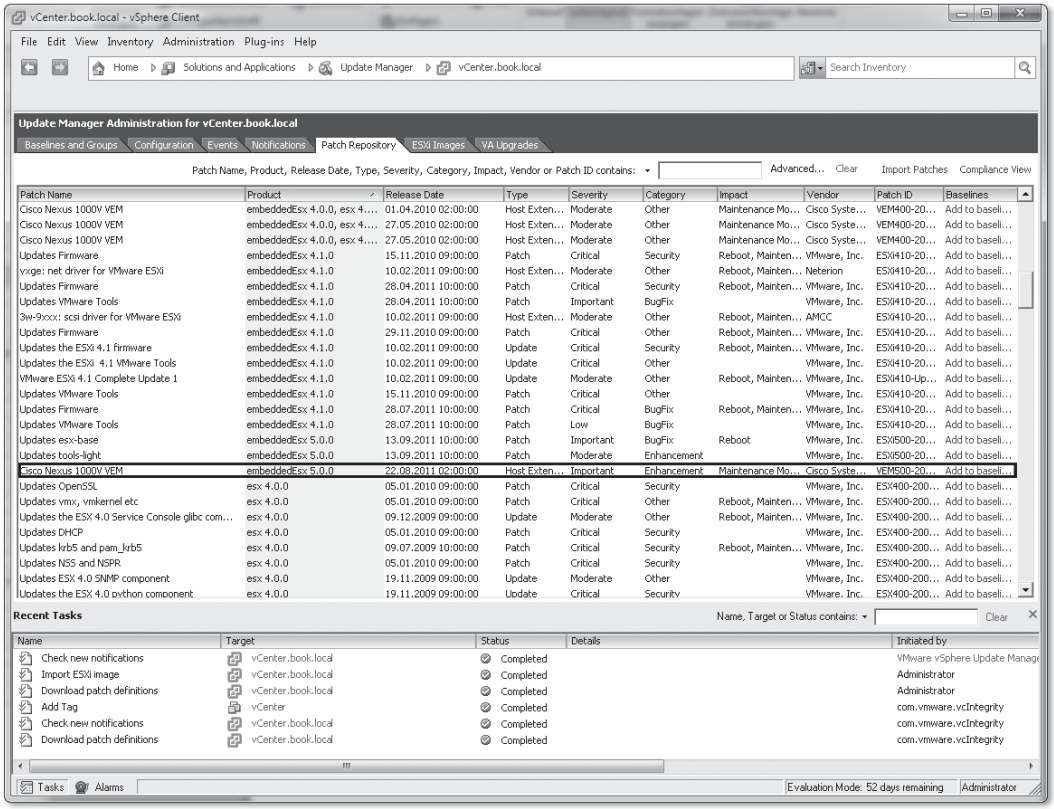


Abbildung 13.10 Patch-Repository des Update Managers

Das geht von keiner zusätzlichen Aktion über Reboot und Maintenance-Modus bis zum Restart des hostd-Dienstes. Am Ende der Zeile eines jeden Patches können Sie diesen einer Baseline hinzufügen. Diese wiederum kann dann zum Patchen genutzt werden.

13.1.6 ESXi Images

Haben Sie im vorhergehenden Reiter die Patches gesehen, werden im folgenden Reiter alle ESXi Images angezeigt, die im System zu finden sind. Dabei ist die Anzeige zweigeteilt. Im oberen Teil finden Sie das importierte Installations-Image und im unteren Teil die enthaltenen Softwarepakete und Treiber.

Die Informationen ähneln denen, die Sie als Ausgabe bekommen, wenn Sie sich im PowerCLI mit dem Befehl `Get-EsxSoftwarePackages` die Softwarepakete eines Images anzeigen lassen. Sie finden hier die Version, den Hersteller, das Acceptance-Level, das Release-Datum und die Größe des Softwarepakets. Weitere Manipulationen können Sie hier nicht vornehmen. Einzig beim Import müssen Sie das Image direkt einer Baseline zuweisen.

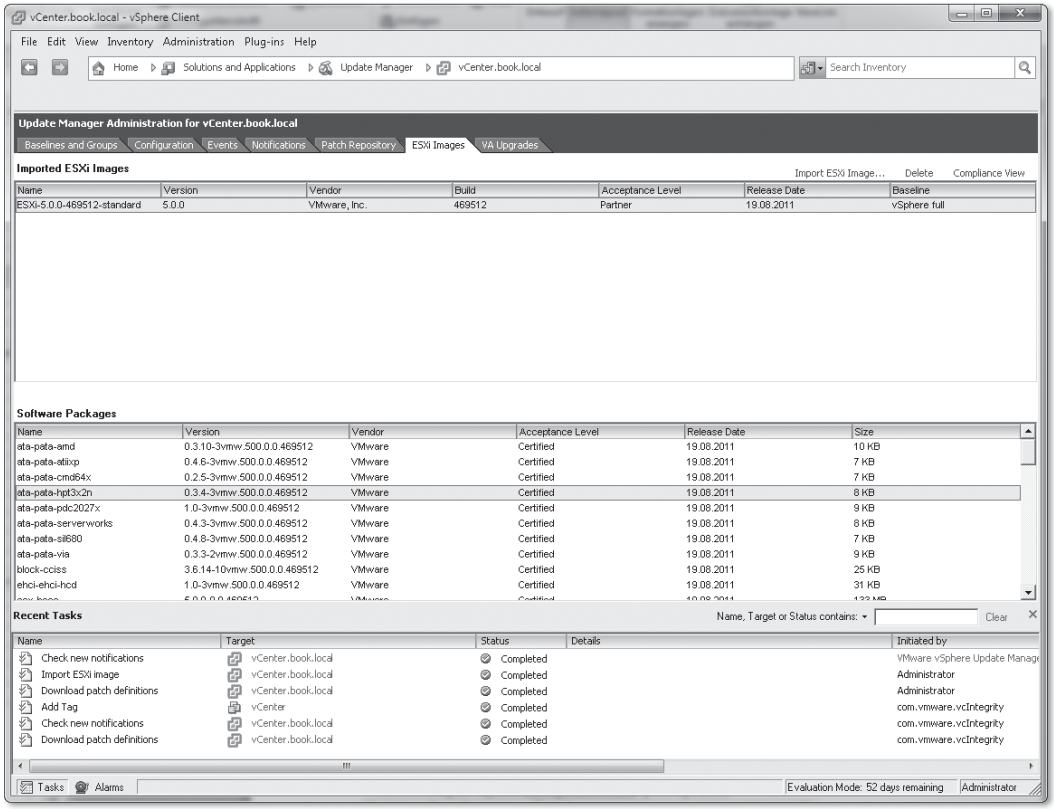


Abbildung 13.11 Anzeige der ESXi-Images

13.1.7 VA Upgrades

Neu mit der Version 5.x ist die Funktion des Patchens von Virtual Appliances (VA). Alle Informationen zu den Aktualisierungen der VAs haben hier ihre Heimat.

13.1.8 Download von Updates

Nachdem Sie alle nötigen Einstellungen vorgenommen haben, können Sie die Updates herunterladen. Dies geschieht am einfachsten über den dafür angelegten Scheduled Task. Mit Rechtsklick auf diesen Task und Auswahl von Run führen Sie ihn aus. Anschließend werden die Updates direkt heruntergeladen (Abbildung 13.12).

Jetzt wird ein Task im Fenster der Recent Tasks gestartet. Hier erkennen Sie, dass der Update Manager Patches herunterlädt (Abbildung 13.13).

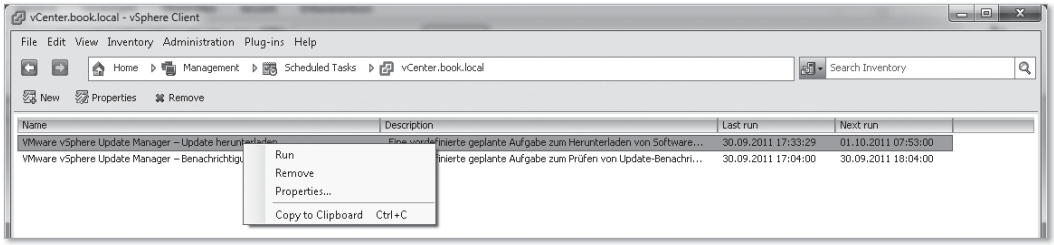


Abbildung 13.12 VMware Update Manager – Download der Patches

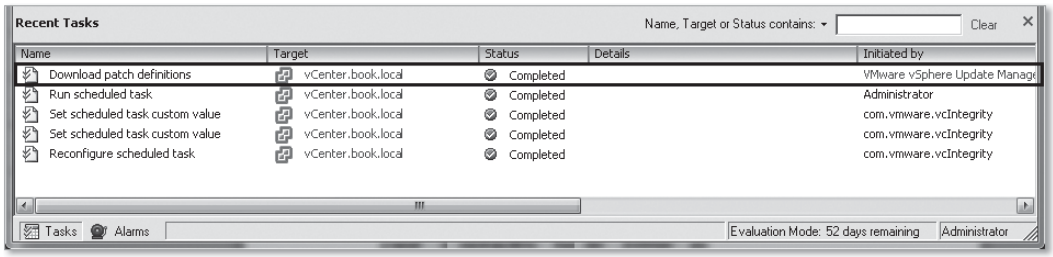


Abbildung 13.13 VMware Update Manager – Task: Download der Patches

Wird der Task zum ersten Mal angestoßen, kann der Vorgang ziemlich lange dauern, je nachdem, welche Patches heruntergeladen werden müssen.

13.1.9 Download von Updates auf Offline-Update-Manager

Zum Herunterladen von Patches auf einen dedizierten Download-Server müssen Sie auf jeden Fall die Kommandozeile bemühen. Zuerst müssen Sie aber die Applikation installieren. Dazu gehen Sie auf das Installationsmedium vom vCenter Server in das Unterverzeichnis *umds*. Dort rufen Sie Datei *VMware-UMDS.exe* auf und führen die Installation durch. Für den Download-Manager gibt es keine GUI. Damit die Routinen einwandfrei funktionieren, sind die Befehle im Programmverzeichnis abzusetzen. Für Sie sind zwei Dateien wichtig: die ausführbare Datei *vmware-umds.exe* und das Konfigurations-File *downloadConfig.xml*.

Der Download-Manager muss auf einem dedizierten Server installiert werden, es darf kein VMware Update Manager auf der Maschine installiert sein. Beide Systeme schließen einander aus!

Die verschiedenen Aufrufparameter der *vmware-umds.exe*-Datei finden Sie in Abbildung 13.14.

Es gibt zwei Wege, zu bestimmen, welche Patches heruntergeladen werden sollen:

1. Parametrierung der Downloads über die Kommandozeile
2. Einschränkung der Downloads durch Anpassen der Konfigurationsdatei

Abbildung 13.14 Befehlsparameter von »vmware-umds.exe«

Im Handbuch wird nur die Nutzung der Kommandozeile beschrieben. Die Befehle für das Deaktivieren des Downloads von ESX-/ESXi 3.x-Patches sehen wie folgt aus:

```
vmware-umds.exe -S -enable-hosts
vmware-umds.exe -S -d esx-3.5.0 embeddedEsx-3.5.0
```

Mit der Kommandozeile können Sie die Konfiguration weiter anpassen. Der einfachere Weg aber ist das Anpassen der Konfigurationsdatei; hier können Sie die Einschränkungen ebenfalls konfigurieren.

In der Konfigurationsdatei (*downloadConfig.xml*) lassen sich die Anpassungen auch manuell vornehmen. Sollen z. B. keine ESX 3.x-Patches heruntergeladen werden, weil Sie eine reine

vSphere-Umgebung haben, entfernen Sie einfach die Zeile `<ESX3xUpdateUrl>...` Schon werden beim Download nur noch Patches für vSphere ab Version 4 berücksichtigt.

```
<Config>
      <patchStore>C:\ProgramData\VMware\VMware Update Manager\Data\
      </patchStore>
      <exportStore></exportStore>
      <proxySettings>
            <useProxyServer></useProxyServer>
            <!-- true -->
            <proxyServer></proxyServer>
            <!-- proxy.vmware.com -->
            <proxyPort></proxyPort>
            <!-- 3128 -->
      </proxySettings>
      <contentSettings>
            <hostInclude id="0001">embeddedEsx-4.0.0-INTL</hostInclude>
            <hostInclude id="0002">embeddedEsx-4.1.0-INTL</hostInclude>
            <hostInclude id="0003">esx-4.1.0-INTL</hostInclude>
            <hostInclude id="0004">embeddedEsx-5.0.0-INTL</hostInclude>
            <hostInclude id="0005">esx-3.5.0-INTL</hostInclude>
            <hostInclude id="0006">embeddedEsx-3.5.0-INTL</hostInclude>
            <hostInclude id="0008">esx-4.0.0-INTL</hostInclude>
            <hostUpdateEnabled>true</hostUpdateEnabled>
            <vaUpgradeEnabled>true</vaUpgradeEnabled>
      </contentSettings>
      <langs>ENU</langs>
      <vaConfig>
            <vaUpgradeUrl id="1">http://vapp-updates.vmware.com/vai-catalog/
            index.xml</vaUpgradeUrl>
      </vaConfig>
      <HostConfig>
            <ESX3xUpdateUrl>https://www.vmware.com/PatchManagementSystem/
            patchmanagement</ESX3xUpdateUrl>
            <ESX4xUpdateUrl>https://hostupdate.vmware.com/software/VUM/
            PRODUCTION/main/vmw-depot-index.xml</ESX4xUpdateUrl>
            <ESXThirdPartyUpdateUrl id="1">https://hostupdate.vmware.com/
            software/VUM/PRODUCTION/csco-main/csco-depot-index.xml
            </ESXThirdPartyUpdateUrl>
            <!-- ESXThirdPartyUpdateUrl id="url3">http://foo.com/index.xml
            </ESXThirdPartyUpdateUrl -->
      </HostConfig>
      <database>
            <initialConnections>8</initialConnections>
            <maxConnections>8</maxConnections>
      </database>
```

```
    <log>
        <name>vmware-downloadService</name>
        <level>verbose</level>
        <memoryLevel>error</memoryLevel>
        <outputToConsole>false</outputToConsole>
        <components>
            <lib.vdb.vdbStatement>
                <level>info</level>
            </lib.vdb.vdbStatement>
            <lib.vdb.vdb>
                <level>info</level>
            </lib.vdb.vdb>
        </components>
    </log>
</Config>
```

In Abbildung 13.15 finden Sie noch ein paar weitere Beispiele für den Download-Manager.

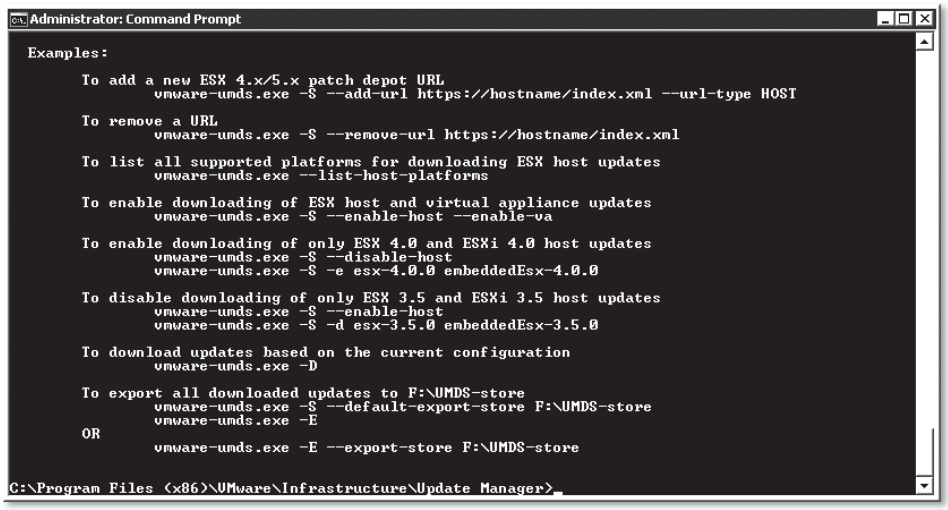


Abbildung 13.15 Beispiele für »vmware-udms.exe«

Als Nächstes können Sie die Updates herunterladen. Dies stoßen Sie mit dem Befehl `vmware-udms -download` an. Ist der Job abgeschlossen, befinden sich die gewünschten Patches im zugehörigen Verzeichnis, das Sie während der Installation als Patch-Repository angegeben haben. Exportieren Sie das Patch-Repository mit dem Befehl `vmware-cmd --export -export-store <Pfad>`.

Wesentlich mehr Funktionen stellt das Tool nicht zur Verfügung, außer den Optionen, einen erneuten Download von Patches anzustoßen oder nur die Patches erneut herunterzuladen, die korrupt sind. Diese Option sollten Sie nur nutzen, wenn das Datenverzeichnis des Update Managers korrupt ist.

Abschließend sind die Patches noch auf dem vCenter-Server zu importieren (Abbildung 13.16). Das erfolgt über das vCenter selbst.

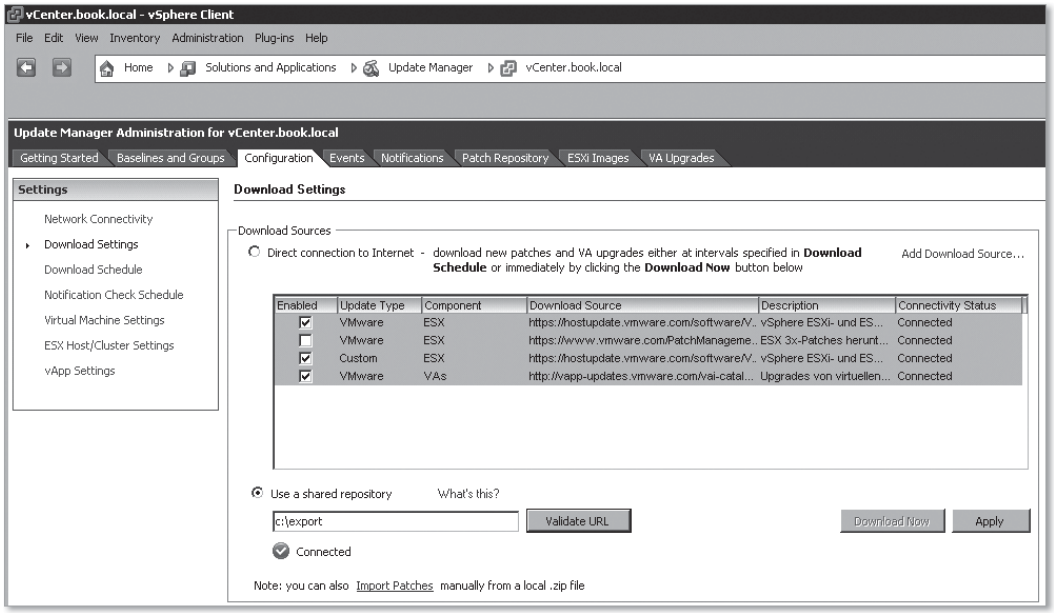


Abbildung 13.16 Import von Patches aus einer externen Quelle

Bitte beachten Sie, dass Sie das Importverzeichnis nicht löschen dürfen. Beim Import der Patches werden nur die Metadaten in das Patch-Verzeichnis kopiert, die Patches selbst verbleiben im Verzeichnis der Importquelle. Ist der Import abgeschlossen, sind die importierten Patches im Repository sichtbar und können genutzt werden (Abbildung 13.17).

Unter dem Punkt Recent Tasks ist der erfolgreiche Importjob noch sichtbar. Nachdem die Patches nun im System hinterlegt sind, können Sie mit den weiterführenden Arbeiten beginnen.

13.1.10 Baselines

Erstellung einer Baseline

Damit die Updates angewandt werden können, müssen Sie eine sogenannte *Baseline* erstellen. Diese Baseline legen Sie im Menü des Update Managers an und weisen sie später einem bestimmten Objekt im Inventory des vCenters zu. So ist es möglich, eine Baseline für die vSphere-Hosts zu erstellen und sie dann entweder einem Datacenter, einem Ordner oder einem einzelnen Host zuzuordnen.

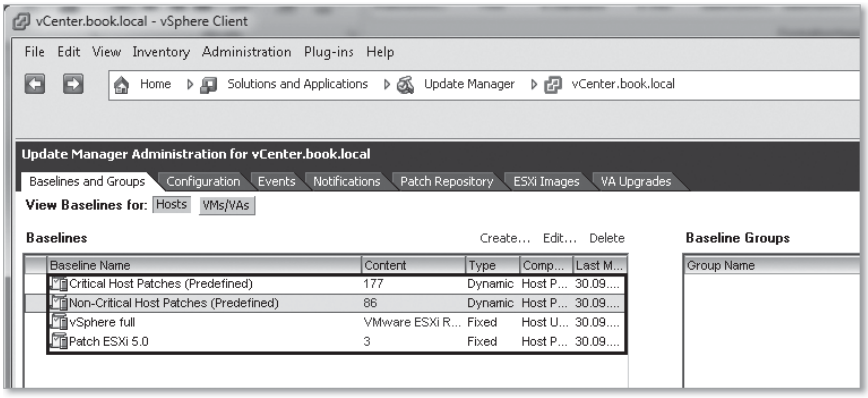


Abbildung 13.17 vCenter-Update-Manager-Baselines

Nach der Installation des vCenter Update Managers stehen bereits zwei Baselines zur Verfügung (in der Auswahl Hosts), eine für kritische und eine für unkritische Patches. In der Ansicht VMs/VAs sehen Sie drei Baselines: eine für die Aktualisierung der VMware Tools, eine für die Aktualisierung der virtuellen Hardware und die dritte für das Upgrade von Virtual Appliances.

Interessant ist die Möglichkeit, eine Baseline zu erstellen, die nicht alle verfügbaren Patches enthält, sondern die Funktionsupdates ausschließt. Somit spielen Sie beim Patchen der Hosts nur die Korrekturen ein. Im umgekehrten Fall besteht die Option, nur Funktionserweiterungen zu installieren. So trennen Sie Patches und Updates und können sie unabhängig voneinander anwenden.

Zur Erstellung einer neuen Baseline dient der Create-Link im Fenster Baselines and Groups des Update Managers. Daraufhin startet ein Wizard, der Sie durch das Erstellen einer neuen Baseline führt (Abbildung 13.18).

Der Dialog stellt vier verschiedene Optionen für das Anlegen einer Baseline zur Auswahl: Host Patch, Host Extension, Host Upgrade und VA Upgrade. Die Baseline für den Host Patch kann einen Fixed-Status bekommen. In diesem Fall werden die Patches aus dem Repository fest zugeordnet. Am Status der Regel wird sich zukünftig nichts ändern. Im Gegensatz dazu steht der Status Dynamic: Bei der Erstellung werden die Regeln dynamisch erstellt. Das bedeutet, dass alle neu heruntergeladenen Patches, die der Auswahl entsprechen, automatisch zur Baseline hinzugefügt werden. Dabei ist es unerheblich, ob Patches schon vorhanden sind oder zukünftig heruntergeladen werden.

In unserem Beispiel erstellen wir zwei Baselines, die nur Patches für die Version ESXi 4.0 enthält, getrennt nach Firmwareupdates und Patches. Nach der Auswahl des Fixed-Modus zeigt der Wizard das Fenster, in dem Sie die Patches der Baseline hinzufügen können (Abbildung 13.19). Das Hinzufügen von Patches erfolgt im oberen Fenster über das Kontextmenü, abgewählt wird im unteren Fenster ebenfalls über das Kontextmenü.

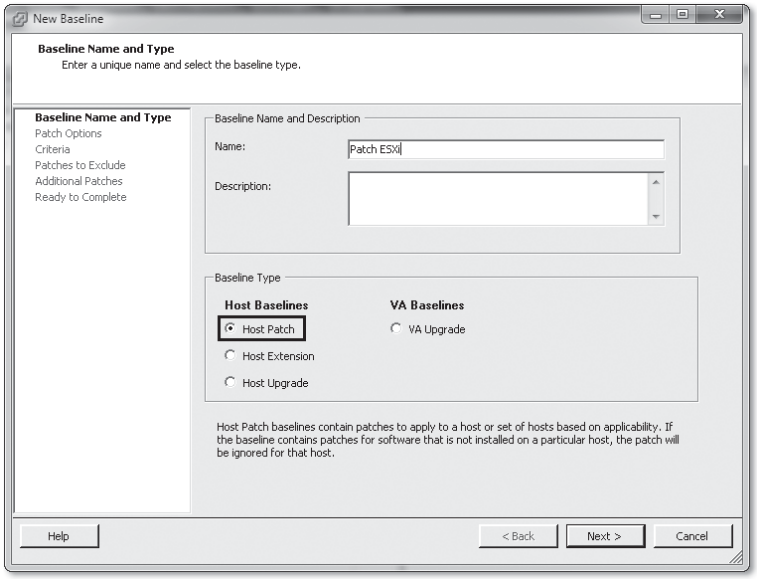


Abbildung 13.18 Erstellen einer neuen Baseline

Öffnen Sie einen Patch per Doppelklick, um den zugehörigen Knowledge-Base-Artikel zu lesen. Voraussetzung dafür ist aber ein funktionierender Internetzugang.

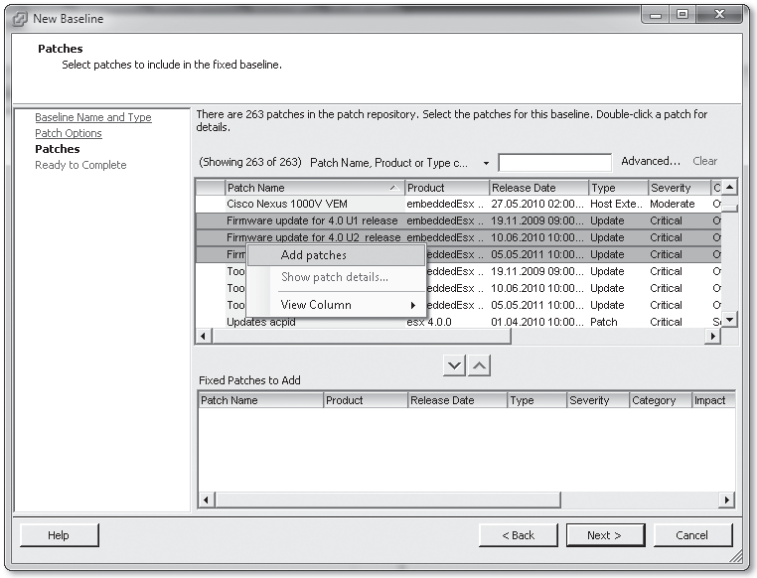


Abbildung 13.19 Aufnahme der Patches in die Baseline

Wären wir den Weg über die dynamische Baseline gegangen, würde sich der Dialog darstellen wie in Abbildung 13.20.

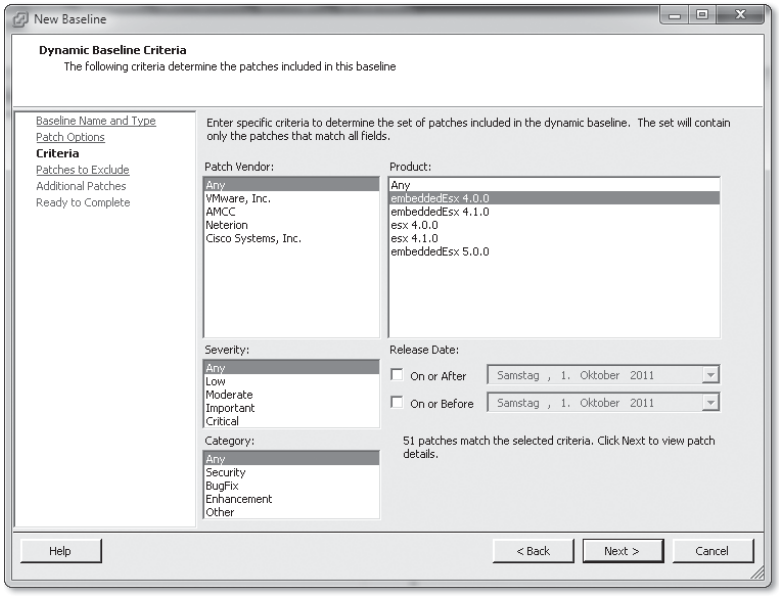


Abbildung 13.20 Erstellung einer dynamischen Baseline

Die Reduzierung der Auswahl auf Firmware-Patches erfolgt im nächsten Fenster über ein Suchkriterium.

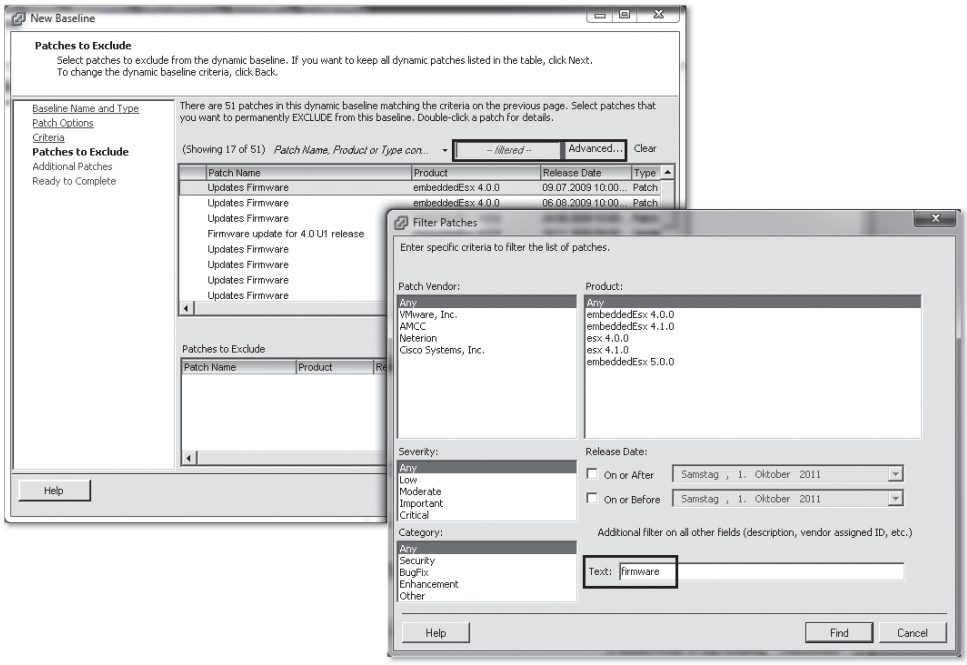


Abbildung 13.21 Auswahlreduzierung über Suchkriterium

Hier sehen Sie sehr schön den Unterschied: Die Baseline ordnet die Patches automatisch zu. Es werden nur Dateien hinzugewählt, die für ESXi bestimmt sind und im Namen das Wort »Firmware« enthalten. Den Filter mit den Inkludierungsoptionen erreichen Sie über den ADVANCED-Link. Im Feld links daneben wird Ihnen angezeigt, dass eine Filteroption gesetzt ist.

Aber zurück zu unserem Beispiel. Nachdem wir noch eine zweite Baseline für die Firmware erstellt haben, zeigt sich das Übersichtsfenster wie in Abbildung 13.22.

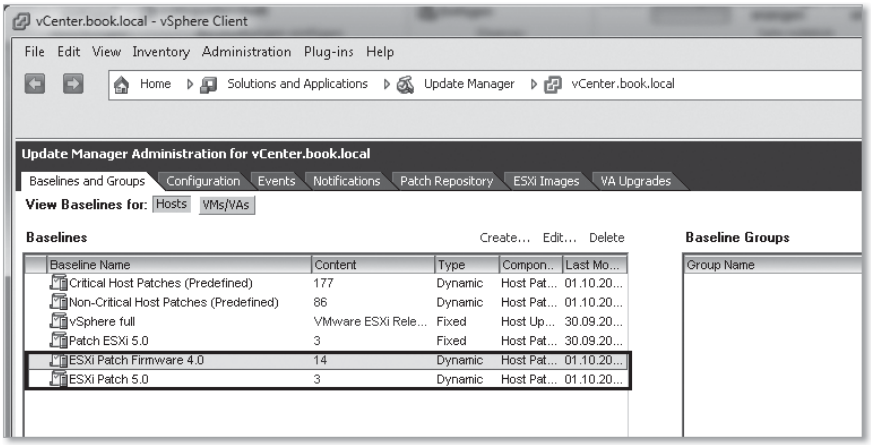


Abbildung 13.22 Erstellte Baselines

Der Vollständigkeit halber möchten wir erwähnen, dass zuvor noch zwei weitere dynamische Baselines erstellt wurden sind, die Sie ebenfalls in der Abbildung sehen.

Erstellung einer Baseline-Gruppe

Auch wenn es möglich ist, die erstellten Baselines direkt an einen oder mehrere Hosts zu binden, bietet der Update Manager eine weitere Möglichkeit der Gruppierung: In *Baseline-Gruppen* können Sie wiederum Patch- und/oder Upgrade-Baselines zusammenfassen. Tun Sie sich selbst und Ihren Kollegen einen Gefallen, und entscheiden Sie sich für eine durchgehende Strategie. Entweder binden Sie Patch- und/oder Upgrade-Baselines an zu patchende Objekte, oder Sie nutzen Gruppen, aber vermischen Sie nicht beides – das wird definitiv unübersichtlich.

Abschließend legen Sie eine Baseline-Gruppe an, in der Sie alle Patches für die ESXi-Systeme sammeln. Über den CREATE-Link erreichen Sie den Dialog zur Erstellung der Gruppe. Im ersten Fenster wird nur der Name abgefragt, und Sie müssen angeben, ob Sie Host-Systeme oder andere Systeme gruppieren wollen. Das Zuordnen der Patches zur Gruppe erfolgt anschließend (Abbildung 13.23), bevor Sie den Dialog schließen.

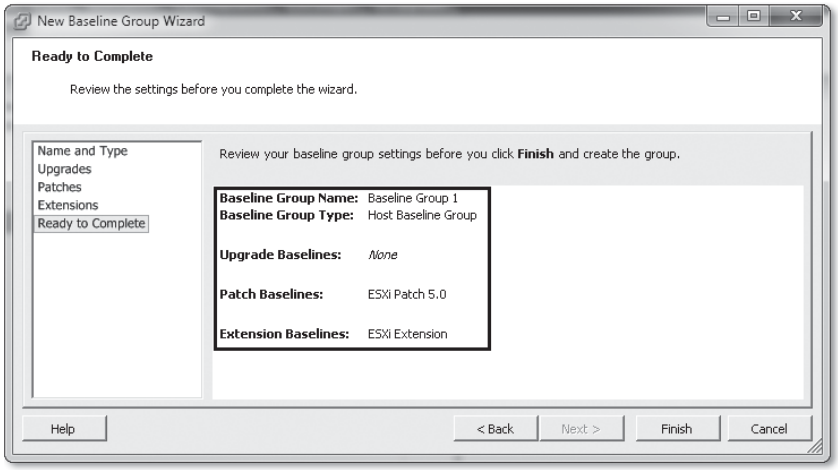


Abbildung 13.23 Zuordnung von Patches zur Gruppe

Hiermit sind die Arbeiten abgeschlossen, und es ist nun möglich, mit den Baselines zu arbeiten.

Arbeiten mit Baselines

Nach den vorbereitenden Arbeiten können Sie die Baseline-Gruppe mit einem Host verbinden (Abbildung 13.24).

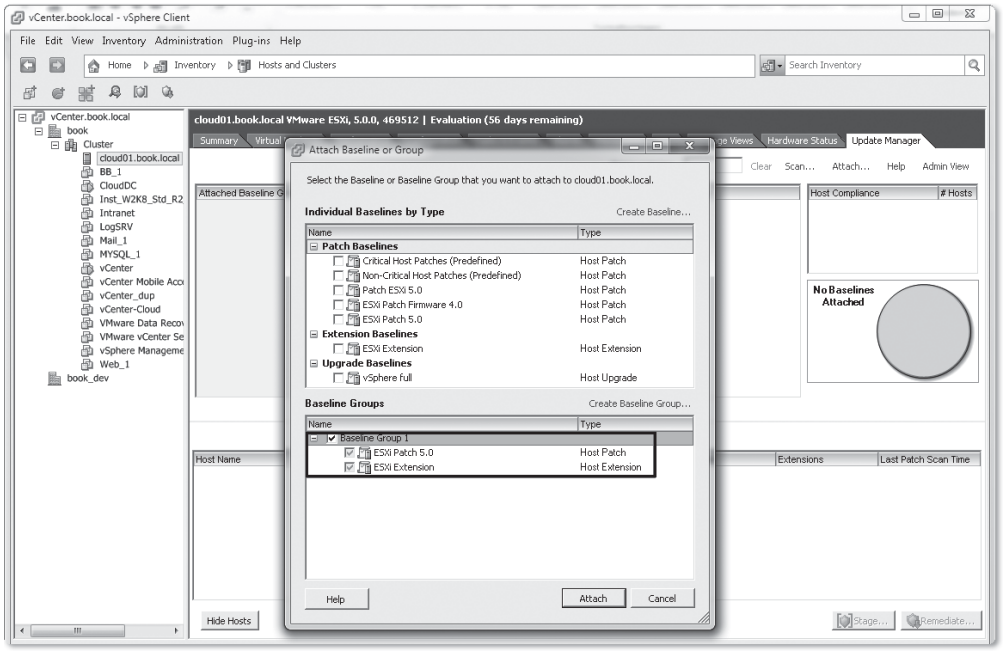


Abbildung 13.24 Verknüpfung von Host und Baseline

An erster Stelle steht die Auswahl eines Hosts oder Clusters; auf dem Reiter des Update Managers erzeugen Sie dann über den Attach-Link eine Verknüpfung zwischen Host und Baseline. Anschließend wird sofort gezeigt, ob der Host compliant ist oder nicht (Abbildung 13.25).

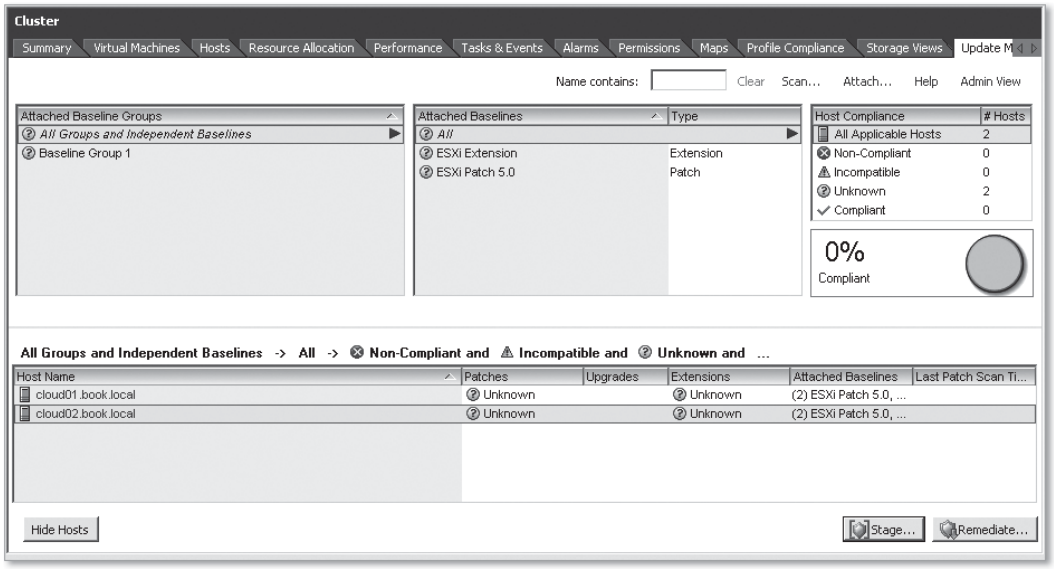


Abbildung 13.25 Compliance-Status

Es ist nicht schwer zu erkennen, dass der Host Patches benötigt, damit er auf dem aktuellen Stand ist.

Doch bevor wir die Patches einspielen – was übrigens über den Remediate-Button geschieht –, möchten wir kurz auf den Stage-Button eingehen. Dieser sorgt dafür, dass die Patches auf die zu patchende Maschine geladen werden. Der eigentliche Patch-Vorgang läuft dann wesentlich schneller ab.

Starten Sie den Patch-Vorgang jetzt, wird angezeigt, welche Baselines mit dem Host verknüpft sind. Es folgt eine Zusammenfassung aller zur Anwendung kommenden Patches mit der Möglichkeit, einzelne zu entfernen. Legen Sie nun fest, ob der Task sofort startet oder ob er zu einem bestimmten Zeitpunkt automatisch die Patch-Arbeiten durchführt. Ist die Aktion angestoßen, stellt sich das vCenter dar wie in Abbildung 13.26.

Hier ist schön zu sehen, dass der Host zuerst automatisch in den Maintenance-Modus gefahren wird, bevor die Patch-Arbeiten beginnen. Nach dem Abschluss der Arbeiten erfolgt ein automatischer Reboot. Ist das System wieder erreichbar, wird erneut ein Compliance-Check angestoßen. Waren die Patch-Arbeiten erfolgreich, zeigt sich das an dem großen grünen Button auf der Update-Manager-Seite.

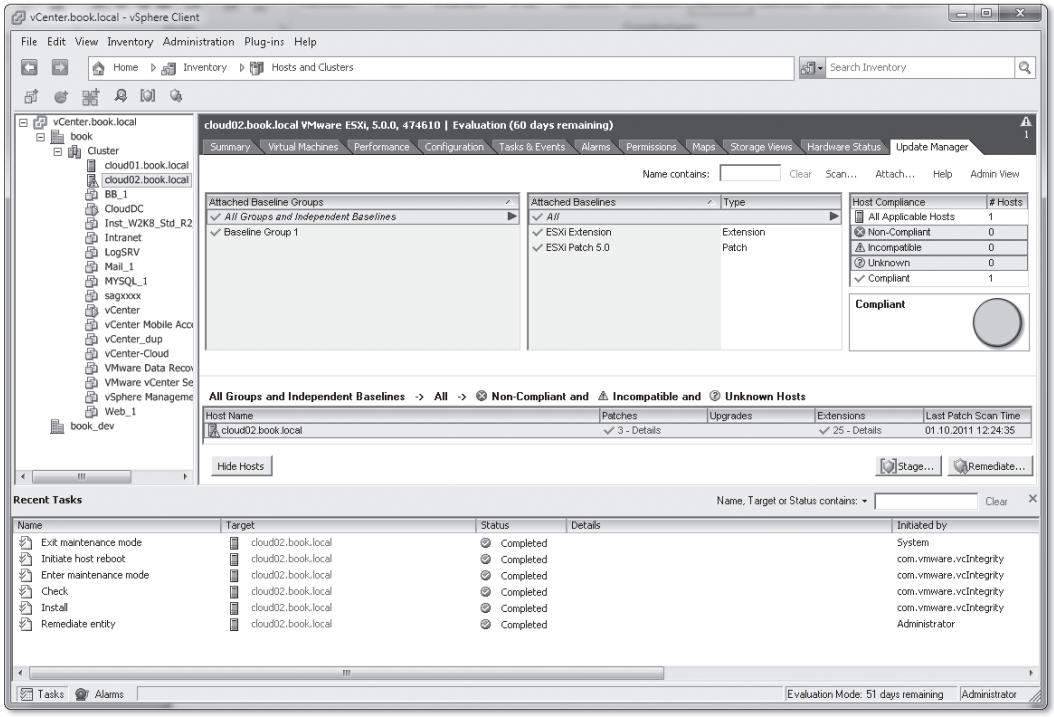


Abbildung 13.26 Patch-Status

Nur keine Angst vor dem Patchen von kompletten Clustern. Es werden natürlich nicht alle Systeme auf einmal gepatcht, sondern nach und nach. Zur Unterstützung wird die Funktion vMotion eingesetzt. Das Patchen beginnt so z. B. mit dem ersten Host. Durch die Aktivierung des Maintenance-Modus werden die laufenden VMs evakuiert und auf die restlichen betriebsbereiten vSphere-Hosts verschoben. Nach dem Abschluss der Patch-Arbeiten wird der Maintenance-Modus automatisch wieder deaktiviert, und der Host kann wieder virtuelle Maschinen aufnehmen. Erst jetzt wird mit dem nächsten Host begonnen. Es bleiben immer so viele Ressourcen frei, wie nötig sind, damit die Leistung der VMs nicht beeinflusst wird. Sie können das aber auch anders einstellen. Das sollten Sie aber nur dann tun, wenn Sie virtuelle Maschinen haben, die durch die Fault-Tolerance-Option ausfallsicher gestaltet werden.

Status einer Baseline und ihrer Objekte

Jede Baseline, die zugewiesen wurde, hat einen bestimmten Status. Dieser hängt davon ab, welchen Status die verknüpften Systeme haben. Es wird der Zustand von einzelnen Hosts angezeigt, es gibt aber auch eine Zusammenfassung, die über den Gesamtstatus informiert und auch grafisch aufbereitet ist (Abbildung 13.27).

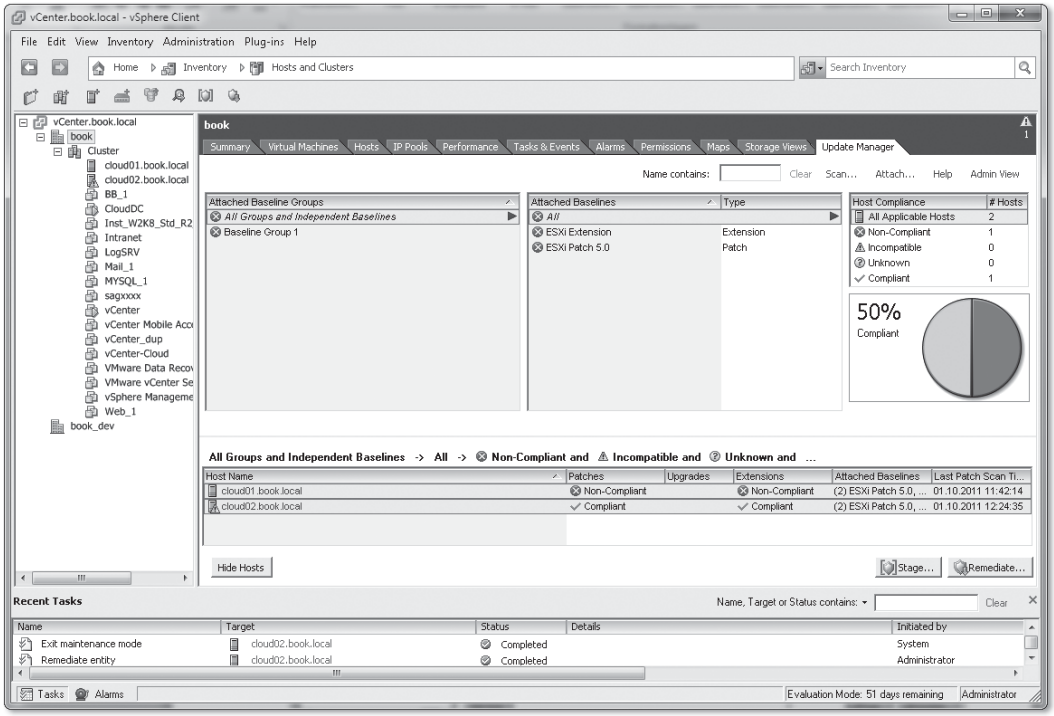


Abbildung 13.27 vCenter-Update-Manager-Status

Sollten Maschinen unter der Spalte UNKNOWN angezeigt werden, müssen Sie einen Scan durchführen, um zu überprüfen, welche Patches installiert wurden. Dazu starten Sie einen SCAN-Task über den entsprechenden Link oder über das Kontextmenü von Host oder Cluster – der dritte Punkt von unten, SCAN FOR UPDATES, führt ebenfalls einen Scan durch.

Update der VMware Tools

Auch mit dieser Version des Update Managers können Sie die VMware Tools und die virtuelle Hardware der virtuellen Maschinen aktualisieren.

Diese Funktion werden vor allem diejenigen zu schätzen wissen, die ein größeres Upgrade vor der Brust haben. Da der Upgrade Manager auch das Upgrade des Hosts unterstützt, können Sie den kompletten Upgradepfad über den Update Manager beschreiten und haben eine zentrale Konsole, die den aktuellen Status dokumentiert.

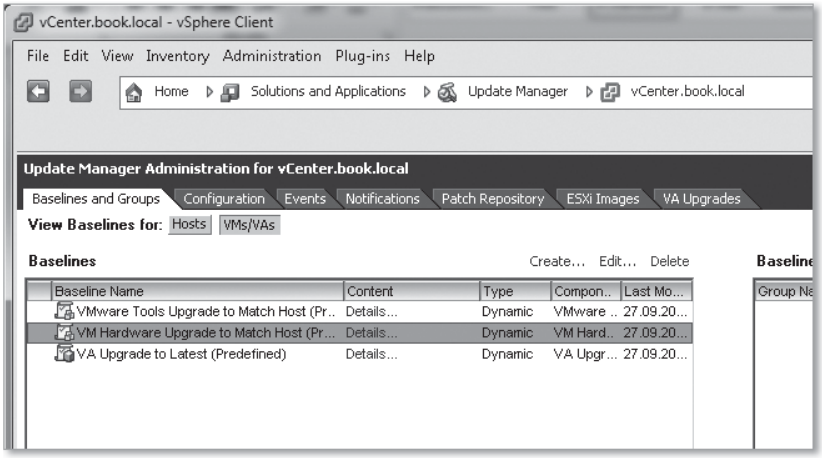


Abbildung 13.28 Vordefinierte Baselines zur Aktualisierung der VMware Tools und virtueller Hardware

13.1.11 Weitere Konfigurationsmöglichkeiten

Manchmal findet man noch so das ein oder andere, wenn man sich direkt im Filesystem bewegt. Bei der Suche nach dem Kommandozeilentool für den Download-Manager ist uns eine Datei aufgefallen, deren Funktion wir Ihnen nicht vorenthalten möchten: Nach dem Aufruf der Datei *C:\Program Files (x86)\VMware\Infrastructure\Update Manager\VMwareUpdateManagerUtility.exe* öffnet sich ein Fenster, das dem Startbildschirm des vSphere-Clients stark ähnelt.

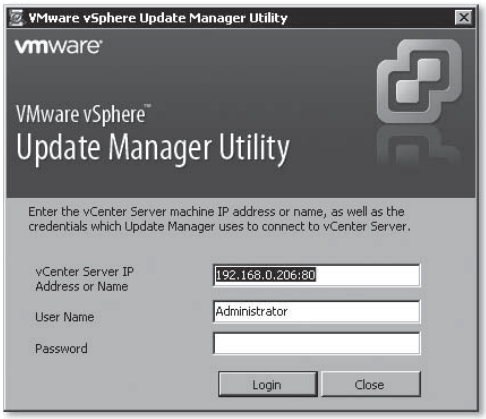


Abbildung 13.29 Anmeldung beim Update Manager Utility

Nach der Anmeldung zeigt sich ein Fenster, das dazu dient, die Konfiguration des VMware Update Managers anzupassen.

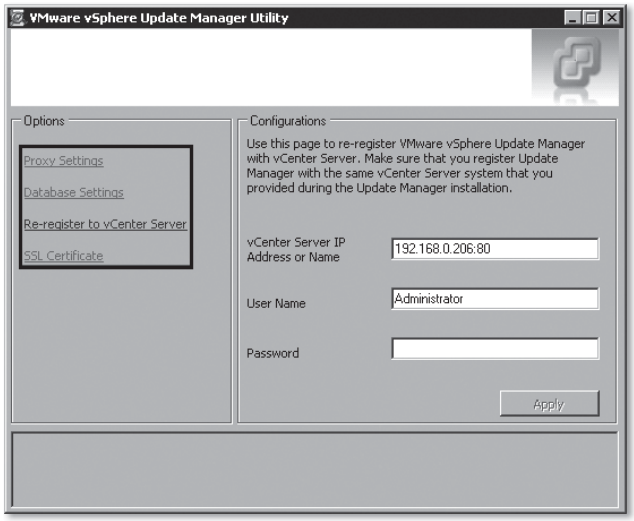


Abbildung 13.30 Nachträgliche Konfiguration des VMware Update Managers

Sie können hier Dinge konfigurieren, die direkt über das vCenter nicht einstellbar sind. Einzig die Proxy-Einstellungen können Sie auch direkt über das vCenter umkonfigurieren. Alle anderen Einstellungen sind nur hier parametrierbar. Das betrifft die Verbindung zur Datenbank, das SSL-Zertifikat und die Registrierung des Update Managers am vCenter-Server.

Im gleichen Verzeichnis befindet sich außerdem ein Kommandozeilen-Tool: der Befehl *vmware-vcicli.exe*. Eine detaillierte Dokumentation zu dem Tool haben wir nicht gefunden; sollten Sie das Tool nutzen wollen, müssen Sie sich durch die Optionen kämpfen, die angezeigt werden, wenn Sie den Befehl ohne Parameter aufrufen. Auf dem Installationsmedium des vCenter Servers finden Sie im Unterverzeichnis für den Update Manager eine Beispieldatei, die Sie nutzen können, wenn Sie den Update Manager unbeaufsichtigt installieren wollen. Dieses Skript trägt den Namen *vci_install.cmd*.

13.2 VMware vCenter Linked Mode

Mit der Einführung des Linked Modes beim vCenter-Server ist es möglich, mehrere vCenter-Server miteinander zu verbinden, so dass Sie einen Single Point of Contact für die Anmeldung haben. Das heißt, dass Sie sich an einem vCenter-Server anmelden und damit auch die verlinkten Hosts und virtuellen Maschinen administrieren können, ohne sich an jeder Infrastruktur extra anmelden zu müssen. Diese Verlinkung nehmen Sie entweder direkt bei der Installation vor – es ist nur der entsprechende Menüpunkt zu Beginn der Installation aufzurufen –, oder Sie stoßen sie nachträglich über das Start-Menü unter Start • Programme • VMware vCenter Server Linked Mode Configuration an (Abbildung 13.31).

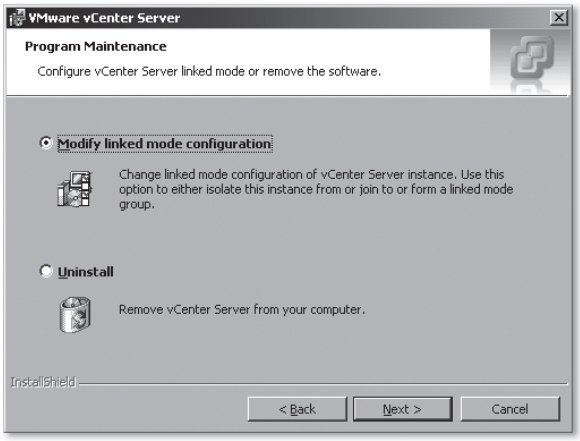


Abbildung 13.31 Einrichtung des Linked Modes für vCenter-Server

Wichtige Voraussetzung ist, dass der vCenter-Server Mitglied einer Domäne ist. Diese Mitgliedschaft sollten Sie vor der vCenter-Installation einrichten. Möchten Sie vCenter-Server miteinander verlinken, die nicht Mitglied derselben Domäne sind, wird ein Two-Way-Trust zwischen den Domänen der vCenter-Server benötigt. Außerdem ist es äußerst wichtig, dass die Namensauflösung in beiden Richtungen funktioniert; andernfalls bricht die Installation ab.

Ist der Punkt für die Verlinkung von vCenter-Servern ausgewählt, haben Sie im folgenden Schritt die Option, das vCenter zu verlinken oder es wieder zu isolieren (Abbildung 13.32).

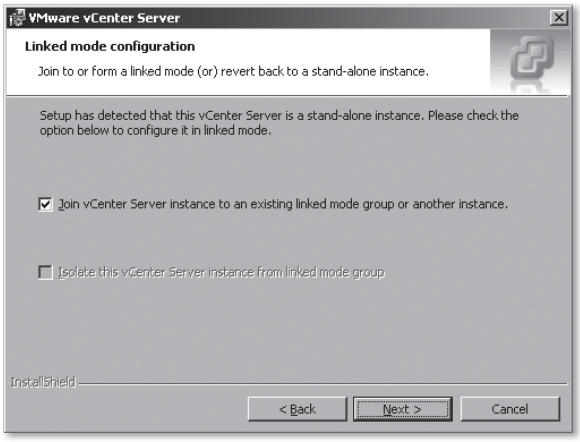


Abbildung 13.32 Verlinkungsoptionen für vCenter-Server

Der folgende Dialog erwartet die Eingabe des Servers, mit dem dieses vCenter verlinkt werden soll. Vorher bekommen Sie aber noch einen Hinweis, welche Versionen miteinander verlinkt werden können.

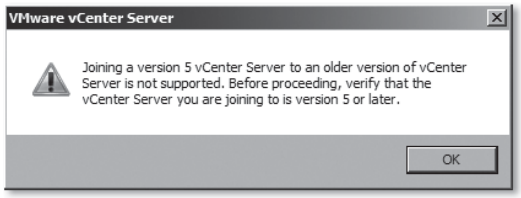


Abbildung 13.33 Verlinkungsmöglichkeiten

Eine Portangabe ist ebenfalls nötig, und auch hierbei kann es keine Kollision mit den anderen vCenter-Portkonfigurationen geben, wenn Sie vom Standard nicht abgewichen sind (Abbildung 13.34).

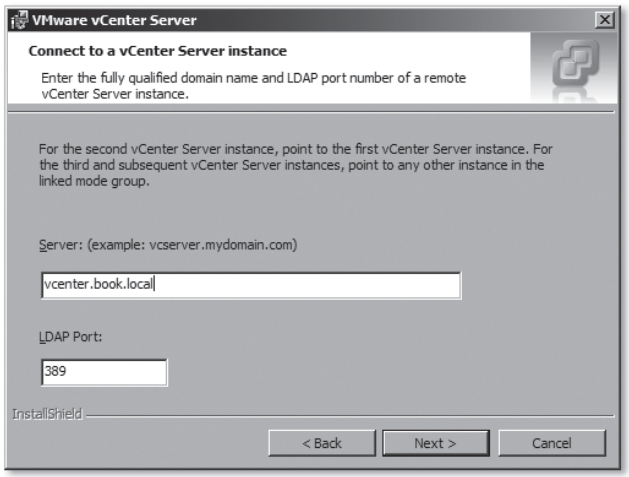


Abbildung 13.34 Angabe des Verlinkungsziels mit Port

Haben Sie das Ziel festgelegt und den NEXT-Button gedrückt, führt die Installationsroutine einige Überprüfungen durch. Probleme werden Sie auf jeden Fall bekommen, wenn die Uhrzeiten der beiden betroffenen vCenter-Server nicht abgeglichen sind. Sie werden dann mit der Fehlermeldung aus Abbildung 13.35 »belohnt«.

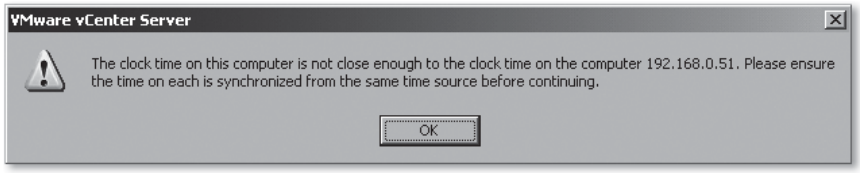


Abbildung 13.35 Ein Uhrzeitabgleich ist notwendig.

Nach der erfolgreichen Installation werden alle verlinkten vCenter-Server zusammen im vSphere-Client angezeigt (Abbildung 13.36).

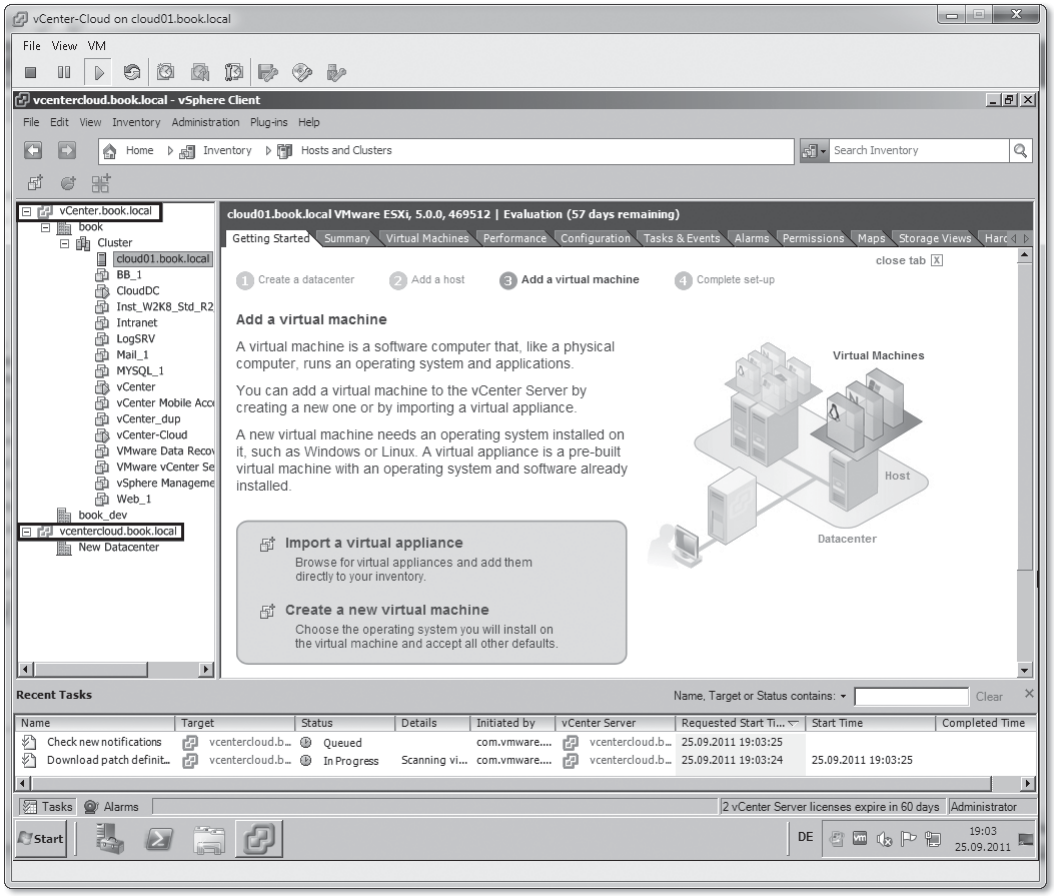


Abbildung 13.36 Verlinkung von zwei vCenter-Servern

Im linken Teil des Clients sind die beiden vCenter-Server zu sehen. Alle Objekte, die zu einem vCenter gehören, werden nur unter dem entsprechenden Element angezeigt, aber es ist keine weitere Anmeldung vonnöten, um auch die zweite Umgebung zu administrieren. Sollten Sie eine größere Umgebung Ihr Eigen nennen, bedenken Sie, dass Sie maximal zehn vCenter-Server miteinander verlinken können. Die Funktionen, die Sie vom vCenter her kennen, ändern sich sonst nicht; alles verhält sich wie bei einem Standalone-System.

13.3 vSphere Management Assistant (vMA)

Die Konfiguration der vMA erfolgt nach dem Import und kann über zwei Wege erfolgen: Entweder nutzen Sie die virtuelle Konsole der vMA, oder Sie führen die Arbeiten über das Webinterface durch.

Es können aber leichte Schwierigkeiten beim Vornehmen der Einstellungen der vMA auftreten, je nachdem, wie Ihr Environment konfiguriert ist. Sollten Sie eine Fehlermeldung beim Starten der Appliance erhalten haben, dann müssen Sie die Einstellungen anpassen. Hoffentlich haben Sie noch im Hinterkopf, wie Sie die IP-Zuweisung beim Import konfiguriert haben. Alternativ sollten Sie wissen, wo Sie die Einstellungen kontrollieren bzw. ändern können. Dazu rufen Sie die Eigenschaften der VM auf und wechseln in den Reiter Optionen.

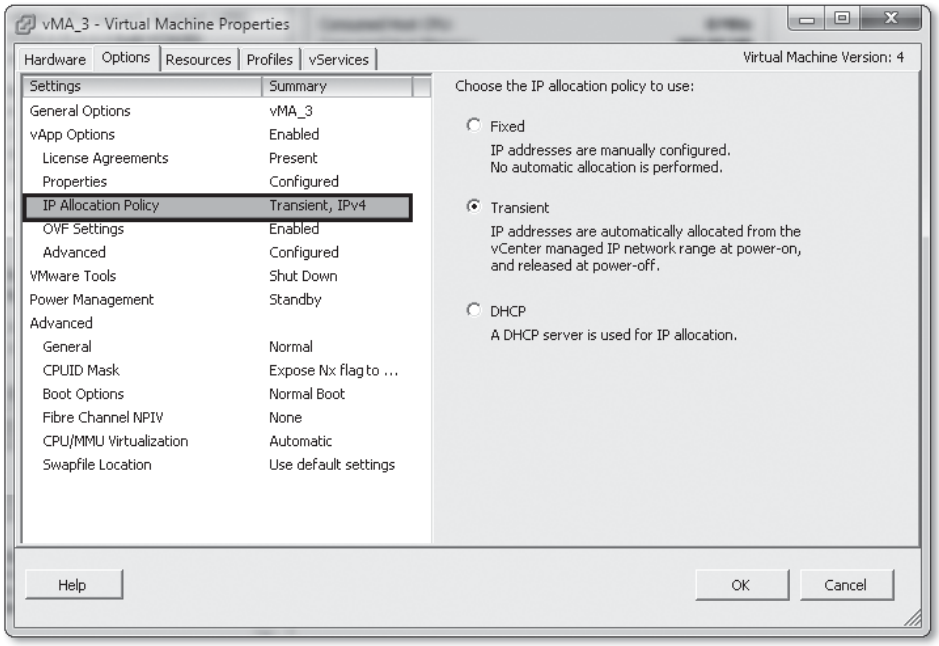


Abbildung 13.37 IP-Konfiguration der vMA

Hinter der Auswahl IP Allocation Policy findet sich die gesuchte Einstellung. Kontrollieren Sie hier, ob die Zuweisung richtig funktioniert. Richten Sie am besten einen IP-Pool an, der die vMA versorgt. Alternativ können Sie aber auch unter Advanced • Properties die Keys löschen, die die vApp versorgen.

Kommen wir zu der eigentlichen Konfiguration der vMA. Wir möchten mit Ihnen beide Wege gehen; Sie können dann entscheiden, welche Art der Konfiguration Sie bevorzugen. Beginnen wir mit der Kommandozeile. Nach dem Import der Appliance wird diese gestartet, und Sie erreichen Sie durch den Aufruf der Konsole.

13.3.1 Kommandozeile

Nach dem Start finden Sie das Fenster aus Abbildung 13.38 vor.

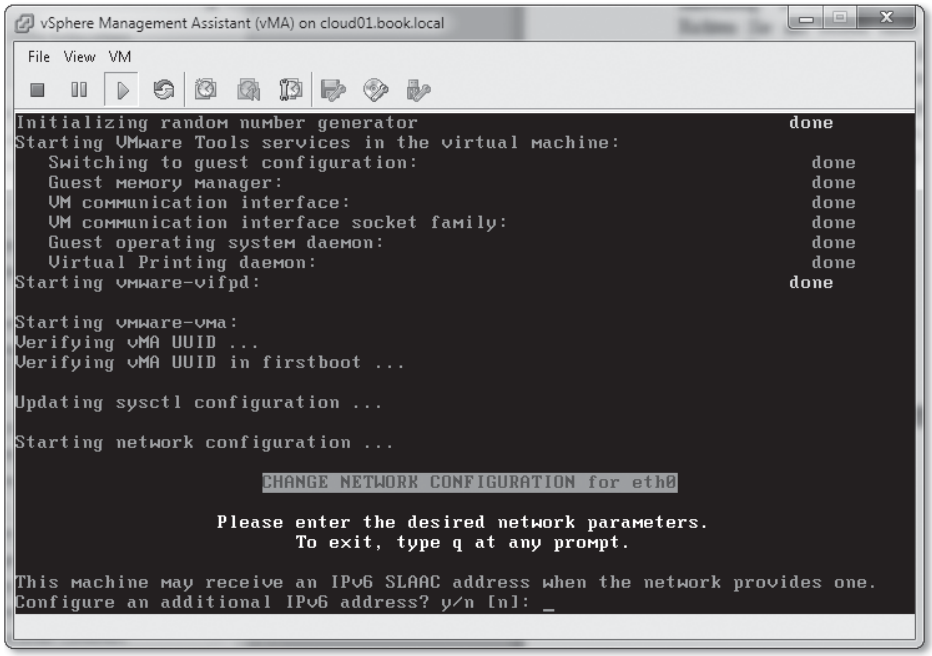


Abbildung 13.38 Basiskonfiguration der vMA

Sollten Sie bei der IP Allocation Policy die Option Fixed ausgewählt haben, können Sie jetzt über die Kommandozeile die IP-Adresse und weitere Einstellungen festlegen. Sollten Sie den Dialog aus Versehen abgebrochen haben, starten Sie ihn neu. Wechseln Sie dazu in das Verzeichnis */opt/vmware/vma/bin* und geben den Befehl `sudo ./vmware-vma-netconf` ein. Haben Sie die beiden anderen Policies konfiguriert, beenden Sie den Dialog mit `q`. Sie werden dann noch aufgefordert, ein Passwort zu vergeben. Die Passwortrichtlinien sind wie folgt:

- mindestens 8 Zeichen
- Großbuchstaben
- Kleinbuchstaben
- Ziffern
- Sonderzeichen

Sollten Sie später das Passwort ändern wollen, so verwenden Sie einfach den Linux-Befehl `passwd`.

Die Maschine versorgt sich dann über den eingestellten Mechanismus mit den Netzwerkparametern. Sind die Arbeiten abgeschlossen, landen Sie im Standardschirm der Appliance.

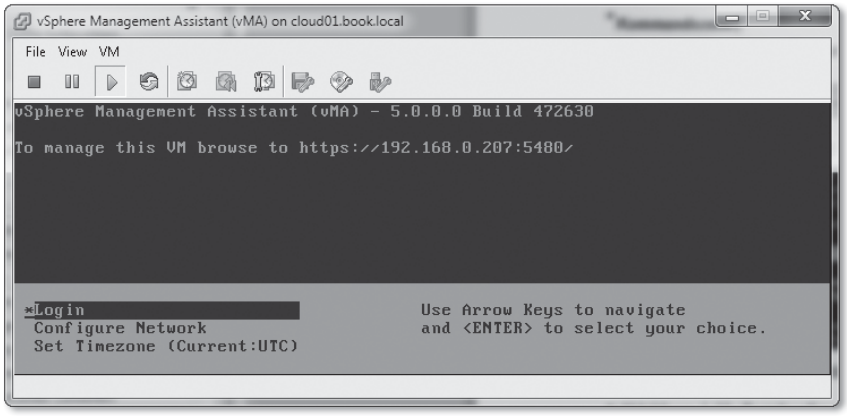


Abbildung 13.39 Standardschirm der vMA

13.3.2 Webinterface

Die weitergehende Konfiguration können Sie jetzt im Webinterface vornehmen. Dazu rufen Sie die URL *https://<IP vMA>:<5480>* auf und melden sich an.

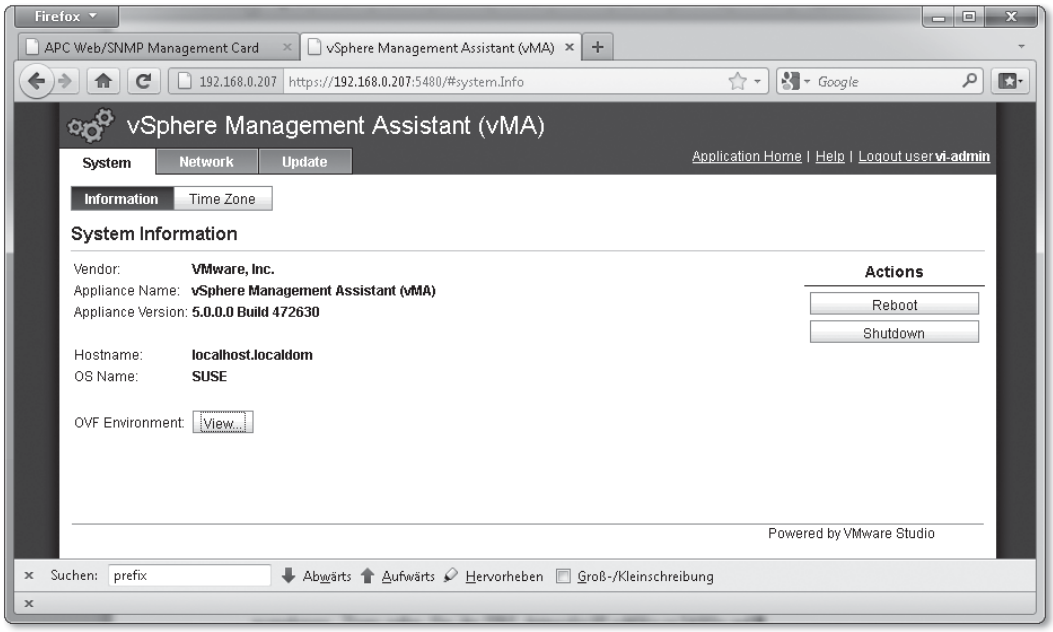


Abbildung 13.40 Konfiguration der vMA

Alle Konfigurationspunkte, die Sie über die Kommandozeile einstellen konnten, können Sie auch hier in einer einfachen Weboberfläche anpassen, mit Ausnahme der Updatefunktion.

Der STATUS zeigt sich mit dem ersten Auswahlpunkt, die eigentliche Update-Funktion verbirgt sich hinter der zweiten Auswahl.

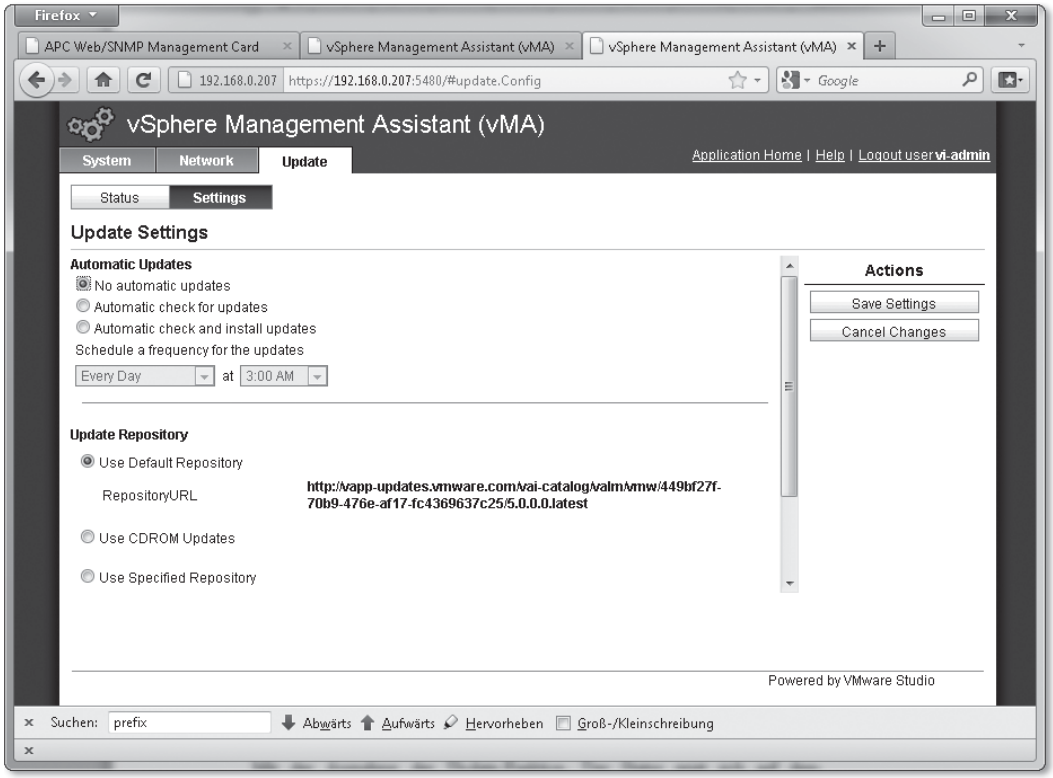


Abbildung 13.41 Update-Mechanismus für die vMA

Hier können Sie die Art des Updates bzw. der Update-Überprüfung einstellen. Aktivieren Sie einen Automatismus, entscheiden Sie, ob das Update nur heruntergeladen oder anschließend auch direkt installiert wird. Dabei dient nicht nur das Internet als Quelle. Die Aktualisierung kann auch über eine CD oder über ein Repository im lokalen Netzwerk erfolgen. Damit sind die Basisarbeiten abgeschlossen, lassen Sie uns nun kurz auf die Nutzung der vMA eingehen.

13.3.3 Basisbedienung

Jetzt sind wir am Ziel angekommen und können uns um die eigentliche Nutzung der vMA kümmern. Für das Absetzen von Befehlen über die vMA gibt es grundsätzlich zwei Wege. Der erste führt über die Konsole der VM selbst, hat aber den Nachteil, dass immer nur ein Administrator Befehle gegen das vCenter oder gegen ESXi-Hosts absetzen kann. Der bessere Weg ist, einen SSH-Client zu nutzen, wie z. B. PuTTY, und damit eine Sitzung auf der vMA öffnen. So können auch mehrere Administratoren gleichzeitig arbeiten, was in größeren Landschaften nicht unbedingt ungewöhnlich ist.

Domänenanbindung

Grundsätzlich sieht VMware unterschiedliche Schritte vor, um sich gegenüber dem vCenter bzw. dem ESXi-Host zu authentifizieren. Sie können die Credentials im lokalen Store ablegen oder in eine Windows-Domäne aufnehmen. In letzterem Fall liegen keine User-Daten auf den vMA. Dieser Weg ist aus unserer Sicht der bessere, aus dem zuletzt genannten Grund.

Der Befehl `sudo domainjoin-cli join <domain-name> <domain-admin-user>` fügt die vMA in eine Windows-Domäne ein, und Sie können nun deren Authentifizierungsmechanismen nutzen. Vergessen Sie den abschließenden Reboot nicht, sonst werden die Änderungen nicht angezogen. Mit der Domänenmitgliedschaft der vMA können Sie eine Unattended Authentifizierung zu allen VMware-Objekten durchführen, Voraussetzung dafür ist, dass diese Objekte Mitglied in der Windowsdomäne ist. Als Fazit ist zu sagen: Wenn die vMA in einer Mitglied einer Domäne ist, dann sollten auch die ESXi-Hosts in derselben Domäne stehen. Wie Sie diese Arbeiten durchführen, dazu kommen wir jetzt. Zuallererst ist ein Tool auf dem Domänen-Controller zu installieren. Es handelt sich dabei um das Tool *ktpass.* Sind Ihre Server immer aktuell gepatcht, so finden Sie die Datei im Filesystem Ihres Servers im Verzeichnis *%windows%\system32*. Erzeugen Sie jetzt auf dem Domänen-Controller eine Datei, und kopieren Sie sie anschließend auf die Virtual Management Appliance. Bevor wir nun zu dem Befehl kommen, treffen wir noch Festlegungen:

- `<vma-dc>` entspricht dem Domänennamen.
- `<foo>` entspricht einem beliebigem Anwender, der administrative Rechte auf dem vCenter-Server hat.

Setzen Sie nun den folgenden Befehl ab:

```
ktpass /out foo.keytab /princ foo@VMA-DC.ENG.VMWARE.COM /pass ca...
  /ptype KRB5_NT_PRINCIPAL
-mapuser <vma-dc>\<foo>
```

Nach dem Durchlauf des Befehls haben Sie die Datei *foo.keytab* erzeugt. Kopieren Sie sie auf die vMA, und zwar in den Pfad */home/local/VMA-DC/foo*. Nun müssen Sie dem Filesystem auf der vMA eine neue Datei spendieren. Das Skript, das Sie jetzt erstellen, sorgt dafür, dass die Kerberos-Tickets aktualisiert werden. Erzeugen Sie dazu ein Skript namens *renew_kerberos* im Verzeichnis */etc/cron.hourly/*, und füllen Sie es mit dem folgenden Inhalt:

```
#!/bin/sh
su - vma-dc\\foo -c '/usr/bin/kinit -k -t /home/local/VMA-DC/foo/
foo.keytab foo'
```

Im Rhythmus von 60 Minuten wird das Ticket über einen Lauf des Skripts aktualisiert.

Bis jetzt haben wir nur mit dem administrativen Account gearbeitet, dem »vi-admin«. Die vMA hat aber noch einen anderen Account: den »vi-user« für den normalen User. Dieser Account hat zwar kein Passwort, kann aber nur genutzt werden, nachdem ein Passwort verge-

ben wurde. Das ist nun keine wirklich schwere Aufgabe: Nach der Anmeldung mit dem »vi-admin« setzen Sie einfach den Befehl `sudo passwd vi-user` ab, und schon ist der Account »vi-user« freigeschaltet. Jetzt haben Sie alle vorbereitenden Arbeiten durchgeführt und können sich nun mit den Hosts bzw. dem vCenter beschäftigen.

Der einfachste Weg zur Administration ist nun, das vCenter der vMA bekannt zu machen. Der Befehl `vifp addserver <FQDN vCenter-Server> --authpolicy adauth` übernimmt diese Aufgabe. Das System fragt Sie nach dem Absetzen des Befehls nach einem Useraccount. Dieser Domänenaccount muss natürlich Rechte auf dem vCenter haben. Der Befehl `vifp listservers -long` gibt Ihnen eine Liste der verbundenen Objekte aus mit weiteren Informationen zur Art des Objekts und zur Authentifizierungsart. Möchten Sie Befehle gegen einen speziellen Host absetzen, ist zuvor das Target festzulegen. Dazu nutzen Sie den Befehl `vifptarget --set | -s <server>`. Die folgenden Kommandos werden nun an den Server `<server>` weitergeleitet.

Fastpath-Authentifizierung

Die Fastpath-Authentifizierung ist ein Weg, eine sessionbezogene Authentifizierung zu nutzen, die aber nicht persistent ist. Dazu nutzen Sie das Kommando `vifp addserver <FQDN Server> --authpolicy fpauth`. Jetzt können Sie weitere Befehle gegen Objekte der virtuellen Infrastruktur absetzen.

Arbeiten mit der vMA

Wir könnten jetzt den Umfang des Buchs locker verdoppeln, indem wir alle Möglichkeiten zur Nutzung von Befehlen zusammenschreiben, aber das Buch hat jetzt schon einen so großen Umfang, dass wir das Thema an dieser Stelle nicht noch weiter ausbreiten wollen. Aus diesem Grund möchten wir Ihnen ein paar Hinweise zum Thema geben und auf die Whitepapers von VMware verweisen, die Sie wälzen können, wenn Sie weitere Informationen zum Thema benötigen. Das Papier zur vMA finden Sie unter *http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vma_50_guide.pdf*.

Eine Referenz für die Kommandozeilenbefehle finden Sie unter:

http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-50-command-line-interface-solutions-and-examples-guide.pdf

Sie sollen aber auch nicht ganz ohne Informationen nach Hause gehen. Sind Ihnen die Befehle von der Service Console noch bekannt? Dann sind Sie gar nicht so weit von den weiteren Arbeiten mit den Hosts entfernt. Sie können einen großen Teil der Befehle von dieser Konsole aus nutzen, es hat sich nur der Ort geändert, an dem die Befehle abgesetzt werden. Aber das wird nach unserer Einschätzung nicht mehr lange der Fall sein. Es gibt ja auch die ESXCLI-Befehle. Diese hat VMware stark ausgebaut, und es scheint so, als ob VMware hier mittelfristig den Schwerpunkt setzen wird.

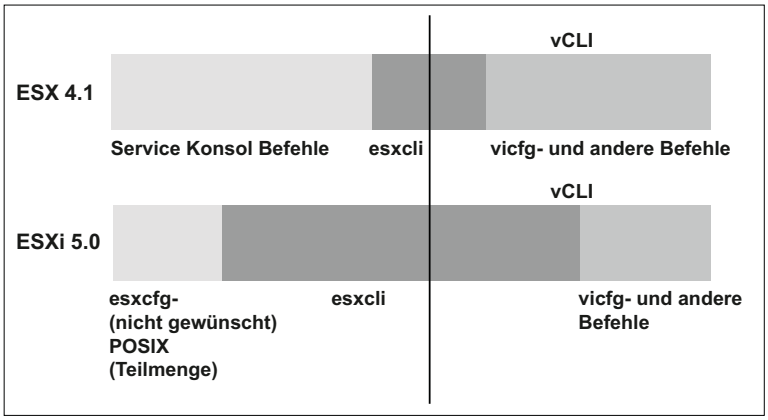


Abbildung 13.42 Verlagerung der Gewichtung der Kommandozeilen-Befehle

Die Grafik in Abbildung 13.42 verdeutlicht, wie sich bei den CLI-Befehlen die Gewichtung geändert hat. Es ist zu erwarten, dass der Trend sich mit den nächsten Versionen weiter verändern wird. Das einzige Tool, das alle Arten von Befehlen zulässt und nicht nur Schwerpunkte in einigen Bereichen hat, ist mittlerweile die PowerShell mit der PowerCLI-Erweiterung. Einige der neuen Funktionen von vSphere 5.0 sind nur über das PowerCLI nutzbar bzw. konfigurierbar.

13.4 VMware ESXi Dump Collector

Nach der Installation des ESXi Dump Collectors finden Sie ein Icon auf der MANAGEMENT-Homepage. Wie schon beschrieben, dient der Dump Collector als zentrales Sammelbecken für Core-Dumps von ESXi-Hosts. Dieser Dienst ist notwendig geworden, weil vSphere 5.x die Funktion bietet, das ESXi im Arbeitsspeicher laufen zu lassen, ohne dass eine lokale Installation erfolgen muss.

Die Konfiguration selbst erfolgt auf dem ESXi-Host. Diesem muss der Collector bekanntgegeben werden. Zwei Wege können Sie hier beschreiten: Die Hostprofile nehmen die Einstellung mit, oder Sie nutzen die Kommandozeile mit dem passenden ESXCLI-Befehl. Den Hosts muss »beigebogen« werden, wie der Dump-Server heißt und über welchen Port mit ihm kommuniziert wird. Das Kommando zum Hinzufügen eines Hosts lautet:

```
esxcli system coredump network set --interface-name vmk0
  --server-ipv4 xx.xx.xx.xx --server-port 6500
```

Der Dump muss über einen *vmkernel-nic* laufen. Angesprochen wird das System über die IP-Adresse, dabei ist der Standardport der IP-Port 6500. Nach der Konfiguration ist die Funktion des dezentralen Dumpens für den Host noch mit dem folgenden Befehl zu aktivieren:

```
esxcli system coredump network set --enable true
```

Alternativ binden Sie die Arbeiten an ein Hostprofil, wie bereits geschrieben. Dazu wechseln Sie auf die Homepage des vCenters, wählen die HOST PROFILE-Option und wählen im folgenden Fenster ein Profil aus, das Sie für die Nutzung des Dump Collectors konfigurieren wollen, oder Sie legen ein neues Profil an. In dem zu editierenden Profil suchen Sie die Option für den Dump Collector und parametrieren die Einstellungen gemäß dem aufgebauten Dump-Collector-Server.

13.5 VMware vSphere Syslog Collector

Der Grund für die Entwicklung eines eigenen Syslog-Servers deckt sich mit den Gründen für die Entwicklung des ESXi Dump Collectors: die neue Option, den ESXi-Host nur im Arbeitsspeicher laufen zu lassen. Nach einem Absturz des Systems wären alle Logs weg, und so könnte im Nachhinein keine Fehleranalyse durchgeführt werden.

Kommen wir zurück zur Konfiguration des Syslog-Ziels. Die Einstellungen können über den vSphere-Client oder über die vCLI konfiguriert werden. Im Client gibt es im Gegensatz zu den anderen Funktionen keinen eigenen Menüpunkt. Die Einstellungen nehmen Sie im KONFIGURATION-Reiter des Hosts vor. Unter SOFTWARE • ADVANCED SETTINGS • SYSLOG • GLOBAL finden Sie die für den Syslog-Server relevanten Einstellungen

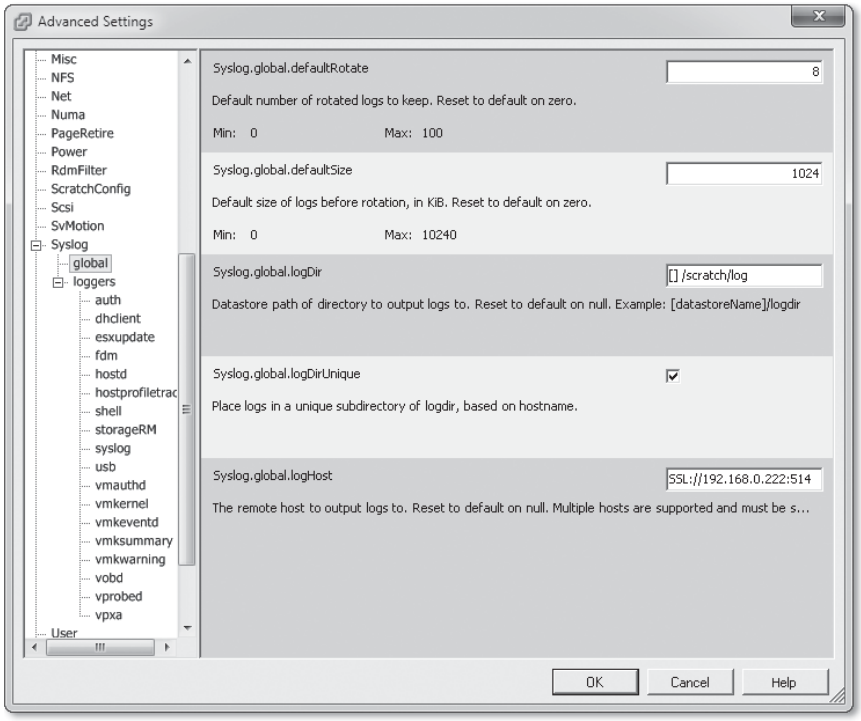


Abbildung 13.43 Syslog-Server-Einstellungen

Lassen Sie uns kurz auf die fünf Parameter eingehen, als da wären:

Parameter	Beschreibung	Defaultwert
Syslog.global.defaultRotate	Anzahl der Logs, die behalten werden sollen. Für remote abgelegte Logs spielt dieser Wert keine Rolle.	8
Syslog.global.defaultSize	Standardgröße des Protokolls in KB, nach dem eine Log-Rotation durchgeführt wird. Dieser Wert hat keinen Einfluss auf Remote-Log-Server.	1024
Syslog.global.logDir	Diesen Parameter haben wir zur Vollständigkeit mit aufgeführt, unsere Recherchen haben aber keine Dokumentation zu diesem Eintrag gefunden	[] /scratch/log
Syslog.global.logDirUnique	Logfiles werden im Verzeichnis *[Datastorename] Verzeichnisname/Filename* abgelegt. Ist das Verzeichnis nicht vorhanden, wird es automatisch angelegt. Dies trifft auch für remote angelegte Datastores zu.	false
Syslog.global.logHost	Hier wird die Adresse eines zentralen Syslog-Servers angegeben. Dabei werden die Protokolle UDP, TCP und SSL unterstützt. Der Eintrag erfolgt in der Form: *<Protokoll>://<Hostname>:514*. Sollten Sie bei der Installation des Syslog-Servers einen anderen Port angegeben haben, so ist das bei der Konfiguration der Adresse entsprechend zu berücksichtigen.	–

Tabelle 13.1 Parameter zur Parametrierung des Log-Servers

Kommen wir nun zur Konfiguration über die Kommandozeile. Zu Beginn sollten Sie sich die Werte der Konfigurationsparameter anzeigen lassen. Das erfolgt mit dem Befehl

```
esxcli system syslog config get
```

Im Fenster werden nun die fünf Parameter mit ihren Werten angezeigt. Möchten Sie einen oder mehrere der Werte anpassen, so können Sie die Manipulation wie folgt vornehmen:

```
esxcli system syslog config set --logdir=/path/to/directory/
  --loghost=RemoteHostname --logdir-unique=<true|false> --default-rotate=NNN
  --default-size=NNN
```

Parameter, die Sie nicht ändern wollen, lassen Sie einfach weg. Sie sehen, es ist recht simpel, die Anpassung für den Syslog-Server vorzunehmen. Damit die Änderungen, die Sie in der Kommandozeile, vorgenommen haben, auch wirksam werden, laden Sie mit dem folgenden Kommando die geänderte Konfiguration und schalten sie aktiv:

```
esxcli system syslog reload
```

13.6 VMware vSphere Authentication Proxy

Der Authentication Proxy ist eine weitere neue Komponente, die VMware mit der Version 5.x eingeführt hat. Er erleichtert die Aufnahme von ESXi-Hosts in ein Active Directory. Sie müssen keine Active-Directory-Credentials eingeben, um einen Host in eine Domäne aufzunehmen.

Sie müssen unterschiedliche Arbeitsschritte durchführen, um den Authentication Proxy zu konfigurieren. Es muss dabei unterschieden werden, welche IIS-Version Sie auf dem Proxy installiert haben. Aus diesem Grund werden wir immer eine kleine Tabelle einfügen, die die unterschiedlichen Konfigurationsschritte für den ISS beschreibt. Zu Beginn der Konfigurationsarbeiten ist den IIS bekanntzugeben, welche Hosts den Dienst nutzen dürfen. Dazu passen Sie bitte die IIS-Konfiguration wie folgt an.

IIS-Version	Arbeitsschritte
IIS 6.x	1. Öffnen Sie die Computer Account Management Web Site. 2. Öffnen Sie das Kontextmenü des virtuellen Verzeichnisses *CAM ISAPI*. 3. Wählen Sie den Menüpunkt Properties • Directory Security • Edit IP Address and Domain Name Restrictions • Add Group of Computers aus.
IIS 7.x	1. Öffnen Sie die Computer Account Management Web Site. 2. Klicken Sie auf der linken Seite auf das Objekt CAM ISAPI, und öffnen Sie den Punkt IPv4 Address and Domain Restrictions. 3. Wählen Sie Add Allow Entry • IPv4 Address Range aus.

Tabelle 13.2 Bekanntgabe der nutzenden Hosts im IIS

Jetzt kommt es darauf an, ob Sie den Host per Auto Deploy aufgesetzt haben oder nicht. Ist dem nicht so, dann müssen Sie das Zertifikat ändern. Hier können Sie ein selbstgeneriertes nutzen oder ein offizielles.

Zertifikatsart	Vorgehensweise
selbsterzeugtes Zertifikat	Haben Sie das Defaultzertifikat durch ein eigenes ersetzt, dann fügen Sie einfach den Host dem vCenter hinzu. Danach vertraut der Authentication Proxy dem Host.
CA-erzeugtes Zertifikat	Fügen Sie das Zertifikat dem lokalen Zertifikatsspeicher auf dem Authentication Proxy hinzu, und starten Sie den Dienst neu. ▶ **Windows 2003** Kopieren Sie das Zertifikat in das folgende Verzeichnis: *C:\Documents and Settings\All Users\Application Data\VMware\vSphere Authentication Proxy\trust* ▶ **Windows 2008** Kopieren Sie das Zertifikat in das folgende Verzeichnis: *C:\Program Data\VMware\vSphere Authentication Proxy\trust*

Tabelle 13.3 Zertifikatskonfiguration

Damit die Funktion des Authentication Proxys für ESXi-Hosts genutzt werden kann, müssen Sie die beiden Systeme miteinander bekannt machen. Bei der Nutzung von Hostprofilen passiert das automatisch. Nutzen Sie diese nicht, so haben Sie einige weitere Schritte abzuarbeiten.

Sie müssen das Zertifikat auf dem Proxy exportieren und auf dem ESXi-Host wieder importieren. Dazu exportieren Sie zuerst das Zertifikat. Der Arbeitsschritt erfolgt wieder im IIS.

IIS-Version	Arbeitsschritte
IIS 6.x	1. Öffnen Sie die Computer Account Management Web Site. 2. Wählen Sie Properties • Directory Security • View Certificate aus. 3. Exportieren Sie das Zertifikat über Details • Copy to File. 4. Aktivieren Sie die zusätzlichen Optionen Do Not Export the Private Key und Base-64 encoded X.509 (CER).
IIS 7.x	1. Öffnen Sie die Computer Account Management Web Site. 2. Öffnen Sie die Bindings-Dialogbox. 3. Wählen Sie HTTPS Bindings aus. 4. Wählen Sie Edit • View SSL Certificate. 5. Exportieren Sie das Zertifikat über Details • Copy to File. 6. Aktivieren Sie die zusätzlichen Optionen Do Not Export the Private Key und Base-64 encoded X.509 (CER).

Tabelle 13.4 Zertifikatsexport

Logischerweise folgt nun der Import auf dem ESXi-Host. Gehen Sie dazu auf den Summary-Tab auf dem Host, der das Zertifikat bekommen soll. Wählen Sie hier unter Ressources einen beliebigen Datastore aus, und browsen Sie diesen. Mit Upload File kopieren Sie das exportierte Zertifikat auf den Datastore. Wählen Sie anschließend das Zertifikat auf dem ESXi-Host aus, und öffnen Sie es.

Gehen Sie auf die Konfigurationsseite des Hosts, und wählen Sie Software • Authentication Services. Der Link Import Certificate bringt Sie einen Schritt weiter. Fügen Sie hier den gesamten Pfad zu dem Zertifikat ein in der Form *<Datastore name><Dateipfad><Zertifikats Dateiname>*. Im unteren Eingabefeld wird die IP-Adresse des Authentication Proxys erwartet. Damit sind die vorbereitenden Arbeiten abgeschlossen. Jetzt können Sie den Host der Domäne hinzufügen. Auch dazu müssen Sie wieder auf den Configuration-Tab des ESXi-Hosts. Ihr Ziel ist wieder die Auswahl Software • Authentication Services. Wählen Sie den Link Properties…, um den Host der Domäne hinzuzufügen.

Mit der Betätigung des Buttons Join Domain schließen Sie die Arbeiten ab. Sollten Sie die Einstellungen des Authentication Proxys suchen, finden Sie sie auf der Homepage des vSphere-Clients.

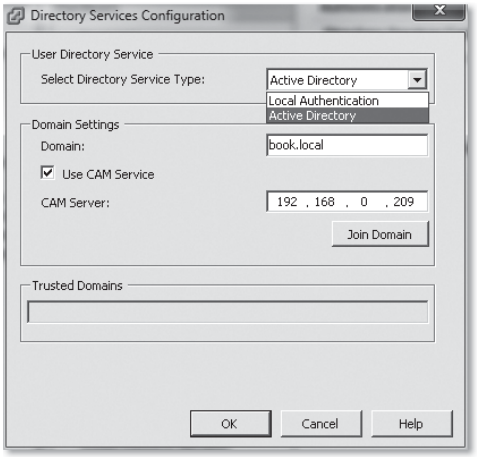


Abbildung 13.44 Hinzufügen des ESXi zur Domäne

13.7 VMware vSphere Image Builder

Haben wir in Kapitel 7 die Installation des Image Builders beschrieben (es ist nichts zu tun, außer das PowerCLI zu installieren), so möchten wir hier exemplarisch einmal darstellen, wie Sie ein Image erstellen. Eine Konfiguration des Image Builders ist nicht notwendig. Die passenden Cmdlets sind Teil des PowerCLI.

Der erste Schritt ist die Bekanntmachung des Depots mit dem folgenden Befehl:

```
Add-EsxSoftwareDepot -DepotUrl C:\Depot\vmware-ESXi-5.0.0-469512-depot.zip
```

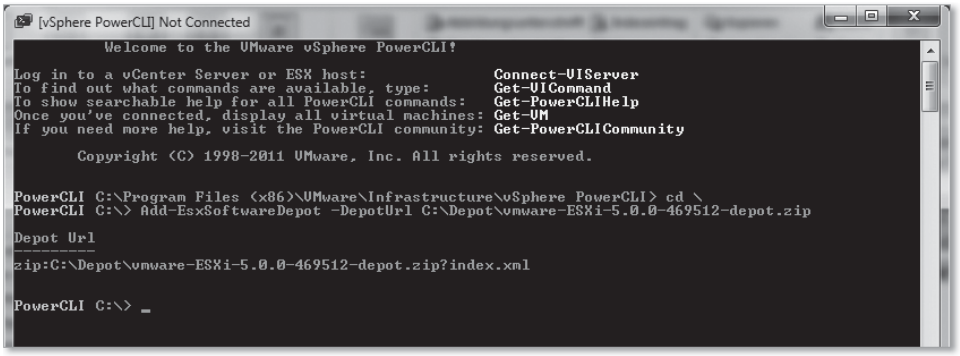


Abbildung 13.45 Erstellen eines Depots

Ein Depotfile kann bereits unterschiedliche Profile enthalten. Diese können Sie sich anzeigen lassen:

```
Get-EsxImageProfile
```

Das Original-Depotfile von VMware selbst enthält bereits zwei Profile: das Standardprofil und das No-Tools-Profil. Diese Profile können Sie nicht ändern, sie sind schreibgeschützt. Das hindert Sie aber nicht daran, diese Profile zu duplizieren und anschließend an Ihre Bedürfnisse anzupassen.

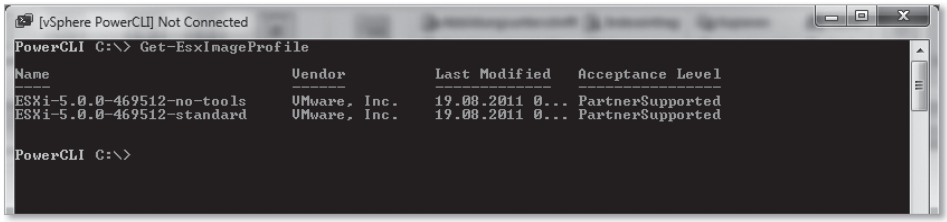


Abbildung 13.46 Profile im Standard-Depotfile

Wir erstellen nun eine Kopie des Standardprofils, um sie später für unsere Arbeiten zu nutzen:

```
New-EsxImageProfile -CloneProfile ESXi-5.0.0-469512-standard
  -Name "Eigene_vSphere5_Installation"
```

Ein sehr wichtiger Punkt ist das Acceptance-Level. Es gibt an, welche VIBs (vSphere Installation Bundle) in das Profil eingebunden werden dürfen. Mögliche Werte finden Sie in Tabelle 13.5.

Acceptance-Level
VMwareCertified
VMwareAccepted
PartnerSupported
CommunitySupported

Tabelle 13.5 Mögliche Werte für das Acceptance-Level

Es kann also erforderlich sein, das Level an Ihre Bedürfnisse anzupassen. Der Befehl sieht dann wie folgt aus:

```
New-EsxImageProfile -CloneProfile ESXi-5.0.0-469512-standard
  -Name "Eigene_vSphere5_Installation" -AcceptanceLevel CommunitySupported
```

Alternativ können Sie einzelne Anpassungen auch nachträglich mit dem Befehl `Set-EsxImageProfile` vornehmen. Lassen Sie uns nun kontrollieren, welche Installationspakete das Profil enthält. Auch hier gibt es ein passendes Kommando:

```
Get-ESXSoftwarePackage
```

Logischerweise sind alle Softwarepakete VIBs, und alle werden geladen, soweit benötigt. Zu Beginn steht nun die Analyse, was zu tun ist. Welche Arbeiten könnten zu erledigen sein? Möglichkeiten wären das Hinzufügen von VMware Infrastructure Bundles oder das Entfernen selbiger.

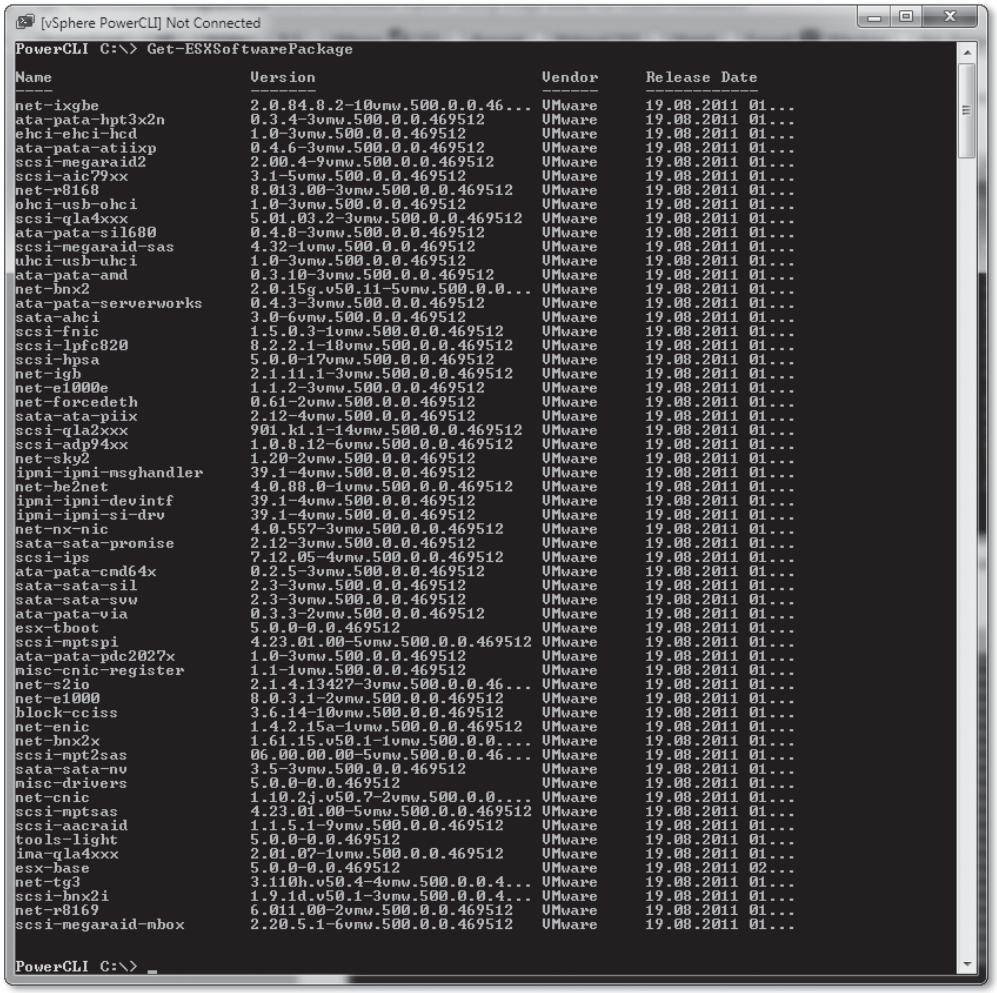


Abbildung 13.47 Installationspakete im Profil

Beide Aktionen möchten wir Ihnen jetzt zeigen. Beginnen wir mit dem Entfernen eines Pakets, was beispielsweise auf jeden Fall relevant ist, wenn ein Treiber aktualisiert werden muss. Zuerst ist dann der alte Treiber zu entfernen, anschließend wird der neue Treiber eingespielt. Als Beispiel ersetzen wir den vorhandenen Fibre-Channel-Treiber von Emulex durch den aktuelleren.

```
Remove-EsxSoftwarePackage -ImageProfile Eigene_vSphere5_Installation
  -SoftwarePackage scsi-lpfc820
```

Wollen Sie kontrollieren, welche Änderungen Sie im Profil vorgenommen haben, verwenden Sie folgenden Befehl:

```
(Get-EsxImageProfile -Name "Eigene_vSphere5_Installation").VibList
```

Nachdem Sie den aktuellen Treiber bei VMware heruntergeladen haben, können Sie ihn zum Profil hinzufügen. Sie finden diesen Treiber unter:

http://downloads.vmware.com/d/details/dt_esxi50_emulex_lpe12000_lpfc820_82210534/dHRAYnQqcGViZHAlJQ==

Weitere Treiber finden Sie unter:

http://downloads.vmware.com/d/info/datacenter_cloud_infrastructure/vmware_vsphere/5_0#drivers_tools

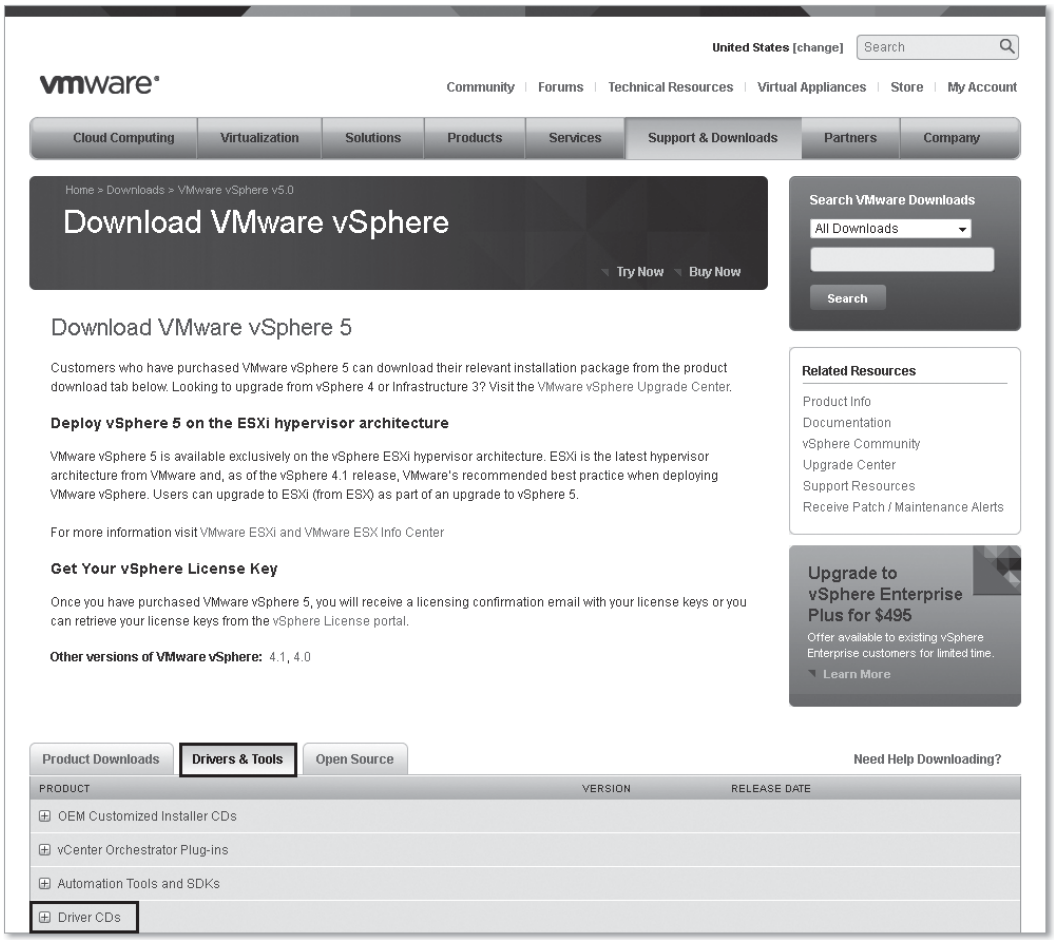


Abbildung 13.48 Neuere VMware-Treiber herunterladen

Kopieren den heruntergeladenen Treiber in das Depotverzeichnis und extrahieren Sie das Offlinebundle aus der ZIP-Datei.

Bevor Sie den neuen Treiber in das Profil laden können, muss Sie ihn zuerst dem Depot hinzufügen:

```
Add-EsxSoftwareDepot -DepotUrl C:\Depot\lpfc820-8.2.2.105.34-offline_
  bundle-476869.zip
```

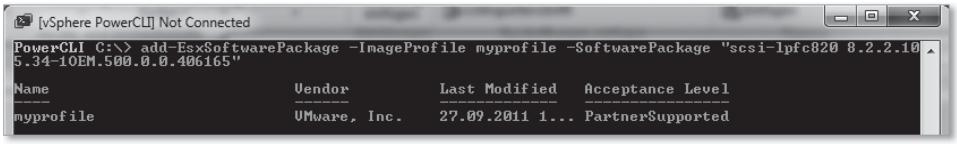


Abbildung 13.49 Einbinden einer Treibers in das Image

Jetzt ist der richtige Zeitpunkt, den neuen Treiber in das Profil zu importieren. Zur Unterscheidung zu dem Originaltreiber binden wir den neuen Treiber mit der Versionsnummer ein, damit der Originaltreiber nicht auch automatisch wieder in das Profil kopiert wird:

```
Add-EsxSoftwarePackage -ImageProfile myprofile
  -SoftwarePackage "scsi-lpfc820 8.2.2.105.34-1OEM.500.0.0.406165"
```

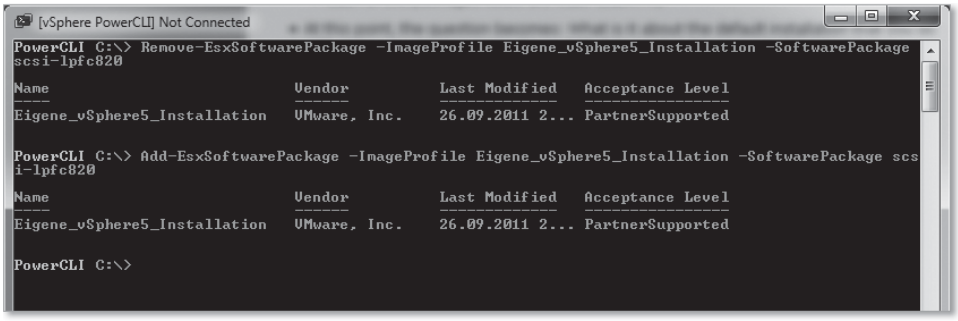


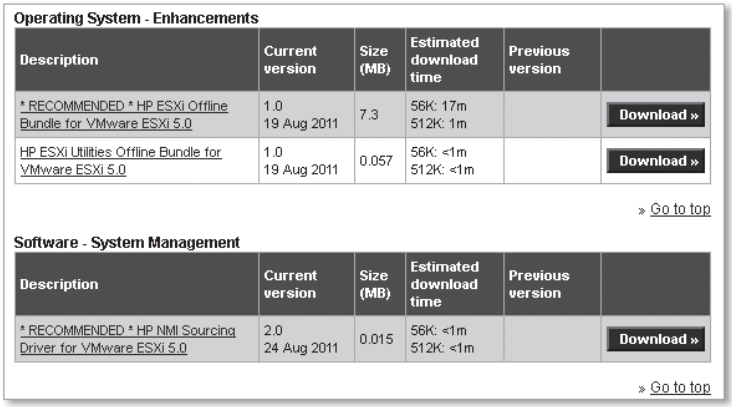
Abbildung 13.50 Entfernen und Hinzufügen von VIBs ins Profil

Lassen Sie uns ein weiteres Beispiel betrachten, bevor wir abschließend ein neues ISO- bzw. Bundle-File erstellen. Nehmen wir als Beispiel den Hardwarehersteller HP. Dieser bietet auf seiner Website drei zusätzliche VIB-Pakete für die Version vSphere 5.x zum Herunterladen.

Hinter den Links verbergen sich drei Files:

- *hp-esxi5.0uX-bundle-1.0-20.zip*
- *hp-HPUtil-esxi5.0-bundle-1.0-23.zip*
- *hp-nmi-esxi5.0-bundle-2.0-11.zip*

Die Files binden Sie bitte mit dem Befehl `Add-EsxSoftwareDepot` in Ihr Depot ein. Schauen Sie sich jetzt die Softwarepakete an, sehen Sie, dass es nun fünf zusätzliche Pakete von HP gibt.



Operating System - Enhancements

Description	Current version	Size (MB)	Estimated download time	Previous version	
* RECOMMENDED * HP ESXi Offline Bundle for VMware ESXi 5.0	1.0 19 Aug 2011	7.3	56K: 17m 512K: 1m		Download »
HP ESXi Utilities Offline Bundle for VMware ESXi 5.0	1.0 19 Aug 2011	0.057	56K: <1m 512K: <1m		Download »

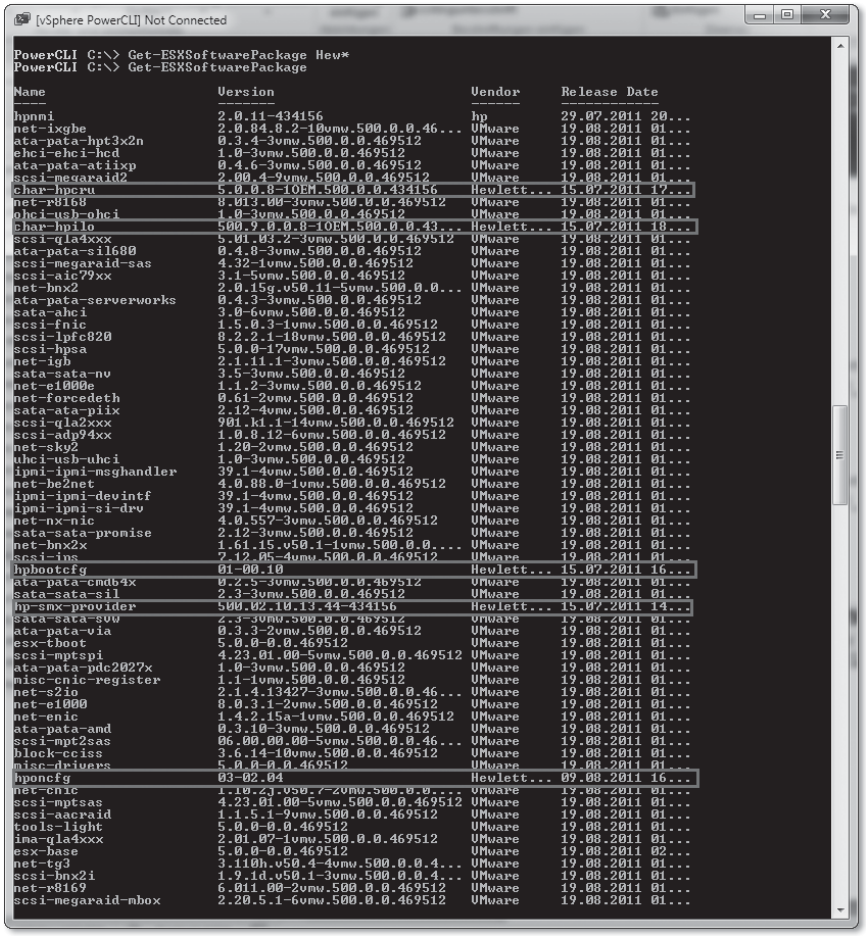
» Go to top

Software - System Management

Description	Current version	Size (MB)	Estimated download time	Previous version	
* RECOMMENDED * HP NMI Sourcing Driver for VMware ESXi 5.0	2.0 24 Aug 2011	0.015	56K: <1m 512K: <1m		Download »

» Go to top

Abbildung 13.51 HP-spezifische Software für vSphere 5.x



```
[vSphere PowerCLI] Not Connected

PowerCLI C:\> Get-ESXSoftwarePackage Hew*
PowerCLI C:\> Get-ESXSoftwarePackage

Name                           Version                        Vendor     Release Date
----                           -------                        ------     ------------
hpnmi                          2.0.11-434156                  hp         29.07.2011 20...
net-ixgbe                      2.0.84.8.2-10vmw.500.0.0.46... VMware     19.08.2011 01...
ata-pata-hpt3x2n               0.3.4-3vmw.500.0.0.469512      VMware     19.08.2011 01...
ehci-ehci-hcd                  1.0-3vmw.500.0.0.469512        VMware     19.08.2011 01...
ata-pata-atiixp                0.4.6-3vmw.500.0.0.469512      VMware     19.08.2011 01...
scsi-megaraid2                 2.00.4-9vmw.500.0.0.469512     VMware     19.08.2011 01...
char-hpcru                     5.0.0.8-1OEM.500.0.0.434156    Hewlett... 15.07.2011 17...
net-r8168                      8.013.00-3vmw.500.0.0.469512   VMware     19.08.2011 01...
ohci-usb-ohci                  1.0-3vmw.500.0.0.469512        VMware     19.08.2011 01...
char-hpilo                     500.9.0.0.8-1OEM.500.0.0.43... Hewlett... 15.07.2011 18...
scsi-qla4xxx                   5.01.03.2-3vmw.500.0.0.469512  VMware     19.08.2011 01...
ata-pata-sil680                0.4.8-3vmw.500.0.0.469512      VMware     19.08.2011 01...
scsi-megaraid-sas              4.32-1vmw.500.0.0.469512       VMware     19.08.2011 01...
scsi-aic79xx                   3.1-5vmw.500.0.0.469512        VMware     19.08.2011 01...
net-bnx2                       2.0.15g.v50.11-5vmw.500.0.0... VMware     19.08.2011 01...
ata-pata-serverworks           0.4.3-3vmw.500.0.0.469512      VMware     19.08.2011 01...
sata-ahci                      3.0-6vmw.500.0.0.469512        VMware     19.08.2011 01...
scsi-fnic                      1.5.0.3-1vmw.500.0.0.469512    VMware     19.08.2011 01...
scsi-lpfc820                   8.2.2.1-18vmw.500.0.0.469512   VMware     19.08.2011 01...
scsi-hpsa                      5.0.0-17vmw.500.0.0.469512     VMware     19.08.2011 01...
net-igb                        2.1.11.1-3vmw.500.0.0.469512   VMware     19.08.2011 01...
sata-sata-nv                   3.5-3vmw.500.0.0.469512        VMware     19.08.2011 01...
net-e1000e                     1.1.2-3vmw.500.0.0.469512      VMware     19.08.2011 01...
net-forcedeth                  0.61-2vmw.500.0.0.469512       VMware     19.08.2011 01...
ata-pata-piix                  2.12-4vmw.500.0.0.469512       VMware     19.08.2011 01...
scsi-qla2xxx                   901.k1.1-14vmw.500.0.0.469512  VMware     19.08.2011 01...
scsi-adp94xx                   1.0.8.12-6vmw.500.0.0.469512   VMware     19.08.2011 01...
net-sky2                       1.20-2vmw.500.0.0.469512       VMware     19.08.2011 01...
uhci-usb-uhci                  1.0-3vmw.500.0.0.469512        VMware     19.08.2011 01...
ipmi-ipmi-msghandler           39.1-4vmw.500.0.0.469512       VMware     19.08.2011 01...
net-be2net                     4.0.88.0-1vmw.500.0.0.469512   VMware     19.08.2011 01...
ipmi-ipmi-devintf              39.1-4vmw.500.0.0.469512       VMware     19.08.2011 01...
ipmi-ipmi-si-drv               39.1-4vmw.500.0.0.469512       VMware     19.08.2011 01...
net-nx-nic                     4.0.557-3vmw.500.0.0.469512    VMware     19.08.2011 01...
sata-sata-promise              2.12-3vmw.500.0.0.469512       VMware     19.08.2011 01...
net-bnx2x                      1.61.15.v50.1-1vmw.500.0.0.... VMware     19.08.2011 01...
scsi-ips                       7.12.05-4vmw.500.0.0.469512    VMware     19.08.2011 01...
hpbootcfg                      01-00.10                       Hewlett... 15.07.2011 16...
ata-pata-cmd64x                0.2.5-3vmw.500.0.0.469512      VMware     19.08.2011 01...
sata-sata-sil                  2.3-3vmw.500.0.0.469512        VMware     19.08.2011 01...
hp-smx-provider                500.02-10.13.44-434156         Hewlett... 15.07.2011 14...
sata-sata-svw                  2.3-3vmw.500.0.0.469512        VMware     19.08.2011 01...
ata-pata-via                   0.3.3-2vmw.500.0.0.469512      VMware     19.08.2011 01...
esx-tboot                      5.0.0-0.0.469512               VMware     19.08.2011 01...
scsi-mptspi                    4.23.01.00-5vmw.500.0.0.469512 VMware     19.08.2011 01...
ata-pata-pdc2027x              1.0-3vmw.500.0.0.469512        VMware     19.08.2011 01...
misc-cnic-register             1.1-1vmw.500.0.0.469512        VMware     19.08.2011 01...
net-s2io                       2.1.4.13427-3vmw.500.0.0.46... VMware     19.08.2011 01...
net-e1000                      8.0.3.1-2vmw.500.0.0.469512    VMware     19.08.2011 01...
net-enic                       1.4.2.15a-1vmw.500.0.0.469512  VMware     19.08.2011 01...
ata-pata-amd                   0.3.10-3vmw.500.0.0.469512     VMware     19.08.2011 01...
scsi-mpt2sas                   06.000.00.00-5vmw.500.0.0.46... VMware    19.08.2011 01...
block-cciss                    3.6.14-10vmw.500.0.0.469512    VMware     19.08.2011 01...
misc-drivers                   5.0.0-0.0.469512               VMware     19.08.2011 01...
hponcfg                        03-02.04                       Hewlett... 09.08.2011 16...
net-cnic                       1.10.2j.v50.7-2vmw.500.0.0.... VMware     19.08.2011 01...
scsi-mptsas                    4.23.01.00-5vmw.500.0.0.469512 VMware     19.08.2011 01...
scsi-aacraid                   1.1.5.1-9vmw.500.0.0.469512    VMware     19.08.2011 01...
tools-light                    5.0.0-0.0.469512               VMware     19.08.2011 01...
ima-qla4xxx                    2.01.07-1vmw.500.0.0.469512    VMware     19.08.2011 01...
esx-base                       5.0.0-0.0.469512               VMware     19.08.2011 02...
net-tg3                        3.110h.v50.4-4vmw.500.0.0.4... VMware     19.08.2011 01...
scsi-bnx2i                     1.9.1d.v50.1-3vmw.500.0.0.4... VMware     19.08.2011 01...
net-r8169                      6.011.00-2vmw.500.0.0.469512   VMware     19.08.2011 01...
scsi-megaraid-mbox             2.20.5.1-6vmw.500.0.0.469512   VMware     19.08.2011 01...
```

Abbildung 13.52 Softwarepakete nach Import der HP-VIB-Pakete für vSphere 5.x

Abschließend bleibt Ihnen nur noch das Erstellen des ISO-Files, wenn Sie direkt mit einem Datenträger arbeiten wollen:

```
Export-EsxImageProfile -ImageProfile Eigene_vSphere5_Installation
  -FilePath C:\depot\Eigene_vSphere5_Installation.iso -ExportToIso
```

Alternativ erzeugen Sie ein Offlinebundle für die Verwendung im Auto-Deploy-Server:

```
Export-EsxImageProfile -ImageProfile Eigene_vSphere5_Installation
  -FilePath C:\depot\Eigene_vSphere5_Installation.zip -ExportToBundle
```

Sie können nicht beide Exporte in einem Schritt erzeugen, sondern müssen beide Zeilen nacheinander aufrufen. Wir hoffen, Sie haben einen kleinen Überblick bekommen, wie Sie mit dem Image Builder arbeiten können, um Ihre Bedürfnisse in diesem Umfeld abzudecken.

13.8 VMware Auto Deploy

Kommen wir zu einer sehr wichtigen neuen Funktion im vCenter-Server, dem Auto Deploy Server. Wieder einmal besetzt VMware ein Thema, bei dem zuvor nur Dritthersteller aktiv waren.

Sollten Sie Abschnitt 13.7 über den Image Builder noch nicht gelesen haben, so sei Ihnen das an dieser Stelle empfohlen, denn Sie benötigen ein Image, das Sie für die Installation nutzen können. Die Installation der Auto-Deploy-Funktion haben wir Ihnen ja schon beschrieben, jetzt geht es an die Konfiguration und die Nutzung.

Hinweis

Bevor Sie den Auto Deploy Server nutzen können, möchten wir Sie noch einmal auf die zusätzlichen Komponenten hinweisen, die auf dem vCenter-Server installiert sein müssen, damit Sie dieses Add-on verwenden können:

- Microsoft PowerShell 2.0
- VMware PowerCLI
- TFTP-Server
- DHCP-Server

Wie schon im Installationskapitel beschrieben, sind wir nicht auf die Installation der zusätzlichen Komponenten eingegangen. Bei der Konfiguration werden wir zumindest den Part beschreiben, der für die Darstellung der Auto-Deploy-Funktion wichtig ist. Es gibt verschiedene freie TFTP-Server, die Sie für diese Belange nutzen können, einige davon haben einen integrierten DHCP haben, Lassen Sie uns exemplarisch zwei Softwarepakete aufführen, um Ihnen einen Anhaltspunkt zu geben:

- TFTP-Server **ohne** DHCP:
  http://www.solarwinds.com/products/freetools/free_tftp_server.aspx
- TFTP-Server **mit** DHCP:
  http://tftpd32.jounin.net/tftpd32_download.html

Achtung

Achten Sie darauf, dass die Ports, die im Netz für die Funktionen benötigt werden, auch freigeschaltet sind, auch auf dem Server.

Die Konfiguration führen wir mit dem TFTP-Server von SolarWinds durch, weil in unserem Netzwerk bereits ein DHCP-Server zur Verfügung steht. Über das Menü File/Configure gelangen Sie in die Konfiguration des TFTP-Servers. Ist diese abgeschlossen, wird ein Verzeichnis im Filesystem angelegt. Haben Sie die Einstellung nicht verändert, ist das der Pfad *C:\TFTP-Root*. Jetzt müssen Sie über die Homepage des vSphere-Clients die Konfigurationsseite des VMware Auto Deploys aufrufen und über den Link Download TFTP Boot Zip die Bootdatei für den TFTP-Server herunterladen.

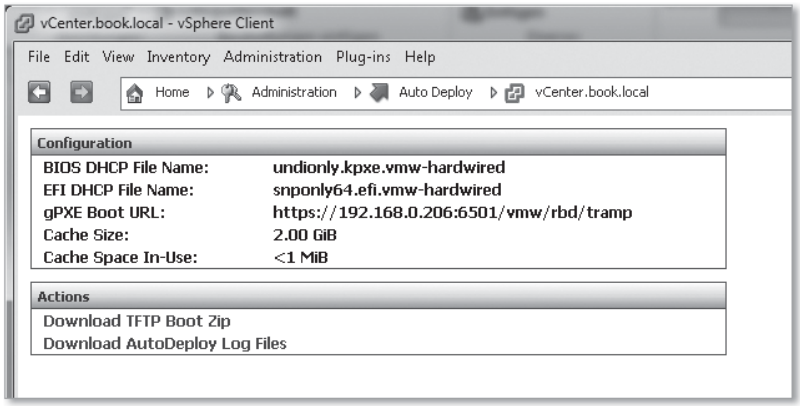


Abbildung 13.53 Download des TFTP-Bootfiles

Arbeiten Sie mit dem Internet Explorer, sollten Sie dazu die Enhanced Internet Security deaktivieren. Entpacken Sie die heruntergeladene Datei in das Verzeichnis des TFTP-Servers. In unserem Fall wäre das *C:\TFTP-Root*.

Damit der Auto Deploy Server einwandfrei funktioniert, müssen Konfigurationsarbeiten am DHCP-Server vorgenommen werden. Die Art der Durchführung ist stark abhängig von dem zum Einsatz kommenden DHCP-Server. In vielen Infrastrukturen kommt der Microsoft-DHCP-Server zum Einsatz, und so gehen wir auf seine Konfiguration genauer ein. Technisch gesehen müssen die Werte #66 und #67 des DHCP angepasst werden.

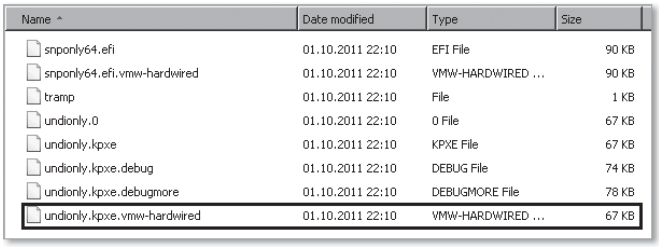


Abbildung 13.54 Inhalt des TFTP-Server-Verzeichnisses

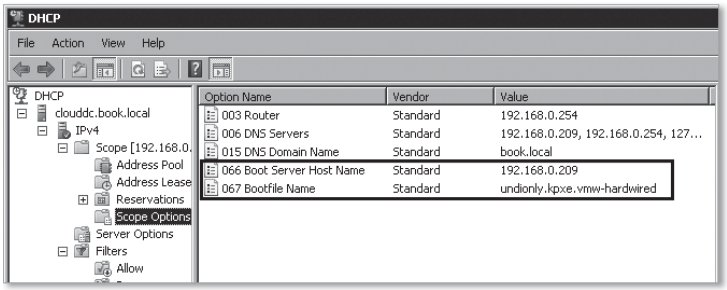


Abbildung 13.55 DHCP-Einstellungen für die Nutzung des TFTP-Dienstes

Als ersten Test können Sie jetzt einen Host booten. Sie werden sehr schnell sehen, ob alles richtig konfiguriert ist. In diesem Fall zeigt eine Fehlermeldung den Erfolg: Das System kann kein ESXi-Image finden. Ähnelt die Meldung, die Sie erhalten, derjenigen in Abbildung 13.56, dann ist alles bis zu dieser Stelle richtig konfiguriert. Sie können die Informationen der Anzeige aber auch für sich nutzen, und zwar, um ein Alleinstellungsmerkmal für den Host zu finden.

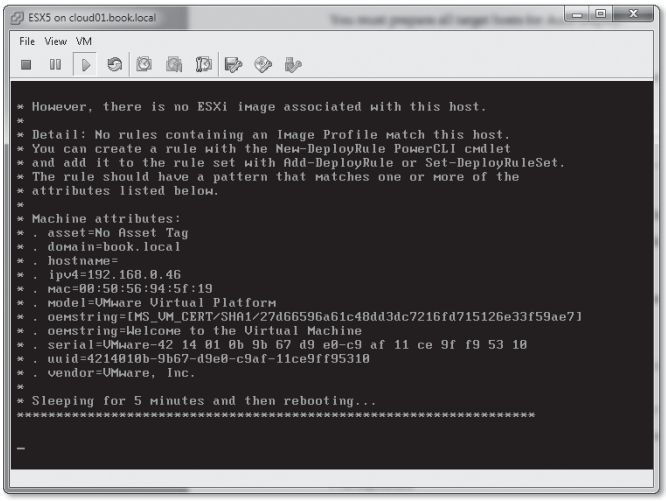


Abbildung 13.56 Verbindung zwischen DHCP und TFTP funktioniert einwandfrei

Die weiteren Arbeiten erfolgen nun im PowerCLI. Wie Sie dieses einrichten, damit Sie Ihre Arbeiten durchführen können, haben wir ja bereits in Kapitel 7 beschrieben.

Verbinden Sie sich zuallererst mit den vCenter-Server:

```
Connect-VIServer 192.168.0.206
```

Wie Sie bereits im vorhergehenden Kapitel gelesen haben, müssen Sie ein Softwaredepot anlegen und bekanntgeben. Das war auch die Ursache für die Fehlermeldung bei Booten des Hosts: Dem System fehlte das Softwaredepot mit einem ESXi-Boot-Image. Verbinden Sie das Installationsimage mit dem Auto-Deploy-Dienst des vCenter Servers:

```
Add-EsxSoftwareDepot c:\tmp\VMware-ESXi-5.0.0-469512-depot.zip
```

In jedem Image sind unterschiedliche Profile enthalten, die Sie mit

```
Get-EsxImageProfile
```

auflisten. Wählen Sie Ihr gewünschtes Profil aus, um es für die Installation zu nutzen. Der Befehl zeigt Ihnen eine Ausgabe wie in Abbildung 13.57.

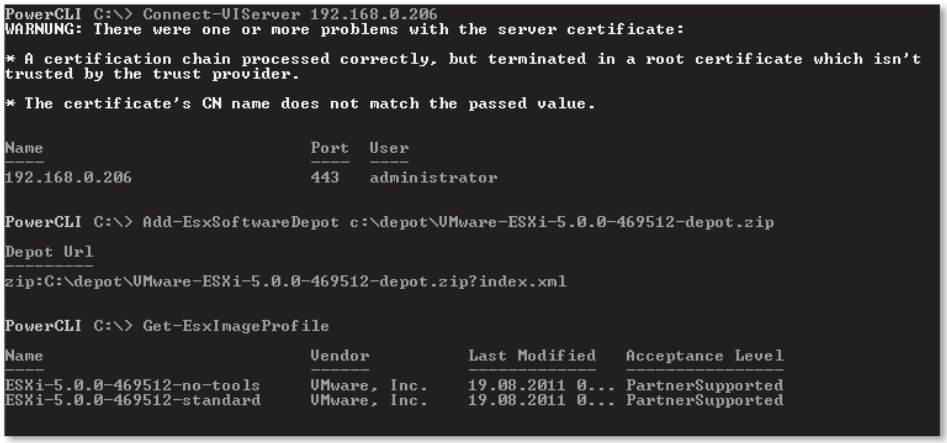


Abbildung 13.57 Anzeige der im Depot enthaltenen Profile

Würden Sie das erste Profil nutzen, könnten Sie vom vCenter-Server aus keine VMware Tools installieren; das wollen wir nicht, deshalb verwenden wir das zweite Profil.

```
New-DeployRule -Name "Virtual-ESX" -Item "ESXi-5.0.0-469512-standard"
  -Pattern "mac=00:50:56:94:5f:19"
```

Das System lädt nun die benötigten Dateien hoch auf den Auto-Deploy-Server, damit die Installation angestoßen werden kann und der Prozess alle benötigten Files erhält. Die MAC-Adresse sorgt dafür, dass das Profil fest einem Host zugewiesen wird. Abschließend ist die Regel zu aktivieren:

```
Add-DeployRule -DeployRule Virtual-ESX
```

Die Installation läuft nun einwandfrei durch, und Sie erhalten einen neuen installierten ESXi-Host; aber der Host, den Sie dann im vCenter vorfinden, muss noch komplett durchkonfiguriert werden. Auch hier möchten wir kurz darauf eingehen, warum es so wichtig ist, auch diese weitergehenden Schritte automatisch durchführen zu können. Der Zeitaufwand für die Konfiguration eines Hosts ist wesentlich höher als für die Installation. Hier ist also Optimierungsbedarf, damit die installierten vSphere-Hosts schnell bereitgestellt werden können. Zu guter Letzt sei wieder die ESXi-»Installation« im Arbeitsspeicher genannt. Kann der Host nicht bis zum letzten Schritt automatisch konfiguriert werden, ergibt diese Art der Installation keinen Sinn. Für diese Herausforderung hat VMware auch das passende Werkzeug im Koffer. Lassen Sie uns darauf nun eingehen.

Am besten nehmen Sie den gerade installierten Host und konfigurieren ihn komplett durch. Beziehen Sie auch den Storage, den NTP, das Netzwerk und alle anderen Einstellungen ein, die Sie in Ihrer Landschaft bzw. im Cluster brauchen werden. Anschließend erstellen Sie ein Hostprofil, in unserem Beispiel nehmen wir den Namen Autoinst-Profil. Achten Sie darauf, dass Sie möglichst alle Einstellungen in dem Hostprofil hinterlegen, so dass Sie bei der Verteilung des Profils keine Einstellungen mehr von Hand erledigen müssen. Mit den jetzt vorgenommenen Einstellungen könnten wir ein neues Profil erstellen, und dann könnte die Installation erfolgen. Lassen Sie uns aber zuvor noch einen weiteren Parameter mit aufnehmen. Wir gehen davon aus, dass die meisten von Ihnen Ihre Hosts zumindest teilweise in Clustern organisiert haben. Damit das auch automatisch funktioniert, ist wieder das PowerCLI zu konsultieren. Es muss der HA-Agent mit an das Profil gebunden werden:

```
Add-EsxSoftwareDepot http://192.168.1.45:80/vSphere-HA-depot
```

Wie schon einmal im Image-Builder-Abschnitt 12.7 beschrieben, erstellen wir nun eine Kopie des Standardprofils und fügen den HA-Agent hinzu. Wir geben hier nur noch einmal die Befehlsliste an, die Erklärungen dazu finden Sie im Image-Builder-Abschnitt.

```
New-EsxImageProfile -CloneProfile ESXi-5.0.0-469512-standard
  -Name "Eigene_vSphere5_Installationmit-HA" -AcceptanceLevel CommunitySupported

Add-EsxSoftwarePackage -ImageProfile "Eigene_vSphere5_Installationmit-HA"
  -SoftwarePackage vmware-fdm
```

Es kann notwendig sein, eine aktive Deploy-Rule vorher zu entfernen. Dazu verwenden Sie den Befehl:

```
Remove-DeployRule -DeployRule <Rule-Name>.
```

Jetzt erstellen Sie eine neue Rolle und geben zusätzlich an, in welchem Cluster das System eingebunden werden soll; in diesem Fall trägt er den Namen `HA-DRS-Cluster-1`:

```
New-DeployRule -Name "ProdHARule" -Item "Eigene_vSphere5_Installationmit-HA",
  Autoinst-Profil, HA-DRS-Cluster-1 -Pattern "mac=00:50:56:94:5f:19"
Add-DeployRule -DeployRule "ProdHARule"
```

Wenn Sie jetzt die Installation erneut starten, werden Sie sehen, dass der Host so konfiguriert wird, wie Sie es wünschen, mit dem passenden Hostprofil versehen und auch in dem Cluster aufgenommen wird.

Hinweis

Wie schon gesagt, können Sie das Profil nur mit einem Host nutzen. Andere Hosts haben möglicherweise zum Teil andere Einstellungen, die Sie aber über das Profil individuell anpassen können, so z. B. die IP-Adresse des vMotion-Netzwerks.

Alle Einstellungen haben wir bis jetzt mit dem klassischen vCenter durchgeführt; wollen Sie mit der Appliance arbeiten, dann ist ein Großteil der Arbeitsschritte identisch, aber das Handling der Dienste ist ein anderes.

13.8.1 VMware Auto Deploy mit der vCenter Server-Appliance

Ein Vorteil der Virtual vCenter Server-Appliance (VCSA) ist, dass Sie keinen dedizierten DHCP- und auch keinen separaten TFTP-Server benötigen. Die Appliance bringt von Haus aus alles mit, was Sie brauchen. Sie müssen das Ganze nur aktivieren und die Konfiguration entsprechend anpassen. Die passenden Stellen werden Sie nicht in der Web-Oberfläche finden, dazu müssen Sie sich schon in die Kommandozeile bemühen.

Für die Einstellungen des DHCP-Dienstes auf der VCSA müssen Sie die Datei */etc/dhcpd.conf* konfigurieren. Die Einstellungen für unsere Landschaft sehen wie folgt aus:

```
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {
pool {
option routers                  192.168.0.254;
option subnet-mask              255.255.255.0;
option domain-name-servers      192.168.0.209;
option domain-name              "book.local";
option time-offset              +3600; # MEZ
default-lease-time              21600;
max-lease-time                  43200;
range                           192.168.0.30 192.168.0.50;
filename        "undionly.kpxe.vmw-hardwired";
allow unknown-clients;
}
```

Für das Thema DHCP ist jetzt aber erst die Hälfte des Weges gegangen. Das System muss jetzt noch wissen, über welches Interface der Dienst bereitgestellt werden soll. Dazu editieren Sie die Datei */etc/sysconfig/dhcpd*. Ergänzen Sie hier den Eintrag

```
DHCPD_INTERFACE="eth<x>"
```

Dabei steht <x> für die Nummer der Netzwerkkarte. Jetzt können Sie den DHCP-Dienst starten. Dazu passen Sie im ersten Schritt die Run-Level-Informationen des Systems an, soll heißen, dass Sie die Systeminformation so anpassen, dass der DHCP-Service automatisch gestartet wird, wenn Sie die Appliance einschalten.

```
chkconfig dhcpd on
```

Es folgt der Start des Dienstes mit:

```
service dhcpd start
```

Jetzt haben wir schon die Hälfte des Weges zurückgelegt und nehmen sofort den letzten Teil in Angriff, den TFTP-Dienst. Auch hier sind einige wenige Konfigurationsschritte durchzuführen. Werfen wir zuerst einen Blick in das Filesystem der VCSA. Dort finden Sie unter dem Pfad */tftpboot* einige Dateien.

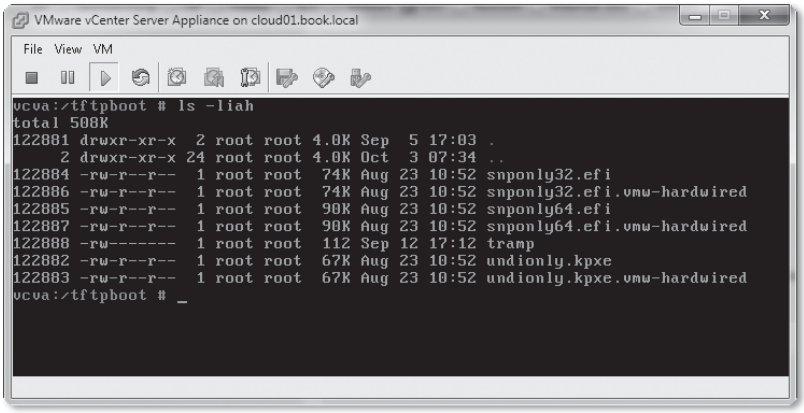


Abbildung 13.58 Inhalt des »tftpboot«-Ordners

Sie sehen, es sind genau die Dateien, die Sie für den TFTP-Dienst benötigen. Jetzt muss nur noch der Dienst aktiviert werden; das kennen Sie ja schon vom DHCP-Dienst:

```
chkconfig atftpd on
```

Es folgt der Start des Dienstes mit:

```
service atftpd start
```

Sie bemerken an dieser Stelle den entscheidenden Vorteil der Appliance: Sie müssen nicht nach anderen Softwarepaketen zu suchen; sie bringt alles mit, was Sie für den Auto Deploy benötigen.

13.9 VMware Data Recovery

Starten Sie nach der Installation die Data Recovery Appliance, bootet das Linux in einen rudimentären Schirm, in dem sich einige einfache Konfigurationsänderungen durchführen lassen (Abbildung 13.59).

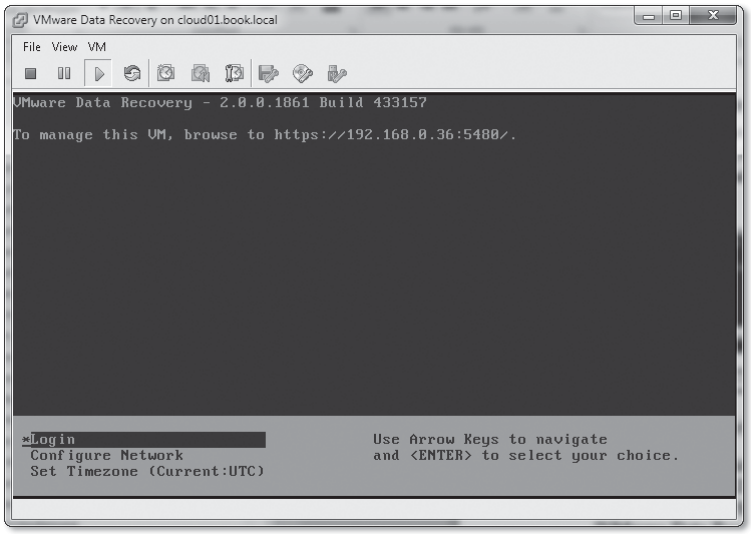


Abbildung 13.59 Startbildschirm der VMware Data Recovery Appliance

An dieser Stelle können Sie die Netzwerkeinstellungen der Appliance anpassen und die Zeitzone konfigurieren. Die bessere Wahl, aus unserer Sicht, ist die Nutzung der Managementoberfläche via Webbrowser. Der Zugriff erfolgt über die im Konsolenfenster angezeigte IP-Adresse. Achten Sie darauf, dass der benötigte Port 5480 im Netzwerk freigegeben ist. Geben Sie die angegebene Adresse im Browser ein, folgt die Anmeldung auf der Oberfläche (Abbildung 13.60).

Abbildung 13.60 Anmeldung an der Managementkonsole

Die Anmeldung für den Administrator erfolgt mit dem User »root« und dem Passwort »vmw@re«. Jetzt können Sie einige Einstellungen an der Server-Konfiguration vornehmen (Abbildung 13.61).

Abbildung 13.61 Hauptfenster der Managementkonsole des Data-Recovery-Servers

Das Hauptfenster der Appliance bietet zwei Reiter. Der erste Reiter ist eine Statusanzeige für das Recovery-System; hier sehen Sie unter anderem die Appliance-Version. Des Weiteren können Sie den Server herunterfahren oder neu booten. Im zweiten Reiter nehmen Sie die Netzwerkeinstellungen vor (Abbildung 13.62).

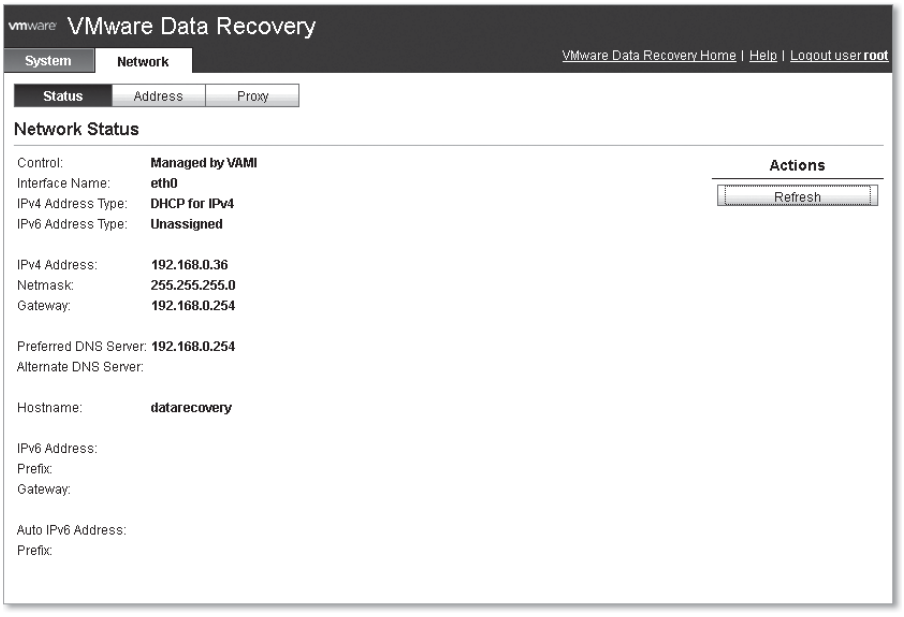


Abbildung 13.62 Kontrolle der Netzwerkeinstellungen

Das erste Fenster zeigt die aktuellen Netzwerkeinstellungen. Nach Aktivierung des Buttons Address lassen sich die IP-Einstellungen anpassen. Entweder aktivieren Sie DHCP mit Obtain configuration from DHCP Server, oder Sie nehmen die IP-Konfiguration in den unteren Eingabefeldern statisch vor (Abbildung 13.63).

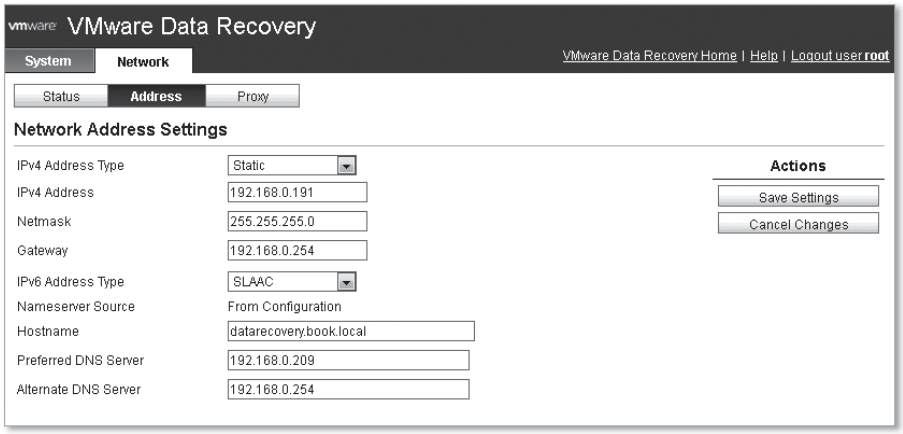


Abbildung 13.63 Konfiguration der IP-Einstellungen

Falls Sie die IP-Konfiguration anpassen, müssen Sie sich nach der Aktivierung der Einstellungen mit SAVE SETTINGS neu mit der Appliance über die dann aktuelle IP-Adresse verbinden. Die vorhergehende Verbindung geht aufgrund der Änderung der IP-Konfiguration verloren.

Falls ein Proxy-Server in Ihrem Environment steht, können Sie ihn unter dem Punkt PROXY aktivieren (Abbildung 13.64).

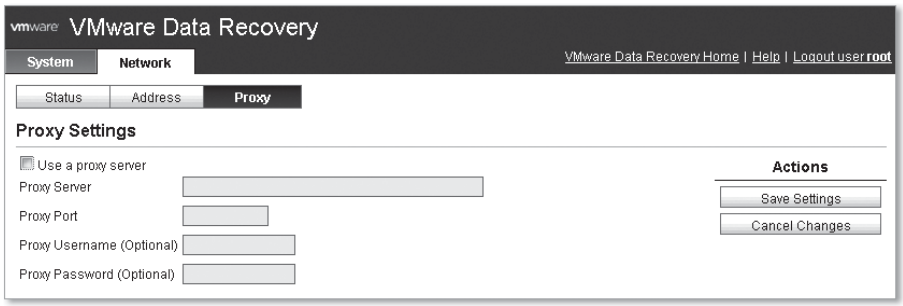


Abbildung 13.64 Proxy-Einstellungen der Data Recovery Appliance

Weitere Einstellungen lassen sich über das Webinterface nicht vornehmen. Sie können den Dialog an dieser Stelle über den LOGOUT-Link verlassen. Die weiteren Funktionen der Data Recovery Appliance rufen Sie über den Data Recovery Client über das vCenter auf. Sie finden ihn unter HOME • INVENTORY • SOLUTIONS AND APPLICATIONS • VMWARE DATA RECOVERY. Mit diesem Client führen Sie die unterschiedlichen Sicherungs- und Rücksicherungsarbeiten durch. Eine Übersicht und eine Anpassung des Clients sind über das vCenter-Plugin möglich. Bevor Sie aber die Appliance weiter konfigurieren können, müssen Sie sich zuerst mit der Appliance verbinden.

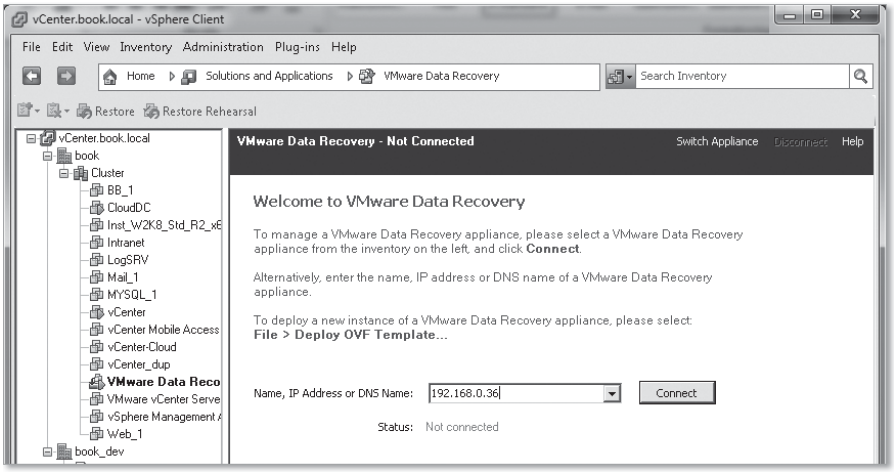


Abbildung 13.65 Verbindungsherstellung mit der VMware Data Recovery Appliance

Wird die Appliance gefunden, so müssen Sie mit einem gültigen Account eine Verbindung zum vCenter-Server herstellen. Nach dem Aufruf des Plugins zeigt sich Ihnen die Oberfläche aus Abbildung 13.65.

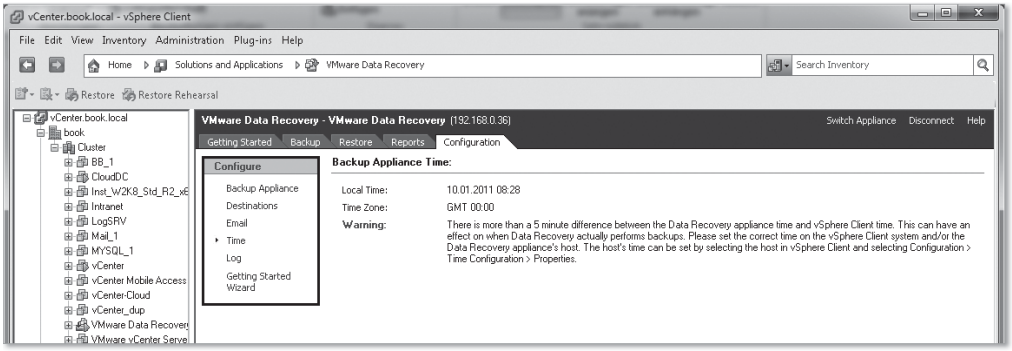


Abbildung 13.66 Oberfläche des Data Recovery Clients

Die allgemeinen Einstellungen für die Sicherungsjobs nehmen Sie unter dem Reiter Configuration vor. Unter dem Punkt Destinations legen Sie das Ziel der Sicherung fest. Als Ziel können SAN (Storage Area Network), NAS (Network Attached Storage) und CIFS (Common Internet File-System) zum Einsatz kommen, also jede von vSphere unterstützte Disk. Auch eine lokale Disk, die Sie nachträglich an die Appliance angehängt haben, kann als Sicherungsziel dienen.

Eine Verbindung mit einem CIFS-Ziel ist über die IP-Adresse oder den FQDN möglich. An dieser Stelle hat VMware nachgebessert. Auf diesem CIFS-Ziel werden die Daten gesichert. Damit die zu sichernde Datenmenge nicht zu umfangreich wird, wird der Datenstrom dedupliziert, was bedeutet, dass identische Daten nicht mehrfach auf das Sicherungsziel geschrieben wer-

den. Sind zu sichernde Daten schon vorhanden, werden im aktuellen Backup-Stream die entsprechenden Dateien nur auf das vorhandene Ziel verlinkt. VMware empfiehlt eine maximale Größe von 500 GB pro Sicherungsziel.

Bei der Deduplizierung müssen Sie einige Punkte beachten. Der Zieldatenträger sollte mindestens doppelt so groß sein wie die zu sichernde Datenmenge. Ist das Ziel kleiner, kann die Appliance nicht richtig deduplizieren. Außerdem stellt ein VMFS-Datastore als Sicherungsziel eine Besonderheit dar: Bei diesem Ziel erfolgt im Gast eine Formatierung mit Nullen; damit funktioniert das Thin Provisioning von VMware nicht mehr. Des Weiteren haben auch viele Storage-Hersteller Probleme mit ihren Thin-Provisioning-Funktionen. Uns ist derzeit nur ein Hersteller bekannt, der mit diesem Umstand sauber umgehen kann, und zwar die Firma HP mit der 3PAR-Produktlinie. Über den Link Log werden die Log-Dateien der VMware Data Recovery Appliance angezeigt.

Der Reiter Backup listet alle erstellten Backup-Jobs. Selbstverständlich können Sie an dieser Stelle mit dem Button New auch neue Jobs erstellen.

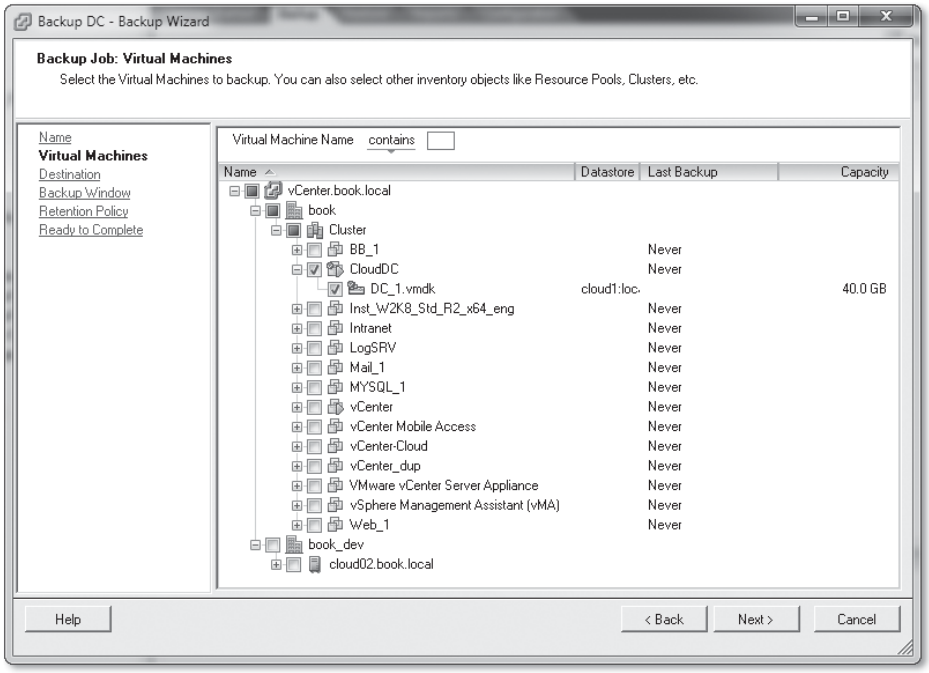


Abbildung 13.67 Erstellung eines Backup-Jobs

Im vorliegenden Beispiel soll die VM CloudDC gesichert werden. Markieren Sie den Server, und wählen Sie im nächsten Schritt das Ziellaufwerk für die Datensicherung aus. Konfigurieren Sie dann das Zeitfenster für die Datensicherung (Abbildung 13.68). Das Management, wann die Datensicherung wirklich zeitlich terminiert wird, obliegt der internen Planung der Software.

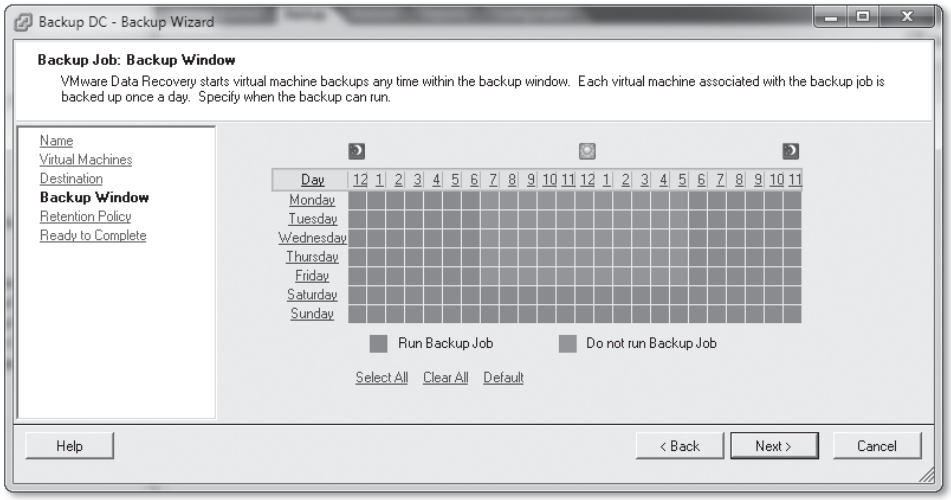


Abbildung 13.68 Datensicherungszeitplan

Im aktuellen Fall ist es dem System erlaubt, montags bis freitags von 0:00 bis 6:59 Uhr und von 18:00 bis 23:59 Uhr zu sichern. An Samstagen und Sonntagen gibt es keine zeitlichen Einschränkungen. Der folgende Schritt beschäftigt sich mit der Aufbewahrungszeit der Sicherung (Abbildung 13.69).

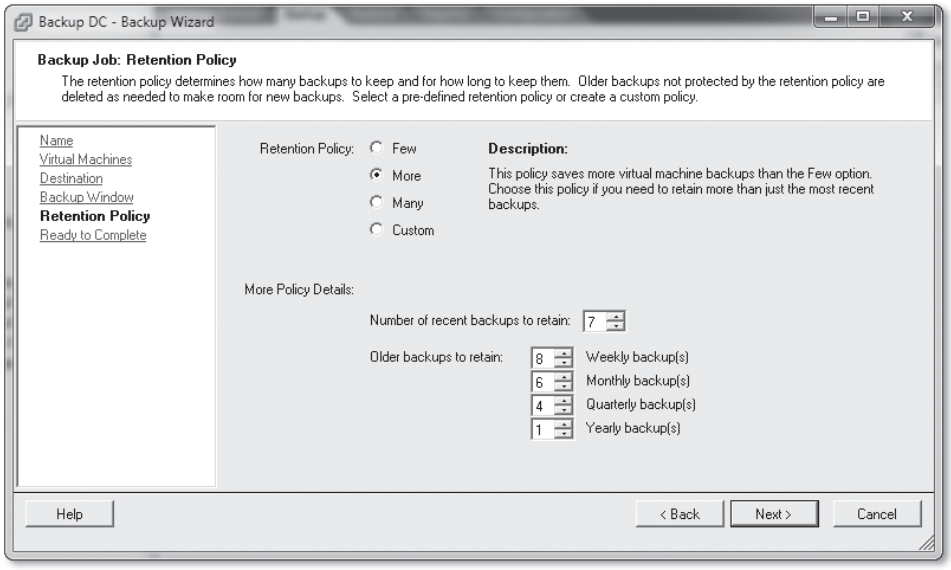


Abbildung 13.69 Aufbewahrungsfristen für die Datensicherung

Drei Sicherungszyklen sind im System vorkonfiguriert. Sollten diese nicht ausreichen, besteht die Option, sich eine eigene Policy einzurichten. Für den von Ihnen definierten Zeitraum

sperren Sie die letzten – in diesem Fall sieben – relevanten Sicherungen. Zusätzlich zu den sieben Sicherungen werden die Sicherungen gesperrt, die den unteren Kriterien genügen.

Nach der Fertigstellung des Jobs können Sie diesem in der zentralen Oberfläche einen sprechenden Namen geben. Das User-Interface bietet die Anpassungsoptionen für den Job. Hier sind alle bereits gesehenen Optionen frei änderbar. Der Backup-Job lässt sich über das Kontextmenü starten. Das System markiert jede virtuelle Maschine, die über einen entsprechenden Job gesichert wird, mit einem neuen Icon. Das Icon der VM enthält dann zusätzlich einen kleinen weißen Haken in einem grünen Kreis. Im Log-Fenster sehen Sie den Erfolg des Backups (Abbildung 13.70).

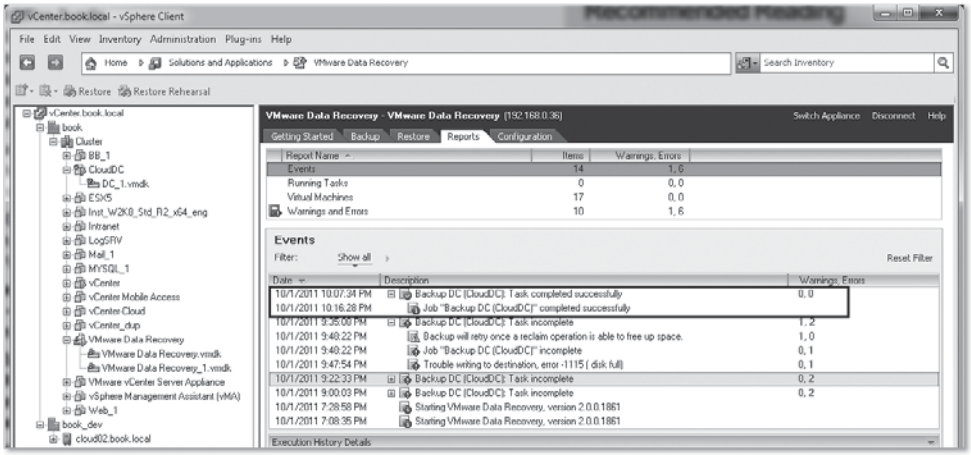


Abbildung 13.70 Positiver Sicherungsabschluss

Wurde eine Maschine gesichert, besteht selbstverständlich die Möglichkeit, den Server wiederherzustellen. Diesen Prozess stoßen Sie über das Kontextmenü der VM an, oder Sie wechseln auf den Reiter Restore (Abbildung 13.71).

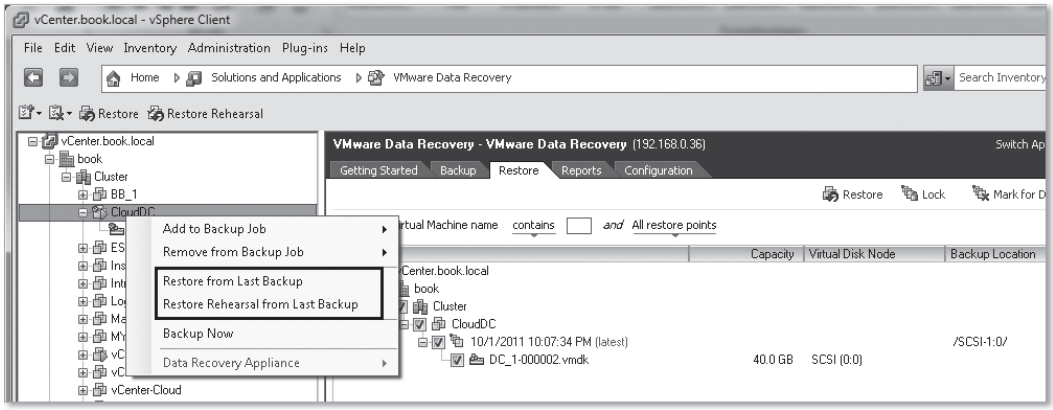


Abbildung 13.71 Restore einer gesicherten Maschine

Die möglichen Funktionen im Reiter Restore und im Kontextmenü unterscheiden sich ein wenig voneinander. Im Reiter Restore starten Sie nicht nur die Wiederherstellung, sondern stellen auch den Umgang mit den erfolgten Sicherungen ein. Mit Lock wird eine Sicherung länger aufbewahrt. Das Gegenteil ist bei Mark for Delete der Fall: Hier erteilen Sie dem System die Freigabe, diese markierte Sicherung zu löschen. Das Kontextmenü enthält den zusätzlichen Punkt Restore Rehearsal. Im Gegensatz zum einfachen Restore wird bei Restore Rehearsal parallel zu der vorhandenen Maschine eine Kopie der VM mit den Sicherungsdaten erstellt. Über diesen Mechanismus besteht die Möglichkeit, Dateien aus der parallel erstellten Maschine herauszukopieren und zurück in das Original zu schreiben. Alternativ legen Sie bei Problemen in einer VM parallel eine Kopie in einem isolierten Netzwerk an, um darin eine Fehleranalyse vorzunehmen.

Achtung

Bedenken Sie bitte, dass zur Durchführung der Datensicherung ein Snapshot in der virtuellen Maschine erstellt wird. Dieser wird erst wieder gelöscht, wenn die Datensicherung abgeschlossen ist. Bei der Planung der LUNs des vSphere-Servers ist das entsprechend zu berücksichtigen. Achten Sie darauf, dass immer genügend freier Plattenplatz auf den LUNs vorhanden ist!

13.9.1 Data Recovery – Hinweise

Im Gegensatz zu anderen VMware-Appliances gibt es keine Möglichkeit, die VMware Data Recovery Appliance upzudaten, es ist auf jeden Fall eine Neuinstallation notwendig. Dies ist aber gar nicht so kritisch, wie es sich anhört, denn die Konfigurationsdaten liegen auf dem Deduplizierungs-Storage neben den Sicherungen. Somit konfiguriert sich die aktualisierte Appliance automatisch, wenn die Daten auf dem Storage erkannt wurden. Aktualisieren Sie den Datensicherungs-Server regelmäßig, denn es werden immer wieder viele Bugfixes und Funktionserweiterungen zur Verfügung gestellt. So profitieren Sie von den Korrekturen und Erweiterungen.

Nun stellt sich abschließend die Frage, wie leistungsfähig die Datensicherungsmaschine ist. Ausführliche Tests haben ergeben, dass es ohne weiteres möglich ist, 100 virtuelle Maschinen mit einer Appliance zu sichern. Machen Sie sich aber keine Sorgen, wenn Ihre Landschaft wesentlich größer ist, denn es ist kein Problem und wird vor allem auch unterstützt, mehrere dieser Server in einer Landschaft zu betreiben. Achten Sie nur darauf, dass Sie die Sicherungszeiten der unterschiedlichen Server miteinander koordinieren.

13.10 Einsatz des VMware vCenter Converters Standalone

Wie bereits im Installationskapitel beschrieben, gibt es den VMware vCenter Converter nur noch in der Standalone-Version. Die ins vCenter integrierte Komponente ist nicht mehr Bestandteil der aktuellen Version. Bevor wir die weitere Vorgehensweise beschreiben, möchten wir kurz erläutern, welche Optionen es gibt und wann sie genutzt werden können.

Der vCenter Converter – viele werden ihn noch als »P2V« oder »VMware Converter« kennen –, ermöglicht die Konvertierung von Computern in eine virtuelle Maschine. Es ist dabei nicht entscheidend, welche Hardware die zu übernehmende Maschine hat. Viel wichtiger ist, dass der Converter in der Lage ist, die systemkritischen Treiber nicht nur zu entfernen, sondern auch durch VMware-konforme zu ersetzen.

Es gibt zwei Möglichkeiten, den Converter zu nutzen: ein sogenannter Coldclone oder ein Hotclone. Bei einem *Coldclone* wird das zu übernehmende System mit einer Converter-CD gestartet, und der Server wird direkt auf einem Host oder vCenter-Server importiert, ohne dass das zu übernehmende System aktiv ist. Das erzeugte Image kann auch auf einem Datenträger gespeichert und anschließend importiert werden.

Im Falle des *Hotclones* wird ein aktiver Server im laufenden Betrieb übernommen. Bevor die Arbeiten beginnen können, wird ein Agent auf dem System installiert. Je nach Gastbetriebssystem ist ein Neustart des Servers notwendig.

Für die Abbildung der Funktion erzeugen Sie einen Snapshot des zu übernehmenden Systems. Alle Änderungsdaten werden in diesen Snapshot geschrieben. So übernehmen Sie zuerst die statischen Daten. Ist dieser Schritt abgeschlossen, erstellen Sie erneut einen Snapshot, und so fort. Dies geschieht so lange, bis die Maschine übernommen ist. Problematisch wird es, wenn die Applikation nicht angehalten wird. Ist die Übernahme abgeschlossen, können sich die Daten der Source-Maschine weiterhin ändern, und damit sind Quell- und Zielsystem nicht identisch. Garantieren Sie deshalb, dass keine Client-Applikation auf das System zugreifen kann. Die Übernahme wird dann auch schneller vonstattengehen.

Hinweis zur Konvertierung

Soll das Hotclone-Verfahren genutzt werden, ist es zumindest bei Datenbankapplikationen empfehlenswert, die Datenbank zu stoppen, bevor Sie die Übernahme starten. Ebenso sollten Sie bei anderen Applikationen verfahren, die hohe Änderungsraten im Content haben.

Die Übernahme von Computern mit dem vCenter Converter funktioniert nicht für alle Betriebssysteme.

OS-Support	Support	Anmerkungen
Windows NT4	nein	Laden Sie sich eine ältere Version der Software herunter.
Windows 2000	nein	Laden Sie sich eine ältere Version der Software herunter.
Windows XP SP3 (32 Bit und 64 Bit)	ja	–
Windows Vista SP2 (32 Bit und 64 Bit)	ja	–

Tabelle 13.6 Unterstützte Betriebssysteme vCenter Converter Standalone

OS-Support	Support	Anmerkungen
Windows 7 (32 Bit und 64 Bit)	ja	–
Windows 2003 SP2 (32 Bit und 64 Bit)	ja	–
Windows 2003 SP2, R2 (32 Bit und 64 Bit)	ja	–
Windows 2008 SP2 (32 Bit und 64 Bit)	ja	–
Windows 2008 R2 (64 Bit)	ja	–
Red Hat Enterprise Linux 2.x – 5.x (32 Bit und 64 Bit)	ja	–
SUSE Linux Enterprise Server 8.x – 11.x (32 Bit und 64 Bit)	ja	–
Ubuntu 8.x – 10.x (32 Bit und 64 Bit)	ja	–

Tabelle 13.6 Unterstützte Betriebssysteme vCenter Converter Standalone (Forts.)

Es wundert nicht, dass es mittlerweile auch möglich, ist mit Fremdherstellertools erstellte Images zu übernehmen. Unterstützt werden Images von Norton Ghost, Symantec Lifestate, Symantec Backup Exec System Recovery, StorageCraft ShadowProtect, Acronis True Image, Parallels, Microsoft Virtual PC, Microsoft Virtual Server, Hyper-V und VMware-VCB-Sicherungs-Images.

13.10.1 Installation der Sysprep-Tools zur Anpassung von Windows-Maschinen

Wie bereits im vorherigen Abschnitt erwähnt, müssen die Microsoft-Sysprep-Tools auf dem VMware vCenter-Converter-Server, auf dem der vCenter Converter ausgeführt wird, vorhanden sein. Anderenfalls ist das Anpassen der zu übernehmenden Maschine beim Import mit dem Converter nicht möglich.

Im Verzeichnis *%ALLUSERSPROFILE*

%\Application Data\VMware\VMware vCenter Converter

Standalone\sysprep befinden sich Ordner für verschiedene Betriebssysteme.

Verzeichnisname	Betriebssystem
xp	Windows XP
xp-64	Windows XP 64 Bit
srv2003	Windows Server 2003
srv2003-64	Windows Server 2003 64 Bit

Tabelle 13.7 Verzeichnisnamen für die Sysprep-Ablage

In den in Tabelle 13.7 genannte Ordner müssen Sie die passenden Sysprep-Tools kopieren. Sie finden die Sysprep-Dateien auf jeder Windows-CD im Verzeichnis *SUPPORT\TOOLS* in der Datei mit dem Namen *Deploy.cab*. Durch das Kopieren der Dateien in die entsprechenden Ordner ist es möglich, die Zielmaschine beim Import anzupassen.

13.10.2 VMware vCenter Converter Standalone

Nach dem Aufruf des Clients und dem Start zeigt sich Ihnen eine ganz eigene Oberfläche (Abbildung 13.72).

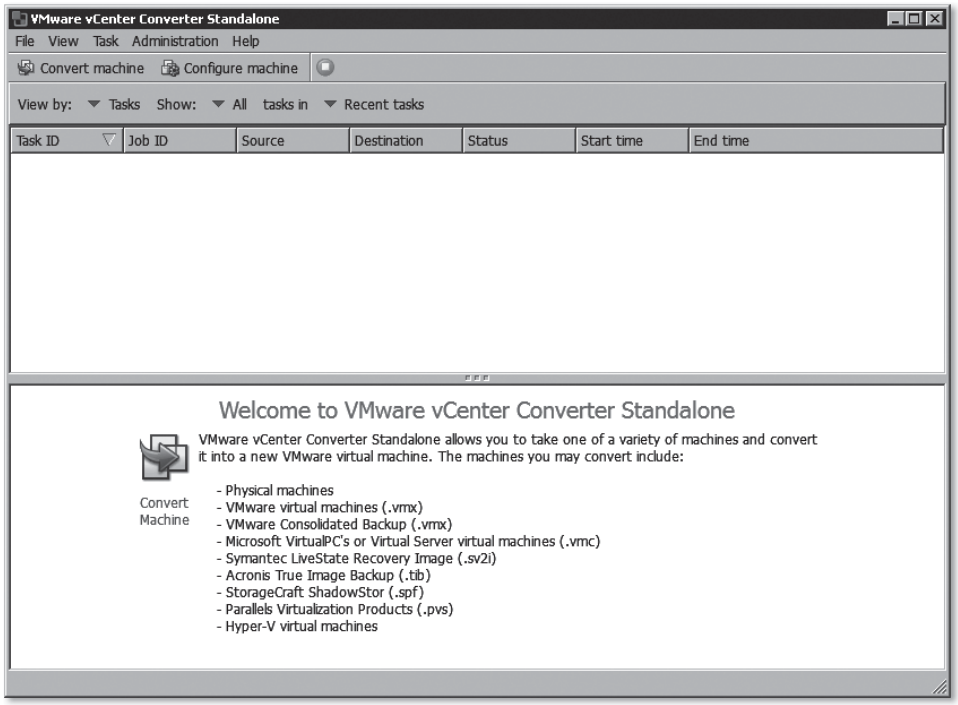


Abbildung 13.72 vCenter Converter Standalone

Über den Link Convert Machine starten Sie den Wizard für den Import eines Computers. Geben Sie direkt auf der ersten Seite die Daten der Quellmaschine ein (Abbildung 13.73).

Unter Select Source Type stehen Ihnen fünf Möglichkeiten zur Auswahl, die Optionen sind vielfältiger als bei der im vCenter integrierten Version. Die Varianten sind: Powered-on machine, VMware Infrastructure virtual machine, VMware Workstation or other VMware virtual machine, Backup image or third-party virtual machine and Hyper-V Server. Des Weiteren ist es möglich, entweder den lokalen Computer oder einen Rechner aus dem Netzwerk zu übernehmen. In Abbildung 13.74 sehen Sie als Übernahmebeispiel einen Computer aus dem Netzwerk.

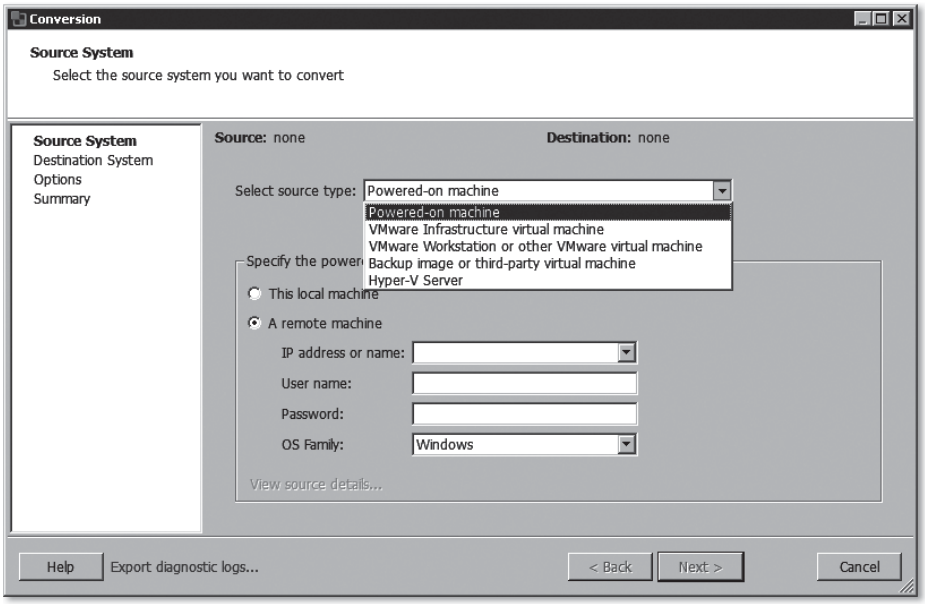


Abbildung 13.73 Daten der Quellmaschine

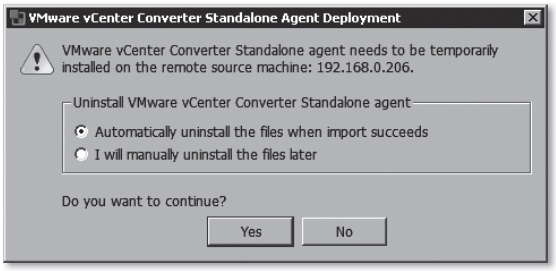


Abbildung 13.74 Verhalten für die Agenteninstallation

Nach einem Klick auf NEXT versucht die Applikation, sich mit der zu übernehmenden Maschine zu verbinden, und fragt anschließend nach dem Ziel. Dabei können Sie aus zwei unterschiedlichen Ansichten wählen, die Ihnen schon aus dem vSphere-Client bekannt sein sollten Das sind die Ansichten HOST AND CLUSTERS oder VMS AND TEMPLATES.

Mit YES beginnt die Verteilung des Agents auf das Quellsystem. Nach einigen Minuten ist der Agent installiert, und es geht an die Eingabe der Parameter für den Host, der die neue virtuelle Maschine aufnehmen soll (Abbildung 13.75). Sagen Sie nun dem System, wo die neue VM abgelegt wird und wie ihr Name sein soll.

Im folgenden Dialog müssen Sie dem System sagen, auf welchem Host die VM angelegt werden soll. Wählen Sie außerdem den Datastore und die Version der virtuellen Maschine. Eine Überprüfung der benötigten Ressourcen findet an dieser Stelle nicht statt.

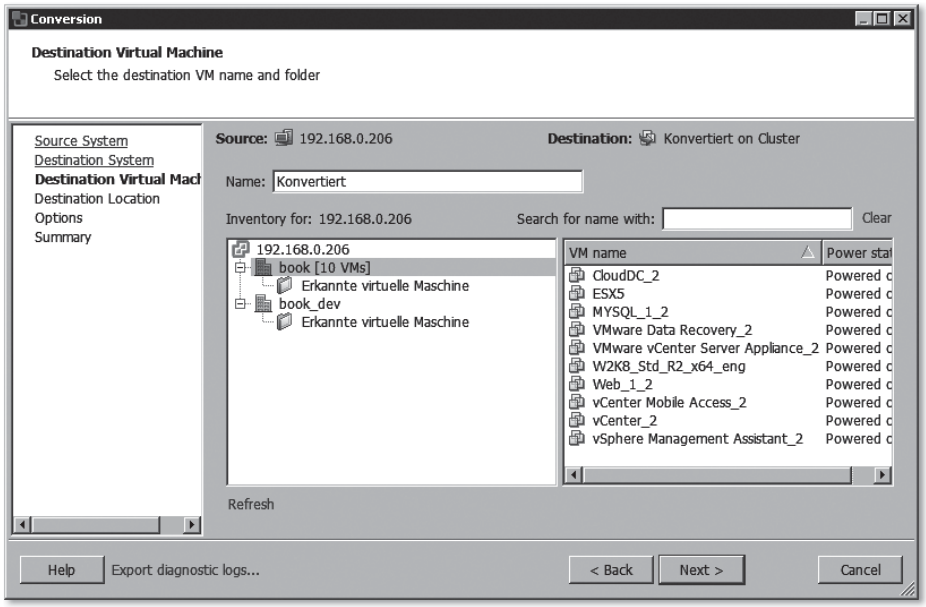


Abbildung 13.75 Ablageziel und Name der konvertierten VM

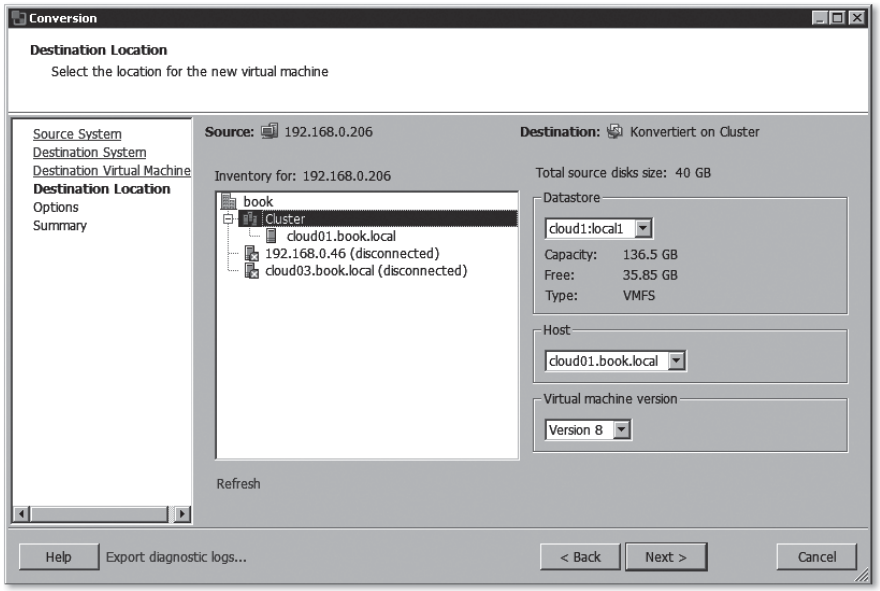


Abbildung 13.76 Ablageziel, Datastore, Host und VM-Version

Im folgenden Dialog können Sie alle Einstellungen für die zu konvertierende VM anpassen. Sie sehen schon, dass der Plattenplatz nicht ausreicht, das liegt aber daran, dass die Konvertierung noch mit einer Festplatte im Thick-Format durchgeführt würde.

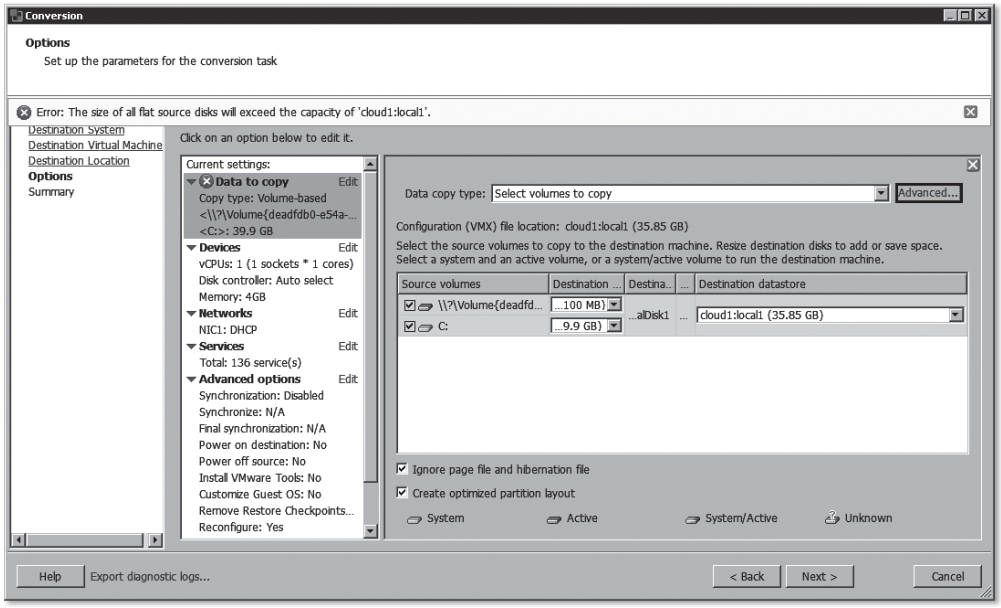


Abbildung 13.77 Anpassung der Festplatteneinstellungen

Options – Data to copy

DATA TO COPY ermöglicht die Anpassung der zu übernehmenden Festplatte. Sie können hier, das ist neu, immer noch den Datastore ändern. Wollen Sie weitergehende Änderungen am Layout vornehmen, wechseln Sie über den gleichnamigen Link in die ADVANCED-Ansicht. Es ist empfehlenswert, die beiden Auswahlfelder im unteren Bereich aktiviert zu lassen. Das optimiert zum einen die neue Zielmaschine und zum anderen die Performance der VM.

Der Reiter SOURCE VOLUMES stellt nur die Auswahl und Ansicht zur Verfügung, welche Festplatten übernommen werden sollen. Weitere Einstellungen sind hier nicht möglich.

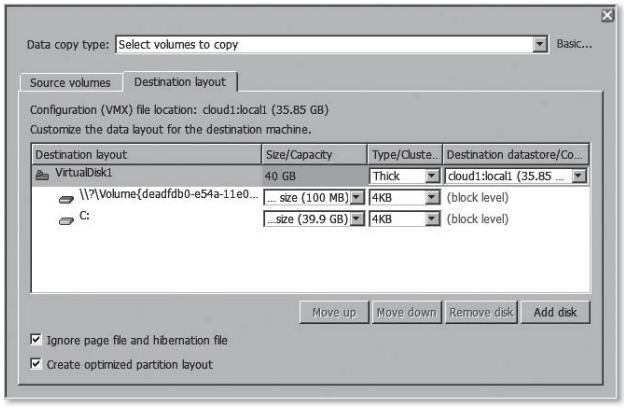


Abbildung 13.78 Festplattenkonfiguration

Richtig interessant ist der Reiter Destination Layout, er bietet weitergehende Konfigurationsoptionen (Abbildung 13.78). Auch hier können Sie selbstverständlich die Ziel-LUN noch einmal anpassen. Ein wohl wichtiger Punkt in diesem Dialog ist die Änderung des Plattentyps von Thick auf Thin oder umgekehrt. Bei der Auswahl Flat wird der gesamte Festplattenspeicher, den die virtuelle Festplatte benötigt, sofort allokiert, so wie es bis zu der Version VI3.x Standard war. Bei Thin wird nur der Plattenplatz belegt, der aktuell auch beschrieben ist.

Die angegebene Festplattengröße markiert die obere Grenze. Achten Sie bei der Nutzung dieser Option darauf, dass genügend freier Platz auf der LUN vorhanden ist. Selbst wenn zu Beginn nur ein Bruchteil der virtuellen Platte genutzt wird, kann der verwendete Plattenplatz ganz schnell steigen und dann Probleme verursachen.

Von Haus aus werden die Platten und Partitionen so abgebildet, wie die Aufteilung auf dem Quellsystem war. Möchten Sie diese Aufteilung ändern, fügen Sie über Add Disk eine neue Festplatte hinzu. Markieren Sie die Partition, die auf eine eigene Festplatte verschoben werden soll, und bringen Sie sie über die Buttons Move up oder Move Down an die gewünschte Position. Diese Vorgehensweise bietet den Vorteil, dass Sie im Nachhinein leicht die Größe einer Partition ändern können, ohne zuvor eine dahinterliegende Partition mit einer passenden Software verschieben zu müssen.

Ebenfalls extrem wichtig und neu in dieser Version des Converters ist die Anpassung der Blockgröße der Zielplatte. Hier haben Sie alle Mittel in der Hand, dafür zu sorgen, dass Sie ein optimales Partition-Alignment haben.

Options – Devices

Der folgende Dialog ist extrem komplex. Einen Großteil der Parameter des Zielcomputers können Sie an dieser Stelle anpassen (Abbildung 13.79). Auf die verschiedenen Optionen gehen wir jetzt einzeln ein. VMware gibt Ihnen durch eine Bewertung der einzelnen Punkte ein Hilfsmittel an die Hand: Ist vor den einzelnen Devices ein rotes oder gelbes Zeichen, sollten Sie sich die entsprechende Konfiguration genau anschauen; es ist nicht ausgeschlossen, dass es dort Probleme gibt.

Bei Devices können Sie mehrere Optionen anpassen: die Anzahl der CPUs bzw. Cores und die Größe des Arbeitsspeichers. Der wichtigste Punkt ist hier aber die Einstellung des Festplatten-Controllers. Es werden nur Controller angezeigt, die in dem System auch genutzt werden können. Ändern Sie den Controller-Type z. B. von IDE auf SCSI, ist es wichtig, dass Sie die VMware Tools automatisch mitinstallieren lassen, damit Ihr System später auch booten kann.

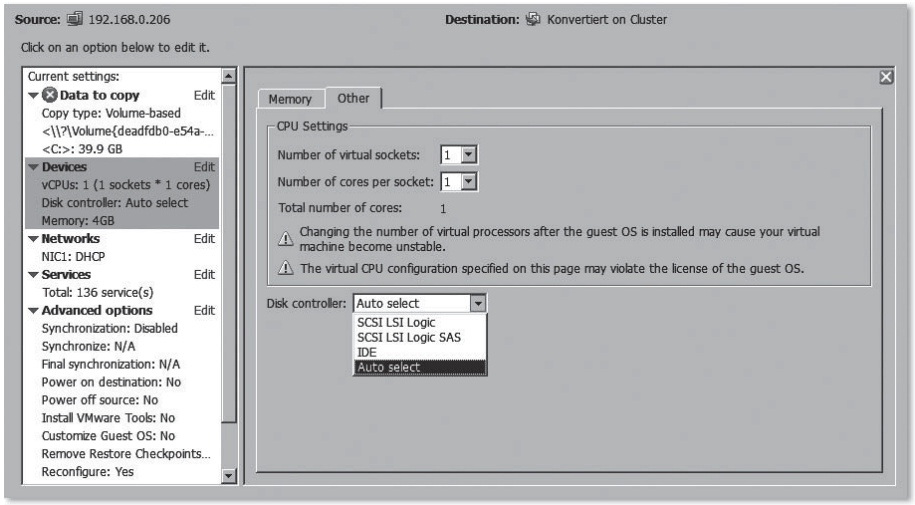


Abbildung 13.79 Anpassung der Parameter der Zielmaschine

Options – Networks

Unter NETWORKS stellen Sie das virtuelle Netzwerk ein, an dem die Zielmaschine angeschlossen werden soll. Den Verbindungsstatus beim Start des Computers bestimmten Sie in der rechten Spalte CONNECT AT POWER-ON (Abbildung 13.80).

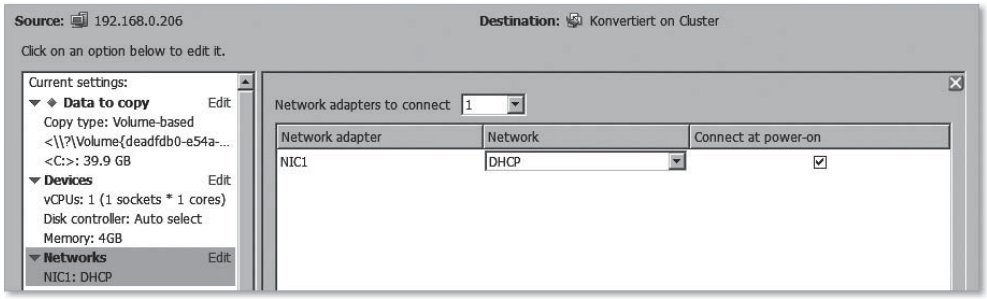


Abbildung 13.80 Konfiguration Netzwerk

Selbstverständlich können Sie zusätzliche Netzwerkkarten hinzufügen. Die Grenze liegt hier bei 10 Adaptern.

Options – Services

SERVICES bietet eine Anpassung der Dienste, sowohl auf dem Quell- als auch auf dem Zielsystem (Abbildung 13.81). Gibt es Dienste, die beim Import besser nicht aktiv sein sollten, so sind sie hier zu deaktivieren. Schauen Sie dazu auf dem Reiter SOURCE SERVICES. Wir denken da z. B. an einen SQL-Server oder ähnliche Dienste, hinter denen sich ein starkes Änderungspotential auf der Festplatte verbergen kann. Nicht alle Dienste sind manipulierbar, aber ein Großteil der

installierten. Die Startart aller Dienste des Zielsystems ist hingegen anpassbar. Beachten Sie, dass der Computer einige Services auf jeden Fall benötigt, damit er starten kann.

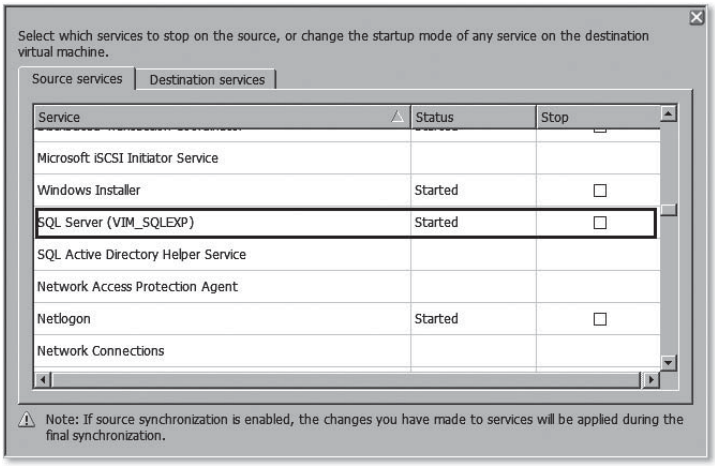


Abbildung 13.81 Dienste-Einstellungen

An dieser Stelle können Sie bereits eingreifen und Dienste auf dem Zielsystem deaktivieren, die über die Systemtools des Server-Hardware-Herstellers installiert wurden. Wechseln Sie dazu auf den Reiter Destination Services. Grundsätzlich sollten Sie aber bei einer Eins-zu-eins-Übernahme an dieser Stelle sehr vorsichtig mit den Änderungen sein.

Options – Advanced Options

Unter Advanced options geben Sie an, welche Aktionen im Rahmen der Übernahme zusätzlich durchgeführt werden sollen (Abbildung 13.82). Dabei wird unterschieden zwischen Aktionen vor dem Abschluss der Übernahme und nach der Übernahme.

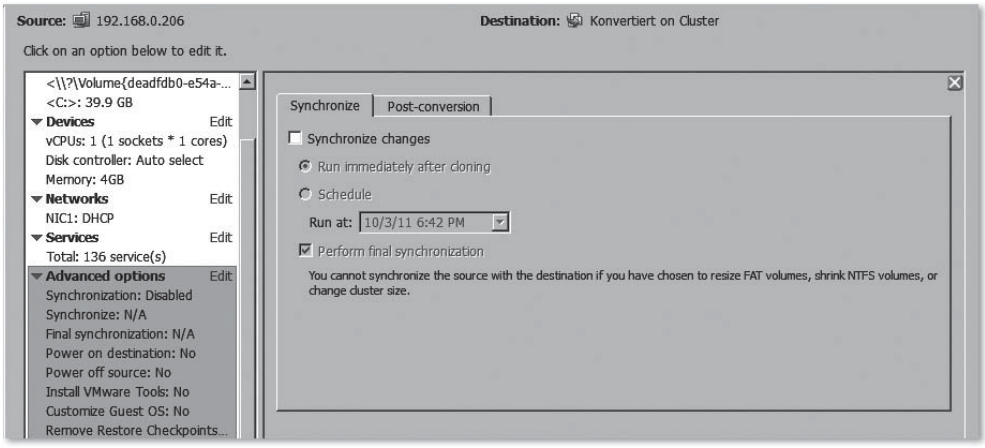


Abbildung 13.82 »Advanced Options« beim vCenter Converter Standalone vor Übernahmeabschluss

Synchronize changes bewirkt, dass nach der kompletten Übernahme des Quellsystems alle nicht benötigten Dienste angehalten und die bis zu diesem Zeitpunkt aufgelaufenen Änderungen im Content auf das Zielsystem synchronisiert werden. Diesen Job können Sie zeitgesteuert oder sofort nach dem Abschluss der Übernahme starten.

Hinweis

Es gibt Randbedingungen, die die Synchronisierung verhindern. Dazu gehören das Ändern von FAT-Partitionen, das Verkleinern von NTFS-Partitionen oder das Anpassen der Cluster-Größe der Festplatte.

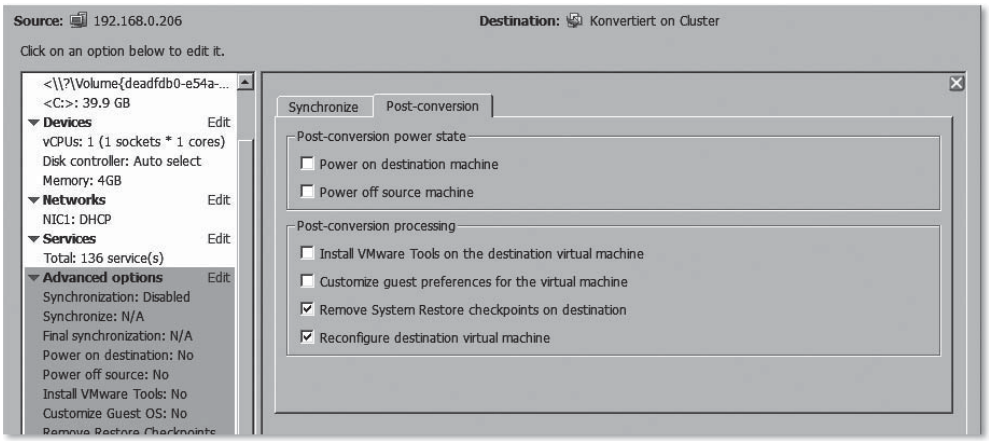


Abbildung 13.83 Verhalten nach der Übernahme

Die nächsten Punkte steuern das Verhalten von Quell- und Zielsystem nach der Übernahme. Sie können die Quellmaschine nach dem Vorgang automatisch starten (Power on Destination machine), oder Sie lassen das Ziel ausgeschaltet (Power off source machine). Achten Sie darauf, dass nicht beide Maschinen gleichzeitig aktiv sind, denn dann wären zwei identische Server im Netz, was zu Problemen führen kann. Install VMware Tools on the Destination virtual Machine ist an sich selbsterklärend. Wir empfehlen, diese Option zu aktivieren.

Der folgende Punkt, Customize guest preferences for the virtual machine, ermöglicht die Anpassung der Systemkonfiguration eines Windows-Servers. Es werden die Eingaben für die in Tabelle 13.8 genannten Punkte erwartet.

Optionen	Parameter
Computer-Informationen	Computername Benutzername Organisationsname Erstellung einer neuen SID

Tabelle 13.8 Parameterübersicht für die Anpassung von Windows-Systemen

Optionen	Parameter
Windows-Lizenz	Einstellung der Lizenzierungsart, pro Server oder pro Arbeitsplatz
Zeitzone	Einstellen der Zeitzone
Netzwerk	Hier stellen Sie die Netzwerkparameter ein.
Arbeitsgruppe/Domain	Steht das Zielsystem in einer Arbeitsgruppe, oder soll es Mitglied einer Domäne sein?

Tabelle 13.8 Parameterübersicht für die Anpassung von Windows-Systemen (Forts.)

Remove System Restore checkpoints on destination entfernt alle gesetzten Punkte der sogenannten Systemwiederherstellung unter Windows, die es ermöglicht, das System zu einem bestimmten Zeitpunkt wiederherzustellen. In den meisten Fällen ist es nicht nötig, im späteren virtuellen System auf diese Punkte zuzugreifen. Reconfigure destination virtual machine installiert die nötigen Device-Treiber. Diese Option sollten Sie auf jeden Fall aktivieren.

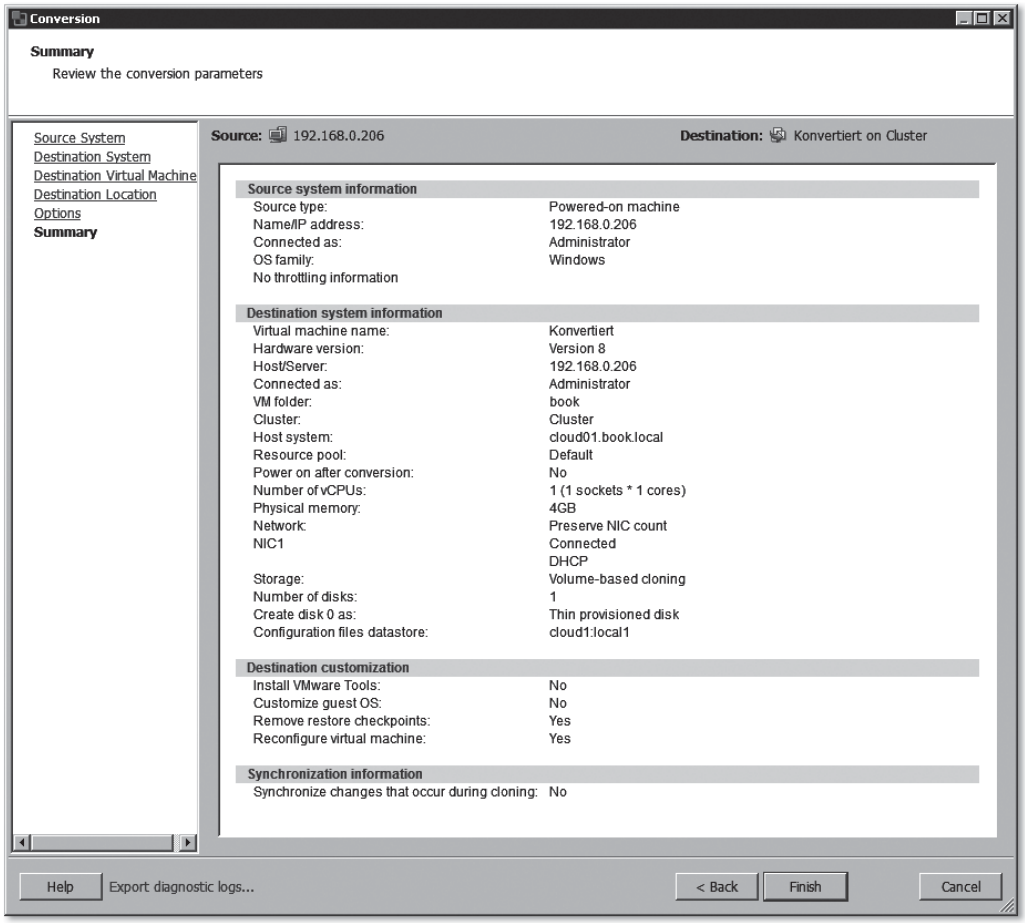


Abbildung 13.84 Zusammenfassung der Übernahme

Nach der Betätigung von Next erscheint eine Zusammenfassung aller Einstellungen. Sollten noch Defizite, also Unstimmigkeiten bei der Konfiguration, vorhanden sein, werden Sie oben im Fenster darauf hingewiesen. Mit Finish starten Sie den Import der Maschine. Der Vorgang nimmt je nach Größe der Quellmaschine eventuell längere Zeit in Anspruch. Im Hauptfenster wird jetzt der Job angezeigt, und Sie können dort den aktuellen Status des Jobs während der Konvertierung kontrollieren.

13.10.3 Nacharbeiten nach der Übernahme

Bevor Sie die importierte Maschine starten, sollten Sie sich die Konfiguration der virtuellen Maschine anschauen. Löschen Sie die Hardwarekomponenten, die Sie nicht benötigen, so z. B. serielle Schnittstelle, parallele Schnittstelle und Audio. Achten Sie auch darauf, dass bei Wechselmedien das Client-Device eingestellt ist. Verbinden sollten Sie Floppy und CD-ROM nur, wenn Sie sie benötigen. Unter Umständen ist es später sehr zeitaufwendig, ein verbundenes CD-ROM zu suchen. Dies kann zu Problemen in der virtuellen Infrastruktur führen und auch Funktionen aushebeln.

Ist der Server dann gestartet, sollten Sie die gesamte installierte Software auf den Prüfstand stellen. Deinstallieren Sie alle vom Hardwarehersteller gelieferten Tools, wie Treiber für Remote-Konsole, RAID-Treiber, Netzwerktreiber und Konfigurationstools für die Computerhardware. Nach der systemspezifischen Software geht es den überflüssigen Treibern des Windows-Systems an den Kragen. Legen Sie dazu eine neue System-Environment-Variable an. Sie lautet `devmgr_show_nonpresent_devices` mit dem Wert 1. Anschließend rufen Sie den Gerätemanager und den Menüpunkt Ansicht • Ausgeblendete Geräte auf. Jetzt können Sie die nicht benötigten Gerätetreiber deinstallieren. Eine relativ einfache Richtschnur ist, sich alle Treiber anzuschauen, die mit einem ausgegrauten Symbol markiert sind. Haben Sie die Arbeiten abgeschlossen, sollten Sie den Computer neu starten. Jetzt kann die Maschine nach einem ausführlichen Applikationstest den Job des alten Servers übernehmen.

Sie können sich die Arbeit auch erleichtern: Es gibt im Netz eine ISO-Datei, die die Arbeit für Sie übernehmen kann. Sie finden den Artikel und den Downloadlink unter:

http://communities.vmware.com/docs/DOC-15187/version/4

Die Vorgehensweise ist dabei ganz einfach: Setzen Sie zuerst, wie bereits beschrieben, die Environment-Variable. Mounten Sie anschließend das heruntergeladene ISO-Image in die VM, und öffnen Sie eine Eingabeaufforderung. Wechseln Sie anschließend auf das ISO, und wählen Sie das für Ihr System richtige Unterverzeichnis.

Windowsversion	Unterverzeichnis
Windows 32 Bit	*i386*
Windows 64 Bit	*x64*
Windows für Itanium-Systeme	*ia64*

Tabelle 13.9 Zuordnung Unterverzeichnis zu Windows-Versionen

In dem Unterverzeichnis befindet sich eine Datei mit dem Namen *removedevices.js*. Starten Sie sie, und die nicht benötigten Gerätetreiber werden für Sie automatisch entfernt.

13.11 Einsatz der vSphere Storage Appliance

Nach der Installation des VSA-Managers finden Sie auf dem Datacenter-Objekt im vSphere-Client einen neuen Reiter VSA MANAGER. Über diesen Reiter erfolgen die Bereitstellung eines VSA-Clusters und der Betrieb des Konstrukts. Haben Sie noch keinen Cluster eingerichtet, stellt sich der Reiter dar wie in Abbildung 13.85.

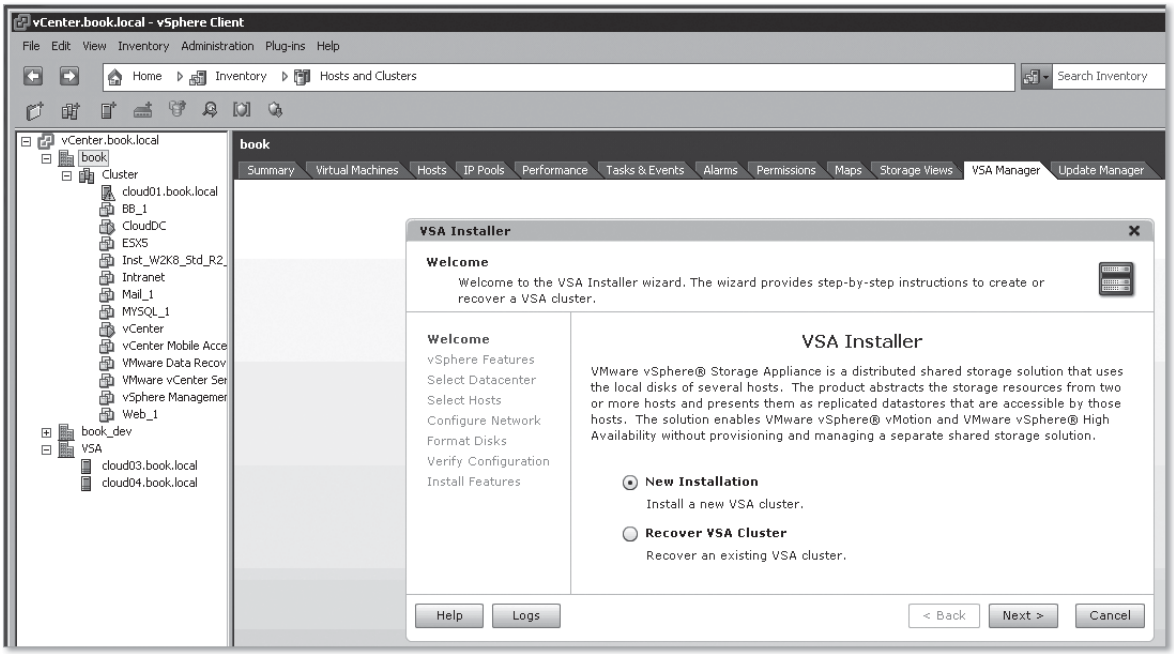


Abbildung 13.85 Konfiguration eines VSA-Clusters

Bevor wir Ihnen zeigen, wie Sie einen Cluster konfigurieren, sollten Sie sich eine Tabelle mit den benötigten IP-Adressen anlegen. Unser Vorschlag findet sich in den folgenden Tabellen mit den verwendeten IP-Adressen, so können Sie sehen, in welchen Netzen die Anbindung erfolgen muss. Für die Punkte, an denen Sie per DHCP vergebene Adressen nutzen können, haben wir das entsprechend markiert.

System	IP-Adressen
vCenter-Server	192.168.0.206
ESXi-Server 1 Management	192.168.0.192
ESXi-Server 2 Management	192.168.0.193
ESXi-Server 3 Management (nur beim Drei-Knoten-Cluster)	192.168.0.194 (Wir haben nur einen Zwei-Knoten-Cluster konfiguriert.)

Tabelle 13.10 Vorhandene IP-Adressen von Hosts und vCenter-Server

Es folgen die IP-Adressen des Clusters und des Service.

System	IP-Adressen
VSA-Cluster	192.168.0.170
VSA-Cluster-Service (nur beim Zwei-Knoten-Cluster)	192.168.0.171

Tabelle 13.11 IP-Adressen des Clusters

Abschließend benötigen Sie noch die zusätzlichen Adressen für die Hosts.

Hosts	System	IP-Adressen
Host 1	Management-IP-Adresse VSA 1	192.168.0.172
	Datastore-IP-Adresse VSA 1	192.168.0.173
	Backend-IP-Adressen VSA 1 (Heart-IP-Adresse)	192.168.100.1
	Feature-IP-Adresse (DHCP möglich)	192.168.0.178
Host 2	Management-IP-Adresse VSA 2	192.168.0.174
	Datastore-IP-Adresse VSA 2	192.168.0.175
	Backend IP-Adressen VSA 2 (Heart-IP-Adresse)	192.168.100.2
	Feature-IP-Adresse (DHCP möglich)	192.168.0.179
Host 3 (nur beim Drei-Knoten-Cluster)	Management-IP-Adresse VSA 3	192.168.0.176
	Datastore-IP-Adresse VSA 3	192.168.0.177
	Backend-IP-Adressen VSA 3 (Heart-IP-Adresse)	192.168.100.3
	Feature-IP-Adresse (DHCP möglich)	192.168.0.180

Tabelle 13.12 Zusätzliche Host-IP-Adressen für den VSA-Cluster

Starten Sie die Konfiguration über den Reiter VSA Manager und den entsprechend benannten Auswahlpunkt. Es wird Ihnen im Folgenden angezeigt, welche Komponenten aktiviert bzw. installiert werden.

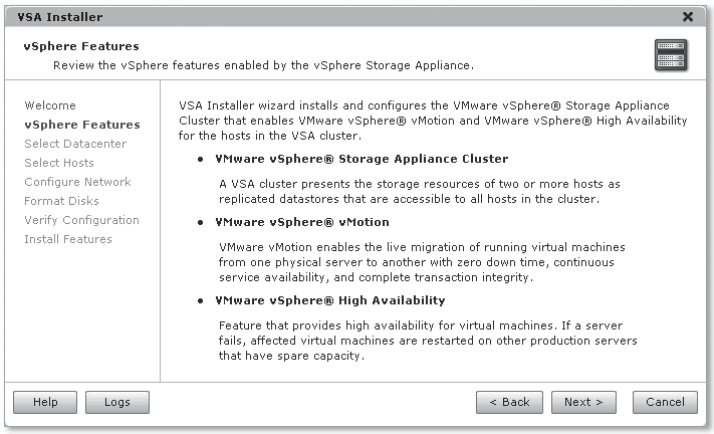


Abbildung 13.86 Für den VSA-Cluster benötigte Komponenten

Sie sehen im nächsten Dialog eine Anzeige aller im vCenter gefundenen Datacenter, denn jedes Datacenter ist ja ein potentieller Ort für einen VSA-Cluster. Wählen Sie einfach das passende Datacenter aus, und Ihnen werden alle Hosts des Datacenters angezeigt, die für einen Cluster genutzt werden können. Dabei wird zwischen den unterschiedlichen CPU-Typen unterschieden. Wählen Sie die zu nutzenden Hosts aus, und setzen Sie die Konfiguration fort. Sollten Sie hier Fehler finden, dann rühren diese meist daher, dass die Hosts nach der Installation schon weitergehend konfiguriert wurden. Bei Problemen im Netzwerkumfeld kann es helfen, in der Konsole auf dem Server die Netzwerkanbindung einmal zurückzusetzen.

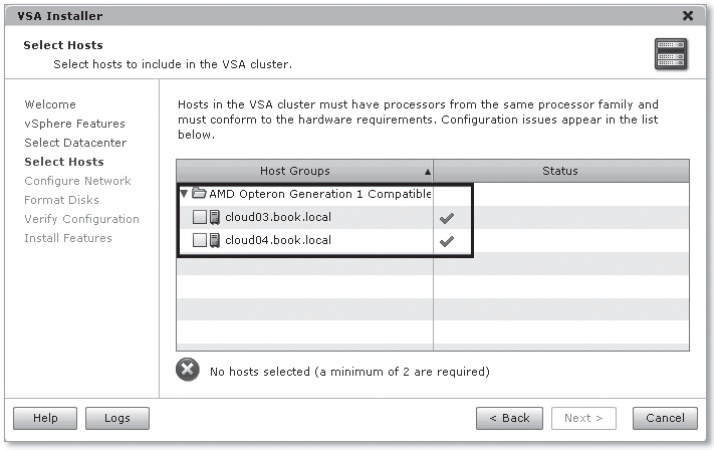


Abbildung 13.87 Auswahl der Mitglieder des Clusters

Ist die Host-Auswahl ohne Beanstandungen, dann wird aus dem roten Kreuz unten ein grüner Haken, und es folgt die Eingabe der IP-Adressen.

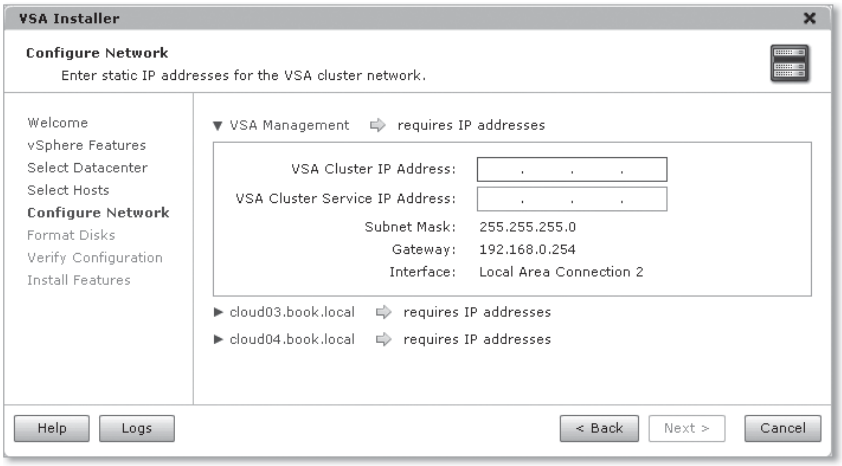


Abbildung 13.88 IP-Adress-Vergabe beim VSA-Cluster

Hier geben Sie die IP-Adressen ein, die Sie sich zuvor für den Cluster herausgesucht haben. Die Adressen werden bei der Eingabe überprüft, und das Ergebnis zeigt sich sofort in der Eingabemaske. Nun müssen Sie festlegen, wie mit dem Plattenplatz umgegangen werden soll. Soll die Formatierung direkt während der Installation erfolgen oder erst beim ersten Zugriff? Bedenken Sie bei der Auswahl, dass die Formatierung während der Einrichtung den Konfigurationsprozess verlängert, aber die Formatierung muss durchgeführt werden, ob nun direkt oder später.

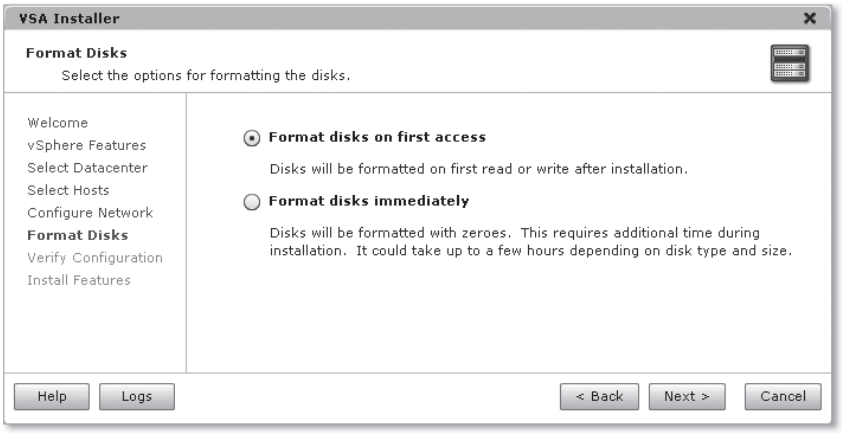


Abbildung 13.89 Formatierungsverhalten des Datastores

Sie sehen nun eine Zusammenfassung und können nach Bestätigung die Konfiguration anstoßen. Nur ein Hinweis, dass alle Daten auf den Datenplatten gelöscht werden, steht nun noch zwischen Ihnen und der Einrichtung.

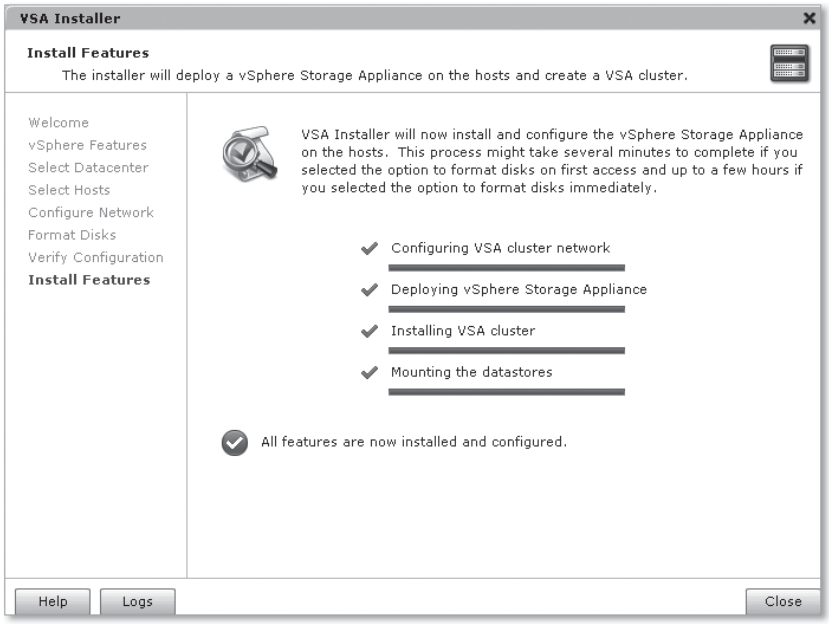


Abbildung 13.90 Erfolgreich abgeschlossene Installation

Nach der erfolgreich abgeschlossenen Konfiguration des VSA-Clusters finden Sie in der Übersicht die passend konfigurierten Systeme vor. Über den VSA MANAGER-Reiter können Sie dann die weitergehenden Konfigurationsarbeiten durchführen.

Die Installationsroutine hat automatisch einen HA-Cluster erstellt und in diesem die Ressourcen passend gesetzt. Die Failover-Kapazität ist auf 50 % gesetzt. So wird gewährleistet, dass immer ausreichend Ressourcen zur Verfügung stehen. Sie sehen auch, dass es keinen lokalen Datastore mehr gibt Abbildung 13.91, der eine nutzbare Menge von Plattenplatz hat. Sie sehen unter dem Punkt STORAGE nur die Reste des lokalen Plattenplatzes, die die Routine nicht vereinnahmt hat. Angelegt werden die virtuellen Maschinen nur auf dem Plattenplatz, der per NFS zur Verfügung gestellt wird. Es hat somit kein Cluster-Knoten lokal nutzbaren Platz.

Werfen wir einen Blick auf die Netzwerkkonfiguration. Sie sehen hier in der Abbildung 13.92 eine sauber beschriftete Netzwerkkonfiguration. So ist sofort klar, welche Portgruppe welche Funktion abbildet.

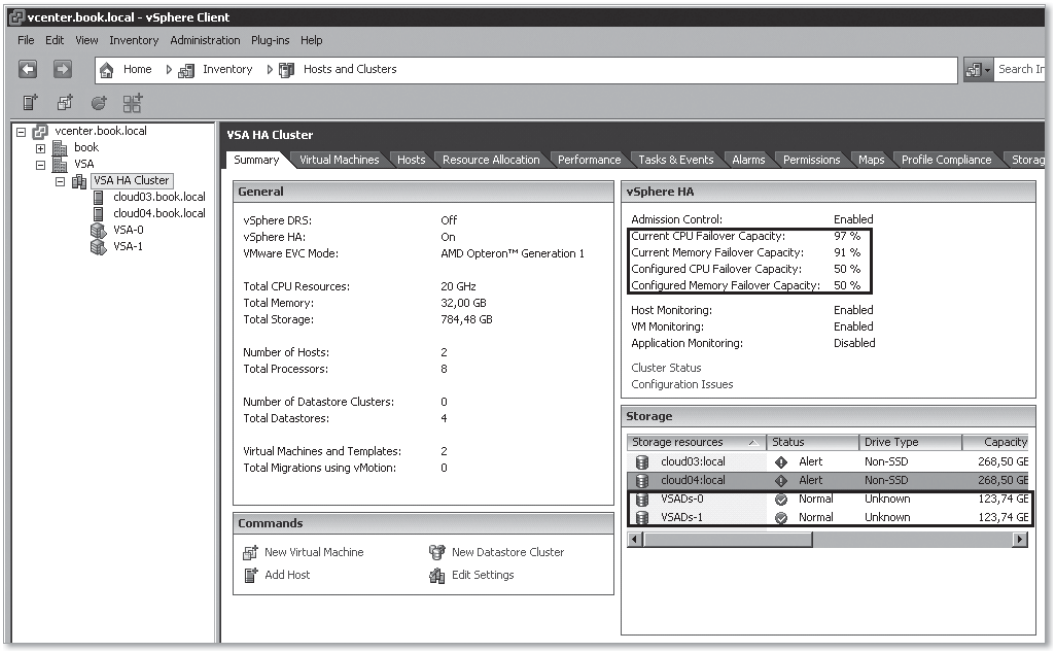


Abbildung 13.91 Ressourcen des VSA-Clusters

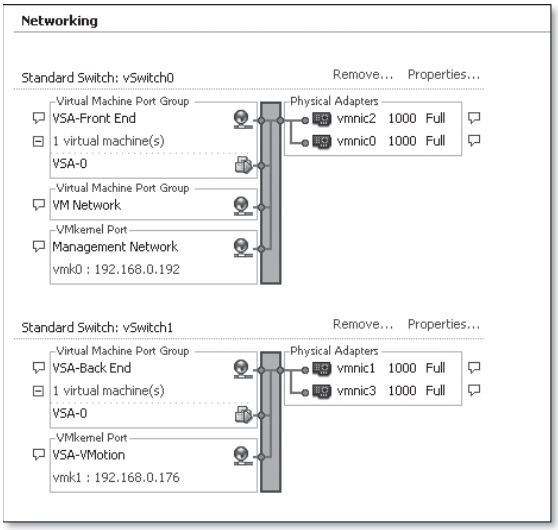


Abbildung 13.92 Switch- und Portgruppenkonfiguration des VSA-Clusters

Lassen Sie uns nun noch einen Blick auf die Konfiguration werfen. Dazu wechseln Sie wieder auf den Reiter VSA Manager. Dort finden Sie jetzt eine dreiteilige Darstellung. Schauen wir zu Beginn auf die Anzeige der Datastores.

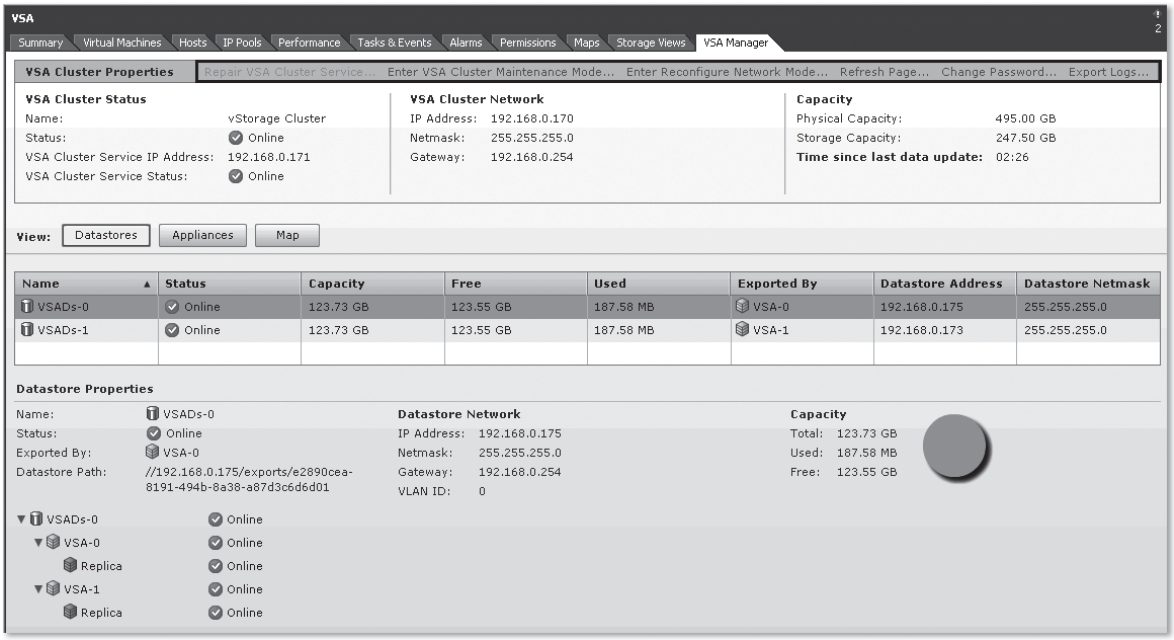


Abbildung 13.93 Übersichtsfenster zu den Datastores des VSA-Clusters

Sie sehen die Datenmengen und den Status des Storages sowie seiner Replikas. Hinter dem Button APPLIANCE finden Sie den Status der virtuellen Maschinen, die die Bereitstellung des NFS-Storages regeln.

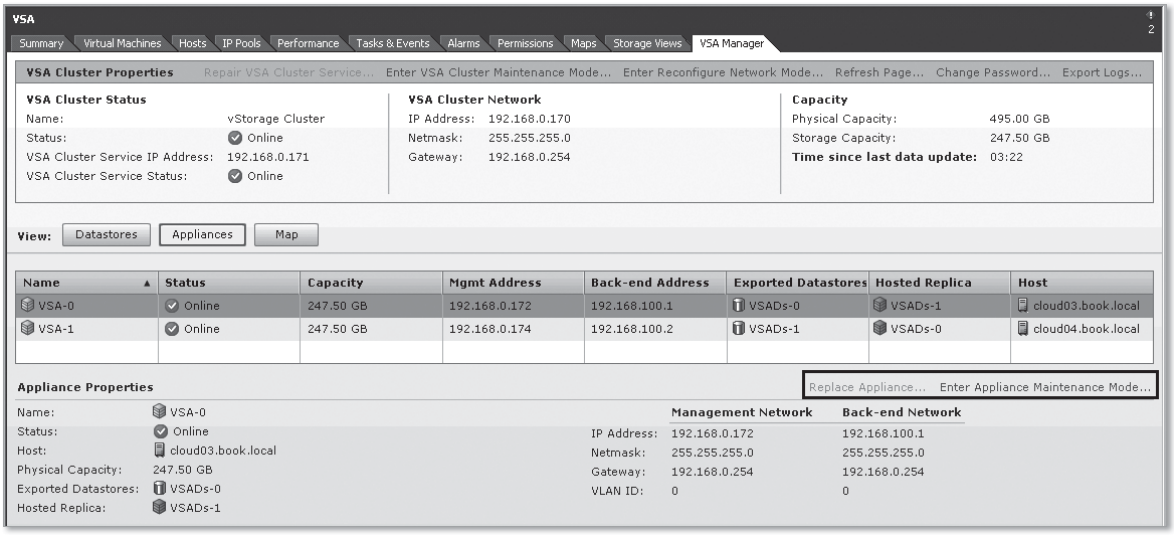


Abbildung 13.94 Übersichtsfenster VSA

Dieses Fenster zeigt die Konfigurationseinstellungen der Appliance. Wie beim ESXi-Host gibt es auch hier einen Maintenance-Modus für Wartungsarbeiten. Über Replace Appliance... ist es möglich, einen defekten ESXi-Host aus einem VSA-Verbund zu ersetzen. Der Knopf Map zeigt Ihnen das Konstrukt des VSA-Clusters in einer grafischen Übersicht an.

Über die Links im oberen Bereich des Fensters administrieren Sie den Cluster. In Abbildung 13.93 sehen Sie die einzelnen Konfigurationspunkte. Beginnen wir mit der Reparatur des Cluster Dienstes. Sollte der Cluster-Dienst angehalten sein oder nicht funktionieren, so wird er in der Oberfläche als Offline markiert. In diesem Fall können Sie über den Link Repair VSA Cluster Service... die Verbindung vom Cluster zum Dienst auf dem vCenter-Server wiederherstellen. Das ist aber nur relevant, wenn Sie einen Zwei-Knoten-Cluster haben.

Zur Verwaltung des Clusters können Sie diesen in seiner Gesamtheit in dem Maintenance-Modus versetzen; wählen Sie dazu den Link Enter VSA Cluster Maintenance Mode aus. Um die Netzwerkkonfiguration anzupassen, verwenden Sie den Link Enter Reconfigure Network Mode. Bis auf die VSA-Systeme müssen alle virtuellen Maschinen heruntergefahren werden, dann können Sie die Anpassungen vornehmen.

Das Passwort des VSA-Accounts ändern Sie unter dem Link Change Password. Dazu müssen Sie wissen, dass während der Installation ein User angelegt wird:

- User: »svaadmin«
- Passwort: »svapass«

Auf Wunsch ändern Sie das Passwort. Der letzte Punkt, Export Logs, spricht ebenfalls für sich selbst: Laden Sie hier die Log-Dateien des Clusters zur weiteren Analyse herunter.

13.11.1 Virtuelle Maschinen auf einem VSA-Cluster

Das Anlegen von virtuellen Maschinen in einem VSA-Cluster unterscheidet sich in keiner Weise von dem Anlegen von VMs in anderen Umgebungen. Es ist aber wichtig zu wissen, dass Memory-Overcommitment nicht unterstützt ist und dass das Swapping ebenfalls nicht zur Stabilität beiträgt. Die Deaktivierung des Memory-Overcommitments erfolgt über die Ressourcen der VM. Aktivieren Sie die Auswahl Reserve all guest memory in den Speichereinstellungen, so ist dem ersten Punkt Rechnung getragen. Das VMX-Swapping deaktivieren Sie in den Eigenschaften der VM. Gehen Sie dazu auf den Reiter Option, und wählen Sie den Unterpunkt Advanced/General aus. Über den Knopf Configuration Parameters gelangen Sie in das Fenster für die Eingabe von zusätzlichen Parametern. Fügen Sie hier den Parameter sched.swap.vmxSwapEnabled hinzu, und setzen Sie ihn auf den Wert false. Damit sind die Konfigurationsarbeiten an den virtuellen Maschinen abgeschlossen.

13.11.2 Deinstallation eines VSA-Clusters

Die Deinstallation eines VSA-Clusters geht nicht einfach über die Systemsteuerung des vCenter-Servers oder über den vSphere-Client. Für die Deinstallation müssen Sie auf dem vCenter-Server in das Verzeichnis *C:\Program Files\VMware\Infrastructure\tomcat\webapps\VSAManager\WEB-INF\test\tool* wechseln. Hier befinden sich verschiedene Dateien, mit denen Sie unter anderem einen VSA-Cluster deinstallieren können. Durchführen können Sie diese Aufgabe mit der Batch-Datei *cleanup.bat*. Der Aufruf der Datei wird aber unweigerlich in einem Fehler enden. Das hängt damit zusammen, dass die Environment-Variable `%JAVA_HOME%`, die in der Datei genutzt wird, nicht besetzt ist. Besetzen Sie die Variable mit dem Wert:

```
JAVA_HOME = C:\Program Files\VMware\Infrastructure\jre
```

Jetzt ist es möglich, den Cluster zu deinstallieren.

Dieses Kapitel beschäftigt sich mit der Ausfallsicherheit und der Hochverfügbarkeit der virtuellen Infrastruktur und ihrer Komponenten. Die Sicherung von Hosts und VMs ist genauso Bestandteil wie die Konfiguration eines Microsoft Cluster Services.

14 Ausfallsicherheit

Autor dieses Kapitels ist Bertram Wöhrmann, Ligarion, bwoehrmann@ligarion.de

Zur Abbildung der Funktionen müssen Sie sich nicht nur auf dem Third-Party-Markt orientieren, auch VMware bietet Software-Add-ons an, mit denen Sie solche Aufgaben durchaus lösen können.

14.1 Sicherung – Rücksicherung

Eines der wichtigsten Themen beim Betrieb einer virtuellen Infrastruktur ist die Sicherung der verschiedenen Komponenten. Zur Datensicherung der virtuellen Maschinen kommen noch Sicherungen der VMware-vSphere-Hosts hinzu. Des Weiteren ist eine Backup-Strategie für den vCenter-Server, die zugehörige Datenbank und weitere Komponenten der Infrastruktur zu erarbeiten. Es gibt verschiedene Alternativen, diese Aufgaben zu erfüllen. In diesem Kapitel gehen wir auf verschiedene Möglichkeiten ein, die einzelnen Komponenten zu sichern.

14.1.1 Sicherung des ESX-Hosts

Wie geht man nun mit der Sicherung der Host-Systeme um? Schauen wir einmal zurück, wie ein Host installiert wird und welche Daten er vorhält.

Die Installation eines vSphere-Hosts geht grundsätzlich sehr schnell. Der Zeitfaktor wird nur dadurch beeinflusst, wie die Installation erfolgt, ob manuell, per Skript oder über eine Installations-Appliance. Die Daten, die ein Host vorhält, sind eigentlich nur Konfigurationsdaten. Alle anderen Informationen gehören zu den virtuellen Maschinen und liegen auf dem Datastore oder in der Datenbank des vCenter-Servers. Mit dem Wegfall der Version ESX entfallen verschiedene Optionen, wie z. B. die Installation eines Datensicherungs-Clients direkt in der Service Console.

Es ist sinnlos, über die Sicherung nachzudenken, wenn Sie aufgrund der Lizenzierung mit Hostprofilen arbeiten können. In diesem Fall gestaltet sich der Prozess der Inbetriebnahme nach der Installation recht einfach. Steht die Funktion der Hostprofile lizenztechnisch nicht

zur Verfügung, können Sie sie auch mit dem Befehl `vicfg-cfgbackup` sichern. Mit der PowerCLI können Sie ebenfalls ein passendes Skript nachbauen, um die Konfiguration zu sichern, bzw. zurückzuschreiben. Anbei die passenden Skripte dazu, die Sie in der Community finden können:

Sicherung:

```
function LoadSnapin{
  param($PSSnapinName)
  if (!(Get-PSSnapin | where {$_.Name   -eq $PSSnapinName})){
    Add-pssnapin -name $PSSnapinName
  }
}

# Load PowerCLI snapin
LoadSnapin -PSSnapinName "VMware.VimAutomation.Core"

# Variables
[string] $vCenter = "vcenter.domain.local" # vCenter FQDN
[string] $BackupPath = "C:\Host_Backup" # Folder to copy the Host backups to

# Connect to vCenter
Connect-VIServer -Server $vCenter
# Get All Connected Hosts
$eVMHs = Get-View -ViewType HostSystem |?{$_.config.product.ProductLineId
  -eq "embeddedEsx"} |?{$_.Runtime.ConnectionState -eq "connected"}

# For each Host in All Connected Hosts
Foreach ($eVMH in $eVMHs)
{
    # Backup Host config
    Set-VMHostFirmware -VMHost $eVMH.name -BackupConfiguration
      -DestinationPath $BackupPath
}
```

Rücksicherung:

```
function LoadSnapin{
  param($PSSnapinName)
  if (!(Get-PSSnapin | where {$_.Name   -eq $PSSnapinName})){
    Add-pssnapin -name $PSSnapinName
  }
}

# Load PowerCLI snapin
LoadSnapin -PSSnapinName "VMware.VimAutomation.Core"
```

```
# Variables
[string] $vCenter = "vcenter.domain.local" # vCenter FQDN
[string] $backupFile = "C:\Host_Backup\configBundle-
esx01.domain.local.tgz" # ESX(i) host backup file
[string] $esxHost = "esx01.domain.local" # FQDN of ESX(i) to be restored
[string] $esxAccount = "root" # local ESX(i) account for the Host to be restored
[string] $esxPasswd = "password" # password for ESX(i) account named above

# Connect to ESX(i) Host
connect-viserver -Server $esxHost -User $esxAccount -Password $esxPasswd

# Put host in maintenance mode
set-VMHost -vmhost $esxHost -state Maintenance
# Get Host Firmware
Get-VMHostFirmware -VMHost $esxHost
# Restore Host Firmware
Set-VMHostFirmware -VMHost $esxHost  -Restore -SourcePath $backupFile -Force

# Disconnect from Host
Disconnect-VIServer -Server $esxHost -Confirm:$false
```

Nähere Informationen zu den Skripten finden Sie unter

http://techdump.co.uk/2011/10/esxi-host-configuration-backup-and-restore-script-using-powercli/

Mit einem Installationsskript oder einer Installations-Appliance sind Neuinstallationen in sehr kurzer Zeit möglich. Das wird eben mit den neuen Funktionen Image Builder und Auto Deploy sehr stark vereinfacht.

Aus unserer Sicht investieren Sie die Zeit, sich mit den neuen Funktionen vertraut zu machen, für eine optimierte automatisierte Installation. Damit schlagen Sie zwei Fliegen mit einer Klappe: Zum einen ist das System im Fehlerfall schnell wieder am Start, zum anderen können Sie neue Systeme schneller in Betrieb nehmen. Setzen Sie nicht die Enterprise-Plus-Lizenz ein, können Sie nicht auf die Auto-Deploy-Funktion zurückgreifen. Es steht Ihnen aber die Option offen, mit dem Image Builder ein für Sie passendes Image zu erstellen. Dieses können Sie über andere Installations-Appliances wie z. B. die EDA verteilen.

14.1.2 Sicherung der Komponenten

Der erste Teil dieses Abschnitts beschäftigt sich mit allgemeinen Möglichkeiten, die verschiedenen Komponenten zu sichern, die für den Betrieb einer virtuellen Landschaft nötig sind. Dabei gehen wir nicht näher auf spezielle Produkte ein. Wir möchten darlegen, was wie gesichert werden sollte bzw. gesichert werden kann.

Wir können Ihnen natürlich nur Empfehlungen geben und technisch darstellen, was möglich ist. In vielen Unternehmen gibt es aber Richtlinien, die dem Administrator erst einmal keinen Spielraum für die Vorgehensweise beim Thema Datensicherung und Datenrücksicherung lassen. Es kann also gut sein, dass Sie erst Entwicklungsarbeit leisten müssen, damit Sie den technisch optimalen Weg gehen können.

Sicherung des Managements

Wir gehen davon aus, dass alle Applikationskomponenten auf einem Server installiert sind. Lediglich die Datenbank kann auch auf einem anderen Server bereitgestellt werden. Für die grundsätzliche Strategie zur Sicherung der betroffenen Server ist es entscheidend, ob Applikationen und Datenbank auf einem System liegen oder nicht. Schon bei der Abwägung, ob Datenbank und Applikation voneinander getrennt werden, sollten Sie die Datensicherung immer in der Planung berücksichtigen. Vergessen Sie nie, dass jede Verfügbarkeit nur so gut ist wie das schwächste Glied in der Kette.

Sicherung des vCenter Servers

Der VMware vCenter Server ist einer der entscheidenden und wichtigsten Faktoren in einer virtuellen Landschaft. Obwohl über diese Komponente alle wichtigen Arbeiten durchgeführt werden und alle Fäden der Umgebung hier zusammenlaufen, ist ein Ausfall des vCenters im Grunde erst einmal nichts, was eine laufende Umgebung stark beeinträchtigt. Zwar stehen einige Funktionen nicht zur Verfügung, das ist aber unter Umständen zu verschmerzen.

Bevor Sie tiefer in die Planung einsteigen, sollten Sie sich vergegenwärtigen, welche Funktionen bei einem Ausfall des Managements nicht zur Verfügung stehen. Tabelle 14.1 zeigt Ihnen, auf welche Eigenschaften Sie bei einem Ausfall verzichten müssen und welche Basiseigenschaften Sie weiterhin im Betrieb unterstützen.

Funktion	Funktion ohne Virtual Center
vMotion	nein
VMware DRS:	nein
VMware Storage DRS:	nein
Resource-Pool	nein
vSphere HA: Restart VM	ja
vSphere HA: Admission Control Add new host to cluster	nein
vSphere HA: Add new host to cluster	nein
vSphere HA: Host rejoins the Cluster	ja
Erstellen eines VDS	nein
Storage-I/O-Kontrolle konfigurieren	nein
Netzwerk-I/O-Kontrolle konfigurieren	nein

Tabelle 14.1 Funktionsstatus bei inaktivem vCenter Server

Mit den Daten, die Ihnen jetzt vorliegen, können Sie entscheiden, wie lange das System ausfallen darf, bevor es für den Betrieb kritisch wird. Darf die Ausfallzeit nur minimal sein, empfehlen wir den Einsatz des vCenter Server Heartbeats, alternativ den Einsatz eines Cold-Standby-vCenter-Servers als virtuelle Maschine.

Alle wichtigen Daten und Informationen des VMware vCenters liegen in der Datenbank. Im Falle einer Zerstörung des vCenters wäre es möglich, den Server neu zu installieren und durch Anhängen der Datenbank direkt weiterzuverwenden. Das geht natürlich nur, wenn die Datenbank auf einem getrennten System zur Verfügung gestellt wird. Die Datensicherung erfolgt in diesem Fall klassisch: für den Applikations-Server als filebasierte Sicherung und für die Datenbank über einen Wartungsplan. Welche Datensicherungssoftware Sie nutzen wollen, bleibt Ihnen überlassen. Es sollte das Produkt zum Einsatz kommen, für das schon Know-how in Ihrem Hause vorhanden ist.

Sicherung der vCenter-Server-Datenbank

Eine der wichtigsten Komponenten in der virtuellen Landschaft ist die Datenbank, mit der das vCenter arbeitet. In dieser Datenbank werden alle relevanten Daten gespeichert. Dementsprechend ist eine Sicherung der Datenbank notwendig und wichtig. Sollte es in Ihrer Firma einen Datenbank-Server für zentrale Aufgaben geben oder auch »nur« einen Datenbank-Server, der noch eine weitere Datenbank aufnehmen kann, dann empfehlen wir Ihnen, diesen zu nutzen. Zum einen wird dann eine einzeln liegende Datenbank nicht vergessen, zum anderen können Sie sie einfach in die Standardprozesse integrieren. Das Thema Sicherung ist dann auch recht einfach abgehandelt: Sie verwenden einfach den bekannten Firmenstandard, was eine einfache Einbettung in die bestehenden Betriebsprozesse bedeutet.

An dieser Stelle beschreiben wir kurz das Prinzip und die Grundlagen einer Datenbanksicherung. Diese Beschreibung ist allgemein gehalten, geht also in keiner Weise auf ein spezielles Produkt ein. Die Datensicherung einer Datenbank kann im Normalfall nicht mit dem Programm zur Datensicherung des Betriebssystems vollständig abgedeckt werden. Mit dieser Software lassen sich nur mehrere oder einzelne Files sichern. Sollen Datenbanken im laufenden Betrieb gesichert werden, benötigen Sie einen herstellerspezifischen Datenbank-Agent, der das Handling für die Arbeiten übernimmt. Dieser Agent garantiert, dass die Sicherung konsistent ist und somit auch für den Aufbau eines neuen Servers genutzt werden kann.

Die einfachste und sicherste Methode der Datenbanksicherung ist eine komplette Sicherung der Datenbank im heruntergefahrenen Zustand. Bei dieser Sicherung sind keine Daten der Datenbank im Zugriff, so dass Sie sie ohne Probleme sichern können. Diese Methode ist allerdings aufgrund der geforderten Verfügbarkeit der Datenbanksysteme meist nicht umsetzbar.

Die Alternative zum Backup der Datenbank im heruntergefahrenen Zustand ist die Sicherung im Onlinemodus. Dabei wird die Datenbank im laufenden Betrieb, also während des Zugriffs auf die Daten, gesichert. Der Nachteil bei dieser Methode ist, dass Inkonsistenzen nicht komplett ausgeschlossen werden können. Trotz alledem wird mindestens einmal, besser aber regelmäßig,

eine Offlinesicherung der Datenbank benötigt. Auf diese Sicherung setzt die Onlinesicherung dann auf. Alle Transaktionen, die in einem Datenbanksystem stattfinden, werden in den Log-Dateien gespeichert. Aus diesem Grund ist es wichtig, diese Log-Dateien ebenfalls zu sichern. Nach dem Rücksichern der Datenbank können Sie so, durch das Einspielen der Transaktionen, einen Status wiederherstellen, der sehr nahe an dem letzten produktiven Stand ist.

Wir empfehlen, eine Offlinesicherung einmal die Woche durchzuführen, sowie eine tägliche Onlinesicherung. Zusätzlich sollten Sie die Log-Dateien mehrmals täglich wegschreiben. Die Rücksicherung erfolgt nach den bekannten Prozessen. Ist die Offlinesicherung eingespielt, verarbeiten Sie die zusätzlich aufgelaufenen Log-Dateien, um so auf den letztmöglichen Stand zu kommen. Das eigentliche Vorgehen bedarf an dieser Stelle keiner näheren Beschreibung.

14.1.3 Sicherung der virtuellen Maschinen

Eine der wichtigsten Aufgaben bei der Sicherung der Daten ist selbstverständlich das Backup der virtuellen Maschinen. Ihnen stehen verschiedene Optionen für die Gewährleistung der Datensicherheit einer virtuellen Maschine zur Auswahl. In diesem Abschnitt erläutern wir näher, welche Wege zum Ziel führen. Als Unterscheidung dient die Sicherung innerhalb oder außerhalb der VM.

Klassische Datensicherung

Die erste Methode der Datensicherung einer virtuellen Maschine ist dieselbe wie bei einem physischen Server. Dabei verwenden Sie die bereits vorhandene Backup-Infrastruktur, um die Daten der virtuellen Maschine zu sichern. Installieren und konfigurieren Sie dazu einen Backup-Agent der verwendeten Backup-Software im Betriebssystem der virtuellen Maschine. Dieser überträgt alle Daten zu einem vorhandenen Backup-Server. Die Datensicherung erfolgt dabei zeitgesteuert über den Client und läuft ins zentrale Management.

Der Vorteil einer solchen Datensicherung ist, dass Sie die bereits verwendete Backup-Infrastruktur ohne Anpassungen oder spezielle Erweiterungen verwenden können. Sie können sogar Maschinen, die von einer physischen Infrastruktur auf eine virtuelle Infrastruktur übernommen wurden, ganz normal weiter sichern, einschließlich der Übernahme der bereits vorhandenen Sicherungsdaten. Legen Sie aber ein Augenmerk auf die Netzwerkanbindung der virtuellen Server, denn der gesamte Datensicherungsstrom läuft über das LAN.

Eine Rücksicherung erfolgt ebenfalls über den Datensicherungs-Client, in gewohnter Manier. Also auch hier gibt es keine Änderung bei den Datensicherungsprozessen.

VMware Consolidated Backup (VCB)

Mit der Version Virtual Infrastructure 3.x liefert VMware ein eigenes Produkt zur Sicherung der virtuellen Maschinen. Mit dem VMware Consolidated Backup (VCB) hat VMware ein Pro-

dukt entwickelt, mit dem sich VMs schnell und komfortabel sichern lassen. Auch wenn das Produkt bereits mit der Version vSphere 4.1 abgekündigt und die Arbeit von dem Produkt Data Recovery abgelöst wurde, möchten wir trotzdem hier kurz auf das Produkt eingehen, denn es wird eine Reihe von Umgebungen geben, die für das Upgrade anstehen und wo die Lösung abgelöst werden muss. Das Thema Data Recovery wird in den Abschnitten 6.9 und Abschnitt 13.9 näher dargestellt.

Was genau war nun VCB, und wie funktionierte das Ganze? Beim VCB handelt es sich um einen sogenannten *Sicherungs-Proxy-Server*. Dieser Server sammelt die Sicherungsdaten der virtuellen Maschinen und gibt sie geschlossen an einen Sicherungs-Server weiter.

Es gibt zwei Varianten, wie die Daten zum Proxy bzw. zum Datensicherungs-Server gelangen können. Liegen die virtuellen Maschinen auf SAN- oder iSCSI-LUNs, können die Daten LAN-free direkt von der LUN gesichert werden. Kommt anderer Storage zum Einsatz, geht der Datenfluss über die Netzwerkkarte der Service Console zum VCB-Server und dann weiter zum Datensicherungs-Server. Hier wird auch der Vorteil des VCB-Systems deutlich: Kann LAN-free gearbeitet werden, entlastet das nicht nur das Netzwerk, sondern steigert auch enorm die Sicherungsgeschwindigkeit. Bedenken Sie bitte, dass Sie im Falle des LAN-free-Backups ein oder mehrere physische Server benötigen, damit ein Zugriff auf die Komponenten im SAN möglich ist. Ein VCB-Server kann nicht unendlich viele Server sichern, darum ist mit dem Einsatz mehrerer VCB-Server zu rechnen. Für das genaue Sizen einer VCB-Landschaft sind im Vorfeld ausgiebige Tests notwendig, um zu bestimmen, wie viele VCB-Proxys benötigt werden.

Müssen die Daten über das LAN direkt gesammelt werden, können Sie als VCB-Proxy auch eine oder mehrere virtuelle Maschinen einsetzen. Der Vorteil an dieser Stelle ist, dass sich als Zielspeicher auch preiswertere NAS-Systeme eignen, im Gegensatz zum teureren SAN. Der Nachteil dabei ist aber, dass der gesamte Datenfluss wieder über das Netzwerk läuft.

Kommen wir zur Funktionsweise. Als Orientierungshilfe für die Beschreibung der Funktionsweise dient Abbildung 14.1.

Mit dem Beginn der Datensicherung initiiert der VCB-Proxy auf der virtuellen Maschine die Erstellung eines Snapshots (❶). Ist dieser Snapshot erstellt, mountet der Proxy-Server diesen Snapshot und sammelt die Daten aus der VM (❷).

Ist die Datensicherung abgeschlossen, wird der Snapshot wieder gelöscht und mit den Daten, die sich während der Sicherung geändert haben, zusammengeführt. Unabhängig von der virtuellen Maschine kann der VCB-Server die Daten des virtuellen Servers nun wegsichern (❸).

Für alle unterstützten Betriebssysteme ist auch eine image-basierte Sicherung möglich. Dabei werden alle Dateien direkt aus dem VMFS auf den VCB-Server gesichert. Das schließt auch die Konfigurationsdateien ein.

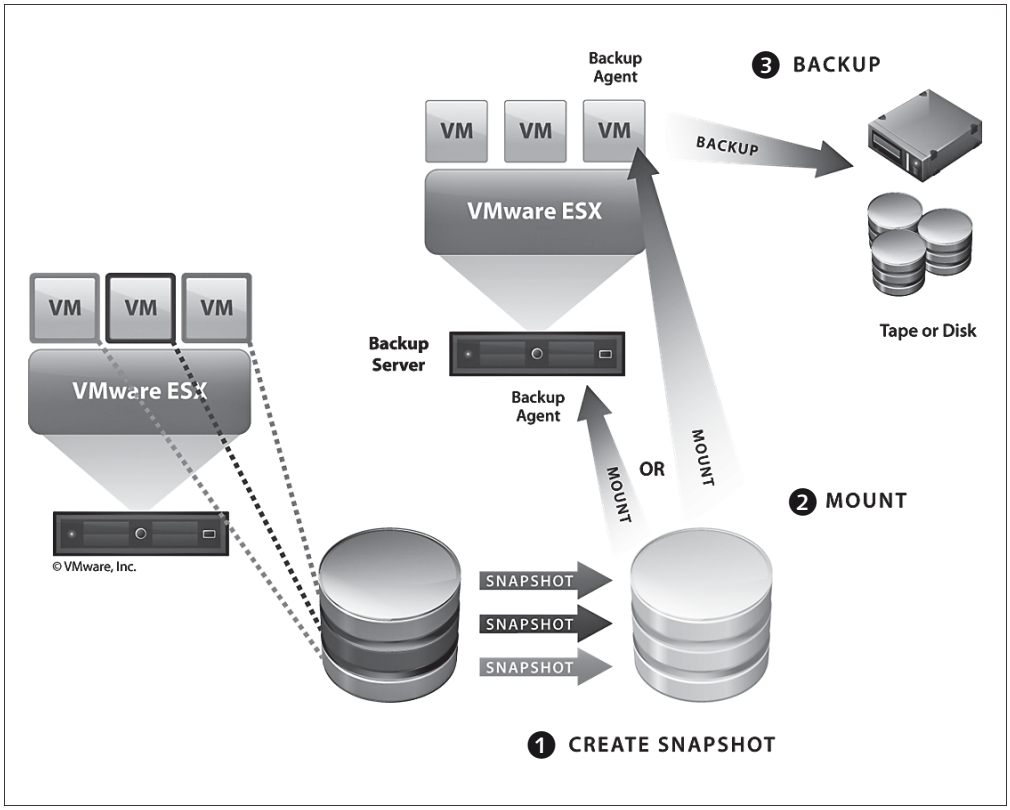


Abbildung 14.1 Arbeitsschritte des VCB-Servers

Setzen Sie auf der zu sichernden VM ein Windows-basiertes Betriebssystem ein, können Sie die Sicherung auch auf File-Level-Ebene durchführen. Beim Datei-Level-Backup gibt es wiederum drei verschiedene Methoden, die Dateien aus der virtuellen Maschine zu sichern: Full file Backup sichert alle Dateien, die in dem virtuellen Server vorhanden sind. Bei einem Differentiellen Backup werden alle Dateien gesichert, die seit einem Full file Backup geändert wurden. Als dritte und letzte Möglichkeit bietet sich die Methode Inkrementelles Backup an. Dabei werden alle Daten gesichert, die seit dem letzten Backup – egal ob Full oder Inkrementell – geändert wurden. In diesem Fall gestaltet sich die Rücksicherung nicht ganz so einfach wie in den vorhergehenden Fällen. Wir unterscheiden mehrere verschiedene Möglichkeiten der Rücksicherung. Jeder für sich muss abschließend entscheiden, welcher Weg für ihn am besten ist. Aus unserer Sicht sind nicht alle beschriebenen Wege im normalen Betrieb wirklich realisierbar. Eine Rolle spielen sicherlich auch die Größe der Landschaft und die Vorgaben, die in der Firma vorherrschen.

Bei der ersten Rücksicherungsoption werden die zu restaurierenden Daten auf dem VCB-Proxy wiederhergestellt. Dann kopieren Sie die wiederhergestellten Daten über einen CIFS-Share auf die entsprechende virtuelle Maschine. Der Vorteil ist sicherlich, dass Sie keinen

Datensicherungs-Client in der VM benötigen; wie praktikabel das Ganze ist, müssen Sie für sich selbst beurteilen.

Achtung

Diese Funktion steht nur zur Verfügung, wenn als Betriebssystem der VM Windows zum Einsatz kommt. Bei anderen Gastbetriebssystemen ist diese Funktion derzeit noch nicht verfügbar.

Für das Zurücksichern von image-basierten Sicherungen gibt es zwei Möglichkeiten: Speichern Sie die Files einer virtuellen Maschine auf dem VCB-Proxy zwischen; anschließend erstellen Sie über den vCenter Converter aus diesen Dateien eine neue VM. Alternativ kopieren Sie die Files über den Proxy direkt auf den Datastore des Hosts und registrieren die virtuelle Maschine über den vCenter-Server neu. Voraussetzung dafür ist aber, dass die alte VM vorher deaktiviert wurde. Die erste Methode eignet sich auch ideal zur Fehlersuche in einem virtuellen Server. Beide Server lassen sich parallel betreiben; die IP-Adresse und den Namen sollten Sie schon vor der Inbetriebnahme anpassen oder den zweiten Server in ein privates Netzwerk stellen.

Die zweite Funktion können Sie in Verbindung mit dem klassischen Backup-Agent einsetzen. Die Full Backups sind so schnell über das Fibre-Channel-Netzwerk ausgeführt, und die filebasierte Sicherung erfolgt über den Datensicherungs-Client. Hier ist ebenfalls, wie bei allen anderen Lösungen, zu prüfen, inwieweit sich die Arbeiten in den bestehenden Datensicherungs- bzw. Restore-Prozess integrieren lassen.

14.1.4 Backup von vSphere-Umgebungen mit NetApp-Storage

Autor dieses Abschnitts ist Oliver Kügow, teamix GmbH, ok@teamix.de.

Die meisten Firmen entscheiden sich für Virtualisierung, da die Konsolidierung der Infrastruktur viele Vorteile mit sich bringt, die wichtigsten sind wohl Kosteneinsparungen, Automatisierung und vereinfachtes Management. Allerdings wird an einigen Stellen vergessen, dass ein hoher Konsolidierungsgrad auch negative Folgeeffekte hat, wie zum Beispiel eine starke Konzentration der Daten auf einen Punkt in der Infrastruktur: dem zentralen Speichersystem. Mit dieser Datenkonzentration auf einen Punkt muss im Alltagsbetrieb umgegangen werden, insbesondere beim Thema Backup.

Vor der Virtualisierung installierte man typischerweise Backup-Agents auf jeden einzelnen Server, die dann über das LAN die Backup-Datenströme an einen zentralen Backup-Server sendeten, der sie wiederum auf Band schrieb. Ein solcher Ansatz ist zwar immer noch möglich, indem Sie einfach die Agenten in jede virtuelle Maschine installieren, allerdings resultieren daraus erhebliche Lastspitzen, sowohl auf dem vSphere-Host als auch auf dem Speichersystem. Diese Problematik müssen Sie mit intelligenten neuen Technologien lösen, ähnlich wie Konsolidierungsfragen durch Virtualisierung gelöst wurden. Sprich: Das Backup muss sich der Virtualisierung und der damit folgenden Datenkonzentration anpassen.

Ein Backup wird immer besser, wenn folgende Kriterien erfüllt werden:

- Niedriges RPO (Recovery Point Objective): Man darf im Falle einer Wiederherstellung möglichst wenig Daten verlieren. Das gewährleisten Sie durch häufiges Ausführen von Backups.
- Niedriges RTO (Recovery Time Objective): Die Wiederherstellung sollte möglichst schnell erfolgen.
- Beim Erstellen des Backups sollten möglichst wenige Daten bewegt werden, sonst kann das Backup-Zeitfenster aufgrund gestiegener Datenmengen nicht mehr eingehalten werden.
- Backups sollten Sie möglichst an geografisch entfernten Orten lagern, damit auch ein Desasterschutz existiert.
- Backups müssen automatisiert durchgeführt werden, manuelle Eingriffe sollten Sie vermeiden. Dazu zählt z. B. neben dem Transport von Bändern auch die manuelle Konfigurationserweiterung oder Anpassung bei Server-Änderungen – diese werden nämlich leicht vergessen.

NetApp löst all diese Anforderungen nahezu perfekt, gerade im Zusammenspiel mit VMware vSphere.

Snapshots bilden die Basis für eine schnelle, effiziente und häufige Datensicherung. Ein NetApp-Snapshot hält den Zustand eines Volumes als Read-only-Kopie eines bestimmten Zeitpunktes fest. Die Snapshots sind performanceneutral und belegen nur so viel Platz, wie sich real Daten geändert haben. Es ist möglich, bis zu 255 Snapshots pro Volume zu erzeugen. Beim Erstellen eines Snapshots werden keine Daten bewegt oder kopiert, sondern lediglich Zeiger auf die vorhandenen Daten eingefroren – das geht sehr schnell: Ein Snapshot ist in weniger als einer Sekunde erstellt.

Die Snapshots liegen allerdings noch auf denselben Disks wie die Originalplatten; das verhindert zwar das versehentliche Löschen von Daten, aber ein ausreichender Desasterschutz fehlt noch. Dafür hat NetApp Replikationsmechanismen wie SnapMirror oder SnapVault im Portfolio – mit diesen Mechanismen werden nur die geänderten Daten über das Netzwerk auf eine andere NetApp-Maschine repliziert. Die Replikation geschieht vollautomatisch und in regelmäßigen Abständen, z. B. einmal pro Stunde. Am besten stellen Sie sich den Vorgang so vor:

- Snapshots halten den (konsistenten) Zustand auf dem produktiven Speichersystem fest.
- Replikation transportiert diese Zustände anschließend auf ein Backup-System, es werden nur blockweise Änderungen seit dem letzten Transport kopiert.

Damit im Zusammenhang mit VMware die virtuellen Maschinen aber in jeder Sicherung konsistent sind, müssen Sie vor der Sicherung per Snapshot die VMs in einen sauberen, definierten Zustand bringen. Es kommen grundsätzlich drei Zustände in Frage:

- VM ausgeschaltet (kalt): Damit ist die Disk der VM sicher konsistent, allerdings spricht die damit verbundene Downtime oft gegen diese Variante.

- VM pausiert (warm): Die VM wird in den Ruhezustand gebracht, das RAM der VM wird auf Disk geschrieben. Da die VM und ihre Applikationen nicht mehr laufen, ist der Zustand auch wirklich konsistent, nur ist auch dies wieder mit (kürzerer) Downtime verbunden.
- VM angeschaltet (hot): Die Disk der virtuellen Maschine muss in einen sauberen Zustand gebracht werden, das kann durch einen VM-Snapshot geschehen. Es gibt keine Downtime, allerdings ist auch keine 100 %ige Konsistenz gewährleistet; VMware spricht hier von »crash-consistent«, also genauso konsistent wie nach einem Absturz. Damit die Applikationskonsistenz gewährt ist, können Sie durch ein Skript in der VM die Applikation vor dem VM-Snapshot in den Backup-Modus bringen. Der FS-Sync-Treiber der VMware Tools leert vor dem VM-Snapshot auch die Schreibcaches der VM. Aktuellere Windows-Versionen verwenden für Applikationskonsistenz den VSS von Microsoft (Volume Shadow Copy Service).

Der gesamte Backup-Vorgang sähe also zusammengefasst so aus:

1. alle VMs im Datastore konsistent machen, VM-Snapshot erstellen
2. NetApp-Snapshot des Datastore-Volumes erstellen
3. die VM-Snapshots wieder löschen
4. den NetApp Snapshot auf ein entferntes NetApp System replizieren

NetApp Tools

Um diesen Ablauf zu koordinieren, gibt uns NetApp mehrere Tools an die Hand:

- SnapManager for Virtual Infrastructure (SMVI)
- Virtual Infrastructure Backup Engine (VIBE)
- SnapCreator Framework

SMVI ist für die meisten Kunden das Tool der Wahl, da es über eine GUI verfügt und offiziell von NetApp unterstützt wird. Allerdings kostet es auch Geld, bezahlt wird für die Software selbst und für Support. Es bietet neben der Backup-Funktion natürlich die Möglichkeit, Restores durchzuführen. Seit Version 2.0 können User sogar einzelne Dateien aus VM-Snapshots selbst wiederherstellen. Neu mit der Version 3 kam die Integration in die NetApp *Virtual Storage Console*, ein vCenter-Plugin.

VIBE ist ein Perl-Skript. Es gibt keine GUI und keinen Support, dafür ist das Tool allerdings kostenlos und im Quelltext verfügbar, Sie können es also auch gut an Ihre eigenen Bedürfnisse anpassen.

SnapCreator ist ein Framework, kein fertiges Backup-Tool. Mit SnapCreator können Backup-Workflows erzeugt werden, die immer einem ähnlichen Schema entsprechen: Applikation konsistent machen (z. B. Datenbank-Hot-Backup-Mode oder VMware SnapShot), anschließend NetApp SnapShot und dann wieder den Backup-Modus der Applikation beenden.

SnapCreator ist so generisch gebaut, dass fast alle Applikationen bedient werden können, unter anderem auch VMware vSphere. Da das Tool nicht explizit auf den Backup-Vorgang von virtuellen Maschinen ausgelegt ist, sondern die VM-Sicherung nur eine Variante unter vielen darstellt, soll es hier nur der Vollständigkeit halber erwähnt und nicht ausführlicher erklärt werden. Weitere Informationen und eine aktive Community zu dem kostenlosen Tool finden Sie unter *www.snapcreator.com*.

Drittanbieter-Tools

Neben den Backup-Tools von NetApp selbst stehen Drittanbieter-Werkzeuge zur Verfügung, die dem Backup/Restore von VMware auf NetApp-Storage dienen.

Ein Insider-Tipp ist die Software NVSAVE von der Firma Cleondris aus der Schweiz. NVSAVE ist die Kurzform von »**N**etApp **V**Mware **SAVE**« – der Name ist also Programm, die Software wurde nur für die Sicherung von virtuellen Maschinen auf NetApp-Storage entwickelt.

Genau wie der SMVI von NetApp unterstützt NVSAVE alle Storage-Anbindungen bzw. Protokolle, also Fibre-Channel, iSCSI und NFS. Über die Funktionalität von SMVI hinaus bietet NVSAVE einige Vorteile:

- SnapVault Integration: SMVI kann die erstellten Snapshots nur per SnapMirror replizieren. Eine bessere Variante für Backups stellt jedoch die SnapVault-Technologie dar, da die SnapShots hiermit auf dem Backup-Ziel länger vorgehalten werden können.
- Schnellere Backups: NVSAVE bietet beim Erstellen der VMware-Snapshots höhere Parallelität und führt den Snapshot-Vorgang dadurch schneller durch. Das Tool wurde speziell für größere Umgebungen mit vielen Tausend VMs entwickelt.
- Schnelle Restores mit FlexClone: Anstatt VMs beim Restore zuerst an den Ursprungsort zurückzukopieren und dann erst zu starten, spart NVSAVE erheblich Zeit, indem es einen NetApp-FlexClone aus dem Snapshot erstellt (sehr schnell) und auf dem Clone die VM sofort einschaltet. Anschließend wird die laufende VM per Storage vMotion auf den ursprünglichen Datastore verschoben.
- Restores vom Secondary: Der oben beschriebene Vorgang des Clonings funktioniert genauso auf dem *SnapVault Secondary,* also der zweiten NetApp, auf die die Backup-Snapshots repliziert wurden. Ebenso unterstützt ist der Restore über ein anderes Protokoll. Beispiel: Produktiv-VMs laufen über Fibre-Channel, Backups erfolgen per iSCSI.
- Minimalistisches Berechtigungskonzept: Es gibt eine klare Trennung der administrativen Verantwortlichkeiten – Backup-Administratoren dürfen nur Backups und Restores durchführen, nicht aber die vSphere-Farm oder das NetApp-Speichersystem administrieren. Bei SMVI gibt es durch Integration der NetApp-GUI in den vSphere-Client immer wieder Probleme beim Berechtigungskonzept: VMware, NetApp und Backup-Administratoren könnten sich potentiell gegenseitig beeinflussen.

Für Kunden mit besonders großen Umgebungen, die meist auch Trennung in der Administration betreiben, kann NVSAVE also eine willkommene Alternative zu den bekannten NetApp-Tools darstellen. Mehr Informationen gibt es auf der Website des Herstellers: *www.cleondris.ch*

SMVI

Der SnapManager for Virtual Infrastructure (SMVI) ist in Bezug auf vSphere die offizielle Backup-Lösung von NetApp und wird von vielen Kunden eingesetzt. Deshalb möchten wir kurz die Funktionsweise von SMVI zeigen, inklusive einer kurzen Anleitung zur Installation.

SMVI ist seit der Version 3.0 ein Teil der sogenannten Virtual Storage Console (VSC), einem vCenter-Plugin das NetApp-Funktionalität in den vSphere-Client und den vCenter Server integriert. Neben dem eigentlichen SMVI bietet die VSC folgende Funktionen:

- Provisionieren von VMware-Datastores auf dem NetApp-Storage
- Erstellen von schnellen VM- und Datastore-Clones, z. B. für virtuelle Desktops bei VMware View
- vereinfachte Konfiguration der vSphere-Server für NetApp Best Practices, darunter: Timeout-Werte, Tuning-Parameter und vDisk-Alignment-Tools

An dieser Stelle gehen wir aber nur auf die Backup- und Restore-Funktionalität ein, die anderen Funktionen werden in Kapitel 10 (Seite 554) erklärt.

Für die Installation der VSC benötigen Sie einen Windows-Rechner; Sie können auch eine virtuelle Maschine verwenden, sollten dann aber darauf achten, dass diese auf einem anderen Datastore liegt als die zu sichernden VMs, weil es sonst während der Sicherung zu unerwünschten Hängern kommen kann. Auch der vCenter Server selbst ist ein guter Installationsort für die VSC.

Die zur Drucklegung aktuelle Version der VSC ist 2.1.1, was auch die erste Version mit Support für vSphere 5.0 war. Sie enthält den SMVI in Version 3.0.4, der ebenfalls mit vSphere 5 kompatibel ist.

Führen Sie den Installer aus, und wählen Sie, ob Sie neben dem obligatorischen Plugin für Monitoring und der gewünschten Funktion des SnapManagers (Backup/Recovery) auch die Cloning-Software installieren wollen. (Abbildung 14.2).

Nachdem der Installer erfolgreich durchgelaufen ist, werden Sie dazu aufgefordert, die VSC mit dem vCenter Server bekannt zu machen. Sie müssen nur die Zugangsdaten eingeben. Wer nicht als Administrator arbeiten möchte und Wert auf eingeschränkte Berechtigungen legt, dem sei das Benutzerhandbuch ans Herz gelegt, dort finden Sie die mindestes benötigten Berechtigungen.

Sofort nachdem das VSC-Plugin am vCenter verbunden wurde, taucht im vSphere-Client bei Hosts, VMs und dem Cluster ganz rechts ein weiteres Reiterkärtchen auf: NetApp. Außerdem finden Sie das Plugin unter Lösungen und Anwendungen, siehe Abbildung 14.4.

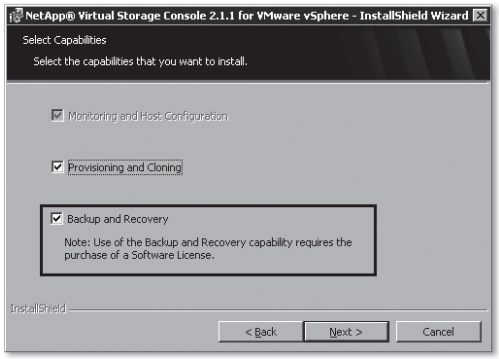


Abbildung 14.2 Paketauswahl des VSC-Installers

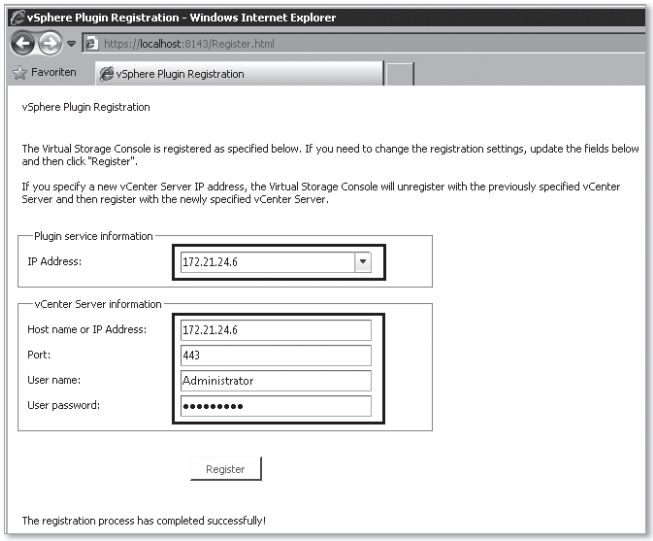


Abbildung 14.3 VSC wird zum vCenter verbunden.

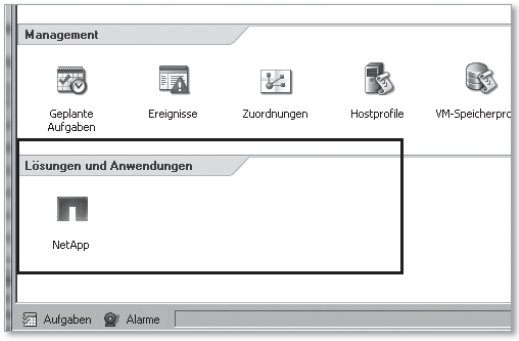


Abbildung 14.4 Das VSC-Plugin im vSphere-Client

Beim Doppelklick auf das NetApp-Logo gelangen Sie in die Administrationsoberfläche der VSC, wo Sie nochmals die vCenter-Konfiguration anpassen können, aber mindestens Ihre NetApp-Storage-Controller hinzufügen müssen, siehe Abbildung 14.5.

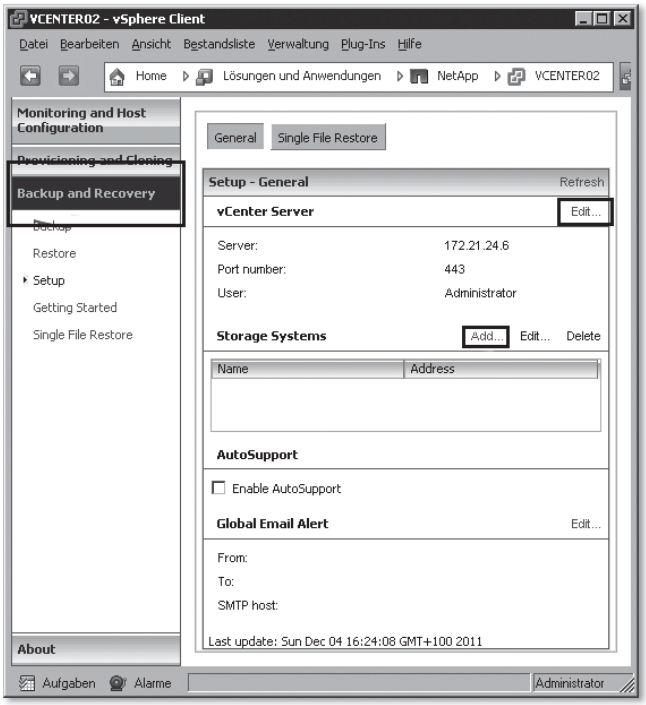


Abbildung 14.5 Grundeinstellungen des Backup-Plugins

Sind diese Grundeinstellungen erfolgt, so kann es darangehen, den ersten Backup-Job einzurichten.

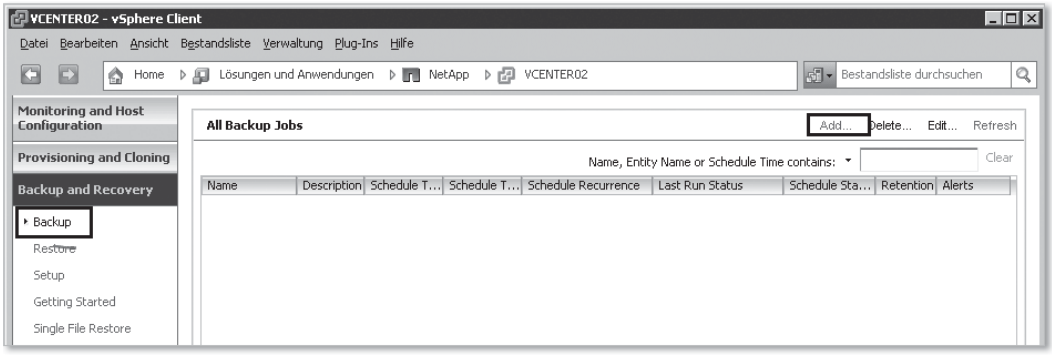


Abbildung 14.6 Den ersten Backup-Job einrichten

Sie sollten auswählen, dass vor Ihrem Backup auch VMware-Snapshots durchgeführt werden, um die VMs in einen möglichst konsistenten Zustand zu bringen (siehe Abbildung 14.7), außerdem soll es stündlich laufen (siehe Abbildung 14.8).

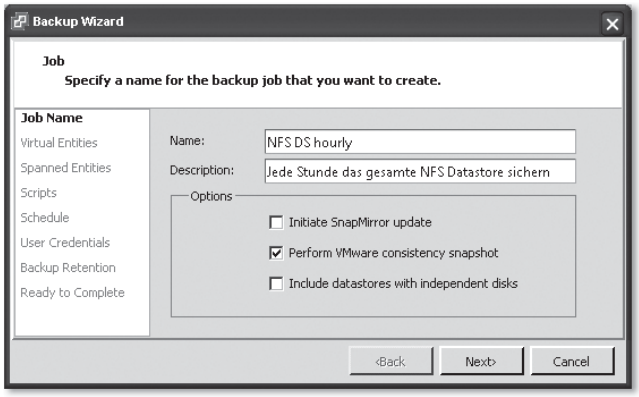


Abbildung 14.7 Backup-Namen und die VM-Snapshots einstellen

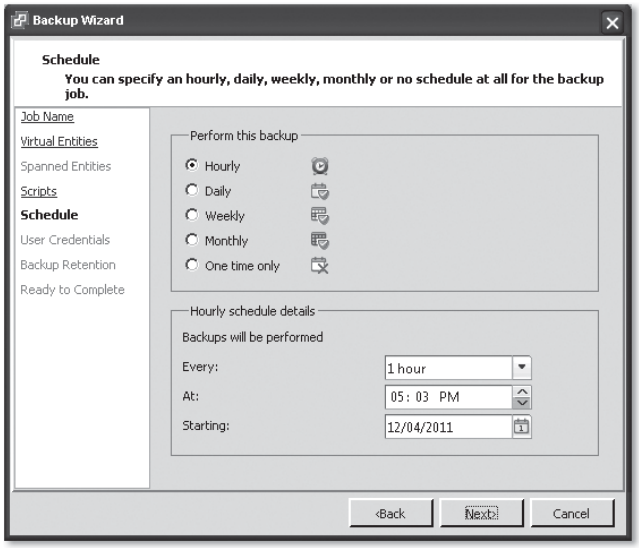


Abbildung 14.8 Backup-Intervall festlegen

Anschließend konfigurieren Sie, dass der gesamte Datastore inklusive aller VMs gesichert wird (Abbildung 14.9).

Der letzte Schritt zur Konfiguration des Sicherungsauftrages ist die Vorhaltedauer der Backups. Wir stellen in unserem Beispiel in Abbildung 14.10 einfach einen Tag ein. Gegebenenfalls stellen Sie auch die E-Mail-Benachrichtigung ein.

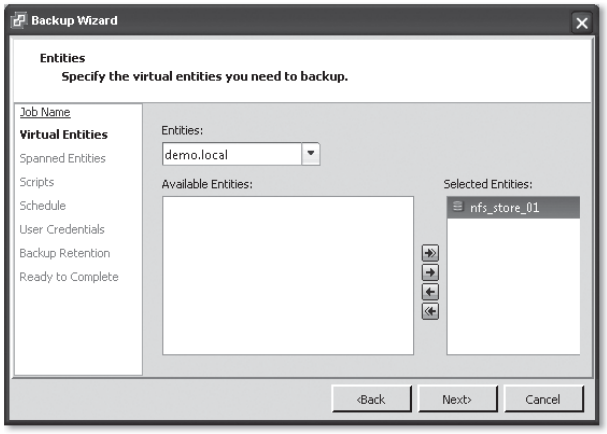


Abbildung 14.9 Den zu sichernden Datastore konfigurieren

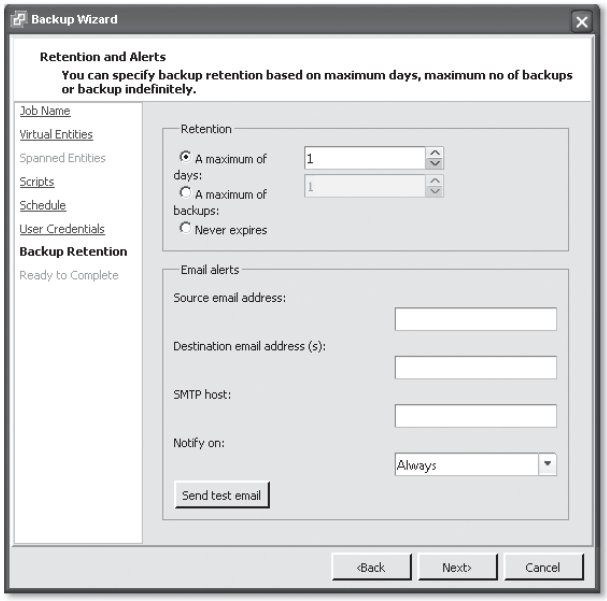


Abbildung 14.10 Vorhaltedauer der Backups

Schließlich können Sie nach dem Speichern des soeben konfigurierten Jobs Ihr erstes Snapshot-basiertes Backup starten. Dies geschieht wie in Abbildung 14.11 durch einen Rechtsklick auf den Job und die Auswahl Run Job Now.

Der Sicherungsauftrag wird nun zügig ausgeführt, ein Backup eines gesamten Datastores ist meist in wenigen Sekunden bis maximal Minuten erledigt. Unser Beispiel in Abbildung 14.12 ist mit weniger als 20 Sekunden extrem – es handelte sich nur um eine einzige VM, die außerdem wenig Last erzeugte.

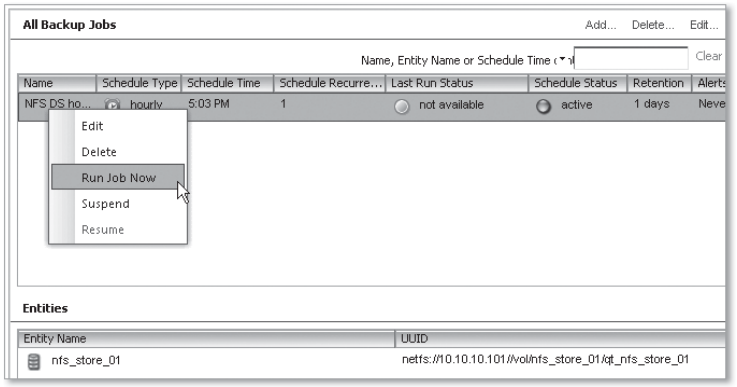


Abbildung 14.11 Die Sicherung manuell starten

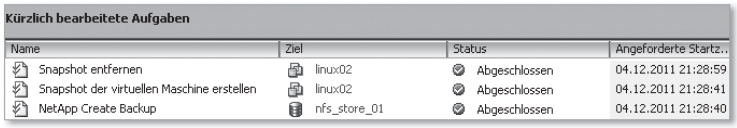


Abbildung 14.12 Das Backup wurde durchgeführt.

Dieser Backup-Weg skaliert gut bis wenige Hundert VMs. Ein Backup dauert nur wenige Minuten. Das SnapMirror-Update wird danach im Hintergrund gestartet und betrifft den eigentlichen Backup-Prozess nicht mehr. Sollten Sie dennoch an die Skalierungsgrenzen von SMVI stoßen, etwa weil Sie mehrere Tausend VMs betreiben, so sei nochmals die Software NVSAVE erwähnt (siehe den Abschnitt »Drittanbieter-Tools« auf Seite 858).

Abschließend möchten wir noch kurz einen Recovery-Vorgang zeigen; in diesem Beispiel spielen wir die gesamte VM zurück. SMVI erlaubt aber auch das Wiederherstellen von einzelnen Dateien innerhalb einer VM aus einem VM-Snapshot oder auch das Recovern einzelner VMDK-Dateien.

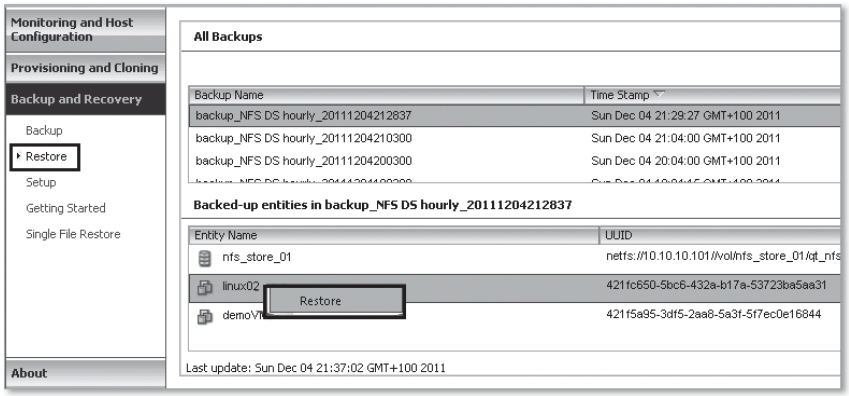


Abbildung 14.13 Restore-Vorgang einer gesamten VM

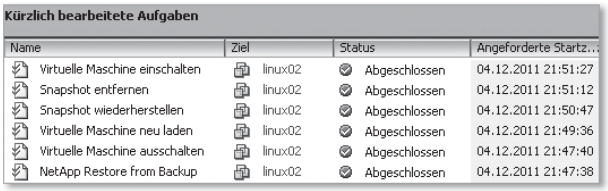


Abbildung 14.14 Restore der gesamten VM in vier Minuten

SMVI verhält sich beim Restore ganzer VMs und auch beim Restore von ganzen VMDK-Dateien unterschiedlich, und zwar abhängig vom verwendeten Storage-Protokoll.

- FC und iSCSI: SMVI erzeugt für die Wiederherstellung der VM einen LUN-Clone des Datastores. Dieser Clone wird an den Host gemappt, und anschließend werden die Files der VM zurück auf den Original-Datastore kopiert.
- NFS: SMVI führt auf dem NetApp Speichersystem einen sogenannten *Single File SnapRestore* durch. Dieser Vorgang verlinkt die alte VMDK-Datei aus dem Snapshot wieder in die Gegenwart. Das ist zwar schneller als ein Kopiervorgang, dauert aber dennoch lange, abhängig von der Größe der VM.

Diese Wiederherstellungsverfahren sind immer noch relativ schnell im Vergleich zu einem klassischen Recovery von Band, allerdings besteht noch Optimierungspotential, das NetApp in künftigen Versionen des SMVI hoffentlich ausschöpfen wird. Schnelle Restores mit Hilfe von Clones waren schon für die Version 3 erwartet, aber selbst in aktuellen Versionen des SMVI ist diese Funktionalität leider noch nicht enthalten.

Momentan bleibt für eine noch schnellere Rücksicherung der VM also nur der manuelle Weg: Erzeugen Sie einen LUN-Clone (oder bei NFS: einen FlexClone) des Datastores, mappen Sie diesen an den ESX-Host, und registrieren Sie direkt auf dem Clone die VM neu. Anschließend können Sie diese direkt auf der Clone-LUN starten. Dadurch läuft die VM innerhalb von Sekunden wieder, unabhängig von der VM-Größe! Damit der Clone wieder entfernt werden kann, müssen Sie anschließend die VM per Storage vMotion auf den ursprünglichen Datastore zurückmigrieren. Dieser Vorgang funktioniert auch mit NFS-Datastores, allerdings ist dafür die FlexClone-Lizenz von NetApp nötig.

VIBE

Die Virtual Infrastructure Backup Engine (VIBE) ist die kostenlose und quelloffene Alternative zum SMVI, allerdings ohne Support und mit etwas mehr Handarbeit. Das Paket ist als kompilierte *.exe*-Datei für Windows und als *.pl*-Skript für diverse Unix-Varianten verfügbar. Für die Perl-Variante müssen Sie allerdings noch einige Perl-Bibliotheken nachinstallieren, was unter Umständen ziemlich aufwendig ist. VIBE können Sie von *now.netapp.com* herunterladen. Nach der Installation auf Windows ist eine *VIBE.exe* verfügbar, es wird auch eine sehr ausführliche Dokumentation als PDF mitgeliefert. Hier möchten wir kurz exemplarisch ein Backup eines FCP-Datastores demonstrieren. Der Ablauf ist identisch mit dem SMVI: Sie machen die

VMs per VM-Snapshot konsistent, lösen anschließend den NetApp-Snapshot aus und entfernen dann die VM-Snapshots wieder.

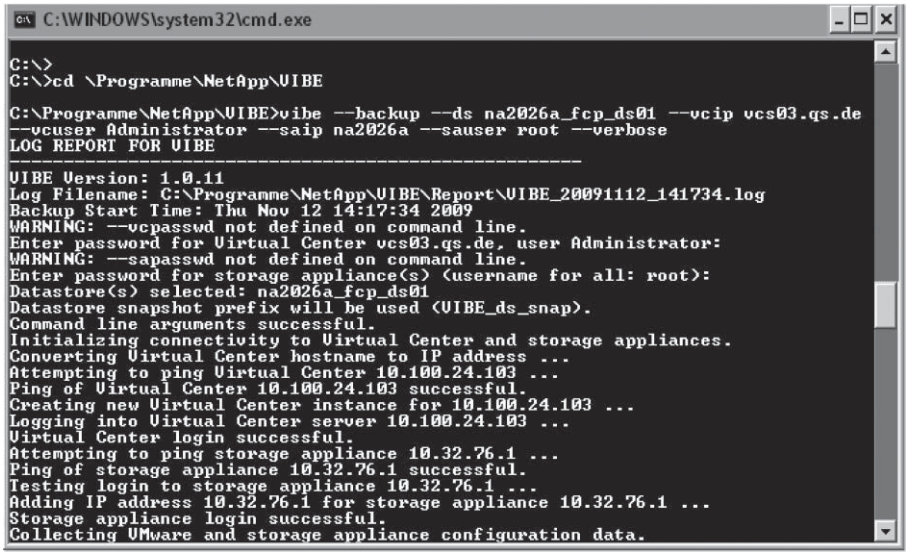


Abbildung 14.15 Backup mit VIBE

Der gesamte Prozess wird im Verzeichnis *Report* in einer Log-Datei für jeden Backup-Vorgang festgehalten. VIBE ermöglicht nach dem Backup auch eine Replikation per SnapMirror – anders als bei SMVI ist sogar eine Sicherung per SnapVault möglich. VIBE kann auch Restores durchführen, allerdings nur von gesamten VMs. Einzelne Dateien aus VMs lassen sich nicht wiederherstellen. Auch ein direkter Restore von VMs von einem Replikationsziel (SnapMirror oder SnapVault) ist mit VIBE leider nicht direkt möglich.

14.1.5 VMware Data Recovery

Mit der Einführung der Version 4.x des vSphere Servers brachte VMware, sehr zur Überraschung von vielen Anwendern, eine eigene Datensicherungs-Appliance auf den Markt. Mit dem Softwarepaket VMware Data Recovery besteht die Möglichkeit, virtuelle Maschinen zu sichern und wiederherzustellen, ohne dass Sie weitere Datensicherungssoftware benötigen. Hier unterscheidet sich das Tool wesentlich von dem VCB-Server, der ja zur Arbeit eine Anbindung an eine bestehende Datensicherungslandschaft benötigt.

Die Installation und Konfiguration von VMware Data Recovery haben wir bereits in Kapitel 6, »Installation«, und Kapitel 13, »Konfiguration von vCenter-Add-ons«, beschrieben. Auch hierbei handelt es sich – in der derzeitigen Version – um ein image-basiertes Sicherungssystem. Die zu sichernden virtuellen Server werden dedupliziert auf ein SAN, NAS, CIFS oder einen lokalen Storage gesichert. Abbildung 14.16 zeigt die Funktionsweise.

Ähnlich dem VCB wird vor dem Beginn der Datensicherung ein Snapshot der zu sichernden VM angefertigt (❶). Danach sorgt die Data-Recovery-Appliance dafür, dass die virtuelle Maschine auf ein unterstütztes Ziel-File-System weggeschrieben wird. Vor dem Schreibvorgang wird kontrolliert, ob identische Daten schon einmal geschrieben wurden. Ist das der Fall, wird lediglich ein Zeiger auf die bestehenden Daten angelegt, ohne die Daten reell noch einmal wegzuschreiben (❷). So wird der benötigte Plattenplatz für die Datensicherung stark reduziert. Ist die Datensicherung abgeschlossen, wird der Snapshot aufgelöst, und die in der Zwischenzeit geänderten Daten werden eingepflegt (❸).

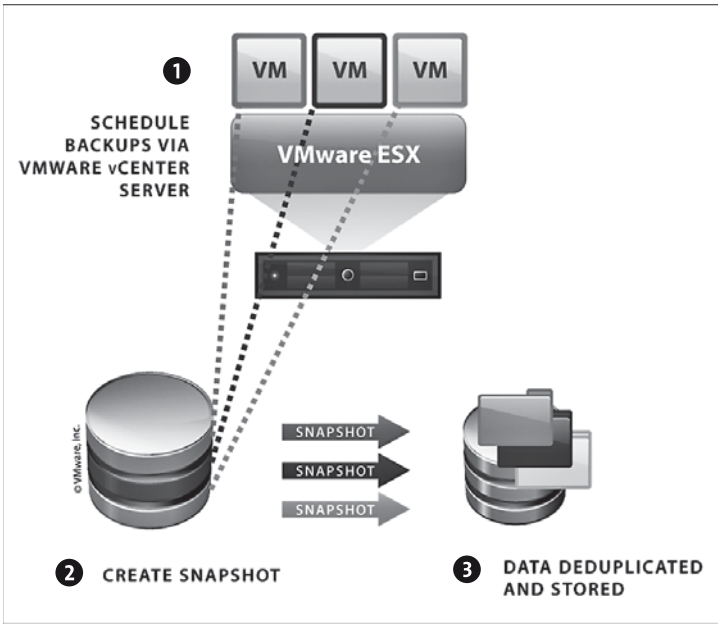


Abbildung 14.16 Sicherung einer VM mit VMware Data Recovery

Für die Rücksicherung ist ebenfalls die Appliance zuständig. Abbildung 14.17 zeigt den Ablauf der Rücksicherung.

Für den Fall, dass eine virtuelle Maschine ausfällt (❶), stoßen Sie über das Data-Recovery-Plugin auf dem vCenter-Server die Rücksicherung an. Als Erstes wählen Sie das Image aus, das zurückgesichert werden soll (❷). Im folgenden Schritt startet der Rücksicherungsvorgang, und die defekte Maschine wird wiederhergestellt (❸). Dabei haben Sie die Wahl, in welcher Form Sie die Rücksicherung durchführen möchten. Der eine Weg führt zur Ersetzung der originalen Maschine, das heißt, das Original wird gelöscht und durch die Sicherung ersetzt. Für eine detaillierte Fehleranalyse können Sie aus einer Sicherung auch einen neuen Server erstellen. Durch eine gezielte friedliche Koexistenz stellen Sie zum einen dem Kunden den Service wieder zur Verfügung und können zum anderen auf dem defekten System eine Fehleranalyse betreiben.

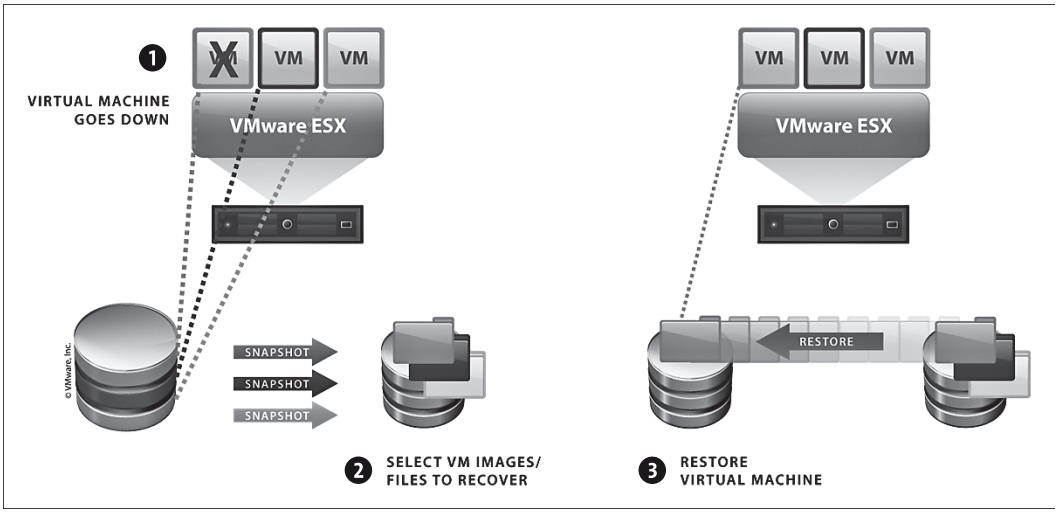


Abbildung 14.17 Rücksicherung einer VM mit VMware Data Recovery

Mittlerweile gibt es eine unterstützte Möglichkeit, einzelne Files aus einer vorhandenen Data-Recovery-Sicherung in eine virtuelle Maschine zurückzusichern. VMware bietet nun ein Tool (File Level Restore) an, das eine solche Rücksicherung ermöglicht. Das Tool unterstützt sowohl Windows- als auch Linux-Betriebssysteme. Sie rufen es in der betroffenen VM auf und können dann nach einer Auswahl Sicherungsdateien mounten. Jetzt können Sie mit dem Explorer nach den Dateien suchen, die zurückgesichert werden sollen.

Mit der Version 5.x hat VMware offiziellen Support für dieses Tool zugesagt; zuvor war die Nutzung zwar möglich, aber es gab keinen offiziellen Support.

14.2 Cluster-Konfiguration

Die Firma VMware unterstützt den Einsatz des Microsoft Cluster Service (MSCS) unter vSphere. Wer sich jetzt fragt, wozu eigentlich, VMware bietet ja auch ein HA für den Host-Ausfall, dem sei gesagt, dass es durchaus Sinn ergibt, einen MSCS-Cluster in einer virtuellen Umgebung aufzubauen. In Kundenumgebungen ist es nicht selten, dass zwar für ein produktives System ein Cluster eingesetzt wird, aber für die Entwicklung vermeintlich Kosten gespart werden, indem ein Standalone-Server verwendet wird. Das muss nicht sein, denn unter VMware ist eine solche Landschaft einfach und kostengünstig abbildbar. Ein weiteres mögliches Szenario ist der Test für das Update einer Cluster-Landschaft. Abseits der produktiven Umgebung können Sie in aller Ruhe die Reihenfolge für ein Update erarbeiten, ohne die Verfügbarkeit der produktiven Kundensysteme zu beeinflussen.

Für die Abbildung eines Clusters gibt es grundsätzlich drei Möglichkeiten: Zum Ersten können Sie den Cluster mit zwei virtuellen Maschinen auf einem Host aufbauen. Alternativ verteilen

Sie die Cluster-Knoten auf mehrere Hosts. Abschließend gibt es auch Support für einen Cluster mit einem physischen und einem virtuellen Knoten. Im Folgenden werden wir einzeln auf die verschiedenen Konfigurationsmöglichkeiten eingehen. Zuvor möchten wir aber noch die Voraussetzungen für den Einsatz von MSCS auf virtuellen Servern erläutern.

14.2.1 Voraussetzungen für den Microsoft Cluster Service

Damit Sie den Cluster unter VMware vSphere unterstützt aufbauen können, müssen soft- und hardwareseitig diverse Voraussetzungen erfüllt sein. Tabelle 14.2 listet die Bedingungen für den Einsatz auf.

Komponente	Bedingung
Betriebssystem	Windows 2003 Service Pack 2 Windows 2008 Service Pack 2 Windows 2008 R2
Virtual SCSI-Adapter	LSI Logic Parallel for Windows Server 2003 LSI Logic SAS for Windows Server 2008 und neuer
Festplattenformat	Anlegen der Festplatten mit der Option EAGERZEROEDTHICK, das heißt, bei der Anlage wird der gesamte Festplattenplatz allokiert und mit Nullen beschrieben.
Virtual NIC	Standardadapter für alle Betriebssysteme
Festplatten- und Netzwerkkonfiguration	Zuerst sind die Netzwerkadapter und anschließend die Festplatten hinzuzufügen.
Anzahl Knoten	Es werden maximal zwei Knoten unterstützt.
I/O-Timeout	Der Wert des Registry-Keys: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Disk\TimeOutValue` ist auf mindestens 60 zu setzen. Bei der Neuerstellung des Clusters wird der Wert automatisch zurückgesetzt.
NTP-Server	Die Zeitsynchronisierung über die VMware Tools deaktivieren und nur die Standarddomänen-Synchronisation nutzen.
Domäne	Beide Knoten müssen Mitglied einer Windows-Domäne sein.

Tabelle 14.2 Voraussetzungen MSCS

Zusätzlich zu diesen Bedingungen müssen Sie bei der Anlage der Festplatten ein Augenmerk darauf richten, wie Sie sie einrichten und wie Sie sie zur Verfügung stellen. Auch hier geben wir Ihnen in Tabelle 14.3 Aufschluss darüber, was unterstützt ist.

Festplattentyp	Cluster auf einem Host	Cluster auf mehreren Hosts	physischer/virtueller Cluster
virtuelle Festplatte im VMFS	ja	nein	nein
Raw Device Mapping, RDM (Virtual Compatibility Mode)	ja	ja	nein
Raw Device Mapping (Physical Compatibility Mode)	nein	ja	ja

Tabelle 14.3 Kompatibilität der einzelnen Festplattentypen

Es ist selbstverständlich möglich, mit virtuellen Maschinen, die vom SAN gebootet werden, einen Cluster aufzubauen. Sie müssen jedoch bedenken, dass solche Landschaften extrem komplex sind und die Fehlersuche sich ebenfalls nicht einfach gestaltet.

Der Microsoft Cluster Service selbst hat noch ein paar Einschränkungen, die den Einsatz verbieten, und zwar:

- Alle zum Einsatz kommenden Hosts müssen dieselbe Version des Host-Betriebssystems haben. Gemischte Umgebungen sind nicht unterstützt.
- Cluster dürfen in HA- und in DRS-Umgebungen eingesetzt werden, aber die DRS-Automation muss auf halbautomatisch gesetzt werden.
- VMware Fault Tolerance ist nicht unterstützt.
- Clustering ist auf iSCSI-, FCoe- und NFS-Platten nicht erlaubt.
- vMotion von Cluster-Knoten wird nicht unterstützt.
- Der Storage darf nicht mit Round-Robin-Multipathing konfiguriert sein.
- N-Port-ID-Virtualisierung (NPIV) ist nicht erlaubt.
- Die Nutzung einer Multipathing-Software im Gast ist nicht legitim.
- Die Bootplatte der VM darf nicht auf einem iSCSI-Device liegen.

Möchten Sie ein Cluster Continuous Replication Environment für Exchange aufsetzen, ist das grundsätzlich möglich. Achten Sie darauf, dass Sie die Cluster-Knoten virtuell aufbauen.

Die Installation der Cluster Services für die drei verschiedenen Möglichkeiten beschreiben wir im folgenden Abschnitt 14.2.2. In den darauf folgenden Abschnitten gehen wir nur noch auf die lösungsspezifischen Dinge ein.

14.2.2 Cluster-Konfiguration auf einem Host

Zur Veranschaulichung der Cluster-Konfiguration auf einem Host dient Abbildung 14.18. Hier ist schön zu sehen, dass beide betroffenen VMs auf einem Host liegen, die Daten aber nicht alle auf einer LUN liegen müssen.

Die einfachste Variante des MSCS in einer virtuellen Infrastruktur ist der Cluster auf einem Host. Als Erstes legen Sie die virtuellen Maschinen mit ihren lokalen, nicht gemeinsam genutzten Ressourcen an.

Erstellen Sie nun die beiden Cluster-Knoten, und nutzen Sie dabei eine »typische« VM-Konfiguration. Zum Einsatz sollte ein unterstütztes Betriebssystem kommen, das selbstverständlich bei der Anlage der VM eingestellt werden muss. Beim Einrichten der Festplatte für das Betriebssystem ist es wichtig, die korrekte Festplattenoption zu wählen. Die Option Support clustering features such as Fault Tolerance wird so nicht mehr ausgewiesen, Sie müssen die Option Thick Provision nutzen; diese stellt die Festplatte so bereit, wie sie bei einem

Cluster benötigt wird (Abbildung 14.19). Hinter dieser Alternative verbirgt sich die Option eagerzeroedthick. Der Speicherplatz der Disk wird direkt reserviert und mit Nullen vollgeschrieben.

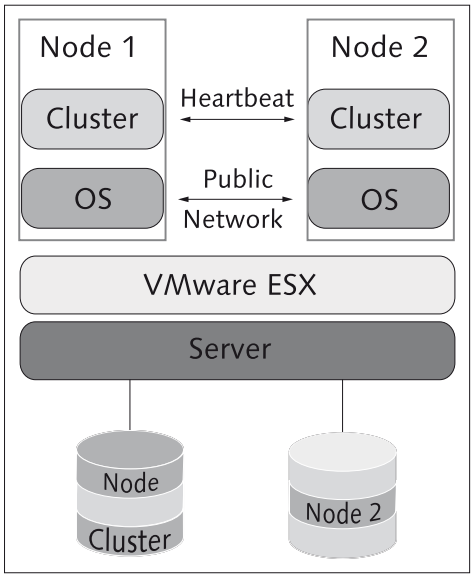


Abbildung 14.18 Microsoft Cluster Service auf einem ESX-Host

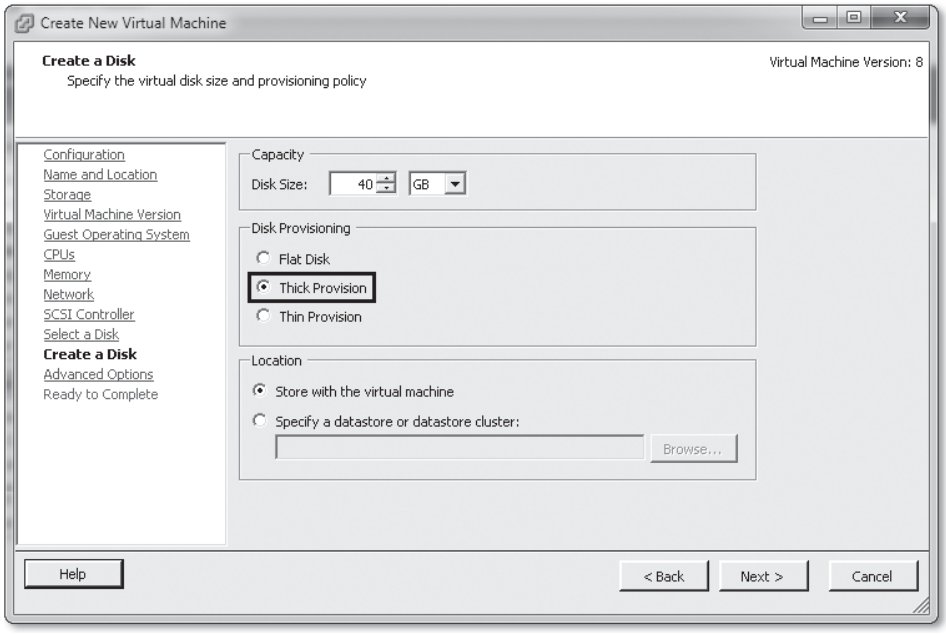


Abbildung 14.19 Konfiguration der lokalen Festplatte des Cluster-Knotens

Bei der Konfiguration des Clusters benötigen Sie mindestens zwei Netzwerkkarten. Die zusätzliche Karte wird dem Server hinzugefügt. Achten Sie darauf, dass Sie für die zweite Karte dieselbe »Hardware« nutzen, die auch bei der ersten Karte zum Einsatz kommt. Im Beispiel ist eine Netzwerkkarte für den internen Heartbeat-Traffic eingerichtet und eine zweite für den Client-Zugriff. Sie sehen außerdem, dass die VM eine aktuelle Hardwareversion hat (Abbildung 14.20).

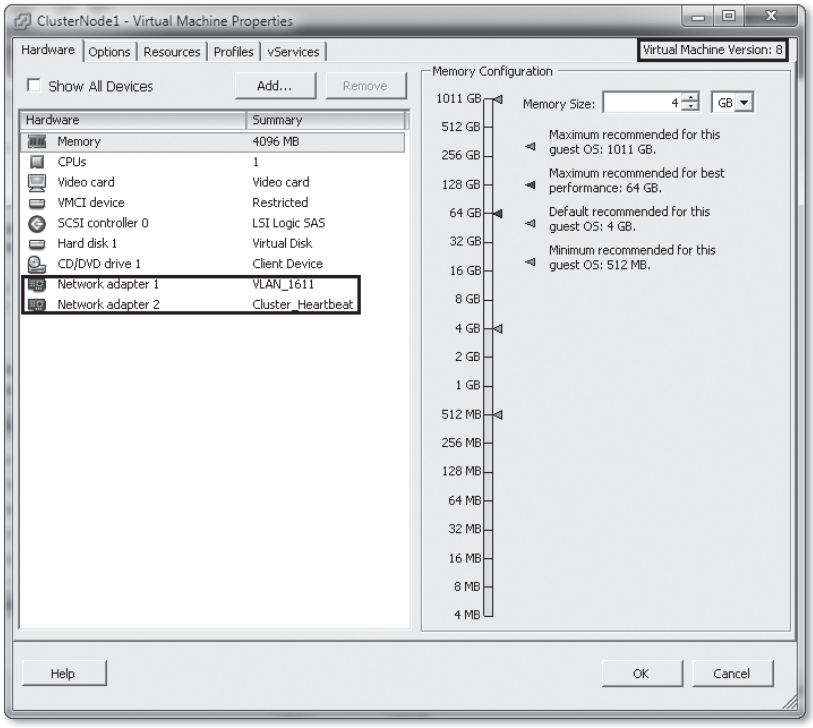


Abbildung 14.20 Konfiguration eines Cluster-Knotens

Den zweiten Cluster-Knoten legen Sie mit der gleichen Konfiguration an. Sind die Server-Hüllen bereitgestellt, installieren Sie auf beiden Systemen das Betriebssystem und bringen es auf das aktuelle Patch-Level. Den Heartbeat konfigurieren Sie in ein privates Netzwerk ohne Gateway, und NetBIOS over TCP/IP deaktivieren Sie. Bevor Sie mit der Einrichtung der gemeinsam genutzten Festplatten beginnen, sollten Sie beide Server in die Domäne aufnehmen.

Jetzt richten Sie eine gemeinsame Festplatte ein. Beginnen Sie mit den Arbeiten auf dem ersten Knoten. Über die Einstellungen des ersten Cluster-Knotens fügen Sie eine neue Festplatte hinzu. Die Festplatte sollte in demselben Verzeichnis liegen wie die Dateien der virtuellen Maschine. Auch in diesem Fall ist die Option zu setzen, dass es sich um eine Cluster-Festplatte handelt (Abbildung 14.21).

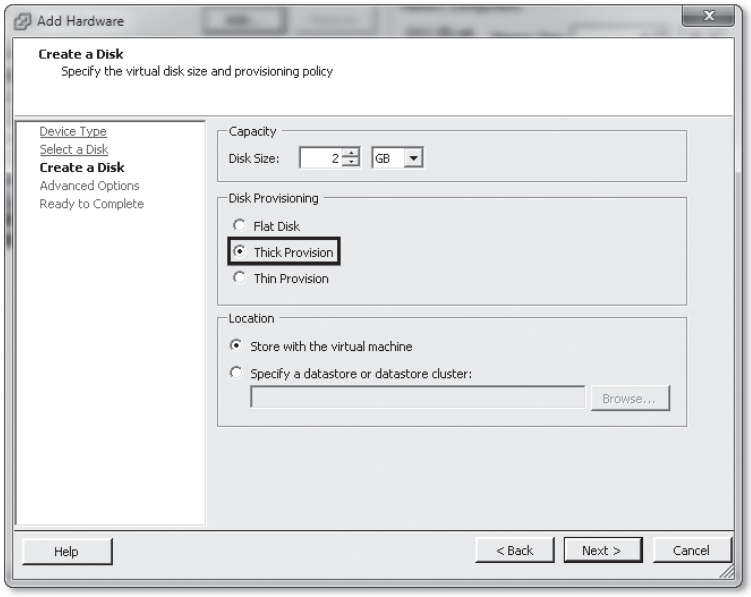


Abbildung 14.21 Anlegen einer gemeinsamen Festplatte auf dem ersten Knoten

Unter den ADVANCED OPTIONS geben Sie bei dem Abschnitt VIRTUAL DEVICE NODE die SCSI-ID für das neue Festplatten-Device an. Die erste Festplatte wird eine ID mit einer führenden Null haben. Aus diesem Grund muss bei der zweiten Festplatte die ID eine andere führende Ziffer haben. Was passiert nun im Hintergrund bei der Änderung der Einstellung? Die erste Ziffer gibt an, über welchen SCSI-Adapter die Festplatte bedient wird. Durch die Auswahl einer anderen führenden Ziffer bei der SCSI-ID wird dem System ein zusätzlicher SCSI-Festplatten-Controller hinzugefügt. Für die weitere Vorgehensweise ist das enorm wichtig. Es wäre sonst nicht möglich, dass zwei virtuelle Systeme auf eine Festplatte zugreifen könnten (Abbildung 14.22).

Die SCSI-ID setzt sich wie folgt zusammen: <Controllernummer>:<SCSI Gerätenummer>.

Nun ist die neue Festplatte in der Konfiguration der VM sichtbar. Über CHANGE TYPE bestimmen Sie den SCSI-Controller-Typ (Abbildung 14.23).

Die Auswahl erfolgt nach der Auswertung der Informationen in Tabelle 14.4.

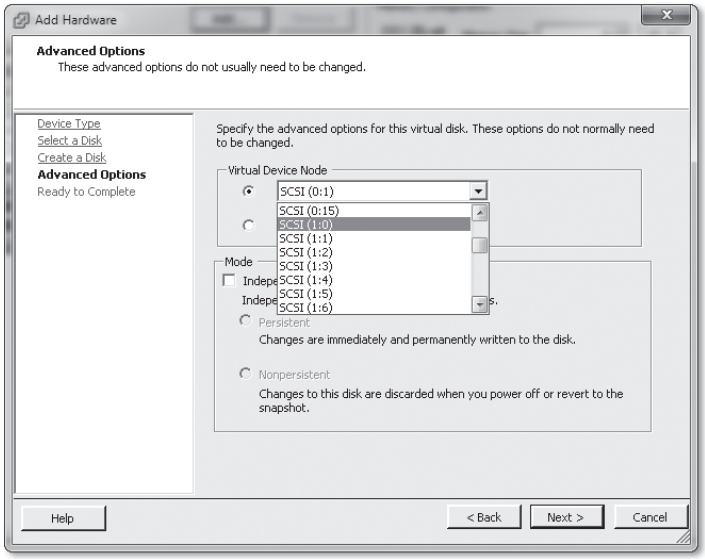


Abbildung 14.22 Auswahl der SCSI-ID

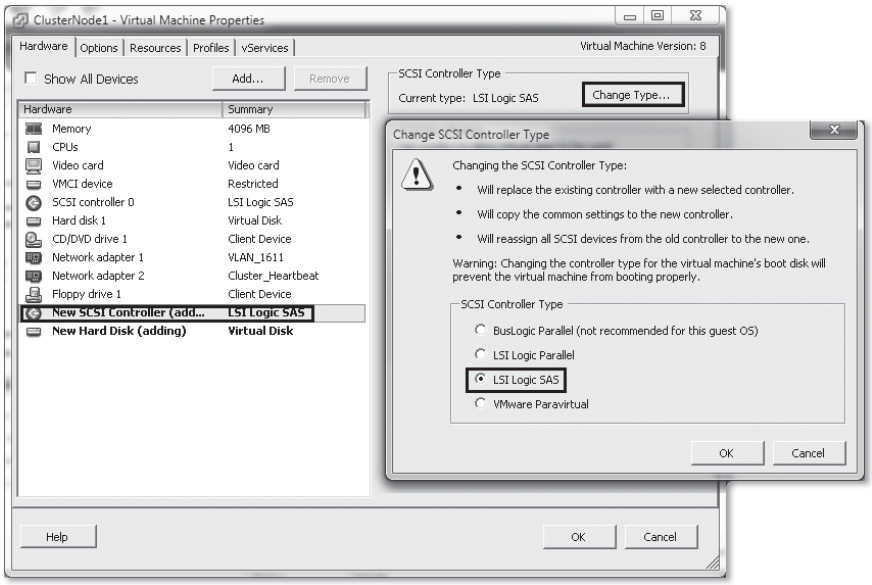


Abbildung 14.23 Auswahl des Controller-Typs für das gesharte Device

Betriebssystem	Controller-Typ
Windows Server 2003	LSI Logic Parallel
Windows Server 2008	LSI Logic SAS

Tabelle 14.4 Abhängigkeit zwischen Betriebssystem und Festplatten-Controller

Damit der Zugriff von zwei virtuellen Maschinen auf eine gemeinsame Festplatte erfolgen kann, ist der Modus für SCSI Bus Sharing zu konfigurieren. In diesem speziellen Fall wählen wir virtual. So können zwei VMs direkt auf eine VMDK-Datei zugreifen, solange sich die zugreifenden virtuellen Maschinen auf einem Host befinden (Abbildung 14.24).

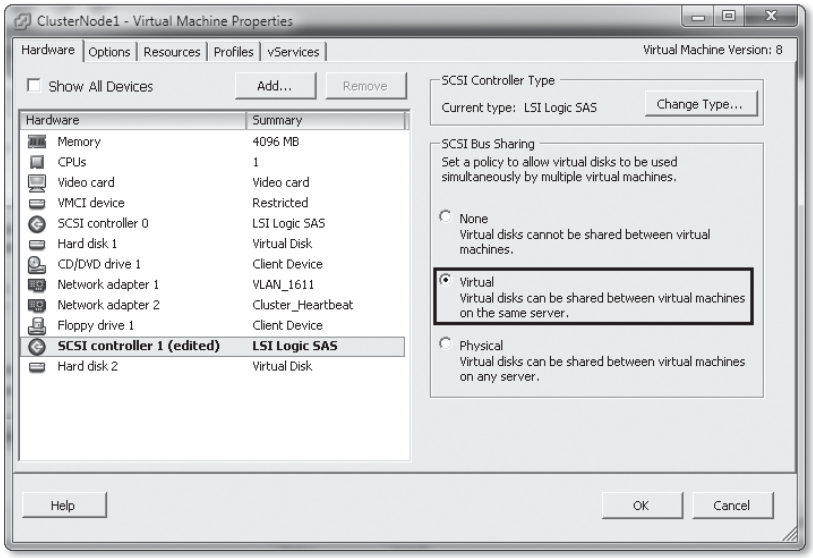


Abbildung 14.24 Konfiguration des SCSI-Bus-Sharings

Die hardwaretechnischen Arbeiten auf dem ersten Knoten sind nun abgeschlossen. Jetzt können Sie mit der Einrichtung des Clusters im Betriebssystem beginnen. Eine funktionierende DNS-Auflösung ist für eine einwandfreie Installation unbedingt erforderlich. Formatieren Sie die zukünftigen gemeinsamen Festplatten in der Computerverwaltung, und versehen Sie sie mit Laufwerksbuchstaben. Stoßen Sie über den Menüpunkt Start • Administrative • Tools • Cluster • Administrator die Installation des Microsoft-Clusters an. Es startet ein Wizard für die Einrichtung des Clusters. Zu Beginn wird die Angabe der Windows-Domäne und des Cluster-Namens erwartet. Im folgenden Dialog geben Sie den Computernamen des ersten Cluster-Knotens an. Jetzt überprüft die Software, ob alle Voraussetzungen für die endgültige Installation des Clusters erfüllt sind (Abbildung 14.25).

Der Wizard erfragt nun die IP-Adresse für den Cluster. Einen Domänen-Account für den Start des Cluster-Dienstes erwartet die Installationsroutine einen Schritt später. Die übliche Installationszusammenfassung wird angezeigt, bevor Sie den eigentlichen Installationsvorgang starten. An dieser Stelle können Sie auch auswählen, auf welcher Festplatte die Quorumdisk installiert werden soll (Abbildung 14.26).

Nach Abschluss der Arbeiten können Sie das Installations-Log einsehen. Beenden Sie den Wizard, stellt sich der Cluster im Cluster Administrator dar (Abbildung 14.27).

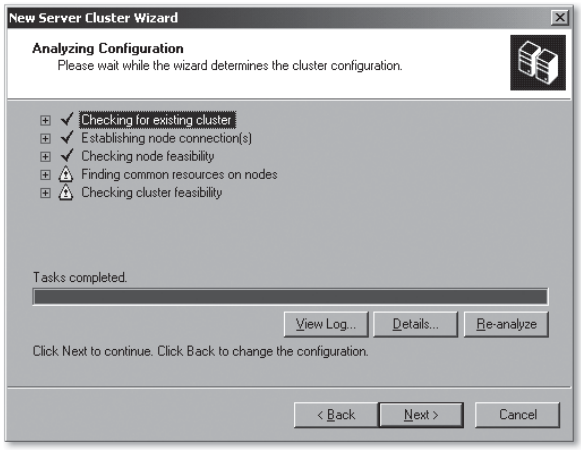


Abbildung 14.25 Check der Cluster-Konfiguration

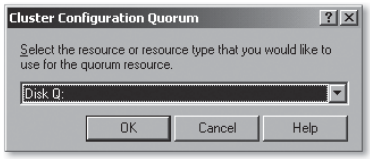


Abbildung 14.26 Auswahl der Quorumdisk

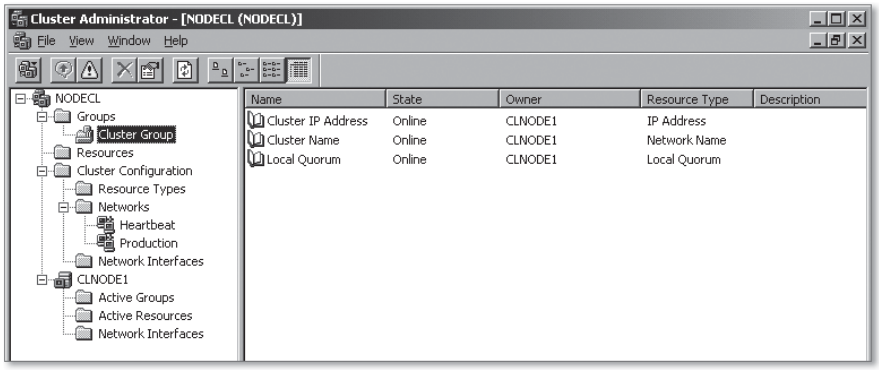


Abbildung 14.27 Cluster nach der Installation des ersten Knotens

Nachdem der erste Cluster-Knoten vollständig konfiguriert und eingerichtet ist, nehmen wir uns den zweiten virtuellen Cluster-Knoten vor. Auch hier ist eine zweite Festplatte mit dem System zu verbinden. Der Unterschied besteht darin, dass wir keine neue Festplatte anlegen, sondern eine bereits vorhandene mit der zweiten VM verbinden. Es handelt sich um die Festplatte, die beim ClusterNode1 an den zweiten Festplatten-Controller gehängt wurde. Geben Sie der Festplatte die gleiche ID wie auf dem ersten Server.

Jetzt ist der Cluster-Service auf dem zweiten Cluster-Knoten bereitzustellen.

Auch starten Sie über den Menüpunkt START • ADMINISTRATIVE TOOLS • CLUSTER ADMINISTRATOR die Aufnahme des zweiten Knotens in den Cluster-Verbund. Für die Aufnahme eines zweiten Knotens gibt es einen eigenen Auswahlpunkt. Hier wird auch die Eingabe des Namens des Clusters erwartet. Jetzt wird, wie bei der Initialinstallation, geprüft, ob alle Voraussetzungen für die Aufnahme des Knotens erfüllt sind. Geben Sie im nächsten Dialogfenster das Passwort des angezeigten Accounts ein, und starten Sie mit zwei weiteren Klicks die Installation. Jetzt ist der Cluster erfolgreich installiert (Abbildung 14.28).

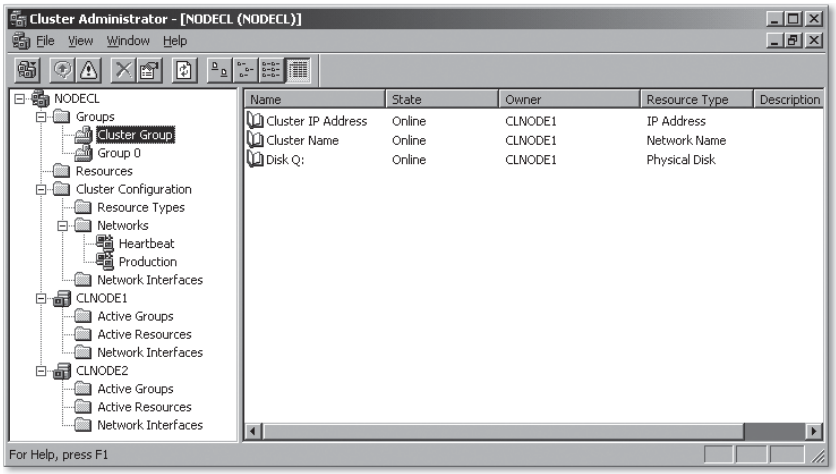


Abbildung 14.28 Erfolgreich installierter Cluster mit zwei Knoten

Die Arbeiten sind jetzt so weit abgeschlossen, dass Sie die Applikation installieren können.

14.2.3 Cluster-Konfiguration über mehrere Hosts

Im Gegensatz zur Konfiguration in Abschnitt 14.2.1 liegen die Cluster-Daten der beiden Knoten nicht auf einer virtuellen Festplatte, sondern auf einer eigenen dedizierten LUN. Beide Cluster-Mitglieder greifen direkt auf den Storage zu. Das File-System wird direkt über das Betriebssystem des Clusters angelegt. Alle anderen virtuellen Maschinen können die Raw LUN nicht sehen (Abbildung 14.29).

Es ist möglich und wird auch unterstützt, den zweiten Knoten eines Clusters über unterschiedliche Hosts zur Verfügung zu stellen. Die Konfiguration und Bereitstellung der beiden Grundmaschinen ist mit den im vorherigen Abschnitt beschriebenen Schritten absolut identisch. Die Arbeiten unterscheiden sich lediglich in der Anlage der gemeinsam genutzten (Shared) Festplatten. In diesem Fall können Sie keine virtuelle Festplatte nutzen, sondern müssen sogenanntes Raw Device Mapping verwenden. Das bedeutet, dass Sie eine SAN-LUN direkt mit der virtuellen Maschine verbinden. Der SCSI-BUS-SHARING-Modus ist auf PHYSICAL zu setzen.

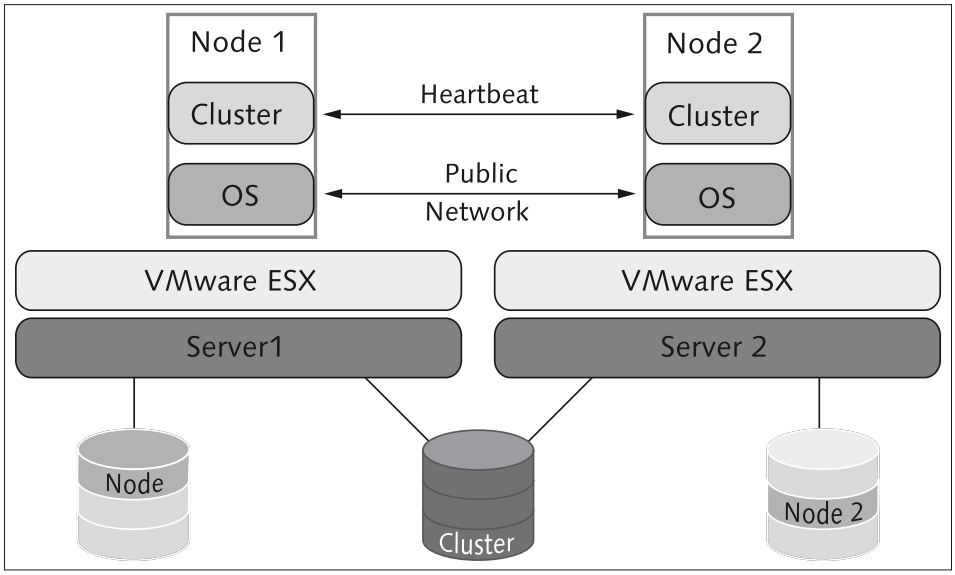


Abbildung 14.29 MSCS mit VMs über zwei Hosts verteilt

Ist diese Platte im Betriebssystem sichtbar, richten Sie das File-System ein. Jetzt stellen Sie den Cluster bereit, was sich von den Arbeitsschritten, die wir schon beschrieben haben, in keiner Weise unterscheidet. Ist der erste Cluster-Knoten betriebsbereit, fügen Sie den zweiten Knoten dem Cluster hinzu. Hierbei gibt es unter Umständen Herausforderungen, die recht einfach zu lösen sind. Das Hinzufügen des zweiten Knotens kann zu Problemen führen, wenn das Raw-Device auf beiden Servern nicht dieselbe ID hat. Das ist durchaus möglich und auch unterstützt. Es kann sein, dass der Knoten sich nicht hinzufügen lässt. In diesem Fall klicken Sie beim Hinzufügen des zweiten Knotens im Auswahlfenster des Computers den ADVANCED-Button (Abbildung 14.30) und deaktivieren die Option für die Verifikation des Storages (Abbildung 14.31).

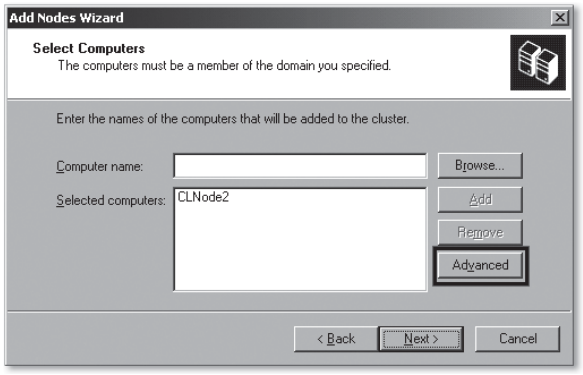


Abbildung 14.30 Aufruf der »Advanced«-Option

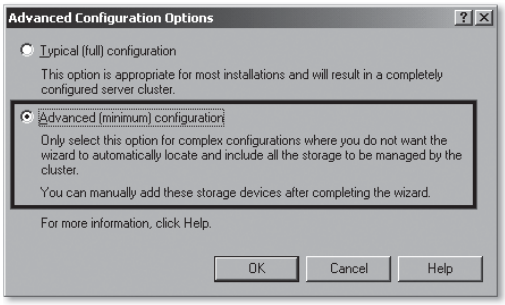


Abbildung 14.31 Aktivierung der »Advanced (minimum) configuration«

Die weitere Vorgehensweise gestaltet sich wie bei der vorherigen Variante.

14.2.4 Cluster-Konfiguration zwischen physischem und virtuellem Knoten

Diese Variante unterscheidet sich nur geringfügig von der Konfiguration in Abschnitt 14.2.3 denn eigentlich liegen die beiden Cluster-Knoten auf verschiedenen Hosts (Abbildung 14.32). Auch wenn der eine Host ein dedizierter physischer Server ist, so liegt der Unterschied nur in der Bereitstellungsreihenfolge.

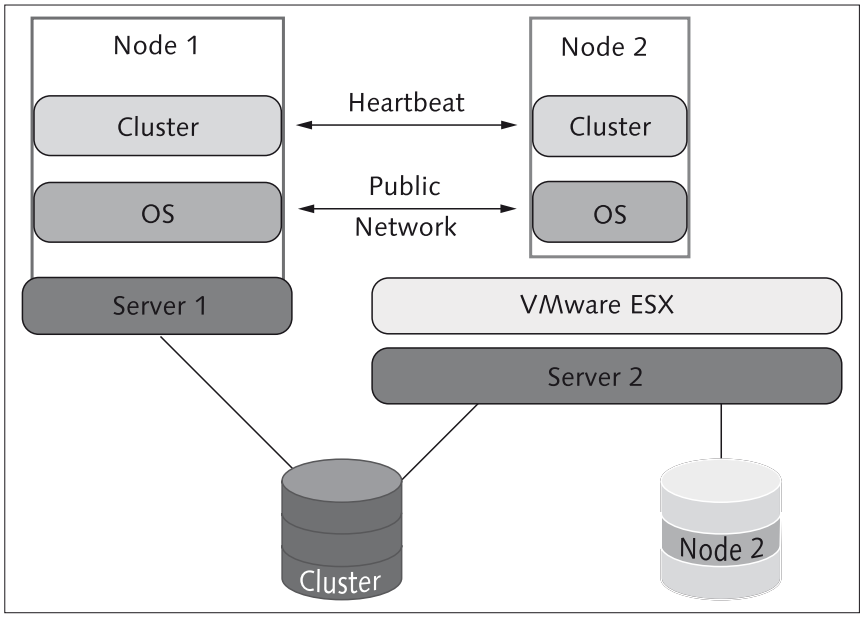


Abbildung 14.32 Physischer/virtueller MS-Cluster

Der Unterschied besteht darin, dass der erste Knoten ein physischer ist. Die Einstellungen in der VM müssen Sie anders als in der zuletzt beschriebenen Variante nicht anpassen. Auch hier wird ein Raw Device Mapping mit physisch gemeinsam genutzten Platten eingesetzt, aber die

Reihenfolge ist eine andere. Nachdem Sie auf beiden Servern das passende freigegebene Betriebssystem installiert haben, fahren Sie mit den Arbeiten auf dem virtuellen Knoten fort. Den physischen Knoten nehmen Sie erst im zweiten Schritt in den Cluster auf.

Welchen Vorteil bringt nun die Nutzung eines physischen/virtuellen Clusters? In Abbildung 14.33 haben wir das einmal veranschaulicht. Schauen Sie sich an, welche Cluster-Typen in der Regel in Betrieb genommen werden, dann fällt auf, dass meistens Active/Passive-Cluster aufgesetzt werden. Das bedeutet: Primär ist ein Knoten aktiv, und der andere wartet darauf, dass der erste den Dienst versagt.

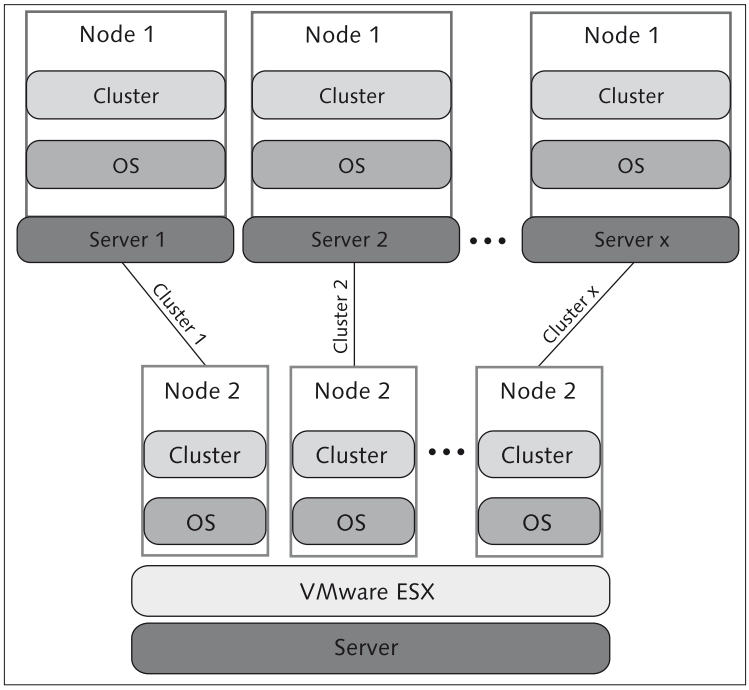


Abbildung 14.33 vSphere-Host mit mehreren MS-Cluster-Knoten

Das führt dazu, dass die Kosten für den Cluster recht hoch sind. Es werden zwei Server gekauft, damit ein Dienst zur Verfügung gestellt werden kann.

Jetzt kommt der Vorteil der Virtualisierung voll zum Tragen. Kommen mehrere Cluster in der Firma zum Einsatz, dann werden die primär aktiven Systeme als physische Maschine abgebildet, und die zweiten Cluster-Knoten werden virtuell aufgebaut. Der Vorteil liegt auf der Hand: Die Maschine, die die virtuellen Systeme aufnimmt, ist zwar etwas größer zu dimensionieren, aber man macht sich den Umstand zunutze, wie unwahrscheinlich es ist, dass alle Cluster gleichzeitig ausfallen. So übernimmt der virtuelle Host die Arbeit im Falle eines Ausfalls oder bei Wartungsaufgaben. Auf diese Weise können Sie die zu nutzenden Ressourcen im Rechenzentrum reduzieren. Sie sparen Stellplatz, Netzwerkports, SAN-Ports, Strom und Klimabedarf.

Dem gegenüber stehen zwar die Lizenzkosten von VMware, aber das rechnet sich recht schnell.

14.3 Virtual Machine Monitoring

Seit der Version 3.5 der Virtual Infrastructure bietet VMware eine Funktion zur Überprüfung der virtuellen Maschinen auf Reaktion. Wann kann die Funktion genutzt werden? Was genau bedeutet die Funktion?

Das Virtual Machine Monitoring ist eine Unterfunktion des vSphere HA, was heißt, dass Sie die Funktion nur in einem aktiven HA-Cluster nutzen können. Erst wenn die HA-Funktionalität in einem Cluster aktiviert ist, steht die Funktion zur Verfügung (Abbildung 14.34).

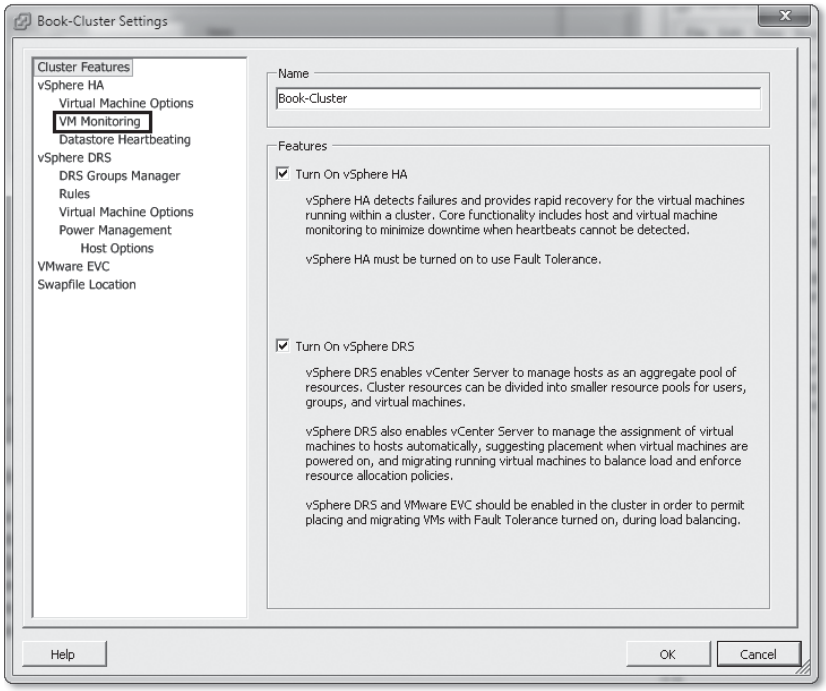


Abbildung 14.34 Virtual Machine Monitoring

Die Funktion ist eine Ergänzung zu dem schon bekannten Heartbeat zur virtuellen Maschine. Der Heartbeat kommuniziert mit den VMware Tools einer virtuellen Maschine, um zu kontrollieren, dass sie noch einwandfrei arbeitet. Antworten die VMware Tools ordnungsgemäß, ist für den Host alles in Ordnung. Weitere Tests werden nicht durchgeführt. An dieser Stelle greift das Virtual Machine Monitoring ein. Dieser Zusatz überwacht zusätzlich die Aktivitäten der Festplatte und der Netzwerkkarte. Zeigen sich bei der Auswertung der beiden Funktionen Unregelmäßigkeiten, wird die virtuelle Maschine neu gestartet. Mit der Version 5.x hat sich

hier eine weitere Änderung ergeben: Sie können die Überwachungsfunktion der VM erweitern. Über die Auswahl VM and Application Monitoring lassen sich über das VM-Monitoring auch Applikationen überwachen. Nutzbar ist diese Funktion aber nur, wenn Ihre Applikation eine passende Schnittstelle zu den VMware Tools hat.

Die Art und Weise, wie die Maschine neu startet, können Sie selbst definieren (Abbildung 14.35). Zuallererst aktivieren Sie das VM Monitoring oben im Fenster. Zwei Optionen bieten sich Ihnen zur Auswahl: Entweder stellen Sie alle Kontrollwerte manuell ein, oder Sie greifen auf die Parameter zurück, die Sie über den Schieberegler regulieren können.

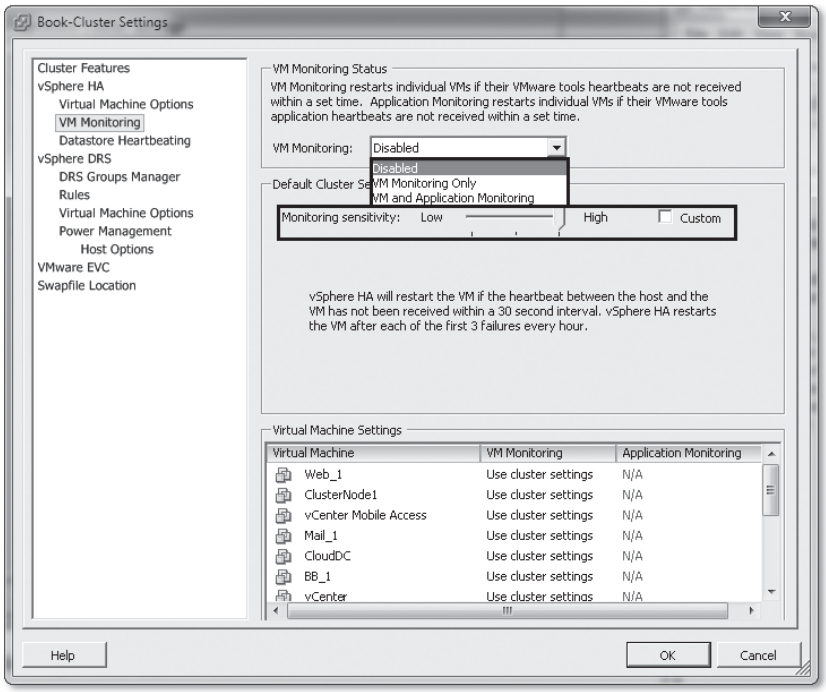


Abbildung 14.35 Konfiguration des VMM

Mit dem Regler lassen sich drei mögliche Parametrierungen einstellen.

Monitoring Sensitivity	Failure Interval	Minimum Uptime	Maximum per VM Resets	Maximum Resets Time Window
low	120 Sekunden	8 Minuten	3	7 Tage
middle	60 Sekunden	4 Minuten	3	1 Tag
high	30 Sekunden	2 Minuten	3	1 Stunde

Tabelle 14.5 Überwachungsparameter des VMM

Das failure interval gibt an, wie lange die Bedingung erfüllt sein muss, bevor ein Fehler angezeigt wird. Die Minimum uptime bezeichnet ein Zeitintervall, das nach dem Start der VM

abläuft, bis das Überwachungstaktsignal erzwungen wird. Erst ab diesem Zeitpunkt wird die VM wieder überwacht. Über das Maximum per VM resets legen Sie fest, wie oft eine virtuelle Maschine maximal neu gestartet werden darf. Das gültige Zeitintervall für die Messung der Anzahl der Reboots ist die Einstellung, die sich hinter dem Wert Maximum resets time window verbirgt.

Der Neustart des virtuellen Servers im Falle eines Fehlers erfolgt automatisch, wenn die Option in der Konfiguration des VMM aktiviert wurde. Die Optionen des Virtual Machine Monitors sind jetzt definiert. Bei den genannten Regeln handelt es sich um die cluster-weite Standardeinstellung für den gesamten HA-Cluster. Diese Einstellung gilt standardmäßig für *alle* virtuellen Maschinen des Clusters. Sollen einige der virtuellen Server anders eingestellt sein, konfigurieren Sie das einzeln für jede VM im unteren Drittel des Einstellungsfensters. Wählen Sie einfach einen virtuellen Server aus, und passen Sie seine Parameter an. Hier treffen Sie wieder auf die bereits bekannten Parameter low, medium, high und custom. Über den Wert none deaktivieren Sie die Überwachungsfunktion für eine VM.

Wir raten Ihnen: Versuchen Sie, mit so wenig granularen Einstellungen auszukommen wie möglich. Es geht sonst einfach die Übersichtlichkeit verloren. Definieren Sie eine Custom-Einstellung, und versuchen Sie dann, mit den vier Kategorien (Low, Medium, High und Custom) zurechtzukommen, die Sie danach zur Verfügung haben.

Der Vollständigkeit halber möchten wir noch erwähnen, dass Sie die Werte für den Cluster auch anders manipulieren können, indem Sie im Einstellungsfenster unter vSphere HA • Advanced Options die Werte für die Einstellungen manuell eintragen. Lassen Sie uns die Werte in Tabelle 14.6 kurz erläutern.

Option	Beschreibung	Standard
clusterSettings	Sollen die Cluster-Einstellungen oder die Einstellungen der VM genutzt werden?	Cluster
enabled	Ist der Service aktiviert?	nein
failureInterval	Definiert, wie lange eine VM maximal nicht antworten darf, bevor sie auf fehlerhaft gesetzt wird.	30 Sek.
maxFailures	Anzahl der Fehler, die im maxFailureWindow auftreten dürfen, bevor die Überwachung eingestellt wird	3
maxFailureWindow	Anzahl von Sekunden, in denen maxFailure auftreten darf, bevor die Überwachung eingestellt wird	1 Sek.
minUpTime	Zeit in Sekunden, die der Server benötigt, um neu zu starten. Für dieses Zeitintervall wird die Überwachung ausgesetzt.	120 Sek.

Tabelle 14.6 Virtual Machine Monitoring – »Advanced Options«

Mit dem VMM können Fehlfunktionen in einem virtuellen Server abgefangen werden. Als Beispiel sei hier der allseits bekannte Bluescreen genannt. Ein solcher Missstand ließe sich mit dem VMM beheben. Es besteht durchaus die Option, mit dieser Funktion die Verfügbarkeit

von virtuellen Maschinen zu erhöhen. Kommt eine Fehlfunktion in einer VM öfter vor, so dass VMM einen Systemneustart durchführt, sollten Sie genau analysieren, warum das so ist. Sie können davon ausgehen, dass in diesem Fall ein Fehler in der VM vorliegt, der selbstverständlich behoben werden muss. Die Zuverlässigkeit der Funktion lässt sich im Grunde genommen sehr einfach testen: Halten Sie einfach die VMware Tools im laufenden Betrieb an. Die Verbindung des Taktsignals reißt ab, und die Maschine wird nach dem festgesetzten Intervall neu gestartet.

14.4 Fault Tolerance

Fault Tolerance ist eine Technologie von VMware, die mit der Version vSphere 4.x neu eingeführt. Sie dient zur unterbrechungsfreien Bereitstellung eines Server-Dienstes.

Die Funktionsweise und die Voraussetzungen von VMware Fault Tolerance haben wir in Kapitel 5, »Cluster«, näher beschrieben.

In diesem Kapitel erhalten Sie einen Überblick über virtuelle Maschinen, ihre Einrichtung und ihren Betrieb.

15 Virtuelle Maschinen

Autor dieses Kapitels ist Carsten Schäfer, G-TAC IT-Beratung, Carsten.Schaefer@G-TAC.de

15.1 Grundlagen

15.1.1 Was ist eine virtuelle Maschine?

Eine virtuelle Maschine gaukelt einem Gastbetriebssystem ein Intel-x86-System vor, wahlweise 32 oder 64 Bit. Die virtuelle Maschine (VM) stellt virtuelle Hardware bereit, damit diese aus der Sicht des Gastbetriebssystems so genutzt werden kann, wie es sich auch bei physischen Servern verhalten würde. Einige Ausnahmen gibt es, diese stellen wir aber in diesem Kapitel vor.

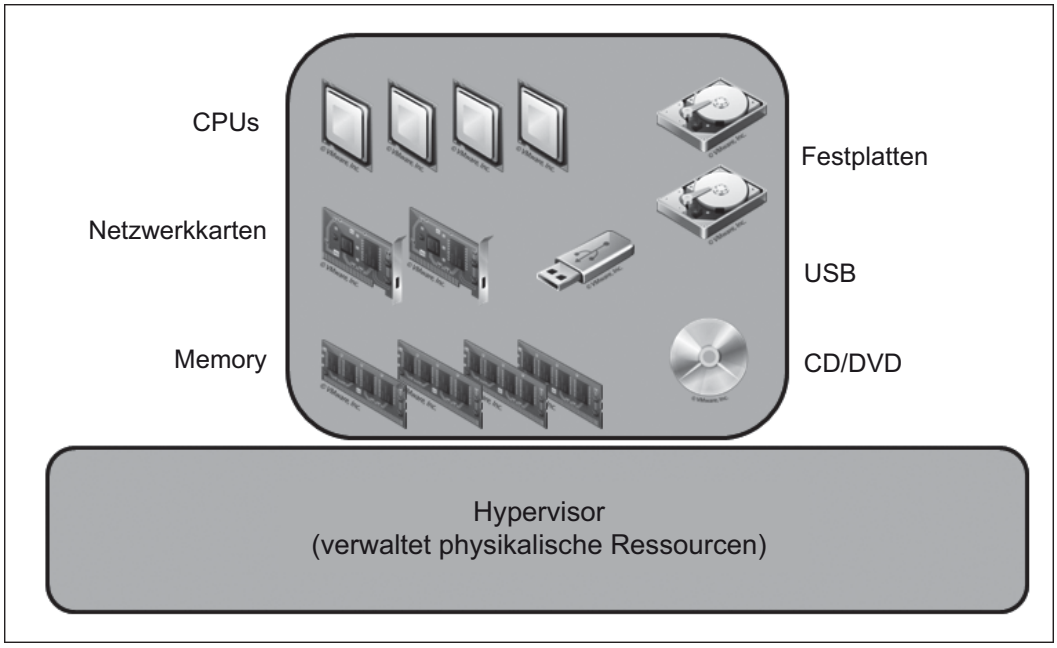


Abbildung 15.1 Eine virtuelle Maschine besteht aus virtueller Hardware.

15.1.2 Virtuelle Hardware

CPU und Speicher

Die CPU und der Hauptspeicher einer virtuellen Maschine werden im Gegensatz zur restlichen virtuellen Hardware nicht emuliert, sondern durch die VMware ESX-Virtualisierungsschicht nahezu identisch mit der physischen Hardware einer VM bereitgestellt. Beim Speicher können Sie durch die VMware-Technologie Memory-Overcommitment mehr Speicher als tatsächlich vorhanden zur Verfügung stellen, indem Sie einen Teil des Speichers einer VM auf Datastores (DAS, SAN, NFS) in Dateiform ablegen, anstatt ihn im physischen RAM des ESX-Servers zu nutzen. Ausführliche Informationen zu den Grundlagen und dem Ressourcenmanagement von CPU und Memory erhalten Sie in Kapitel 2, »vSphere-Architektur«.

Diskettenlaufwerk

Das Medium des virtuellen Diskettenlaufwerks einer VM können Sie auf unterschiedliche Weise konfigurieren. Dabei bleibt die virtuelle Hardware im Gastbetriebssystem immer identisch, aber das Medium kann jederzeit angepasst werden. Außerdem ist es möglich, verschiedene Quellen als Medium zu nutzen. Die virtuelle Maschine sieht unabhängig von der Quelle immer ein lokales Diskettenlaufwerk mit oder ohne Diskette. Des Weiteren kann das Medium im laufenden Betrieb der VM hinzugefügt oder entfernt werden (Device-Status) oder grundsätzlich beim Starten der VM immer zur Verfügung stehen.

Folgende Möglichkeiten stehen zur Verfügung:

- Client Device
  Diese Einstellung ermöglicht das Verbinden des Diskettenlaufwerks im Gast mit einem physisch vorhandenen Diskettenlaufwerk oder einem Floppy-Image auf dem PC oder Server, auf dem der vSphere-Client läuft und die VMware Console geöffnet werden kann. Bei Nutzung eines Images muss dieses nur vom vSphere-Client-Programm erreichbar sein und nicht vom ESX-Server oder der virtuellen Maschine.
- Host Device
  Diese Einstellung bietet eine Verbindung zu dem im ESX-Server eingebauten Diskettenlaufwerk. Dabei müssen Sie die Unix-Schreibweise des Devices verwenden, z. B. */dev/fd0*. Diese Einstellung ist nicht empfehlenswert, da es zu Problemen mit vMotion und DRS kommen kann. Außerdem blockiert eine eingelegte bootfähige Diskette möglicherweise sämtliche VMs mit konfiguriertem Host-Device beim Starten, da die virtuellen Maschinen von Diskette booten.
- Use existing floppy image in datastore (»bestehendes Floppy-Image im Datastore verwenden«)
  Bei dieser Einstellung kann ein vorhandenes Floppy-Image auf dem VMware-Datastore benutzt werden. Dieses muss vorher in ein beliebiges Verzeichnis auf dem VMware-Datastore kopiert werden. Außerdem kann das lokale */vmimages*-Verzeichnis (hier liegen auch

die Images der VMware-Tools-Installationen) des ESX-Servers genutzt werden. Allerdings gelten hier die gleichen Nachteile bezüglich vMotion und DRS wie bei der Nutzung des Host-Devices.

- Create new floppy image in datastore (»neues Floppy-Image im Datastore erstellen«)
  Bei dieser Einstellung wird ein neues Floppy-Image auf dem VMware-Datastore angelegt und dann der VM bereitgestellt. Die Auswahl dieser Option bleibt nicht bestehen, sondern die vorherige Option, Use existing floppy image in datastore, wird aktiviert und als Auswahl das neu erstellte Floppy-Image definiert.

CD-ROM-/DVD-Laufwerk

Genau wie das Diskettenlaufwerk können Sie auch ein virtuelles CD-ROM-/DVD-Laufwerk einer VM konfigurieren. Die grundsätzlichen Eigenschaften sind mit denen des virtuellen Diskettenlaufwerks identisch, allerdings bestehen bessere Möglichkeiten zur Nutzung von Medien mit großen Datenmengen.

Folgende Möglichkeiten stehen zur Verfügung:

- Client Device
  Diese Einstellung ermöglicht das Verbinden des CD-ROM-/DVD-Laufwerks im Gast mit einem physisch vorhandenen CD-Laufwerk auf dem PC oder Server, auf dem der vSphere-Client läuft und die VMware Console geöffnet werden kann. Alternativ verbinden Sie das Laufwerk des Gastes auch mit einem ISO-Image. Dieses Image muss vom vSphere-Client aus erreichbar sein. Das Verbinden können Sie erst im eingeschalteten Zustand der virtuellen Maschine durchführen.
- Host Device
  Diese Einstellung bietet eine Verbindung zum im ESX-Server eingebauten CD-ROM-/DVD-Laufwerk. Dabei müssen Sie die Unix-Schreibweise des Devices verwenden, z. B. */vmfs/devices/cdrom/mpx.vmhba0:C0:T0:L0*. Bitte beachten Sie die Einschränkungen für vMotion.
- Datastore ISO file
  Bei dieser Einstellung kann ein vorhandenes ISO-Image auf einem VMware-Datastore verwendet werden. Dieses muss vorher in ein beliebiges Verzeichnis auf dem VMware-Datastore kopiert werden.
- Passthrough IDE
  Dies ist die Standardeinstellung für die Verbindung zu einem physischen Laufwerk und bietet die größte Performance.

  Optional definieren Sie hier die exklusive Nutzung des Laufwerks von der virtuellen Maschine.
- Emulate IDE
  Die Einstellung bietet nur Lesezugriff auf eine CD oder DVD, da der Zugriff emuliert wird.

Abschließend können Sie die ID des virtuellen Devices ändern. Standardmäßig ist diese beim ersten Laufwerk immer 0:0, beim zweiten 0:1, beim dritten 1:0 und beim vierten Laufwerk 1:1.

SCSI-Controller

Als SCSI-Controller werden folgende Typen unterstützt:

- BusLogic Parallel
- LSI Logic Parallel
- LSI Logic SAS
- VMware Paravirtual

Der BusLogic-Parallel-Controller wird von älteren Gastbetriebssystemen, z. B. Windows 2000, verwendet. Den LSI-Logic-Parallel-Controller hingegen nutzen neuere Betriebssysteme, so ist z. B. ab Windows Server 2003 der native Support für diesen Controller bereits im Betriebssystem integriert. Der LSI-Logic-SAS-Controller steht in virtuellen Maschinen ab der Version 7 zur Verfügung, und in Windows Server 2008 und später findet sich hierfür auch native Unterstützung.

Der VMware-Paravirtual-Controller (PVSCSI) ist ebenso erst ab der Version 7 von VMs einsetzbar und bietet die beste Performance bei geringerer CPU-Auslastung; allerdings wird dieser Controller-Typ im Gastbetriebssystem erst ab Windows 2003 und ab RHEL 5 unterstützt.

Damit Sie diesen Adaptertyp einsetzen können, muss in der VM das Gastbetriebssystem mit den VMware Tools bereits installiert sein. Erst ab Windows 2003 können Sie diesen Adapter auch für Boot-Festplatten einsetzen. Sollten Sie mit Betriebssystemen im Gast arbeiten, die keine native Unterstützung für Boot-Festplatten mitbringen, dann installieren Sie das Betriebssystem mit dem dafür vorgesehenen Standard-Controller, z. B. LSI Logic, installieren die VMware Tools und ändern dann nachträglich den Adaptertyp auf PVSCSI.

Der Einsatz eines PVSCSI-Controllers bringt leider auch einige Nachteile mit sich:

- Das Hinzufügen oder Entfernen von Festplatten im laufenden Betrieb (Hot Add) bedingt einen Rescan des SCSI-Busses aus dem Gastbetriebssystem heraus.
- Möglich sind Leistungseinbußen, sobald von einer Festplatte ein Snapshot existiert oder sobald ein ESXi-Host in das Memory-Overcommitment läuft.
- Microsoft Failover Cluster wird mit diesem Adaptertyp nicht unterstützt.
- Bei RHL 5 wird dieser Adaptertyp für die Boot-Festplatte nicht unterstützt. Verwenden Sie in diesem Fall für die Bootpartitionen wie bislang einen LSI-Controller. Den PVSCSI-Controller setzen Sie dann zum Betrieb weiterer Festplatten in der VM ein, um z. B. Daten oder Datenbanken darauf abzulegen.

Bei der Änderung des Controller-Typs müssen Sie darauf achten, dass das Gastbetriebssystem über die notwendigen Treiber verfügt, da das Betriebssystem ansonsten die virtuellen Festplatten nicht mehr sehen und verwenden kann. Hierzu installieren Sie entweder die Treiber des zukünftigen Controllers vorher im Gast, oder Sie fügen zu dem bestehenden Controller den neuen Controller hinzu, um die Treiber zu installieren und abschließend den ursprünglichen Controller zu entfernen.

Zusätzlich können Sie eine Richtlinie über das SCSI-Bus-Sharing definieren. Weitere Informationen dazu erhalten Sie in Abschnitt 15.2.2, »Festplattenkonfiguration«.

Netzwerkkarten

Eine virtuelle Maschine kann je nach Gastbetriebssystem aus folgenden Netzwerkkartentypen auswählen:

- E1000
- Flexible
- VMXNET 2 (Enhanced)
- VMXNET 3

Nachfolgend finden Sie weitere Informationen über die von VMware je nach ausgewähltem Gastbetriebssystem bereitgestellten Netzwerkadaptertypen:

- **E1000**
  Die virtuelle Netzwerkkarte emuliert eine Intel-82545EM-Gigabit-Ethernet-Karte und wird in den meisten modernen Betriebssystemen unterstützt. Dieser Adaptertyp ist auch die Standardeinstellung für Windows Server ab 2003 und ab Windows XP 64 Bit. Unter Linux finden Sie Unterstützung für diesen Adaptertyp ab der Kernel-Version 2.4.19.
- **Flexible**
  Dieser Typ ist, wie der Name schon preisgibt, ein flexibler, der zwischen den Netzwerkadaptertypen »vlance« und »VMXNET« umschalten kann. Während des Bootvorgangs einer VM verhält sich dieser Typ wie der Typ vlance. Sind die VMware Tools im Gastbetriebssystem installiert, schaltet der Adapter auf den VMXNET-Adapter um. Andernfalls bleibt er im Modus des Typs vlance; das bringt zwar optimale Kompatibilität, aber garantierte Performanceeinbußen. Der vlance-Adapter emuliert die doch schon recht betagte 10-MBit-Netzwerkkarte AMD 79C970 PCnet32.
- **VMXNET 2 (Enhanced)**
  Für 32-Bit- und 64-Bit-Windows-Gastbetriebssysteme ab Windows Server 2003 und Windows XP ist dieser Typ eine optimierte Variante des VMXNET-Adapters und steht seit ESX 3.5 (VM-Hardware-Version 4) zur Verfügung. Die VMware Tools werden hierfür zwingend benötigt.

  Dieser Typ erweitert den VMXNET um verschiedene Features wie z. B. die Unterstützung von Jumbo-Frames. Eine Einschränkung bei diesem Typ ist die Kompatibilität der VM beim

Einsatz älterer ESX-Server (vor 3.5) in einem Datacenter. Hierbei können Sie keine VM zwischen einem ESX 3.5- und einem älteren ESX-Host migrieren.

Allerdings wird dieser Typ nicht von allen Betriebssystemen im Gast unterstützt, sondern nur von den folgenden:

- Microsoft Windows 2003 (32 und 64 Bit)
- Microsoft Windows XP, 32 Bit
- Red Hat Enterprise Linux 5.0, 32 und 64 Bit
- SUSE Linux Enterprise Server 10, 32 und 64 Bit
- Red Hat Enterprise Linux 4.0, 64 Bit
- Ubuntu Linux, 64 Bit

- **VMXNET 3**

  Dieser Typ erweitert den Typ VMXNET 2 und stellt VMwares dritte Generation der paravirtualisierten Adapter dar. Er bietet die meisten Netzwerk-Features und höchste Performance, ist aber erst ab der Hardwareversion 7 der virtuellen Maschinen verfügbar. Der Einsatz der VMware Tools ist bei diesem Typ zwingend erforderlich.

  Dieser Typ wird nur von folgenden Betriebssystemen unterstützt:

  - Microsoft Windows XP und später, 32 und 64 Bit
  - Microsoft Windows 2003 und später, 32 und 64 Bit
  - Red Hat Enterprise Linux 5.0 und später, 32 und 64 Bit
  - SUSE Linux Enterprise Server 10 und später, 32 und 64 Bit
  - Asianux 3 und später, 32 und 64 Bit
  - Debian 4/Ubuntu 7.04 und später, 32 und 64 Bit
  - Sun Solaris 10 U4 und später, 32 und 64 Bit

  Zusätzlich zu den in VMXNET 2 neuen Features bringt der VMXNET-3-Adapter Unterstützung für folgende Netzwerk-Features mit:

  - MSI/MSI-X
  - Receive Side Scaling (wird ab Windows 2008 unterstützt und muss explizit aktiviert werden)
  - IPv6-Checksum
  - IPv6 TCP Segmentation Offloading (TSO)
  - VLAN Off-Loading
  - Erhöhung der TX/RX-Ringgrößen (wird in der virtuellen Maschine aktiviert)

Hardware	Maximum
SCSI-Controller	4
Devices pro SCSI-Controller (z. B. Festplatte)	15
Devices insgesamt, unabhängig vom VM-Betriebssystem	60
Größe einer SCSI-Festplatte	2 TByte minus 512 Byte
virtuelle CPUs	32
maximaler Speicher	1 TByte
Netzwerkkarteny	10
IDE-Devices	4
Diskettenlaufwerke	2
parallele Ports	3
serielle Ports	4
Größe der Swap-Datei	1 TByte
Verbindungen via Remote-Konsole	40
USB-Controller	1
verbundene USB-Devices	20
verbundene USB-3.0-Devices	1
Videospeicher (Grafikkarte)	128 MB

Tabelle 15.1 Maximale Ausstattung einer VM

15.1.3 Bestandteile einer virtuellen Maschine

Eine virtuelle Maschine setzt sich aus verschiedenen Dateien zusammen, deren Namen alle den Namen der virtuellen Maschinen besitzen und durch die Endung unterschieden werden:

- **VMX-Datei**
  Diese Datei enthält die Konfiguration der virtuellen Maschine, wie diese z. B. im vSphere-Client über SETTINGS im Kontextmenü einer VM eingerichtet wurde.
- **VMDK-Datei**
  Diese Datei stellt die virtuelle Festplatte dar, und pro virtuelle Festplatte existieren zwei Dateien. Beispiel: Hat eine VM eine Festplatte, so existieren die zwei Dateien *servername.vmdk* und *servername-flat.vmdk*. Dabei enthält die Datei *servername.vmdk* Informationen über die emulierte physische Zusammensetzung sowie den Namen der eigentlichen Datei mit den Festplattendaten, in der Regel die Datei *servername-flat.vmdk*.

  Pro Festplatte einer VM werden diese Dateien erstellt, dabei bekommen alle weiteren virtuellen Festplatten die Namen der VM mit dem Anhang *_durchlaufende Nummer*, z. B. *servername_1.vmdk* und *servername_1-flat.vmdk*.

```
ide1:0.startConnected = "false"
floppy0.startConnected = "false"
floppy0.fileName = ""
floppy0.clientDevice = "true"
ethernet0.present = "true"
ethernet0.virtualDev = "e1000"
ethernet0.networkName = "VM Network"
ethernet0.addressType = "generated"
svga.vramSize = "8388608"
disk.EnableUUID = "true"
guestOS = "windows7srv-64"
uuid.bios = "56 4d f5 f5 8d b2 8c f8-0f 0a e5 97 7a 86 62 2e"
vc.uuid = "52 c5 42 be 74 a0 93 1c-69 99 e7 19 35 46 1b 28"
snapshot.action = "keep"
sched.cpu.min = "0"
sched.cpu.units = "mhz"
sched.cpu.shares = "normal"
sched.mem.min = "0"
sched.mem.shares = "normal"
tools.upgrade.policy = "manual"
replay.supported = "FALSE"
replay.filename = ""
scsi0:0.redo = ""
pciBridge0.pciSlotNumber = "17"
pciBridge4.pciSlotNumber = "21"
pciBridge5.pciSlotNumber = "22"
pciBridge6.pciSlotNumber = "23"
pciBridge7.pciSlotNumber = "24"
scsi0.pciSlotNumber = "160"
ethernet0.pciSlotNumber = "32"
vmci0.pciSlotNumber = "33"
scsi0.sasWWID = "50 05 05 65 8d b2 8c f0"
ethernet0.generatedAddressOffset = "0"
tools.remindInstall = "false"
hostCPUID.0 = "0000000a756e65476c65746e49656e69"
hostCPUID.1 = "000106760004080000ce3bdbfebfbff"
hostCPUID.80000001 = "00000000000000000000000000120100800"
guestCPUID.0 = "0000000a756e65476c65746e49656e69"
guestCPUID.1 = "000106760001080080822010febfbff"
guestCPUID.80000001 = "00000000000000000000000000120100800"
userCPUID.0 = "0000000a756e65476c65746e49656e69"
userCPUID.1 = "000106760004080000822010febfbff"
userCPUID.80000001 = "00000000000000000000000000120100800"
evcCompatibilityMode = "FALSE"
vmotion.checkpointFBSize = "8388608"
unity.wasCapable = "false"
ethernet0.generatedAddress = "00:0c:29:86:62:2e"
vmci0.id = "2055627310"
tools.syncTime = "FALSE"
uuid.location = "56 4d 6f f2 f4 b8 b1 ad-08 f6 74 1b f1 61 94 41"
cleanShutdown = "FALSE"
migrate.hostlog = "./vc5-23199294.hlog"
sched.swap.derivedName = "/vmfs/volumes/4ec6385d-3041dc4d-8ed2-001f290d0809/vc5/vc5-23199294.vswp"
```

Abbildung 15.2 Der Inhalt einer Konfigurationsdatei (»VMX«)

- **VSWP-Datei**
  Diese Datei ist die Swap-Datei pro virtuelle Maschine. Die Größe ist identisch mit der RAM-Größe abzüglich einer etwaig vorhandenen RAM-Reservierung der VM. Dieses Swapfile benötigt der VMkernel, um der virtuellen Maschine die konfigurierte Speichermenge auch dann zur Verfügung zu stellen, wenn der physische Speicher des ESX-Servers dies nicht mehr hergibt.

  Bedenken Sie bei Ihrer Planung der Datastores, dass sich zu den VMDK-Dateien immer diese Dateien hinzugesellen, sobald die VM eingeschaltet wird. Bei virtuellen Maschinen mit sehr großem Speicher wird der Plattenplatz auf einem Datastore sehr schnell knapp. Vergeben Sie eine RAM-Reservierung auf 100 %, wird die Swap-Datei auf eine Größe von 0 verkleinert. Die Swap-Datei hat immer die Größe »zugewiesene Speichergröße – Speicherreservierung«.

- **VMXF-Datei**
  Diese Datei enthält erweiterte Konfigurationsdaten.
- **VMSD-Datei**
  Diese Datei speichert Meta-Informationen über eventuell vorhandene Snapshots einer VM.
- **VMSN-Datei**
  Die Snapshot-Dateien mit den Daten tragen diese Endung
- **NVRAM-Datei**
  Diese Datei enthält die BIOS-/EFI-Einstellungen einer VM.
- **LOG-Dateien**
  Die Dateien mit der Endung *.log* speichern die Protokollierung der VM-Aktivitäten und sind im Fehlerfalle für das Troubleshooting sehr nützlich. Die aktuelle Datei heißt immer *vmware.log*, die älteren Dateien *vmware-n.log*, wobei n eine fortlaufende Nummer ist. Hat die aktuelle Datei die maximale Größe erreicht, so wird sie mit der nächsthöheren Nummer versehen, und eine leere *vmware.log*-Datei wird angelegt.
- **VMSS-Datei**
  Diese Datei wurde bei einer suspendierten VM erstellt und enthält deren eingefrorenen Status.

15.2 Erstellung von virtuellen Maschinen

Virtuelle Maschinen können Sie über verschiedene Wege erstellen:

- über den vSphere-Client mit dem New Virtual Machine-Wizard
- vSphere PowerCLI oder vCLI (PowerShell- und Kommandozeilenbefehle)
- Cloning (erstellt Replikas von bestehenden VMs)
- Deploy OVF Template (importiert eine im OVF-Format gespeicherte VM oder vApp)
- Deploy from Template (VMware-Provisioning-Methode)
- VMware Converter (P2V-Migration von bestehenden physischen Servern)
- weitere Anwendungen wie VMwares Lab Manager oder VMwares Lifecycle Manager

Auf den folgenden Seiten beschreiben wir die Wizard-Methode via vSphere-Client. Mit Hilfe des vSphere-Clients legen Sie eine VM entweder im Virtual Center an oder, wenn Sie auf einem ESXi-Server verbunden sind, direkt auf diesem. Eine VM im vCenter kann unter folgenden Objekten erstellt werden:

- Cluster
- Host
- Virtual Machine Folders

Je nach Verbindungsart (vCenter oder ESXi) und Startobjekt variieren die einzelnen Schritte des Wizards; er fragt nur die für die aktuelle Auswahl notwendigen Informationen ab.

Den New Virtual Machine-Wizard starten Sie beispielsweise, indem Sie das jeweilige Objekt markieren und im Kontextmenü den Befehl New Virtual Machine auswählen.

Im ersten Schritt werden Sie gefragt, ob Sie eine typische (Typical) oder eine angepasste (Custom) Installation einer VM durchführen möchten. Die beiden Wege unterscheiden sich darin, dass der Wizard bei der Auswahl von Typical eine Reihe von standardmäßigen Voreinstellungen annimmt. Des Weiteren wird bei Typical die Hardwareversion der VM basierend auf dem Ziel ESXi-Host ausgewählt; bei Custom können Sie diese verändern. Bei der Auswahl von Custom werden zusätzliche Schritte abgefragt. Hier finden Sie eine Übersicht der beiden Wege:

typische Installation	benutzerdefinierte Installation
Name and Location	Name and Location
Specific Host	Specific Host
Storage	Storage
	Virtual Machine Version
Guest Operating System	Guest Operating System
	CPUs
	Memory
	Network
	SCSI Controller
Create Network Connections	–
Create a Disk	Select a Disk / Create a Disk
	Advanced Options
Ready to Complete	Ready to Complete

Tabelle 15.2 Vergleich der Schritte einer typischen und einer angepassten Installation

Die Schritte zur Erstellung einer virtuellen Maschine im Custom-Modus sind:

1. Nach dem Starten des Wizards und Auswahl von Custom vergeben Sie den Namen der VM und wählen einen Ablageort aus. Dieser Name ist zum einen der Inventarname der VM, zum anderen werden die Dateien, die die VM auf dem Dateisystem des Datastores abbilden, anhand dieses Namens benannt. Die maximale Länge ist 80 Zeichen.
2. Wählen Sie den ESXi-Host aus, auf dem die virtuelle Maschine angelegt werden soll.
3. Legen Sie den Resource-Pool fest, sofern die VM in einem Resource-Pool abgelegt werden soll.
4. Definieren Sie den Datastore, das heißt, auf diesem VMFS-Laufwerk werden die Dateien der VM gespeichert. Zusätzlich können Sie hier ein Speicherprofil auswählen.

5. Hier legen Sie fest, in welcher Hardwareversion die VM angelegt werden soll.
   - Version 7: für alle ESX/ESXi-Server der Version 4.x
   - Version 8: für alle ESXi-Server der Version 5.x
6. Wählen Sie das Gastbetriebssystem aus.
7. Legen Sie die Anzahl der CPU-Sockets und die Anzahl der CPU-Cores pro CPU-Socket fest.
8. Je nach ausgewähltem Gastbetriebssystem schlägt der Wizard einen Memory-Standardwert vor, den Sie aber anpassen können.
9. Legen Sie die Netzwerkverbindungen der virtuellen Maschine fest. Dabei geben Sie an, wie viele virtuelle Netzwerkkarten diese VM erhalten soll, mit welchem Netzwerk diese Netzwerkkarten jeweils verbunden werden sollen und welcher Netzwerkkarten-Typ verwendet werden soll.
10. Der Wizard schlägt den optimalen SCSI-Controller vor. Sie wählen aus folgender Liste aus:
    - BusLogic Parallel
    - LSI Logic Parallel
    - LSI Logic SAS
    - VMware Paravirtual

    Im Wizard ist die Standardeinstellung je nach Gastbetriebssystem bereits vorgewählt.
11. Haben Sie den Controller festgelegt, folgt nun die Auswahl der virtuellen Disk. Hier haben Sie bis zu vier Möglichkeiten:
    - Create a new virtual disk: Der Wizard erstellt eine neue virtuelle Festplatte, und Sie legen im folgenden Schritt die Größe, den Speicherort (im Verzeichnis der VM oder auf einem alternativen Datastore) und die Art der Festplattenbereitstellung fest:
      - Thick Provisioning Lazy Zeroed: Legt die Festplatte in der gewünschten Größe an und schreibt zur Erstellungszeit keinen Inhalt in die Festplattendatei. Dies war in der vSphere-Vorgängerversion die Standardeinstellung.
      - Thick Provisioning Eager Zeroed: Die Festplatte wird in der gewünschten Größe angelegt und mit Nullen beschrieben. Dabei wird auf dem physischen Datenträger der für diese Festplattendatei reservierte Speicherbereich komplett mit Nullen beschrieben. Dieser Schreibvorgang dauert, je nach Festplattengröße, unterschiedliche lange. Diese Option ist für VMware FT eine Grundvoraussetzung.
      - Thin Provision: Die Festplatte wird in einer kleinen Größe angelegt und wächst, je nach Auslastung durch das Gastbetriebssystem, bis zur maximalen Größe an.
    - Use an existing virtual disk: Sie wählen im nächsten Schritt eine virtuelle Disk in Form einer VMDK-Datei aus.
    - Raw Device Mappings: Bestimmen Sie nachfolgend eine LUN im SAN, die von der VM direkt angesprochen wird.

- Do not create disk: Sie überspringen diesen Schritt und weisen eine virtuelle Festplatte später zu.

12. Sie haben die Möglichkeit, die SCSI-Device-ID oder IDE-Device-ID zu verändern oder den Independent-Disk-Mode zu aktivieren:

    Die Optionen Persistent und Non-persistent legen fest, ob Änderungen an der virtuellen Festplatte unwiderruflich in die Festplatte geschrieben werden oder bei einem Power-off der VM wieder verworfen werden. Beim Einsatz des Independent-Disk-Modes sind keine Snapshots für diese Festplatte möglich.

13. Der letzte Schritt im Wizard zeigt eine Zusammenfassung aller gewählten Optionen an und bietet nochmals die Gelegenheit, verschiedene Einstellungen zu ändern oder weitere Optionen einzustellen. Hierbei wird die virtuelle Maschine im Bearbeitungsmodus angezeigt.

15.2.1 Netzwerkkonfiguration

Während des Anlegens der VM können Sie im Wizard eine bis mehrere Netzwerkkarten der VM hinzufügen. Nachträglich können die bestehenden Netzwerkkarten im ausgeschalteten Zustand der VM verändert oder gelöscht sowie neue hinzugefügt werden.

Beim Anlegen einer Netzwerkkarte geben Sie den Typ an und wählen die auf dem ESX-Server konfigurierte Portgruppe aus. Die zur Verfügung stehenden Netzwerktypen sind abhängig von der Version der VM (diese wiederum richtet sich danach, auf welchem ESX-Host die VM erstellt oder aktualisiert wurde) und dem Gastbetriebssystem.

Die Auswahl des Adaptertyps steht nur beim Hinzufügen einer Netzwerkkarte zur Verfügung. Wenn eine VM bereits angelegt und die Auswahl des Gastbetriebssystems unter Options • General Options • Guest Operating Systems geändert wurde, lässt sich der Typ eines bestehenden Netzwerkadapters nicht ändern. Die für das neu ausgewählte Gastbetriebssystem verfügbaren Netzwerkkarten werden nur beim Hinzufügen neuer Netzwerkadapter als Option angeboten.

Bei der automatischen Vergabe der MAC-Adresse stellt VMware sicher, dass diese Adresse auf den ESX-Servern bislang noch nicht verwendet wurde, und garantiert dadurch eine Eindeutigkeit. Bei der manuellen Vergabe müssen Sie selbst dafür sorgen.

15.2.2 Festplattenkonfiguration

In diesem Abschnitt erhalten Sie weitere Informationen über die verschiedenen Modi einer virtuellen Festplatte, das RDM (Raw Device Mapping) sowie das SCSI-Bus-Sharing.

Independent – Non-independent

Der Virtual-Disk-Mode non-independent ist der standardmäßig eingestellte Modus einer Virtual Disk. In diesem Modus verhält sich eine virtuelle Festplatte einer VM genauso, wie es

eine physische Festplatte täte – er verwaltet sämtliche Schreibzugriffe auf die Festplatte durch das Gastbetriebssystem.

Der Independent Mode verhindert, dass für diese Festplatte ein Snapshot erstellt werden kann, und bietet wiederum zwei verschiedene Optionen an:

- **Persistent Mode**
  Im Persistent Mode werden alle Daten direkt auf die Festplatte geschrieben, das heißt, die Festplatte funktioniert im Endeffekt ganz normal.
- **Non-persistent Mode**
  Der Non-persistent Mode ist das genaue Gegenteil des Persistent Modes, es werden nämlich keine Änderungen der virtuellen Festplatte zurückgeschrieben. Alle Änderungen, die in REDO-Log-Dateien geschrieben werden, gehen beim Ausschalten oder Reset der virtuellen Maschine unwiederbringlich verloren. Diese Option wäre beispielsweise sinnvoll für Kiosk-PCs oder auch PCs in einer Hotel-Lobby, wo nach der Abmeldung sämtliche Änderungen im Gast-Datensatz wieder verworfen werden.

RAW Device Mapping

Unter VMware ESXi ist es möglich, eine physische Festplatte direkt der virtuellen Maschine zuzuordnen. Aber diese physische Festplatte muss zwingend eine LUN aus dem SAN oder eine Festplatte an einem ausschließlich für den VMkernel genutzten SCSI-Adapter sein. Dabei wird immer die komplette Festplatte beansprucht, was eine Formatierung im VMFS von vornherein ausschließt. Allerdings muss der Festplatten-Controller über eine eindeutige SCSI-Serial verfügen, damit Sie die angeschlossenen Festplatten mittels RDM nutzen können. RDM ist weiterhin für die Verwendung der NPIV-Fibre-Channel-Virtualisierung notwendig.

Um eine solche Festplatte anzulegen, wählen Sie beim Hinzufügen einer virtuellen Festplatte den Punkt Raw Device Mappings aus. Dabei wird im Heimatverzeichnis der VM auf einem Datastore eine Zuordnungsdatei (RDM File) erstellt, die statt des direkten Zugriffes genutzt wird und sich auch als VMDK-Datei zeigt. Werden VMs mit RDM geclont, werden die RDM-Festplatten automatisch im Heimatverzeichnis der virtuellen Maschine in Form virtueller Festplatten erstellt. Diese Information ist besonders zu beachten, da keine Warnung über den freien Festplattenplatz eines Datastores erscheint. Bei einem Clone einer VM mit 1 TB RDM würde eine Festplattendatei von 1 TB auf dem Datastore der VM angelegt!

Bei der Auswahl des Kompatibilitätsmodus Physical kann das Gastbetriebssystem direkt auf die SAN-LUN zugreifen, was z. B. für SAN-aware-Anwendungen sinnvoll ist.

Nachteilig ist, dass eine VM mit RDM (Raw Device Mapping) im Physical-Modus nicht geclont werden und auf Basis dieser VM kein Template erstellt werden kann. Außerdem werden für diesen Festplattenmodus keine Snapshots unterstützt.

Nur wenn Sie beim Anlegen dieser Festplattenzuordnung unter dem Punkt Compatibility Mode die Option Virtual auswählen, stehen Ihnen alle erweiterten Festplattenmodi wie

Persistent oder Non-persistent (im Modus Independent) zur Verfügung. Auch besteht in diesem Modus die Möglichkeit, von VMware-Snapshots Gebrauch zu machen. Eine Disk in diesem Modus kann geklont werden; dabei wird der Inhalt der LUN in eine VMDK-Datei kopiert.

Gerade im Umfeld des VMware ESX Servers gibt es Server-Installationen, in denen physische Festplatten ihren Nutzen voll entfalten: die Cluster-Systeme, genauer gesagt Cluster zwischen virtuellen und physischen Systemen oder auch Cluster zwischen virtuellen und virtuellen Systemen, die ohne RDM-Festplatten nicht realisierbar wären.

SCSI-Bus-Sharing

Das SCSI-Bus-Sharing ermöglicht das gleichzeitige Verwenden der virtuellen Festplatten durch mehrere virtuelle Maschinen. Dies wird z. B. beim Einsatz von Microsoft-Clustern in virtuellen Maschinen für die gemeinsam genutzte Festplatte wie die Quorum-Disk benötigt.

Die Einstellung ist eine Konfiguration des SCSI-Controllers und muss vom jeweiligen Host unterstützt werden. Folgende Optionen stehen zur Auswahl:

- None
  Die virtuellen Festplatten an diesem SCSI-Controller können nicht mit anderen VMs gemeinsam verwendet werden.
- Virtual
  Die virtuellen Festplatten an diesem SCSI-Controller können von anderen VMs mitverwendet werden, sofern diese auf dem gleichen ESX-Server liegen.
- Physical
  Die virtuellen Festplatten an diesem SCSI-Controller können von anderen VMs mitverwendet werden, auch wenn diese auf anderen ESX-Servern liegen.

15.2.3 Aktualisieren der virtuellen Hardware

Wenn Sie nicht auf der grünen Wiese mit einer vSphere-Implementierung starten, so haben Sie in Ihrer aktuellen Umgebung bereits virtuelle Maschinen im Einsatz, die beispielsweise mit der Hardwareversion 7 ausgestattet sind. vSphere 5 bringt die Hardwareversion 8 mit, und VMwares Empfehlung an dieser Stelle ist, die aktuelle Hardwareversion zu verwenden.

Das Aktualisieren der VM-Hardware geschieht über den Befehl Upgrade Virtual Hardware, beispielsweise über das Kontextmenü einer VM.

Laut VMware-Empfehlung sollten Sie allerdings vor dem VMware-Hardware-Upgrade erst die VMware Tools aktualisieren. Der Vorgang benötigt unter Windows mehrere Neustarts der VM und geht insgesamt so vonstatten:

1. Update der VMware Tools
2. Reboot

3. Herunterfahren der VM
4. Upgrade der VM-Hardware
5. Start der VM
6. Erkennung der neuen Hardware durch Windows
7. Reboot

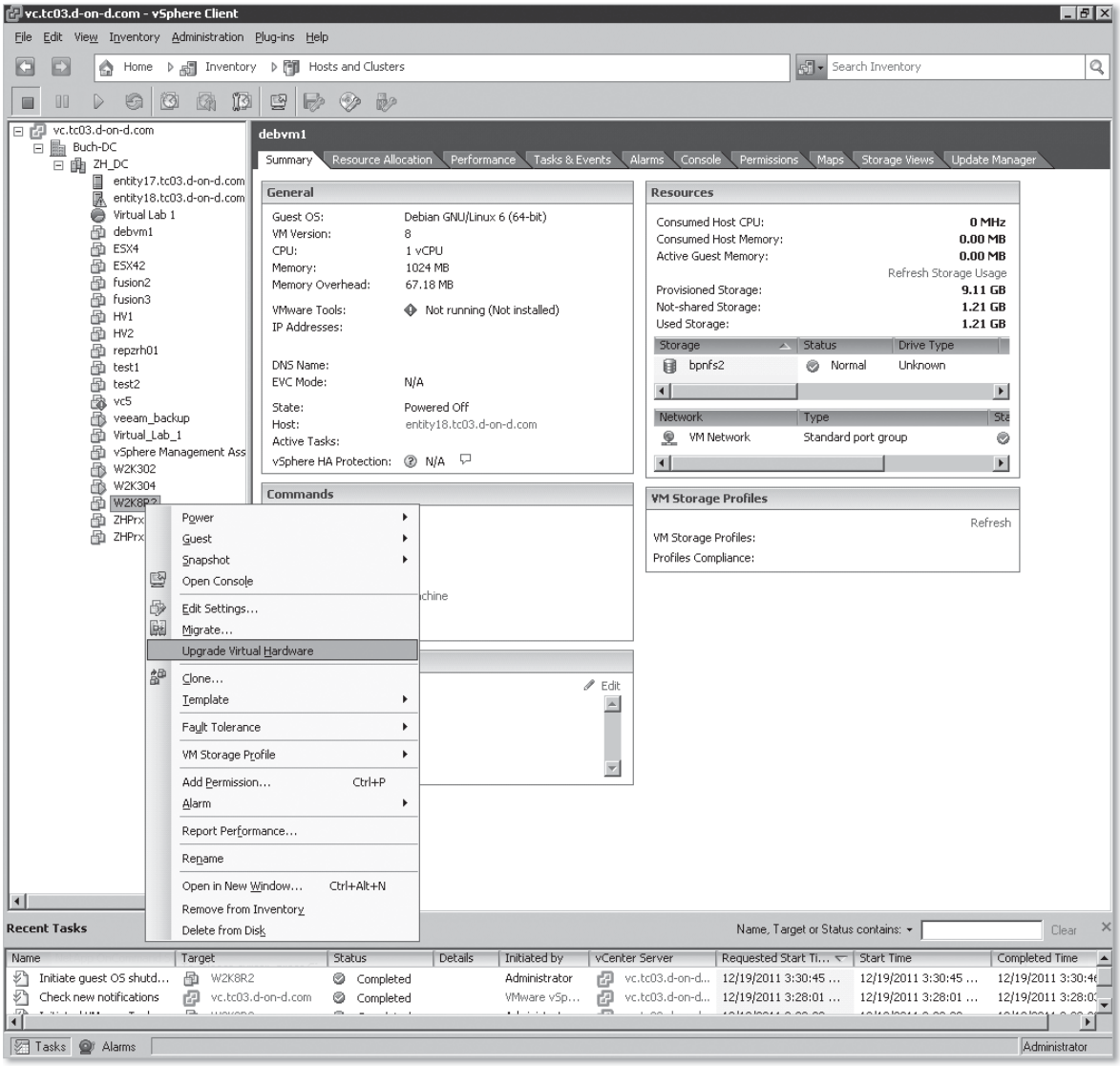


Abbildung 15.3 Upgrade der VM-Hardware

Unter Linux ist der Vorgang identisch, nur dass lediglich für den Hardware-Upgrade ein Reboot beziehungsweise ein Herunterfahren notwendig ist. Nach dem Upgrade haben Sie eine VM mit aktueller virtueller Hardware. Jetzt können Sie auch die neuen VM-Features einsetzen.

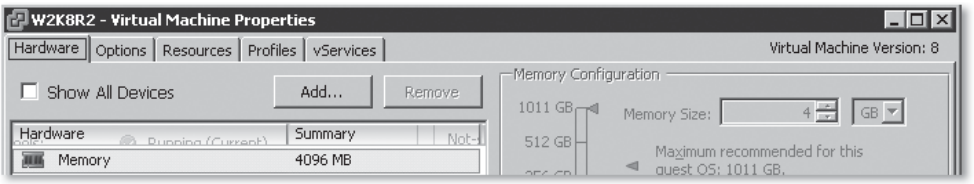


Abbildung 15.4 Die VM wurde auf die aktuelle Version aktualisiert.

15.3 vSphere DirectPath I/O

Mit Hilfe von vSphere DirectPath I/O können Gastbetriebssysteme direkt auf Hardware im ESXi-Host zugreifen, sofern die Hardware des Hosts dafür freigegeben wurden. Sollten Sie z. B. mit Ihrer VM intensiven Netzwerkverkehr bewältigen wollen, so können Sie an der Virtualisierungsschicht vorbei auf Netzwerkkarten im ESXi-Host zugreifen und diese in der virtuellen Maschine als virtuelle Hardware verwenden. Dabei wird in Verbindung mit der Cisco Unified Computing System (UCS) Platform auch vMotion dieser virtuellen Maschine unterstützt. Zu beachten ist, dass ein PCI-Gerät im ESXi-Server als Passthrough-Gerät freigeschaltet werden muss und dann nicht mehr für den VMkernel zur Verfügung steht, also nicht mehr vom ESXi-Server selbst genutzt werden kann.

In Abbildung 15.5 sehen Sie die Schritte, um einen USB-Controller eines ESXi-Hosts in die VM durchzureichen. Im ersten Schritt geben Sie das passende PCI-Gerät, hier einen Intel-ICH10-USB-Controller, des ESXi-Hosts zur Weitergabe an die virtuellen Maschinen freiwerden. Wählen Sie hierzu im vSphere-Client den ESXi-Host aus, klicken Sie im Tab Configuration auf Advanced Settings und dann auf Configure Passthrough. Sie erhalten dann eine Übersicht über die Hardware des ESXi-Hosts und wählen das PCI-Gerät aus.

Nachdem Sie den Passthrough des PCI-Geräts aktiviert haben, starten Sie den Add Hardware-Wizard Ihrer virtuellen Maschine und wählen Add PCI-Device aus. Im nächsten Schritt in Abbildung 15.6 wählen Sie das gewünschte PCI-Gerät, in unserem Fall den USB-Controller, aus.

Ihr Gastbetriebssystem erkennt die neue Hardware, installiert die notwendigen Treiber und zeigt diese dann wie in Abbildung 15.7 in der Hardware-Übersicht an.

Weiterführende Informationen über ESXi und Passthrough-Devices finden Sie in Kapitel 12, »Konfiguration von ESXi und vCenter«.

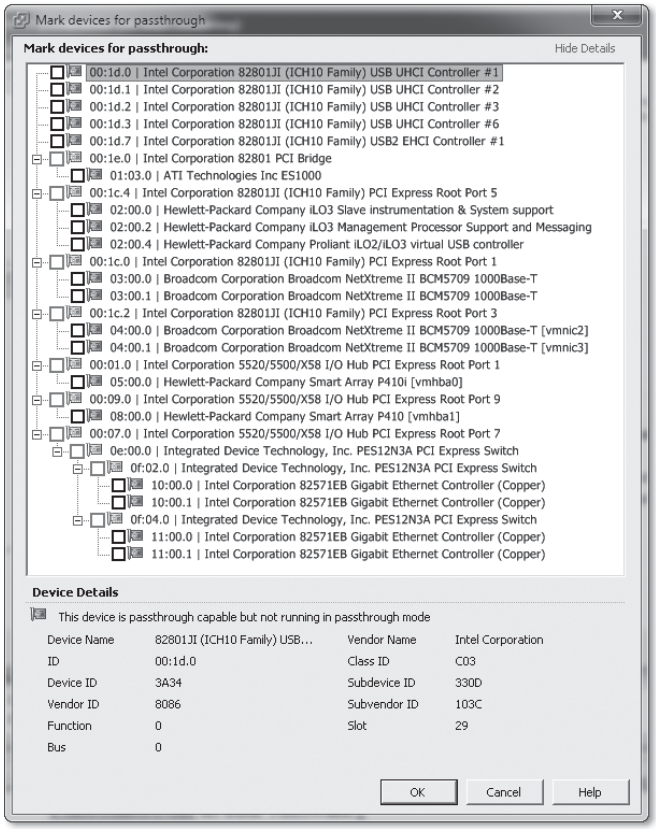


Abbildung 15.5 Wählen Sie die Hardware des ESXi-Hosts aus, die Sie an virtuelle Maschinen durchreichen möchten.

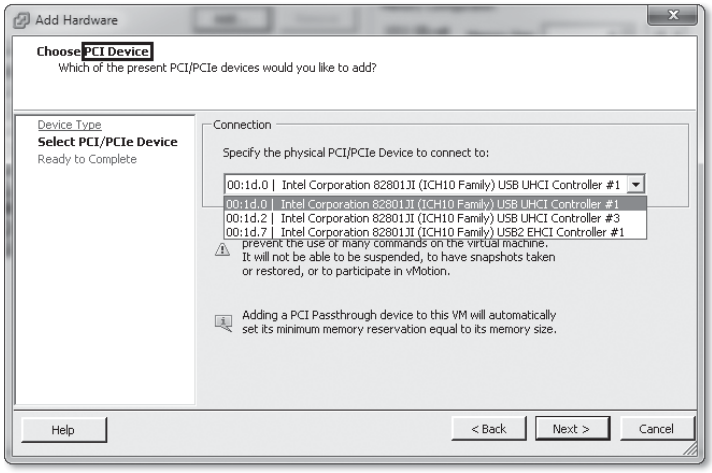


Abbildung 15.6 Wählen Sie ein PCI-Device des ESXi-Hosts zur Verwendung in der VM aus.

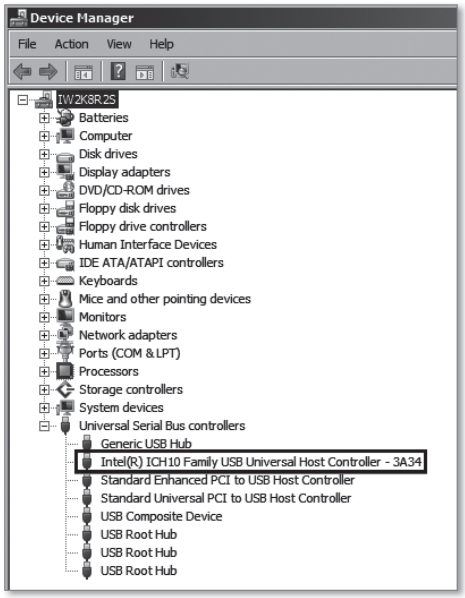


Abbildung 15.7 Das PCI-Device des ESXi-Hosts, hier der USB-Controller, ist jetzt in der virtuellen Maschine einsatzbereit.

15.4 Eigenschaften einer virtuellen Maschine – Optionen

Für jede virtuelle Maschine können Sie individuell weitere Einstellungen treffen. Diese umfassen im Groben:

- Anzeige des Namens und des Ablageorts der VM, Möglichkeit zur Änderung des Namens
- Änderung der Auswahl des Gastbetriebssystems
- vApp-Optionen
- Verhalten der VM bei Power-Aktivitäten (Einschalten, Ausschalten, Reset, Suspend)
- VMware-Tools-bezogene Einstellungen wie das Aktivieren von VMware-Tools-Skripten, Überprüfung der Version und gegebenenfalls Aktualisierung dieser beim Einschalten der VM oder Zeitsynchronisation mit der VM
- Verhalten der VM bei Betriebssystem-Standby
- erweiterte Einstellungen wie z. B. Logging, Debug-Modus, vMotion-Kompatibilität, Bootverhalten, Aktivierung der VMI-Paravirtualisierung, Zuweisung von Fibre-Channel-WWNs, Optionen zur Virtualisierung der MMU (Memory Management Unit) und Auswahl des Speicherorts der Swap-Datei

15.4.1 Änderung des Namens der VM

In den Eigenschaften einer VM im Reiter Optionen haben Sie im Abschnitt General Options die Möglichkeit, den Namen der VM zu ändern. Diese Änderung wirkt sich aber nicht auf das VMFS aus, auf dem die Dateien dieser VM liegen, das heißt, der Verzeichnisname, in dem sich die VM befindet, und die Namen aller Dateien werden nicht geändert. Die Änderung kann nur bei ausgeschalter VM durchgeführt werden. Ebenso finden Sie an gleicher Stelle den kompletten Pfad des Ablageorts der VM-Dateien.

15.4.2 Änderung des Gastbetriebssystems

In den Eigenschaften einer VM im Reiter Optionen können Sie im Abschnitt General Options das konfigurierte Gastbetriebssystem ändern. Die VM muss dabei ausgeschaltet sein. Eine Änderung an dieser Stelle wirkt sich nicht auf das Gastbetriebssystem direkt aus, es wird lediglich die Konfigurationseinstellung in der VMX-Datei geändert. Auf dieser Konfigurationseinstellung jedoch beruhen sämtliche Empfehlungen zur Hardwareausstattung einer virtuellen Maschine. Bereits eingerichtete virtuelle Hardware, die durch das Anlegen der VM durch z. B. den Wizard definiert wurde, ändert sich nicht nachträglich. Je nach getroffener Auswahl wird auch die Art des VMware-Tools-Setups geändert, um es an die Rahmenbedingungen des Betriebssystems anzupassen. Diese Option zum Ändern des Gastbetriebssystems ist sinnvoll, wenn das Gastbetriebssystem einer VM durch ein Upgrade aktualisiert wird, z. B. Windows Server 2003 auf Windows Server 2008.

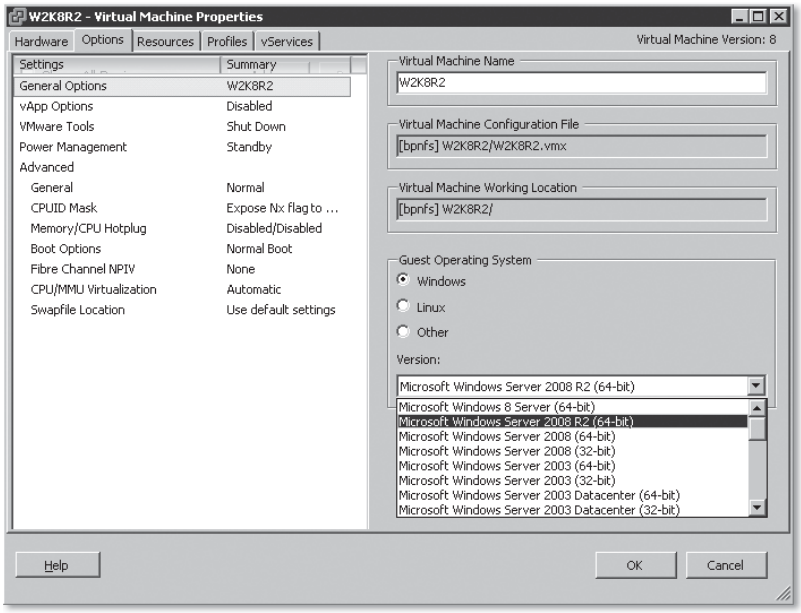


Abbildung 15.8 Unter »Options« sehen Sie den Ablageort der Dateien der virtuellen Maschine ein, können den Namen der VM im vCenter-Inventory und das Gastbetriebssystem ändern.

15.4.3 Erweiterung der Power-Aktivitäten durch die VMware Tools

Nach der Installation der VMware Tools im Gastbetriebssystem bieten die »Power«-Buttons weitere Optionen zum Verhalten der VM respektive deren Betriebssystems. Diese Einstellung können Sie im auch im eingeschalteten Zustand einer VM vornehmen; Sie finden sie unter VMware Tools.

- **»Power Off«-Schalter**
  Diesen Schalter können Sie anstelle seiner standardmäßigen Funktion zum »harten« Ausschalten einer VM (Hard Power-off) auch zum geregelten Herunterfahren des Gastbetriebssystems und anschließendem Ausschalten umkonfigurieren (Soft Power-off). Des Weiteren ist auch die systemweite Standardeinstellung möglich. Wie diese aktuell konfiguriert ist, wird bei der Auswahl angezeigt.
- **Reset-Schalter**
  Diesen Schalter können Sie anstelle seiner standardmäßigen Funktion zum »harten« Ausschalten einer VM (Hard Reset) und anschließenden Neustart der VM auch zum geregelten Herunterfahren des Gastbetriebssystems und anschließenden Neustart dieser umkonfigurieren (Soft Reset). Auch die systemweite Standardeinstellung ist möglich. Wie diese aktuell konfiguriert ist, wird bei der Auswahl angezeigt.

Der Power On-Schalter zum Einschalten oder Reaktivieren (Resume) einer VM lässt sich nicht umkonfigurieren.

15.4.4 Automatische Ausführung der VMware-Tools-Skripte

Die VMware Tools können im Gastbetriebssystem je nach Power-Aktivität Skripte ausführen, um z. B. Datenbankdienste zu stoppen oder zu starten.

Die möglichen Skripte sind:

- Nach dem Einschalten einer VM (Power On-Schalter einer ausgeschalteten VM) wird das Skript *poweron-vm-default* ausgeführt.
- Nach dem Reaktivieren (Fortsetzen) aus dem Suspend-Modus (Power On-Schalter bei suspendierter VM) wird das Skript *resume-vm-default* ausgeführt.
- Vor dem Suspendieren (Anhalten) einer VM (Pause-Schalter bei eingeschalteter VM) wird das Skript *suspend-vm-default* ausgeführt. Unter einem Windows-Gast wird eine per DHCP vergebene IP-Adresse der VM freigegeben, und unter Linux werden die Netzwerkdienste gestoppt.
- Vor dem Herunterfahren einer VM (Power Off-Schalter bei eingeschalter VM) wird das Skript *poweroff-vm-default* ausgeführt.

Die standardmäßig aktivierten und vorhandenen Skripte liegen innerhalb der virtuellen Maschine bei einem Windows-Betriebssystem im Verzeichnis *%ProgramFiles%\VMware\VMware Tools* und bei einem Linux-Betriebssystem im Verzeichnis */etc/vmware-tools*.

Möchten Sie hingegen eigene Skripte verwenden, so hinterlegen Sie diese in der virtuellen Maschine und definieren den Pfad in der Konfiguration der VMware Tools im Reiter Scripts.

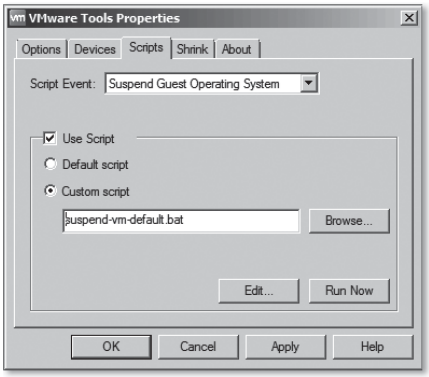


Abbildung 15.9 Anstelle der Defaultskripte können Sie in der VM eigene Skripte verwenden.

Die Konfiguration nehmen Sie im Reiter Options der VM-Eigenschaften im Bereich VMware Tools vor.

15.4.5 Automatische Aktualisierung der VMware Tools

Bei jedem Einschalten einer VM können Sie überprüfen lassen, ob die neueste Version der VMware Tools im Gastbetriebssystem installiert ist, und diese bei Bedarf installieren. Beachten Sie dabei, dass bei der Verwendung von Windows-VMs ein Neustart nach Aktualisierung der VMware Tools durchgeführt und bei Linux-VMs die Netzwerkverbindung kurz unterbrochen wird. Sie aktivieren dieses Feature im Reiter Options der VM-Eigenschaften, Bereich VMware Tools.

15.4.6 Zeitsynchronisation der VM mit dem ESX-Server

Das Feature Zeitsynchronisation übermittelt dem Gastbetriebssystem durch die VMware Tools die jeweilige Zeit vom ESX-Server. Diese Kommunikation findet direkt über den VMkernel statt, der dem Gastsystem die Uhrzeit zur Verfügung stellt, das heißt, es muss keine Netzwerkverbindung zwischen dem Host-System und der virtuellen Maschine bestehen. Sie aktivieren die Zeitsynchronisation durch VMware im Reiter Options der VM-Eigenschaften unter VMware Tools.

Beachten Sie dabei, dass die VMware Tools im Abstand von 60 Sekunden die neue Uhrzeit übernehmen. Außerdem wird die Uhrzeit nur vor- und nicht zurückgestellt, da es im Normalfall bei virtuellen Maschinen nur zu einer verlangsamten Zeitberechnung kommt. Eine Ausnahme besteht bei der Nutzung mancher Linux-Systeme, deren Kernel-Konfiguration zu einer beschleunigten Zeitberechnung führt. In diesem Fall müssen Sie einen Kernel-Parameter (Grub Boot Parameter clock = pit) anpassen.

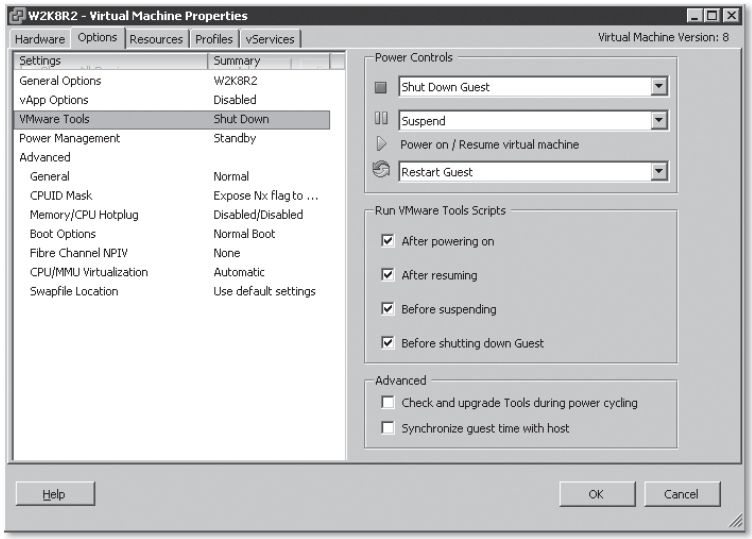


Abbildung 15.10 Einstellung der Power-Aktivitäten, VMware-Tools-Aktualisierung und Zeitsynchronisation der virtuellen Maschine

15.4.7 Power-Management des Gastbetriebssystems

Durch die POWER MANAGEMENT-Einstellungen lässt sich das Verhalten einer VM durch einen Standby-Modus des Gastbetriebssystems ändern. Die Standardeinstellung weist eine VM an, in den SUSPEND-Modus zu gehen. Alternativ ändern Sie dies abhängig vom Gastbetriebssystem, so dass die VM im normalen Power-on-Status bleibt, aber das Gastbetriebssystem in den Standby-Modus geht. Diese Einstellung nehmen Sie im Bereich POWER MANAGEMENT vor.

15.4.8 Erweiterte Konfiguration: Logging, Debugging, Acceleration und erweiterte Konfigurationsparameter

Standardmäßig ist das Protokollieren aller VM-Aktivitäten aktiv; deaktivieren Sie es bei Bedarf, z. B. bei Ressourcenproblemen. Diese Änderung ist auch im eingeschalteten Zustand einer VM möglich. Die Protokolldateien finden Sie auf dem VMFS-Volume im jeweiligen Ordner der VM (diesen können Sie im ersten Abschnitt des Reiters OPTIONS einsehen), sie tragen die Endung *.log*.

In Ausnahmefällen wird der VMware-Support Sie anweisen, eine VM mit zusätzlichen Debug-Features zu betreiben. Dabei werden zur Fehleranalyse erweiterte Informationen zur Laufzeit einer VM in eine Datei geschrieben. Je nach Gastbetriebssystem stehen Ihnen neben den Debug-Informationen auch Statistiken zur Verfügung. Dieses Feature lässt sich nur bei ausgeschalteter VM aktivieren.

Um die maximale Geschwindigkeit im Betriebssystem einer VM zu erhalten, ist die Beschleunigung (Acceleration) einer VM grundsätzlich aktiv. In bestimmten Fällen behindert dies die

Installation oder Ausführung einer Applikation und kann deaktiviert werden. Meistens finden Sie hierzu die Information im VMware-Forum, oder Sie erhalten sie direkt vom VMware-Support.

In seltenen Fällen wird Sie der VMware-Support bei Problemen mit bestimmten Applikationen in einer VM anweisen, entweder bestehende erweiterte Konfigurationsparameter zu ändern oder neue hinzuzufügen. Gehen Sie hier mit größter Vorsicht vor, da neu erstellte Einträge nicht mehr gelöscht werden können, und das Entfernen des Values des Key-Value-Paares kann bei bestimmten Parametern eine VM nicht mehr startbar hinterlassen. In solch einem Fall müssen Sie die VM-Einstellungen dokumentieren, eine neue VM mit der Option, eine vorhandene Disk als virtuelle Festplatte (oder mehrere) zu nutzen, erstellen und nach dem Kopieren aller VMDK-Dateien aus dem Speicherplatz der zerstörten VM in das Verzeichnis der neuen VM die VMDK-Dateien in die VM einbinden.

Alle genannten Einstellungen nehmen Sie im Reiter Options in den Eigenschaften einer VM im Abschnitt Advanced • General vor.

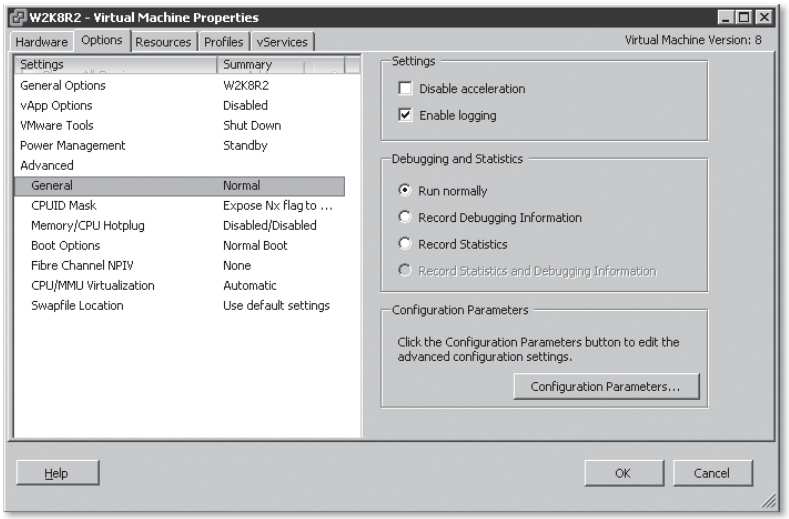


Abbildung 15.11 Einstellungen zu Logging, Acceleration und den erweiterten Konfigurationsparametern

15.4.9 Erweiterte Konfiguration: CPU Identification Mask

Die CPU Identification Mask unterstützt die Kompatibilität von unterschiedlichen CPUs der ESX-Server bei vMotion-Operationen. Diese Einstellungen können nur bei ausgeschalteter VM vorgenommen werden und verstecken in erster Linie das Nx-Flag der CPU vor den Augen des Gastbetriebssystems, damit die VM auf einen ESX-Host ohne das CPU-Nx-Flag live migriert werden kann.

Diese Einstellung ist auf der Basis einzelner virtueller Maschinen zu treffen und ist im Vergleich zum Feature EVC (Enhanced vMotion Compatibility) eher die angestaubte Variante.

EVC wird auf Basis des Clusters aktiviert, erstellt die CPU-Gleichheit direkt auf den ESX-Servern und stellt so die CPU-Kompatibilität für vMotion-Operationen sicher. Weitere Informationen zu EVC finden Sie in Kapitel 5, »Cluster«.

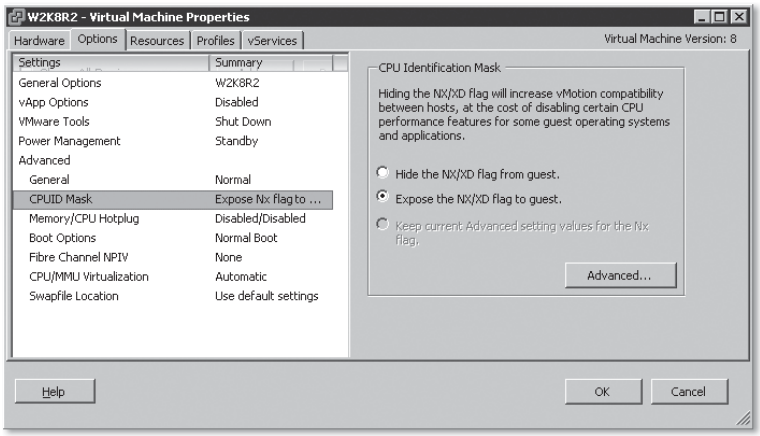


Abbildung 15.12 CPU-Kompatibilitätseinstellungen

15.4.10 Erweiterte Konfiguration: Memory/CPU Hot Plug

Das Hinzufügen von weiteren CPUs oder Memory einer eingeschalteten virtuellen Maschine steuern Sie pro VM. Schauen Sie vor der Verwendung dieser Möglichkeiten in der VMware-Dokumentation *GuestOS_guide.pdf* nach, ob das eingesetzte Gastbetriebssystem dies unterstützt!

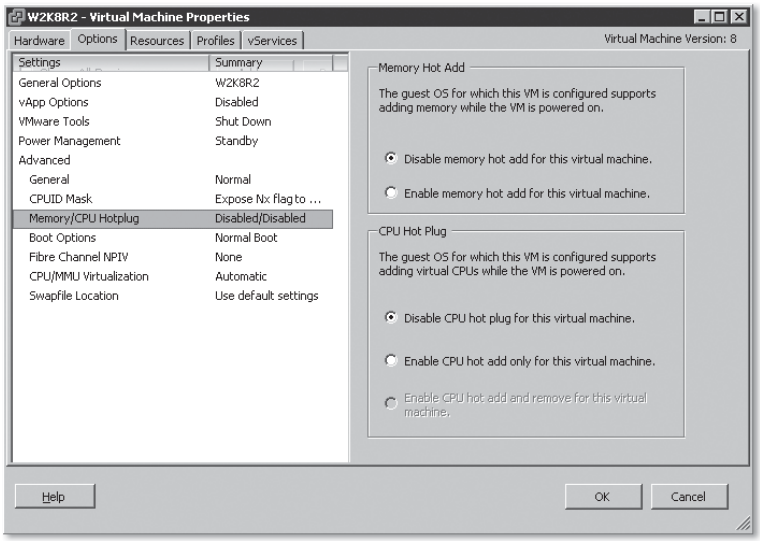


Abbildung 15.13 Einstellungen der Hot-Add- und Hot-Plug-Features

15.4.11 Erweiterte Konfiguration: Boot Options

In den Boot Options (siehe Abbildung 15.14) definieren Sie die von der virtuellen Hardware eingesetzte Firmware oder beeinflussen das Startverhalten der VM dahingehend, dass direkt in das BIOS der VM gelangen.

Die erste Einstellung legt die Firmware der virtuellen Maschine fest. Dieses Feature ist neu in vSphere 5, und die gängige Einstellung ist BIOS. Mit der Einstellung EFI können Sie das BIOS gegen UEFI (Unified Extended Firmware Interface) austauschen – der Nachfolger des BIOS. UEFI brauchen Sie z. B., wenn Sie Max OS X als Gastbetriebssystem betreiben wollen. Die Optionen sind je nach gewähltem Gastbetriebssystem selektierbar, und bei Mac OS X ist EFI bereits vorausgewählt. Die Einstellung Power-On Boot Delay verzögert den Start der VM nach Klick auf den Power on-Button. Damit bleibt Ihnen ausreichend Zeit, um in die VMware Console zu wechseln und dort via Esc, F2 oder F12 mit dem BIOS der VM zu interagieren. Bitte beachten Sie, dass die Zeit hier in Millisekunden angegeben wird, und daher sind Werte ab 2.000 sinnvoll.

Die Bootoption Force BIOS Setup respektive Force EFI Setup startet beim nächsten Einschalten einer VM sofort das BIOS-/EFI-Setup. Diese Einstellung gilt nur einmalig für den nächsten Startvorgang. Die ab vSphere 5 ebenfalls neue Einstellung Failed Boot Recovery startet automatisch die VM neu, sobald die konfigurierte Boot-Festplatte nicht gefunden wurde. Die Bootoptionen stellen Sie in den Eigenschaften der VM im Reiter Options in der Rubrik Advanced • Boot Options ein.

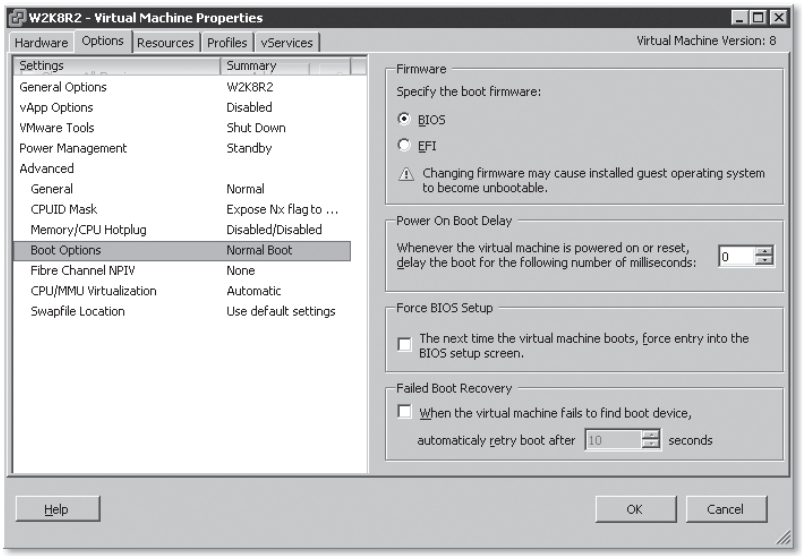


Abbildung 15.14 Einstellungen zur Firmware und zum Boot-Verhalten

15.4.12 Erweiterte Konfiguration: Fibre Channel NPIV

Bei der direkten Verwendung von FC-HBAs durch virtuelle Maschinen, die NPIV (N-Port-ID-Virtualisierung) beherrschen, greift eine VM mit einem eindeutigen WWN (World Wide Name) direkt auf die Hardware zu. NPIV ermöglicht die Zuweisung mehrerer WWNs auf einen Fibre-Channel-HBA. Wie der Name bereits vermuten lässt, teilen sich hierbei mehrere N_PORTs einen physischen N_PORT. Die Fibre-Channel-Switches sowie die im ESXi-Server verwendeten FC-HBAs müssen diese Technik unterstützen. Beim Einschalten der betreffenden virtuellen Maschine erstellt der ESXi-Server einen virtuellen Port (VPORT) auf dem FC-HBA, der dann für den Datenaustausch zwischen der virtuellen Maschine und der RDM dient.

Bei der Erstellung der LUNs, die von diesen virtuellen Maschinen verwendet werden, ist zu beachten, dass die LUNs mit den WWNs der virtuellen Maschine sowie denen der ESX-Server maskieren müssen. Die neuen WWNs erstellen Sie bei ausgeschalter VM in deren Eigenschaften im Reiter Options im Abschnitt Fibre Channel NPIV. Deaktivieren Sie dort die Checkbox Temporarily Disable NPIV for this virtual machine ❶, und generieren Sie die WWNs durch Klick auf Generate new WWNs ❷.

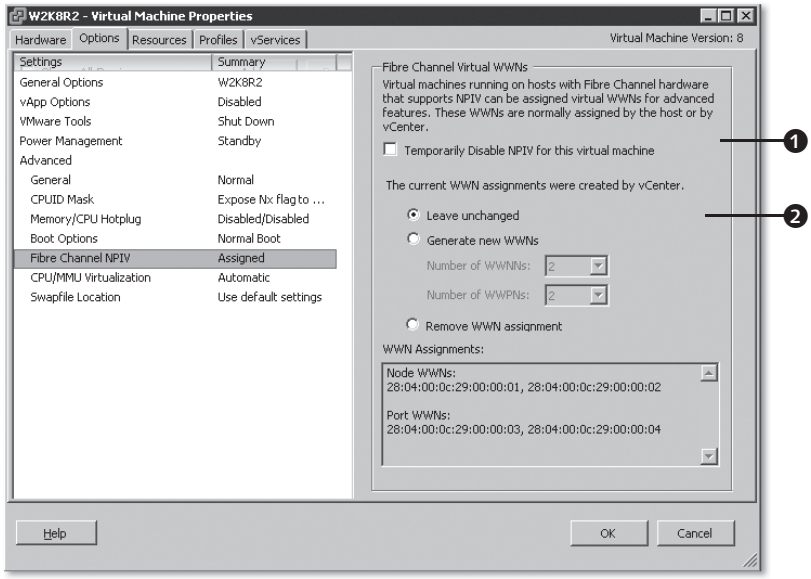


Abbildung 15.15 Aktivierung der NPIV einer virtuellen Maschine

15.4.13 Erweiterte Konfiguration: CPU/MMU Virtualization

Vor der Einführung von hardwarebasierter Virtualisierungsunterstützung in den CPUs erreichte der Virtual Machine Monitor (VMM) eines ESXi-Servers die CPU-Virtualisierung nur mit Hilfe von Software. Dabei wurde die Binary Translation (BT) zur Virtualisierung des Instruction-Sets einer CPU verwendet, und Shadow Page Tables dienten zur Virtualisierung der Memory Management Units.

Die erste hardwarebasierte Unterstützung seitens der Hersteller kam mit Intel VT-x und AMD-V. Der nächste Schritt wurde durch Intel EPT und AMD RVI eingeläutet, um die hardwarebasierte MMU-Virtualisierung zu ermöglichen. Mit dieser Einstellung steuern Sie auf Ebene von einzelnen VMs die von der Hardware angebotene CPU-Virtualisierungsunterstützung. Folgende Optionen stehen hierbei zu Verfügung:

- Automatic
  Dieser Modus erkennt, welche Features die CPU-Hardware konkret unterstützt, und aktiviert die Verwendung der Hardwareunterstützung für die Virtualisierung des Instruction-Sets oder der Memory Management Units.
- Use software for instruction set and MMU virtualization
  Der VMM verwendet zur CPU-Virtualisierung für diese virtuelle Maschine nur die native softwarebasierte Virtualisierung.
- Use Intel VT-x/AMD-V for instruction set virtualization and software for MMU virtualization
  Der VMM verwendet nur die von Intel VT-x oder AMD-V angebotene Unterstützung zur Virtualisierung des Instruction-Sets. Die MMUs werden weiterhin durch VMwares Software virtualisiert.
- Use Intel VT-x/AMD-V for instruction set virtualization and Intel EPT/AMD RVI for MMU virtualization
  Der VMM verwendet nur die von Intel VT-x oder AMD-V angebotene Unterstützung zur Virtualisierung des Instruction-Sets und die Intel-EPT-/AMD-RVI-Unterstützung der MMU-Virtualisierung.

Die Konfiguration nehmen Sie in den Eigenschaften der VM im Reiter Options unter Advanced • Virtualized MMU vor.

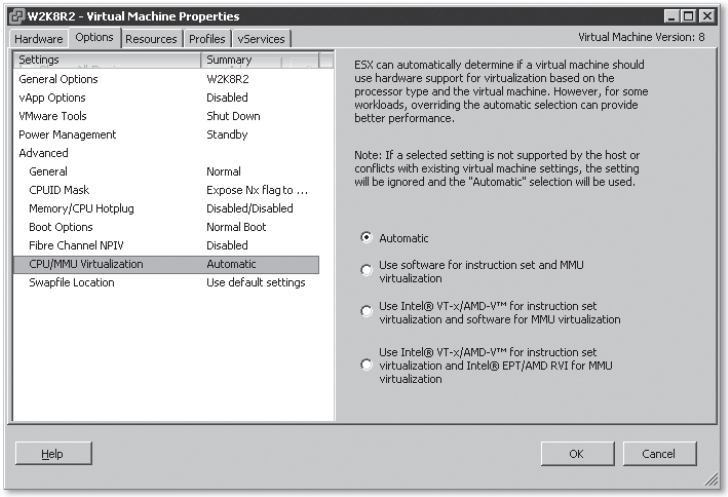


Abbildung 15.16 Einstellungen zur CPU-/MMU-Virtualisierung

15.4.14 Erweiterte Konfiguration: Swapfile Location

Das Swapfile einer VM kann entweder mit den VM-Dateien gemeinsam abgelegt werden, oder Sie verwenden dafür einen eigenen Swapfile-Datastore. Die grundlegende Einstellung legen Sie auf ESXi-Ebene fest, bei Verwendung von Clustern (HA oder DRS) wird diese Einstellung auf Ebene des Clusters definiert und an die ESXi-Server vererbt. Hierbei sollten Sie beachten, dass ein anderer Ablageort als der empfohlene (gemeinsam mit den anderen VM-Dateien) gegebenenfalls die Performance von vMotion-Operationen beeinflusst, da die lokale Swap-Datei mit übertragen werden muss.

Sie können die Einstellung pro VM überschreiben. Ihnen stehen folgende Optionen zur Verfügung:

- Default
  Es wird die vom ESXi-Host oder Cluster vererbte Einstellung verwendet.
- Always store with the virtual machine
  Wenn Sie auf ESXi- oder Cluster-Ebene die Ablage der Swapfiles in einem eigenen Datastore definiert haben, überschreibt diese Einstellung den Ablageort für diese VM. Es wird für diese VM der gleiche Ablageort wie für die VM-Dateien verwendet.
- Store in the host's swapfile datastore
  Wenn Sie auf ESXi- oder Cluster-Ebene standardmäßig den gleichen Ablageort wie für die VM-Dateien definiert haben, überschreibt diese Einstellung den Ablageort für diese VM. Es wird für diese VM der auf ESX- oder Cluster-Ebene definierte Swapfile-Datastore verwendet.

15.5 Ressourcenmanagement einer VM

Unter dem *Ressourcenmanagement* einer VM versteht man die erweiterten Einstellungen zum Performanceverhalten wie Reservierung, Limitierung und priorisierte Zuweisung von Ressourcen einer VM von den virtuellen Hardwarebausteinen CPU, Memory und Disk sowie die Möglichkeit zur Zuweisung einer dedizierten physischen CPU.

Diese Einstellungen nehmen Sie in den Eigenschaften einer VM im Reiter Resources vor. Die Hintergründe von CPU- und Memory-Management sind detailliert in Kapitel 2, »vSphere-Architektur«, beschrieben.

15.5.1 CPU-Ressourcen

Die Einstellungen zu CPU-Shares, dem CPU-Limit und einer CPU-Reservation konfigurieren Sie in den Eigenschaften einer virtuellen Maschine im Reiter Resources im Abschnitt CPU. Die CPU-Affinity sowie die Hyperthreading-Einstellung legen Sie im Abschnitt Advanced

CPU fest. Empfehlungen zum Umgang mit diesen Einstellungen finden Sie in Kapitel 2, »vSphere-Architektur«.

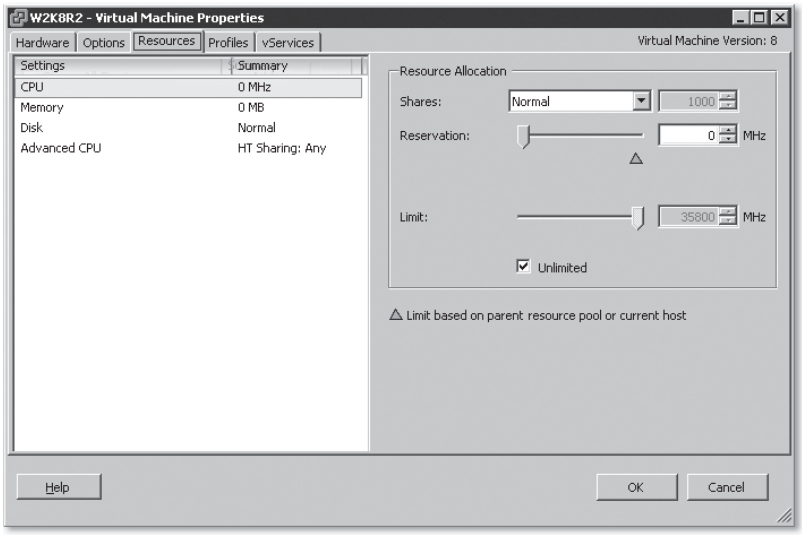


Abbildung 15.17 Einstellung der CPU-Ressourcen

CPU-Shares

Die einer VM zugewiesenen CPU-Shares definieren, mit welcher Priorität einer virtuellen Maschine freie CPU-Rechenkapazität zugewiesen wird; mit den CPU-Shares legen Sie die Wichtigkeit einer VM beim Zugriff auf die Ressource CPU fest. Da alle virtuellen Maschinen anteilige Ressourcen der physischen CPUs des ESX-Servers erhalten, weisen die Memory-Shares eine relative Priorität zwischen den VMs zu.

Die Shares werden in der Regel in drei Stufen justiert: High, Medium und Low. Dabei entspricht High dem Wert 2000, Medium dem Wert 1000 und Low dem Wert 500. Zusätzlich zu diesen Einstellungen können Sie den Wert direkt unter Custom bestimmen. Die drei Werte High, Medium und Low legen ein Verhältnis von 4 : 2 : 1 fest.

CPU-Limit

Einer VM können Sie ein Limit für die CPU-Auslastung in MHz zuweisen. Per Default ist diese Einstellung unlimited, was besagt, dass eine VM sich bei Bedarf so viel CPU-Ressourcen anfordern kann, wie sie benötigt und wie natürlich die zugewiesene physische CPU zu leisten vermag.

Hinweis

Das Limit kann nie tiefer sein als der Wert der CPU-Reservation.

CPU-Reservation

Die Reservierung von CPU-Ressourcen einer VM legt eine garantierte Menge von CPU-Rechenleitung in MHz fest. Diese Mindestmenge muss beim Starten der VM auf einem ESXi-Server zur Verfügung stehen und wird durch die Admission Control überprüft. Sollte die CPU eine nicht ausreichende Menge von MHz zur Verfügung haben, so zeigt die Admission Control eine Fehlermeldung an.

Der Standardwert der CPU-Reservation ist 0 und kann nie höher sein als der Wert des CPU-Limits einer VM. Die Reservierung einer CPU-Reservierung für eine VM müssen Sie mit Bedacht wählen, denn dies limitiert automatisch die verfügbaren CPU-Gesamtressourcen eines ESXi-Servers.

CPU-Affinity

Eine weitere Konfigurationsmöglichkeit einer VM im Bereich der CPU ist die direkte Zuweisung der virtuellen CPU auf eine physische CPU, die Definition der CPU-Affinity. Diese Technik sollten Sie nur in Ausnahmefällen verwenden, da sie etliche Auswirkungen auf andere Bereiche hat: Zum einen setzt sie die CPU-Lastverteilung des ESXi-Servers außer Kraft, zum anderen kollidiert diese CPU-Zuordnung mit eventuell vorgenommenen Einstellungen von CPU-Shares und einer CPU-Reservation, da durch das Umgehen der CPU-Lastverteilung den Forderungen seitens der VM eventuell nicht mehr nachzukommen ist.

Die CPU Admission Control kann mit der CPU-Affinity nicht korrekt umgehen, und als Folge davon sind die Überprüfungen, die die Admission Control durchführt, um die Ressource CPU zuzusichern, nicht mehr korrekt. Auch kann das Verschieben der VM auf einen anderen ESXi-Host Probleme mit sich bringen, da nicht sichergestellt ist, dass der andere ESXi-Server die gleiche Ressource CPU zur Verfügung stellt; hierbei würde dann die CPU-Affinity ignoriert. Diese Konfigurationsmöglichkeit finden Sie im Reiter Resources unter Advanced CPU.

Hyperthreading

Der ESXi-Server verteilt die Last zwischen den Cores, um eine ausgewogene Auslastung zu erreichen. Wenn für eine logische CPU keine Last gefordert wird, wird sie in einen speziellen Ruhezustand (Halt State) geschaltet. Dabei profitiert eine VM auf dem Core von der zusätzlichen Performance dieser CPU. Um virtuelle Maschinen mit für Hyperthreading problematischen Anwendungen ohne das Feature zu betreiben, existieren in der erweiterten Konfiguration von virtuellen Maschinen folgende Einstellungen:

- Any
  Any ist die Standardeinstellung und ermöglicht das Teilen der logischen CPUs eines Cores mit entweder einer weiteren virtuellen CPU der gleichen VM oder einer virtuellen CPU einer weiteren VM. Diese Einstellung bietet, sofern die Anwendungen dafür ausgelegt sind, die optimale Performance.

- None
  None schaltet das Hyperthreading für die gewählte virtuelle Maschine aus. Eine virtuelle CPU wird einer logischen CPU eines Cores zugeordnet, die zweite logische CPU wird in den Halted State geschaltet. Da diese Einstellung eine virtuelle CPU vom restlichen System isoliert, wird diese Konfiguration für hyperthreading-problematische Applikationen verwendet und sollte nur nach Aufforderung seitens VMware-Support oder Herstellersupport der Anwendung implementiert werden.
- Internal
  Internal beschränkt die Nutzung der zwei logischen CPUs auf eine VM und gilt daher nur für VMs mit aktiviertem Virtual SMP (Symmetric Multi-Processing). Eine VM teilt sich den Core nicht mit anderen VMs, sondern der Core wird nur die virtuellen CPUs einer VM verwendet. Wurde diese Einstellung für eine UniproZessor-VM ausgewählt, schaltet ESXi diese Einstellung automatisch auf None.

Diese Einstellung hat keinen Einfluss auf die Verteilung und Priorisierung von CPU-Ressourcen an die virtuelle Maschine. Diese Konfigurationsmöglichkeit finden Sie im Reiter Resources unter Advanced CPU.

15.5.2 Memory-Ressourcen

Die Einstellungen zu Memory-Shares, dem Memory-Limit und einer Memory-Reservation konfigurieren Sie in den Eigenschaften einer virtuellen Maschine im Reiter Resources im Abschnitt Memory. Empfehlungen zum Umgang mit diesen Einstellungen finden Sie in Kapitel 2, »vSphere-Architektur«.

Memory-Shares

Die einer VM zugewiesenen Memory-Shares definieren, mit welcher Priorität einer virtuellen Maschine freie Speicherbereiche zugewiesen werden: Memory-Shares legen also die Wichtigkeit einer VM beim Zugriff auf den Speicher fest. Da alle virtuellen Maschinen aus dem gemeinsamen Bereich, dem Virtual-Machine-Memory, den Speicher erhalten, legen die Memory-Shares eine relative Priorität zwischen den VMs fest.

Die Memory-Shares werden in der Regel in drei Stufen eingeteilt: High, Medium und Low. Dabei entspricht High dem Wert 2000, Medium dem Wert 1000 und Low dem Wert 500. Zusätzlich zu diesen Einstellungen können Sie den Wert direkt unter Custom bestimmen. Die drei Werte High, Medium und Low legen ein Verhältnis von 4:2:1 fest.

Memory-Limit

Einer VM können Sie ein Limit für die Speichernutzung zuweisen. Per Default ist diese Einstellung unlimited, was bewirkt, dass eine VM die RAM-Menge erhält, die in ihrer Ressourcenkonfiguration definiert ist, allerdings immer in Abhängigkeit vom aktuellen Overcommit-

ment-Status des ESX-Servers. Dies bedeutet, dass nur ein ESXi-Server, der nicht overcommitted ist, einer VM von Beginn an den maximalen Speicher zuordnet.

Memory-Reservation

Die Speicherreservierung einer VM legt eine garantierte Speichermenge fest, die einer VM beim Starten zugewiesen wird. Diese Mindestmenge muss beim Starten der VM auf einem ESX-Server zur Verfügung stehen und wird durch die Admission Control überprüft. Sollten nicht ausreichend Speicher zur Verfügung stehen, so zeigt die Admission Control eine Fehlermeldung an.

Der Standardwert der Memory-Reservation ist 0 und kann nie höher sein als das dieser VM zugewiesene RAM, aber das regelt bereits der vSphere-Client, da Sie keinen höheren Wert als die zugewiesene Speichermenge auswählen können. Den Speicher für eine VM müssen Sie mit Bedacht reservieren, denn dies limitiert automatisch den verfügbaren Speicherbereich auf einem ESX-Server. Eine Abkürzung, um das komplett zugewiesene RAM zu reservieren, steht Ihnen unter dem Punkt Reserve all guest memory zur Verfügung.

Um virtuelle Maschinen hoch performant zu gestalten, können Sie u. a. die Reservierung von Memory auf 100 % setzen. Dies ist aber mit Vorsicht einzusetzen, da die Memory-Reservierung von mehreren virtuellen Maschinen die Funktionalität von vSphere HA blockiert, indem die Current Failover Capacity im Summary der HA-Cluster-Eigenschaften auf null gesetzt wird.

Folgende Beispielberechnung soll die Hintergründe dazu erläutern:

- In einer Umgebung stehen drei ESXi-Server, die mit jeweils 16 GByte RAM ausgestattet sind.
- Alle drei ESXi-Server wurden zu einem HA-Cluster konfiguriert.
- Auf diesen ESXi-Servern sind 30 virtuelle Maschinen im Einsatz. Die konfigurierte Speichergröße dabei ist wie folgt:
  - 1 VM mit 4 GByte
  - 4 VMs mit je 2 GByte
  - 15 VMs mit je 1 GByte
  - 10 VMs mit je 512 MByte
- Keine der virtuellen Maschine wurde mit einer Memory-Reservierung versehen.
- Die Cluster Failover Capacity ist jetzt mit einer 1 angegeben.

Die pro ESXi-Server maximal adressierbare Speichergröße beträgt ca. 30 GByte. Diese Erhöhung fußt auf der Einbeziehung von swap-basiertem Speicher.

Ändern Sie jetzt die Konfiguration der größten virtuellen Maschine mit 4 GByte auf eine Memory-Reservierung von 100 %, wird die Failover-Kapazität mit 0 neu berechnet. Eine

Failover-Kapazität von 0 ist aber mit dem Ausschalten des HA-Clusters gleichzusetzen, da die HA-Agents keine verfügbaren Ressourcen im Cluster-Verbund mehr sehen.

Folgende Berechnung soll aufzeigen, dass trotz der Memory-Reservierung besagter VM und der Angabe einer Failover-Kapazität von 0 genügend Ressourcen zur Verfügung stehen:

- physischer Speicher aller drei ESXi-Server: 3 × 16 = 48 GByte
- swap-basierter Speicher aller drei ESXi-Server: 3 × 16 = 48 GByte
- maximal möglicher Verbrauch aller virtuellen Maschinen = 32 GByte
- durchschnittlicher realer Verbrauch aller virtuellen Maschinen (da eine VM im Durchschnitt nur 20–50 % des ihr maximal zur Verfügung stehenden Speichers nutzt) = 12 GByte

Somit hätte der HA-Cluster trotzdem noch ausreichend Ressourcen zur Verfügung, um den Ausfall eines ESXi-Servers zu verkraften.

VMware verwendet zur Slot-Berechnung die virtuelle Maschine mit der am stärksten konfigurierten Speicherausstattung, und dieser Slot wird mit der Anzahl der virtuellen Maschinen multipliziert. Dadurch entsteht der Berechnungs- und Anzeigefehler in den Summaries von HA.

Weitere Hintergrundinformationen über vSphere HA und die Slot-Berechnung finden Sie in Kapitel 5, »Cluster«.

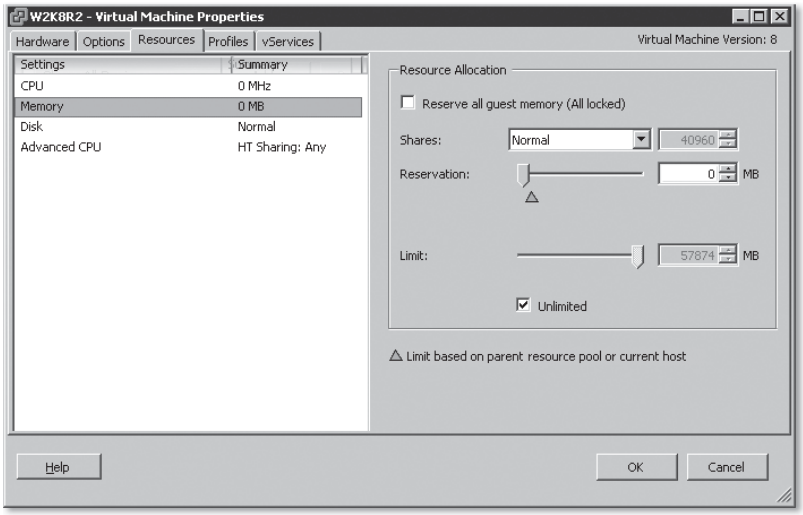


Abbildung 15.18 Einstellungen der Memory-Ressourcen

NUMA Memory Affinity

Ebenfalls im Reiter Resources finden Sie unter Memory im NUMA Memory Affinity-Bereich die Möglichkeit, festzulegen, wie auf ESXi-Servern mit NUMA-Speicherarchitektur der virtuelle

Speicherbereich einer virtuellen Maschine im physischen Speicher des ESXi-Servers abgelegt werden soll. Diese Einstellung ist nicht für VMs verfügbar, die auf DRS-Clustern abgelegt sind. Nach dem Verschieben einer virtuellen Maschine auf einen anderen ESXi-Server werden diese Einstellungen gelöscht.

Hinweis

Wenn Sie alle Nodes selektieren, entspricht diese Einstellung wieder der Einstellung No Affinity!

NUMA (Non-Uniform Memory Access) ist eine Hardwareoptimierung des Speicherzugriffs. Durch den Einbau von immer mehr CPUs in die Server-Systeme stellte sich der Speicher bzw. der Speicherzugriff als Flaschenhals heraus, da die CPUs über den Systembus mit dem Speicher kommunizieren müssen. NUMA verbindet nun mehrere kleinere Einheiten (Knoten, Nodes) von CPU und Speicher über eine Hochgeschwindigkeitsverbindung. Jetzt kann eine CPU auch Speicher aus einem anderen Knoten ansprechen, was zu Geschwindigkeitseinbußen führt, da die Daten zuerst über die NUMA-Verbindung übertragen werden müssen.

Der ESXi-Server stellt durch seinen NUMA-Scheduler sicher, dass entweder die CPU-Lastverteilung und die Speicherablage dynamisch optimiert werden oder nur die CPU-Last optimal auf den Numa-Knoten verteilt wird. Dazu wird jeder virtuellen Maschine auf einem NUMA-fähigen System ein sogenannter *Home-Node* zugewiesen, und bei der Speicherzuteilung wird der Speicher dann bevorzugt aus dem Home-Node zugewiesen. Ändert sich die Systemauslastung, so kann der NUMA-Scheduler den Home-Node der virtuellen Maschine auf einen anderen NUMA-Knoten ändern. Dabei wird auch der von der VM genutzte Speicher auf den Speicher im neuen Home-Node verschoben.

Unter bestimmten Umständen können virtuelle Maschinen nicht vom NUMA-Scheduler des ESXi-Servers verwaltet werden und somit auch nicht von der Optimierung durch NUMA profitieren. Dies ist etwa der Fall, wenn die virtuelle Maschine mehr virtuelle CPUs als physische CPUs in einem NUMA-Knoten hat oder wenn für eine virtuelle Maschine die CPU-Affinity manuell gesetzt wurde.

In bestimmten Fällen ist es sinnvoll, den NUMA-Scheduler manuell zu beeinflussen, indem Sie entweder einer virtuellen Maschine eine CPU (CPU-Affinity) oder einen bestimmten Speicherbereich zuweisen (NUMA Memory Affinity). Dies gilt z. B. für VMs mit einer sehr speicherintensiven Anwendung.

NUMA-Informationen über Ihr System finden Sie im Bereich Memory des `esxtop`-Tools.

15.5.3 Disk-Ressourcen

Die Disk-Shares konfigurieren Sie in den Eigenschaften einer virtuellen Maschine im Reiter Resources im Abschnitt Disk. Die einer VM zugewiesenen Disk-Shares definieren, mit welcher Priorität eine virtuelle Maschine I/O-Zugriff auf die Festplatten-Subsysteme erhält. Sie

legen die Wichtigkeit einer VM beim Festplattenzugriff fest, oder anders ausgedrückt, es wird zwischen den VMs eine relative Priorität bestimmt.

Die Disk-Shares werden in der Regel in drei Stufen justiert: High, Medium und Low. Dabei entspricht High dem Wert 2000, Medium dem Wert 1000 und Low dem Wert 500. Zusätzlich zu diesen Einstellungen können Sie den Wert direkt unter Custom festlegen. Die drei Werte High, Medium und Low legen ein Verhältnis von 4 : 2 : 1 fest. Die Zuweisung von Disk-Ressourcen-Shares erfolgt allerdings in Produktionsumgebungen recht selten. Des Weiteren können Sie mit Limit – IOPs festlegen, ob eine virtuelle Festplatte einer VM in der Anzahl der maximalen I/O-Operations per second (IOPS) limitiert werden sollen. Die Standardeinstellung ist unlimitiert.

15.6 USB-Geräte an virtuellen Maschinen

Sollten Sie USB-Festplatten oder USB-Dongles an virtuelle Maschinen verbinden wollen, so stehen Ihnen bei vSphere 5 zwei Möglichkeiten mittels VMwares USB-Passthrough zur Verfügung: Zum einen können Sie USB-Geräte an ESXi-Hosts anschließen und dann an VMs verbinden, die auf diesem ESXi-Host laufen. Zum anderen können Sie mit Hilfe des vSphere-Clients oder des vSphere Webclients USB-Geräte an virtuelle Maschinen verbinden, die an dem PC angeschlossen sind, auf dem der vSphere-Client läuft.

Grundsätzlich gilt, dass Sie USB-Geräte, entweder am ESXi-Host oder am Client angeschlossene, nur mit einer VM verbinden können. Das USB-Gerät steht daher nach dem Verbinden mit der VM nicht mehr in der Auswahlliste im Add Hardware-Wizard.

Hinweis

USB-Geräte nach der neuen USB-3.0-Spezifikation können Sie bislang nur an Linux-VMs mit dem USB-Controller-Typ xHCI nutzen und wenn das USB-Gerät am lokalen Client, auf dem der vSphere-Client läuft, angeschlossen ist.

15.6.1 USB-Passthrough

Technisch sind bei USB-Geräteverbindungen folgende Elemente involviert:

- **USB-Arbitrator**
  Dieser Dienst läuft standardmäßig auf dem ESXi-Server und verwaltet die USB-Geräteverbindungsanfragen und ist auch für die Weiterleitung des Datenverkehrs der USB-Geräte verantwortlich.
- **USB-Controller**
  Dies ist der virtuelle USB-Hardware-Chip in der virtuellen Maschine; es können maximal zwei installiert sein.

Ein USB-Arbitrator kann maximal 15 USB-Controller verwalten; daher sollten Sie diese Beschränkung bei Ihrer Planung berücksichtigen.

- **USB-Gerät**
  Das USB-Gerät ist letztendlich das am physischen USB-Port eines ESXi-Servers oder eines PCs angeschlossene Gerät. Sie können davon zur gleichen Zeit maximal 20 an eine virtuelle Maschine verbinden. Des Weiteren ist 20 auch die maximale Anzahl von vom ESXi-Server verwaltbaren USB-Geräten, die gleichzeitig an virtuelle Maschinen verbunden sind.

15.6.2 USB-Autoconnect

Mittels USB-Autoconnect verbindet sich die virtuelle Maschine mit dem verbundenen USB-Gerät in folgenden Fällen immer wieder automatisch:

- wenn die VM aus- und wieder eingeschaltet wird, oder auch suspendiert und wieder aktiviert wird
- das USB-Gerät abgezogen wird und am gleichen USB-Port wieder angeschlossen wird
- das USB-Gerät aus- und wieder eingeschaltet wird
- das USB-Gerät eine andere Identität meldet, z. B. ein iPhone nach einem Firmware-Upgrade

Intern arbeitet vSphere auf Basis des USB-Hardware-Pfads und nicht mit der Kennung des USB-Gerätes. Daher wird das gleiche USB-Gerät nicht automatisch wieder mit der VM verbunden, wenn es an einen anderen USB-Port gesteckt wird. Allerdings wird ein anderes USB-Gerät wieder mit der VM verbunden, wenn unmittelbar vorher ein USB-Gerät über den gleichen USB-Port verbunden war. Aber hier müssen Sie darauf achten, dass jeweils die gleiche USB-Spezifikation (USB 1.1 und USB 2.0) verwendet wurde.

15.6.3 Kompatible vSphere-Funktionen

Beim Einsatz von USB-Passthrough können Sie folgende vSphere-Funktionen nutzen:

- vSphere vMotion
  Bei der erstmaligen Verbindung des USB-Geräts zur VM muss diese auf dem ESXi-Host laufen, an dem das USB-Gerät physisch angeschlossen ist. Ist die Verbindung einmal hergestellt und wurde das USB-Gerät für den Einsatz von vMotion konfiguriert, dann bleibt die Verbindung zum USB-Gerät auch nach einem vMotion-Vorgang bestehen.

  Allerdings kann die USB-Verbindung nach einer Trennung nicht wieder hergestellt werden. Dazu muss die VM wieder zurück auf den ESXi-Host verschoben werden, an dem das USB-Gerät verbunden ist.

  Das Gleiche gilt für nach dem Ausschalten oder Suspendieren einer VM, da dadurch die USB-Geräteverbindung unterbrochen wird. Hier greift leider USB-Autoconnect nicht.
- vSphere DRS (Distributed Resource Scheduling)

Nicht unterstützt sind:

- vSphere Fault Tolerance
- vSphere DPM (Distributed Power Management)
  Sollten Sie über den vSphere-Client das am Client lokal angeschlossene USB-Gerät mit der VM verbinden, so steht dem Einsatz von vSphere DPM nichts im Wege. Die Beschränkung gilt nur, wenn Sie vom ESXi-Host aus das USB-Gerät verbinden. Der Hintergrund ist einfach erklärt: Wenn mittels vMotion die virtuelle Maschine verschoben wurde und der ESXi-Host keine VMs mehr beherbergt, kann vSphere DPM diesen ESXi-Host in den Schlafmodus versetzen. Dadurch werden aber alle USB-Verbindungen, die VMs noch mit USB-Geräten an diesem ESXi-Host haben könnten, unterbrochen. Überlegen Sie, ob für diesen Cluster das vSphere DPM ausgeschaltet werden kann.
- Hot Add von Speicher, CPUs oder PCI-Geräten
  Beim Hot Add werden alle USB-Geräteverbindungen zu virtuellen Maschinen unterbrochen. Sollten zur gleichen Zeit z. B. Datentransfers laufen, so müssen Sie mit Datenverlusten rechnen. Idealerweise trennen Sie vorher alle USB-Geräteverbindungen und fügen dann weitere Hardware via Hot Add hinzu.

Hinweis

USB-CD-/DVD-Laufwerke werden als SCSI-Geräte verwaltet und können daher nur bei ausgeschalteten ESXi-Host angeschlossen oder entfernt werden. Hot Add wird nicht unterstützt!

15.6.4 Das Verbinden von USB-Geräten

Das Verbinden von USB-Geräten wird ab der Virtuellen-Hardware-Version 7 unterstützt und bedarf mindestens eines USB-Controllers in der virtuellen Hardware. Daher fügen Sie im ersten Schritt Ihrer virtuellen Maschine einen, maximal zwei USB-Controller hinzu. Beachten Sie bitte folgende Auswahlmöglichkeiten:

- Controller-Typ xHCI
  Unterstützt USB 3.0, 2.0 und 1.1; nur Linux-Gastbetriebssysteme (Kernel-Version von 2.6.35 oder höher).
- Controller-Typ EHCI+UHCI
  Unterstützt USB 2.0 und 1.1 für alle unterstützten Gastbetriebssysteme.

Über den Add Hardware-Wizard wählen Sie den USB-Controller aus; im nächsten Schritt (siehe Abbildung 19.19) werden Sie nach dem Typ gefragt.

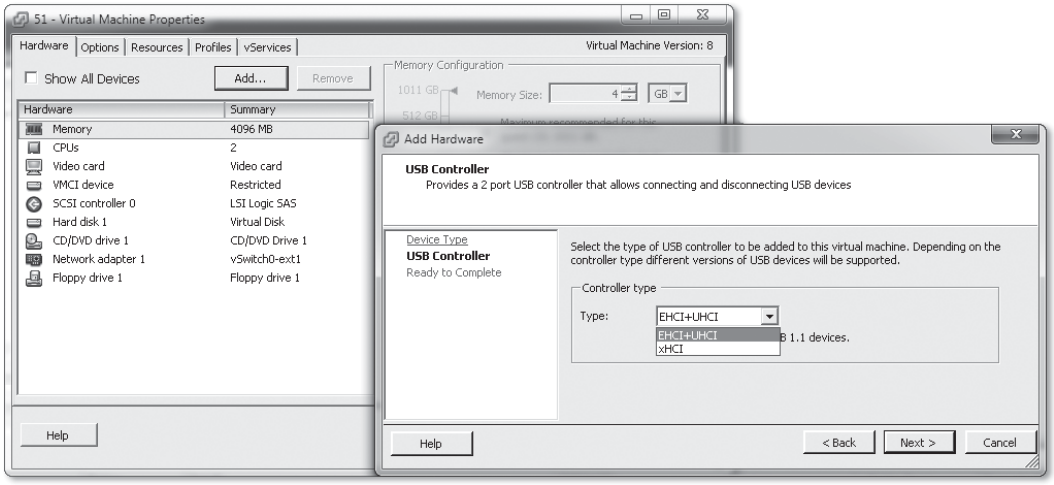


Abbildung 15.19 Beim Hinzufügen eines USB-Controllers werden Sie nach dem Typ gefragt.

Der neue USB-Controller ist jetzt als neue virtuelle Hardware vorhanden (siehe Abbildung 15.20).

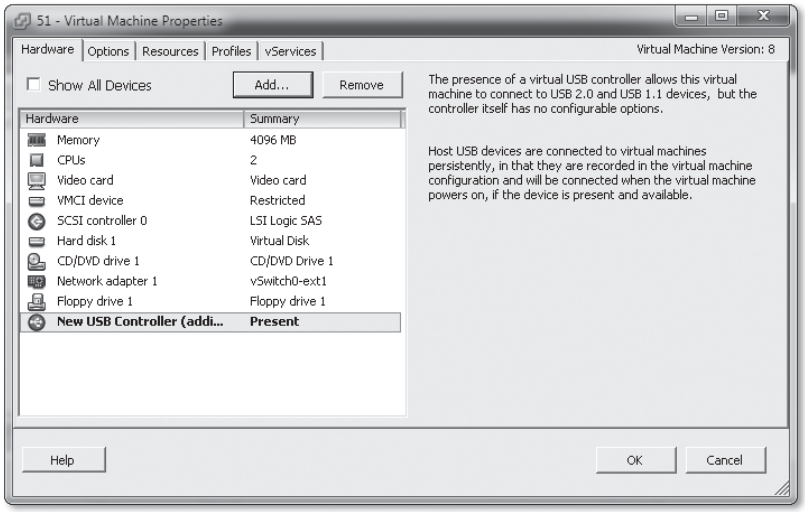


Abbildung 15.20 Der USB-Controller wurde der virtuellen Maschine hinzugefügt.

In Ihrem Gastbetriebssystem hat Windows jetzt die neue Hardware erkannt und die Treiber hierfür installiert (siehe Abbildung 15.21).

Jetzt kümmern Sie sich um das eigentliche Hinzufügen des gewünschten USB-Gerätes. Nachdem Sie ein USB-Gerät mit dem ESXi-Host oder dem lokalen Client, auf dem Ihr vSphere-Client läuft, verbunden haben, starten Sie wieder den ADD HARDWARE-Wizard der VM. Wählen Sie jetzt USB DEVICE aus (siehe Abbildung 15.22).

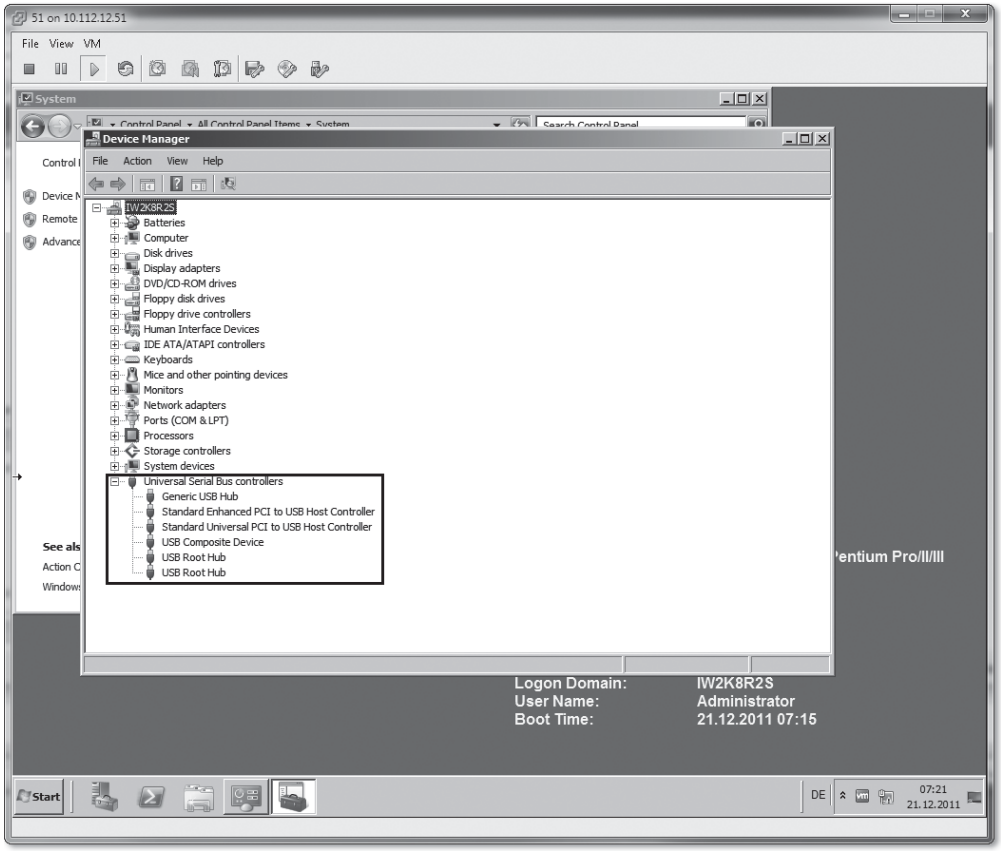


Abbildung 15.21 Der USB-Controller steht jetzt in Windows zur Verfügung.

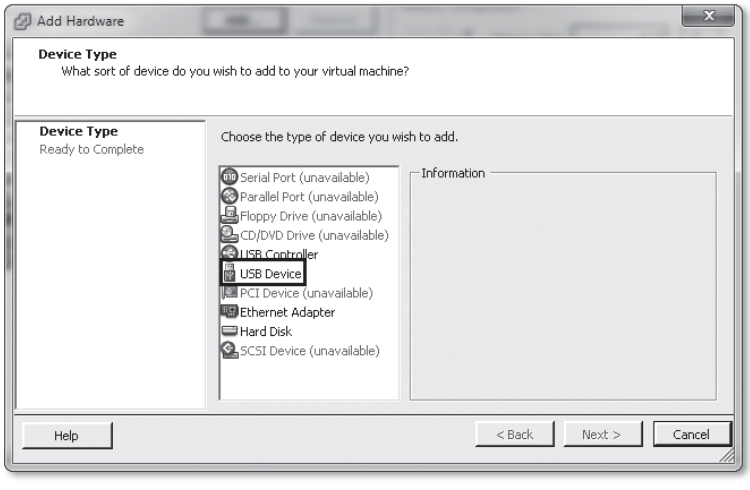


Abbildung 15.22 Das Hinzufügen eines USB-Gerätes zur virtuellen Hardware

Sie finden im nächsten Wizard-Schritt alle zur Auswahl stehenden USB-Geräte. Sollten Sie vMotion mit dieser VM nutzen wollen, so wählen Sie neben der Auswahl des USB-Gerätes auch die Option SUPPORT VMOTION WHILE DEVICE IS CONNECTED.

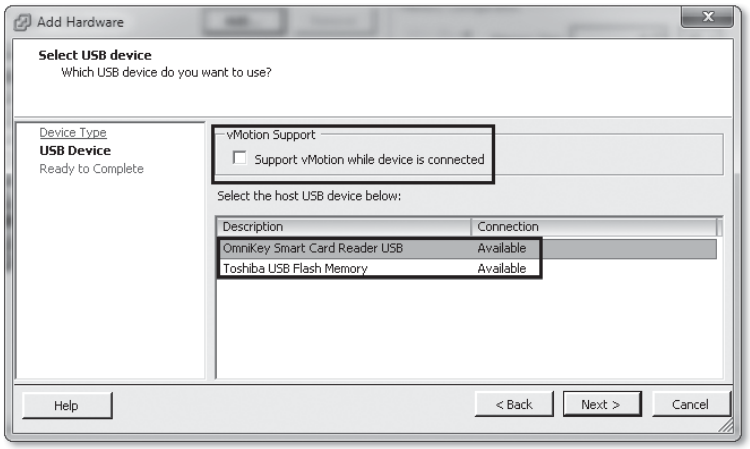


Abbildung 15.23 Die Auswahl des USB-Gerätes mit Aktivierung von vMotion-Unterstützung

Das USB-Gerät, hier ein Smart-Card-Reader für USB, wurde der virtuellen Hardware hinzugefügt:

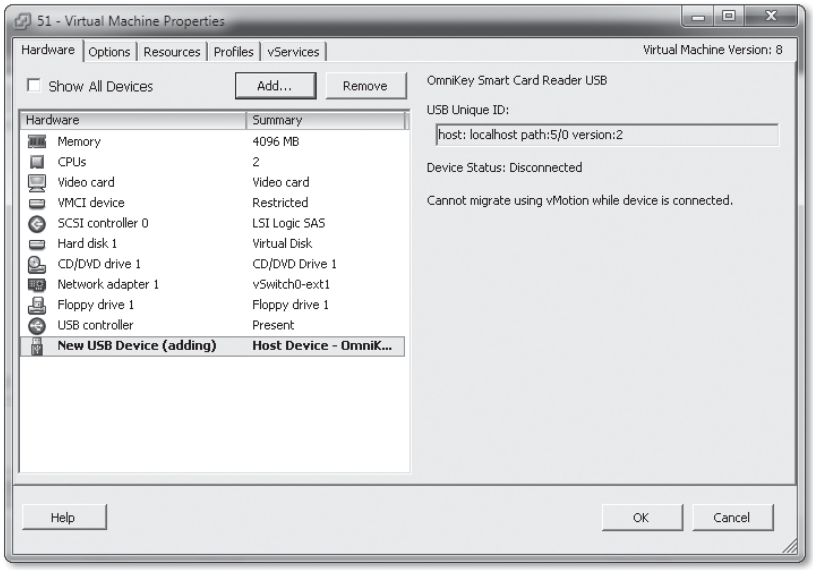


Abbildung 15.24 Das USB-Gerät wurde der virtuellen Hardware hinzugefügt.

Ihr Gastbetriebssystem erkennt das USB-Gerät, installiert die Treiber und zeigt den Smart-Card-Reader in Ihrer HARDWARE-Übersicht an:

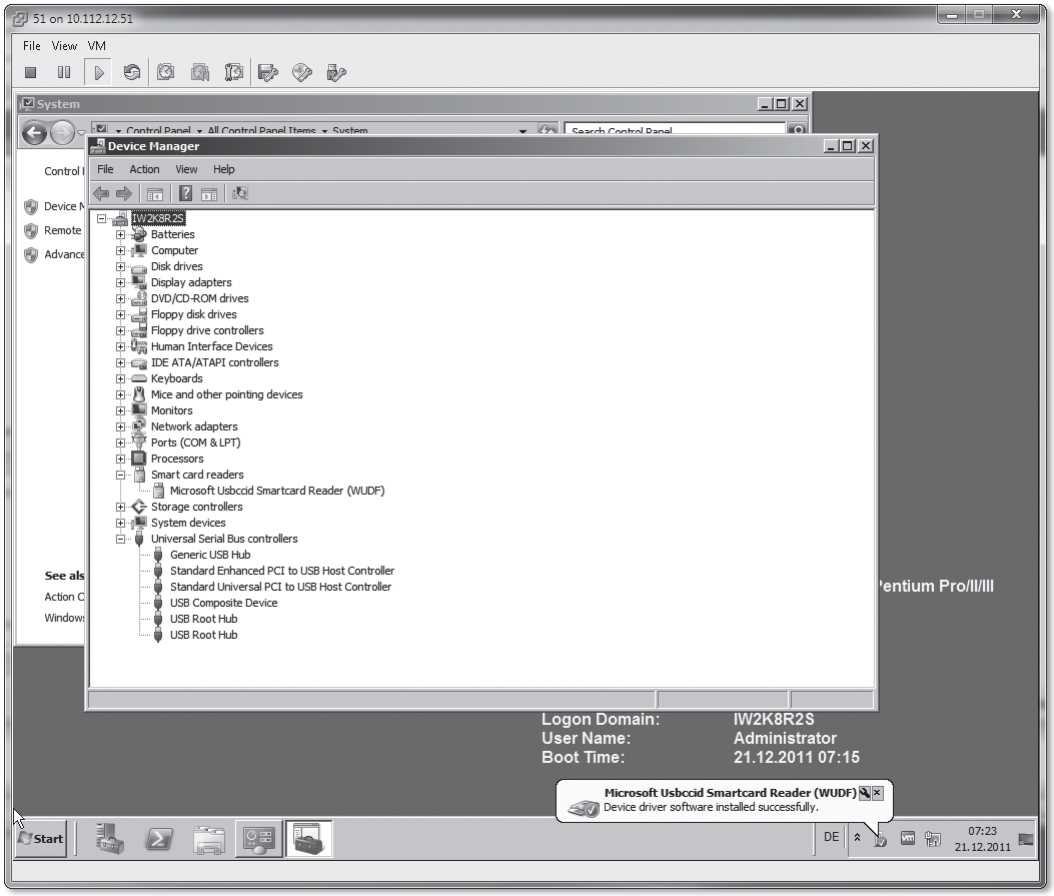


Abbildung 15.25 Windows hat den Smart-Card-Reader erkannt und die Treiber installiert.

15.6.5 Das Entfernen von USB-Geräten

Wählen Sie in der HARDWARE-Übersicht ihrer VM das USB-Gerät aus, und klicken Sie auf REMOVE. Idealerweise entfernen Sie das USB-Gerät im Gastbetriebssystem, so dass kein Datenverlust entstehen kann. Optional können Sie auch den USB-Controller wieder aus der virtuellen Hardware entfernen. Nachdem Sie das USB-Gerät aus der VM entfernt haben, steht es anderen virtuellen Maschinen wieder zur Verfügung.

15.7 VM-Speicherprofile (VM Storage Profiles)

Mit Hilfe der VM-Speicherprofile haben Sie die Möglichkeit, bestimmte Anforderungen an den Festplattenspeicher einer VM zu definieren und dadurch die Dateien einer VM auf dem passenden Datastore abzulegen. Diese Anforderungen können für die Konfigurationsdateien

einer VM und den Festplattendateien unterschiedlich sein. Des Weiteren hinterlegen Sie pro Datastore neben den systemdefinierten Speicherfunktionen eigene benutzerdefinierte Speicherfunktionen (User-defined Storage Capabilities) und in den VM-Speicherprofilen legen Sie die Speicherfunktionen fest, die zwingend von diesem VM Speicherprofil erfüllt sein müssen. Ein Compliance-Check pro VM zeigt Ihnen an, ob der Datastore, auf dem die VM-Dateien liegen, diese Anforderungen erfüllt.

So können Sie über diese Profile kritischen VMs einen performanteren Speicher zuweisen und auch im Laufe eines VM-Lebens regelmäßig überprüfen, ob die VMs noch auf den Datastores abgelegt sind, die laut VM-Speicherprofil hierfür vorgesehen waren.

Die VM-Speicherprofile können in Verbindung mit Speicher-DRS (Storage DRS) verwendet werden. Achten Sie darauf, dass alle Datastores in einem Cluster die gleichen Speicherfunktionen haben.

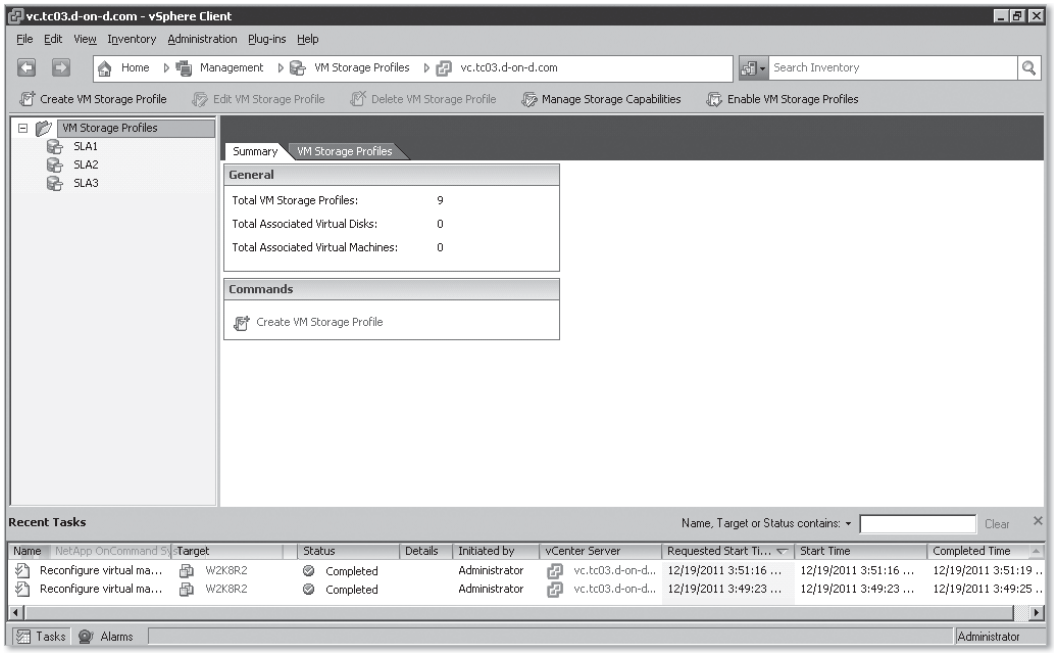


Abbildung 15.26 Hier finden Sie alle Befehle zur Erstellung und Aktivierung der VM-Speicherprofile sowie der benutzerdefinierten Speicherfunktionen.

15.7.1 Festlegen der benutzerdefinierten Speicherfunktionen

Neben den via VASA kommenden systembedingten Speicherfunktionen legen Sie eigene Speicherfunktionen fest und weisen diese dann den Datastores zu.

Starten Sie im HOME-Bildschirm vom vSphere-Client, und klicken Sie unter MANAGEMENT auf das Icon VM-SPEICHERPROFILE. Unter der Menüleiste klicken Sie dann auf SPEICHERFUNKTIONEN VERWALTEN, um Ihre eigenen Speicherfunktionen zu definieren. Bedenken Sie, dass systembedingte Speicherfunktionen bereits in dieser Liste stehen. Über den Schalter HINZUFÜGEN vergeben Sie zuerst den Namen der Speicherfunktion und bei Bedarf einen erklärenden Text. Diese Einträge können Sie jederzeit bearbeiten und auch wieder löschen.

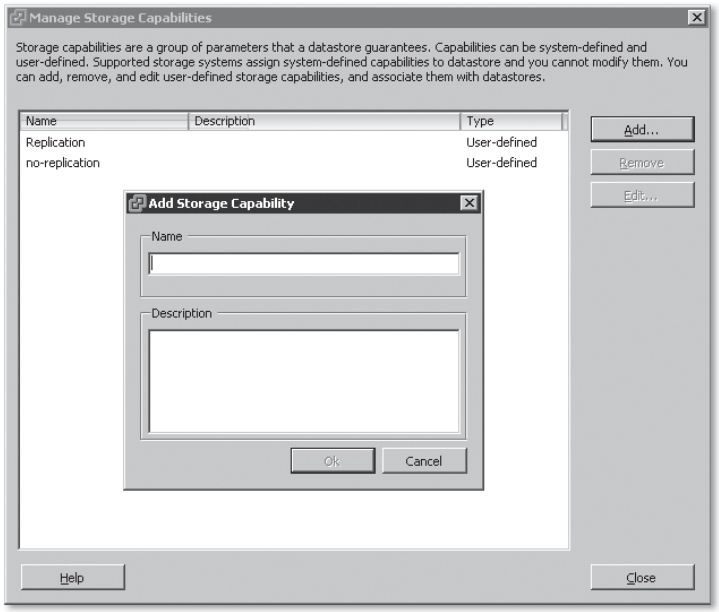


Abbildung 15.27 Festlegen von benutzerdefinierten Speicherfunktionen

Diese Speicherfunktionen verarbeiten Sie im nächsten Schritt, wenn Sie VM-Speicherprofile anlegen.

15.7.2 Erstellen von VM-Speicherprofilen

Nachdem Sie die Speicherfunktionen erstellt haben, legen Sie einzelne VM-Speicherfunktionen fest, indem Sie diese Speicherfunktionen als Bestandteil des VM-Speicherprofils hinterlegen.

Im vSphere-Client wählen Sie VM-SPEICHERPROFIL ERSTELLEN entweder aus der Iconleiste oder aus dem Kontextmenü auf dem Hauptknoten im linken Bereich. Geben Sie zuerst einen Namen an und gegebenenfalls einen beschreibenden Text. Im nächsten Wizard-Schritt klicken Sie die Speicherfunktionen (systembedingte und benutzerdefinierte) an, die Sie als Bestandteil dieses Profils ansehen. Diese VM-Speicherprofile weisen Sie im nächsten Schritt den Datastores zu.

15.7.3 Zuweisen von benutzerbedingten Speicherfunktionen

Die vorhin erstellten benutzerbedingten Speicherfunktionen weisen Sie jetzt den Datastores zu. Entweder gehen Sie hierzu über den Menüpunkt Datenspeicher und Datenspeicher-Cluster in der Bestandsliste oder über Hosts und Cluster.

In der Bestandsliste wählen Sie Datenspeicher und Datenspeicher-Cluster und selektieren einen Datastore. Den Befehl Benutzerdefinierte Speicherfunktion zuweisen finden Sie entweder im Kontextmenü des Datastores oder im rechten Bildschirmbereich unter Befehle. Aus der vorher erfassten Liste wählen Sie jetzt eine Speicherfunktion aus, die für diesen Datastore zutrifft.

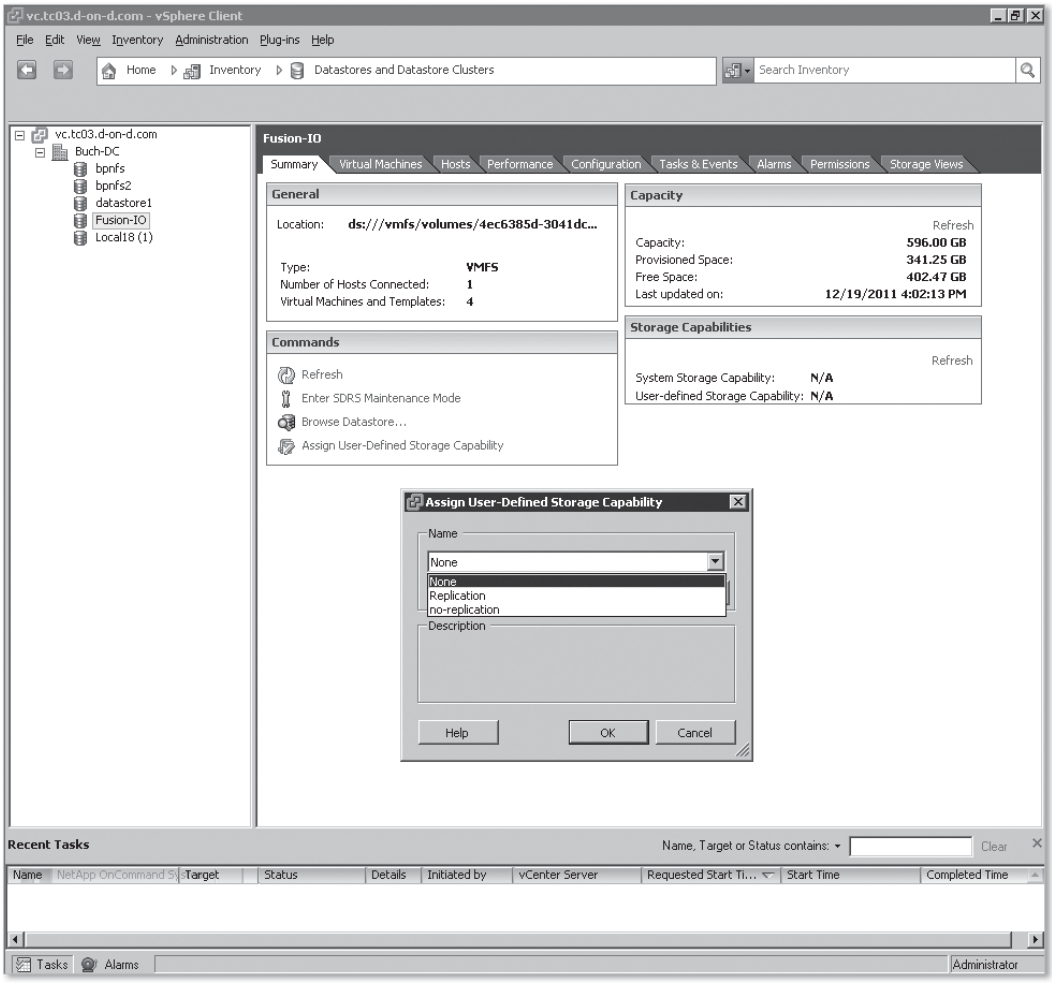


Abbildung 15.28 Zuweisen der benutzerdefinierten Speicherfunktionen

Nachdem Sie die VM-Speicherprofile erstellt und die Datastores mit verschiedenen Speicherfunktionen versehen haben, gilt es, bei den virtuellen Maschinen zu hinterlegen, auf welche Arten von Datastores diese zu laufen haben.

15.7.4 Verwenden von VM-Speicherprofilen

Die VM-Speicherprofile können über drei Wege zum Einsatz kommen:

- beim Bereitstellen von neuen VMs
- beim Migrieren von VMs
- den VMs im laufenden Betrieb zuweisen

Beim Bereitstellen von virtuellen Maschinen können Sie beim Schritt Speicher ein VM-Speicherprofil auswählen. Anhand dieser Auswahl wird die Anzeige der Datastores gefiltert in kompatible und nicht-kompatible Datastores. Das Gleiche gilt beim Migrieren von virtuellen Maschinen via vMotion. Sie können dennoch ein Datastore aus der Liste der nicht-kompatiblen auswählen. Zur Folge hat dies nur, dass diese VM später als nicht-compliant gilt.

Bei einer bereits existierenden VM finden Sie in den Eigenschaften dieser den Reiter Profile. Dort wählen Sie ein Home-VM-Speicherprofil, das für die Konfigurationsdateien einer VM gilt, und auch pro virtueller Festplatte ein VM-Speicherprofil. Möchten Sie keine Unterscheidung treffen, dann können Sie nach der Auswahl des Home-VM-Speicherprofils den etwas unglücklich benannten Schalter Weitergeben an Festplatten klicken, um dieses Speicherprofil auch allen virtuellen Festplatten zuzuweisen. Sie können auch jeder virtuellen Festplatte einer VM ein anderes VM-Speicherprofil zuweisen. Dies ist technisch möglich, nur ob es sinnvoll ist, gilt es genau zu überprüfen.

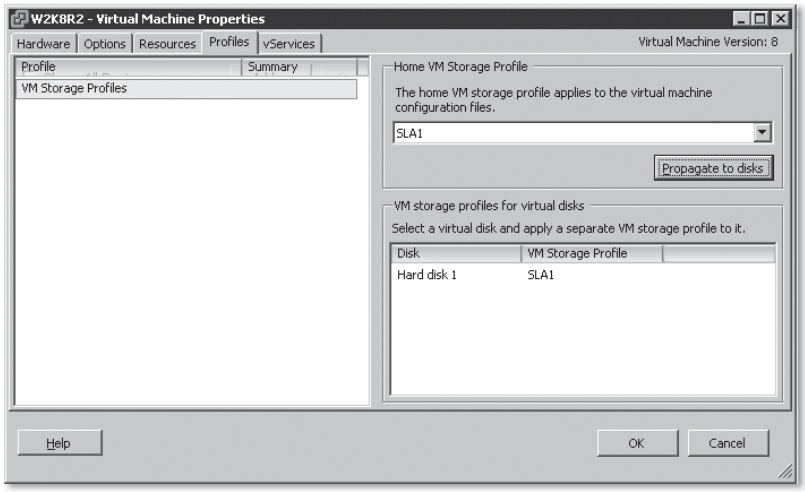


Abbildung 15.29 Einer VM wird ein VM-Speicherprofil zugewiesen.

Nach der Zuweisung können Sie bei der virtuellen Maschine überprüfen lassen, ob der Ablageort der VM-Dateien dem ausgewählten VM-Speicherprofil der VM entspricht. Klicken Sie dazu im Kontextmenü der VM unter VM-Speicherprofil auf den Menüpunkt Profil-Übereinstimmung prüfen. Dies führt intern einen Compliance-Check durch und meldet entweder eine Profi-Übereinstimmung oder ein rotes Ausrufezeichen. Da sich dieser Zustand jederzeit ändern kann, wird das Datum der letzten Überprüfung mit ausgegeben.

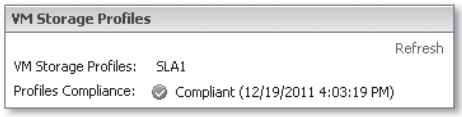


Abbildung 15.30 Das Profil und der verwendete Datastore stimmen überein.

15.8 Starten, Stoppen und weitere Power-Aktivitäten

Eine virtuelle Maschine kann in einem der folgenden Power-Zustände sein:

- **eingeschaltet**
- **ausgeschaltet**
- **suspended**
  Die virtuelle Maschine wurde eingefroren und der Speicherinhalt in eine Datei aus dem File-System geschrieben. Der Befehl »Resume« befreit eine VM aus diesem Zustand und bringt sie wieder zurück in den normalen Betriebsmodus.

Je nach aktuellem Zustand einer VM können Sie verschiedene Power-Aktivitäten durchführen:

- **Power on**
  Schaltet die virtuelle Maschine ein. Optional führen Sie nach der Installation der VMware Tools im Gastbetriebssystem ein Skript nach dem Einschalten der VM aus.
- **Power off**
  Schaltet die virtuelle Maschine aus. Optional führen Sie nach der Installation der VMware Tools im Gastbetriebssystem ein Skript vor dem Ausschalten der VM aus.
- **Suspend**
  Hält eine VM an. Optional führen Sie nach der Installation der VMware Tools im Gastbetriebssystem ein Skript vor dem Suspendieren der VM aus. Der eingefrorene Zustand der virtuellen Maschine wird in einer Datei mit der Endung *.vmss* gespeichert und wird für das Reaktivieren wieder benötigt.

- **Resume**
  Das Reaktivieren einer suspendierten (angehaltenen) VM mit dem Power on-Button oder dem gleichnamigen Befehl. Optional führen Sie nach der Installation der VMware Tools im Gastbetriebssystem ein Skript nach dem Reaktivieren der VM aus.
- **Reset**
  Vereint die zwei Power-Aktivitäten »Power off« und »Power on« in einem Schritt. Nach der Installation der VMware Tools im Gastbetriebssystem und entsprechender Umkonfiguration einer VM in den Optionen können Sie das Gastbetriebssystem geregelt herunterfahren und neu starten.

Nach der Installation der VMware Tools im Gastbetriebssystem stehen weitere Power-Aktivitäten zur Verfügung. In den Optionen einer VM lässt sich das Verhalten bei »Power on«, »Power off« und »Restart« umkonfigurieren, so dass nachfolgende Power-Aktivitäten wahlweise zur Verfügung stehen:

- **Shut down guest**
  Bei einem »Power off« wird anstelle des direkten Ausschaltens einer VM das Betriebssystem zuerst geregelt heruntergefahren und dann die VM ausgeschaltet.
- **Restart guest**
  Bei einem »Reset« wird anstelle des direkten Ein- und Ausschaltens einer VM das Betriebssystem zuerst geregelt heruntergefahren und dann die VM neu gestartet.

15.9 Installation des Gastbetriebssystems

Die Installation des Gastbetriebssystems kann mittels Installationsmedium erfolgen: Entweder haben Sie hierfür eine CD/DVD oder ein ISO-Image. Empfohlen ist jedoch das Bereitstellen neuer VMs über Vorlagen (Templates). Weiterführende Hinweise über Templates finden Sie später in diesem Kapitel. An dieser Stelle stellen wir kurz die Installation über ein Installationsmedium vor: Beides können Sie in der Remote-Konsole einer virtuellen Maschine mit dem CD-/DVD-Laufwerk verbinden und im BIOS der VM konfigurieren, dass die virtuelle Hardware vom CD-/DVD-Laufwerk booten soll.

Konfigurieren Sie im ersten Schritt Ihre VM so, dass sie beim Starten ein verbundenes CD-ROM-/DVD-Laufwerk hat und dieses auch ein Installationsmedium enthält, beispielsweise ein verbundenes ISO-Image eines VMware-Datastores (Abbildung 15.31).

Danach können Sie Ihre VM anweisen, direkt in das BIOS zu booten, um dort die Bootreihenfolge umzustellen (Abbildung 15.32).

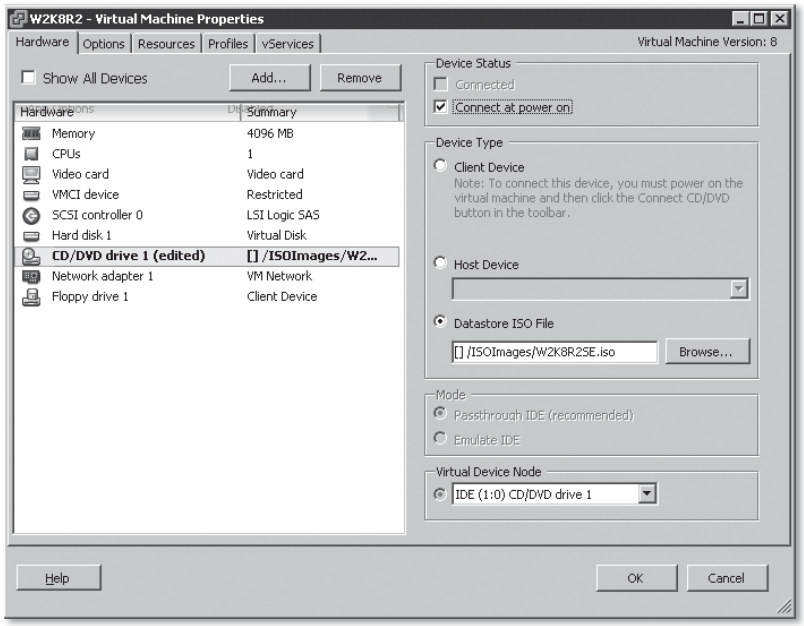


Abbildung 15.31 Ihre VM startet mit verbundenem ISO-Image.

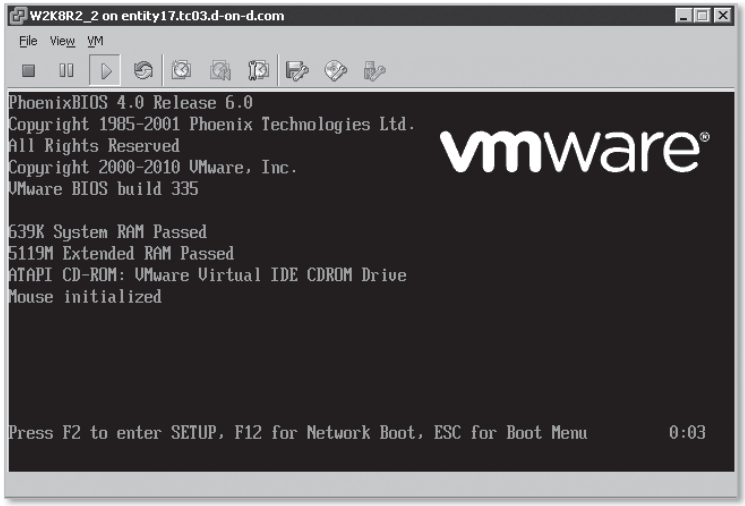


Abbildung 15.32 Drücken Sie die »Esc«-Taste, um zum »Boot Menu« der VM zu gelangen.

Alternativ drücken Sie während des Startvorgangs innerhalb der VM die Esc-Taste, um das Boot-Device auszuwählen (Abbildung 15.33).

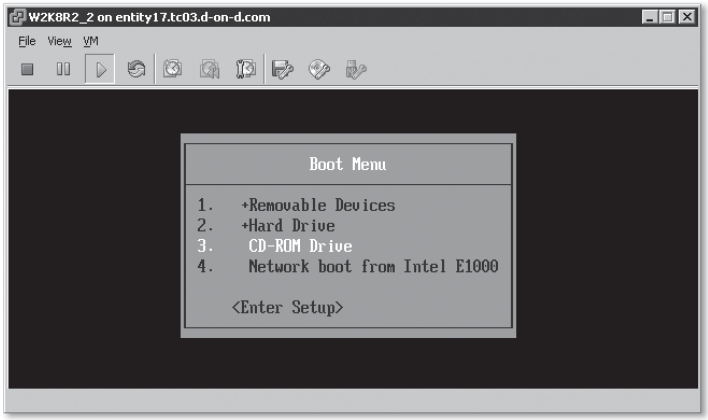


Abbildung 15.33 Legen Sie im »Boot Menu« fest, von wo die VM starten soll. Zum Starten via CD-ROM/DVD wählen Sie hier Nummer 3.

Beim nächsten Starten der VM wird vom angehängten ISO-Image gebootet. Der Setup-Vorgang des Betriebssystems wird gestartet. Ebenso funktioniert der netzwerkbasierte Installationsvorgang über ein Netzwerk-Boot mittels PXE, z. B. für Windows-Betriebssysteme über Windows Remote Installation Services (RIS) oder Windows Deployment Services (WDS). Die Netzwerkkarte versucht, eine DHCP-Adresse zu erhalten, um einen Installations-Service zu finden (Abbildung 15.34).

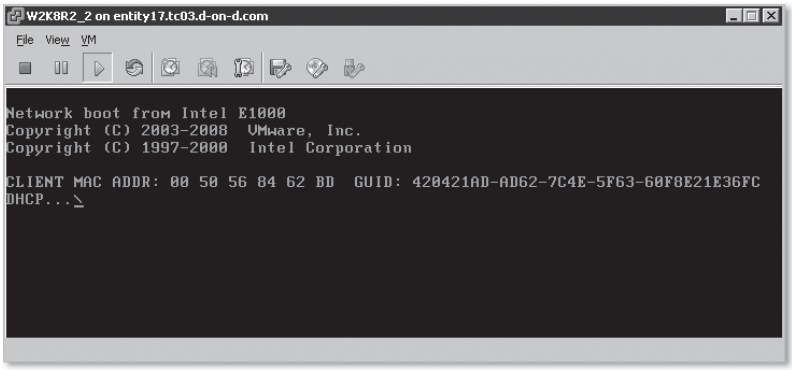


Abbildung 15.34 Netzwerk-Boot der VM

15.10 Konfiguration und Anpassung von virtuellen Maschinen

15.10.1 Ändern der Hardware

Sie können nach der Erstellung einer virtuellen Maschine deren Hardwareausstattung erweitern. Dabei müssen Sie immer die maximal erlaubte Ausstattung einer VM beachten. Zur Auswahl stehen je nach Hardwareversion der virtuellen Maschine folgende virtuelle Geräte:

- serieller Port
- paralleler Port
- Diskettenlaufwerk
- DVD-/CD-ROM-Laufwerk
- USB-Controller
- Netzwerkkarte (Ethernet)
- Festplatte
- SCSI-Gerät

Des Weiteren können Sie die Anzahl der CPUs erhöhen und die Größe des RAM-Speichers ändern.

15.10.2 Hinzufügen weiterer Hardware im laufenden Betrieb (Hot Add)

Das Hinzufügen von Speicher und CPUs steht ab der Hardwareversion 7 von virtuellen Maschinen zur Verfügung, unter der Voraussetzung, dass das Gastbetriebssystem dies ebenso unterstützt. Außerdem unterscheiden sich die verfügbaren vSphere-Editionen – Hot Add wird nur in den Editionen Enterprise und Enterprise Plus angeboten.

Das Feature müssen Sie auf der Basis der virtuellen Maschine aktivieren. Dabei stehen diese Schalter nur dann zur Verfügung, wenn Sie in den Eigenschaften einer virtuellen Maschine auch ein Gastbetriebssystem ausgewählt haben, das Hot Add unterstützt. Das grundsätzliche Aktivieren von Hot Add muss allerdings im ausgeschalteten Zustand der VM erfolgen. Nach dieser Vorbereitung können Sie der laufenden VM weitere CPUs oder mehr Speicher zuweisen. Die nächste Hürde ist das Gastbetriebssystem – entweder es erkennt die neue Hardware im laufenden Betrieb, oder es benötigt einen Neustart. Hier kommt es ganz auf die Hot-Add-Unterstützung im Betriebssystem an. Das Entfernen von Speicher und CPUs im laufenden Betrieb wird nicht unterstützt – hierzu müssen Sie die VM stoppen.

Hinweis

Hot Add wird nicht in Verbindung mit VMware FT (Fault Tolerance) unterstützt!

Hot Add von Speicher

Das Hinzufügen von mehr Speicher in laufenden Betrieb funktioniert nicht bei einem Windows Server 2003 Standard, sondern erst ab der Enterprise Edition. Dabei ist es unerheblich, ob es sich um 32 oder 64 Bit handelt. Eine Einschränkung bei der Windows Server 2008 Standard Edition: Hier ist ein Neustart des Gastes erforderlich, damit das Betriebssystem den Speicher erkennt.

Nach dem Hinzufügen von mehr Speicher zu einer VM mit einem Linux-Betriebssystem kommt es in manchen Fällen vor, dass das Gastbetriebssystem den neuen Speicher nicht erkennt. Schauen Sie sich den Speicherstatus an, und setzen Sie ihn dann manuell online.

Für Red Hat Enterprise Linux und CentOS verwenden Sie folgende Befehle:

- den Speicher finden: `grep line /sys/devices/system/memory/*/state`
- den Speicher online setzen: `/sys/devices/system/memory/memory[number]/state`

Überprüfen Sie abschließend mit dem Befehl `free` den jetzt zur Verfügung stehenden Speicher.

Hot Add von CPUs

Das Hinzufügen von weiteren CPUs funktioniert bei Microsofts Betriebssystemen nur mit Windows Server 2008, unabhängig von der Edition. Damit das Betriebssystem die neue CPU nutzen kann, muss der Gast – außer bei der 64-Bit-Datacenter-Edition – neu gestartet werden.

Das Hinzufügen von weiteren CPUs bei laufenden Linux-Gästen wird ab der Kernel-Version 2.6.14 unterstützt. Eine ausführliche Erklärung hierzu finden Sie unter *http://www.kernel.org/doc/Documentation/cpu-hotplug.txt*.

VMware hat ein Dokument veröffentlicht, das das Hinzufügen von virtuellen CPUs in einem Linux-Gast detailliert beschreibt: *http://communities.vmware.com/docs/DOC-10493*. Das Hinzufügen von virtuellen Multicore-CPUs wird erst ab der neuen Hardwareversion 8 unterstützt. Sollten Sie noch mit Version 7 arbeiten müssen, beschränken Sie die Anzahl der Cores pro Socket auf einen.

Hinweis

Das Hinzufügen weiterer CPUs bei einer aktiven VM unterbricht kurzzeitig alle eventuell vorhandenen Verbindungen von USB-Passthrough-Geräten!

Hot Add von Festplatten

Das Hinzufügen von weiteren Festplatten oder weiteren Netzwerkkarten wird seit ESX 3.5 unterstützt, und die Verwendung im Gast ist auch hier wieder abhängig vom jeweiligen Betriebssystem.

Das Erweitern von bereits existierenden Festplatten erweitert nur die Größe der Festplatte. Im Betriebssystem selbst müssen Sie die jeweilige Partition um diesen neuen Bereich vergrößern. Bei Windows 2003 können Sie das mit `diskpart.exe` durchführen, sofern es sich nicht um die Bootpartition handelt. In diesem Fall müssen Sie auf Tools von Drittherstellern zurückgreifen oder die Boot-Festplatte als eine weitere Platte an eine andere Windows 2003-VM anhängen und dort erweitern. Ab Windows 2008 können Sie, auch für Boot-Partitionen, bequem das Disk Management im Server Manager verwenden. Bei Linux setzen Sie den Befehl `fdisk` ein.

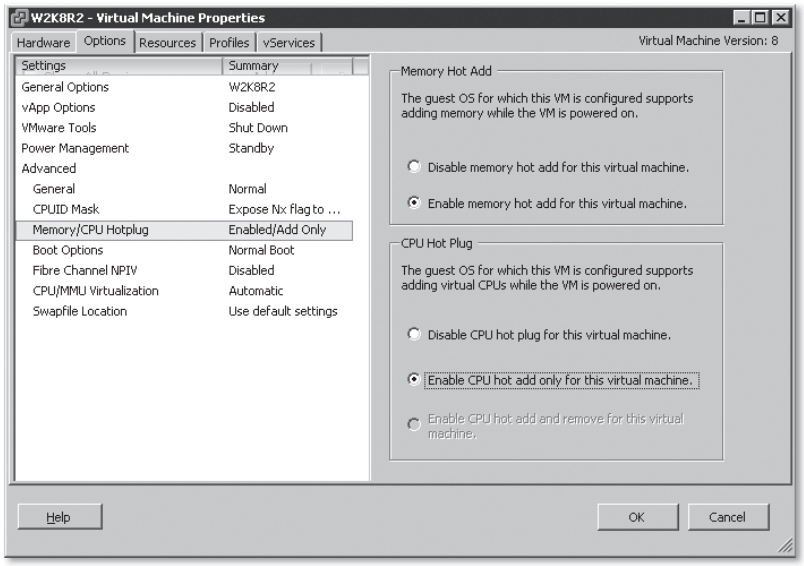


Abbildung 15.35 Aktivierung der Hot-Add-Funktionalität pro virtueller Maschine

15.10.3 Statische MAC-Adresse über GUI

Sie können die MAC-Adresse einer VM über den vSphere-Client statisch setzen. In den Eigenschaften einer VM wählen Sie die Netzwerkkarte aus und klicken dann auf MANUAL; jetzt können Sie die letzten sechs Stellen der MAC-Adresse frei editieren. Der manuell nutzbare MAC Adressbereich liegt im Bereich von 00:50:56:00:00:00 bis 00:50:56:3F:FF:FF.

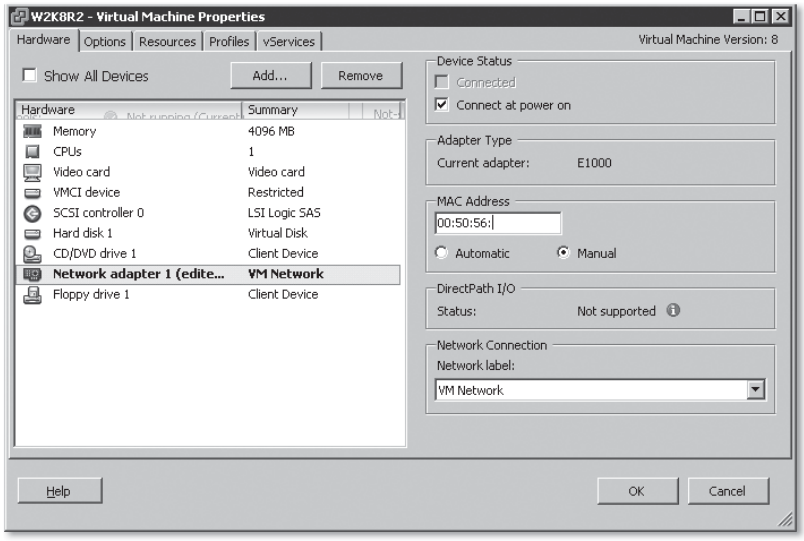


Abbildung 15.36 Optional vergeben Sie manuell eine MAC-Adresse.

Diese manuelle Vergabe stellt einen erhöhten Verwaltungsaufwand dar, da Sie sicherstellen müssen, dass die manuell vergebenen MAC-Adressen nicht versehentlich doppelt zugewiesen werden. Sinnvoll ist dieser Einsatz beispielsweise dann, wenn eine Anwendung auf die MAC-Adresse lizenziert wurde. Wird hingegen eine physische Maschine mit solch einer Software in eine virtuelle Maschine überführt, können Sie die MAC-Adresse der physischen Maschine nicht in den Einstellungen einer VM setzen, da hier die Herstellerkennung in der MAC-Adresse bereits vorgegeben ist. Alternativ setzen Sie dann die MAC-Adresse manuell in der Netzwerkkartenkonfiguration des Gastbetriebssystems.

15.10.4 Umgang mit Wechselmedien

Einer VM können Sie Floppy- oder CD-/DVD-Laufwerke zuweisen und diese entweder mit einem physischen Laufwerk oder mit einem Image verbinden. Das physische Laufwerk kann zum einen ein physisches Laufwerk auf dem ESXi-Server sein, zum anderen ein physisches Laufwerk auf dem PC oder dem Windows-Server, auf dem die VMware Console des vSphere-Clients läuft. Das Gleiche gilt für das Image: Es kann auf einem Datastore liegen und über den ESXi-Host an das Laufwerk der VM verbunden werden oder auf einem Windows-Share und über die VMware Console des vSphere-Clients verbunden werden.

Beim Einsatz von VMware vMotion müssen Sie darauf achten, dass die zu verschiebende VM keine aktive Verbindung ihres Floppy- oder CD-/DVD-Laufwerks besitzt, egal ob zu einem physischen Laufwerk des ESXi-Servers, einem PC oder einem ISO-Image. Sollte eine Verbindung noch bestehen, lässt sich der vMotion-Vorgang nicht ausführen. Kommt VMware DRS zum Einsatz, das das Verteilen von VMs auf weniger ausgelastete ESXi-Server automatisch bis semi-automatisch durchführen will, kann ein verbundenes Floppy- oder CD-/DVD-Laufwerk innerhalb der VM diesen Mechanismus lahmlegen.

Client-Devices

Die Laufwerksverbindungen zu Client-Devices steuern Sie über die VMware Console innerhalb des vSphere-Clients. Dabei wählen Sie zwischen dem physischen Laufwerk des PCs oder Servers, auf dem der vSphere-Client läuft, und einem ISO-Image, das über ein Laufwerk des PCs erreichbar ist:

In Abbildung 15.38 sehen Sie das via Image eingebundene CD-Laufwerk mit der Möglichkeit, die Verbindung zum ISO-Image via VMware Console (Disconnect …) wieder zu unterbrechen.

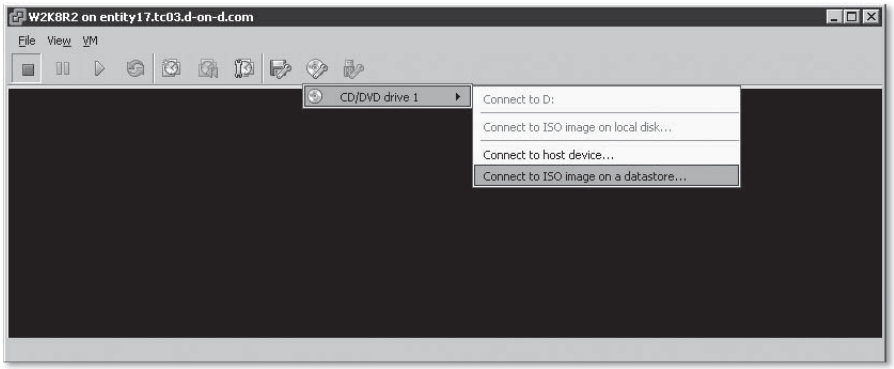


Abbildung 15.37 Das Verbinden eines CD-/DVD-Laufwerks mit einem auf einem Datastore liegenden ISO-Image

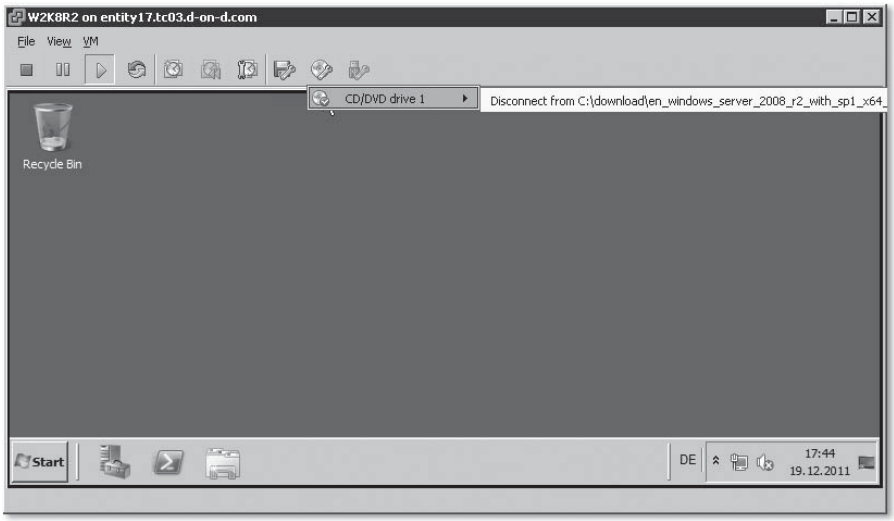


Abbildung 15.38 Verbundenes CD-/DVD-Laufwerk wieder entfernen

15.11 Optimierung einer virtuellen Maschine

Nachfolgend finden Sie einige generelle Empfehlungen, um virtuelle Maschinen optimal zu betreiben:

- Gehen Sie sparsam mit Remote-Konsole-Verbindungen um, denn diese verbrauchen CPU-Zeit, auch wenn keine Interaktion stattfindet.
- Seien Sie ebenfalls sparsam bei virtuellen CPUs, da nicht jedes System alle CPUs auch optimal ausnutzt und vSMP durch seinen Virtualisierungs-Overhead weitere Ressourcen des ESXi-Servers verbraucht.

- Die zugewiesene RAM-Menge sollte sich nach der wirklich benötigten Menge des Servers und seiner Applikationen richten. Eine sparsame Vergabe von RAM verhindert das Memory-Overcommitment, das selbst zwar mehr RAM zur Verfügung stellt, als ein ESXi-Server physisch bietet, aber eben auch weitere CPU-Zeit des ESXi-Servers zur Bereitstellung des Speichers benötigt. Je nach Applikationen bringt eine Erhöhung des Speichers einer VM nicht unbedingt mehr Leistung. Auch existieren Anwendungen (SQL Server, Exchange Server), die jeden verfügbaren Speicher allokieren, aber nicht unbedingt dadurch performanter werden.
- Zur Optimierung der VM-Performance können Sie CPU-Reservierungen vergeben, um das buchstäbliche Verhungern einer VM zu vermeiden. Ebenso sollten Sie aber auch den Einsatz von CPU-Maximum bedenken, um weniger wichtige Server-Systeme bei der Gier nach CPU-Zeit zu zügeln.
- Ein weiterer wichtiger Aspekt ist die virtuelle Hardware einer VM. Virtuelle Hardware, die von der VM nicht benötigt wird, sollten Sie aus dem System entfernen. Dazu gehören CD-/DVD-Laufwerke, Floppy-Laufwerke, nicht benötigte Netzwerkkarten, serielle und parallele Schnittstellen. Auch sollten verbundene ISO-Images der Wechselmedien nicht verbunden sein, wenn sie nicht benötigt werden.
- Weitere Optimierung erreichen Sie durch den Einsatz der VMware Tools. Achten Sie darauf, dass Sie möglichst die aktuellste Version verwenden. Ausführliche Informationen über die VMware Tools erhalten Sie in Abschnitt 15.12, »VMware Tools«.

Je nach eingesetztem Gastbetriebssystem gibt es verschiedene Möglichkeiten, das Betriebssystem selbst zu tunen. Dies gilt nicht nur für den Einsatz als virtuelle Maschinen, auch physische Server freuen sich über diese Art von Administratoren-Aufmerksamkeit.

Windows

- Defragmentierung der Festplatten
- Aktivierung des Write-through-Cache der Festplatte (im Gerätemanager, in den Eigenschaften der Festplatte, auf dem Reiter Policies)
- Deaktivierung von nicht benötigten Diensten
- Deaktivierung von visuellen Desktop- und Mauseffekten und Entfernung von Hintergrundbildern
- Deaktivierung von Screensavern

Linux

- Verwendung eines Kernels ab der Version 2.4
- keine Verwendung von X-Windows
- nur Installation benötigter Packages
- eventuell Optimierung des Kernels

- Deaktivierung von nicht benötigten Diensten, Daemons und Hintergrund-Tasks
- eventuell Einsatz der VMI-Paravirtualisierung

15.12 VMware Tools

Die VMware Tools sind eine Ansammlung von Treibern und Tools speziell für virtuelle Maschinen. Dabei bieten die spezifischen Treiber eine optimale Performance für die VM, und die Tools erleichtern die Verwaltung einer VM. Diese Tools stehen für Windows-Betriebssysteme, Linux, Solaris, FreeBSD, Mac OS X sowie für NetWare zur Verfügung und sollten idealerweise grundsätzlich installiert werden. Zwar ist das Betriebssystem in der VM auch ohne VMware Tools lauffähig, aber die Empfehlung ist, die VMware Tools zu installieren und auch regelmäßig bei Erscheinen einer neueren Version zu aktualisieren.

Die VMware Tools ermöglichen oder bieten:

- optimierte Treiber für die virtuelle Hardware
- Synchronisierung der Uhr einer VM
- Shutdown- oder Restart-Power-State-Operationen (Skripte, die bei diesen Operationen gestartet werden)
- Drag & Drop zwischen der VM und dem Betriebssystem, auf dem die VMware Console läuft
- automatische Freigabe des Cursors/Fokus beim Verlassen der VM mit der Maus in der VMware Console
- erweiterte Speicherverwaltung seitens des ESXi-Servers durch den Memory-Control-Driver
- absturzkonsistente Snapshots durch den Filesystem Sync Driver

Die Tools werden bei der Installation als ISO-Image im Gastbetriebssystem bereitgestellt, und die Setup-Routine startet automatisch. Der VMware venter ist zuständig für das Einbinden des ISO-Images innerhalb der VM in das virtuelle CD-/DVD-Laufwerk.

Die VMware Tools umfassen:

- **VMware Tools Service**
  Unter Windows wird der Dienst *vmtoolsd.exe* installiert, unter Mac OS X *vmware-tools-daemon* und unter Linux/Solaris der Dämon *vmware-gust*. Dieser Service ist die Grundlage für die Zeitsynchronisation und der VM-Heartbeat zwischen ESXi-Server und dem Gastbetriebssystem, er steuert die Skripte, die durch Power-Aktionen initiiert werden, und steuert auch die Bildschirmauflösung des Gastes in der Console. Unter Windows ist der Service außerdem für das Mausverhalten in der VMware Console zuständig sowie für die sogenannten Quiesced Snapshots.

- **VMware-Gerätetreiber**
  Für das Gastbetriebssystem werden optimierte Treiber für die virtuelle Hardware bereitgestellt, der SVGA-Bildschirmtreiber, der VMXNET-Netzwerkkartentreiber, der BusLogic-SCSI-Treiber, der paravirtualisierte SCSI-Treiber und die Treiber für Maus, Audio sowie das Shared-Folder-Feature. Des Weiteren werden ein Memory-Treiber und ein Synchronisierungstreiber installiert.
- **VMware Tools Toolbox**
  Die Toolbox dient zum Ändern von Einstellungen, zum Verkleinern der virtuellen Disk und zum Verwalten der virtuellen Geräte (Floppy, CD-ROM).
- **VMware Scripts**
  Verschiedene Skripte, die bei Power-State-Änderungen der VM im Gastbetriebssystem ausgeführt werden. Die Ausführung wird über die Eigenschaften einer VM gesteuert.
- **VMware-User-Prozess**
  Auf Windows-Betriebssystemen wird die *VMwareUser.exe* installiert und auf Linux und Solaris-Betriebssystemen der *vmware-user*-Prozess. Dieser Prozess ermöglicht u. a. Copy & Paste und Drag & Drop zwischen dem Gast und dem Betriebssystem, auf dem die VMware Console ausgeführt wird.

15.12.1 Zeitsynchronisation

Die Zeitsynchronisation einer VM ist die einzige Möglichkeit einer VM, die korrekte Zeit zu erhalten, da eine VM über keine CMOS-Uhr verfügt. Natürlich existieren etliche betriebssystemeigene Methoden, um die Uhrzeit abzugleichen, z. B. Windows-Server, die als Mitglieder einer Domäne immer die korrekte Zeit von einem Windows-Zeitgeber erhalten. Auch nach einem Suspend muss die Uhrzeit der VM aktualisiert werden, da sie während des Suspendierens ebenso angehalten wurde.

Sollten Sie Microsoft-Domain-Controller virtualisieren, dann empfiehlt sich auf jeden Fall die Verwendung der Windows-eigenen Zeitsynchronisierung und keine Vergabe der Zeit via VMware. Ansonsten ist die Zeitvergabe über die VMware Tools der empfohlene Weg, sofern die ESXi-Server mit einer externen Zeit via NTP konfiguriert wurden.

15.12.2 Installation der VMware Tools

Die Installation der VMware Tools kann zum einen manuell nach der Installation des Gastbetriebssystems oder auch als unbeaufsichtigte Variante durchgeführt werden. Das vCenter kann die VMware Tools beim Starten der VM überprüfen und gegebenenfalls eigenständig aktualisieren.

15.12.3 Manuelle Installation

Die manuelle Installation starten Sie über den Befehl INSTALL VMWARE TOOLS entweder über das Kontextmenü der VM oder über das Hauptmenü unter INVENTORY • VIRTUAL MACHINE. Dadurch wird an das Laufwerk des Gastbetriebssystems ein ISO-Image angehängt, und das Setup wird gestartet. Nachfolgend beschreiben wir die Installationsvorgänge für Linux, Solaris und Windows.

Linux

Mounten Sie zuerst die CD und entpacken Sie das TAR-Archiv, danach können Sie die VMware Tools wie gewohnt installieren (`x.x.x.` gibt die Versionsnummer an, `yyyy` die Build-Nummer):

```
mount -t iso9660 /dev/cdrom /mnt/cdrom
tar -xvfz /mnt/cdrom/VMwareTools-x.x.x-yyyy.tar.gz
cd vmware-tools-distrib
./vmware-install.pl
```

Um die korrekte Installation der VMware Tools zu überprüfen, werfen Sie einen Blick in das SUMMARY einer virtuellen Maschine im vSphere-Client. Dort sollte der Status der VMware Tools mit OK angezeigt werden.

Solaris

Die Installation erfolgt bei Solaris immer über ein TAR-Archiv.

```
mount -t iso9660 /dev/cdrom /mnt/cdrom
cp /cdrom/vmwaretools/VMwareTools-solaris.tar.gz /tmp
cd /tmp
gunzip ./vmwaretools/VMwareTools-solaris.tar.gz
tar -xvf VMwareTools-solaris.tar
./vmware-tools-distrib/vmware-install.pl
```

Hinweis: Ein textbasiertes Setup leitet durch die Installation der Treiber.

Windows

1. Nach dem Startbildschirm entscheiden Sie sich für den Installationstyp: TYPISCH, VOLLSTÄNDIG oder BENUTZERDEFINIERT.
2. Wählen Sie unter BENUTZERDEFINIERT die zu installierenden Komponenten (Abbildung 15.39).
3. Installieren Sie die VMware Tools.
4. Nach Abschluss der Installation booten Sie die virtuelle Maschine.

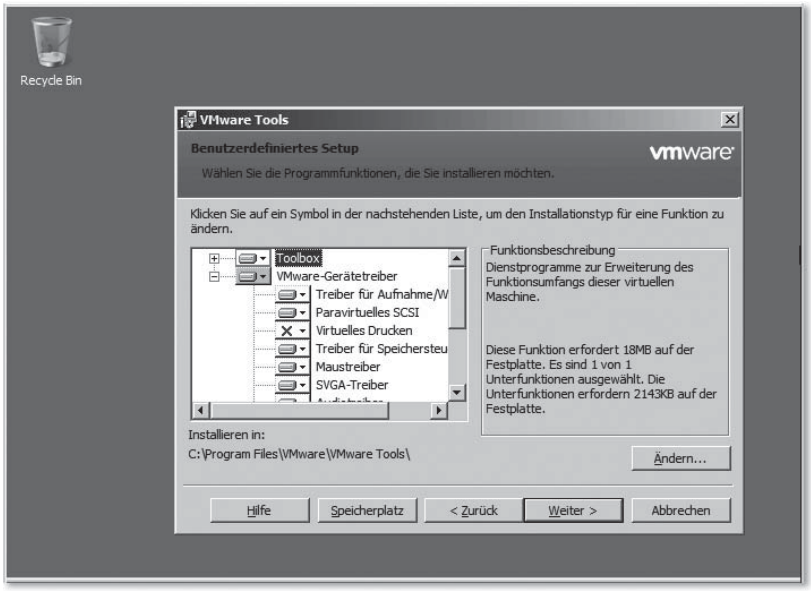


Abbildung 15.39 Auswahl der zu installierenden Komponenten

Um die korrekte Installation der VMware Tools zu überprüfen, werfen Sie einen Blick in das SUMMARY einer virtuellen Maschine im vSphere-Client. Dort sollte der Status der VMware Tools mit OK angezeigt werden.

15.12.4 Aktualisierung der VMware Tools

Eine neue Version der VMware Tools gelangt in Form von Patches auf den ESX-Host, und der vSphere-Client zeigt pro VM den Status der VMware Tools an. Veraltete VMware Tools werden im SUMMARY einer VM mit einem OUT OF DATE gekennzeichnet.

Manuell

Die Aktualisierung der VMware Tools auf eine neue Version nehmen Sie analog zur Installation vor. Im ersten Schritt geben Sie an, ob vCenter für Sie das Upgrade automatisiert vornehmen soll oder ob Sie den Wizard manuell füttern möchten, um die zu installierenden Komponenten ändern zu können.

Automatisiert durch vCenter

Das vCenter unterstützt das automatische Aktualisieren der VMware Tools. Dazu aktivieren Sie in den Eigenschaften einer VM im Reiter OPTIONS unter VMWARE TOOLS den Befehl CHECK AND UPGRADE TOOLS DURING POWER CYCLING (Abbildung 15.41). Bei jedem Einschalten der VM wird jetzt überprüft, ob eine neue Version der VMware Tools zur Verfügung steht, und diese dann automatisch installiert.

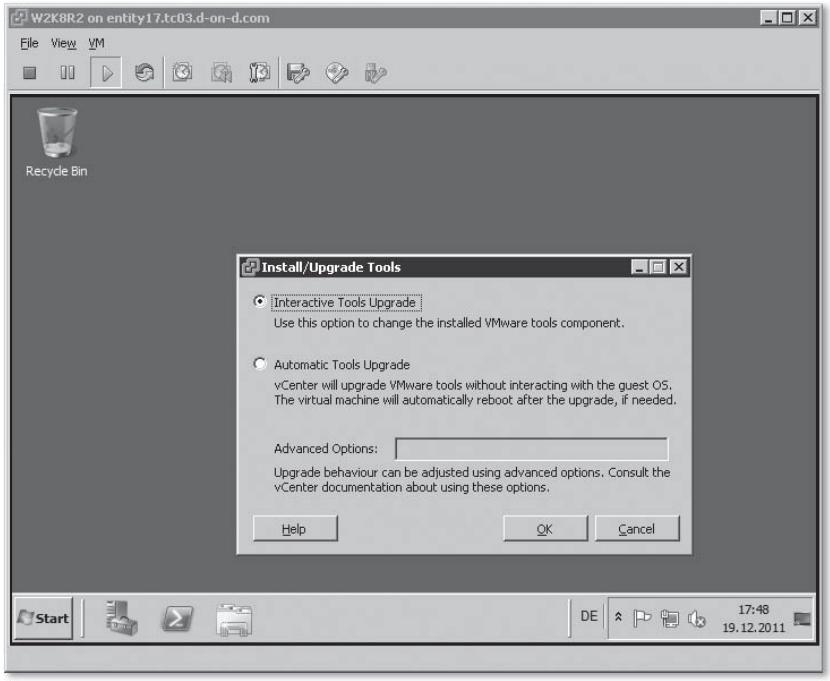


Abbildung 15.40 Upgrade der VMware Tools

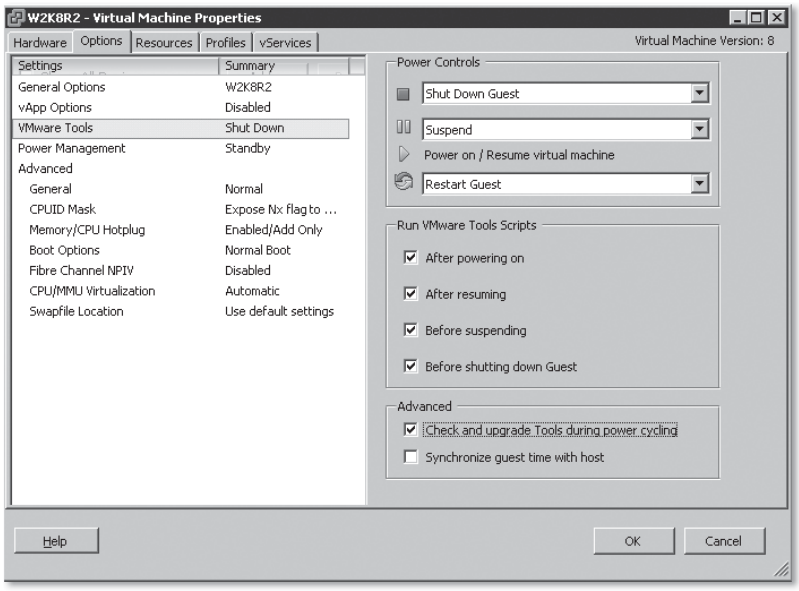


Abbildung 15.41 vCenter überprüft und aktualisiert die VMware Tools eigenständig.

15.13 Migration von virtuellen Maschinen

15.13.1 Verschiedene Arten der Migration

Die Migration einer VM ist das Verschieben einer virtuellen Maschine von einem ESXi-Server auf einen anderen ESXi-Server. Dabei wird unterschieden, ob die VM eingeschaltet oder ausgeschaltet bzw. suspendiert ist. Abschließend wird die verschobene VM auf dem Ziel-ESXi-Server registriert und kann dort gestartet werden.

Das Verschieben einer eingeschalteten VM wird *vMotion* genannt und setzt zum einen voraus, dass die Dateien der VM (Konfiguration, virtuelle Festplatte etc.) auf einem gemeinsam genutzten Storage-Bereich (via iSCSI, SAN oder NFS) abgelegt sind. Zum anderen müssen Sie die CPU-Kompatibilität der ESXi-Server beachten. Bei vMotion wird die VM ohne Unterbrechung im Gastbetriebssystem vom Ursprungs-ESXi-Server live auf einen anderen ESXi-Server verschoben. Die VM-Dateien bleiben dabei an ihrem aktuellen Speicherort liegen.

Zur Durchführung des vMotion-Vorgangs einer VM muss sichergestellt sein, dass die VM keine Verbindung zu einem CD-ROM oder einem Floppy-Laufwerk des ESXi-Hosts besitzt. Bei der Validierung des Ziels wird dies als Fehler angezeigt. Eine Verbindung zu einem Client-Device oder einem ISO-Image stellt kein Hindernis für vMotion dar.

Das Verschieben der eingeschalteten VM kann mit unterschiedlichem Prioritätslevel erfolgen, HIGH PRIORITY und STANDARD PRIORITY. Die Einstellung HIGH PRIORITY stellt sicher, dass auf dem Ziel-Server ausreichend Ressourcen zur Verfügung stehen, und reserviert diese, damit die VM während der Migration verfügbar ist. Hat der ESXi-Server nicht ausreichend Ressourcen, wird die Migration nicht durchgeführt. Die Einstellung STANDARD PRIORITY reserviert keine Ressourcen auf dem Ziel und führt die Migration auch bei Ressourcenengpässen durch. Dabei kann es vorkommen, dass die VM kurzzeitig nicht zu erreichen ist.

Eine ausgeschaltete oder auch suspendierte VM muss nicht zwingend auf einem zentralen Storage liegen und bedingt auch keine CPU-Kompatibilität der ESXi-Server. Hierbei lassen sich die VMs auch zwischen Datacentern verschieben. Vor dem endgültigen Verschieben der VM können Sie wählen, ob die Dateien einer VM ebenfalls verschoben werden oder ob sie am bisherigen Speicherplatz liegen bleiben (sofern sie auf einem zentral verfügbaren Speicherbereich abgelegt wurden). Damit der Speicherort der VM-Dateien bei einer Migration nicht verändert wird, muss sich dieser auf einem zentralen Storage befinden, damit der Ziel-ESXi-Server die Dateien auch im Zugriff haben kann.

Das Feature Storage vMotion ermöglicht die Live-Migration einer VM zwischen verschiedenen Datastores. Dabei erfolgt Storage vMotion auf einem ESXi-Server; die Dateien einer VM werden von einem Datastore auf einen anderen verschoben, ohne dass der Betrieb einer VM unterbrochen werden muss. Diese Art der Migration ist sinnvoll, um z. B. alle VMs eines Datastores zu verschieben und nachfolgend an diesem Datastore Wartungsarbeiten durchführen zu können. Abschließend können die verschobenen VMs wieder zurück auf den ursprünglichen Datastore verschoben werden. Ein weiterer Verwendungszeck ist die optimale Last-

verteilung zwischen verschiedenen Datastores ohne Ausfall der darauf liegenden VMs. Der ESXi-Server benötigt für diese Migration ebenfalls eine vMotion-Lizenz und sollte ausreichend Ressourcen für zwei Instanzen der zu verschiebenden VM bereitstellen.

15.13.2 Verwendung des Migration-Wizards zur Migration einer VM

Das Verschieben einer virtuellen Maschine starten Sie über den vSphere-Client mittels des Migration-Wizards. Diesen rufen Sie vom Menü oder Kontextmenü einer VM über den Befehl Migrate auf. Die Schritte des Wizards variieren je nach Art der Migration und je nach Ziel.

Den Migration-Wizard können Sie auch über Drag & Drop starten. Lassen Sie dabei die VM auf einem ESXi-Host, einem Cluster oder einem Resource-Pool fallen. Je nach Ziel wird der Schritt Select Destination nicht mehr angezeigt, da die Auswahl schon getroffen wurde, z. B. wenn das Ziel ein ESXi-Server ist oder ein Resource-Pool, der einem ESXi-Host zugeordnet wurde. Eine detaillierte Beschreibung und Anleitung finden Sie in Kapitel 4, »vMotion und Storage vMotion«.

15.14 Templates und Clones

15.14.1 Was sind Templates, und welchen Nutzen bringen sie?

Unter Templates versteht man Vorlagen oder Vorlagendateien, die dazu dienen, bei der Erstellung z. B. eines neuen Word-Dokumentes Zeit einzusparen. Das ist jedoch nicht alles: Sie grenzen auch Fehlerquellen ein oder beseitigen sie, indem sie – um beim Word-Beispiel zu bleiben – sich wiederholende Textpassagen in eine Vorlage speichern und mittels dieser immer wieder neue Dokumente erstellen. Natürlich hat dies auch den entscheidenden Nachteil, dass bei einem Fehler in der Vorlage alle darauf basierenden Dokumente ebenfalls von diesem Fehler befallen sind. Aber es gibt nur eine Fehlerquelle, nämlich einzig und allein die Vorlage selbst. Daher sollten Sie auch bei der Anlage des ersten Templates äußerst sorgfältig vorgehen, um spätere Probleme schon im Voraus auszuschließen.

Mittlerweile hat man dieses doch sehr nützliche Verfahren nicht nur bei Word oder allgemeinen Dokumenten eingebracht, sondern auch in Form von Images für physische Maschinen, z. B. durch Symantec Ghost. Dort installiert man ein Betriebssystem mit allen benötigten Anwendungen, löscht die individuellen Einstellungen wie die Netzwerkkonfiguration und sichert diese Daten in einem Image. Mit diesem Image werden dann alle weiteren Systeme deutlich schneller und fehlerfreier installiert, als es manuell möglich wäre. Einen großen Nachteil hat dieses Verfahren, zumindest bei physischen Maschinen: Es läuft nur bei identischer Hardwarekonfiguration sicher und fehlerfrei.

Virtuelle Maschinen passen durch die immer gleiche virtuelle Hardware allerdings perfekt in den Mechanismus von Templates. Hinzu kommt, dass meistens nur eine Datei (die Festplattendatei des Betriebssystems) benötigt wird und nicht einmal ein Imaging-Tool eingesetzt

werden muss, um ein Image herzustellen, denn Sie haben dieses automatisch, sobald die virtuelle Maschine fertig installiert ist. Daher empfiehlt es sich auch, die System- und Datenpartition einer VM zu trennen und als unterschiedliche Festplattendateien anzulegen.

Wenn wir diesen Gedanken weiterspinnen, kommen wir sehr schnell darauf, dass nicht nur ein Template, sondern viele verschiedene Templates erstellt und hinterlegt werden können, die verschiedenste Betriebssysteme mit unterschiedlichsten Softwareständen und Service Packs enthalten. Dadurch lassen sich in kürzester Zeit – bei guter Festplattenleistung in ca. 15 Minuten – neue virtuelle Maschinen auf der Basis eines Templates erstellen. Diesen Vorgang könnten Sie sogar noch automatisieren, um beispielsweise eine Test- oder Entwicklungsumgebung regelmäßig neu aufzusetzen. Aber vor allem das Disaster-Recovery wird durch Templates sehr verbessert, da Sie mehrere Templates für die einzelnen Service-Pack-Stände Ihrer virtuellen Maschinen hinterlegen und sie je nach ausgefallenem System entsprechend »zurücksichern« können. So schnell können Sie kein physisches System in seinem Ursprungszustand wiederherstellen.

15.14.2 Templates im vCenter

Unter VMware ist ein Template genau das, was man von ihm erwartet: eine komplette Kopie einer virtuellen Maschine. Dabei ist es Ihnen überlassen, ob Sie nur das reine Gastbetriebssystem inklusive der aktuellen Patches installiert haben oder auch eine Anzahl von Applikationen. Dieses Template verwenden Sie, um schnell und ohne weiteres Wissen über die VM-Spezifikation neue virtuelle Maschinen des gleichen Typs ins Leben zu rufen.

Die Templates sind ebenso wie die virtuellen Maschinen im vCenter sichtbar und lassen sich auch mit den gleichen Hilfsmitteln gruppieren, indem Sie sie in Foldern zusammenfassen oder auch mit Zugriffsrechten belegen. Um die Templates von den virtuellen Maschinen zu unterscheiden, haben die Template in der Darstellung im Inventory des vSphere-Clients leicht abgeänderte Icons. Eine zusätzliche Kennzeichnung, z. B. mit *_Template*, schadet sicher nicht, um einen Überblick über die virtuelle Infrastruktur zu behalten. Alternativ können Sie auch alle Templates in einem Ordner ablegen.

15.14.3 Templates erstellen, bearbeiten und löschen

Zum Erstellen von Templates können Sie zwischen folgenden Vorgehensweisen wählen:

- eine virtuelle Maschine in ein Template konvertieren
- eine virtuelle Maschine in ein Template clonen
- ein existierendes Template in ein neues Template clonen

Die ersten zwei Möglichkeiten wandeln entweder eine existierende virtuelle Maschine in ein Template um (Convert to Template) oder kopieren eine virtuelle Maschine in ein Template (Clone to Template).

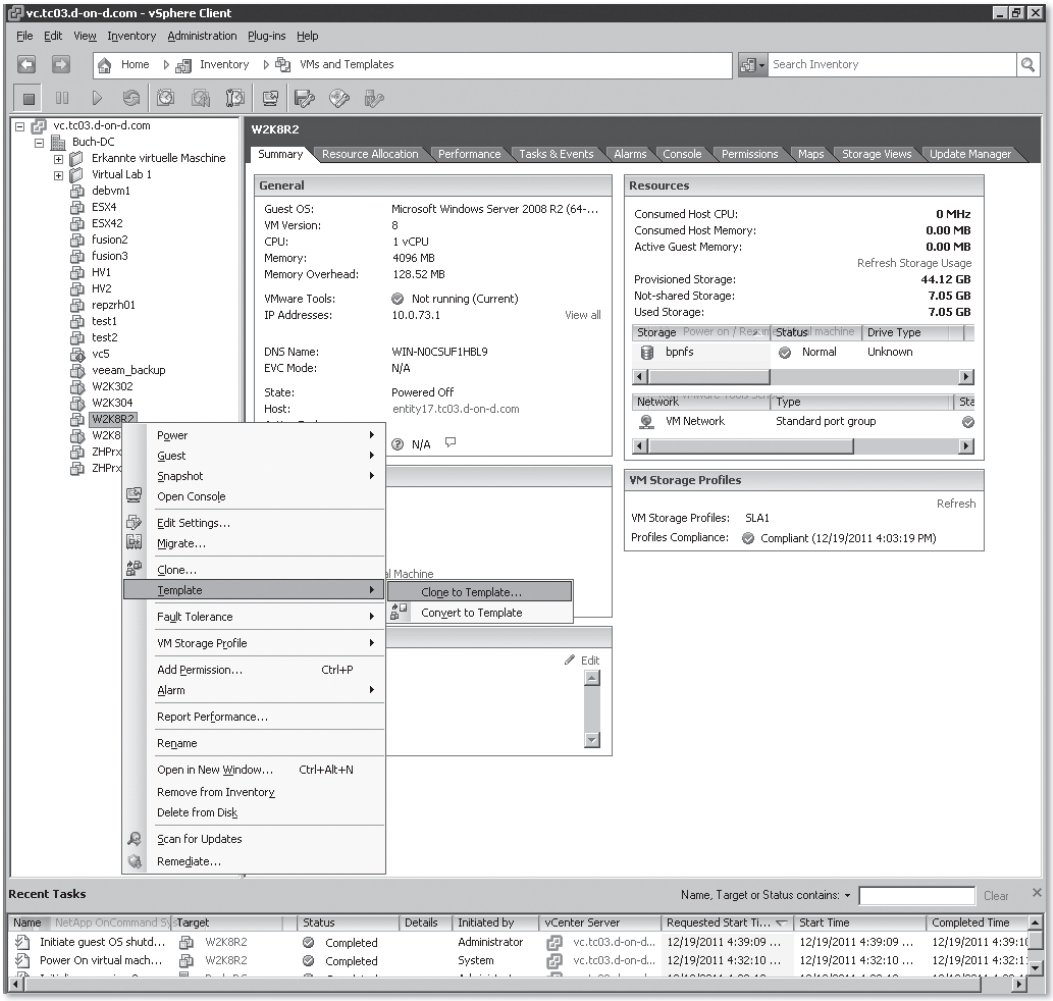


Abbildung 15.42 Zwei Möglichkeiten, aus einer VM ein Template zu erstellen

Bei CLONE TO TEMPLATE wird eine Kopie der ausgewählten virtuellen Maschine erstellt. Dabei vergeben Sie für das Template einen Namen, wählen einen Zielordner aus, selektieren den ESXi-Host und wählen den Datastore aus.

Bei CONVERT TO TEMPLATE hingegen wandeln Sie eine bestehende virtuelle Maschine in ein Template um.

15.14.4 Virtuelle Maschinen mit Hilfe von Templates erstellen

Das Deployment von virtuellen Maschinen erfolgt in der Regel durch DEPLOY VIRTUAL MACHINE FROM THIS TEMPLATE aus dem Kontextmenü eines Templates. Alternativ wandeln Sie

ein Template in eine virtuelle Maschine um. Im Deployment-Prozess werden Sie nach dem Namen der neuen virtuellen Maschine gefragt, nach dem Ziel-Host oder -Cluster, gegebenenfalls nach einem Resource-Pool und dem Datastore, auf dem die Dateien abgelegt werden sollen. Der letzte Schritt des Wizards bietet Ihnen wieder die Gelegenheit, den GUEST CUSTOMIZATION-Wizard aufzurufen. (Eine Beschreibung des GUEST CUSTOMIZATION-Wizards finden Sie im folgenden Abschnitt.)

Geben Sie dem vCenter nach diesen Einstellungen einen Moment Zeit, um die Dateien des Templates in eine neue virtuelle Maschine zu kopieren und das Betriebssystem zu modifizieren.

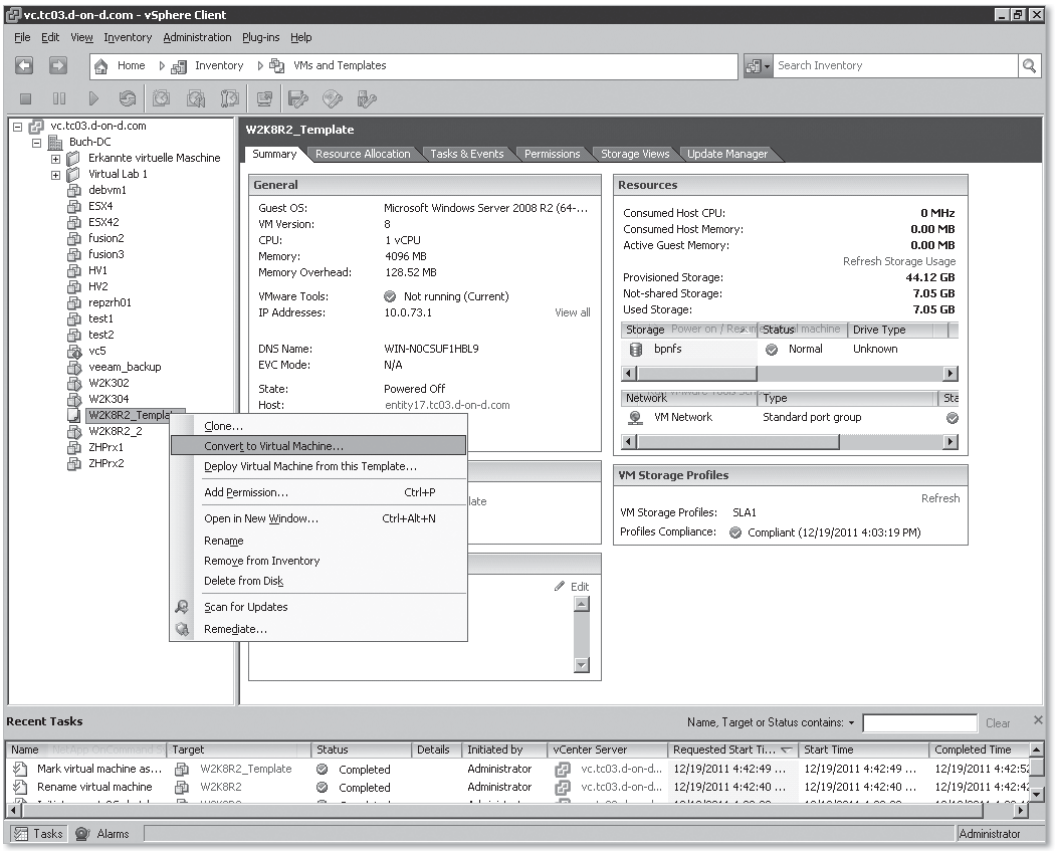


Abbildung 15.43 Zwei Wege, aus einem Template eine VM zu erstellen

15.14.5 Was sind Clones, und wie erstellt man sie?

Ein Clone ist eine direkte Kopie einer bestimmten virtuellen Maschine mit der Möglichkeit, das Gastbetriebssystem der Kopie am Ende des Vorgangs anzupassen. Sie starten den Vorgang durch Auswahl des Befehls CLONE aus dem Kontextmenü einer virtuellen Maschine.

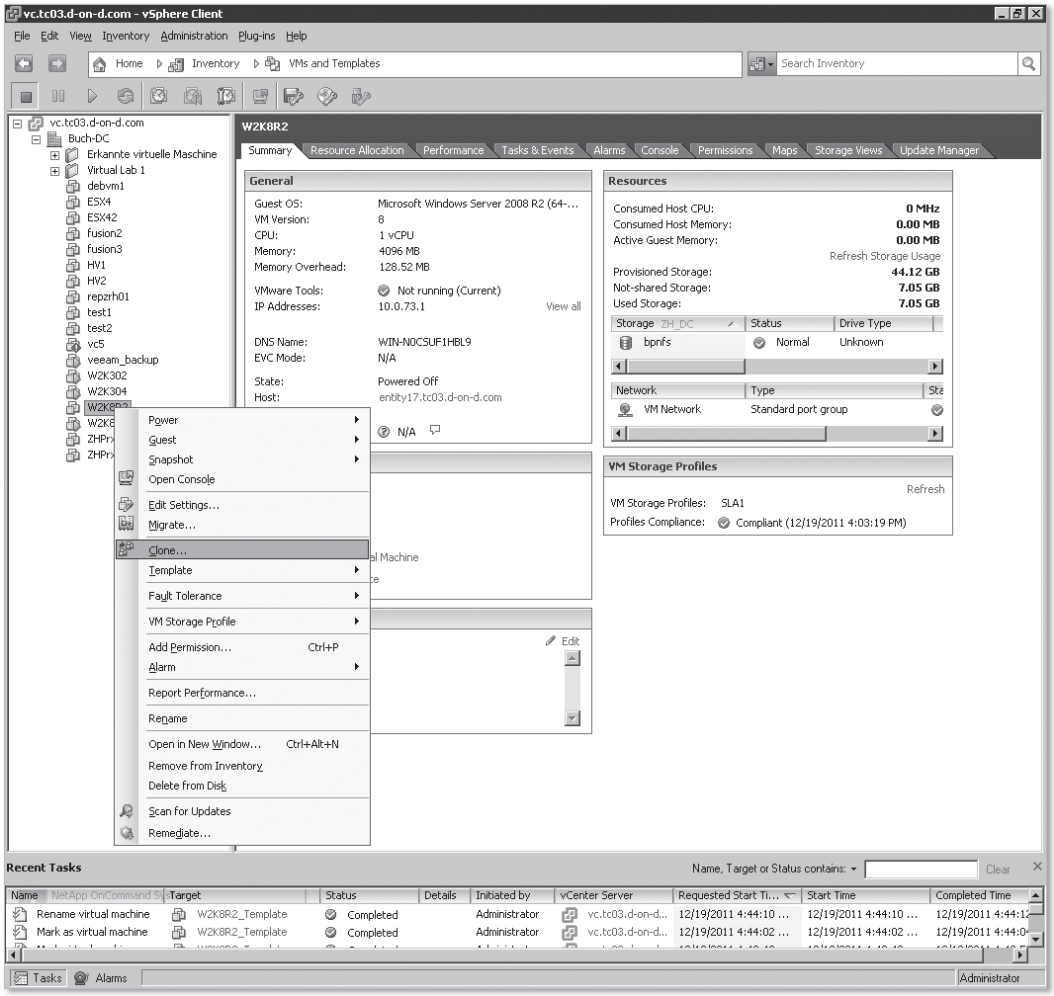


Abbildung 15.44 Eine virtuelle Maschine clonen

Nach dem Start des Clone-Wizards geben Sie für den Clone an, wie er benannt werden soll und in welcher Folder-Struktur er abgelegt werden soll. Zusätzlich wählen Sie den Ziel-ESXi-Server, gegebenenfalls einen Resource-Pool und den Datastore aus. Am Ende legen Sie fest, ob das vCenter das Gastbetriebssystem des Clones bearbeiten soll.

Geben Sie dem vCenter nach diesen Einstellungen einen Moment Zeit, um die Dateien der virtuellen Maschine zu kopieren und das Betriebssystem zu modifizieren.

15.15 Anpassen der Gastbetriebssysteme

Mit dem Guest Customization-Wizard passen Sie die Gastbetriebssysteme Windows (ab 2003) oder Linux (RHEL 2-5, SLES 8-10) während des Deployment-Vorgangs an. Dabei können Sie z. B. den Host-Namen oder die Netzwerkkarten-Konfiguration verändern.

Speziell für Windows bietet dieser Wizard die Möglichkeit, der neuen VM eine neue SID zu geben. Dieser Computer Security Identifier (SID) kennzeichnet verschiedene Windows-Systeme im Netzwerk und sollte bei Deployment-Prozessen, die auf dem Imaging-Verfahren beruhen, für jede neue Windows-Installation verändert werden. Letzteres war bis November 2009 die gängige Meinung aller Windows-Experten und wurde auch so seit Windows-NT-Zeiten für Image-based Deployment-Prozesse gelebt. Doch der Entwickler des Tools *NewSID*, Mark Russinovich, erschütterte am 3. November 2009 die IT-Jünger schwer, als er das Tool *NewSID* als »retired« kennzeichnete und dabei in seinem Blog dem Mythos der *Machine SID Duplication* ein Ende bereitete. Möge ein jeder sich selbst darüber informieren: *http://blogs.technet.com/markrussinovich/archive/2009/11/03/329 1024.aspx*

Den Guest Customization-Wizard rufen Sie am Ende von Cloning- oder Deployment-Prozessen auf. Entweder tragen Sie alle gewünschten Änderungen Schritt für Schritt in den Wizard ein, oder Sie wählen aus der Datenbank des Customization Specifications Managers eine Spezifikation aus.

15.15.1 Voraussetzungen

Der Wizard setzt in beiden Fällen (Windows und Linux) voraus, dass die VMware Tools in der virtuellen Maschine installiert sind. Speziell für Windows wird die Installation des Microsoft-Tools *Sysprep* auf dem vCenter und für Linux im Gastbetriebssystem eine Perl-Installation benötigt.

Sysprep

Für die Anpassung von Windows-Betriebssystemen stellt Microsoft das Tool Sysprep bereit. Microsoft bietet es für die Betriebssysteme Windows XP, Windows Server 2000–2003, jeweils 32 und 64 Bit, an. Sie finden die jeweilige Version für Ihr Gastbetriebssystem auf Microsofts TechNet. Das Microsoft-Tool muss mit all seinen Dateien im jeweiligen Unterverzeichnis in *%ALLUSERSPROFILE%\VMware\VMware VirtualCenter\sysprep* liegen.

Für Windows 2008 sowie für Vista wird das Tool nicht auf dem vCenter benötigt, da es bereits im Betriebssystem enthalten ist. Des Weiteren werden die Einstellungen jetzt über eine XML-Datei geregelt, die vom vCenter vor dem Anpassen des Gastbetriebssystems auf den Gast kopiert wird. In der Community häufen sich jedoch die Meldungen, dass die vollständige Anpassung eines Windows 2008-Servers oft fehlschlägt. Ein einfacher Workaround ist, vor dem Umwandeln der Windows Server 2008-VM die Betriebssystemeinstellung in »Vista« zu ändern. Nachdem Sie von diesem Template eine VM erstellt haben und die Anpassungen im

Betriebssystem fehlerfrei durchgeführt wurden, ändern Sie in der virtuellen Maschine die Angabe des Gastbetriebssystems wieder in »Windows Server 2008«.

Sollten Sie Probleme mit der Anpassung des Gastbetriebssystems haben, finden Sie detaillierte Informationen in folgenden Log-Dateien:

- Windows: *%WINDIR%\temp\vmware-imc*
- Linux: */var/log/vmware/customization.log*

15.15.2 Bearbeiten von Anpassungsspezifikationen

Sie starten den Customization Specifications Manager im vSphere-Client über VIEW • MANAGEMENT • CUSTOMIZATION SPECIFICATIONS MANAGER (siehe Abbildung 15.45) oder über die Adressleiste.

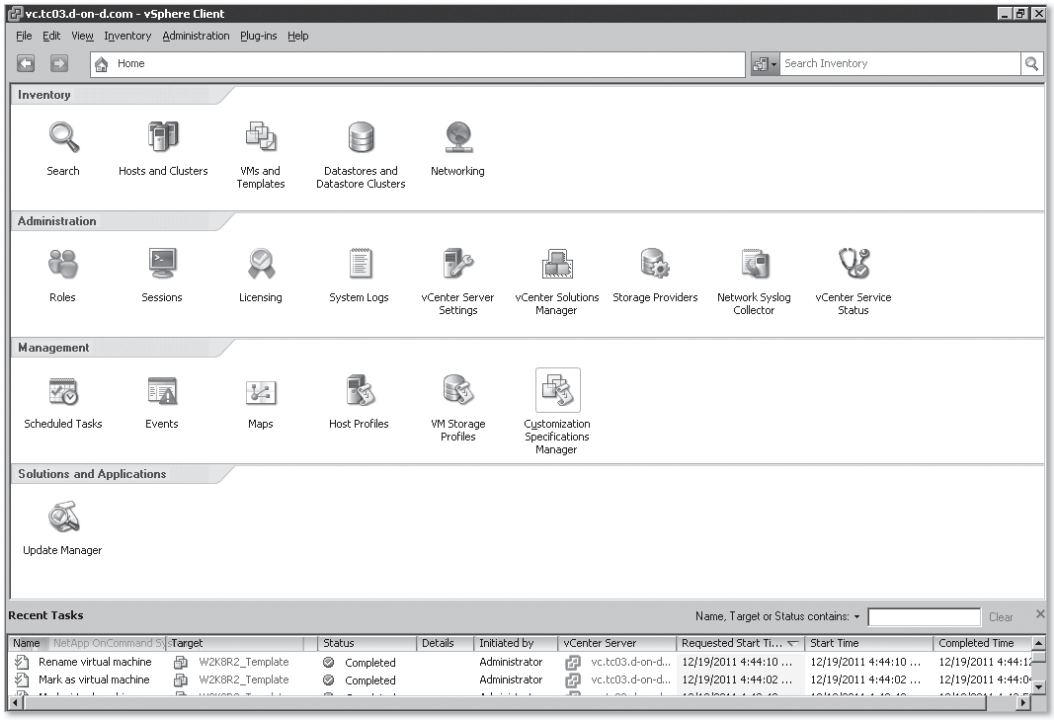


Abbildung 15.45 Starten des Customization Specifications Managers

Dort können Sie jetzt neue Spezifikationen erstellen oder importieren sowie bestehende Spezifikationen duplizieren, bearbeiten, exportieren oder löschen.

Das Erstellen oder Bearbeiten einer Spezifikation sieht wie folgt aus:

1. Wählen Sie das Gastbetriebssystem aus (Windows oder Linux).
2. Geben Sie die obligatorischen Registrierungsinformationen an.
3. Wählen Sie, wie der Host-Name der virtuellen Maschine vergeben werden soll:
   - Sie geben einen festen Namen ein.
   - Der Name der virtuellen Maschine soll als Host-Name übernommen werden.
   - Der Name wird durch den Anwender eingegeben.
   - Der Name wird von einem externen Tool vergeben.

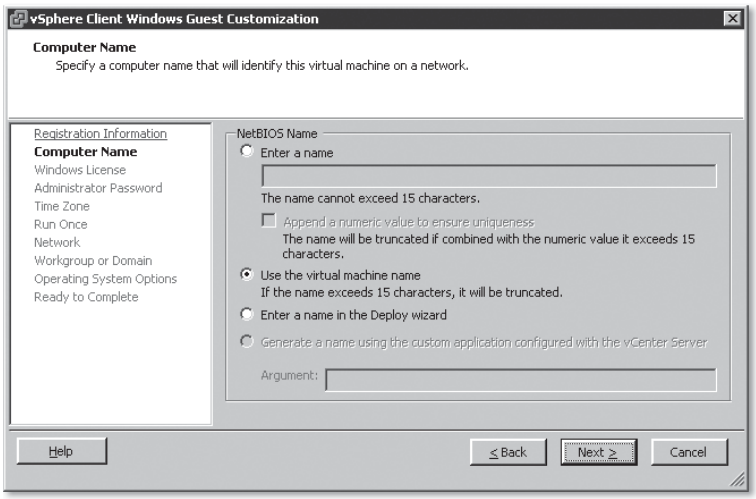


Abbildung 15.46 Setzen des Host-Namens

4. Nur in Windows-Systemen geben Sie jetzt den Product-Key ein und hinterlegen die Lizenzinformationen.
5. Ebenfalls nur in Windows-Systemen geben Sie ein Administratorkennwort ein und bestimmen, wie viele automatisierte Anmeldevorgänge nach der Installation durchgeführt werden sollen.
6. Legen Sie die Zeitzone fest.
7. Wiederum nur für Windows-Systeme können Sie Run-once-Skripte angeben.
8. Bei der Netzwerkkartenkonfiguration wählen Sie zwischen der typischen Einstellung, der Verwendung von DHCP für alle Netzwerkkarten und der angepassten Einstellung. Letzteres ermöglicht Ihnen, für die virtuelle Maschine entweder eine feste IP-Adresse im Wizard zu hinterlegen oder dem Anwender die Möglichkeit zu geben, eine IP-Adresse anzugeben.
9. Entscheiden Sie für Windows-Systeme, ob sie einer Workgroup oder einer Domäne angehören sollen, und hinterlegen Sie den Account, um diese Aktion durchzuführen.

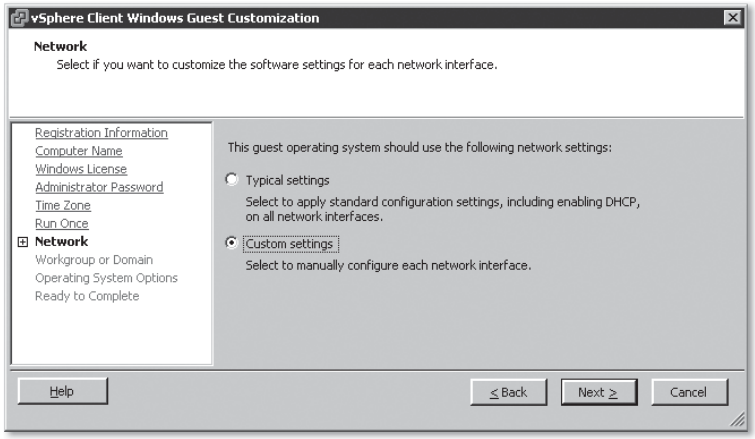


Abbildung 15.47 Mit Hilfe der »Custom settings« legen Sie …

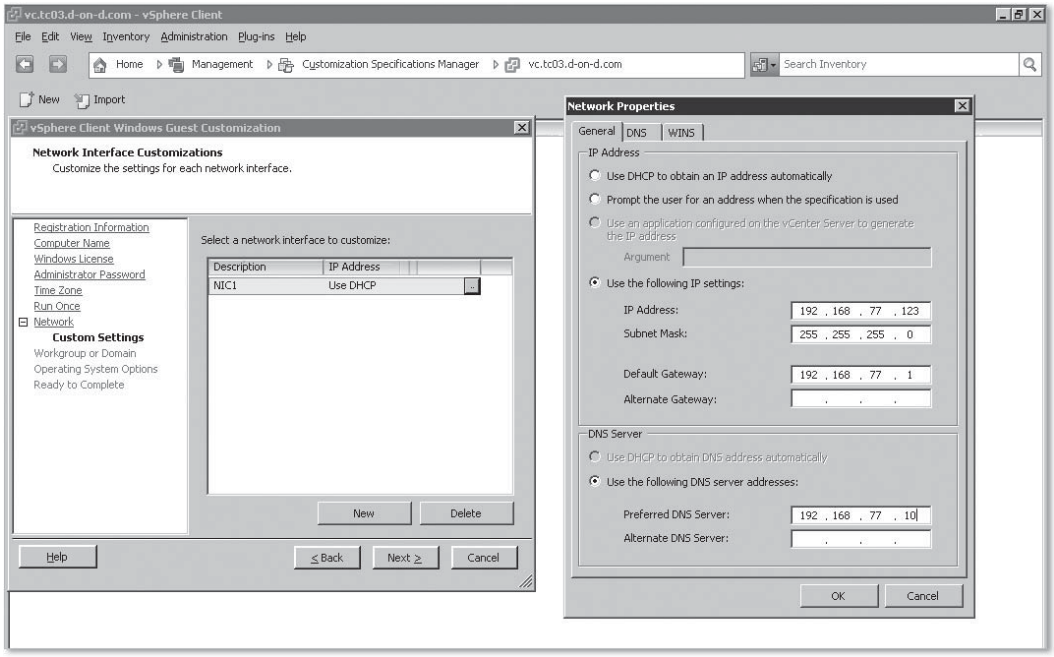


Abbildung 15.48 … die IP-Adressen der VM und des DNS-Servers fest.

10. Die letzte Einstellung gilt wiederum nur für Windows-Systeme und automatisiert die Vergabe einer neuen SID.

Der letzte Schritt des Wizards fasst nochmals alle Informationen auf einen Blick zusammen.

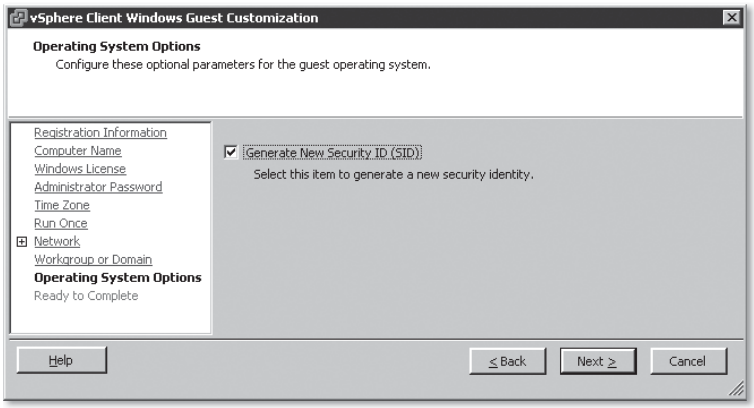


Abbildung 15.49 Soll für das Windows-System eine neue SID erstellt werden?

15.15.3 Anpassung des Gastbetriebssystems

Die Anpassung eines Gastbetriebssystems wird entweder am Ende eines Clone-Vorgangs gestartet oder durch das Deployment einer virtuellen Maschine mittels Templates. Dabei bekommen Sie jeweils im letzten Schritt des Wizards die Möglichkeit, den Customization-Wizard zu starten.

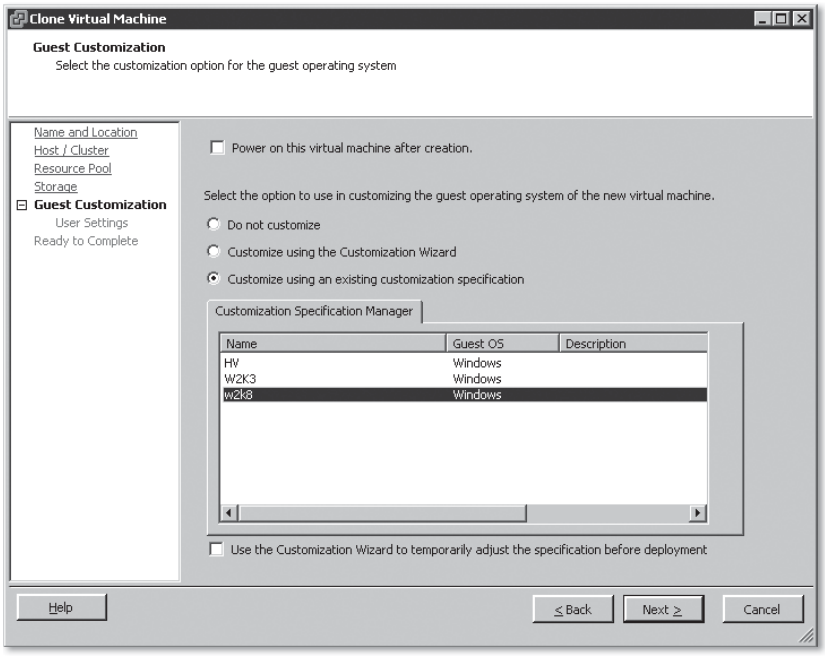


Abbildung 15.50 Anpassung einer neuen virtuellen Maschine am Ende eines Clone-Vorgangs mittels gespeicherter Spezifikationen

Dabei stehen Ihnen zwei Optionen zur Verfügung: Bei Customize using the Customization Wizard legen Sie die Einstellungen für das Betriebssystem in den folgenden Schritten des Wizards fest. Eine vorher erstellte und abgespeicherte Konfiguration wählen Sie bei Customize using an existing customization specification aus. Hierbei können Sie außerdem angeben, ob Sie gewisse Bereiche der ausgewählten Konfiguration vor dem Anwenden noch abändern möchten.

15.16 Snapshots

15.16.1 Funktionsweise

Ein Snapshot erstellt eine Momentaufnahme einer virtuellen Maschine inklusive des Gastbetriebssystems. Dabei werden je nach Art des Snapshots der aktuelle Zustand der virtuellen Festplatte(n), die Eigenschaften der VM sowie der aktuelle Zustand des RAMs eingefroren und im Verzeichnis der VM auf dem Datastore abgelegt. Sie können zu jedem Zeitpunkt wieder zu einem beliebigen Snapshot zurückspringen, womit alle Änderungen und Einstellungen, die in der VM seit Erstellung des Snapshots erfolgten, obsolet sind. Dies ist das ideale Werkzeug, um die Installation neuer Software oder Konfigurationsänderungen zuerst zu testen. Der Zustand einer VM nach einem Snapshot, z. B. nach der erfolgreichen Installation einer neuen Software, kann als fester Zustand wieder persistiert werden. Dabei werden alle Änderungen der VM, d. h. insbesondere der virtuellen Festplatte, auf die ursprüngliche Festplatte übertragen, und die Snapshot-Dateien werden gelöscht. Somit enthält die Festplattendatei den zum jetzigen Zeitpunkt gültigen Zustand einer VM.

Die Erstellung von mehreren Snapshots der gleichen VM ist möglich. Damit wird jeder Zwischenschritt, z. B. während einer Installation mehrerer Softwarepakete oder Updates, abgelegt und dient als eine Art Recovery-Point. Sie können zu einem beliebigen Snapshot innerhalb der Hierarchie zurückspringen und alle Änderungen, die seit der Erstellung dieses bestimmten Snapshots gemacht wurden, verwerfen. Im Gegensatz dazu kann auch jeder beliebige Zustand persistiert werden. In Summe ist eine Hierarchietiefe von 32 Stufen möglich. Bedenken Sie, dass mit jedem neuen Level die Zeit zum Verwerfen oder zum Persistieren eines Snapshots ansteigt.

Bei der Erstellung eines Snapshots wird der in diesem Moment gültige Zustand einer VM eingefroren. Bei primär schreibenden Applikationen, z. B. Datenbank-Servern, ist zwar während der Erstellung des Snapshots die volle Funktionalität der Anwendung gegeben. Aber beim Zurücksetzen einer VM auf einen Snapshot kann es zu Inkonsistenzen kommen, wenn während der Erstellung schreibende Operationen durchgeführt wurden. Hier empfiehlt es sich, die jeweiligen Dienste oder Anwendungen zu stoppen, bevor Sie einen Snapshot erstellen. Bei Domänen-Controllern wird aber grundsätzlich davon abgeraten, Snapshots anzuwenden, da Sie sonst mit USN-Rollback-Problemen zu kämpfen haben (*http://support.microsoft.com/kb/875495*)! Die Performance einer VM wird nach der Erstellung eines Snapshots eventuell

beeinträchtigt, da alle Änderungen im Gastbetriebssystem respektive in der virtuellen Festplatte in einer weiteren Datei auf dem Datastore gespeichert werden.

Kurzübersicht der Snapshot-Manager-Befehle:

- Delete
  Dieser Befehl fügt den ausgewählten Snapshot dem Parent-Snapshot (übergeordneter Snapshot) hinzu und löscht die Snapshot-Datei. Der Inhalt der VM-Festplatte bleibt unverändert.
- Delete All
  Dieser Befehl fügt alle Snapshots vor dem »You Are Here«-Status dem Parent-Snapshot hinzu und löscht alle Snapshot-Dateien. Der Inhalt der VM-Festplatte bleibt unverändert.
- Go To
  Dieser Befehl setzt den Inhalt der virtuellen Festplatte in den ausgewählten Zustand zurück, das heißt, der Inhalt der VM-Festplatte wird auf einen vorherigen Stand gebracht.
- Revert To Snapshot
  Dieser Befehl setzt den Inhalt der virtuellen Festplatte auf den Parent-Snapshot zurück, der Inhalt der VM-Festplatte wird also auf einen vorherigen Stand verändert.

15.16.2 Snapshot-Dateien auf dem Datastore

Nach der Erstellung eines Snapshots werden auf dem Datastore im Verzeichnis der virtuellen Maschine mehrere Dateien erstellt. Hier eine Beschreibung der wichtigsten Dateien:

- VMSN-Datei
  Diese Datei existiert pro Snapshot und enthält die Konfiguration einer VM zu dem Zeitpunkt, als der Snapshot erstellt wurde. Diese Datei ist lesbar und beinhaltet im Wesentlichen die Einstellungen der VMX-Datei.

  Die Nummer des Snapshots wird im Dateinamen angezeigt, z. B.:

  VM_NAME-Snapshot1.vmsn → erster Snapshot
  VM_NAME-Snapshot2.vmsn → zweiter Snapshot
- VMSD-Datei
  Diese Datei existiert pro VM einmalig und speichert die Definitionen vorhandener Snapshots einer VM.
- -NNN.VMDK-Datei
  Diese Datei existiert pro Snapshot und enthält die Änderungen der virtuellen Festplatte. Über den Inhalt der VMSD-Datei wird eine VMDK-Datei mit einer laufenden Nummer einem bestimmten Snapshot zugeordnet.

  Die fortlaufende Nummer erzeugt Dateinamen ähnlich dieser:

  - *VM_NAME-000001.vmdk*
  - *VM_NAME-000002.vmdk*

15.16.3 Hilfe bei Problemen

Wenn Sie mit Snapshots Probleme haben, z. B. wenn sie sich nicht mehr löschen oder zusammenführen lassen, dann finden Sie im Blog von Dennis Zimmer einen guten Artikel, der die gängigen Snapshot-Probleme und deren Lösung beschreibt:

http://www.vmachine.de/cms/index.php/de/component/content/article/1/655-wenn-snapshots-zur-qual-werden

15.16.4 Die Snapshot-Hierarchie

Mit Hilfe des Snapshot-Managers können Sie alle Snapshots einer VM einsehen und komfortabel verwalten, d. h. bestimmte Zustände persistieren oder verwerfen. Der Snapshot-Manager zeigt den Hierarchiebaum an und stellt die Beziehungen der Snapshots zueinander dar:

Jeder Snapshot hat einen direkten Parent-Snapshot und, sofern er nicht der letzte in der Hierarchie ist, einen direkten Child-Snapshot. Ein Snapshot kann mehrere Child-Snapshots haben. Aus dieser Hierarchie können Sie einen bestimmten Snapshot auswählen und zu diesem zurückspringen, d. h. den Zustand der VM basierend auf diesem Snapshot wiederherstellen. Dabei werden alle vorhandene Child-Snapshots entfernt. Das Persistieren von Snapshots hat zur Folge, dass alle vorherigen Snapshots gelöscht und die differenten VMDK-Daten in die VMDK-Datei eingefügt werden.

Beispiel: Ein neuer Server VRZMD01 wird mit SQL 2008 R2 Server und dem IIS (Internet Information Server) installiert. Abschließend werden alle Datenbanken von einem bestehenden SQL-Server migriert. Die untenstehenden Screenshots dokumentieren das Leid des Administrators, da sehr viele Probleme dabei auftreten. Zum Glück ist es nicht immer so.

1. Das Betriebssystem inklusive der aktuellen Patches und diversen Agenten des neuen Servers »W2K8R2_2« wurde installiert und von dieser Grundinstallation ein Snapshot erstellt. Sollte in einem nachfolgenden Schritt etwas schiefgehen, können Sie jederzeit zu diesem Ausgangspunkt zurückkehren (Abbildung 15.51).

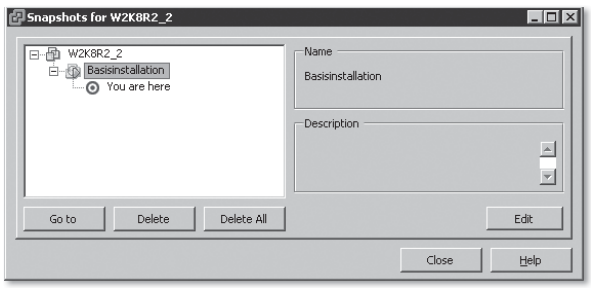


Abbildung 15.51 Erster Snapshot nach der Grundinstallation

2. Im nächsten Schritt installieren Sie den IIS und erstellen die virtuellen Verzeichnisse und verschiedene Application-Pools (Abbildung 15.52).

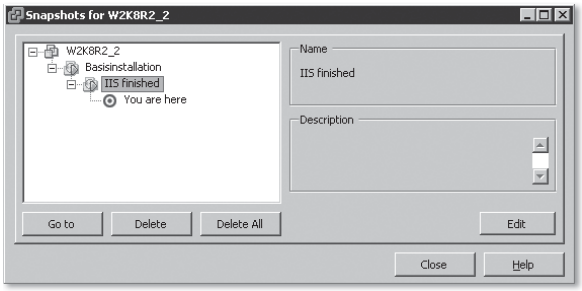


Abbildung 15.52 Snapshot nach der IIS-Installation

3. Nach der Erstellung des letzten Snapshots wurde der SQL Server 2008 R2 installiert, doch die Installation brach aus unerklärlichen Gründen ab und hinterließ Fragmente auf dem Server. Wählen Sie den letzten Snapshot aus (Button Go to), um die Installation erneut zu wagen (Abbildung 15.53).

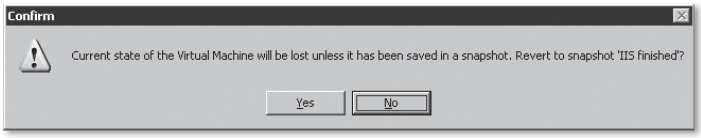


Abbildung 15.53 SQL-Installation schlug fehl; einen Schritt zurückgehen.

4. Jetzt ist die Installation des SQL-Servers geglückt, und die Datenbanken wurden erfolgreich migriert. Zu diesem Zeitpunkt können Sie alle Snapshots löschen (Abbildung 15.54).

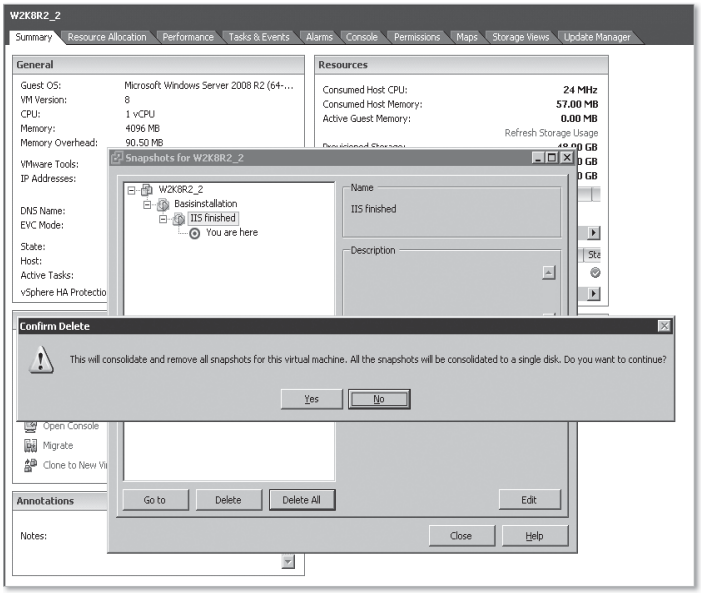


Abbildung 15.54 Löschen aller Snapshots

15.16.5 Das Erstellen eines Snapshots (Take Snapshot)

Das Erstellen eines Snapshots erfolgt am einfachsten über den vSphere-Client. Je größer das RAM der virtuellen Maschine und je höher die Last des ESXi-Servers, desto länger dauert die Erstellung eines Snapshots. Ein Snapshot kann bei jedem beliebigen Power-State einer virtuellen Maschine durchgeführt werden, also im eingeschalteten Zustand – dann mit RAM-Inhalt –, im ausgeschalteten Zustand oder im suspendierten Zustand.

Nach der Auswahl der VM im vSphere-Client rufen Sie entweder im Kontextmenü den Befehl Snapshot • Take Snapshot auf, oder Sie gehen über das Menü Inventory • Virtual Machine des vSphere-Clients. Zur eindeutigen Identifikation des Snapshots geben Sie einen Namen an, z. B. »PreSQLSETUP«. Optional geben Sie noch eine erklärende Beschreibung dazu ab. Nach dem Klick auf OK startet der Snapshot-Vorgang, und Sie können den Fortschrittsgrad im Fenster Recent Tasks überwachen.

15.16.6 Das Persistieren eines Snapshots (Delete Snapshot)

Ein wenig missverständlich sind die zwei Schalter Delete und Delete All im Snapshot Manager. Hinter diesen Befehlen verbirgt sich das Persistieren der seit der Erstellung eines Snapshots aufgelaufenen Änderungen an der virtuellen Disk in die physische Datei mit anschließendem Löschen aller Snapshot-Dateien – kurz, als wenn nie ein Snapshot erstellt wurde. Nach diesem Vorgang ist ein *revert* zu diesen Snapshot nicht mehr möglich, da er nicht mehr existiert.

Sie können im Snapshot Manager einzelne Snapshots auswählen und löschen, aber eine sehr schnelle Möglichkeit, alle Snapshots einer virtuellen Maschine zu löschen und somit den aktuellen Zustand der virtuellen Maschine in die Dateien zu persistieren, ist der Schalter Delete All.

Hinweis

Das Löschen von Snapshots ist im vSphere-Client nur über den Snapshot-Manager möglich.

15.16.7 Das Verwerfen des aktuellen Zustands oder die Wiederherstellung eines Snapshots (Revert to Snapshot)

Auch beim Verwerfen des aktuellen Zustands oder Wiederherstellen eines Snapshots führt der einfachste Weg über den vSphere-Client. Sie haben drei Möglichkeiten, um den direkten Vorgänger-Snapshot wiederherzustellen:

- Hinter dem Menüpunkt Inventory • Virtual Machine • Snapshot klicken Sie den Button Revert to Current Snapshot. Im Kontextmenü der VM finden Sie unter Snapshot ebenfalls den Befehl Revert to Current Snapshot.
- Klicken Sie auf den Button Revert to Current Snapshot in der Toolbar.

Jeder dieser Wege stellt den Parent-Snapshot einer virtuellen Maschine wieder her, also den jeweils letzten Snapshot. Wenn Sie die VM auf einen früheren Snapshot als den letzten zurücksetzen möchten, müssen Sie den Snapshot-Manager verwenden. Dieser zeigt Ihnen alle bestehenden Snapshots und bietet die Möglichkeit, bestimmte Snapshot-Zustände auszuwählen. Markieren Sie den gewünschten Snapshot, zu dessen Stand Sie springen möchten, und klicken Sie GOTO.

15.17 Die virtuelle Maschine im vSphere-Client

Der vSphere-Client bietet Ihnen über die virtuellen Maschinen eine ganze Reihe von Informationen. Wählen Sie im INVENTORY eine VM aus, und klicken Sie sich durch die Reiter:

Reiter »Summary«

Der erste Reiter, SUMMARY, bietet Ihnen eine Übersicht über die Konfiguration der virtuellen Maschine sowie der aktuell von ihr genutzten Ressourcen. Zusätzlich finden Sie Befehle, die Sie an der VM durchführen können und die Sie auch im Kontextmenü oder in der Menüleiste erreichen.

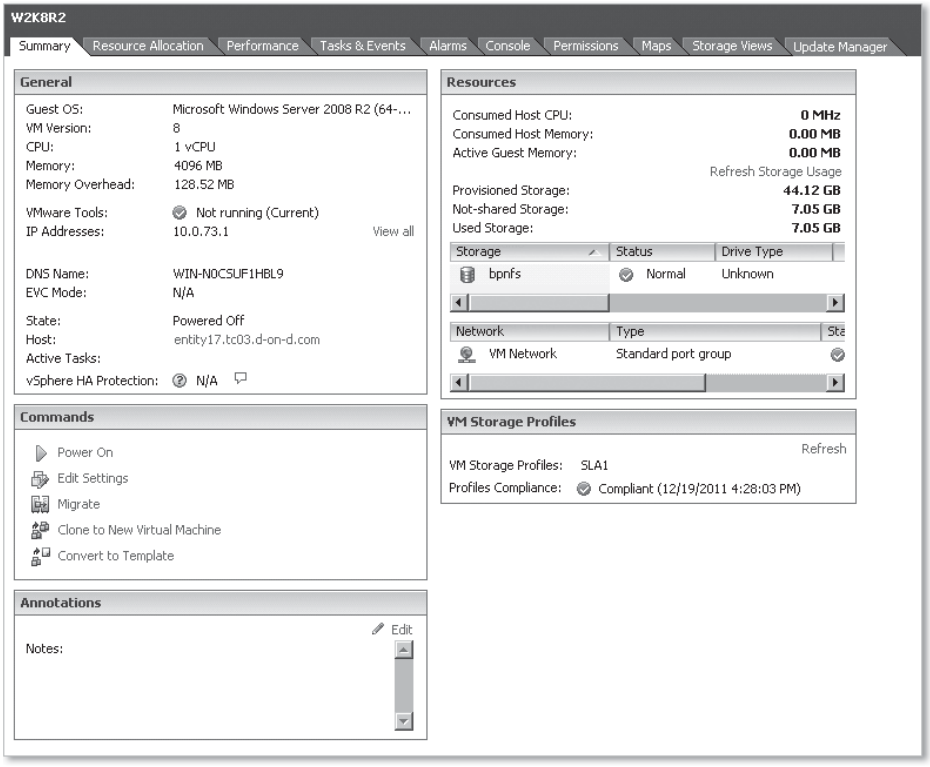


Abbildung 15.55 Die Übersichtsseite einer virtuellen Maschine

Erklärungsbedürftig wären folgende Angaben:

- Memory Overhead: der Virtualisierungs-Overhead, der auf dem ESXi-Server erzeugt wird, um diese VM zu verwalten; variiert je nach Anzahl der vCPUs, zugewiesenem Speicher und je nachdem, ob der Gast ein 32- oder 64-Bit-Betriebssystem ist
- Consumed Host CPU: auf dem ESXi-Server von der virtuellen Maschine genutzte CPU-Ressourcen in MHz
- Consumed Host Memory: auf dem ESXi-Server von der virtuellen Maschine genutzter Speicher
- Active Guest Memory: der benutzte Speicher in der virtuellen Maschine
- Provisioned Storage: die der VM garantiert auf dem Datastore zugewiesene Speichermenge
- Not-shared Storage: von der VM allein genutzte Speichermenge auf dem Datastore
- Used Storage: von der VM aktuell benötigter Speicherplatz auf dem Datastore

Reiter »Resource Allocation«

Der Resource Allocation-Reiter bietet Ihnen im Vergleich zur Summary-Seite detailliertere Informationen über die CPU- und Speichernutzung Ihrer virtuellen Maschine.

Im oberen Teil des CPU-Bereichs finden Sie analog zur Summary-Seite wieder den Wert Consumed, der den aktuellen CPU-Verbrauch dieser virtuellen Maschine in MHz angibt. Zusätzlich sehen Sie den Wert Active, der für den geschätzten CPU-Verbrauch auf dem ESXi-Server in MHz dieser VM steht, sofern es keinen CPU-Ressourcenwettbewerb zwischen dieser und anderen VMs gibt. Bei der Vergabe eines CPU-Limits wird dieser Wert immer unter dem definierten Limit liegen. Im unteren Teil des Bereichs CPU sehen Sie die Werte einer eventuell eingestellten CPU-Ressourcenallokierung (zu finden in den Eigenschaften einer VM, Reiter Resources). Zusätzlich wird hier der Wert Worst Case Allocation angezeigt, der die maximal für diese VM zu vergebende CPU-Ressource in Bezug auf die physische Ausstattung des ESXi-Servers angibt. Oben im Bereich Memory finden Sie unter Host Memory wieder analog zur Übersichtsseite die Angabe Consumed, die die auf dem ESXi-Server allokierte Speichermenge für diese VM anzeigt. Der Wert Overhead Consumption informiert Sie über die aktuell benötigte Menge des für Memory-Overhead reservierten Speichers.

Der Bereich Guest Memory zeigt Ihnen die folgenden Werte an:

- Private: vom ESXi-Host für diese VM geschützte, private Speichermenge
- Shared: vom ESXi-Host mit anderen VMs gemeinsam (»shared«) benutzte Speichermenge
- Swapped: vom ESXi-Host mit Hilfe der Auslagerung in eine Swap-Datei gewonnener Speicherbereich
- Ballooned: vom ESXi-Host mit Hilfe der Ballooning-Technik von dieser VM wiedergewonnener Speicherbereich

- Unaccessed: die bislang noch nie von der VM referenzierte Speichermenge
- Active: aktuell von der VM genutzte Speichermenge des ESXi-Hosts

In der unteren Hälfte des Memory-Bereichs sehen Sie die Werte einer eventuell eingestellten Memory-Ressourcenallokierung (zu finden in den Eigenschaften einer VM, Reiter Resources). Zusätzlich gibt hier der Wert Worst Case Allocation die maximal für diese VM zu vergebende Speichermenge an, also die der VM zugewiesene Speichermenge zuzüglich der Speichermenge für den Virtualisierungs-Overhead.

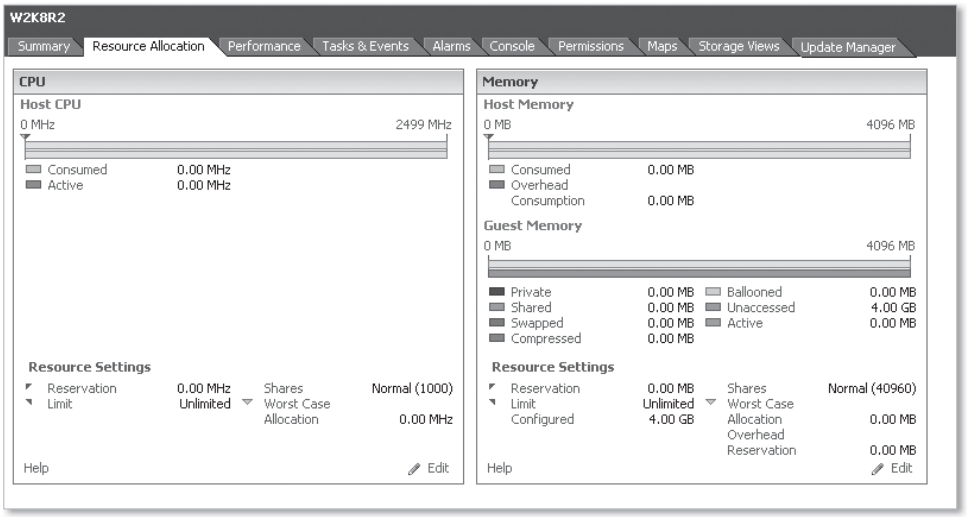


Abbildung 15.56 Die Ressourcenallokierung einer VM

Reiter »Performance«

Im Reiter Performance können Sie die Performance-Werte der Core Four (CPU, RAM, Disk, Network) einsehen – entweder in Echtzeit oder als historische Daten. Zum einen sind die Werte absolut angegeben, im Falle der CPU also in MHz, oder in Prozent, also der Anteil der von der VM genutzten Ressource.

Die Ansicht verändern Sie mit Klick auf die Combo-Box bei Switch to und wählen die Ressource aus, zu der Sie die Performancedaten sehen möchten. Zu jedem Ressourcentyp werden Ihnen vordefinierte Performancezähler angezeigt.

Möchten Sie andere Informationen von diesem Counter einsehen oder auch die vom vCenter-Server historisierten Daten, so klicken Sie auf Chart Options und konfigurieren dort Ihre Ansicht. Zu jeder Ressource können Sie die entweder Echtzeitdaten oder die historisierten Daten des letzten Tages, der letzten Woche, des letzten Monats oder des letzten Jahres anzeigen lassen. Alternativ geben Sie unter Custom einen genauen Zeitraum an. Diese Einstellungen können Sie als Chart abspeichern, um zu einem späteren Zeitpunkt Ihre Vorlage wieder zu verwenden.

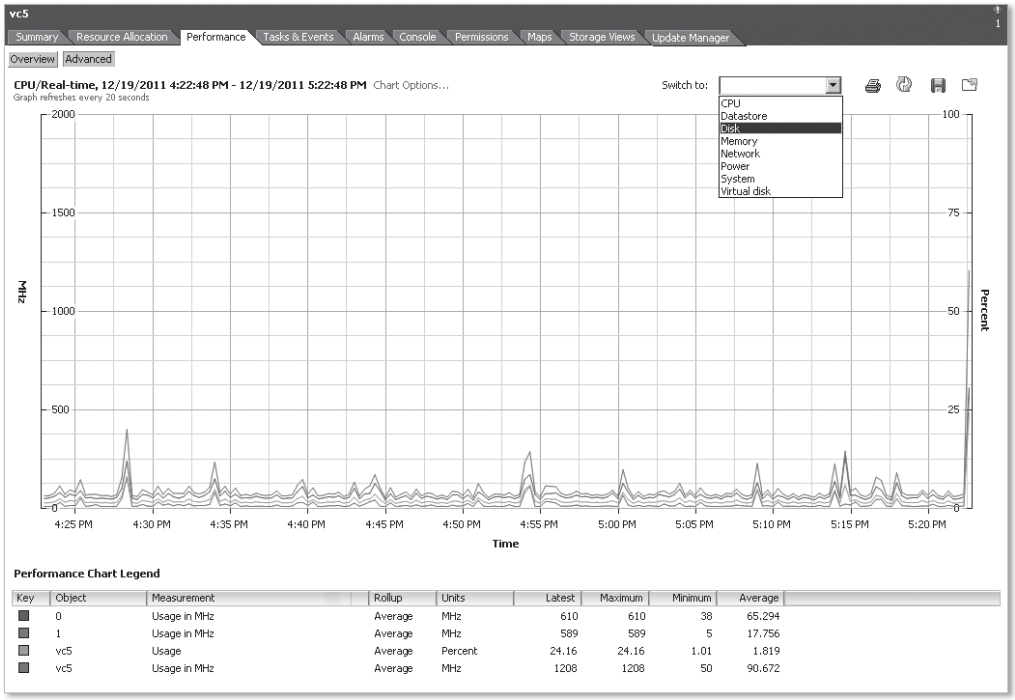


Abbildung 15.57 Ansicht der Standard-Performance-Counter

Bedenken Sie bei den historisierten Daten, dass sie über die Zeiträume hinweg geglättet dargestellt werden! So erkennen Sie z. B. bei einer Monatsansicht nicht, dass vor drei Wochen Ihr ESXi-Host für eine Stunde einen Vollausschlag gezeigt hat.

Reiter »Task & Events«

Der Reiter Task & Events zeigt Ihnen eine Übersicht von an dieser VM durchgeführten Aktivitäten (Tasks) an oder von Ereignissen (Events), die zu dieser VM aufgetreten sind. Wählen Sie in der Übersicht einen Task oder ein Event aus, so erhalten Sie im unteren Fensterbereich detaillierte Informationen dazu.

Die Listen können Sie nach allen Kriterien, die Sie in der Übersicht sehen, sortieren (z. B. nach Datum, nach Name, nach Status).

Reiter »Alarms«

Unter Alarms können Sie zum einen Alarmdefinitionen hinterlegen und zum anderen alle zu dieser VM aufgetretenen Alarme einsehen. Ein Alarm wird beispielsweise ausgelöst durch zu hohe Ressourcenauslastung oder durch Fehler bei Migrationen (vMotion). Ein ausgelöster Alarm kann wiederum selbst Aktionen ausführen wie das Senden eines SNMP-Traps.

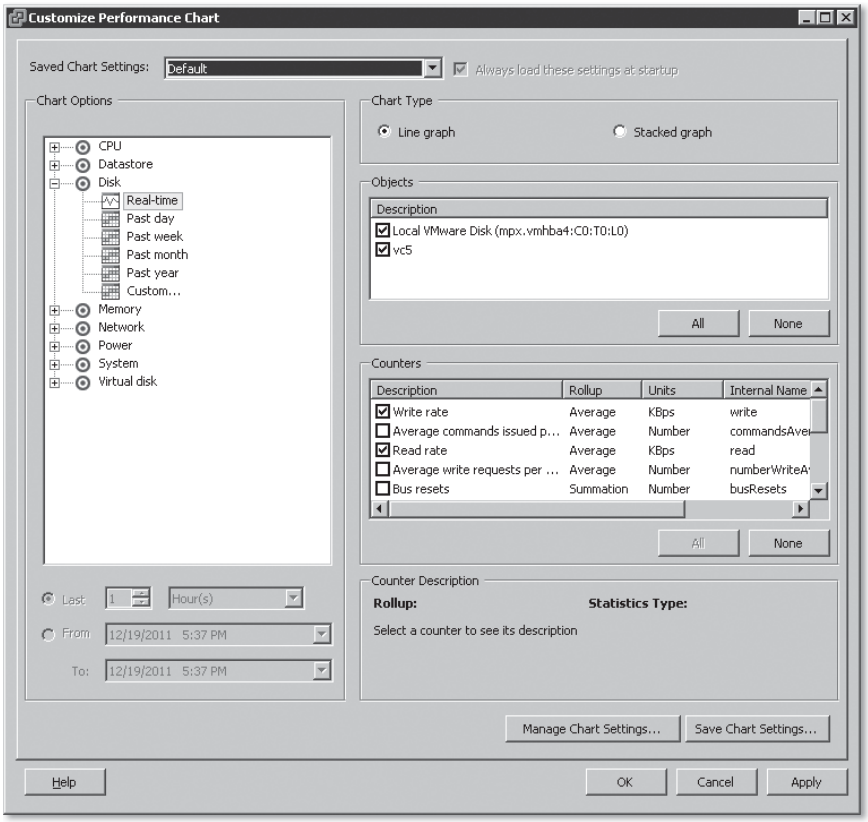


Abbildung 15.58 Die Konfiguration eigener Performance-Charts

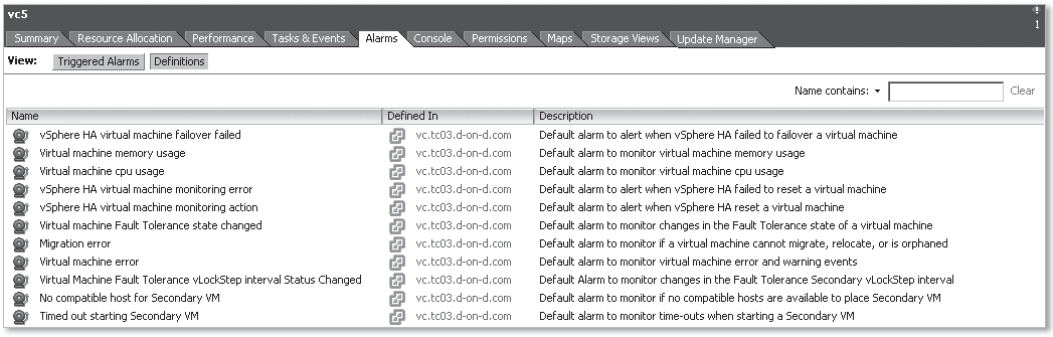


Abbildung 15.59 Die vordefinierten Alarme einer VM

Reiter »Console«

Im Reiter CONSOLE haben Sie eine direkte Sicht auf die Konsole des Betriebssystems. Sie stehen praktisch im Rechenzentrum vor diesem Server. Komfortabler stellen Sie eine Konsolen-

verbindung her, indem Sie die Remote-Konsole über das Kontextmenü einer VM starten. Hier haben Sie nicht nur die Konsole in einem eigenen Fenster, losgelöst von der aktuellen vSphere-Client-Ansicht, Sie erstellen und verwalten damit auch die Snapshots oder verwalten das Floppy- oder CD-ROM-/DVD-Laufwerk der VM.

Sollten zwei vSphere-Administratoren zur gleichen Zeit die Konsole einer VM öffnen, so erhalten beide einen nicht zu übersehenden Hinweisbalken, dass eine weitere Verbindung zur Konsole hergestellt wurde.

Die Probleme mit einer Konsolenverbindung können sich auf den verschiedensten Wegen bemerkbar machen. Die möglichen Fehlermeldungen sehen sie in Abbildung 15.60.

```
Error connecting: Host address lookup for server <SERVER> failed: The
requested name is valid and was found in the database, but it does not
have the correct associated data being resolved for Do you want to try
again?

Error connecting: cannot connect to host <host>: A connection attempt
failed because the connected party did not properly respond after a
period of time, or established connection failed because connected
host has failed to respond. Do you want to try again?

Error connecting: You need execute access in order to connect with the
VMware console. Access denied for config file.
```

Abbildung 15.60 Mögliche Fehler bei einer Konsolenverbindung

Zusätzlich könnten Sie von folgenden Problemen heimgesucht werden:

- Die Konsolenverbindung lässt sich nicht öffnen.
- Die Konsole ist leer (schwarzer Bildschirm).
- Die Konsolenverbindung wird durch einen Timeout getrennt.
- Der vMotion-Vorgang schlägt fehl.

Hierzu gibt es eine Reihe von Dingen, die zu beachten oder zu konfigurieren sind:

- Stellen Sie sicher, dass zwischen dem ESXi-Host und dem PC mit dem vSphere-Client die Zeit synchron ist. Idealerweise verwenden Sie NTP.
- Der ESXi-Server sowie der PC mit dem vSphere-Client benötigt eine korrekte Namensauflösung via DNS. Dies ist der am häufigsten anzutreffende Fehler bei Problemen mit der Konsolenverbindung.
- Hat Ihr ESXi-Server zwei Netzwerkkarten in der Service Console konfiguriert, so dürfen diese nicht im gleichen Netzwerk hängen.
- Überprüfen Sie, dass die */var*-Partition nicht vollgelaufen ist.

Reiter »Permissions«

Im Reiter Permissions fügen Sie Benutzer, die entweder aus dem am vCenter-Server angeschlossenen Active Directory oder der lokalen Windows-Benutzerverwaltung stammen, zu

vordefinierten Rollen hinzu und weisen sie einzelnen virtuellen Maschinen zu. Idealerweise legen Sie die Berechtigung eine oder mehrere Stufen höher fest; z. B. haben Sie einen Folder *Linux-Server*, in dem all Ihre Linux-Server vereint sind, und definieren dafür eine Rolle »Linux-Admins«, die gewisse Berechtigungen auf diesen Folder erhält. Somit erben die Rolleninhaber für alle virtuellen Maschinen in diesem Folder die notwendigen Rechte. Weitere Informationen dazu erhalten Sie in Kapitel 12, »Konfiguration von ESX und vCenter«.

Reiter »Maps«

Die Maps können Sie auf allen Objektebenen (Datacenter, Cluster, ESX, Folder, VM etc.) einsehen. Sie zeigen alle mit diesem Objekt verbundenen Einheiten und deren Bezug untereinander an.

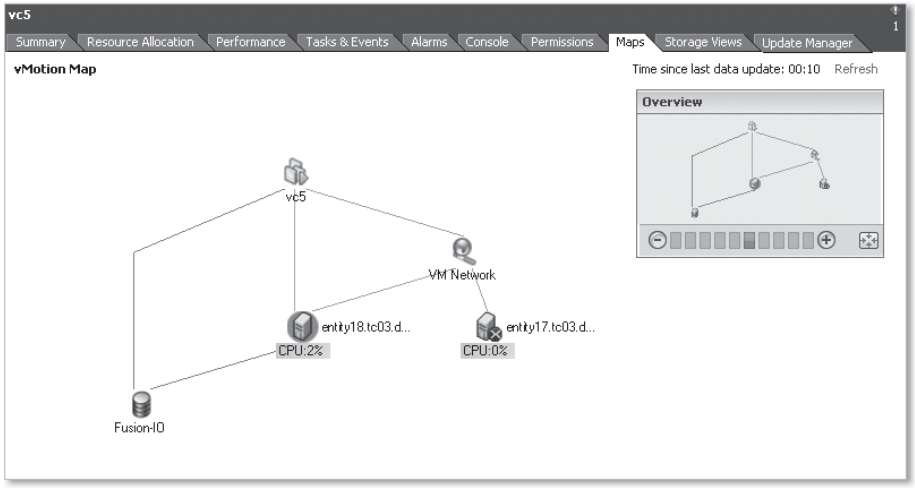


Abbildung 15.61 Die Map einer virtuellen Maschine

15.18 Erweitertes VM-Management

15.18.1 Killen einer hängenden VM

Wenn das Stoppen einer virtuellen Maschine über den vSphere-Client nicht mehr den gewünschten Erfolg bringt, dann gibt es noch Wege, dies über z. B. die vCLi direkt auf dem ESXi-Servers durchzuführen, auf dem die virtuelle Maschine aktiv ist. Dazu müssen Sie aber zuerst über den vSphere-Client den ESXi-Server in Erfahrung bringen, der die VM beherbergt.

- Finden zuerst Sie zur VM die notwendige World Number heraus:
  `esxcli vm process list`
- Das »sanfte« Stoppen einer VM initiieren Sie in der vCLI durch:
  `esxcli vm process kill -type=soft -world-id=WorldNumber`

- Bringt dieser Befehl nicht den gewünschten Erfolg, versuchen Sie das »harte« Stoppen der VM mit `hard` oder sogar mit `force`:

  ```
  esxcli vm process kill -type=hard -world-id=WorldNumber
  esxcli vm process kill -type=force -world-id=WorldNumber
  ```

- Alternativ können Sie auch den Befehl `vim-cmd` in der vCLI einsetzen. Hierzu müssen Sie zuerst weitere Infos über die VM erhalten:

  ```
  vim-cmd vmsvc/getallvms
  ```

- Mit Hilfe der so ausfindig gemachten VMID schalten Sie die VM aus:

  ```
  vim-cmd vmsvc/power.off VMID
  ```

- Mit diesem Befehl erhalten Sie den Power-Status der VM:

  ```
  vim-cmd vmsvc/power.getstate VMID
  ```

- Als letzte Möglichkeit steht Ihnen das Killen des Prozesses der virtuellen Maschine zur Verfügung. Dazu brauchen Sie einen SSH-Zugang zum ESXi-Server, und gegebenenfalls müssen Sie vorher die SSH-Shell auf der ESXi-Konsole aktivieren. Auch bei dieser Methode machen Sie zuerst die PID (Process-ID) der VM ausfindig:

  ```
  ps | grep <VM>
  ```

  Die erste Zahl der Ausgabe ist die Process-ID, die zweite Zahl die Process-ID des Elternprozess. Mit der Letzteren im Gepäck setzen Sie jetzt den `kill`-Befehl ein, um die VM endgültig zu stoppen:

  ```
  kill -9 ProcessID
  ```

Bedenken Sie bitte, dass alle Methoden versuchen, die virtuelle Maschine zu stoppen, ungeachtet dessen, ob das Gastbetriebssystem bereits heruntergefahren wurde oder nicht. Im schlimmsten Falle müssen Sie mit Datenverlust rechnen!

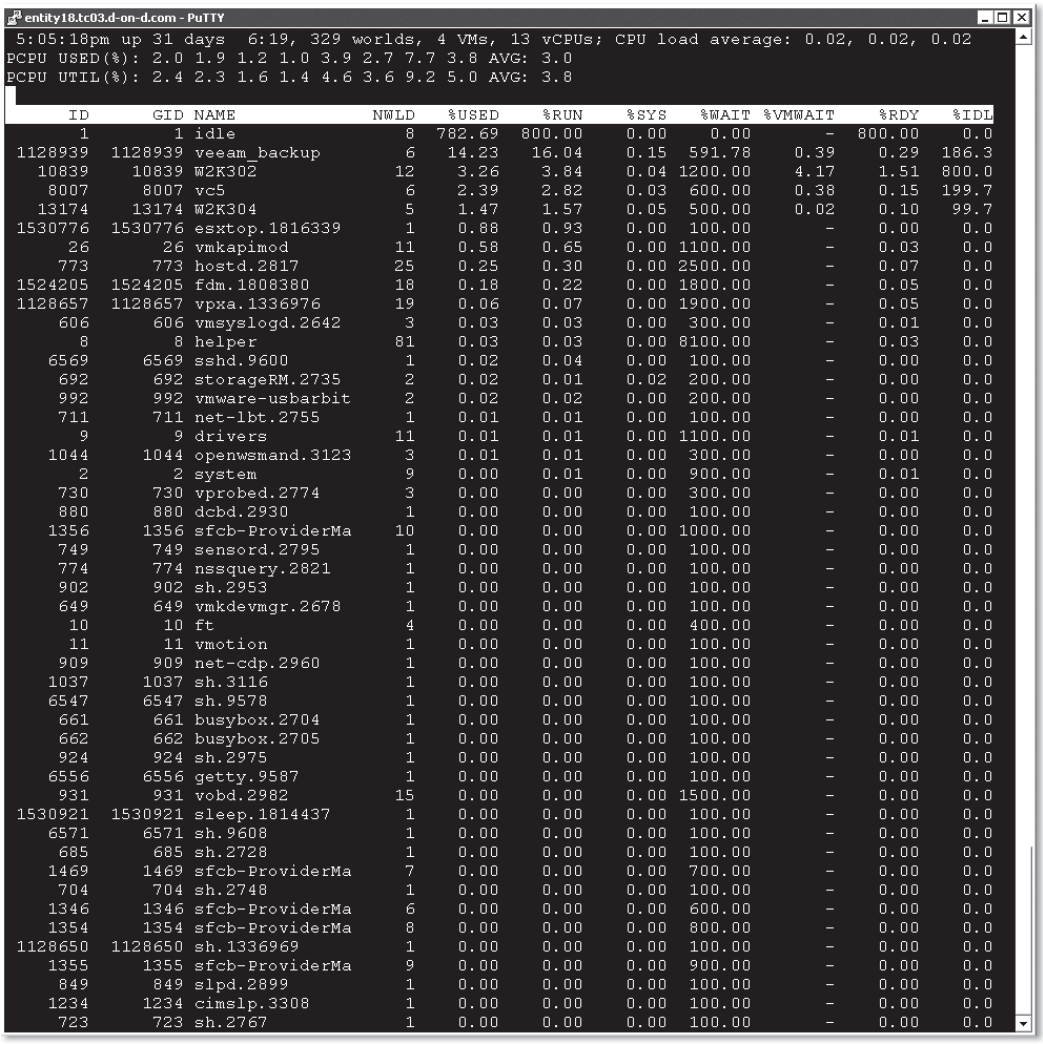
15.18.2 Überwachung der CPU-Performance von virtuellen Maschinen mit »esxtop«

Um einen recht guten Einblick in den Ressourcenhunger Ihrer virtuellen Maschinen zu erhalten, bietet sich der Befehl `esxtop` bzw. `resxtop` an, den Sie auf der SSH-Konsole des ESXi-Servers eingeben. Sie erhalten alle möglichen Werte über die CPU- und Speicher-Auslastung, die Storage-Adapter oder Storage-Device-Auslastung und über die Netzwerklast. Bedenken Sie, dass Sie grundsätzlich alle zu ermittelnden Werte über eine ausreichend lange Zeit verfolgen müssen, um aussagekräftige Informationen zu erhalten!

Möchten Sie den CPU-Verbrauch Ihrer virtuellen Maschinen überwachen, so starten Sie `esxtop` und werten die Zahlen zur aktuellen CPU-Auslastung in den CPU-Statistiken aus. Schauen Sie sich hier den Wert von `%RDY` in der Zeile an, wo der Name Ihrer VM in der ersten Spalte (`Name`) steht.

Der `%RDY`-Wert steigt an, wenn die virtuellen CPUs in der VM CPU-Zeit vom physischen ESXi-Server benötigen, aber dieser sie nicht liefern kann. Hauptsächlich sind dort die Werte inte-

ressant, die nicht dauerhaft über 5 % (Warning) oder sogar über 10 % (Error) liegen. Je höher der %RDY-Wert ist, desto langsamer ist also Ihre virtuelle Maschine. Allerdings gilt dieser Wert bei einer virtuellen CPU in der VM; hat die VM vier virtuelle CPUs, so wäre der Wert bei 20 auf Warnung und bei 40 auf Error.



entity18.tc03.d-on-d.com - PuTTY

```
 5:05:18pm up 31 days  6:19, 329 worlds, 4 VMs, 13 vCPUs; CPU load average: 0.02, 0.02, 0.02
PCPU USED(%): 2.0 1.9 1.2 1.0 3.9 2.7 7.7 3.8 AVG: 3.0
PCPU UTIL(%): 2.4 2.3 1.6 1.4 4.6 3.6 9.2 5.0 AVG: 3.8

      ID       GID NAME             NWLD   %USED    %RUN    %SYS   %WAIT %VMWAIT    %RDY   %IDL
       1         1 idle                8  782.69  800.00    0.00    0.00       -  800.00    0.0
 1128939   1128939 veeam_backup        6   14.23   16.04    0.15  591.78    0.39    0.29  186.3
   10839     10839 W2K302             12    3.26    3.84    0.04 1200.00    4.17    1.51  800.0
    8007      8007 vc5                 6    2.39    2.82    0.03  600.00    0.38    0.15  199.7
   13174     13174 W2K304              5    1.47    1.57    0.05  500.00    0.02    0.10   99.7
 1530776   1530776 esxtop.1816339      1    0.88    0.93    0.00  100.00       -    0.00    0.0
      26        26 vmkapimod          11    0.58    0.65    0.00 1100.00       -    0.03    0.0
     773       773 hostd.2817         25    0.25    0.30    0.00 2500.00       -    0.07    0.0
 1524205   1524205 fdm.1808380        18    0.18    0.22    0.00 1800.00       -    0.05    0.0
 1128657   1128657 vpxa.1336976       19    0.06    0.07    0.00 1900.00       -    0.05    0.0
     606       606 vmsyslogd.2642      3    0.03    0.03    0.00  300.00       -    0.01    0.0
       8         8 helper             81    0.03    0.03    0.00 8100.00       -    0.03    0.0
    6569      6569 sshd.9600           1    0.02    0.04    0.00  100.00       -    0.00    0.0
     692       692 storageRM.2735      2    0.02    0.01    0.02  200.00       -    0.00    0.0
     992       992 vmware-usbarbit     2    0.02    0.02    0.00  200.00       -    0.00    0.0
     711       711 net-lbt.2755        1    0.01    0.01    0.00  100.00       -    0.00    0.0
       9         9 drivers            11    0.01    0.01    0.00 1100.00       -    0.01    0.0
    1044      1044 openwsmand.3123     3    0.01    0.01    0.00  300.00       -    0.00    0.0
       2         2 system              9    0.00    0.01    0.00  900.00       -    0.01    0.0
     730       730 vprobed.2774        3    0.00    0.00    0.00  300.00       -    0.00    0.0
     880       880 dcbd.2930           1    0.00    0.00    0.00  100.00       -    0.00    0.0
    1356      1356 sfcb-ProviderMa    10    0.00    0.00    0.00 1000.00       -    0.00    0.0
     749       749 sensord.2795        1    0.00    0.00    0.00  100.00       -    0.00    0.0
     774       774 nssquery.2821       1    0.00    0.00    0.00  100.00       -    0.00    0.0
     902       902 sh.2953             1    0.00    0.00    0.00  100.00       -    0.00    0.0
     649       649 vmkdevmgr.2678      1    0.00    0.00    0.00  100.00       -    0.00    0.0
      10        10 ft                  4    0.00    0.00    0.00  400.00       -    0.00    0.0
      11        11 vmotion             1    0.00    0.00    0.00  100.00       -    0.00    0.0
     909       909 net-cdp.2960        1    0.00    0.00    0.00  100.00       -    0.00    0.0
    1037      1037 sh.3116             1    0.00    0.00    0.00  100.00       -    0.00    0.0
    6547      6547 sh.9578             1    0.00    0.00    0.00  100.00       -    0.00    0.0
     661       661 busybox.2704        1    0.00    0.00    0.00  100.00       -    0.00    0.0
     662       662 busybox.2705        1    0.00    0.00    0.00  100.00       -    0.00    0.0
     924       924 sh.2975             1    0.00    0.00    0.00  100.00       -    0.00    0.0
    6556      6556 getty.9587          1    0.00    0.00    0.00  100.00       -    0.00    0.0
     931       931 vobd.2982          15    0.00    0.00    0.00 1500.00       -    0.00    0.0
 1530921   1530921 sleep.1814437       1    0.00    0.00    0.00  100.00       -    0.00    0.0
    6571      6571 sh.9608             1    0.00    0.00    0.00  100.00       -    0.00    0.0
     685       685 sh.2728             1    0.00    0.00    0.00  100.00       -    0.00    0.0
    1469      1469 sfcb-ProviderMa     7    0.00    0.00    0.00  700.00       -    0.00    0.0
     704       704 sh.2748             1    0.00    0.00    0.00  100.00       -    0.00    0.0
    1346      1346 sfcb-ProviderMa     6    0.00    0.00    0.00  600.00       -    0.00    0.0
    1354      1354 sfcb-ProviderMa     8    0.00    0.00    0.00  800.00       -    0.00    0.0
 1128650   1128650 sh.1336969          1    0.00    0.00    0.00  100.00       -    0.00    0.0
    1355      1355 sfcb-ProviderMa     9    0.00    0.00    0.00  900.00       -    0.00    0.0
     849       849 slpd.2899           1    0.00    0.00    0.00  100.00       -    0.00    0.0
    1234      1234 cimslp.3308         1    0.00    0.00    0.00  100.00       -    0.00    0.0
     723       723 sh.2767             1    0.00    0.00    0.00  100.00       -    0.00    0.0
```

Abbildung 15.62 CPU-%RDY-Werte einer VM mit »esxtop« ermitteln

Zusätzlich zu diesem Prozentwert können Sie sich über den vSphere-Client die Performancestatistik für READY anzeigen lassen. Dieser Wert wird dort in Millisekunden angegeben (siehe Abbildung 15.63 auf der nächsten Seite).

Weiterführende Dokumente von VMware finden Sie unter *http://communities.vmware.com/docs/DOC-9279* und *http://viops.vmware.com/home/docs/DOC-1404.pdf*.

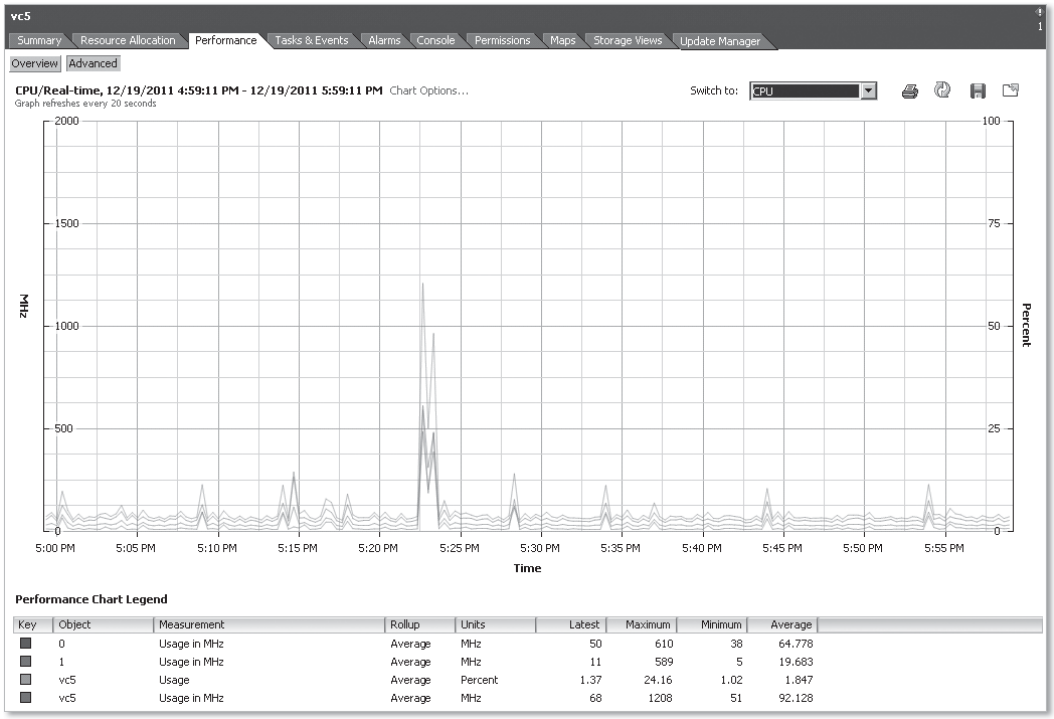


Abbildung 15.63 Weitere CPU-Performance-Werte einer VM

Der VMware Capacity Planner ist ein Werkzeug, das im Umfeld eines Migrationsvorhabens eingesetzt werden kann. Es unterstützt die IT durch Fakten bei ihren Entscheidungen und ermöglicht dadurch nachhaltige Planungssicherheit in Migrationsprojekten.

16 Kapazitätsplanung mit dem VMware Capacity Planner

Autor dieses Kapitels ist Günter Baumgart, guenter.baumgart@anmax.de

Das nun folgende Kapitel beschäftigt sich mit dem VMware Capacity Planner und entstand, als die Version 2.8.1 Build 49255 des VMware Capacity Planner Data Managers für die Betrachtung von IT-Umgebungen eingesetzt wurde.

In der Regel befinden sich unterschiedlichste Server in einem Unternehmen. Das können beispielsweise Mailserver, Fileserver, Datenbank-Server usw. sein. Jeder Server im Unternehmen stellt mindestens einen Dienst zur Verfügung. In den meisten Unternehmen hat sich im Laufe der Jahre die Anzahl der Dienste, die benötigt werden, dramatisch vergrößert. Durch diesen Zuwachs an effektiv nicht ausgelasteten Servern stoßen die Rechenzentren oder Server-Räume vielerorts an ihre Leistungsgrenzen.

Oftmals teilen sich auch unterschiedlichste Unternehmen ein Rechenzentrum, wobei die Trennung der einzelnen Bereiche, die die Unternehmen benutzen, sehr häufig durch Gitterwände erfolgt. Hier kommt es dann auch durchaus vor, dass ein Bereich derart große Wärmemengen produziert, dass andere Bereiche stillgelegt werden müssen oder nur eingeschränkt genutzt werden können.

Jede Höheneinheit in einem Rechenzentrum ist kostspielig und muss bezahlt werden. Das beschriebene Szenario der eingeschränkten Nutzung oder gar die Stilllegung von Stellfläche ist der Kostengau für einen Rechenzentrumsbetreiber!

Klimageräte, die Stromversorgung, Anschlüsse an das Unternehmens- oder Speichernetzwerk, Stellfläche für neue Server-Schränke etc., all diese Ressourcen sind begrenzt, und eine Aufrüstung sprengt oft den finanziellen Rahmen des IT-Etats.

Spätestens an dieser Stelle gilt es nun zu überlegen, ob es Ansätze für die Virtualisierung von Server-Landschaften gibt, um durch Optimierung die Kosten im Rechenzentrum zu senken.

Mit der vorliegenden Version des VMware Capacity Planners ist es nun auch möglich, physische Desktops auf ihre Virtualisierungsfähigkeit zu betrachten und den Weg zu bereiten, um

auch derartige Vorhaben in die Tat umzusetzen. Capacity-Planning zur Vorbereitung von erfolgreicher Desktop-Virtualisierung werde ich allerdings in meinem Buch (ISBN 978-3-8362-1787-3) zur Desktop-Virtualisierung – das für Anfang 2013 bei Galileo Computing geplant ist – detailliert behandeln, so dass ich an dieser Stelle auf dieses Thema nicht weiter eingehen werde.

16.1 Erste Vorüberlegungen zu einem Migrationsprojekt

Entscheidet sich die Unternehmens-IT nun für eine Virtualisierung der physischen Systeme, löst sich das eine oder andere angesprochene Problem schnell auf. Nicht zuletzt dadurch, dass die Hardware, die zur Virtualisierung herangezogen wird, höchst effizient genutzt wird.

Damit aber die zur Virtualisierung benötigte Hardware, wie beispielsweise Host und Storage, auch im Hinblick auf den Nutzungsgrad optimal verwendet wird, bedarf es unterschiedlichster Informationen. Die Frage, wie Host und Storage beschaffen sein müssen, kann natürlich nur beantwortet werden, wenn die späteren Belastungen, die durch die virtuellen Maschinen entstehen werden, vor dem Virtualisierungsvorhaben bereits bekannt sind. Sehr oft liegt der Nutzungsgrad – oder anders gesagt, die mittlere Auslastung eines Servers – zwischen fünf und fünfzehn Prozent. Natürlich gibt es immer wieder temporäre Spitzenlasten, die aber in den seltensten Fällen die volle Leistung moderner Server-Systeme ausschöpfen.

Einige Server-Systeme lassen sich gar nicht so einfach virtualisieren, da Spezialhardware wie Faxkarten oder Ähnliches in diesen Servern eingebaut ist. Hier scheint auf den ersten Blick keine Virtualisierung möglich zu sein. In derartigen Fällen müssen Sie über andere Lösungsmöglichkeiten nachdenken. In diesem Beispiel böte es sich an, die Faxkarte durch ein Faxmodem, das im lokalen Netzwerk erreichbar ist, zu ersetzen und dann den Server zu virtualisieren. Der virtuelle Fax-Server nutzt dann für den Faxempfang und -versand das Faxmodem im LAN. Hier denkt man auch sofort an Banking-Systeme, bei denen die Aufgabenstellung fast identisch ist. In diesem Zusammenhang stellt sich auch immer wieder die Frage, wie mit Dongles umzugehen ist. Auch hierbei ist es immer ratsam, zuerst einmal mit dem Hersteller der Software zu sprechen. In den meisten Fällen halten die Softwarehersteller bereits eine Lösung vor, um ihre Software auch in virtuellen Umgebungen zertifiziert betreiben zu können.

Ebenfalls muss die Frage nach dem zukünftigen Wachstum im Zusammenhang mit Daten und Diensten im Vorfeld beantwortet werden. Überlegungen im Hinblick auf die Möglichkeit der Skalierung des Gesamtsystems sollten Sie an dieser Stelle ebenfalls in die Planungen einbeziehen. Auch müssen Sie bei der Konzeption der virtuellen Infrastruktur die Ressourcen berücksichtigen, die für die Bereitstellung einer hochverfügbaren Lösung notwendig sind.

Oftmals können die soeben genannten Punkte nicht hinreichend beantwortet werden. Nicht immer ist die Auslastung der zu virtualisierenden Systeme vollständig transparent, und Fragen wie »Zu welchem Zeitpunkt ist der Server wie belastet?« bleiben häufig unbeantwortet.

Natürlich ist der Unternehmens-IT bekannt, dass z. B. während der Monatsübergänge oder anderer markanter Zeitpunkte in einem Unternehmen unter Umständen mit einem Anstieg der Last auf den Server-Systemen zu rechnen ist, aber genauere Aussagen dieser Art sind eher die Ausnahme. An dieser Stelle sei darauf hingewiesen, dass viele Virtualisierungsprojekte genau daran kranken, dass die Auslastung der zu virtualisierenden physischen Server-Landschaften im Vorfeld nicht genügend genau untersucht wurde.

Ein weiterer interessanter Aspekt wäre, wenn der Load eines einzelnen Servers bezogen auf die Zeit bereits vor der Virtualisierung bekannt wäre. Lägen derartige Informationen vor, wäre es leicht möglich, die spätere Belastung der Hosts optimal auszuloten. Dies gilt selbstverständlich für alle zu virtualisierenden Systeme.

Im nun folgenden Beispiel werden wir unabhängig von Taktraten und Benchmarks einen Sachverhalt beleuchten, der in der Praxis des Öfteren vorkommt. Der Server, den wir betrachten, verfügt über zwei CPUs. Die CPUs des Systems werden im Mittel um die zehn Prozent genutzt. Außerdem sind die CPUs unterschiedlich stark ausgelastet; CPU0 wird deutlich höher belastet als CPU1. Der Dienst, der von diesem Server bereitgestellt wird, kann augenscheinlich ein Zweiwegesystem nicht optimal ausnutzen. Eine Balance in der Belastung der CPUs funktioniert also nicht vollständig. Kurz gesagt, haben wir eine minimal ausgelastete physische Zweiwegemaschine mit zwei unsymmetrisch belasteten CPUs, und dabei haben wir noch nicht einmal den Faktor der Taktfrequenz des Server-Systems in die Betrachtung einbezogen.

Das heißt, die physische Maschine, die wir in diesem Beispiel betrachten, ist gänzlich ungeeignet, was Ausstattung und Dimensionierung angeht. Wäre es da nicht sinnvoll, den Einsatz dieser physischen Maschine zu überdenken und sie gegen eine besser an die Anforderungen des Dienstes angepasste Hardware auszutauschen? Würde der Dienst dieser physischen Maschine nun in eine virtuelle Maschine konvertiert, würden wir natürlich eine Einwegemaschine erstellen. Des Weiteren wäre die virtuelle CPU bei dieser virtuellen Maschine auch so konfiguriert, dass sie nur die Leistung garantiert, die vorher in der physischen Maschine genutzt wurde.

Der eingangs genannte unter zehn Prozent liegende Nutzungsgrad in der physischen Umgebung läge dann in der virtuellen Umgebung wesentlich höher. Da ja die Ressourcen der virtuellen Maschine geringer dimensioniert wurden, verbesserte sich der Nutzungsgrad, was die Effizienz steigerte.

Spätestens an dieser Stelle wird überdeutlich, dass eine Migration eines Environments umso erfolgreicher wird, je detailliertere Informationen bereits im Vorfeld über das Lastverhalten der Umgebung zur Verfügung stehen. In diesem Kontext ist es natürlich möglich, alle Daten, die für eine erfolgreiche Virtualisierung einer physischen Server-Umgebung benötigt werden, an den Servern abzufragen und manuell oder teilautomatisiert auszuwerten. Die Frage hierbei ist allerdings: Steht mir die erforderliche Zeit dafür zur Verfügung? Das Werkzeug, welches es mir ermöglicht, eine derartige Untersuchung einer IT-Landschaft auch in kürzester Zeit vorzunehmen steht mir mit dem VMware Capacity Planner zur Verfügung.

16.2 Arbeitsweise und Funktion des Capacity Planners

Der VMware Capacity Planner stellt sich als Framework dar (Abbildung 16.1) und besteht im Wesentlichen aus zwei Teilen: Zum einen handelt es sich um den Data Collector und zum anderen um das Information Warehouse bei VMware in Palo Alto im Silicon Valley. Der Data Collector ist z. B. eine physische x86/x64-Maschine, auf der das Betriebssystem Microsoft Windows 2008 Server installiert wurde. Als Applikation wird VMware Data Collector installiert. Natürlich ist es erforderlich, die Applikation auch noch entsprechend den Rahmenbedingungen des Environments zu administrieren, aber dazu in Kapitel 16.2.2 später mehr.

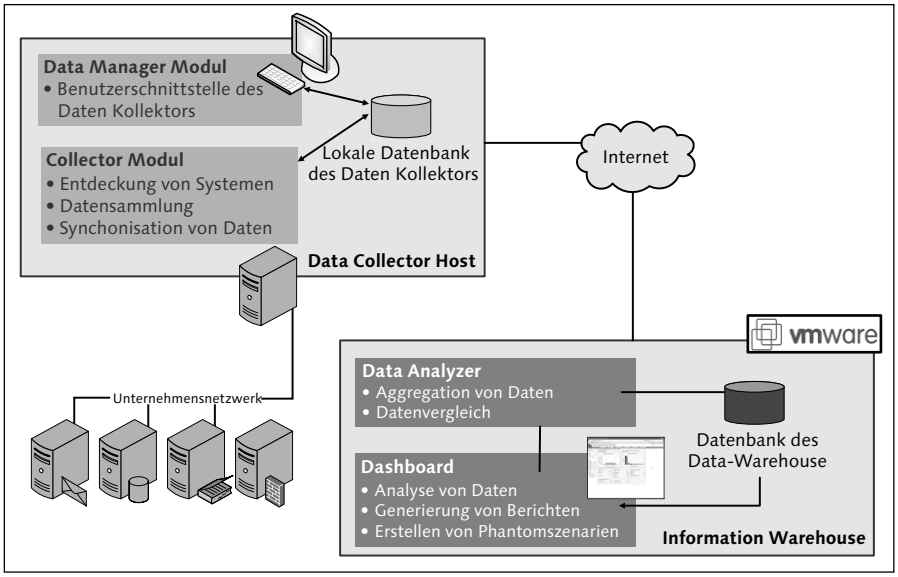


Abbildung 16.1 Framework Capacity-Planning

16.2.1 Data Collector und Information Warehouse

Der Data Collector wird in das zu analysierende Environment gebracht und im lokalen Unternehmensnetzwerk in Betrieb genommen. Nun steht er in dem zu analysierenden Environment und sammelt Informationen über die hier befindlichen Server. Der Data Collector arbeitet ohne den Einsatz von Agenten. Das heißt, es ist nicht erforderlich, zusätzliche Software auf einem der zu untersuchenden physischen Server zu installieren. Welche Server betrachtet werden und welche nicht, legen Sie ebenfalls im Zuge der bereits angesprochenen Administration des Data Collectors fest.

Bei den Daten, die der Data Collector einsammelt, handelt es sich um Inventarisierungs- und Performancedaten. Der Data Collector kann somit als die Datenquelle angesehen werden.

Das Information Warehouse, die Datensenke, im Silicon Valley ist der Teil des Frameworks, der die Daten, die der Data Collector einsammelt, empfängt und aufbereitet. Das Information

Warehouse ist eine gesicherte und kontrollierte zentrale Datenbank. In dieser Datenbank lagern die Daten, die alle im Einsatz befindlichen Data Collectors, anliefern. Die Bezeichnung Data Collector wird im deutschen Sprachgebrauch mit Datenkollektoren übersetzt. Die Daten werden, bevor sie in die Datenbank aufgenommen werden, überprüft und bereinigt. Da alle Data Collectors weltweit ihre Daten in diese Datenbank transferieren, entsteht eine enorme Datenbasis, die auch zu Vergleichszwecken herangezogen werden kann. In frei einstellbaren zeitlichen Intervallen werden die Daten von der Quelle zur Senke übertragen (Abbildung 16.2). Die Übertragung der Daten erfolgt SSL-verschlüsselt über HTTP.

In der Regel werden die Daten über einen Zeitraum von einem Monat gesammelt. Im Anschluss daran wird die Messung beendet bzw. das Sammeln der Daten eingestellt. Alle Messdaten stehen nun zur Auswertung im Information Warehouse bereit. In den nächsten Schritten werden die Daten dann anhand unterschiedlichster Kriterien analysiert und erläutert. Ein Data Collector kann durchschnittlich etwa 500 Zielsysteme im Netz überwachen. In einem Netzwerk können mehrere Data Collectors betrieben werden, so dass auch Server-Umgebungen mit einer weitaus größeren Anzahl an physischen Zielsystemen mit diesem Verfahren analysiert und betrachtet werden können.

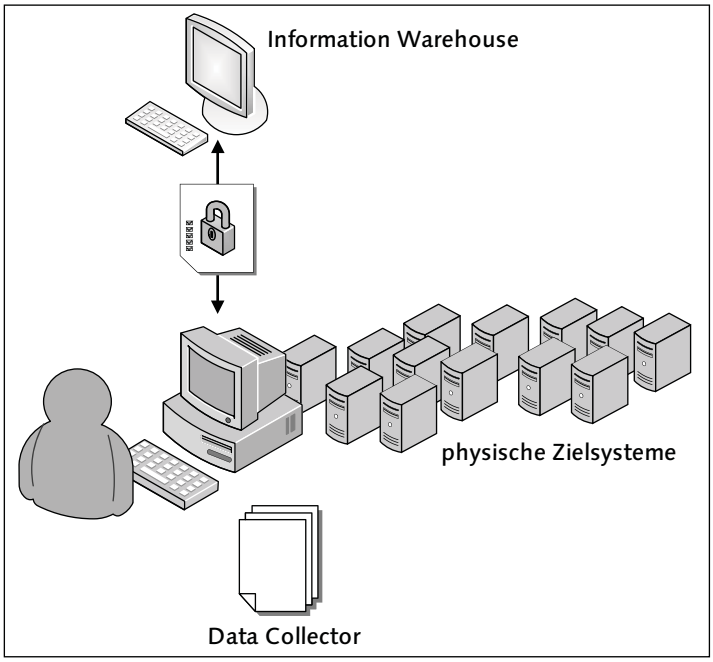


Abbildung 16.2 Datenübertragung zum Information Warehouse

16.2.2 Collector-Modul

Ein Data Collector wird, wie bereits erwähnt, auf einem Windows-System installiert. Er läuft als Windows-Service im Hintergrund. Der Data Collector setzt sich aus drei Teilen zusammen:

einer lokalen Datenbank, dem Data-Manager-Modul und dem Collector-Modul. Das Collector-Modul des Data Collectors wird zur Entdeckung der physischen Server-Systeme im Netzwerk eingesetzt. Außerdem übernimmt es auch die Übertragung der Daten zum Information Warehouse. Es sammelt detaillierte Inventarisierungsdaten über die Hardware und die installierte Software auf den Zielsystemen. Das Collector-Modul sammelt auch die wichtigsten Performancedaten der zu untersuchenden Server. Es sei an dieser Stelle abermals darauf hingewiesen, dass es nicht erforderlich ist, zur Gewinnung dieser Daten Agenten auf den zu untersuchenden physischen Ziel-Server-Systemen zu installieren.

Bei den Zielsystemen kann es sich um Windows-, Linux- oder Unix-Systeme handeln. Bei Windows-Systemen werden die Daten mittels der Standard-Interfaces ermittelt. Wenn es sich bei den Zielsystemen um Linux- oder Unix-Systeme handelt, werden die Leistungs- und Inventarisierungsdaten unter Zuhilfenahme einfacher Skripte ermittelt. Hierzu wird eine Verbindung über die Secure Shell (SSH) zum Zielsystem aufgebaut.

Der Data Collector verfügt über einen Task- bzw. Job-Planer. Dieser Scheduler ermöglicht ein zeitgesteuertes Ausführen von Umgebungsanalyse-, Inventarisierungs-, Leistungsdatenermittlungs- und Datensynchronisationsmodulen. Die zeitlichen Intervalle sind sehr fein granulierbar, wie Sie in Abbildung 16.3 erkennen.

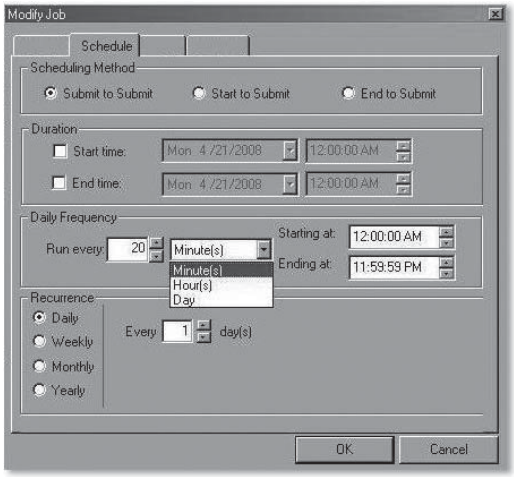


Abbildung 16.3 Job-Planer

16.2.3 Data-Manager-Modul

Der Benutzer arbeitet, wie bereits erwähnt, mit der grafischen Benutzerschnittstelle des Data Collectors, dem Data Manager. Über diese Benutzerschnittstelle können Sie das System konfigurieren und administrieren. Hierzu gehören sowohl die Erstellung und Konfiguration von Collection-Jobs als auch die Eingabe von Benutzerkennung und Kennwortkombinationen für den Zugang zu den Zielsystemen.

Der Datenmanager erlaubt Ihnen im ersten Schritt, bevor die automatischen bzw. die zeitgesteuerten Jobs abgearbeitet werden, erste manuelle Überprüfungen. Konkret bedeutet dies, dass Sie u. a. Verbindungstests wie auch gezielte Inventarisierungen und Performancemessungen der zu untersuchenden Systeme manuell durchführen können. Eine Überprüfung der Datensynchronisation zwischen dem Data Collector und dem Information Warehouse ist ebenfalls mit dem Data Manager möglich. Auch ermöglicht der Data Manager Ihnen eine erste Sicht auf die ermittelten Rohdaten, bevor sie manuell oder mittels Automatismen in das Information Warehouse übertragen werden.

16.2.4 Data Analyzer

Der Data Analyzer stellt das Herzstück, die Analytical Engine, des Information Warehouse dar. Er ermöglicht Auswertungen bei der Kapazitätsplanung. Hierbei werden unterschiedlichste Verfahren angewendet, um Aussagen im Hinblick auf Aggregation, Trendanalyse und Benchmarking bezogen auf die Messwerte einer physischen Umgebung zu tätigen. Das heißt, der Data Analyzer unterstützt die Analyse von Belastungsprofilen und die Erstellung von Modellszenarien. Durch derartige Modellszenarien, die auch als Phantomszenarien bezeichnet werden, ist es möglich, Empfehlungen dahingehend auszusprechen, welche virtuellen Maschinen auf einem Host optimal zusammenpassen.

16.2.5 Dashboard

Das Dashboard ist die webbasierte Benutzerschnittstelle zum Data Warehouse und zum Data Analyzer. Es ermöglicht den Zugriff auf die vom Data Collector gewonnenen Daten aus der physischen Umgebung. Außerdem regelt es den Zugriff auf die Funktionen des Data Analyzers. Auch gewährleistet das Dashboard den direkten Zugriff auf den Data Collector und stellt die unterschiedlichsten Informationen über Capacity-Planning zur Verfügung. Die gesamte projektbezogene Organisation die erforderlich ist, um ein Data-Collector-Projekt durchzuführen, kann mit dem Dashboard umgesetzt werden.

Unter anderem bedeutet das im Einzelnen:

- Anzeige des Status der Datensammlung
- Remote-Steuerung von unterschiedlichen Tasks des Data Collectors
- Bereitstellung von Templates für Analyse und Synthese
- Darstellung der gesammelten Daten in unterschiedlichster Art und Weise
- Szenariomodellierung
- Performance-Monitoring und Trendanalyse
- Entdeckung und Meldung von Anomalien und Alarmen

- Aufzeigen von Konsolidierungsmöglichkeiten
- Erkennen von Systemen, die sich nicht zur Konsolidierung eignen
- Erkennen von veralteten und unbrauchbaren Zielsystemen

16.3 Die Arbeit mit dem Capacity Planner

Nachfolgend beschreiben wir die Arbeitsweise mit dem Capacity Planner näher. In den vorangegangenen Abschnitten haben wir die Funktionen der einzelnen Module des Capacity-Planner-Frameworks zum besseren Verständnis des Gesamtbildes kurz erläutert. Dazu war es notwendig, die beiden Hauptbestandteile des Capacity Planners, den Data Collector und das Information Warehouse, in ihre Bestandteile zu zerlegen. Im weiteren Verlauf sehe ich davon ab, über das Data-Manager-Modul, das Collector-Modul oder die Data-Collector-Datenbank zu sprechen. Das Gleiche gilt für das Information Warehouse. Auch hier unterscheiden wir nicht mehr zwischen dem Data Analyzer, dem Dashboard und der Information-Warehouse-Datenbank.

16.4 Die Arbeit mit dem Data Collector

16.4.1 Auffinden der Zielsysteme

Im ersten Schritt wird der Data Collector dazu verwendet, alle Server der zu vermessenden Umgebung ausfindig zu machen. Damit er diese Aufgabe auch erfüllen kann, gibt es unterschiedliche Vorgehensweisen. Zum einen ist es möglich, die Adressen und Zugangsdaten aller zu untersuchenden Server mittels Datei in den Data Collector zu importieren. Handelt es sich um wenige zu untersuchende Systeme, können Sie die Adress- und Zugangsdaten dem Data Collector auch manuell angeben. Eine weitere Möglichkeit, die zu untersuchenden Systeme zu erkennen, besteht darin, die Server mittels LAN-Manager und/oder Active Directory im Netzwerk zu finden. Sollten diese beiden Methoden nicht zum gewünschten Erfolg führen, gibt es auch noch den Weg, das Netzwerk im Hinblick auf bestimmte IP-Ranges (Hauptsächlich für Linux/Unix Discovery) zu durchsuchen.

Letztendlich wird in einem komplexen Environment, das untersucht wird, immer eine Kombination aus den genannten Verfahren zur Auffindung der Zielsysteme angewendet werden.

16.4.2 Verbindungsaufbau zu den Zielsystemen

Im nächsten Schritt, nachdem alle in die Messung einbezogenen Systeme gefunden und die Anmeldeinformationen für die Zielsysteme im Data Collector hinterlegt wurden, können Sie damit beginnen, Verbindungstests zu den einzelnen Zielsystemen durchzuführen. Die Verbindungstests verwenden unterschiedlichste Methoden, je nachdem, welches Betriebssystem auf dem Zielsystem installiert ist.

Methoden zur Datengewinnung im Windows-Umfeld

Im Windows-Umfeld werden unterschiedlichste Verfahren genutzt, um die Informationen über die Server zu sammeln. Aus diesem Grund ist ein einwandfreies Funktionieren der im Folgenden aufgeführten Methoden Voraussetzung für eine korrekte Funktion des Data Collectors.

- Name Resolution / `ping`
- Traceroute / `tracert`
- Read IPC$ Map / `share`
- Read Remote Registry
- Access WMI Namespace
- Access Performance Manager

Methoden zur Datengewinnung bei Unix und Linux

Im Umfeld von Unix und Linux werden die folgenden Verfahren benutzt. Auch hier gilt wieder: Ein einwandfreies Funktionieren der aufgeführten Methoden ist Voraussetzung für eine fehlerfreie Funktion des Data Collectors.

- Name Resolution – `ping`
- Traceroute / `traceroute`
- SSH Secure Shell Execution

Bei Linux- und Unix-Systemen ist es zusätzlich notwendig, den SSH-Sicherheitsschlüssel lokal im Data Collector zu hinterlegen. Zu diesem Zweck öffnen Sie über den Data Manager ein Unix-Terminal zum entsprechenden Server. Es muss für alle Methoden garantiert sein, dass die aufgelisteten Verfahren ohne Einschränkung während der Sammlungsphase zwischen Data Collector und den Zielsystemen genutzt werden können.

16.4.3 Manuelle Inventarisierung

Nachdem Sie sichergestellt haben, dass die Verbindung zwischen dem Data Collector und den Nodes bzw. Zielsystemen verfügbar ist, können Sie manuell einmalig einen ersten vollständigen Inventarisierungs-Task zu Testzwecken anstoßen. Nodes bzw. Zielsysteme, die durch den Discovery-Task erfolgreich identifiziert wurden, werden nun inventarisiert. Hierbei wird sowohl die Hardware als auch die auf dem Zielsystem installierte Software aufgenommen. Die Inventarisierung bzw. Systemanalyse bezieht sich auf den Zeitpunkt der Durchführung. Das heißt: Erfolgt nach der Inventarisierung eine Veränderung am Zielsystem, wird diese natürlich auch erst beim nächsten Inventarisierungsdurchlauf dokumentiert. Die Inventarisierungsinformationen werden gewöhnlich im ersten Schritt der Untersuchung mittels Windows Management Instrumentation (WMI) und dann im nächsten Schritt aus der Registry des Zielsystems ermittelt.

Betreiben Sie die Zielsysteme unter Unix oder Linux, erfolgt die Inventarisierung über die Secure Shell (SSH). An dieser Stelle stellt sich die Frage, worauf das Zielsystem untersucht wird. Im Wesentlichen werden die Punkte Chassis, Prozessor, Memory, Laufwerke und Adapter, File-System, Netzwerk-Interface, Applikationen und Services analysiert, wie Sie in Abbildung 16.4 erkennen.

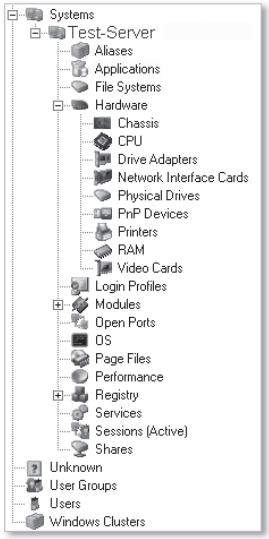


Abbildung 16.4 Merkmale des Ziel-Servers »Test-Server« im Hinblick auf das Betriebssystem und die Hardware

Die Inventarisierung erfolgt multithreaded. Sollte die Inventarisierung mit der einen Methode nicht erfolgreich abgeschlossen werden können, wird eine andere Methode zur Informationsgewinnung angewendet (»Auto-detect Method«). Dadurch wird sichergestellt, dass eine gewisse Redundanz in diesem Verfahren enthalten ist. Der Vorgang der Inventarisierung kann je nach Komplexitätsgrad des Zielsystems eine gewisse Zeitspanne in Anspruch nehmen. Zur Überprüfung des Inventarisierungsvorganges wird für jede Inventarisierung eines einzelnen Zielsystems eine Protokolldatei (Log-File) auf dem Data Collector abgelegt.

16.4.4 Manuelle Leistungsdatenermittlung

Auch bei der Leistungsdatenermittlung ist eine Verbindung zu den Zielsystemen, wie in Abschnitt 16.4.3, »Manuelle Inventarisierung«, beschrieben, sicherzustellen. Sind die Zielsysteme also erreichbar, können Sie nun wiederum exemplarisch einen manuellen Leistungsmessungs-Task anstoßen. Bei allen Nodes, die durch den Discovery-Task erfolgreich identifiziert wurden, wird nun eine Performancemessung durchgeführt. Das Verfahren zur Leistungsdatenermittlung generiert statistische Daten der Zielsysteme. Die Gewinnung von Leistungsdaten der Zielsysteme geschieht bei Systemen, die unter Windows laufen, über den Performance Monitor (Perfmon).

Bei Unix- oder Linux-Systemen werden die Leistungsdaten durch das Ausführen von speziellen Skripten ermittelt. Der Prozess der Leistungsmessung verbindet sich bei zu vermessenden Unix- oder Linux-Zielsystemen zuerst über eine Secure-Shell-(SSH-)Verbindung. Im Anschluss daran werden unterschiedliche Skripte ausgeführt, um die benötigten Messwerte am Zielsystem abzufragen. Die Daten werden in einem weiteren Prozessschritt dann mittels SCP (Secure Copy Protocol) an den Data Collector zurückgegeben.

Der Leistungsdatenbericht enthält folgende Messungen:

- CPU-Statistik
- Prozessorauslastung
- Processor Queue Length
- Memory-Auslastung
- Netzwerk-Auslastung
- physische Disk-Auslastung
- Logical Disk Size

16.4.5 Die Datensynchronisationsfunktion des Data Collectors

Bevor eine Datensynchronisation zwischen Data Collector und Information Warehouse über eine gesicherte Verbindung durchgeführt wird, wird der Besitzer der Daten mittels Pseudonym anonymisiert. Dieses Verfahren bietet bereits eine gewisse Basissicherheit. Um die Forderung nach Anonymität noch weiter zu erhöhen, ist es möglich, zusätzlich Server- und Domänennamen zu verbergen. Durch diese Maßnahmen wird die Forderung nach Vertraulichkeit und Integrität während der Synchronisation der Daten erfüllt.

Damit Sie sich ein Bild vom Ablauf des Synchronisationsprozesses des Data Collectors machen können, erläutern wir diesen nun näher. Im ersten Schritt werden die Dateien z. B. aus einem erfolgreichen Inventarisierungs- und Leistungsdatenermittlungsprozess in einem Unterverzeichnis des Data Collectors mit der Bezeichnung *Outbox* abgelegt. Die Namen der Dateien, die die Inventarisierungsdaten enthalten, beginnen mit *Inv_*, und diejenigen der Dateien mit den Leistungsdaten beginnen mit *Stats_*. An dieser Stelle sei darauf hingewiesen, dass sämtliche Aktionen, die der Data Collector ausführt, in der Message-Box des Data Collectors protokolliert werden.

In Schritt zwei wird eine Log-Datei gespeichert. Diese Log-Datei enthält u. a. die Ausgabe der Message-Box des Data Collectors. Anschließend wird der Inhalt der Outbox an das Information Warehouse übertragen und eine Kopie aller Dateien, die die Inventarisierungs-, Leistungs- und Log-Daten enthalten, in ein Archivierungsverzeichnis geschrieben. Im Anschluss daran wird der aktuelle Inhalt der Outbox gelöscht.

Falls Sie die optionale Funktion (Abbildung 16.5), Remote-Konfiguration des Data Collectors mittels Information Warehouse, nutzen, werden diesbezügliche Informationen in diesem Schritt zurückübertragen. Für den Fall, dass Sie die Funktionalität der automatischen Produktupdates aktiviert haben, werden ebenfalls entsprechende Updates für den Data Collector übertragen.

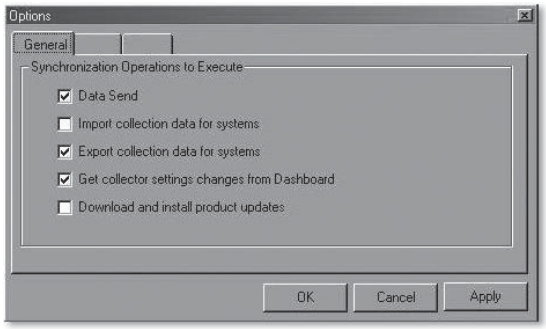


Abbildung 16.5 Optionale Einstellungen zur Datensynchronisation

16.4.6 Automatisierte Ausführung von Jobs

Die zeitgesteuerte Ausführung von Aufgaben (Abbildung 16.6) ermöglicht es, die bereits beschriebenen Einzelaktionen wie Verbindungsaufbau zu den Zielsystemen, Inventarisierung der Zielsysteme, Leistungsdatenmessung an den Zielsystemen und Datensynchronisationsfunktion zwischen Data Collector und Information Warehouse zu automatisieren.

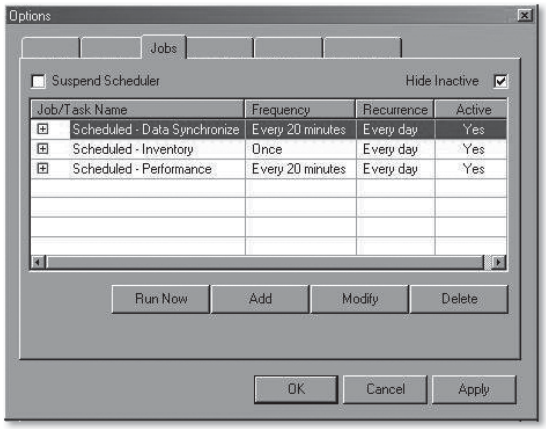


Abbildung 16.6 Zeitgesteuerte Jobausführung

Wie bereits in Abbildung 16.6 dargestellt, ist die zeitliche Steuerung der automatischen Ausführung von Jobs sehr fein einstellbar. Es können Daten zu unterschiedlichsten Zeitpunkten und Intervallen gemessen werden. Die zeitliche Abfolge bei der Messwerterfassung hängt

natürlich unmittelbar damit zusammen, inwieweit Änderungen an den Zielsystemen stattfinden. Normalerweise sind Veränderungen in Bezug auf Inventar im Server-Umfeld eher selten anzutreffen. Ziehen wir das Patchen der Systeme in diesem Zusammenhang noch in Betracht, sollte in der Regel eine tägliche Inventarisierung völlig ausreichend sein.

Im Falle der Leistungsdatenermittlung ist sicherlich eine wesentlich häufigere Durchführung des Jobs notwendig. In Abbildung 16.6 wurde die Ausführung der Jobs Datensynchronisation und Leistungsdatenmessung auf alle 20 Minuten eingestellt. Es ist nicht unbedingt erforderlich, die Datensynchronisation synchron zur Leistungsdatenmessung auszuführen. Bei der Leistungsdatenermittlung trifft die eingangs aufgestellte These, dass ein direkter Zusammenhang zwischen Mess- und Belastungsintervall der Zielsysteme besteht, zu. Hier gilt es, sich vorab die zu vermessenden Nodes näher anzuschauen und die Automation entsprechend anzupassen.

16.4.7 Registrierung des Data Collectors im Information Warehouse

Die Data-Collector-System-ID wurde zum Zeitpunkt der Installation des Data Collectors erzeugt und in der Windows-Registry unter

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\
VMware Capacity Planner\Common\Settings

abgelegt. Während der Installation des Data Collectors wurde außerdem eine sogenannte Database-ID erzeugt. Die Database-ID kann innerhalb des Data Collectors angezeigt werden (Abbildung 16.7). Die Registrierung des Data Collectors im Information Warehouse erfolgt, indem Sie die Database-ID im Dashboard des Information Warehouse in ein entsprechendes Formular eintragen. Dieses Formular enthält auch die Company-ID. Nachdem die Eintragung erfolgt ist, wird im Information Warehouse die System-ID des Data Collector ermittelt und über das Dashboard angezeigt. Der Vorgang der Registrierung des Data Collectors im Information Warehouse ist somit abgeschlossen.

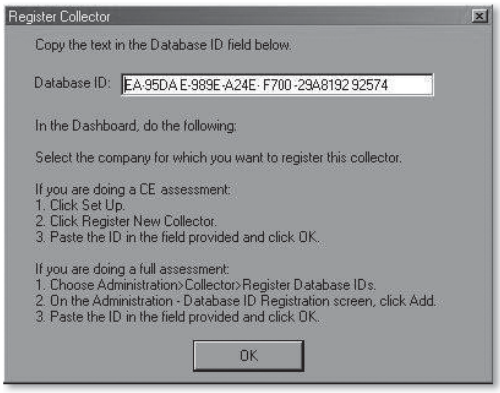


Abbildung 16.7 Registrierung des Data Collectors am Information Warehouse

Nun existiert eine Zuordnung zwischen der Company-ID, der System-ID und der Database-ID. Die Inventarisierungs-, Performance- und Log-Dateien, die der Data Collector zum Information Warehouse überträgt, werden zur Identifizierung mit der System-ID und der Zeit gestempelt. Dieses Verfahren ermöglicht eine anonymisierte Datensynchronisation zwischen dem Data Collector und dem Information Warehouse.

Die Nomenklatur der Dateien stellt sich wie folgt dar:

- *Leistungsdaten*: *Stats_<SystemID>_<yyyymmddhhmmss>.csv*
- *Inventarisierungsdaten*: *Inv_<SystemID>_<yyyymmddhhmmss>.csv*
- *Protokolldatei*: *LogFile_<SystemID>_<yyyymmddhhmmss>.log*

16.5 Das Dashboard im Detail

Das Dashboard des Capacity Planners ist, wie bereits eingangs erläutert, eine Anwendung, die von VMware gehostet und über das Internet zur Verfügung gestellt wird. Dadurch kann mittels Browser von jedem Internetanschluss aus direkt auf das Dashboard zugegriffen werden.

Aufbau und Benutzung des Dashboards

Bei der aktuellen Version des Dashboards handelt es sich um 2.8.1 Build 49255. Sie weist gegenüber der Version, die im vSphere 4-Buch erläutert wurde, viele Veränderungen auf. Im Wesentlichen wurden die bereits vorhandenen Funktionalitäten durch zusätzliche Funktionen ergänzt. Außerdem wurde die Menüstruktur des Dashboards vollständig umgebaut. Auf den ersten Blick ist es etwas ungewohnt, aber Sie werden schnell feststellen, dass die wichtigsten Werkzeuge nach wie vor vorhanden, jedoch im Menü an anderen Orten zu finden sind.

Das Dashboard stellt Ihnen über ein Menü (Abbildung 16.8) neuerdings sieben unterschiedliche Bereiche zur Verfügung. Die einzelnen Bereiche erlauben einerseits die Verwaltung des Accounts und den Zugriff auf die über die Zielsysteme gesammelten Daten und ermöglichen andererseits, auf die Auswertungsfunktionalität des Dashboards zuzugreifen.

Abbildung 16.8 Die einzelnen Rubriken des Dashboards im Information Warehouse

Den Zugriff auf das Dashboard und die Menüoptionen können Sie, falls unterschiedliche Nutzer an der Auswertung der Daten der Zielsysteme oder der Überwachung des Kapazitätsplanungsprojektes beteiligt sind, auch durch die Vergabe von Policies regeln. So ist es z. B. denkbar, dass der Hauptadministrator einen Read-only-User erstellt, der nur eingeschränkt im Dashboard agieren kann. Hierbei kann ein Benutzer, der vom Hauptadministrator erstellt und

mit administrativen Rechten ausgestattet wurde, sämtliche Funktionalitäten des Dashboards nutzen. Eine derartige Rolle könnte zum Beispiel für den Kunden oder Beauftragenden eingerichtet werden, so dass dieser während des gesamten Kapazitätsplanungsprojektes ständig alle Daten einsehen kann und somit immer gut informiert ist.

Die Funktionen der einzelnen Bereiche des Dashboards, die wir im Folgenden näher erläutern, sind von ganz unterschiedlicher Art.

Dashboards

Der Bereich Dashboards gestattet einen Überblick in Form von Statistiken über den Status der gemessenen Server (Abbildung 16.9) sowie das Inventar und der Leistungsdaten aller Zielsysteme. Außerdem können Sie in diesem Bereich unterschiedlichste Überprüfungen vornehmen. Im Einzelnen sind das Informationen darüber, wann und welche Daten vom Data Collector zum Dashboard gesendet wurden, ob Daten verworfen wurden oder wie die gewonnenen Daten sich im Detail darstellen.

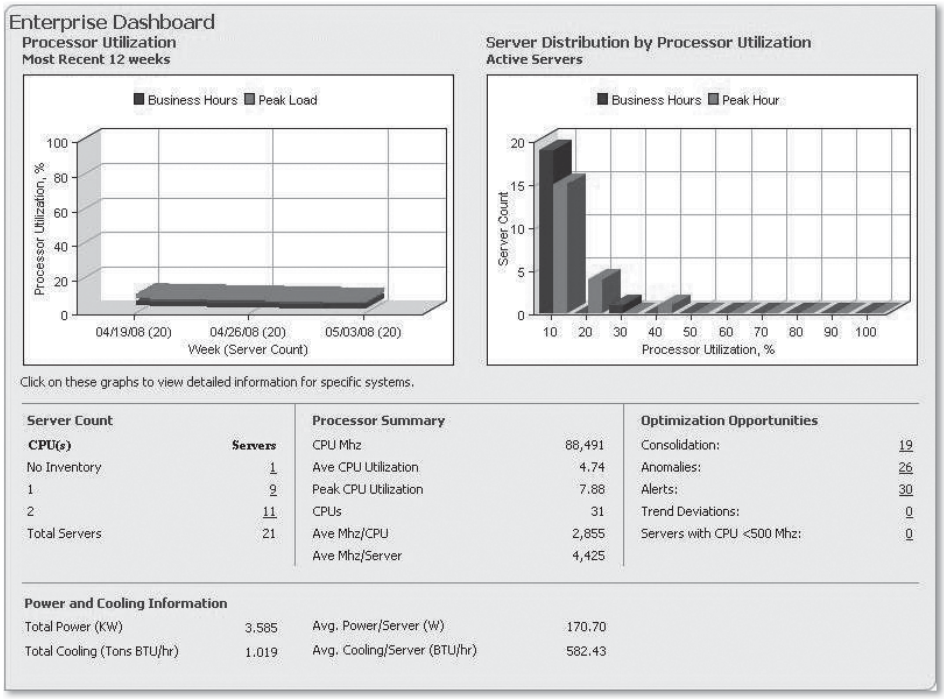


Abbildung 16.9 Gesamtüberblick über den Status der gemessenen Server

Was früher einmal unter Enterprise Summary zu finden war, befindet sich in dieser Version unter Collection Dashboard im Bereich Dashboards Abbildung 16.8. Die einzelnen Rubriken des Dashboards im Information Warehouse. Collection Dashboard gibt einen guten Überblick über die zu inventarisierenden Zielsysteme sowie deren Domain-Zugehörigkeit. In

diesem Menü befindet sich unter Desktop Dashboard der Zugang zu den Statistiken über den Status der gemessenen Desktops.

Diese Rubrik ist neu und ermöglicht Capacity-Planning-Projekte im Umfeld des Desktops bzw. der Computerarbeitsplätze, an denen der Anwender seine Arbeitet verrichtet. Capacity-Planning zur Vorbereitung von erfolgreicher Desktop-Virtualisierung werde ich in meinem Buch zur Desktop-Virtualisierung detailliert behandeln, so dass ich an dieser Stelle auf dieses Thema nicht weiter eingehen werde.

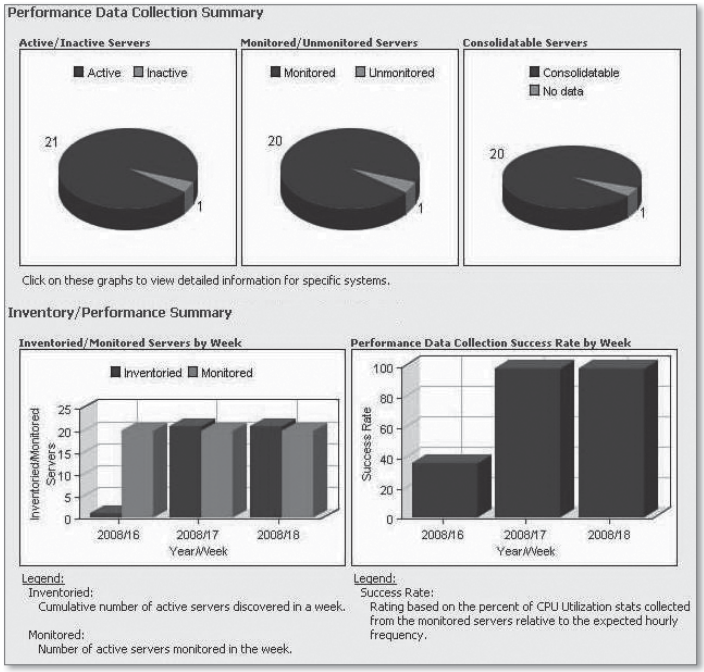


Abbildung 16.10 Zu inventarisierende Server-Systeme

Inventory

Beim Inventory geht es um die Bereitstellung der Inventarisierungsdaten der Zielsysteme. Die Inventarisierungsdaten werden in drei Rubriken unterteilt:

1. Inventory Summary
2. Software Inventory
3. Hardware Inventory
4. User Inventory
   - Login Inventory
   - Network Inventory
   - User Groups Inventory

Inventory Summary zeigt Ihnen ein vollständiges Enterprise-Summary Ihrer Zielsysteme an. Alle global relevanten Systemkomponenten wie zum Beispiel die einzelnen Nodes, die Menge der kumulierten CPUs, RAM-Cards, Disks, NICs oder die Total Power in KW und das Total Cooling in Tons BTU/hr werden geordnet nach den Node-Typen – Server und Desktops – dargestellt. Durch einfaches Anklicken einzelner Werte springen Sie direkt in den Auswertebereich.

Die Rubriken Software und Hardware Inventory enthalten allerdings eine große Zahl weiterer Unterpunkte, unter denen Sie die folgenden Analysebereiche befinden:

- Installed Applications
- Operating Systems
- Services
- File Systems
- Chassis
- Processors
- Memory
- Drives
- Drive Controllers
- Network Interface Cards
- Video Cards
- Plug and Play Devices
- Printers

An dieser Stelle kann man wirklich sagen, dass auch die Struktur des Dashboards gegenüber früheren Versionen eine enorme Verbesserung erfahren hat. Jedes einzelne für eine Analyse erforderliche Thema können Sie nun aus dem Hauptmenü heraus direkt erreichen. Die ganze Menüführung ist bedeutend intuitiver, und dadurch ist das Arbeiten mit dem Dashboard wesentlich einfacher geworden. Benötigen Sie zum Beispiel Daten zu den Video Cards – also den Grafikkarten – der Zielsysteme. können Sie diese unter dem Punkt Hardware Inventory sofort einsehen. Sind Sie an Informationen zu Ihren Applications interessiert, wählen Sie Software Inventory und dann Installed Applications; so werden alle auf den Zielsystemen installierten Applikationen aufgelistet, so dass Sie sich einen vollständigen Überblick über den Installationszustand verschaffen können. Zusätzlich zur tabellarischen Listung wird eine grafische Verteilung aller auf den Zielsystemen installierten Applikationen angezeigt. Die auf den Zielsystemen laufenden Services finden Sie unter Services. Mit File-Systems analysieren Sie alle File-Systems, die den Zielsystemen zur Verfügung stehen.

Diese Vorgehensweise gilt selbstverständlich für sämtliche Elemente, die sich unter Software Inventory und Hardware Inventory befinden.

In der Vorgängerversion des Dashboards gab es in der dritten Gruppe des Menüs den Punkt Asset Information. Hier konnten Sie den Zielsystemen weitere Inventarisierungsinformationen wie Anschaffungsdatum, Beschaffungspreis oder monatliche Kosten für Leasing hinzufügen. Dieser Punkt befindet sich nun an einer anderen Stelle im Menü. Auch hier ist der neue Einstiegspunkt, um die Daten Ihrer Assets zu ergänzen, wesentlich besser gewählt worden. Sie finden im Menü Reports unter Asset Information Reports eine Liste Ihrer Zielsysteme. Wählen Sie eines Ihrer Zielsysteme aus, und klicken Sie es an. Anschließend klicken Sie auf den Reiter Asset Info. Nun öffnet sich eine neue Seite, auf der Sie Ihre Zusatzdaten zu Ihren Assets angeben können. Wollen Sie von dieser Seite wieder zurück in den Hauptbereich oder auf die Seite, die auch das Hauptmenü enthält, klicken Sie einfach unten rechts auf den Button Close.

Die dritte Rubrik ermöglicht Zugang zu den Bereichen User-, Login-, Network- und User-Groups-Inventory. In diesen Bereichen finden Sie Details zur Benutzeranmeldung oder zum Benutzerstatus und die Anzahl der Benutzerkonten. Außerdem können Sie unter Network Inventory unter anderem umfassende Netzwerkinformationen wie zum Beispiel Name, Mask oder Gateway sowie unterschiedlichste Informationen über Anwender anzeigen. Mit dem letzten Punkt, User Groups Inventory, erstellen Sie eine Inventarliste der Benutzergruppen.

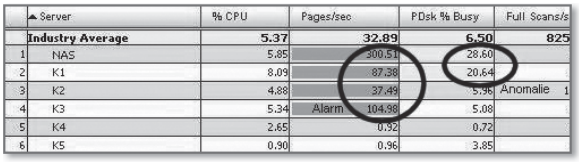
Performance

Von den Hunderten unterschiedlichster Arten von Leistungsdaten, die aus den Zielsystemen gewonnen werden könnten, werden effektiv nur wenige benötigt. Da dem Capacity Planner durch die Inventarisierung bekannt ist, welche Software auf den Zielsystemen installiert ist, berücksichtigt er nur die Leistungsindikatoren, die in direktem Zusammenhang mit der installierten Software stehen. Dadurch werden auf höchst effiziente Weise nur die Messwerte genommen, die tatsächlich benötigt werden. Es werden für jeden Indikator Minimal-, Maximal- und Durchschnittswerte aufgezeichnet.

1. Performance Summary
   - Storage Summary
   - User Summary
   - Network Summary
   - Location Summary
2. Forecast Critical Processors
   - System Processors Balance
   - System Processors Load
   - Network Latency
   - Trends
3. Performance Groups

Im Menüpunkt Performance Summary können Sie die gemessenen Leistungsdaten der Zielsysteme mit den Industriedurchschnittswerten des Information Warehouse sowie den darin

hinterlegten Benchmarks von Softwareherstellern gegenüberstellen. Die Industriedurchschnittswerte setzen sich aus allen Daten der letzten vier Wochen zusammen, über die das Information Warehouse verfügt. Dadurch können Systeme identifiziert werden, die signifikant vom Industriedurchschnitt abweichen. In einer tabellarischen Darstellung werden die vom Data Collector gemessenen Basisleistungswerte den entsprechenden Industriedurchschnittswerten gegenübergestellt und Alarme sowie Anomalien farbig hervorgehoben (Abbildung 16.11).



	Server	% CPU	Pages/sec	PDsk % Busy	Full Scans/s
	Industry Average	**5.37**	**32.89**	**6.50**	**825**
1	NAS	5.85	300.51	28.60	
2	K1	8.09	87.38	20.64	
3	K2	4.88	37.49	5.96	Anomalie 1
4	K3	5.34	Alarm 104.38	5.08	
5	K4	2.65	0.92	0.72	
6	K5	0.90	0.96	3.85	

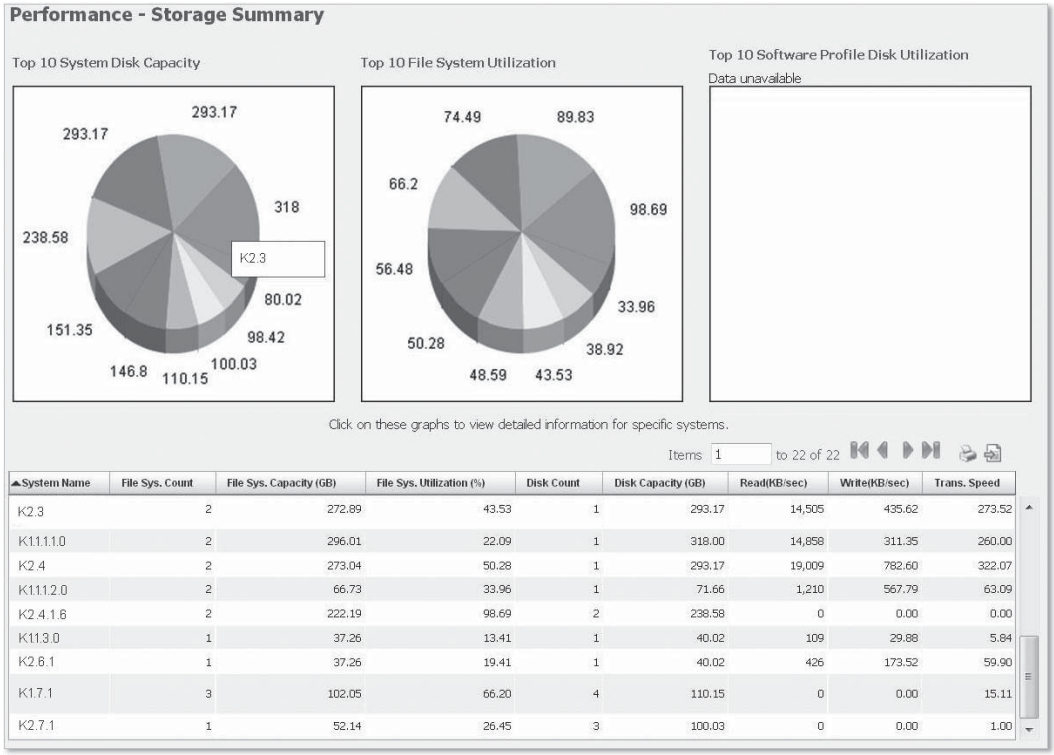
Abbildung 16.11 Unter »Performance Summary« wurde innerhalb von »Data Filter Performance Counters« auf »MS SQL Server« gestellt.

Hierbei steht Rot für Alarme. Alarme treten auf, wenn die vom Data Collector gelieferten Messwerte die von den Softwareherstellern hinterlegten Schwellenwerte überschreiten. Gelb hinterlegte Felder stehen für Anomalien, die auftreten, wenn die Messwerte zu stark von den Industriedurchschnittswerten abweichen.

Im Menüpunkt Storage Summary können Sie die Messwerte, die in unmittelbarem Zusammenhang mit den Speichersystemen stehen, einsehen und analysieren. Abbildung 16.12 gibt Ihnen einen Eindruck von der Art der Darstellung. Alle Werte mit Relevanz werden übersichtlich in Form einer Tabelle gelistet. Durch Anklicken einzelner Zielsysteme in der Tabellenspalte System Name gelangen Sie direkt in den Bereich, der alle Daten des ausgewählten Zielsystems enthält. Außerdem werden in Form von dreidimensionalen Kreisdiagrammen die unterschiedlichen Verteilungen von Häufigkeiten wichtiger Parameter dargestellt. Klicken Sie einen der Kreisausschnitte in einer der Grafiken an, beispielsweise den Bereich 318 GB Datenträgerkapazität, werden Sie auf eine andere Seite verlinkt. Diese Seite zeigt dann ebenfalls grafisch unterstützt ein sehr genaues Bild vom Storage des entsprechenden Zielsystems.

Die Auswertungsbereiche User-, Network- und Location-Summary sind von der Art des Aufbaus und der Strukturierung quasi identisch und liefern Ihnen themenbezogen ebenfalls detaillierte Informationen.

Die Funktion Forecast Critical Processors identifiziert die kritischen Server, ermöglicht dann den Einstieg in die nähere Untersuchung der einzelnen Server und gibt einen Ausblick auf die zukünftige Entwicklung (Abbildung 16.13). Nehmen wir einmal an, dass einer der zu betrachtenden Server als kritisches System eingestuft wurde. In Forecast Critical Processors sehen wir nun detailliert in tabellarischer und in grafischer Darstellung, welche Indikatoren betroffen sind und wie sie sich voraussichtlich in Kürze entwickeln werden.



System Name	File Sys. Count	File Sys. Capacity (GB)	File Sys. Utilization (%)	Disk Count	Disk Capacity (GB)	Read(KB/sec)	Write(KB/sec)	Trans. Speed
K2.3	2	272.89	43.53	1	293.17	14,505	435.62	273.52
K1.1.1.1.0	2	296.01	22.09	1	318.00	14,858	311.35	260.00
K2.4	2	273.04	50.28	1	293.17	19,009	782.60	322.07
K1.1.1.2.0	2	66.73	33.96	1	71.66	1,210	567.79	63.09
K2.4.1.6	2	222.19	98.69	2	238.58	0	0.00	0.00
K1.1.3.0	1	37.26	13.41	1	40.02	109	29.88	5.84
K2.6.1	1	37.26	19.41	1	40.02	426	173.52	59.90
K1.7.1	3	102.05	66.20	4	110.15	0	0.00	15.11
K2.7.1	1	52.14	26.45	3	100.03	0	0.00	1.00

Abbildung 16.12 »Storage Summary«

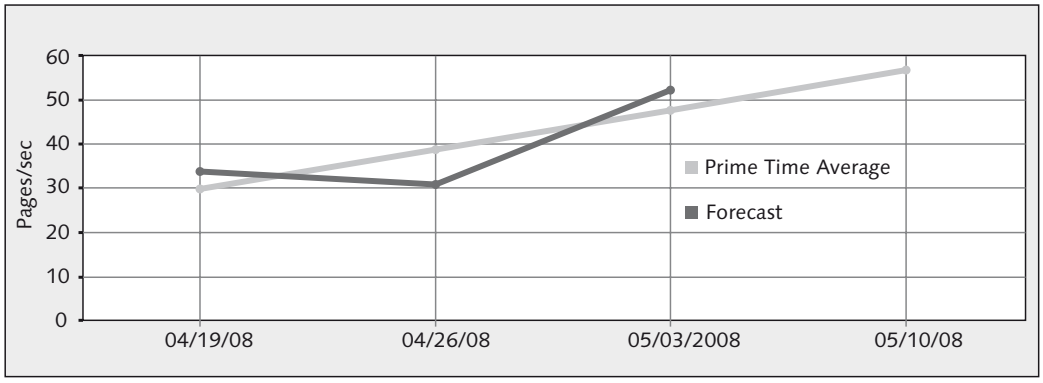


Abbildung 16.13 Der helle Graph stellt die voraussichtliche Entwicklung eines erhöhten Paging-Aufkommens dar.

Das Dashboard erstellt eine Vorhersage und zeigt die zukünftige Entwicklung der betroffenen Indikatoren auf.

Mittels System Processors Balance (ehemals Server Processors Balance, so steht es auch noch in der Online-Hilfe) werden die Unterschiede bei den Nutzungsgraden der einzelnen

CPUs respektive CPU-Kerne eines Servers, die als äußerst signifikant in Erscheinung treten, gekennzeichnet. In der aktuellen Version der System Processors Balance wird davon ausgegangen, dass physische Server, die zur Disposition stehen, nach wie vor maximal acht CPUs besitzen, unabhängig davon, ob es sich um logische oder physische Kerne handelt. Somit wird eine CPU, die über einen physischen Kern mit Hyperthreading- oder Multithreading-Implementierung verfügt, in der Auswertung als zwei getrennte CPUs dargestellt.

Im Tabellenausschnitt in Abbildung 16.14 sehen Sie die Leistungswerte der CPUs einiger der physischen Server, die der zu untersuchenden Gruppe angehören. Die mit einer stärkeren Umrahmung gekennzeichneten Bereiche zeigen die eingangs erwähnten signifikant unterschiedlichen Prozessorauslastungen der zu untersuchenden Server-Systeme.

	Server	CPU0	CPU1	CPU2	CPU3	CPU4	CPU5	CPU6	CPU7
1	NAS	21,70	19,34	-	-	-	-	-	-
2	K1	11,98	14,94	3,88	3,51	-	-	-	-
3	K2	4,05	3,96	5,67	3,79	-	-	-	-
4	K3	7,03	5,61	-	-	-	-	-	-
5	K4	3,22	2,74	3,10	3,22	-	-	-	-
6	K5	2,22	0,45	0,39	0,56	-	-	-	-

Abbildung 16.14 Unterschiedliche Belastung der CPUs eines Servers

In unserem Beispiel gilt es zu beachten, dass die Server K1 und K2 (Abbildung 16.14) mit CPUs bestückt sind, die über einen physischen Kern mit Hyperthreading-Erweiterung verfügen, die CPU von K3 jedoch nicht. Die Processor Balance Table stellt sich nun wie in Abbildung 16.15 dar.

Host Name	HyperThreaded
K1	True
K2	True
K3	False
K4	True

Abbildung 16.15 Server mit und ohne Hyperthreading-CPUs

Die erste physische CPU von K1 wird stark genutzt, die zweite physische CPU in wesentlich geringerem Umfang. In der Tabelle (Abbildung 16.14) stellen CPU0 und CPU1 jeweils einen logischen Kern der ersten physischen CPU dar. CPU2 und CPU3 von K1 bilden die zweite physische CPU des Servers. Diese zweite CPU ist gegenüber der ersten CPU in geringerem Umfang ausgelastet. Derartige Sachverhalte deuten oftmals darauf hin, dass die Dienste der physischen Systeme keine optimale Nutzung im Hinblick auf den Einsatz von Multiprozessor- oder Multikernsystemen und Hyperthreading-Implementierung gewährleisten.

Eine weitere Möglichkeit, sich die physischen Server anzuschauen, ist die Überprüfung mittels System Processors Load. Die Untersuchung der Prozessorauslastung wird ebenfalls über eine Tabelle (Abbildung 16.16) ermöglicht. Sie gibt Aufschluss darüber, wie hoch die Auslastung während der Business Hours (Hauptgeschäftszeit zwischen 7 Uhr und 18 Uhr) und der Peak Hour (Hauptbelastungszeit) ist.

	Server	CPUs	Mhz	Business Hours	Peak Load	Peak Hour
1	NAS	2	1,862	20.52	31.26	0
2	K1	2	3,051	8.58	17.60	2
3	K2	2	3,052	4.37	7.58	2

Abbildung 16.16 Prozessorauslastung bezogen auf die volle Stunde

Die Spalte CPUs gibt an, wie viele CPUs ein Server enthält. Der Wert zeigt ausschließlich physische Kerne an. Unter MHz wird die Taktfrequenz der CPU angezeigt. Business Hours stellt dar, wo die mittlere Auslastung der CPU während der Geschäftszeit liegt, und Peak Load informiert über die mittlere Belastung während der Hauptbelastungszeit. Die Peak Hour steht für eine Stunde innerhalb des 24-Stunden-Rhythmus; eine 1 bedeutet also 1 Uhr, eine 0 bedeutet 0 Uhr, und die 17 steht für 17 Uhr.

Ein neu hinzugekommener Punkt namens Network Latency gestattet Ihnen eine erweiterte Auswertung des Netzwerkes. Hier wird die Latenz der beteiligten Core-Netze zur weiteren Auswertung und Beurteilung in einer Tabelle dargestellt. Bei den zur Auswertung zur Verfügung stehenden Daten handelt es sich um gemessenes Zahlenmaterial zu den folgenden Zeilenüberschriften:

- Destination Network
  (Zielnetzwerk)
- Low Value ms
  (Minimalwert in Millisekunden) ms
- Business Hours Peak Load
  (Maximalwert innerhalb der Hauptgeschäftszeit in Millisekunden)
- Average Value ms
  (Mittelwert in Millisekunden)
- Peak Hour
  (Hauptbelastungszeitraum)

Die Performance-Trend-Analyse Trends zeigt die acht Hauptleistungsindikatoren eines physischen Server-Systems über einen Messzeitraum von bis zu 13 Wochen an (Abbildung 16.17). Die Darstellung der Hauptleistungsindikatoren ist so skaliert, dass alle acht Parameter in einem Diagramm dargestellt werden können. Hierdurch wird es möglich, alle Hauptleistungsindikatoren über die gleiche Zeitspanne zu beobachten. Geht zum Beispiel aus dem Diagramm eine hohe Belastung der CPU zeitgleich mit hohem Aufkommen an Memory-Paging hervor, können Sie daraus schließen, dass nicht ein Dienst oder eine Applikation das System überlastet, sondern aller Voraussicht nach ein Mangel an Hauptspeicher die Ursache für das Verhalten des Systems ist.

Oftmals erkennen Sie genau an diesem Sachverhalt, nämlich dass zwei oder mehr Indikatoren zeitgleich ein ähnliches Verhaltensmuster aufweisen, dass eine Anomalie vorliegt.

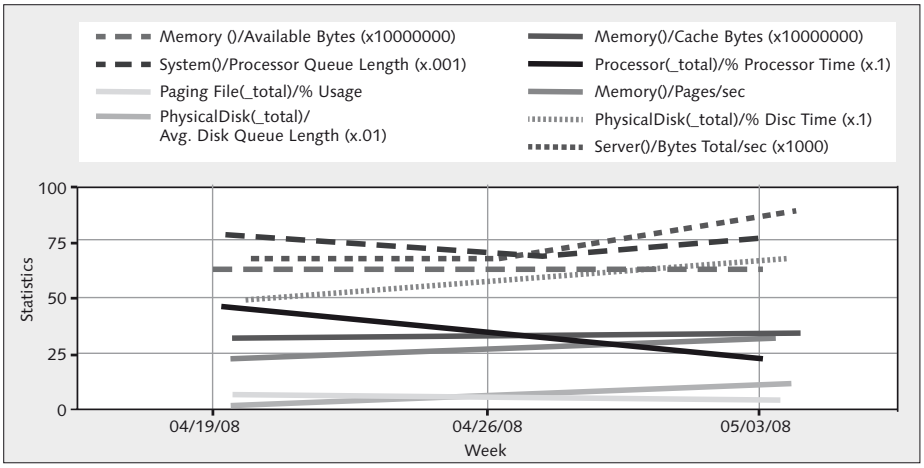


Abbildung 16.17 Trendanzeige der acht Hauptleistungsindikatoren

Analyze

Bevor Sie die einzelnen Systeme optimieren können, müssen Sie erst einmal herausfinden, welche Systeme und Applikationen überhaupt Performanceprobleme haben. Wie in früheren Abschnitten bereits erläutert, überprüft das Dashboard des Capacity Planners, wie die Server-Daten im Vergleich zu Hersteller-Benchmarks und industriellen Mittelwerten stehen.

Hier noch einmal zur Erinnerung: Anomalien liegen den industriellen Mittelwerten zugrunde und Alarme den Benchmarks der Hersteller.

Server und Applikationen, die außerhalb der üblichen Parameter arbeiten, werden gekennzeichnet. Außerdem werden diejenigen Systeme identifiziert, die ihre Ressourcen unverhältnismäßig verbrauchen oder diese nicht effizient nutzen. Also werden die Daten in tabellarischer Form angezeigt, und Sie können sie nach Belieben sortieren. Die Indikatoren, bei denen die Hersteller-Benchmarks oder die generischen industriellen Mittelwerte überschritten wurden, werden mit einem Flag versehen.

Diese Kennzeichnung ermöglicht das genaue Erkennen der Schwächen der Systeme. Hierdurch können Sie z. B. feststellen, welche Dienste sich für eine Konsolidierung eignen. Auch erkennen Sie in diesem Bereich der Untersuchung, inwieweit Sie physische Systeme verändern sollten, um eventuelle Schwächen der Systeme zu kompensieren. In einem nächsten Schritt können Sie dann das physische System entsprechend verändern. Im Anschluss an eine solche Maßnahme wird eine erneute Messung unter Umständen zeigen, dass der Mangel behoben ist und eine Migration unter den aktuellen Aspekten durchaus sinnvoll sein könnte.

Die vergangenen vier Wochen stehen zur Auswertung der Daten im Bereich Anomalien und Alarme zur Verfügung. Über eine Filterfunktion ist es möglich, jeweils eine der vergangenen vier Wochen für eine Analyse auszuwählen. Wie Sie in den entsprechenden Tabellen (Abbildung 16.18 und Abbildung 16.19) sehen, werden alle Zielsysteme, die Anomalien oder

Alarme aufweisen, gelistet. Hierbei werden die Anomalien oder Alarme nochmals unterschiedlich gekennzeichnet, je nachdem, wie stark die Werte vom Schwellenwert abweichen.

	Host	Average Weeks of Data	Statistics Found	Average Anomaly Score
1	NAS	2	4	3.86
2	K3	2	1	3.19
3	K6	2	1	3.63

Abbildung 16.18 Anomalien

Überschreitet z. B. ein Indikator den Schwellenwert des generischen industriellen Mittelwertes, wird er in der entsprechenden Tabelle (Abbildung 16.19) durch ein rotes Ausrufungszeichen gekennzeichnet. Die Überschreitung des Thresholds durch den Prime Time Average ist im vorliegenden Fall überdeutlich.

	Info	Inv	Perf	Class (Instance) \ Metric	Industry Average	Threshold	Standard Deviations	Prime Time Average	Low Load	Peak Load
1		I	P	Memory () \ Cache Bytes Peak	310.66	400.00	0.00	1755.63	1755.63	1755.63

Abbildung 16.19 Auflistung aller Anomalien eines Zielsystems

Der Mittelwert aller Standard Deviations (Abbildung 16.19) eines Zielsystems entspricht dem Average Anomaly Score (Abbildung 16.18), wobei Statistics Found (Abbildung 16.20) die Summe aller Anomalien eines Zielsystems anzeigt.

	Host	Average Weeks of Data	Statistics Found	Average Alert Score
1	NAS	2	3	4.56
2	K3	2	1	3.23
3	K1	2	3	1.32

Abbildung 16.20 Alarme

Unter Trend Deviations können Sie alle Zielsysteme betrachten, bei denen die aktuellen Daten erheblich von den für sie ursprünglich ermittelten Trend- bzw. den tendenziell zu erwartenden Daten abweichen. Unter Forecast Alerts werden möglicherweise eintretende Alarme einzelner Leistungsindikatoren angezeigt. Die Voraussage erstreckt sich über einen Zeitraum von höchstens einem Jahr. Die Spalte Weeks Till Alert gibt an, in wie vielen Wochen mit einem Alarm bei dem entsprechenden Indikator zu rechnen ist.

Unter dem Menüpunkt Software Analysis finden Sie den Button Select Profiles. Auf dieser Seite können Sie aus einer umfangreichen Liste sogenannte Application Profiles (Abbildung 16.21) auswählen. Hierbei handelt es sich um Applikationen, deren Belastungsprofile bezüglich der Hardware, auf denen sie betrieben werden, zur Verfügung stehen. Diese Applikationsprofile zeigen z. B. die mittlere Anzahl von CPUs eines Servers an, auf dem eine der ausgewählten Applikationen läuft.

Unter Hardware-, Network-, Location- und User-Analysis ist es möglich, unter Zuhilfenahme von Profile Wizards eigene Profile zu erstellen. Diese Profile können Sie dann im Zuge der Auswertung einsetzen.

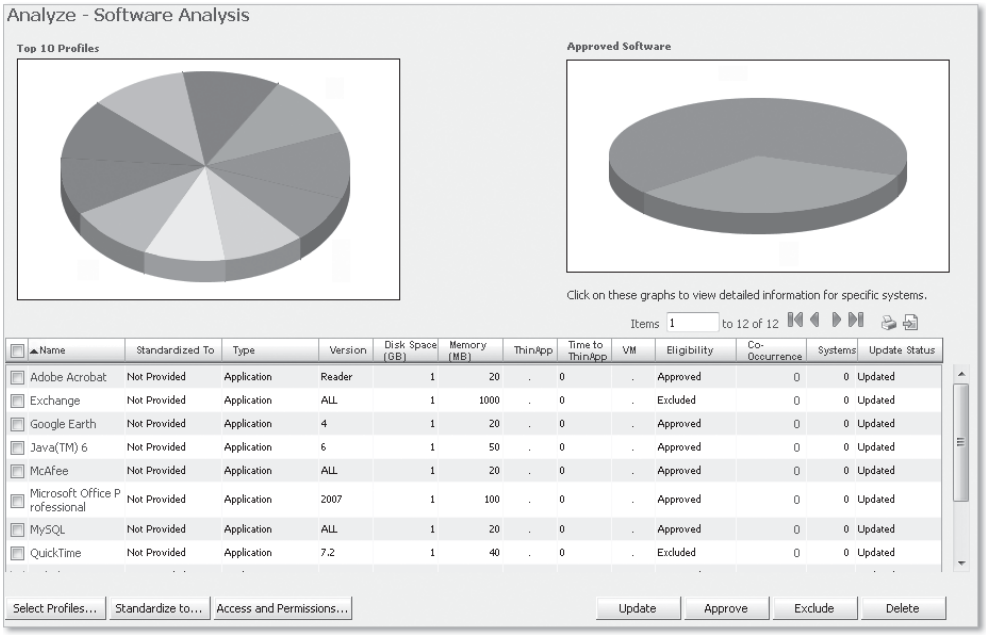


Abbildung 16.21 In »Software Analysis« wählen Sie die unterschiedlichen »Application Profiles« aus.

Auch der Menüunterpunkt Base Images ist neu hinzugekommen. Er führt zur Seite Software Base Image Management. Hier können Sie Software Base Images erstellen, die Sie später innerhalb des Optimization Scenarios auswählen und nutzen können.

Die Auswahl Optimization Scenarios gestattet den Zugang zur Kernfunktionalität des Data Warehouse. Da in dieser Version des Data Warehouse der Menüeintrag Optimize weggefallen ist, befindet sich der Zugang zum Optimization Scenarios nun auch recht passend hier im Menüpunkt Analyze. Das Konsolidierungsszenario stellt nach wie vor ein Framework bestehend aus einzelnen Punkten wie Gruppenbildung, Scenario-, Hardware-, Report- und Notification-Templates dar. Die Beziehungen zwischen Templates, Szenarien, Gruppen und Schwellenwerten ist in Abbildung 16.22 grafisch dargestellt.

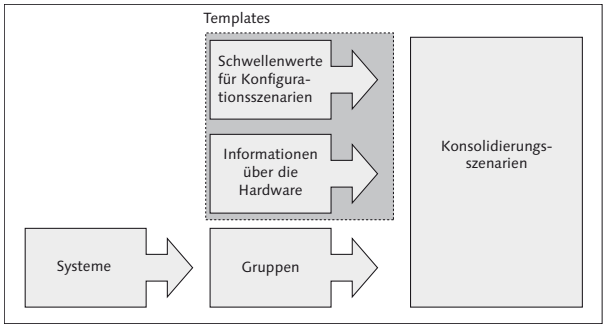


Abbildung 16.22 Konsolidierungsszenario

Wir werden in Abschnitt 16.7, »Auswertung«, noch hinreichend auf die Funktionen und den Umgang mit dem Optimization Scenarios eingehen.

Mittels Compare Systems können Sie die Belastungsdaten von Servern anzeigen, auf denen eine bestimmte Applikation läuft. Diese Belastungsdaten sind gesammelte Industriedaten und stammen aus dem Bestand des Information Warehouse. Die vom eigenen Data Collector gemessenen Belastungsdaten der Server beziehen sich auf die Applikation, die im zu vermessenden Environment, in dem der Data Collector steht, vorhanden sind. Hier ist es nun möglich, dass die Daten einer bestimmten Applikation ausgewählt und angezeigt werden. Die Belastungsdaten aus dem Information Warehouse lassen sich ebenfalls bezüglich einer bestimmten Applikation filtern (Abbildung 16.23).

Abbildung 16.23 Die Auswahl eines Applikationsfilters, der auf die Belastungsdaten aus dem Information Warehouse angewendet wird

Somit können Sie nun die gemessenen Belastungsdaten vom eigenen Data Collectorden Belastungsdaten aus dem Information Warehouse, die bezüglich der gleichen Applikation gefiltert wurden, gegenüberstellen (Abbildung 16.24).

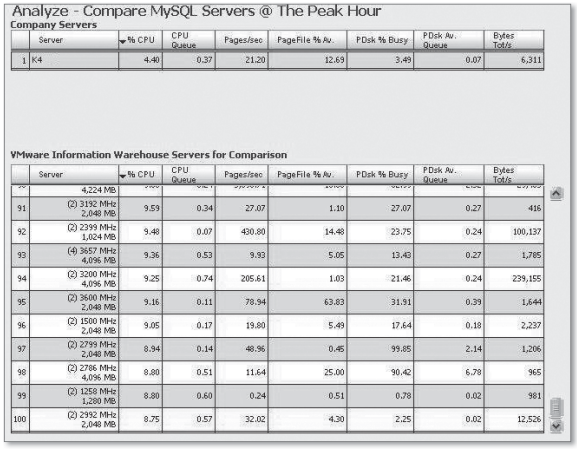


Abbildung 16.24 Gegenüberstellung der Belastungsdaten

Damit Sie auch die eigenen inventarisierten Server-Hardware-Daten und die Server-Hardware-Daten aus dem Information Warehouse möglichst in Übereinstimmung bringen können, stehen die Daten von 100 Servern wahlfrei zum Vergleich zur Verfügung. Hierbei hat das Information Warehouse in einer Vorabanalyse bereits eine möglichst große Übereinstimmung der Leistungsdaten ermittelt.

An dieser Stelle ist es sinnvoll, einen kurzen Blick in das Menü Project zu werfen, da Sie durch die neue Menüstruktur nun die meisten Templates dort erreichen sind. Hier im Menü Project unter Project Tools • Project Global Settings können Sie Parameter einstellen, die eine Auswertung oder Beurteilung der Konsolidierungsvorhaben ermöglichen. Das Formular Allowed Hardware Templates gestattet Ihnen als Administrator des Dashboards, für andere Nutzer Einschränkungen bei der Auswahl von Hardware-Templates vorzunehmen; z. B. sind prinzipiell zwei Einstellungen grundsätzlich möglich:

Zum einen können Sie alle Templates für die Auswertung und Beurteilung zulassen. Zum Anderen berechtigt Sie die andere Einstellung dazu, Templates nach Hersteller, Name eines Templates oder nach der Modellbezeichnung der Hardware für die Auswertung zu nutzen. Unter Project Tools • Scenario Templates • CE Scenario and Hardware Templates legen Sie die Bedingungen, wie eine Auswertung oder Beurteilung abzulaufen hat, fest. Ebenfalls hier im Menü Project unter Project Tools • Szenario Templates können Sie mit New... die Vorlage A Blank Scenario benutzen. Mit A Blank Scenario ist es beispielsweise erforderlich, alle Einstellungen über den Consolidation Scenario Template Wizard selbst vorzunehmen. In anderen Vorlagen wie CE Moderate Scenario Template oder CE Aggressive Scenario Template wurden bereits diverse Einstellungen getroffen. Die Angaben, die Sie unter Report Titles and Labels machen können – Basisinformationen der Auswertung des Konsolidierungsvorhabens im System –, finden Sie jetzt auch hier im Menü Project unter Project Tools • Project Global Settings und dann im Reiter Report Titles and Labels.

1. Software Analysis
   - Hardware Analysis
   - Network Analysis
   - Location Analysis
   - User Analysis
2. Base Image
   - Optimization Scenarios
3. Anomalies
   - Alerts
   - Trend Deviations
   - Forecast Alerts
4. Compare Systems

Reports

Ebenfalls neu in dieser Version des Data Warehouse ist der Menüpunkt Reports. Sie können in diesem Bereich alle möglichen Reports erstellen und einsehen. Die Menüstruktur ist hierbei wie folgt gegliedert:

1. Custom Reports
   - Optimization Reports
2. Asset Information Report
   - Vintage System Report
3. Optimization Report

Unter Custom Reports können Sie einerseits neue Templates für diverse Reports durch einen Report Wizard erstellen und andererseits Berichte selbst generieren. Das Erstellen von Berichten basiert entweder auf Standardvorlagen, die schon im System hinterlegt sind, oder auf selbsterstellten Vorlagen. Die Berichtsgenerierung ist auch zeitgesteuert möglich. Eigens zu diesem Zweck steht ein entsprechender Automatismus zur Verfügung. Die Vorgehensweise ist wie folgt: Zuerst ordnen Sie einer Report-Vorlage, z. B. einer aus den im System hinterlegten, eine Company-ID zu. Im Anschluss daran nutzen Sie diese Report-Vorlage dann entweder so, wie sie ursprünglich erstellt wurde, oder Sie ändern sie entsprechend den eigenen Wünschen ab. Nun können Sie anhand der soeben erstellten Vorlage ein neues Report-Template erstellen und über New TemplateS from reports zur Reporterzeugung nutzen.

Optimization Reports stellt eine Rubrik zur Verfügung, in der Sie mit drei möglichen Varianten zur Generierung von Berichten arbeiten können. Die Berichtsvarianten sind nach wie vor der Zwischenbericht und der finale Bericht, wobei es für den finalen Bericht nun zwei unterschiedliche Ausprägungen gibt: eine Executive Summary Presentation und ein Assessment Report erstellen. Schon der Zwischenbericht hat gegenüber früheren Versionen eine deutlich höhere Qualität erreicht. Dafür, dass der Progress Report lediglich einen Überblick über den Status der aktuell laufenden Überprüfung liefern soll, ist der automatisiert erzeugte Zwischenbericht bereits mehr als hinreichend. Die Executive Summary Presentation ist ein PDF-Dokument, das an eine Folienpräsentation in der Machart eines Management-Summarys erinnert. Mit dieser Präsentation können Sie eine umfassende High-Level-Zusammenfassung durchführen. Der dritte Report, der Assessment Report, stellt den finalen Bericht des Assessments dar. Er ist recht umfangreich und enthält alle relevanten Daten und Messwerte. Auch die Arbeitsweise und Funktion des Capacity-Plannings wird erläutert. Außerdem ist der Bericht bereits mit einem Inhaltsverzeichnis und einer Gliederung versehen. Hier können Sie jetzt ansetzen und den finalen Bericht dann mit Ihren Erfahrungen und Schlussfolgerungen versehen, so dass auf der Basis dieses Berichts ein erfolgreiches Projekt möglich wird. Sowohl Zwischen- als auch die finalen Berichte können Sie in dieser Rubrik erzeugen und dann natürlich auch herunterladen.

Unter EDIT REPORT SETTINGS können Sie im Bereich REPORT LABELS und REPORT TITLES Projektname und andere projektrelevanten Daten anpassen. Diesen Bereich erreichen Sie auch direkt über den Menüeintrag OPTIMIZATION REPORT SETTINGS. Auch neu ist der Eintrag ASSET INFORMATION REPORT. Hierbei handelt es sich allerdings lediglich um eine Tabelle, in der alle Zielsysteme übersichtlich aufgelistet sind. Durch das Anklicken eines der Zielsysteme gelangen Sie sofort in die Datendarstellungsbereiche (HARDWARE, SOFTWARE, SERVICES, ASSET INFO, LOAD PROFILE, TRENDING, GROUPS und RECOMMENDATIONS) der einzelnen Zielsysteme.

Der Bereich VINTAGE SYSTEM REPORT ist mit dem Bereich ASSET INFORMATION REPORT zu vergleichen. Der Aufbau ist quasi identisch. Hier können Sie ebenfalls die Datendarstellungsbereiche der vorhandenen Vintage-Systeme direkt anspringen. Vintage-Systeme sind etwas betagtere Systeme, also zum Beispiel ältere Server-Modelle mit CPU-Taktraten nicht geringer als 10 MHz, die Sie eventuell noch im Bestand haben und nun unter Virtualisierungsgesichtspunkten betrachten möchten.

Project

In der Rubrik PROJECT sind grundsätzlich alle organisatorischen Einstellungen, die den Capacity Planner betreffen, möglich. Unter REGISTER DATABASE ID tragen Sie die Database-ID des Data Collectors ein. Mit CONFIGURE COLLECTORS unter COLLECTOR TOOLS legen Sie Einstellungen des Data Collectors remote über das Dashboard fest.

Meldungen, die darüber informieren, ob z. B. der Data Collector ordnungsgemäß seine Daten an das Dashboard überträgt, lassen sich ebenfalls in dieser Rubrik definieren. Hierbei bieten sich Einstellungsmöglichkeiten, ob derartige Meldungen allen (SHARED) oder lediglich einem Einzelnen (PRIVATE) zugestellt werden.

Der Punkt MANAGE SYSTEMS gestattet es, sich mit dem Task-Status der Zielsysteme zu beschäftigen oder bestimmte Systeme vom Konsolidierungsszenario zu isolieren. Auch für den Fall, dass das Sammeln der Daten bei einem Data Collector nicht erwartungsgemäß funktioniert, unterstützen die Bereiche TROUBLESHOOT SYSTEMS und TROUBLESHOOT COLLECTORS unter COLLECTOR TOOLS Sie bei der Ursachenforschung.

Unter SYSTEM GROUPS erstellen Sie Gruppen. Hierbei wird zwischen logischen und physischen Gruppierungen unterschieden. Außerdem gibt es bereits im System hinterlegte Gruppierungsmöglichkeiten. Sie können aber auch Gruppen nach eigenen Kriterien erstellen. Eine Gruppe stellt eine Ansammlung von Servern dar, die nach bestimmten Merkmalen klassifiziert werden. Auch ist Gruppenbildung von Servern in Konsolidierungsszenarien sehr hilfreich. Sie können Gruppen nach unterschiedlichsten Kriterien bilden, wie Domain-Zugehörigkeit, Standortabhängigkeit oder Applikationsbezug.

PROJECT DATA RANGE gestattet es Ihnen, den Zeitraum einer Analyse zu selbst zu definieren. Hierbei können Sie die Wochen angeben, wann das Projekt starten und enden soll. Die Ana-

lyse basiert auf den Daten, die während der vergangenen vier Wochen des definierten Zeitbereichs empfangen wurden.

Im Untermenü Collector Tools unter Performance Counters können Sie sämtliche Leistungsmessungen, die die aktiven Indikatoren in den letzten vier Wochen lieferten, untersuchen. Sollte ein Environment derart umfangreich sein, dass die maximale Obergrenze von 500 Zielsystemen für einen Data Collector überschritten wird, müssen Sie einen weiteren Data Collector einsetzen. Hierbei kann ein Lastausgleich der eingesetzten Data Collectors erforderlich werden. Zu diesem Zweck stehen unter Load Balance Collectors und Load Balance Collectors • Systems unterschiedlichste Verfahren zur Verfügung.

Ein weiterer Punkt in diesem Abschnitt des Dashboards, Job History, zeigt eine zeitbezogene Liste aller Jobs des Data Collectors hier im Dashboard an.

Die Menüpunkte Performance Counters und Scenario Templates haben wir im Bereich des Menüpunktes Performance in Abschnitt 16.5 unter der Überschrift »Performance« bereits ausgiebig besprochen. Hierzu können Sie ebenfalls die ergänzende Abbildung 16.11 konsultieren.

Unter Custom Report Templates verwalten Sie die vorhandenen Templates für die Erstellung von Custom Reports im Menü Reports und erstellen eigene Templates.

Unter den Menüpunkten System-, Storage- und Cluster-Templates können Sie themenbezogene Templates auswählen und eigene erstellen. Ausgewählt und angewendet werden diese Templates dann innerhalb des Optimization Scenarios. Cluster-Templates benötigen sowohl System- als auch Storage-Templates. Das bedeutet, dass Sie erst die Basis-Templates erstellen müssen, bevor Ihnen ein Cluster-Template zur Verfügung steht und Sie entsprechende Testszenarien durchspielen können.

Die Seite der Software Profile Reports zeigt die vorhandenen Profilvorlagen gelistet in einer Tabelle. Hier können Sie die Mittelwerte der Daten für Processor Configuration, Memory, Peak CPU Utilization, Peak RAM Utilization, Peak Disk Utilization und Peak Network Utilization ablesen. Grafisch aufbereitet sehen Sie zusätzlich, welche Applikationen zugelassen sind und welches Virtualisierungsverhältnis vorliegt. Alle Daten können Sie zusätzlich ausdrucken oder als CSV-Datei exportieren. Die Menüpunkte Software Profile Templates und Hardware Profile Templates dienen zur Verwaltung. Wie in den anderen Vorlagenbereichen können Sie auch hier Templates auswählen und natürlich eigene Vorlagen erstellen.

1. Register Database IDs
   - Manage Systems
   - Troubleshoot Systems
   - System Groups
   - Project Data Range

2. Collector Tools
   - Configure Collectors
   - Load Balance Collectors
   - Troubleshoot Collectors
   - Load Balance Collector – Systems
   - Job History
   - Performance Counters
3. Collector Tools
   - Project Tools
   - Project Global Settings
   - Custom Report Templates
   - System Templates
   - Storage Templates
   - Cluster Templates
   - Software Profile Report
   - Software Profile Templates
   - Hardware Profile Templates

Administration

Sie können sämtliche Einstellungen den eigenen Account betreffend vornehmen. Außerdem ist es möglich, Gastkonten anzulegen, wo Sie anderen im Projekt Mitwirkenden ebenfalls gestatten, je nach administrativem Grad unterschiedlichste Einstellungen, Überwachungen oder Auswertungen vorzunehmen. Von der Passwortvergabevorschrift über das Setzen von Verfallsdaten der Gastkonten bis hin zur Überwachung, wer wo und wann welche Seite besucht oder welche Auswertung vorgenommen hat, ist in diesem Bereich alles möglich.

Unter Notifications können Sie vordefinierte Vorlagen zur Erstellung von Benachrichtigungen auswählen (Abbildung 16.25).

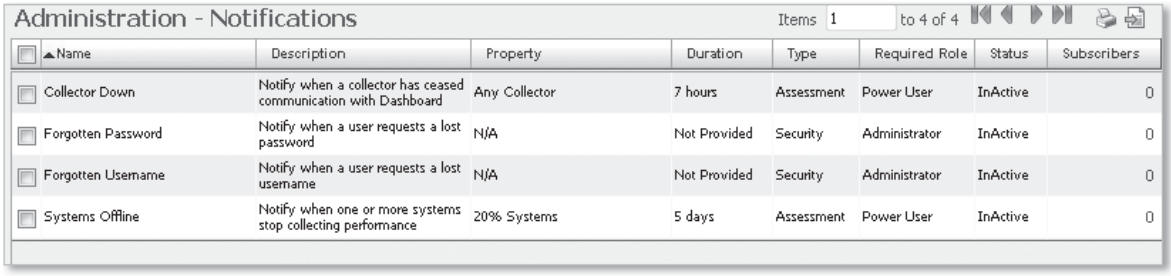


Abbildung 16.25 Auswahl von Vorlagen zur Benachrichtigung im Störfall

Nachdem Sie derartige Benachrichtigungen ausgewählt haben, können Sie sie im Menü ADMINISTRATION unter NOTIFICATIONS in die Benachrichtigungs-Queue einstellen und aktivieren.

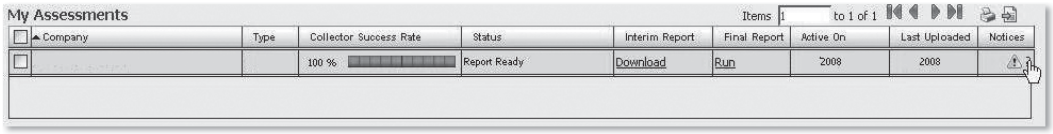


Abbildung 16.26 Abruf der Benachrichtigung im Störfall

Die Benachrichtigungen finden Sie dann im Dashboard unter HOME im Reiter COMPANIES und im entsprechenden Assessment (Abbildung 16.26). Außerdem wird eine Benachrichtigungs-E-Mail an die E-Mail-Adresse des Owners, die im Benachrichtigungsformular eingetragen wurde, gesendet.

1. MY ACCOUNT
   - CHANGE PASSWORD
2. COMPANY INFO
   - COMPANY SETUP
   - MY COMPANYS
   - MY PROJECTS
   - USERS
   - USERS GROUPS
   - ACCESS AND PERMISSIONS
   - SECURITY POLICY
   - ACTIVITY LOG
   - NOTIFICATIONS
   - SUBSCRIPTIONS

16.6 Ablauf eines Kapazitätsplanungsprojekts

Prinzipiell besteht zwischen einem Kapazitätsplanungsprojekt und jedem anderen Projekt keinerlei Unterschied hinsichtlich Organisation und Ablauf. Ein Kapazitätsplanungsprojekt erstreckt sich meistens über einen Zeitraum von vier Wochen.

Zu Beginn wird gemeinsam mit dem Auftraggeber ein Initial Workshop angesetzt. Am Ende des Kapazitätsplanungsprojektes steht ein gemeinsames Schlussmeeting mit Präsentation und Besprechung der Ergebnisse sowie des weiteren Vorgehens im Folgeprojekt – Umsetzung und

Migration. Es werden Meilensteine während des Projektes definiert und zwischenzeitlich Vorabergebnisse mit dem Auftraggeber durchgesprochen. Genau wie in thematisch anders gearteten Projekten ist eine genaue Kenntnis der Ansprechpartner, ihrer Rollen im Unternehmen und ihrer Kontaktdaten unabdingbar. Zu diesem Zweck ist es immer sehr hilfreich, sich bereits vor dem Projekt entsprechende »Contact-Info-Sheets« (Abbildung 16.27) zu erstellen und sie vom Auftraggeber ausfüllen zu lassen.

Zuständigkeit	Name	Telefon	eMail	Fax	Bemerkung
Primärkontakt (Auftraggeber)					
Primärkontakt (Auftragnehmer)					
Technischer Support (VMware)					
Technischer Support (Auftraggeber)					
Technischer Support (Auftragnehmer)					
Administration (Backup)					
Administration (Security)					
Administration (Netzwerk)					
Administration (Storage)					

Abbildung 16.27 Projektbezogene Kontaktdaten

Außerdem ist es vor Projektbeginn sehr hilfreich, sich bei dem oder den Verantwortlichen auf der Seite des Auftraggebers mittels »Pre-Screen Phone Interview« wichtige Vorabinformationen zu verschaffen, zum Beispiel: Werden lokale Administrationsrechte für jedes Zielsystem benötigt, befinden sich Proxy-Server in der Umgebung, oder ist das zu betrachtende Environment über mehrere Standorte hinweg verteilt? In diesem Zusammenhang sollten Sie den Auftraggeber auch dazu anhalten, eine Liste der zu betrachtenden Server-Systeme (Abbildung 16.28) zu erstellen.

Lfd Nr.	Computername (physikalisch)	Computername (NetBIOS)	IP-Adresse	Subnetmask	
1					
2					
3					

Abbildung 16.28 Formular zur Erfassung der Zielsysteme

Eine Gruppierung auf Tabellenebene nach Windows-, Linux- und Unix-Zielsystemen ist von Vorteil, sollte es erforderlich sein, Server-Listen in den Data Collector zu importieren.

Ein auch nicht zu vernachlässigender Faktor ist die zeitliche Abfolge des Projektes. Der Auftragnehmer ist natürlich sehr daran interessiert, dass er im Vorfeld bereits über die Timeline und die bereitzustellenden Ressourcen informiert ist. Der Data Collector hilft der Unternehmens-IT, ihre Vorhaben optimal zu unterstützen. Vergessen Sie aber bitte nicht, dass er immer noch ein Fremdkörper in der Kundenumgebung ist. Zeitverläufe lassen sich in vielerlei Art und Weise darstellen. Es gibt sehr unterschiedliche Werkzeuge, um Projekte zeitlich abzubilden.

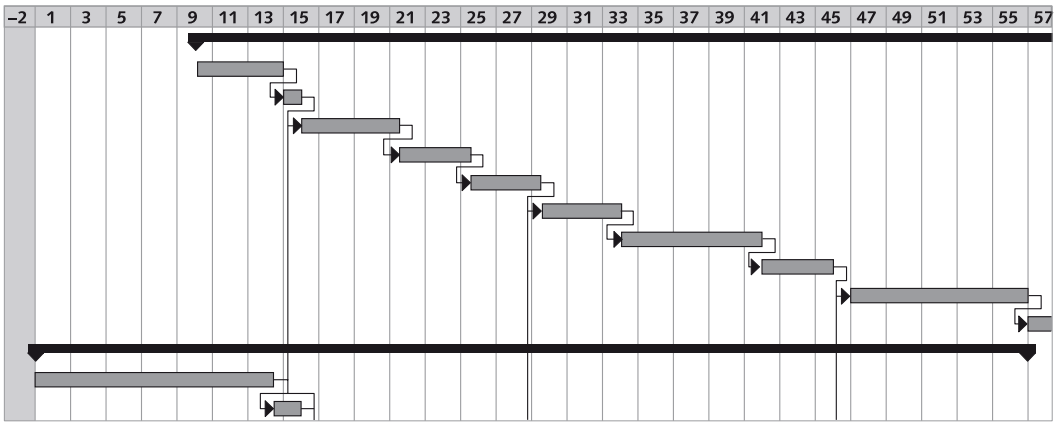


Abbildung 16.29 Gantt-Diagramm zur zeitlichen Ablaufplanung

Ob Sie nun ein Gantt-Diagramm (Abbildung 16.29) oder eine zeitliche Planung mittels Tabelle erstellen – um zwei mögliche Verfahren aufzuzählen –, bleibt Ihren Vorlieben überlassen. Fest steht allerdings, dass im Zuge eines professionell angegangenen Kapazitätsplanungsprojektes Derartiges unbedingt erforderlich ist.

16.6.1 Company-ID-Request

Wird ein Data Collector in einer Server-Umgebung einer Organisation aufgestellt, besteht seine Aufgabe grundsätzlich darin, Daten über die Server bzw. Zielsysteme und deren bereitgestellte Dienste zu sammeln. Damit die gesammelten Daten auch ausgewertet werden können, ist es unabdingbar, diese an das Information Warehouse zu übertragen. Dies wird primär aber erst dadurch möglich, dass innerhalb des Information Warehouse ein Projekt eröffnet wird. Ein derartiges Projekt geht mit der Vergabe einer Company-ID einher (Abbildung 16.30). Eine Company-ID, bezogen auf eine bestimmte Organisation, beantragen Sie bei VMware.

Solch ein Company-ID-Request ist einer der ersten Schritte in einem Kapazitätsplanungsprojekt. Sie beantragen eine Company-ID auf der Internetseite von VMware unter *http://mylearn1.vmware.com/cp/?mL_method=CompanyID*. Hier pflegen Sie in ein Formular die Daten der Organisation ein, für die Sie eine Company-ID beantragen. In der Regel dauert die Bearbeitung des Antrages 24 Stunden. Nach diesem Zeitraum steht innerhalb des Dashboards eine entsprechende Company-ID zur Verfügung. Eine detaillierte Anleitung zur Beantragung einer Company-ID erhalten Sie bei VMware unter der Überschrift »Capacity Planner Company ID Request Guide« (*http://mylearn.vmware.com/lcms/mL_faq/1147/companyidguide.doc*).

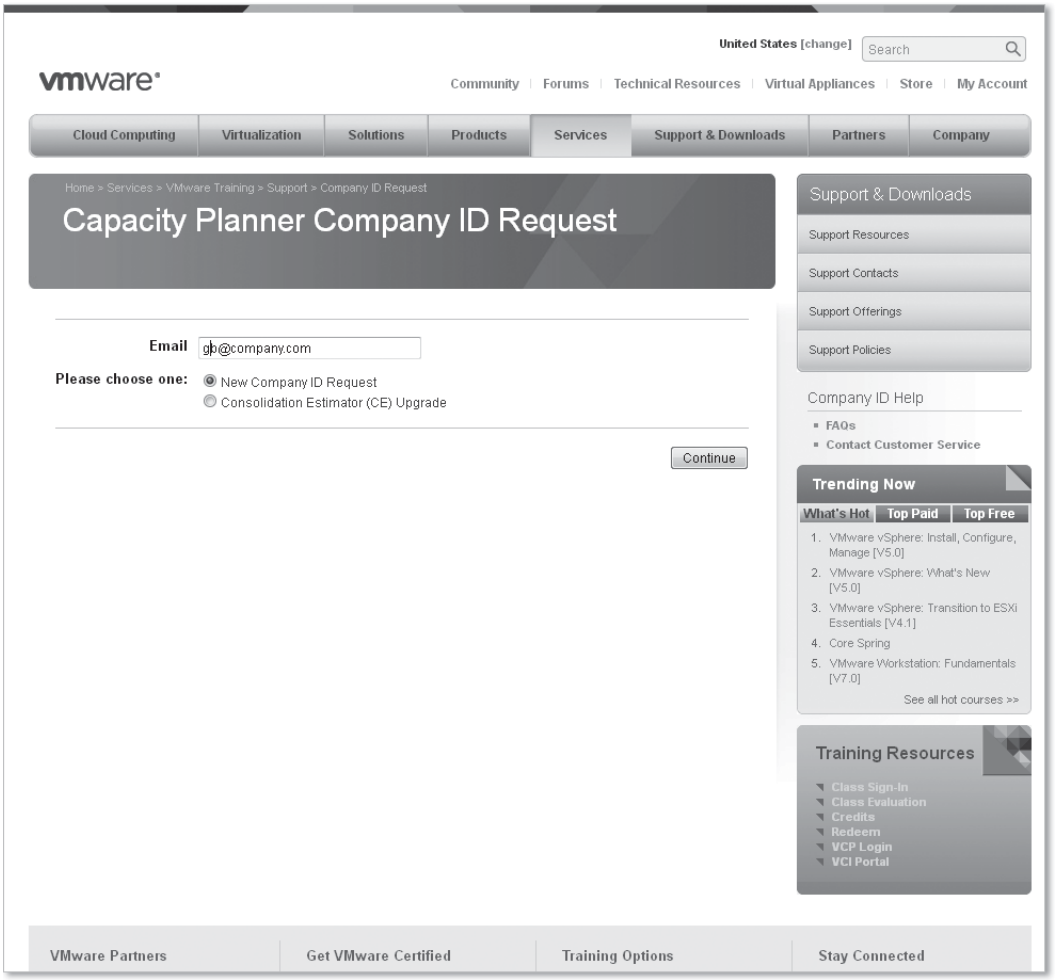


Abbildung 16.30 Einen Antrag auf die Zuteilung einer Company-ID stellen

16.6.2 Vorbereitende Maßnahmen

Da der Data Collector ja in einem fremden Environment arbeiten muss, bedarf es einiger Abstimmung mit denjenigen, die den Betrieb des zu untersuchenden Environments verantworten. Meistens sind es nur Kleinigkeiten, die eine Kapazitätsmessung behindern und dadurch für Verstimmung sorgen können. Damit es gar nicht erst so weit kommt, sind einige grundsätzliche Vorgaben, die bereits vor der Aufstellung eines Data Collectors kommuniziert werden sollten, sehr hilfreich. Hierzu gehört, dass der Data Collector einen Internetzugang benötigt. Der Data Collector wird die Verbindung zum Information Warehouse über die Ports 80 und 443 aufbauen. Dann dürfen zwischen dem Data Collector und den zu überprüfenden Systemen keine Firewalls, wie beispielsweise Desktop-Firewalls, den Informationsfluss blockieren. Des Weiteren muss sichergestellt sein, dass Remote-Registry und auch WMI auf den

zu überprüfenden Windows-Servern aktiviert wurde. Der Data Collector muss als ein zusätzlicher Server in dem Environment, in dem er arbeiten soll, betrachtet werden.

Natürlich benötigt er auch eine IP-Adresse, die Adresse eines DNS und eines Default-Gateways. Wie bereits dargelegt, ist es meistens auch von großem Vorteil, wenn eine Liste erstellt wurde, in der alle zu untersuchenden Server enthalten sind. Je detaillierter diese Liste ist, desto weniger Informationen müssen am Tag der Inbetriebnahme des Data Collectors zusammengetragen werden.

Daten wie das primäre DNS-Suffix, NetBIOS/Computernamen und dazugehörige Domänennamen, IP-Adressen sowie die entsprechenden Subnetzmasken der zu untersuchenden Server-Systeme sind oft sehr hilfreich. Ein immer wieder äußerst heikles Thema sind die Anmeldenamen und Passwörter der Zielsysteme. Die Anmeldedaten der zu untersuchenden Server müssen dem Data Collector in jedem Fall mitgeteilt werden. Hier sollten Sie im Vorfeld unbedingt darauf achten, dass am Tage der Inbetriebnahme des Data Collectors die entsprechenden Geheimnisträger zugegen sind. Der Data Collector arbeitet ohne Agenten. Hieraus folgt, dass er die unterschiedlichen Dienste eines zu untersuchenden Servers bezüglich Inventarisierungs- und Performancedaten befragt. Es muss sichergestellt sein, dass Ping, Traceroute, Zugriff auf Remote-Registry, den Performance Manager usw. bei Zielsystemen mit Windows-Betriebssystem möglich sind. Linux- oder Unix-Server müssen über Ping und Traceroute erreichbar und der Zugriff muss über Secure Shell möglich sein.

Die Umgebungen, in denen der Data Collector eingesetzt wird, verfügen oftmals über Notstromversorgungen. Es ist von großem Vorteil, dass der Data Collector hiervon profitiert. Ein störungsfreier Betrieb des Data Collectors muss in jedem Fall das Ziel sein. Immer wieder wird während des Messzeitraumes der Data Collector als Verursacher von zusätzlicher Netzlast gesehen. In dem Zeitraum, in dem der Data Collector läuft, kommt es natürlich in den im Data Collector gesetzten Messintervallen zu diversen Anfragen an die zu untersuchenden Server-Systeme. Diese Transfers sind allerdings innerhalb eines mittelstark belasteten Netzes eher vernachlässigbar und in der Regel von äußerst kurzer Dauer. Es ist natürlich niemals wirklich auszuschließen, dass unter Umständen einzelne Systeme während der Messzyklen mit unterschiedlichen Meldungen reagieren. Dies ist während einer Datensammlung allerdings völlig normal.

Betriebssysteme, die zur Analyse freigegeben sind

Nachfolgend sind die Betriebssysteme aufgeführt, die von der Version 2.8 des Capacity Planner Data Collectors untersucht werden können. Natürlich wächst die Liste der zu betrachtenden Betriebssysteme mit jeder neuen Version des Capacity Planner Data Collectors.

1. Microsoft-Windows-Betriebssysteme
   - Windows NT 4.0 Server
   - Windows NT 4.0 Professional Workstation
   - Windows 2000 Server

- Windows 2000 Advanced Server
- Windows 2000 Datacenter
- Windows 2000 Server (64-Bit Itanium)
- Windows 2000 Professional Workstation
- Windows XP Professional
- Windows XP Professional (64-Bit x86/EM64T/AMD64)
- Windows 2003 Server
- Windows 2003 Server (64-Bit Itanium)
- Windows 2003 Server (64-Bit x86/EM64T/AMD64)
- Windows Vista Enterprise
- Windows Vista Business
- Windows Vista Ultimate
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

2. Unix-Betriebssysteme
   - Sun Solaris 7 (SPARC)
   - Sun Solaris 8 (SPARC)
   - Sun Solaris 9 (SPARC)
   - Sun Solaris 9 (x86)
   - Sun Solaris 10 (SPARC)
   - Sun Solaris 10 (x86)
   - HP-UX 10.xx (PA-RISC)
   - HP-UX 11 (PA-RISC)
   - HP-UX 11.11 (PA-RISC)
   - HP-UX 11.22 (PA-RISC)
   - HP-UX 11.23 (Itanium)
   - AIX 5.1
   - AIX 5.2
   - AIX 5.3
3. Linux-Betriebssysteme
   - SUSE Linux Enterprise 11
   - SUSE Linux Enterprise Server 9

- SUSE Linux 10
- SUSE Linux 9
- SUSE Linux 8
- Red Hat Linux 9
- Red Hat Linux 8
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux (ES/AS/WS) 5
- Red Hat Enterprise Linux (ES/AS/WS) 4
- Red Hat Enterprise Linux (ES/AS/WS) 3

16.6.3 Überwachung der Messung

Die Überwachung des Data Collectors bzw. der Messung ist über unterschiedliche Wege möglich. Prinzipiell stehen zwei Methoden zur Verfügung. In der einen Variante können Sie den Data Collector indirekt überwachen. Das heißt, Sie kontrollieren die Ergebnisse, die der Data Collector produziert und an das Information Warehouse überträgt.

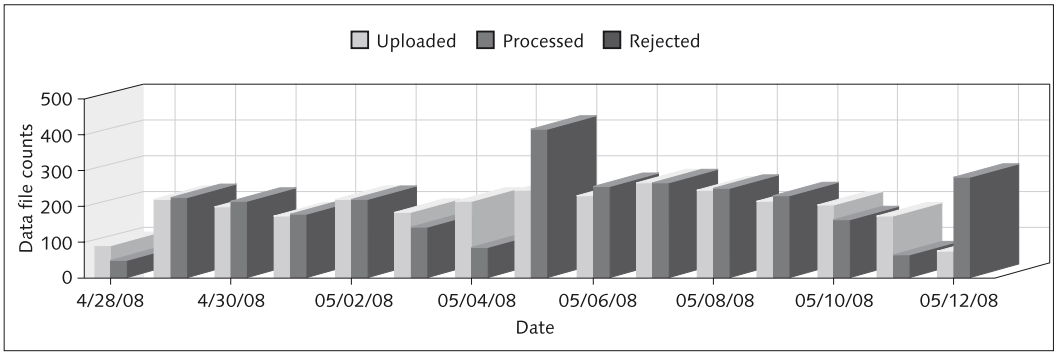


Abbildung 16.31 Datei-Übertragungsstatistik

Hier bietet sich der Bereich Collection Dashboard geradezu an. Die Rubriken Collector Data File Statistics (Collector Stats) (Abbildung 16.31), Data Files Received (Data File Stats) (Abbildung 16.32), Performance Data File Events (Performance Uploads) usw. geben Aufschluss über die Aktivitäten des Data Collectors.

Die andere Variante ist, sich direkt mit dem Data Collector zu verbinden. Dies geschieht in der Regel über Remote-Zugriffe, z. B. über eine VPN-Verbindung. Über eine derartige Verbindung ist es dann auch möglich, administrative Veränderungen am Data Collector vorzunehmen. Stehen derartige Zugänge nicht zur Verfügung, können Sie den Data Collector auch über das Dashboard des Information Warehouse fernsteuern, und zwar im Bereich Project unter Collector Tools • Configure Collectors.

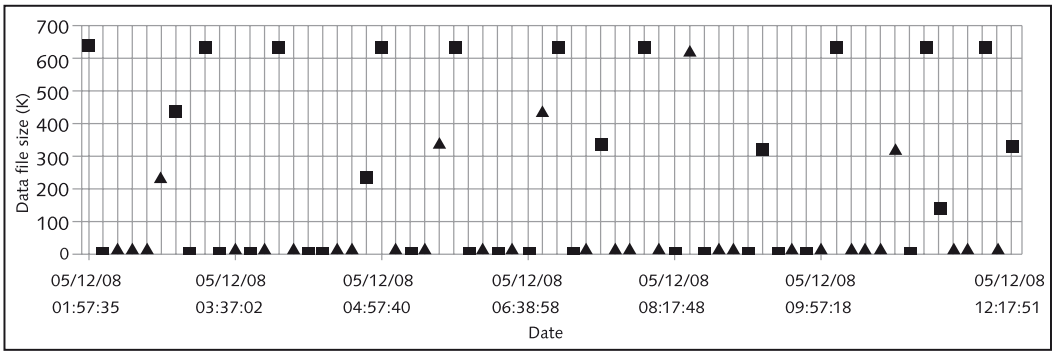


Abbildung 16.32 Empfangsstatistik der Leistungs- und Inventarisierungsdaten (Data File Stats)

16.6.4 Außerbetriebnahme des Data Collectors

Nachdem der Data Collector seinen Dienst über das Untersuchungszeitfenster absolviert hat und somit die Sammlungsperiode abgeschlossen ist, können Sie ihn außer Dienst stellen. Dies geschieht in der Regel durch das Herunterfahren und Ausschalten des Data Collectors.

16.7 Auswertung

Ein BCE (Basic Consolidation Estimate) stellt eine Überprüfung des Environments im Hinblick auf die geplante Konsolidierung dar – quasi ein Basisgutachten zur Virtualisierungsfähigkeit der untersuchten Server-Umgebung.

16.7.1 Phantom-Server

Das Dashboard des Data Warehouse stellt eine umfangreiche Sammlung an Hardware-Templates, die auch als *Modellsysteme* bezeichnet werden, zur Verfügung und erlaubt die Erstellung eigener Hardware-Templates.

Diese Hardware-Templates bzw. -Vorlagen werden auch *Phantom-Server* genannt. Ein Phantom-Server wird durch die Angabe von unterschiedlichen Leistungsdaten (Abbildung 16.33) beschrieben. Das heißt, anhand von Definitionen, wie die Menge an Hauptspeicher oder die Anzahl der CPU-Kerne usw., kann ein virtueller Host im Dashboard hinterlegt werden. Wie am Anfang des Abschnitts beschrieben, stehen derartige Phantom-Server bereits in großer Anzahl im Dashboard zur Verfügung.

Außerdem ist es möglich, aus diesen bereits hinterlegten Phantom-Servern neue Phantom-Server zu generieren. Natürlich können Sie diese dann nach Belieben abändern. Auch ist es vorstellbar, von Grund auf selbstdefinierte Phantom-Server zu erstellen. All diese auf der Basis von Templates oder von Grund auf neu erstellten Phantom-Server sind selbstverständlich innerhalb des Dashboards abspeicherbar, so dass sie bei zukünftigen Auswertungen ebenfalls

zur Verfügung stehen. Sowohl Host-Modelle als auch Modelle der Zielsysteme sind innerhalb des Dashboards zugänglich.

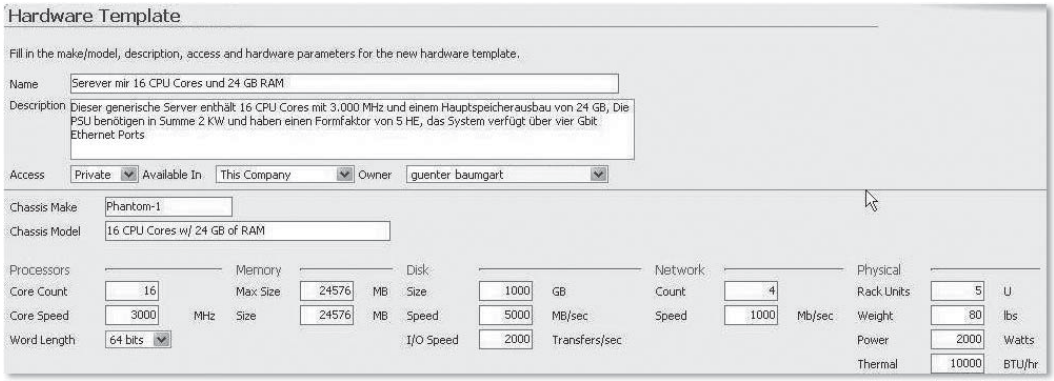


Abbildung 16.33 Hardware Template eines generischen Phantom-Servers

16.7.2 Konsolidierungsszenario

Das Konsolidierungsszenario basiert im Grunde auf einem einfachen Modell. Die gemessenen Daten, die aus einer realen physischen Server-Umgebung stammen, werden als Grundlage für die Virtualisierung der physischen Systeme genutzt.

Die Systeme, deren Datenbasis anzeigt, dass keine Virtualisierung möglich ist, werden gekennzeichnet und im Zuge einer Migrationsuntersuchung nicht weiter berücksichtigt. Daten derartiger Systeme können Sie mit den Möglichkeiten, die das Dashboard des Information Warehouse zur Verfügung stellt, näher untersuchen. Stellt sich heraus, dass die kritischen Werte dieser Systeme eventuell durch diverse Maßnahmen oder Optimierungen an den physischen Systemen zu verbessern sind, kann eine erneute Untersuchung hier letztendlich doch noch zu einer Virtualisierungsempfehlung und einer damit verbundenen Anhebung des Virtualisierungsverhältnisses führen.

Nachdem nun alle physischen Maschinen, die sich auf der Basis ihrer Daten für ein Konsolidierungsszenario eignen, in Form von Modellen bereitstehen, kann der Prozess des Konsolidierungsszenarios nun beginnen.

Unter Analyze im Menüpunkt Optimization Scenarios starten Sie durch Anklicken des Buttons New ein neues Consolidation Scenario. Sofort erscheint ein Assistent bzw. Wizard, der Sie durch die einzelnen Schritte eines Konsolidierungsszenarios führt. In den ersten Schritten wählen Sie die Art des Consolidation Scenarios. Zur Auswahl stehen Desktop- und Server-Consolidation. Im nächsten Schritt wählen Sie dann ein Scenario Template aus. In einem nächsten Prozessschritt ist es möglich, die gemessenen Server zu gruppieren.

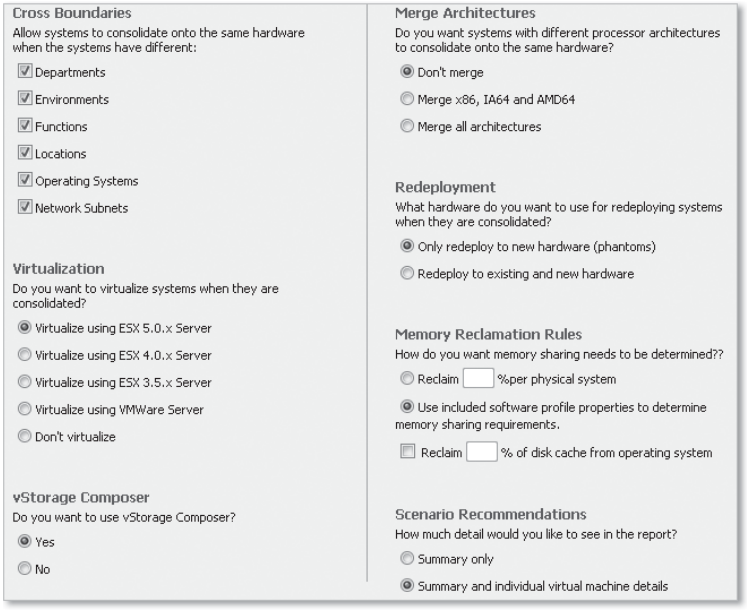


Abbildung 16.34 Formular zur Einstellung diverser Regeln

Ein weiterer Schritt im Prozess erlaubt es, mannigfaltig Regeln (Abbildung 16.34) im Szenario zu hinterlegen, beispielsweise auch um bereits bestehende Hardware in die bevorstehende Betrachtung einzubeziehen. Außerdem können Sie die Granularität der Darstellung der Ergebnisse einstellen. Im Anschluss daran wählen Sie ein BASE-IMAGE, das Sie zuvor erstellt haben, und geben an, wie viele VIRTUAL-MACHINE-TEMPLATES Sie in diesem Szenario generieren möchten. Im weiteren Verlauf des CONSOLIDATION SCENARIOS haben Sie auf der Seite CONFIGURE CLUSTER, HARDWARE & SHARED STORAGE die Möglichkeit, nach der Auswahl eines Phantom-Servers, den Sie später in der Realität als Host einsetzen möchten, bereits erste Daten zu betrachten. Hierbei bietet der Wizard ein QUICK ASSESSMENT (Abbildung 16.35) an, das, wie der Name schon sagt, bereits zum jetzigen Zeitpunkt eine erste Voranalyse für die Komponenten PROZESSOR, MEMORY, DISK-SPEED UND NETWORK-SPEED zulässt. Durch die Auswahlbox VARIANCE (Abbildung 16.35) nehmen Sie eine Einstellung vor.

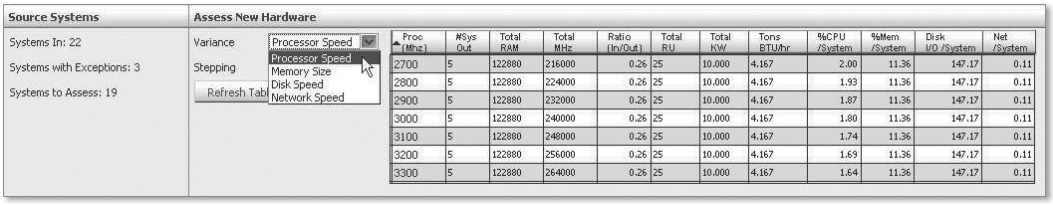
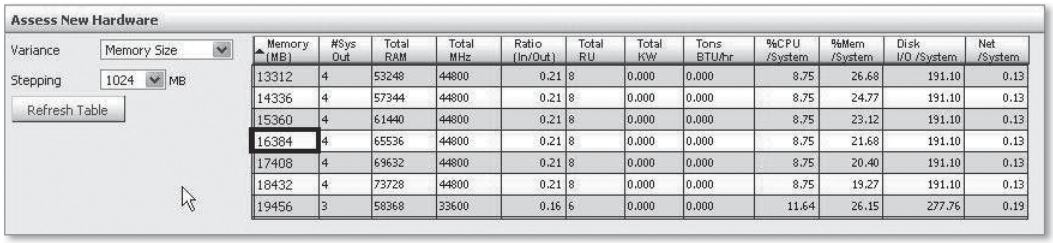


Abbildung 16.35 Quick Assessment

Doch erläutern wir anhand des Hauptspeichers ein Beispiel für das Quick Assessment. Hierbei gehen wir von einem auf 16 GB eingestellten Hauptspeicher aus. Die Tabelle, mit der Sie ein Quick Assessment vornehmen, besteht aus sieben Zeilen. Die mittlere Zeile stellt den aktuell eingestellten maximalen Hauptspeicher des Modell-Hosts dar. Nun ist eine Betrachtung in drei Stufen (Abbildung 16.36) möglich. Über die Combo Box Stepping können Sie Stufen von einem Viertel GB, einem halben GB und einem GB einstellen. In diesem Beispiel haben wir eine Abstufung von einem GB gewählt.

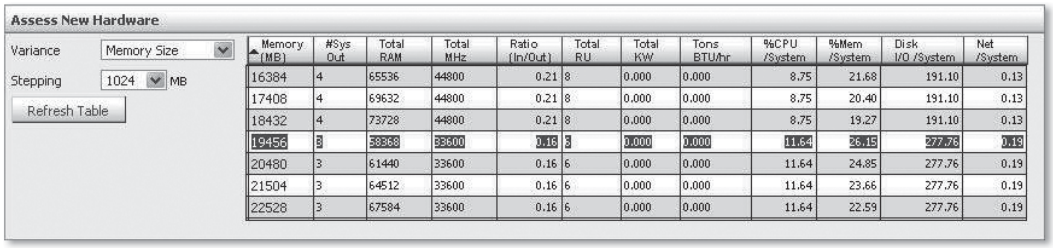
Wie Sie deutlich erkennen, werden bei der aktuellen Hauptspeicherwahl vier Hosts benötigt. Erst ab 19 GB Hauptspeicherbestückung wird es möglich, lediglich drei Hosts einzusetzen, um alle ausgewählten Zielsysteme in einer virtuellen Server-Landschaft zu betreiben. Diese Aussage beruht allerdings ausschließlich auf der Betrachtung der Hauptspeicherausstattung. Um eine nachhaltige Aussage zu treffen, wie viele Hosts Sie tatsächlich benötigen, müssen Sie selbstverständlich alle anderen maßgeblichen Faktoren ebenfalls berücksichtigen.



Memory (MB)	#Sys Out	Total RAM	Total MHz	Ratio (In/Out)	Total RU	Total KW	Tons BTU/hr	%CPU /System	%Mem /System	Disk I/O /System	Net /System
13312	4	53248	44800	0.21	8	0.000	0.000	8.75	26.68	191.10	0.13
14336	4	57344	44800	0.21	8	0.000	0.000	8.75	24.77	191.10	0.13
15360	4	61440	44800	0.21	8	0.000	0.000	8.75	23.12	191.10	0.13
16384	4	65536	44800	0.21	8	0.000	0.000	8.75	21.68	191.10	0.13
17408	4	69632	44800	0.21	8	0.000	0.000	8.75	20.40	191.10	0.13
18432	4	73728	44800	0.21	8	0.000	0.000	8.75	19.27	191.10	0.13
19456	3	58368	33600	0.16	6	0.000	0.000	11.64	26.15	277.76	0.19

Abbildung 16.36 Quick Assessment: Memory liegt bei 16 GB.

Durch Anklicken des Eintrags 19456 (19 GB) in der Spalte Memory (MB) wird nun die Tabelle geschrieben und dieser Wert in die mittlere Zeile eingetragen. Des Weiteren wird der Hauptspeicher des Modellsystems von 16 GB auf 19 GB erhöht. Sie erkennen nun, dass sich bis zur letzten Zeile der Tabelle (Abbildung 16.37) keine Veränderung bei der Anzahl der Server ergibt.



Memory (MB)	#Sys Out	Total RAM	Total MHz	Ratio (In/Out)	Total RU	Total KW	Tons BTU/hr	%CPU /System	%Mem /System	Disk I/O /System	Net /System
16384	4	65536	44800	0.21	8	0.000	0.000	8.75	21.68	191.10	0.13
17408	4	69632	44800	0.21	8	0.000	0.000	8.75	20.40	191.10	0.13
18432	4	73728	44800	0.21	8	0.000	0.000	8.75	19.27	191.10	0.13
19456	3	58368	33600	0.16	6	0.000	0.000	11.64	26.15	277.76	0.19
20480	3	61440	33600	0.16	6	0.000	0.000	11.64	24.85	277.76	0.19
21504	3	64512	33600	0.16	6	0.000	0.000	11.64	23.66	277.76	0.19
22528	3	67584	33600	0.16	6	0.000	0.000	11.64	22.59	277.76	0.19

Abbildung 16.37 Quick Assessment: Memory liegt bei 19 GB.

Falls im Hinblick auf das geplante Virtualisierungsvorhaben diese Menge an Hosts nicht erwünscht ist, können Sie nun im Weiteren untersuchen, ob bezogen auf den Hauptspeicherausbau eine weitere Reduzierung der benötigten Hosts im Rahmen des Quick Assessments

möglich ist. Zu diesem Zweck führen Sie das soeben beschriebene Vorgehen in gleicher Art und Weise fort.

Im letzten Schritt legen Sie Schwellenwerte für die Betrachtung fest (ADJUST SYSTEM THRESHOLDS). Hierbei hinterlegen Sie unter anderem Obergrenzen für die Auslastung des Hauptspeichers oder den maximalen Nutzungsgrad des Netzwerkes (Abbildung 16.38). Im Anschluss daran werden die gemessenen Daten der Zielsysteme (Modelldaten der Zielsysteme) die aus der realen physischen Server-Umgebung stammen, mit den Modelldaten der Hosts (Phantom-Server) in Korrelation gebracht.

Processors			Memory			Disk			Network		
CPU Usage	50	% of 5040 MHz	RAM Usage	90	% of 8192 MB	Speed	100	% of 50 MB/sec	Speed	100	% of 4000 MB/sec
Queue	3		Page File Usage	70	% of 12288 MB	IO Speed	100	% of 10000 Transfers/sec			

Abbildung 16.38 Formular zur Einstellung der Schwellenwerte

Als vorbereitende Maßnahme für eine erste Näherung ist es auch in dieser Rubrik möglich, ein QUICK ASSESSMENT durchzuführen. Dieses ist dem bereits bei »Hardwarevorlagen« in der Abbildung 16.33 beschriebenen Verfahren sehr ähnlich. Das Resultat ist eine bestimmte Menge von Phantom-Servern, die später die virtuellen Maschinen in einer gemittelten Kombination hosten können.

16.7.3 Ergebnis

Als Ergebnis der Korrelation von zugrundegelegtem Phantom-Server (Abbildung 16.39) und Messdaten der Zielsysteme wird nun einerseits die Menge der benötigten Phantom-Server und andererseits eine Zusammensetzung der Hosts im Hinblick auf die zukünftig virtualisierten Zielsysteme (Abbildung 16.40) angezeigt.

		Capacity												
		Processors			Memory	Disk			Network		Physical			
	Make/Model	Count	Speed (MHz)	Word Length	Size (MB)	Size (GB)	I/O (MB/sec)	I/O (Trans/sec)	Count	Speed (MB/sec)	Rack Units	Weight (lbs)	Power (W)	Thermal (BTU/hr)
☆	Phantom	4	2,660	32	16,384	146	250	1,000	4	1,000	2	50	0	1,480

Abbildung 16.39 Modell eines Phantom-Servers

Im vorliegenden Beispiel werden auf Phantom-Server 1 acht Zielsysteme und auf Phantom-Server 2 sechs Zielsysteme platziert. Wie Sie an den einzelnen Werten (Abbildung 16.40) deutlich sehen, stellt sich die Belastungsbilanz recht optimiert und ausgeglichen dar.

Zielsysteme, die aus unterschiedlichsten Gründen für eine Virtualisierung nicht geeignet sind, werden ebenfalls dargestellt. Hierbei werden auch die Gründe für die Nichtvirtualisierungsempfehlung hervorgehoben. Im vorliegenden Beispiel wird eine Ausgrenzung des Zielsystems MO mit zu hohem Paging (Abbildung 16.40) begründet.

			Processor		Memory				Disk		Network
	Target System Name	Source System Name(s)	% Used	Queue per CPU	% Used	File Sys Cache (MB)	Page File %	Paging (Pg/sec)	I/O (Trans/sec)	I/O (MB/sec)	Speed (MB/sec)
Systems with Exceptions											
	MO	MO	10.27	0.03	24.68	183.32	2.90	**1,684.80**	116.95	6.91	6.94
New Systems											
	Phantom1-1	HO LE PE SA SC TI TR VM	16.24	0.31	65.68	1,058.93	7.98	131.26	406.71	4.65	0.26
	Phantom2-1	AIN MOS GO ON AP2 VMP	13.18	0.36	69.47	1,123.93	7.40	138.31	158.46	8.19	0.12

Abbildung 16.40 Phantom-Server und Zielsysteme

16.7.4 Was bedeutet Verfügbarkeit?

Im Umfeld von High Availability stellt sich immer die Frage, wie hoch die Verfügbarkeit denn tatsächlich sein soll. Auch sollten Sie genau hinterfragen, was mit Verfügbarkeit eigentlich genau gemeint ist – Verfügbarkeit des Storage, der Hosts, der virtuellen Maschinen, der Dienste oder des Gesamtsystems? Sie müssen sich in diesem Zusammenhang immer vor Augen führen, dass, wenn z. B. die Forderung von Five-Nines-Verfügbarkeit für das Gesamtsystem gestellt wird, praktisch gesehen das Speichersystem, auf dem die virtuellen Maschinen liegen, quasi innerhalb eines Jahres überhaupt nicht ausfallen darf, da Five Nines lediglich gut fünf Minuten Betriebsunterbrechung im Jahr für das Gesamtsystem zulässt.

Ein Jahr sind $31{,}536 \times 10^6$ Sekunden. Eine »five-nine« Verfügbarkeit kann auch als $100\,\% - 99{,}999\,\% / 100\,\% = 10 \times 10^6$ ausgedrückt werden. Hieraus ergibt sich dann ein Zeitraum von $31{,}536 \times 10^6\ s \times 10 \times 10^6 = 315{,}36\ s$.

16.7.5 Berücksichtigung von Verfügbarkeit

In den folgenden Überlegungen wird der Hochverfügbarkeits-Service der virtuellen Infrastruktur zugrunde gelegt. Die Gewährleistung des High-Availability-Service hängt in dieser Betrachtung im Wesentlichen von der Verteilung der Ressourcen ab. Primär kann also gesagt werden, dass der Verbund im Idealfall bei einfacher High-Availability-Redundanz so viele Ressourcen benötigt, dass der Ausfall eines Knotens im Gesamtverbund abgefangen werden kann. Bei einem Zweiknotensystem kann also, wenn ein Knoten ausfällt, der zweite Knoten die ausgefallenen Ressourcen zur Verfügung stellen.

In Bezug auf die Ressource CPU bedeutet das, dass genauso viel CPU-Ressourcen vom verbleibenden Knoten bereitstehen, wie auf dem ausgefallenen Knoten von den virtuellen Maschinen genutzt wurden. Besteht der Verbund aus drei Knoten und fällt ein Knoten aus, müssen die verbleibenden beiden Knoten die verlorene Ressource abfangen. In unserem Beispiel

würde das bedeuten, dass die Ressource CPU gleichermaßen von zwei Hosts bereitgestellt werden müsste. Hierbei stellt sich nun die Frage, inwieweit der verbleibende Verbund noch Redundanz im Hinblick auf den Ausfall eines weiteren Knotens bereitstellen soll. Dazu nun mehr.

Bei einem High-Availability-Verbund mit noch mehr Hosts gilt die gleiche Anforderung. Nur werden derartige Überlegungen beliebig kompliziert. Bleiben wir aber der Einfachheit halber bei unserem Zweiknotenbeispiel. Nehmen wir einmal an, dass in unserer Simulation der Modell- bzw. Phantom-Server mit 8 GB RAM sowie zwei Single-Core-CPUs mit je 2.800 MHz ausgestattet ist. Nach der Simulation stellt sich uns das folgende Ergebnis dar:

- $CPU_{(Phantom\ 1)}$: 5 %
- $CPU_{(Phantom\ 2)}$: 8 %
- CPU_{total}: 13 %

Das Ergebnis des Modellszenarios lautet: Es werden mindestens zwei Hosts benötigt, um die Dienste, die es zu virtualisieren gilt, zu betreiben. Für die Ausnutzung der CPU bedeutet das, dass der Nutzungsgrad im Verbund bei gerade einmal 13 % liegt. Im Hinblick auf den Hauptspeicher des Verbundes stellt sich ein nicht zufriedenstellendes Ergebnis ein. Wie Sie an den Zahlen sehen, liegt der Ausnutzungsgrad 44 % über den vorhandenen Ressourcen des gewählten Phantom-Servers.

- $RAM_{(Phantom\ 1)}$: 69 %
- $RAM_{(Phantom\ 2)}$: 75 %
- RAM_{total}: 144 %

In einem nächsten Auswertungslauf wählen wir einen Phantom-Server, der 16 GB Hauptspeicher und zwei Single-Core-CPUs mit je 2.800 MHz aufweist. Wie wir aus dem vorhergehenden Szenario herausgearbeitet haben, sind zwar die beiden CPUs in keiner Weise erforderlich, aber in unserem Beispiel bleiben wir der Einfachheit halber bei dem ursprünglich gewählten Hardwaremodell. Die Ergebnisse für den Nutzungsgrad der CPU bleiben also identisch, so dass wir hierauf nicht weiter eingehen.

- $RAM_{(Phantom\ 1)}$: 46 %
- $RAM_{(Phantom\ 2)}$: 26 %
- RAM_{total}: 72 %

Das Ergebnis spricht für sich. Der Hauptspeicher des Zweiknotenverbundes wird maximal zu 72 % ausgelastet. Fällt z. B. Phantom 1 aus, wird Phantom 2 mit Verbrauchern oder, besser gesagt, virtuellen Maschinen belastet, die zusätzlich dem Host 26 % Hauptspeicher abverlangen. An dieser Stelle sei darauf hingewiesen, dass der aus mehr als zwei Knoten bestehende Verbund – neben der höheren Verfügbarkeit – einen weiteren großen Vorteil bietet; am Beispiel des Dreiknotenverbundes wird dies sehr deutlich: Durch den Ansatz, drei Knoten einzusetzen, wird es mittels dieser erhöhten Redundanz möglich, einen der Knoten ohne den Ver-

lust von einfacher Redundanz zu warten respektive auf- oder umzurüsten. Sollte nämlich einer der beiden verbleibenden Knoten während der Wartung des dritten Knotens ausfallen, arbeitet die Anlage gemäß High Availability weiter, und die Dienste für den Endbenutzer stehen nach der Übernahme durch den verbleibenden Knoten schnellstens wieder zur Verfügung. Das Betriebspersonal muss also nicht sofort eingreifen. Die Voraussetzung für ein derartiges Sicherheitsniveau ist allerdings, dass in dem soeben beschriebenen Dreiknotenverbund jeder der Knoten sämtliche virtuellen Maschinen vollständig übernehmen und hinreichend mit Ressourcen versorgen kann.

16.7.6 Betrachtung der Skalierbarkeit

Ein weiterer Aspekt ist, dass Sie die Auslastung der Hosts nicht bei oder zu nah an 100 % planen sollten. In der Praxis kommt in der Regel nach der Inbetriebnahme einer virtuellen Infrastruktur entgegen allen Vorsätzen der IT einer Organisation schnell die eine oder andere virtuelle Maschine hinzu. Aus diesem Grund ist eine großzügigere Planung äußerst empfehlenswert. Faktoren wie zukünftiges Wachstum sind unbedingt einzuplanen. Was auch immer wieder bei der Planung im Verbund der Hosts unterschätzt wird, ist die Berücksichtigung einer virtuellen Testumgebung.

Gerade im Hinblick auf Experimente mit geclonten Produktivsystemen sollten Sie hinreichend Ressourcen einplanen. Wie wir im Beispiel des Modellszenarios (Abbildung 16.40) veranschaulicht haben, gibt es sehr oft Systeme, die sich aus den bereits genannten Gründen nicht virtualisieren lassen. Meistens werden diese Systeme, nachdem die Gründe für eine Nichtvirtualisierung bekannt geworden sind, nach Problembehebung zu einem späteren Zeitpunkt virtualisiert. Die Ressourcenanforderungen dieser Zielsysteme müssen Sie bei der Auslegung der Hosts unbedingt berücksichtigen. Sollte eine Organisation sich dann auch noch für das Thema Virtual Desktop Infrastructure begeistern, sind die Anforderungen an die Ressourcen noch schwieriger festzumachen, da im Hinblick auf Virtual Desktop Infrastructure z. B. der Personalbestand eines Unternehmens einen noch unmittelbareren Einfluss auf die Ressourcen der IT hat als im Umfeld von bereitzustellenden Diensten.

Da diese Technik virtuelle Rich Clients bereitstellt, sind die Anforderungen oftmals entsprechend hoch. In Anbetracht dieser Situation sind die Entscheidungen für die richtige Hardware nicht einfach und hängen von unterschiedlichsten Faktoren ab. Werden einige große Server gewählt – verfügen also die Hosts über viel CPU, eine große Menge an Hauptspeicher und sind mit umfangreichen Festplattensubsystemen ausgestattet –, so ist dies anders zu bewerten, als wenn im Environment eine große Anzahl von geringer ausgestatteten Hosts eingesetzt wird. Auch im Hinblick auf die Lizenzierung einer Umgebung ist es wichtig zu entscheiden, ob die Zahl der Knoten in einem Server-Verbund begrenzt werden darf oder nicht. Durch moderne Server gibt es allerdings noch eine weitere Variante, die beleuchtet werden muss.

Durch den Fortschritt bei der CPU-Architektur steigt die Zahl der Kerne in einer CPU stetig. Waren es früher Zweikernsysteme, so sind es heute Vierkernsysteme, und mit einem Ende

dieses Trends ist eher nicht zu rechnen. Nehmen wir einmal an, dass ein Server die Möglichkeit bietet, mit acht Sockeln ausgestattet zu werden. Werden diese Sockel dann mit Vierkern-CPUs bestückt, verfügt das Gesamtsystem über 32 Kerne. Derartige Hosts stellen auch noch beispielsweise 256 GB Hauptspeicher zur Verfügung. Hosts dieser Klasse können ohne weiteres mit um die 100 anspruchsvollen virtuellen Maschinen belastet werden. Bei zwei voll ausgebauten Hosts dieser Leistungsklasse ist es unter Umständen möglich, eine Knotenobergrenze festzulegen. Bei kleineren Systemen ist die Entscheidung für eine Festlegung auf eine Obergrenze wesentlich schwieriger zu treffen.

An dieser Stelle nun ein Beispiel bezogen auf die Menge von CPUs respektive Kerne in den CPUs: Werden zwei Hosts mit je vier Sockeln zugrunde gelegt, von denen nur je zwei Sockel mit Vierkern-CPUs bestückt wurden, verfügt das Environment bereits über insgesamt 16 Kerne. Da das System in unserem Beispiel bisher aber nur halb ausgebaut wurde, ist noch Raum für Wachstum. An dieser Stelle muss die Entscheidung getroffen werden, ob bei Wachstum über die noch im Verbund verfügbaren acht Sockel hinaus ein weiterer Knoten eingesetzt oder ob schon zum jetzigen Zeitpunkt mit stärker ausbaubaren Hosts begonnen werden soll.

Abgesehen von der Anzahl der CPU-Kerne kann auch die Aufnahme der elektrischen Leistung bei kleineren Systemen deutlich höher liegen. So würden bei dem hier erläuterten Beispiel zwei Achtwegemaschinen ca. ein Kilowatt weniger Leistungsaufnahme bedeuten als vier Vierwegemaschinen, und bei acht Zweiwegemaschinen läge der Verbrauch noch höher. Dabei lassen wir noch ganz außer Acht, wie sich dies auf den Bedarf an Höheneinheiten und Kühlleistung auswirkt.

Außerdem benötigen mehr Server-Systeme auch mehr Anschlüsse an das Storage-Netz, was ein weiterer nicht zu vernachlässigender Faktor ist. Hierbei wird sehr deutlich nachvollziehbar, dass die Betrachtungen der unterschiedlichen Umgebungen in Hinsicht auf die Fragestellung der Skalierbarkeit sehr differieren. Jede Umgebung muss individuell für sich betrachtet werden.

16.7.7 Ermittlung des Konsolidierungsverhältnisses bzw. der Grad der Konsolidierung bei der Virtualisierung

Der Grad der Konsolidierung zeigt die Qualität der Migration an. Das heißt, es wird ein Wert ermittelt, der aufzeigt, wie hoch die Migrationsquote sein wird. Hierzu wird die Menge aller physischen Server-Systeme, die zur Migration anstehen, mit der Zahl der physisch verbleibenden Server-Systeme – sprich der Server-Systeme, die aus den unterschiedlichsten Gründen nicht virtualisiert werden können – ins Verhältnis gesetzt. Es handelt sich quasi um eine Vorher-Nachher-Betrachtung bezogen auf die Gesamtzahl der Server-Systeme.

Nehmen wir einmal an, dass es 53 Zielsysteme zu virtualisieren gilt. Des Weiteren hat sich herausgestellt, dass 3 Zielsysteme nicht virtualisierbar sind. Der Grund hierfür könnte sein, dass die Systeme einen derart hohen Verbrauch an Ressourcen haben, dass eine Virtualisierung nicht sinnvoll wäre. Das Fazit ist: Es sollen 50 physische Server-Systeme virtualisiert werden. Auch

haben wir herausgefunden, dass sieben ESX-Server benötigt werden, um die 50 virtuellen Maschinen zu hosten.

Das Konsolidierungsverhältnis bezogen auf unser Beispiel ermitteln wir dann wie folgt:

Definition:

- die Menge aller physischen Server im Environment: Srvs In
- die Menge der ermittelten ESX-Hosts: ESX Srvs Out
- die Server, die sich nicht virtualisieren lassen: Exception Servers
- Con Ratio bzw. Konsolidierungsverhältnis: CR
- Con Ratio bzw. Konsolidierungsverhältnis in %: CR (%)

Berechnung:

$$CR = \frac{\text{Srvs In}}{\text{ESX Srvs Out} + \text{Exception Servers}}$$

$$CR\,(\%) = 100 \cdot \left[1 - \frac{1}{CR}\right]$$

Beispiel:

Srvs In = 53 Stück

ESX Srvs Out = 7 Stück

Exception Servers = 3 Stück

$$CR = \frac{53}{7 + 3}$$

$$CR = 5{,}3$$

$$CR\,(\%) = 100 \cdot \left[1 - \frac{1}{5{,}3}\right]$$

$$CR\,(\%) = 81,13$$

Ergebnis:

Das Konsolidierungsverhältnis beträgt 81 %.

16.7.8 Der Weg zum CP-Admin

Einen Zugriff auf das Dashboard sowie die Möglichkeit, den Data Collector einzusetzen, erhält ein Consultant, indem er bei VMware den Lehrgang »Instructor Lead Capacity Planner« absolviert. Dieser Lehrgang kann ausschließlich von einem Mitarbeiter eines Unternehmens durchgeführt werden, das eine entsprechende VMware-Partnerschaft hält.

Hat nun ein Consultant die Zulassung erlangt, verfügt er auch über einen Zugang zum Dashboard und kann hier für weitere Consultants entsprechende Accounts anlegen. Damit diese Consultants ihre Arbeit mit dem Capacity Planner aufnehmen können, schreibt VMware vor, dass sie eine Onlineschulung bei VMware absolvieren.

Unter *http://mylearn1.vmware.com* (Abbildung 16.41) können Sie den Kurs »Installing the Data Manager« absolvieren.

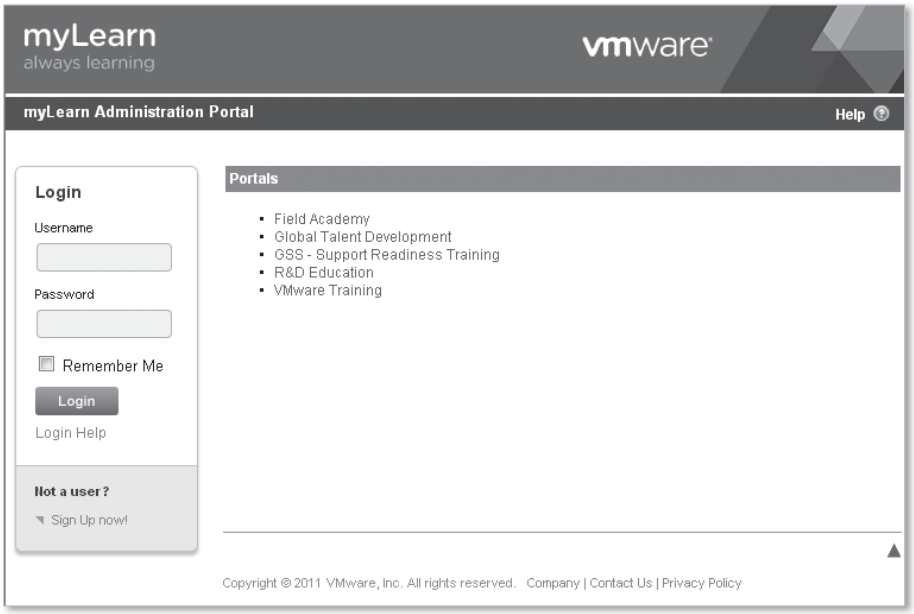


Abbildung 16.41 Das »myLearn Administration Portal«

VMware hat mit vSphere 5 und dem Wegfall des ESX Servers mit Service Console wesentliche Neuerungen im Sicherheitsumfeld eingeführt. Diese reichen von neuen Firewall-Funktionen bis hin zu Compliance-Software.

17 Sicherheit

Autor dieses Kapitels ist Dennis Zimmer, opvizor GmbH – opvizor.com, virtuellemaschinen@email.de – vmachine.de

Die Service Console weilt nicht mehr unter uns – zumindest mit vSphere 5 und dem dazugehörigen ESXi 5. Damit gehören viele Sicherheitsrisiken und Sicherheitsprobleme der Vergangenheit an, da in der Service Console ein Red Hat Enterprise Linux 5 mit vielen Open-Source-Komponenten lief, die potentiell Sicherheitslücken aufwiesen, die durch stetige Updates geschlossen werden mussten. Das heißt, ab einer reinrassigen vSphere 5-Umgebung muss die Anzahl der Host-Patches zwingend sinken. Den Beweis hatte man allerdings schon in den letzten Jahren erbracht, da die vorherigen ESXi-Versionen im Vergleich zu den ESX-Versionen deutlich weniger Patches benötigten.

Allerdings sollten Sie auch beim ESXi den SSH-Zugang nicht dauerhaft aktivieren und den Lockdown-Mode ebenfalls anschalten, damit kein lokaler Zugriff mehr möglich ist. Außerdem empfehlen wir nach wie vor, die VMkernel-Managementadapter in ein geschütztes Netzwerk zu stellen, ein sehr starkes »root«-Passwort zu wählen und mit den Hostprofilen zu arbeiten, um die Konfiguration sicherzustellen. VMware sichert zwar bereits nach der Installation viele offensichtliche Schwachstellen ab, trotzdem gibt es einige Aspekte zu beachten. VMware hat ein gesondertes Dokument zum Thema ESX-Sicherheit erstellt, das hier zu finden ist:

http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-50-security-guide.pdf

Oder in Kurzform: *http://tinyurl.com/vsphere5security*

17.1 VMware ESXi

Trotz ESXi hat der Administrator keinen Freibrief bei der Sicherheitsbedenken- und Netzwerkplanung. Zumindest sollten Sie in jedem Fall das von ESXi genutzte Managementnetzwerk als erste Angriffsstelle betrachten und es daher möglichst durch getrennte LAN- (Management Netzwerk-) oder VLAN-Umgebungen abschotten, so dass nicht jeder Benutzer oder sogar DMZ-Angreifer Zugriff darauf erhalten kann.

17.1.1 Hardware-Management-Schnittstellen

Neben den Management-Ports der ESX-Hosts sollten Sie unbedingt die Hardwareverwaltung via iLO, DRAC usw. bedenken. Diese sollte ebenfalls abgeschottet vom normalen Anwendernetzwerk existieren, und Standardpasswörter sollten Sie zwingend ändern. Es existieren Beispiele im Internet, die es sogar bis auf die *Heise.de*-Newsseite (Hackerangriff auf VMware-Infrastruktur der GEMA) geschafft haben und deutlich aufzeigen, warum Sie keine Standardpasswörter verwenden sollten.

17.1.2 Security Profile

VMware hat dem ESXi 5 eine komplett neue Firewall spendiert, die zahlreiche Anpassungen zulässt und grafisch per vSphere-Client und auch automatisiert mittels PowerCLI verwaltet werden kann. Die Sicherheitseinstellungen finden Sie in der Konfiguration des ESX-Hosts (Abbildung 17.1).

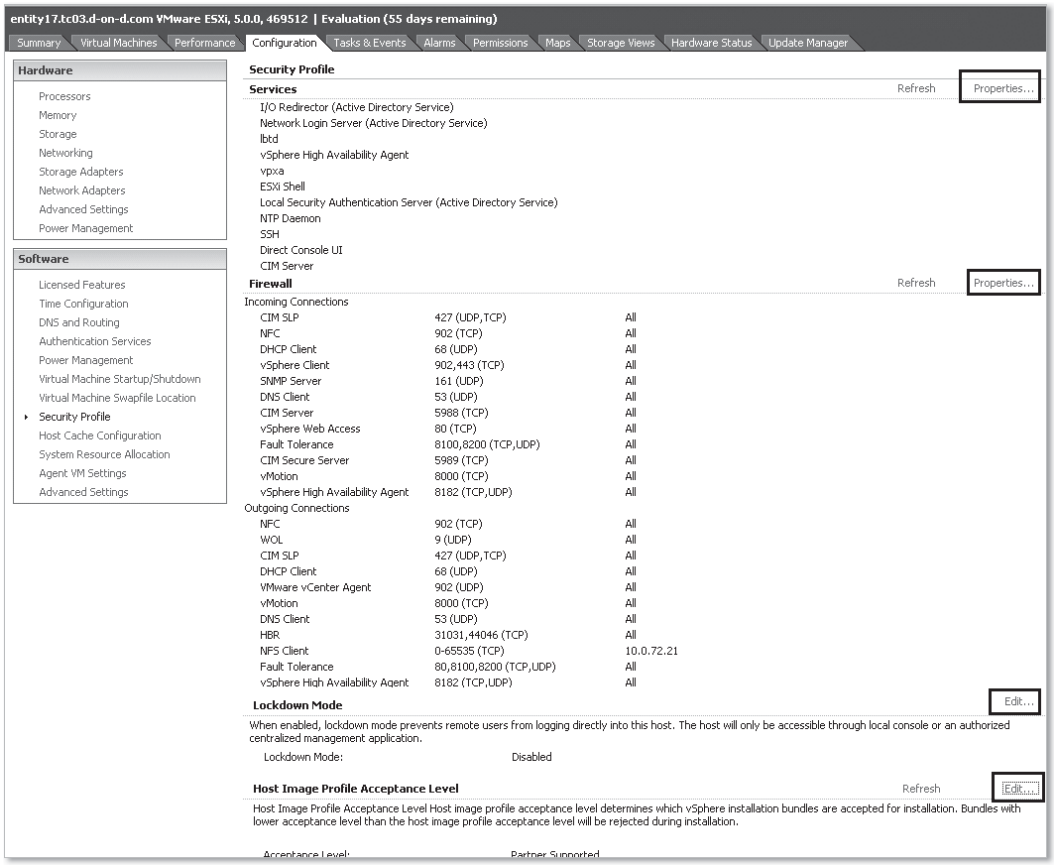


Abbildung 17.1 Firewall-Konfiguration ESX

Im SERVICES-Bereich können Sie die bereits mit der Installation mitgebrachten Dienste für den Netzwerkverkehr freischalten. Diese Dienste werden entweder aktiviert oder deaktiviert und können danach auf den entsprechenden Netzwerkports kommunizieren.

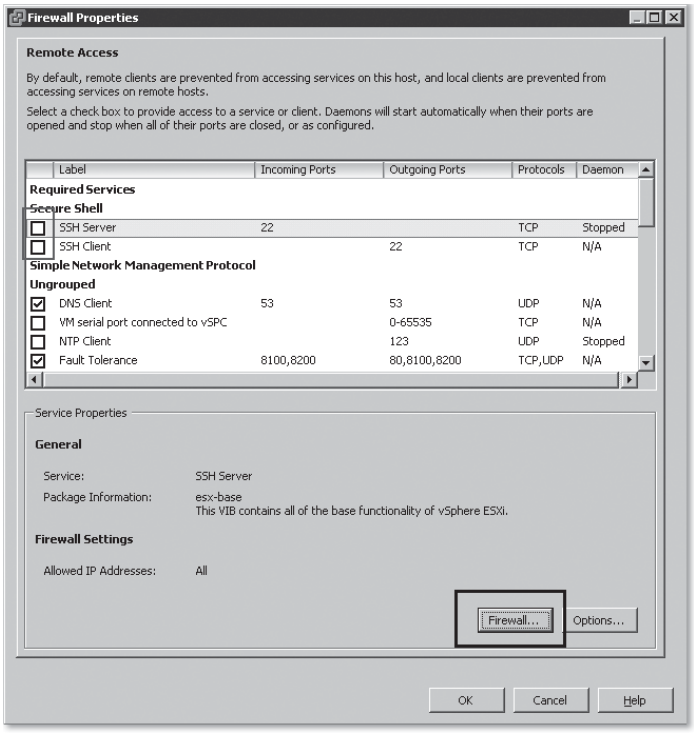


Abbildung 17.2 Firewall-Details

Im Bereich FIREWALL verwalten Sie die integrierte Firewall, die den Datenverkehr anhand der Portnummer, der Protokollart (UDP, TCP) und der Richtung bzw. der Netzwerkadressen erlaubt oder blockiert. Mit der PROPERTIES-Auswahl gelangen Sie in die Konfiguration der Firewall (Abbildung 17.2) und können mittels FIREWALL...-Knopf die erlaubten Netzwerke umstellen (Abbildung 17.3).

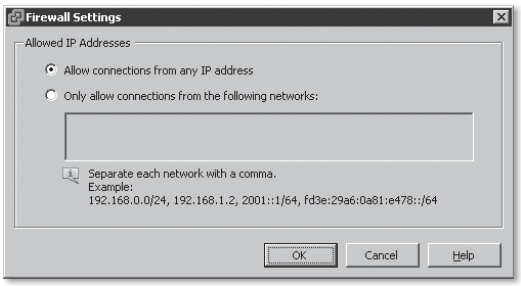


Abbildung 17.3 Netzwerke können eingeschränkt werden.

Mit der Aktivierung des Lockdown-Modus sperren Sie den ESX-Server gegen Zugriffe aus dem Netzwerk ab. Somit ist es nur noch über die lokale Konsole (z. B. über Hardwaremanagementtools wie HP iLO) und mittels erlaubter Verwaltungswerkzeuge (z. B. vSphere-Client) möglich, auf den ESX-Server zuzugreifen.

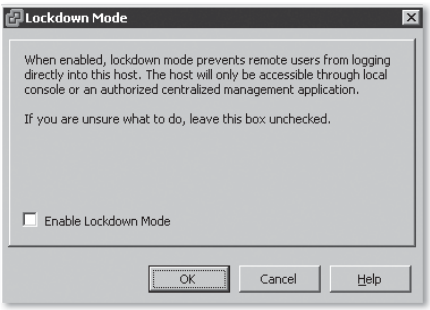


Abbildung 17.4 Lockdown-Modus

Auch ohne die Service Console ist es möglich, Software auf dem ESX System zu installieren, z. B. Hardwaremodule wie Cisco Nexus 1000v. Innerhalb der Sicherheitseinstellungen des ESX können Sie jedoch beschränken, welche Art Softwarepakete erlaubt sind. VMware Certified stellt die höchste Hürde dar, Community Supported die geringste.

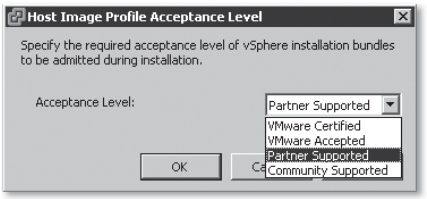


Abbildung 17.5 Welche Installationspakete sind zugelassen?

17.2 »root«-Zugriff

In einem Linux-System bedeutet »root«-Zugriff die Berechtigung zur uneingeschränkten Verwaltung aller Dienste und Dateien. Daher ist es von enormer Bedeutung, den »root«-Zugriff möglichst eingeschränkt zu halten und vor allem einen unautorisierten Zugriff unter allen Umständen zu verhindern. Eine Anmeldung per Benutzer-Account mit Standardberechtigung und Wechsel zu »root« bei Bedarf wird empfohlen.

Die definitiv wichtigste Maßnahme ist immer die Wahl eines komplizierten Kennworts. Außerdem sollten Sie das Kennwort in regelmäßigen Abständen ändern.

Wichtig

Die Benutzer »root« und »vpxuser« und die Gruppe »root« dürfen nicht gelöscht werden, da sonst Zugriffsprobleme durch den vSphere-Client und auch ESX-eigene Prozesse programmiert sind. Außerdem sollten Sie den Benutzer »vpxuser« und sein Kennwort nicht anpassen, da dieser Benutzer vom vCenter genutzt und verwaltet wird.

17.2.1 Troubleshooting-Modus über die Konsole

Damit über SSH auf den ESX-Host zugegriffen werden kann, müssen der ESXi-Shell- und der SSH-Dienst aktiviert werden, die in der Host Konfiguration zu finden sind (Abbildung 17.6).

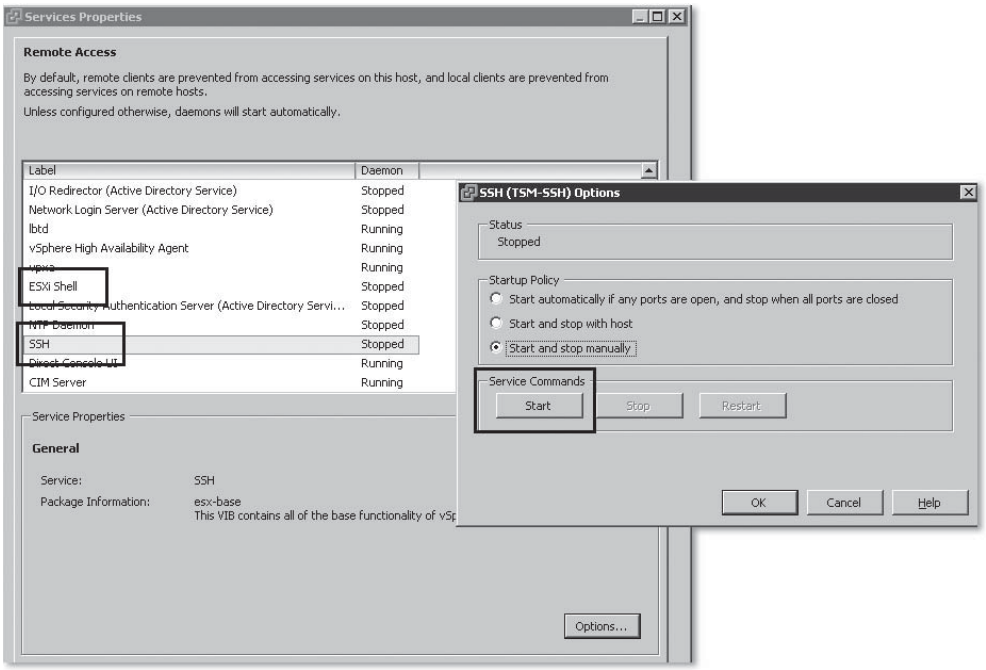


Abbildung 17.6 Starten der ESXi-Shell und der SSH-Unterstützung

17.3 Benutzerverwaltung

Wenn Sie Wert auf Sicherheit legen, kommen Sie an zwei grundlegenden Einstellungen nicht vorbei: *Passwortkomplexität* und *Passwortgültigkeit*

Außerdem ist es bei vorhandenen Benutzerverwaltungen wie Active Directory (AD), bei denen diese Regelungen meist schon gelten, interessant, diese AD-Anmeldung auch für die Anmeldung unter VMware ESX zu nutzen. Die AD-Integration richten Sie über den Auswahlpunkt Authentication Services ein (Abbildung 17.7).

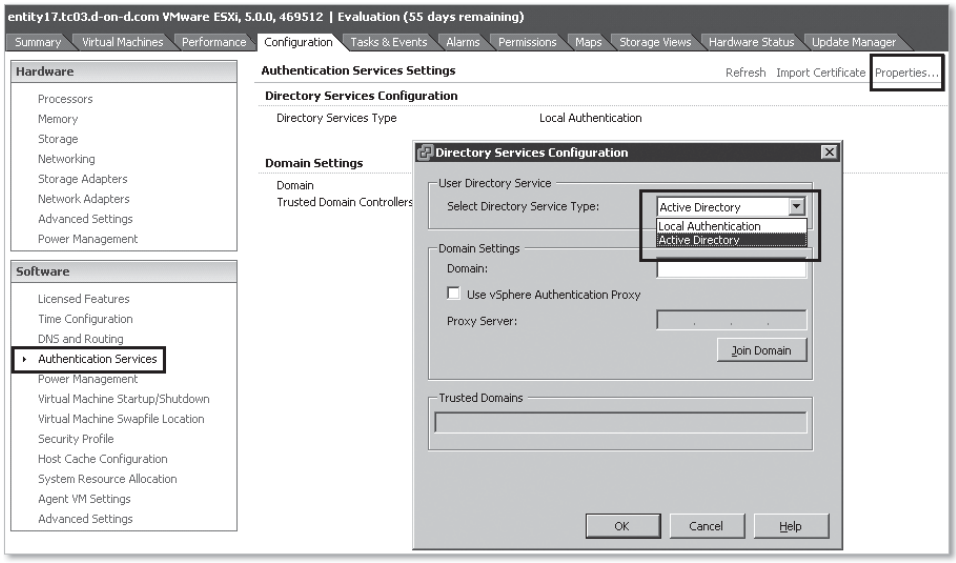


Abbildung 17.7 Active-Directory-Integration

Um die Komplexität der Konfiguration wesentlich zu vermindern, hat VMware den Befehl `vicfg-authconfig` eingeführt, mit dem Sie die meisten Konfigurationseinstellungen zur Benutzerverwaltung durchführen können.

Integration in AD über PowerCLI:

```
$host | Get-VMHostAuthentication | Set-VMHostAuthentication
-Domain someDomain.vmware.com -User username -Password pass
```

AD verlassen:

```
$host | Get-VMHostAuthentication | Set-VMHostAuthentication -LeaveDomain
```

kann mit `-force` als Parameter erzwungen werden.

Übereinstimmung der Uhrzeit

Bei Kerberos-Verwendung müssen Sie darauf achten, dass die Uhrzeit aller an der Authentifizierung teilnehmenden Systeme übereinstimmt. Eine maximale Abweichung von 5 Minuten wird toleriert.

17.3.1 Zurücksetzen des »root«-Passworts

Dies ist nur mit ESX4 möglich! Es kann vorkommen, dass Sie irgendwann vor Ihrem seit Monaten problemlos laufenden ESX-Server stehen und sich anmelden möchten, aber das »root«-Passwort nicht mehr wissen. Da der Server immer noch in der vCenter-Verwaltung ist, können Sie die virtuellen Maschinen allerdings per vMotion verschieben oder zumindest herunterfahren.

Im Fall eines direkten Konsolenzugriffs auf das System – lokal, über einen KVM-Switch oder per Hardwaremanagement (iLO, RSA etc.) – können Sie das System durch Strg+Alt+Entf zum Neustart bewegen und am Grub-Bootmenü Linux im Single-User-Modus booten. Um den Single-User-Modus zu benutzen, geben Sie einfach im Grub-Bootmenü `linux single` ein. Dadurch bootet nur die Service Console, und »root« wird automatisch angemeldet. Die Passwortänderung führen Sie dann mit `passwd root` aus.

Alternative: Starten Sie den vSphere-Client auf dem ESX-Server, rufen Sie Users & Groups auf, dann root Edit und anschließend Change Password.

17.4 Firewall

VMware hat den ESXi 5 Server mit einer komplett überarbeitete Firewall ausgestattet. Genauer gesagt existierte unter ESXi 4 keine richtige Firewall, sondern nur Listener auf bestimmten Ports.

17.4.1 Firewall-Regeln anzeigen

Eine Auflistung des derzeit gültigen Regelwerks sehen Sie mit dem Befehl `esxcfg-firewall -q` ein, den Sie auf vMA oder dem vCLI ausführen können.

Außerdem müssen Sie Firewall-Systeme bedenken, die möglicherweise zwischen dem Administrations-Client oder vCenter bzw. dem Lizenz-Server und dem ESX-Server platziert sind.

Port	Richtung	Daten
80	eingehend TCP	Ungesicherter HTTP-Zugriff für VMware WebAccess, wird allerdings auf Port 443 umgeleitet.
443	eingehend TCP	WebAccess-Verbindungen von SDK-Zugriffen (API) entweder zum vCenter-Server oder direkt zum VMware ESX-Server, z. B. durch Zusatzsoftware
902	eingehend TCP ausgehend UDP	▸ vSphere-Client-Zugriff auf den vCenter-Server ▸ vCenter-Server-Zugriff auf den ESX-Server ▸ direkter vSphere-Client-Zugriff auf den ESX-Server ▸ ESX-Server-Host-Zugriff auf andere ESX-Server für Migration und Provisioning
903	eingehend TCP	▸ vSphere-Client-Zugriff auf die Konsolen virtueller Maschinen ▸ WebAccess-Client-Zugriff auf die Konsolen virtueller Maschinen
2049	eingehend TCP ausgehend TCP	Datenübertragungen von den NFS-Speichergeräten. Dieser Port wird auf der VMkernel-Schnittstelle und nicht auf der Service Console (ESX 4)verwendet.

Tabelle 17.1 Portübersicht VMware ESX 4 und 5.x unter vSphere

Port	Richtung	Daten
2050–5000	ausgehend TCP eingehend UDP ausgehend UDP	Datenverkehr zwischen dem ESX-Server für vSphere HA und den EMC Autostart Manager
3260	ausgehend TCP	Datenübertragungen von den Software-iSCSI-Speichergeräten. Dieser Port wird auf der VMkernel-Schnittstelle und auf der Service Console (ESX 4)verwendet. Bei Nutzung eines iSCSI-HBA muss dieser für den Port freigeschaltet werden; die Service Console (ESX 4)ist in diesem Fall nicht betroffen.
8000	ausgehend TCP eingehend TCP	Eingehende vMotion-Anfragen. Dieser Port wird nur auf der VMkernel-Schnittstelle verwendet.
8042–8045	ausgehend TCP eingehend UDP ausgehend UDP	Datenverkehr zwischen den ESX-Servern für vSphere HA und den EMC Autostart Manager
9000–9100	eingehend TCP	VMware Update Manager

Tabelle 17.1 Portübersicht VMware ESX 4 und 5.x unter vSphere (Forts.)

Die komplette Liste aller TCP- und UDP-Ports für vCenter-Server und andere Netzwerkmanagement-Komponenten finden Sie unter: *http://kb.vmware.com/kb/1012382*

17.4.2 Firewall-Bedienung

Der ESX-Server bringt einen Befehl zur Verwaltung der Firewall mit, der die wichtigsten Einstellungen ermöglicht: `esxcfg-firewall`.

Aktion	Befehl
Firewall-Status anzeigen	`esxcli network firewall get`
Firewall aktivieren/deaktivieren	`esxcli network firewall set --enabled/--disable`
aktive Firewall-Regeln auslesen	`esxcli network firewall ruleset list`

Tabelle 17.2 Verwendung von »esxcfg-firewall«

Oder per PowerCLI:

```
$ftpFirewallExceptions = Get-VMHostFirewallException -VMHost $host | where
{$_.Name.StartsWith('FTP')}  $ftpFirewallExceptions |
Set-VMHostFirewallException -Enabled $true
```

17.4.3 Custom Ports

Die mitgelieferten Dienste reichen in den wenigsten Fällen aus, da viele Zusatzprogramme wie Hardwaremanagement- oder Backup-Software eigene Ports nutzen. Allerdings ist es kein Problem, diese Ports freizuschalten, wenn Richtung, Protokoll und Portnummer bekannt sind. Der Parameter `-o` des Befehls `esxcfg-firewall` in der vCLI hilft an dieser Stelle weiter:

Syntax:

```
esxcfg-firewall -o <port,tcp|udp,in|out,name>
```

Beispiele:

```
esxcfg-firewall -o 11111,tcp,in,custom1
esxcfg-firewall -o 11111,tcp,out,custom2
esxcfg-firewall -o 11111,udp,in,custom3
esxcfg-firewall -o 11111,udp,out,custom4
```

Um die Ports wieder zu schließen, verwenden Sie einfach statt des `-o`-Parameters `-c`:

```
esxcfg-firewall -c 11111,udp,out,custom4
```

Um eine ganze Reihe von neuen Ports zu öffnen mittels vMA oder Linux vCLI:

```
for
(( x=8500; x<=8550; x++ )); do esxcfg-firewall -o $x,tcp,in,commvaulttest;
esxcfg-firewall -o $x,tcp,out,commvaulttest; done
```

Um neue Regelwerke zu aktivieren, können Sie das `esxcli`-Kommando nutzen:

```
esxcli --server=Servername network firewall refresh
```

17.5 SSL-Zertifikat

Während des ersten Starts des ESX-Servers wird durch den hostd automatisch ein SSL-Zertifikat erstellt. Dieses wird ab diesem Zeitpunkt für die Kommunikation zwischen Browser und ESX-Server bzw. zwischen VMware vCenter und ESX-Server genutzt. Wegen der Erzeugung über eine eigene und nicht über eine offizielle Zertifizierungsstelle ist dieses Zertifikat nicht vertrauenswürdig. Das Zertifikat ist im Verzeichnis */etc/vmware/ssl* zu finden und besteht aus den zwei Dateien *rui.crt* (öffentliches Zertifikat) und *rui.key* (privater Schlüssel). Diese können Sie durch eigene Zertifikatsdateien ersetzen.

Tipp

Das Zertifikat wird immer beim Start des `/etc/init.d/hostd restart`-Kommandos gesucht und gegebenenfalls neu erstellt. Daher können Sie durch Löschen oder Umbenennen der Zertifikatsdateien eine Neuerstellung erzwingen.

Achten Sie bei der Zertifikatserstellung darauf, dass keine Kennwortsätze (verschlüsselte Schlüssel) verwendet werden, da der VMware ESX-Server diese nicht interpretieren kann.

17.6 Überwachung

Den vSphere-SNMP-Agent aktivieren Sie am besten über den Befehl `vicfg-snmp.pl` im VMware vSphere Command-Line Interface. Dieses finden Sie unter *http://www.vmware.com/support/developer/vcli/*.

Aktivieren per `vicfg-snmp.pl` unter dem Community-String `public`:

```
vicfg-snmp.pl --server 192.168.1.10 --username root
  --password password -c public
vicfg-snmp.pl --server 192.168.1.10 --username root
  --password password --show
vicfg-snmp.pl --server 192.168.1.10 --username root
  --password password -enable
vicfg-snmp.pl --server 192.168.1.10 --username root
  --password password --show
```

Anpassung der Firewall:

```
esxcfg-firewall -e snmpd
```

SNMP-Traps

Bei Nutzung der VMware-SNMP-Dienste müssen die Trap-Ziele mittels vCLI oder PowerCLI konfiguriert werden:

```
vicfg-snmp.pl --server <host>--username <user> --password
<pass>-t <IP address>@162/<Community>
```

Oder im PowerCLI:

```
$hostSNMP = Get-VMHostSNMP
$hostSNMP = Set-VMHostSNMP $hostSNMP -Enabled:$true -ReadOnlyCommunity 'secret'
```

17.7 Protokollierung

Die Protokollierung ist ein wesentlicher Bestandteil einer abgesicherten Infrastruktur, um Anpassungen, Fehler und Ausfälle einsehen und nachvollziehen zu können. Eine zentrale Protokollierung mittels Syslog-Dienst ist sehr zu empfehlen.

Zentrale Protokollierung

In der Standardeinstellung protokolliert der Syslog-Dienst nur lokal. Dies können Sie allerdings umstellen, so dass ein zentraler Syslog-Server im Netzwerk alle Protokolldaten erhält.

VMware vSphere 5 liefert auf dem Installationsmedium des vCenter Servers einen eigenen Syslog-Dienst zur Installation unter Windows mit. Natürlich können Sie auch eigene Syslog-Server verwenden, z. B. von SolarWinds.

Den zentralen Syslog-Server müssen Sie auf jedem ESX-Server in den ADVANCED SETTINGS unter dem Punkt SYSLOG konfigurieren, wo der Parameter SYSLOG.GLOBAL.LOGHOST anzupassen ist (Abbildung 17.8). Sollen mehrere Syslog-Server genutzt werden, trennen Sie diese mittels Komma.

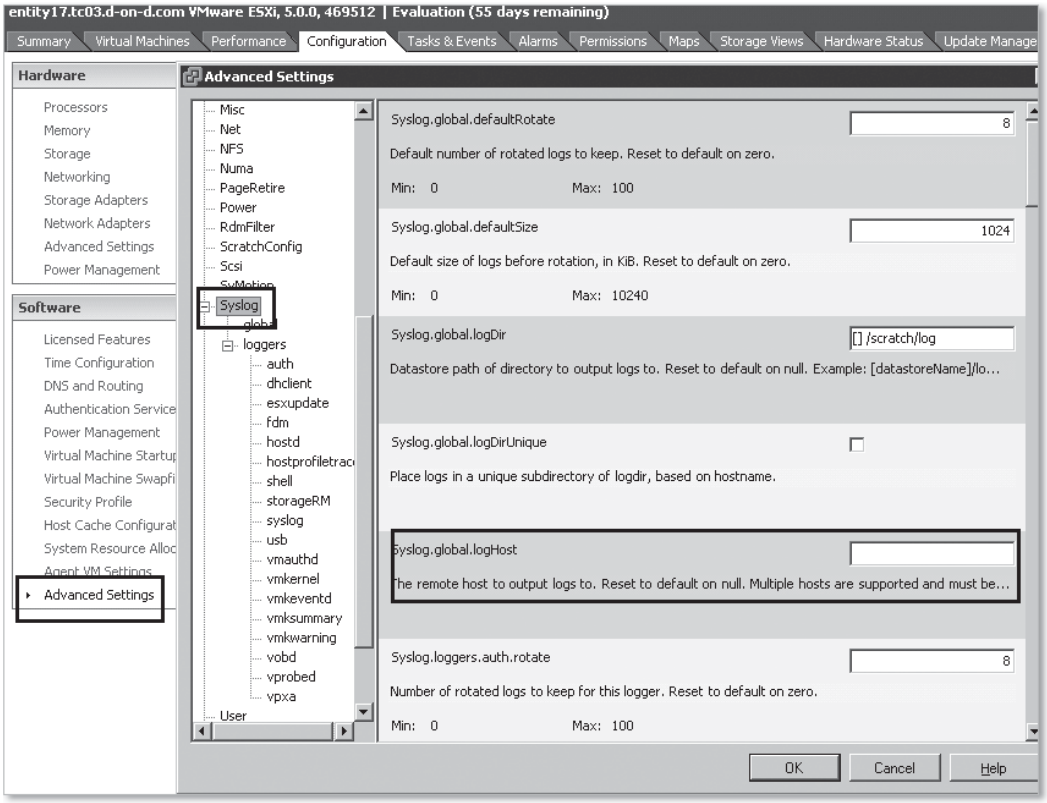


Abbildung 17.8 Einstellung des zentralen Syslog-Servers

Um möglichst lange möglichst viele Informationen in den Protokolldateien auf dem ESX-Host sehen zu können, aber die Protokolldateien auch nicht zu groß werden zu lassen, können Sie pro Protokollierer (*Logger*, z. B. *esxupdate*, *vmkwarning*) die Rotationen (Anzahl der vorzuhaltenden Dateien, nach Rotation aufgrund der Größe) und die Maximalgröße (SIZE – ab dieser Größe wird das Originalprotokoll rotiert) einstellen (Abbildung 17.9).

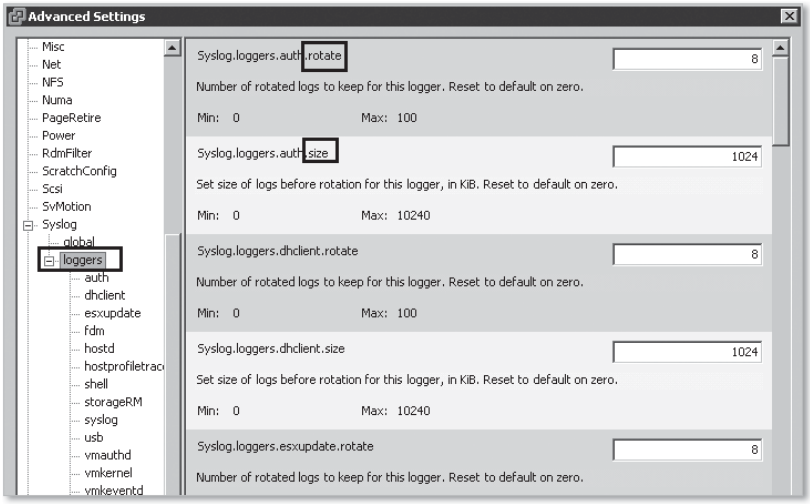


Abbildung 17.9 Syslog-Log-Rotate

Rotierung der Protokolldateien virtueller Maschinen

Jede virtuelle Maschine schreibt ein Protokoll in die Datei *vmware.log* in ihrem Heimatverzeichnis. Werden diese Protokolldateien zu groß, kann es zur kompletten Nutzung des Datastores kommen, was zu erheblichen Problemen beim Betrieb der virtuellen Maschinen führt.

Zur Lösung dieses Problems sollten Sie die Protokolldateien entweder löschen oder in gewissen Abständen rotieren, sobald eine gewisse Dateigröße erreicht wird. VMware ESX rotiert im Standard mit bis zu sechs Dateien, d. h. eine aktuelle Datei und fünf alte Protokolle. VMware schlägt die Protokollgröße von 500 KB als ausreichenden Wert vor. Die Protokollierung ist pro virtueller Maschine zu konfigurieren, was mittels vSphere-Client oder Kommandozeile möglich ist. Folgende Werte sind von Interesse: `log.rotateSize` (Größe der Log-Dateien in Bytes) und `log.keepOld` (Anzahl der zu haltenden alten Protokolldateien).

vSphere-Client: Edit Settings • Options • Advanced • Configuration Parameters • Add Row.

Externe Protokollierung

Neben der normalen Protokollierung auf den Festplatten ist ein weiterer Aspekt interessant, wenn es um die Sicherheit und um die Durchgängigkeit der Protokollierung geht: die Protokollierung über die serielle Schnittstelle. Dieses Verfahren wird vor allem im Bereich von Sicherheitskomponenten wie Firewall- oder Backbone-Routern angewandt und bietet im VMware ESX-Umfeld zwei große Vorteile:

- *Sicherheit vor Manipulation*
  Daten werden nicht auf die lokalen Festplatten, sondern über die serielle Schnittstelle auf ein weiteres Gerät geschrieben. Da dies nur in eine Richtung passiert, kann ein Angreifer keine Spuren verwischen, indem er die Protokolldateien nachträglich manipuliert.

- *Sicherheit vor Plattenausfällen*
  Fallen die lokalen Festplatten aus, ist ohne die Nutzung serieller Leitungen keine Protokollierung mehr möglich. Das Gerät an der seriellen Schnittstelle protokolliert auch bei Ausfall der lokalen Platten munter weiter.

Um den ESX-Server zur seriellen Protokollierung zu bewegen, sind folgende Schritte notwendig:

1. Anbindung eines zweiten Systems über die serielle Schnittstelle (z. B. per Null-Modem-Kabel)
2. Konfiguration des ESX-Servers zur Verwendung einer seriellen Schnittstelle – über vMA oder vCLI (`1` = COM1, `2` = COM2):

   ```
   esxcfg-advcfg -s 1 /Misc/LogToSerial
   ```

3. Starten eines Terminalprogramms für serielle Schnittstellen auf dem zweiten System mit Protokollierung auf der Festplatte

17.8 Nützliche Zusatzsoftware

Neben den »Papier«-Anweisungen zur Härtung des ESX-Hosts ist es sehr interessant, sich die folgenden kostenlosen Softwareprodukte näher anzuschauen, da diese eine automatische Konfigurationsüberprüfung oder auch -überwachung bieten.

17.8.1 HyTrust

HyTrust ist der Man-in-the-Middle einer virtuellen Infrastruktur, d. h., die HyTrust-Appliance sitzt netzwerktechnisch zwischen dem Administrator und der virtuellen Infrastruktur (z. B. vCenter) und überwacht die Anmeldevorgänge und Aktionen und ist auch in der Lage, diese zu blocken.

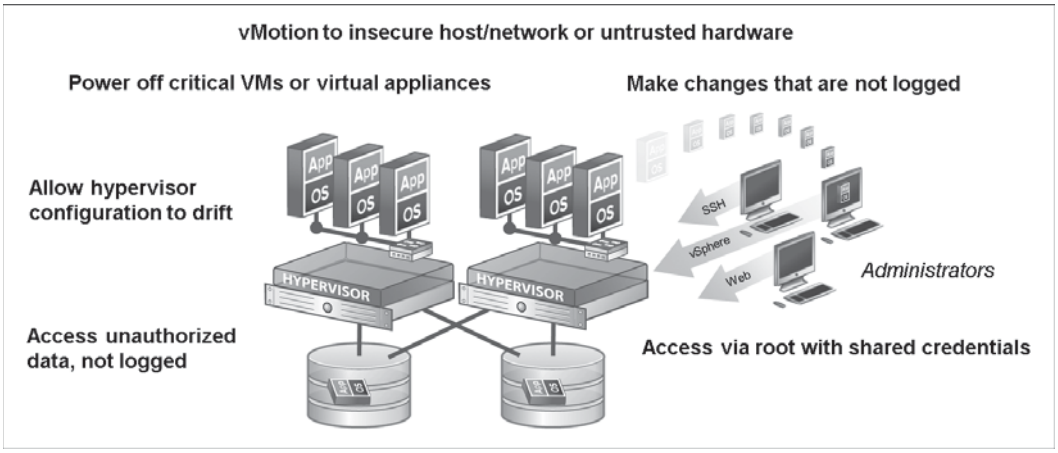


Abbildung 17.10 HyTrust-Szenario der möglichen Angriffe – Quelle: www.hytrust.com

Die Idee zur HyTrust-Appliance ist zwar simpel, aber hocheffizient, da keine Anpassungen im Netzwerk nötig sind. Die Appliance fügt sich als transparenter Proxy ein und verhindert die beliebigen Zugriffe, wie sie in Abbildung 17.10 zu sehen sind.

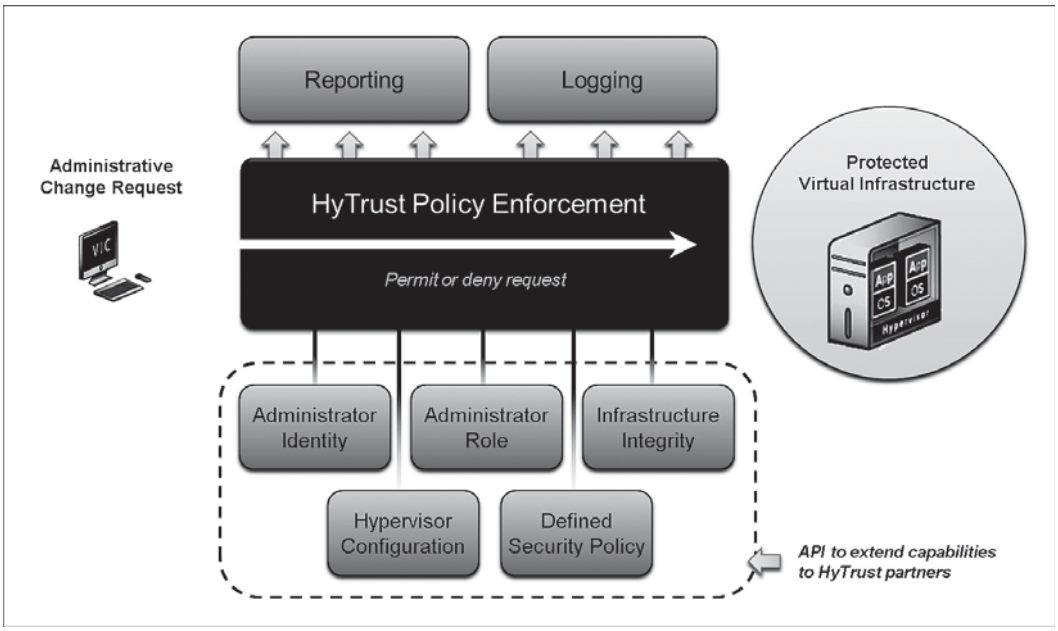


Abbildung 17.11 HyTrust-Konzept – Quelle: www.hytrust.com

Das HyTrust-Konzept besteht aus einem Regelwerk (Abbildung 17.11), das über die vorhandene virtuelle Infrastruktur »gestülpt« wird, d. h., bevor sich jemand am vCenter anmeldet, überprüft die HyTrust-Appliance dessen Berechtigung (z. B. auch bezüglich Netzwerkursprung). Außerdem können Sie komplexe Profile anlegen, die Tätigkeiten einzelner Personen durchführen sollen. Falls ein Benutzer im vCenter versehentlich mehr Rechte auf eine DMZ-VM als gewünscht hat, verhindert HyTrust die Anpassung der VM trotzdem, indem die Kommunikation zwischen vSphere-Client und vCenter Server bereits frühzeitig abgefangen und geblockt wird (Abbildung 17.12). Sämtliche Vorgänge werden protokolliert und können entsprechend dokumentiert werden.

Die Rollen und ihr Funktionsumfang werden zentral in der HyTrust-Appliance hinterlegt. Sie müssen sich daher nicht um die einzelnen ESX-Hosts oder vCenter-Systeme kümmern, sondern haben einen zentralen Ansatzpunkt (Abbildung 17.13).

Außerdem lassen sich mittels HyTrust Reports (Abbildung 17.14) generieren, die die VMware-Infrastruktur auf PCI-Compliance-Regeln hin testen und das entsprechende Ergebnis grafisch aufbereitet wiedergeben.

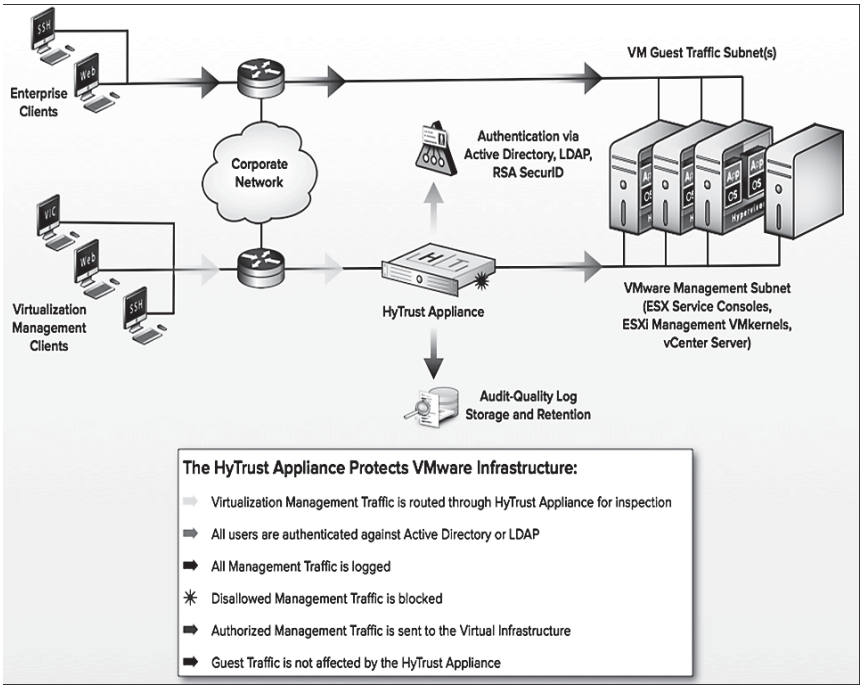


Abbildung 17.12 HyTrust-Design – Quelle: www.hytrust.com

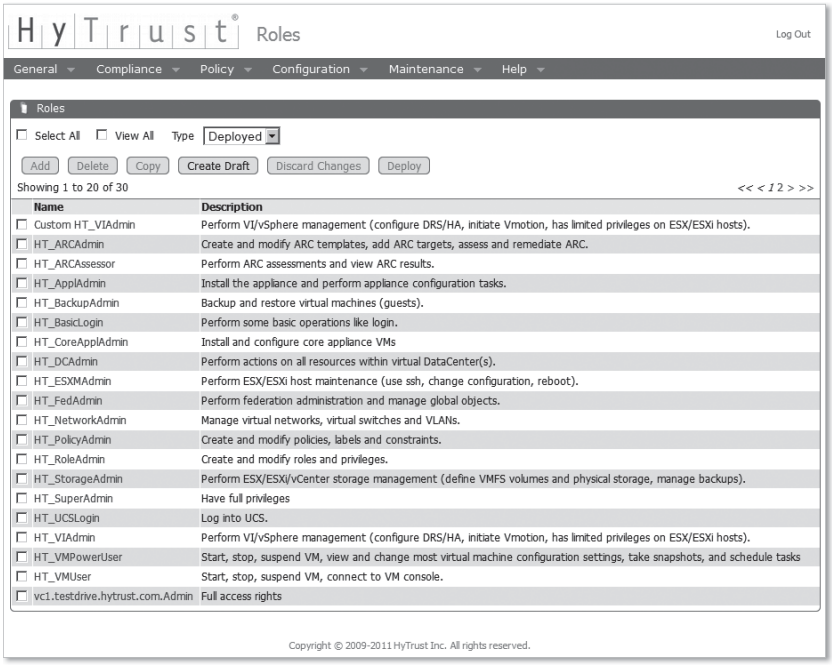


Abbildung 17.13 HyTrust – Rollenverteilung in der Appliance – Quelle: www.hytrust.com

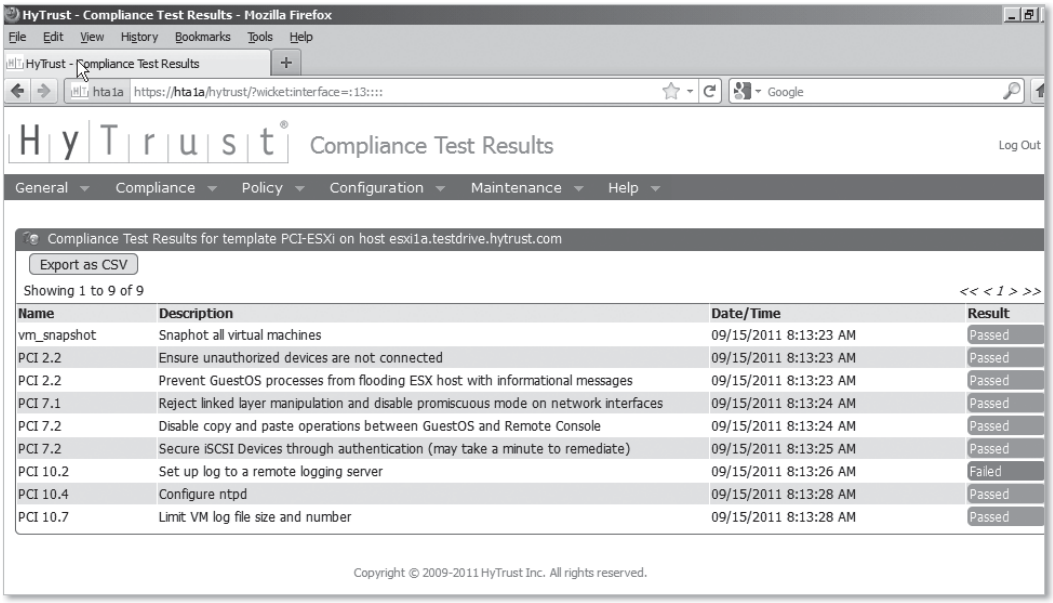


Abbildung 17.14 HyTrust PCI Compliance Report

17.8.2 icomasoft Opvizor

icomasoft Opvizor ist eine Software-as-a-Service-Lösung, die die VMware-Infrastruktur auf Konfigurations- und Protokollfehler sowie Sicherheitsprobleme und missachtete Best Practices hin untersucht und Sie mit einem »Lösungs-Dashboard« unterstützt.

Aktuell ist Opvizor in der Version 1.5 verfügbar und kann als Windows-Service im lokalen Netz (nur wenige MB großer Agent, der einmalig im Netzwerk installiert wird) oder per virtuelle Appliance in die VMware-Infrastruktur integriert werden. Nach einer Konfiguration mittels Browser können Sie Ihre Infrastrukturdaten online analysieren lassen.

Das Alleinstellungsmerkmal an Opvizor ist die zentrale Analysekomponente, die regelmäßig angepasst und erweitert wird, ohne dass der Endkunde Wartungen oder Updates durchzuführen hat. Wird ein Fehler bei einem Kunden auf der Plattform erkannt oder von einem Nutzer gemeldet, erstellt icomasoft die entsprechende Regel, so dass die Infrastrukturanalyse direkt auf dem neuesten Stand ist und alle anderen betroffenen Nutzer benachrichtigen und vorwarnen kann.

Da die Analyse online stattfindet, können Sie alle Daten lokal anonymisieren und verschlüsseln lassen, bevor Sie diese hochladen. Somit sind Sie sicher, keine IP-Adressen, Host-Namen oder Netzwerknamen in der Konfiguration oder den Protokolldaten auf die Opvizor-Plattform zu laden. Sie können den kompletten Vorgang und die verwendeten Daten einsehen.

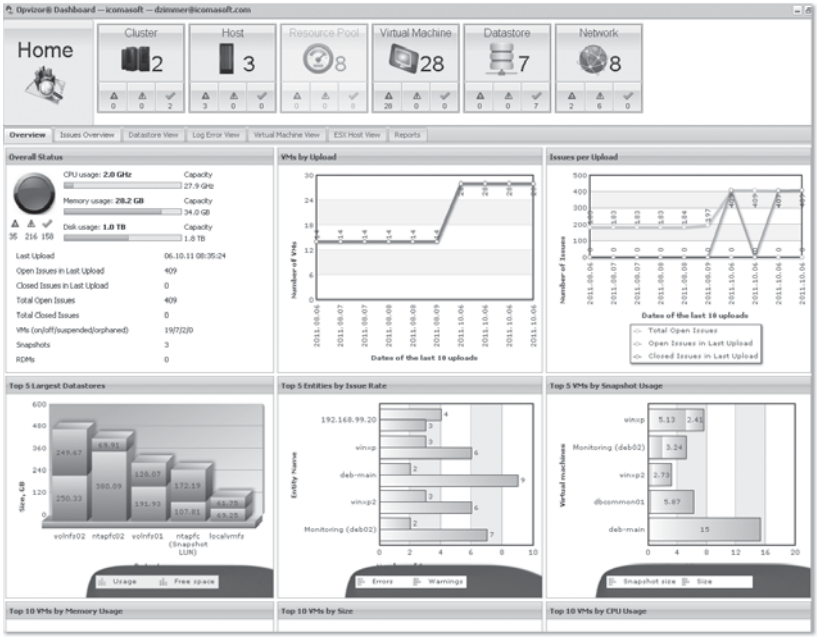


Abbildung 17.15 Opvizor-Dashboard – Quelle: www.opvizor.com

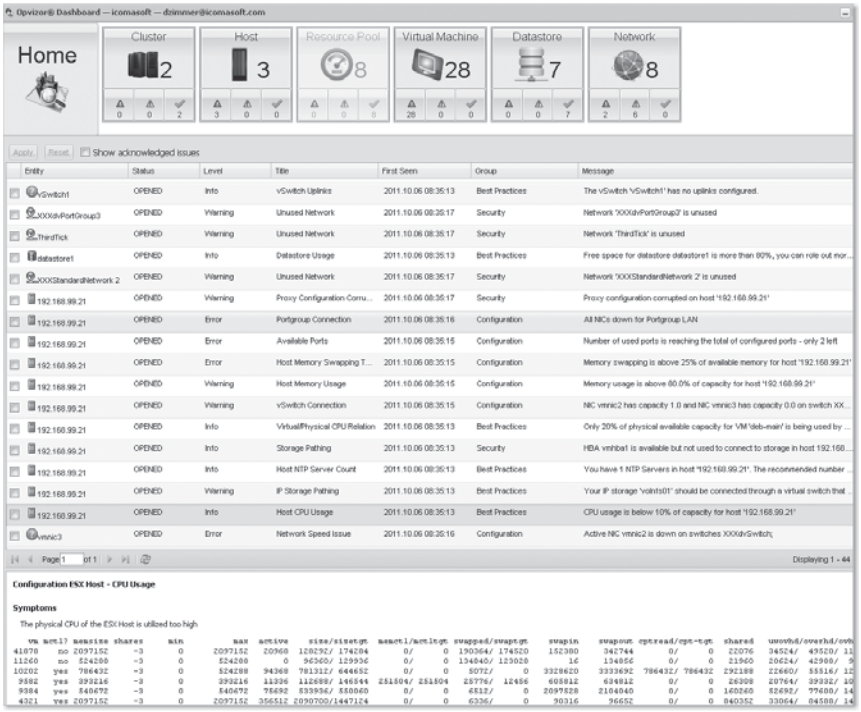


Abbildung 17.16 In der vSphere-Infrastruktur gefundene Probleme – Quelle: www.opvizor.com

17.9 Virtuelle Maschinen in der DMZ

Ein sehr gern diskutierter Schritt ist die Nutzung von virtuellen Maschinen in der DMZ. Dabei ist immer seltener das Ob eine Fragestellung, sondern vielmehr das Wie.

17.9.1 Isolation

Ein sehr einfach verständlicher Weg führt über die Absicherung der virtuellen Umgebung, indem diese isoliert wird, das heißt, der ESX-Server kann nur lokal angesprochen werden. Dazu werden Firewall-Systeme zwischen Internet, DMZ und LAN eingerichtet, die sämtlichen Netzwerkverkehr auf den Management Adapter oder die Service Console (ESX 4) des ESX-Hosts verbieten. Außerdem wird auf dem ESX-Host selbst die Firewall sehr konservativ konfiguriert und der Zugriff auf die Dienste per *hosts.allow-/deny*-Dateien sehr restriktiv eingerichtet.

Sämtliche Konfiguration muss entweder über die lokale Konsole an dem ESX-Host passieren oder über ein speziell zugelassenes Managementsystem, das an die SDK von VMware andocken kann, um entweder per vSphere-Client oder vCenter zu kommunizieren.

Das Management--Netzwerk muss natürlich von den Netzwerken der virtuellen Maschinen getrennt werden. Setzen Sie iSCSI oder NFS ein, müssen Sie auch diese Netze gegen Angriffe aus der virtuellen Maschine schützen, das heißt, auch hier muss eine Trennung erfolgen.

Je nach Sicherheitsstandard dürfen Sie keine VLANs nutzen, wodurch sich die Anzahl der Netzwerkports zwangsweise erhöht.

17.9.2 Firewalls und VMs

Es ist selbstverständlich möglich, auch in den virtuellen Maschinen Firewall-Software zu installieren und zu betreiben. Allerdings sind gerade Firewall-Funktionen enorme Netzwerk- und CPU-Ressourcenfresser, die häufig die IRQs belegen. Daher werden die Host-CPU und das Netzwerk deutlich belastet, wenn in jeder VM eine Firewall konfiguriert ist. VMware arbeitet allerdings sehr eng mit den Hardwareherstellern zusammen, wodurch dieses Problem vor allem durch neue Netzwerkkarten mit intelligenter IRQ-Nutzung relativiert wird.

Eine Alternative aus eigenem Hause hat VMware mit den vShield Zones entwickelt, die wir in Anhang B, »VMware-vShield-Zones-Produktfamilie«, getrennt beschreiben.

Ohne die Nutzung von Firewalls ist es allerdings nicht möglich, virtuelle Maschinen, die sich in den gleichen Portgruppen befinden, gegeneinander zu schützen, da eine Portgruppe mit einem physischen Switch ohne VLAN-Einrichtung vergleichbar ist.

17.9.3 PVLAN

Private VLANs (PVLANs) bieten hervorragende Möglichkeiten, virtuelle Maschinen voneinander abzuschotten, indem Sie die Modi Promiscuous, Community und Isolated verwenden.

- *Promiscuous* erlaubt jeglichen Datenverkehr und wird meist nur für das Parent-VLAN genutzt und nicht für die VM-Netze.
- *Community* erlaubt es allen virtuellen Maschinen, die Teil des Community-PVLANs sind, sich beliebig im Netzwerk zu unterhalten. Somit können VMs im Community-Netz nur im eigenen Netzwerk und mit Promiscuous-Netzwerken kommunizieren.
- *Isolated* erlaubt nur die Kommunikation mit Promiscuous-Netzen und nicht mit Community-Netzwerken und auch nicht mit anderen VMs im gleichen Isolated-Netzwerk. Diese Form des PVLANs bringt definitiv den höchsten Sicherheitsgrad bezüglich Kommunikationseinschränkung.

17.9.4 Best Practices

Es existieren allgemeine Best Practices, um virtuelle Maschinen in der DMZ zu betreiben, die Sie allerdings gegen die eigene Umgebung und deren Möglichkeiten abwiegen und prüfen müssen.

- ESX-Hosts mit eigenen LUNs für die DMZ-VMs verwenden
- ESX-Hosts in der DMZ von ESX-Hosts im normalen LAN trennen
- keine DMZ-VMs mit LAN-VMs auf dem gleichen ESX-Host oder der gleichen LUN mischen
- Bei der Nutzung von DRS-Clustern müssen entsprechende Regeln zum Schutz vor automatischer Migration getroffen werden, um keine Mischumgebungen zu schaffen.
- Storage vMotion und vMotion werden im Klartext durchgeführt, daher sollten diese Netze vom Netzwerk der virtuellen Maschinen getrennt werden.

17.10 VMs und der Virenschutz

Ein sehr unschönes Problem wurde in den letzten Jahren oft bei Kunden festgestellt, die in den VMs sehr aktive Virenschutzprodukte betreiben, da diese häufig Pattern-Updates laden und installieren. Dieses Problem wird beim Betrieb von vielen virtuellen Desktops enorm, da sich die Anzahl der Pattern-Updates aufgrund der hohen Anzahl virtueller Desktops nicht selten verhundertfacht.

17.10.1 Pattern-Updates

Dabei wurde auch festgestellt, dass manche Virenschutzsoftware zwar nur wenige MByte an Pattern-Aktualisierung lädt, allerdings das Entpacken der Pattern und Integrieren in die Viren-

schutzsoftware mehrere Hundert MByte an Daten verändert. Dies stört bei einem Server nicht weiter, bei Hunderten oder Tausenden Desktops jedoch sehr, da der Storage im Hintergrund doch sehr belastet wird. Daher sollten Sie eine Trennung der Updatezyklen nach Server-Gruppen in Betracht ziehen, so dass immer nur Teile der Infrastruktur zur gleichen Zeit aktualisiert werden.

17.10.2 CPU-Last im Host

Ein weiteres Problem bei der Nutzung von Virenschutzsoftware in den Gästen liegt im sporadischen Lastverhalten der Gäste, was sich direkt auf die Host-Systeme und deren CPU-Last auswirkt. Hier wurde schon öfter beobachtet, dass der Task-Manager in den virtuellen Maschinen eine sehr geringe CPU-Nutzung anzeigte, während die Ansicht über `esxtop` oder die CPU-Grafiken des vSphere-Clients eine andere Wahrnehmung hin zur Volllast hatte. Es stellte sich in der Vergangenheit bereits öfter heraus, dass der Virenschutz eine gewisse Mitschuld hatte. VMware und natürlich auch die Virenschutzhersteller verbessern das Zusammenspiel jedoch stetig.

17.10.3 Antwortzeiten im Gast

Virtuelle Maschinen können aufgrund der gemeinsamen Nutzung der physischen Hardware im Gegensatz zu physischen Systemen niemals schneller als diese werden. Allerdings ist es auch nicht möglich, bei gleicher Ausstattung die gleichen Maximalergebnisse zu erreichen. Trotzdem sind die Leistungsunterschiede minimal und daher zumeist zu vernachlässigen.

Bei der Nutzung von Virenschutzsoftware haben sich allerdings die etwas langsameren Antwortzeiten über das Netzwerk als Problem dargestellt, so dass z. B. ein Pattern-Update länger dauert als auf der physischen Hardware. Auch hier wieder der Hinweis: Bei 10 Servern merkt dies niemand, bei 1.000 wird es langsam sehr deutlich.

Hier helfen nur Verbesserungen durch die Hersteller und eine Gruppierung der Systeme. Zum Beispiel ist eine Trennung der Updatezyklen nach Server-Gruppen sinnvoll, so dass immer nur 50 oder 100 Systeme aktualisiert werden und die nächsten 100 erst fünfzehn Minuten später.

17.10.4 Fileserver mit Virenschutz

Die Königsklasse der Ressourcenvernichtung besteht natürlich im Betrieb eines virtuellen Fileservers mit eingeschaltetem Virenschutz. Natürlich ist ein virtueller Fileserver bei gleicher Ausstattung etwas langsamer als ein physisches System. Dedizierte NAS-Produkte, wie beispielsweise NetApp Filer, sind nochmals deutlich schneller. Kommt der Virenschutz hinzu, so ist eine solche Lösung nur für kleinere Umgebungen (kleine Unternehmen oder Projektgruppen) mit wenigen Hundert Benutzern sinnvoll. Allerdings verfügt man in größeren Umgebungen auch meist über dedizierte physische Fileserver oder NAS-Systeme, die genau auf diese

Anwendungsprofile ausgelegt sind. Aus einigen der oben genannten Gründe wurde die VMsafe-API entwickelt, die Prozesse des Virenschutzes in virtuellen Infrastrukturen optimieren und absichern soll.

17.11 VMware VMsafe-API

VMware hat mit vSphere die VMsafe-API ins Leben gerufen, die auf einer Initiative begründet ist, dass Hersteller von Sicherheitssoftware die Kernel-Informationen und damit auch die Informationen über alle virtuellen Maschinen mitlesen können. Damit würde sich ein Agent in jedem Gastbetriebssystem erübrigen, was deutliche Last von den VMware-Systemen nähme.

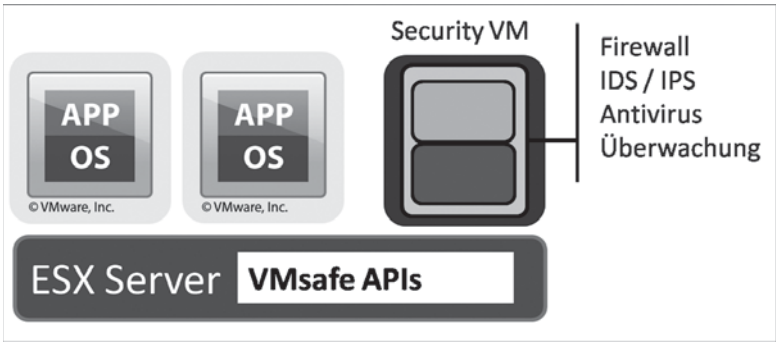


Abbildung 17.17 Durch VMsafe geschützte VMs

Zum Beispiel sind Hersteller von Antivirensoftware durch die VMsafe-API in der Lage, Informationen vom VMkernel direkt zugestellt zu bekommen und diese auf Viren und andere Schadsoftware hin zu analysieren. Dazu muss von der Idee nur eine Antivirusinstanz als virtuelle Appliance vorhanden sein und den Datenverkehr, die Hauptspeicherzugriffe, die Prozesse oder den Netzwerkverkehr überwachen und gegebenenfalls eingreifen. Die VMsafe-API kann vom Endanwender nicht konfiguriert oder manipuliert werden und muss seitens VMware natürlich so sicher aufgestellt werden, dass keine Entwickler von Schadsoftware in den gleichen Genuss kommen können. Daher arbeitet VMware auch sehr eng mit Unternehmen wie McAfee, Symantec oder Trend Micro zusammen.

Oftmals sind die Lizenzierungsmodelle von Software auf den ersten Blick nicht so klar, wie mancher es sich wünschen würde. Im folgenden Kapitel werden wir genau diesen Sachverhalt angehen. Wir werden versuchen, ein Höchstmaß an Transparenz in die Lizenzierung von vSphere und die damit verbundenen Fragestellungen zu bringen. Außerdem werden wir Fragen zum Support behandeln und das Lizenzportal näher beleuchten.

18 Die Lizenzierung von vSphere

Autor dieses Kapitels ist Günter Baumgart, guenter.baumgart@anmax.de

Die Lizenzierungsmodelle der Softwarehersteller sind sehr unterschiedlich. Jeder Hersteller hat eigene Methoden, seine Software zu vermarkten. Hier gilt es, gut darauf zu achten, dass das Lizenzierungssystem vor der Bestellung verstanden wurde, da sonst sehr schnell große Schäden entstehen. Im Vorfeld müssen immer sehr viele Fragen beantwortet werden, darunter:

- Wie viele Pakete oder Bundles gibt es überhaupt?
- Welche Merkmale sind in welchem Paket enthalten?
- Was kosten Lizenzen?
- Worauf basiert die Lizenzierung eigentlich?

Sicher haben Sie sich auch schon oft derartige Fragen stellen müssen und hoffentlich auch immer richtige Antworten bekommen. Die Beispiele zur Lizenzierung, die Sie auf den Folgeseiten finden werden, enthalten hier und da auch Preise. Diese stammen aus der Preisliste von VMware (Oktober 2011). Bitte fragen Sie, wenn Sie eine Beschaffung planen, immer nach aktuellen Preisen für die Lizenzen. Prüfen Sie lieber einmal mehr nach, ob sich in der Kombination der Softwaremerkmale kürzlich Änderungen ergeben haben. Wer möchte schon, nachdem er sich alles mühevoll zusammengestellt hat und im Unternehmen unterschiedlichste Hürden nehmen musste, letztendlich erfahren, dass der Etat doch nicht ausreicht? Der umgekehrte Fall kommt eigentlich eher seltener vor.

Auch müssen Sie immer im Auge behalten, dass es sogenannte *Acceleration-Kits* gibt. Hierbei handelt es sich um Pakete, die im Vergleich zu Einzellizenzen einen deutlichen Preisvorteil bieten. An dieser Stelle wird bereits klar, dass eine genaue Kenntnis der VMware-Lizenzthematik zu Einsparungen führen kann.

18.1 Die unterschiedlichen Editionen und Pakete

VMware bietet zum Zeitpunkt der Drucklegung dieser neuen Auflage mehrere unterschiedliche Gruppen von Paketen an. In der Vergangenheit musste beachtet werden, dass nicht alle Pakete erweiterbar waren. Dies ist in der aktuellen Version 5 von vSphere nicht mehr der Fall. Der große Vorteil hierbei liegt auf der Hand: Sie müssen sich im Vorfeld keine Gedanken mehr darüber machen, wie und in welcher Form Sie zukünftig Ihre Umgebung betreiben möchten. Sie können einfach später auf eine andere Version hochrüsten und die benötigten Merkmale und Erweiterungen erst dann nutzen, wenn Sie sie auch brauchen. Eine Fehlinvestition ist somit nicht mehr so schnell getätigt.

18.1.1 Grundlegende Informationen zur Lizenzierung

Mit der neuen Version hat sich bei der Lizenzierung vieles gegenüber der früheren Version geändert. Es sind Begriffe wie *Virtual Memory* (vRAM) und *Physical Memory* (pRAM) hinzugekommen, die die erhebliche Veränderung im Bereich der Lizenzierung einer virtuellen Plattform maßgeblich beeinflussen. Unter *pRAM* versteht man den in einen physischen Server eingebauten Hauptspeicher (RAM). Mit *vRAM* wird der Hauptspeicher einer virtuellen Maschine bezeichnet (Abbildung 18.1).

Eine wesentliche Neuerung ist, dass die Lizenzierung von vSphere 5 weder die Anzahl der Kerne pro Prozessor noch den physischen RAM pro Server beschränkt. Es ist also entgegen früherer Lizenzierungsmethoden völlig unerheblich, ob die eingesetzte CPU vier, sechs, acht, zehn oder zwölf Kerne enthält.

Die zweite große Veränderung in der Lizenzierung ist die sogenannte *vRAM-Berechtigung*. Diese sagt aus, dass jede vSphere 5-Prozessorlizenz eine vRAM-Berechtigung enthält. In den aktuellen Versionen sind das 32 GB, 64 GB oder 96 GB vRAM je CPU-Lizenz. Die unterschiedlichen Werte sind an die unterschiedlichen Lizenzklassen, wie z. B. Standard, Enterprise oder Enterprise Plus, gebunden. Bei der bisherigen Betrachtungsweise lag der Fokus immer auf einer Lizenz und der hierin enthaltenen vRAM-Berechtigung. Was geschieht aber beim Management von vSphere-Hosts mit vCenter? Um diese Frage zu beantworten, ist es erforderlich, einen neuen Begriff, den *vRAM-Pool*, ins Spiel zu bringen. Ein vRAM-Pool beschreibt die Gesamtsumme der verfügbaren vRAM-Berechtigungen, die von einer einzelnen VMware vCenter-Server-Instanz oder durch mehrere Instanzen von VMware vCenter-Server im Linked-Mode-Betrieb in einer Umgebung verwaltet werden. Beachten Sie bitte unbedingt, dass jede Edition von vSphere einen separaten vRAM-Pool darstellt. Das bedeutet, dass die Editionen (Standard, Enterprise, Enterprise Plus) identisch sein müssen, wenn Sie Ihrem bereits bestehenden vRAM-Pool zusätzliche Lizenzen bzw. vRAM hinzufügen möchten. Ein Mischen ist nicht möglich! Wenn Sie versuchen, einem bestehenden vRAM-Pool Lizenzen von unterschiedlichen Editionen hinzuzufügen, hat dies keine Auswirkung. Er wird also keine Vergrößerung des vRAM-Pools stattfinden.

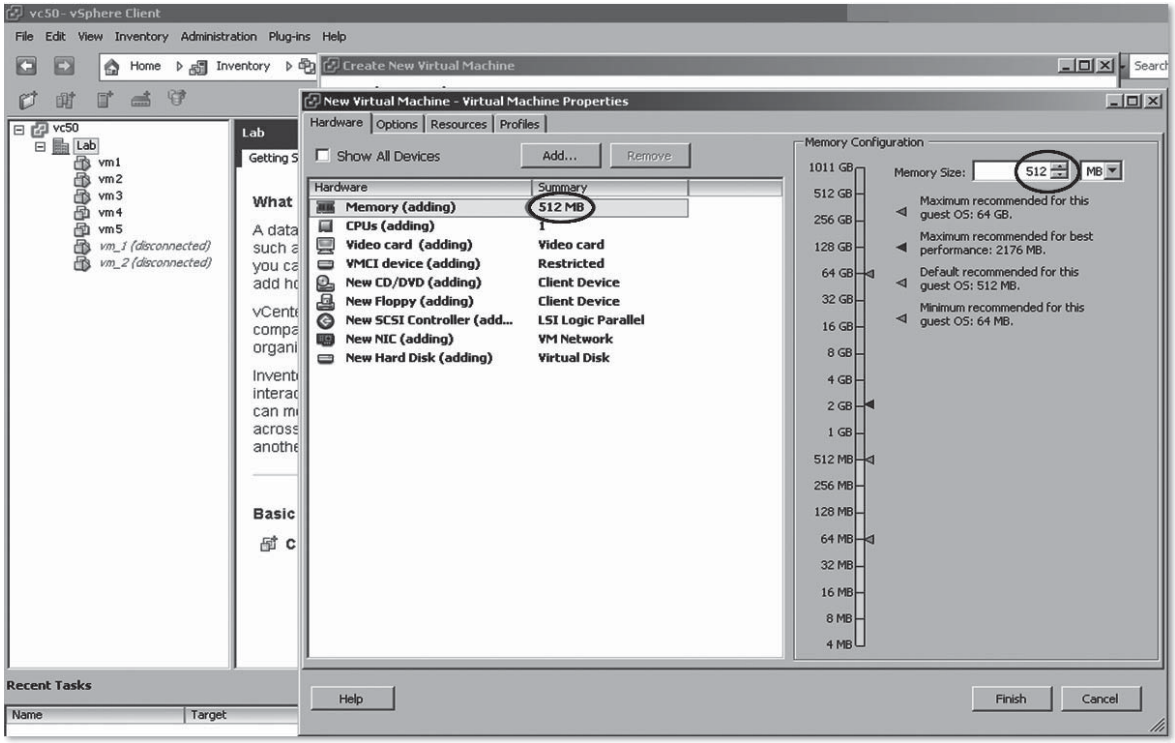


Abbildung 18.1 An dieser Stelle wird der virtuellen Maschine der virtuelle Hauptspeicher (vRAM) zugeordnet. Der vRAM ist also die Speichermenge, die für eine virtuelle Maschine konfiguriert wird.

Halten wir also fest: Bei Bedarf können Sie die verfügbare vRAM-Pool-Kapazität durch Hinzufügen weiterer Prozessorlizenzen der gleichen Edition erhöhen. Außerdem können wir festhalten, dass die vRAM-Pool-Kapazität die maximal nutzbare Kapazität bei einer vorliegenden Anzahl von lizenzierten Prozessoren ist.

Bisher haben wir ausschließlich über die Bereitstellung und Ergänzung von vRAM in unterschiedlichen Editionen berichtet. An dieser Stelle betrachten wir nun den Verbrauch oder auch die Nutzung von vRAM. Grundsätzlich können nur eingeschaltete virtuelle Maschinen vRAM-Kapazität nutzen. Die sich im Environment befindlichen ausgeschalteten virtuellen Maschinen, in denen vRAM vergeben wurde (Abbildung 18.1), zählen nicht als Verbraucher von vRAM.

An dieser Stelle möchte ich Ihnen ein konstruiertes Beispiel geben, um diesen Sachverhalt ganz deutlich herauszustellen. Nehmen wir einmal an, dass die zu betrachtende Umgebung keinen freien vRAM mehr besitzt. Die eingeschalteten virtuellen Maschinen belegen sämtliche innerhalb des vRAM-Pools befindlichen Ressourcen. Es wird aber unbedingt eine zusätzliche virtuelle Maschine für das Backup benötigt, die momentan aufgrund zu knapper Ressourcen ausgeschaltet bleiben muss. Die virtuelle Maschine für das Backup soll allerdings

ausschließlich außerhalb der Kernarbeitszeit eingeschaltet und betrieben werden. In dieser Zeit können jedoch andere Dienste, die nur innerhalb der Kernarbeitszeit benötigt werden, abgeschaltet werden. Dieses Beispiel zeigt ganz deutlich den Fall, dass eine Überschreitung des maximal nutzbaren vRAMs in einer Umgebung zu vermeiden ist, indem virtuelle Maschinen in unterschiedlichen Zeitfenstern den verfügbaren vRAM nutzen können.

Zur Überwachung der vRAM-Auslastung in Echtzeit wurde in das vCenter-Alarmsystem eine entsprechende Funktion integriert. Bei einer Überschreitung der maximalen Ressourcen produziert das System Meldungen. Eine Einschaltungsverhinderung oder Abschaltung von virtuellen Maschinen seitens des Systems erfolgt in dieser Version nicht!

Das Verschieben von virtuellen Maschinen mittels vMotion erfordert keinen gesonderten vRAM. Da der vRAM über alle Hosts derselben vSphere-Edition hinweg unter einem vCenter-Server in einem Pool zusammengefasst wird, kann jede virtuelle Maschine auf jedem Host eines vRAM-Pools ausgeführt werden.

In der Regel sind alle in den Hosts enthaltenen CPUs einer Umgebung lizenziert. Falls die Umgebung mehr vRAM benötigt, als diese sämtlichen in der Umgebung befindlichen vRAM-Berechtigungen, also Prozessorlizenzen, können Sie weitere Prozessorlizenzen in den vCenter-Server eingeben. Hierbei erhöht sich die vRAM-Kapazität des vRAM-Pools.

Ein Nebeneffekt ist, dass es eine Art Überhanglizenz in Bezug auf mögliche Host-Prozessoren in der virtuellen Umgebung gibt. In eine derartig lizenzierte Umgebung können Sie natürlich auch zu einem späteren Zeitpunkt noch einen weiteren Host integrieren, ohne eine weitere Lizenz in den vCenter-Server eintragen zu müssen.

Sollten in Ihrer Umgebung zwei vCenter in der Standard-Edition mittels Linked Mode verbunden worden sein, erstreckt sich der vRAM-Pool selbstverständlich über beide vCenter.

18.1.2 vSphere 5 – for free

Der ESXi Server ist nach wie vor die kostenfreie Variante des Hypervisors zur Server-Virtualisierung aus der VMware-Produktfamilie. Wie Abbildung 18.2 zeigt, unterstützt diese Server-Variante Acht-Wege-vSMP, 32 GB physischen Hauptspeicher, eine unlimitierte Anzahl von CPUs mit einer unbeschränkten Anzahl von Kernen, 32 GB vRAM sowie Thin Provisioning. Das Bemerkenswerte an der kostenfreien Variante ist, dass der physische Hauptspeicher (pRAM) limitiert ist.

Merkmale	ESXi
vSMP (Virtual Symmetric Multi-Processing)	8-way
pRAM je Host (physical Memory)	32 GB
vRAM je Host (virtual Memory)	32 GB
physical CPU je Host	unlimited
physical Cores per CPU	unlimited
Thin Provisioning	
vCenter Agent für VMware-Host	
Update Manager	
vStorage APIs für Data Protection	
Data Recovery	
HA (High Availability)	
VMotion™	
VSPC (Virtual Serial Port Concentrator)	
Hot Add	
vShield Zones	
Fault Tolerance	
VAAI (Storage-APIs für die Array-Integration)	
MPIO (Storage-APIs für Multipathing)	
Storage Vmotion ™	
DRS (Distributed Resources Scheduler)	
DPM (Distributed Power Management)	
Storage I/O Control	
Network I/O Control	
Distributed Switch	
Host Profiles	
Auto Deploy	
Storage DRS	
Profilgesteuerter Speicher	
Lizenzkosten für einen Host	0 EUR
Stand der Preisliste: Oktober 2011	

Abbildung 18.2 Die Leistungsmerkmale des ESXi, der freien Version des VMware Bare Metal Hypervisors.

18.1.3 vSphere 5 – Small Business

Eine weitere Möglichkeit, Virtualisierung zu praktizieren, stellt VMware mit den beiden Essential-Paketen zur Verfügung.

Essential ist in zwei unterschiedlichen Variationen erhältlich: als Essential und als Essential Plus. Das Interessante daran ist, dass der vCenter Server in beiden Paketen in der Version Foundation enthalten ist. Der vCenter Server kann in diesen Versionen zwar nur in einem Dreiknotenverbund eingesetzt werden, aber das ist bei modernen Servern ja unter Umständen kein Nachteil.

Denken Sie an dieser Stelle z. B. an Server, die mit zwei Sockeln ausgestattet sind und jeweils 12 Kerne je CPU enthalten. Ein derartiger Dreiknotenverbund enthält immerhin 72 Kerne. Diese Menge an möglicher Leistung ist für viele kleine Anwender oftmals viel mehr als hinreichend.

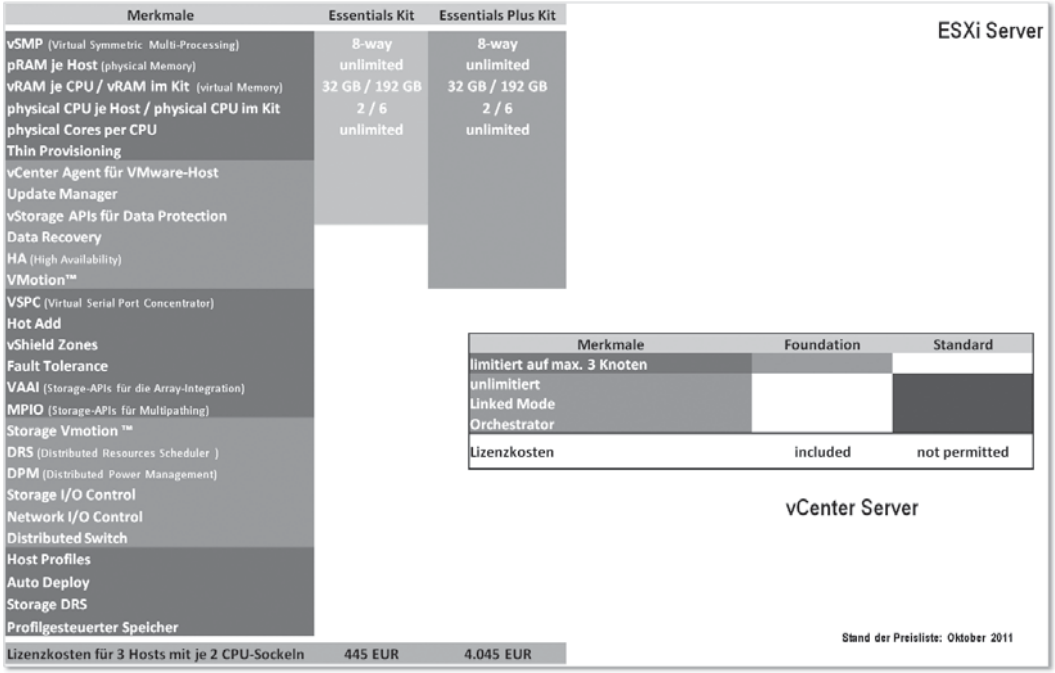


Abbildung 18.3 Die Leistungsmerkmale des Small-Business-Paketes

Die Leistungsmerkmale dieser beiden Essential-Versionen können sich wirklich sehen lassen (Abbildung 18.3). Zusätzlich zu den Merkmalen der ESXi-Version umfassen die Essential-Versionen den vCenter Agent, die vStorage API für Data-Protection und den Update Manager. Die Variante Essential Plus bietet darüber hinaus High Availability (HA), Data Recovery und vMotion. Das ganze Essential-Paket ist in beiden Varianten für drei Hosts mit je zwei CPU Sockeln ausgelegt. Da vSMP auch in dieser Edition für acht Wege enthalten ist, dürfen virtuelle Maschinen maximal acht virtuelle CPUs enthalten. Die Größe des physischen RAMs eines Hosts ist in diesem Lizenzmodell unbeschränkt. Natürlich gibt es auch keinerlei Beschränkungen der maximalen Anzahl der Kerne in den CPUs, die in den Hosts enthalten sind. Allerdings ist die vRAM-Berechtigung je Host-Prozessor auf 32 GB begrenzt. Das vRAM-Pooling legt somit die maximale Obergrenze der Nutzung von vRAM für die virtuellen Maschinen auf 3 × 2 × 32 GB, was 192 GB entspricht, fest.

Was die Erweiterung angeht, bietet VMware gegenüber früher alle Möglichkeiten des Upgrades. Upgrades von Essential hin zu Essential Plus sind genauso möglich wie von beiden Essential-Versionen auf jedes andere Acceleration-Kit für Enterprise-Environments. So ist ein Upgrade von vSphere 5 Essentials auf vSphere 5 Enterprise Plus Acceleration-Kit ohne weiteres möglich. Dem Wachsen einer Umgebung und die Erweiterung der Funktionalität von Umgebungen sind somit aus der Sicht der Lizenzierung keine Grenzen gesetzt.

18.1.4 vSphere 5 – Standard, Enterprise und Enterprise Plus

Die drei Editionen vSphere 5 Standard, Enterprise und Enterprise Plus haben natürlich ebenfalls keinerlei Beschränkungen; lizenztechnisch ist auch hier immer noch alles möglich. Die Lizenzierung geschieht auf Basis eines einzelnen Sockels. Das heißt, dass Sie beispielsweise für einen physischen Server, der mit vier Sockeln ausgerüstet ist, die alle mit CPUs bestückt sind, vier ESX-Server-Lizenzen benötigen.

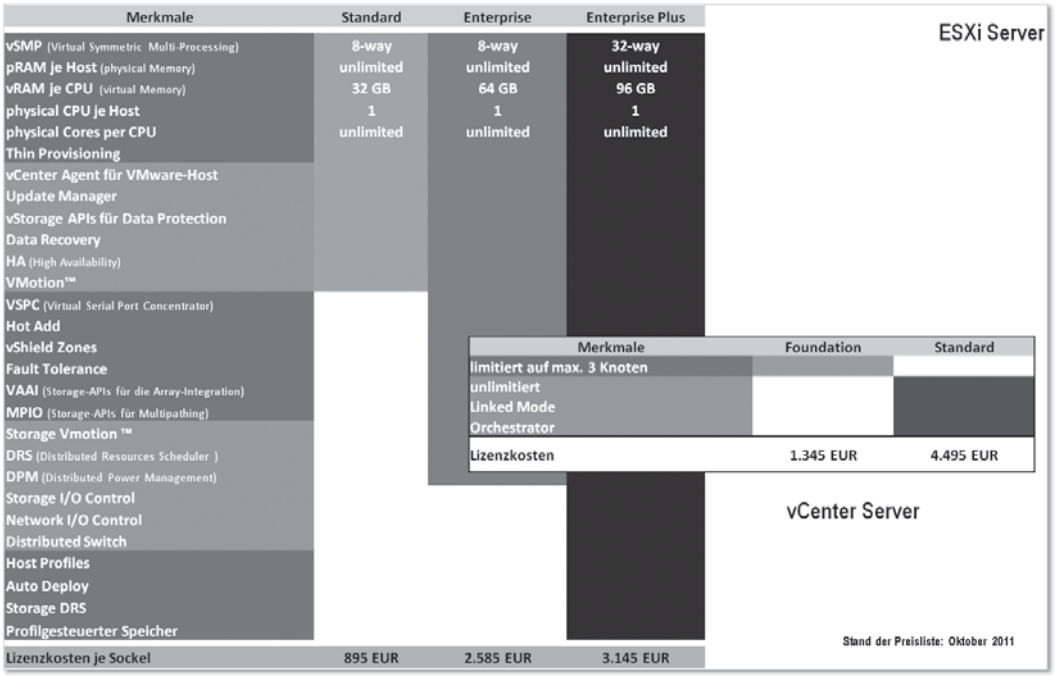


Abbildung 18.4 Die Leistungsmerkmale der Editionen im Enterprise-Umfeld

Die Beschränkung bezüglich der Kerne einer CPU ist gegenüber früher aufgehoben worden. Es gilt: Die Anzahl von Kernen einer CPU ist unlimitiert. Des Weiteren unterstützt vSMP in den Versionen Standard und Enterprise 8-Wege- und in der Version Enterprise Plus sogar 32-Wege-vSMP. Die Ausstattung der Hosts mit Hauptspeicher (pRAM) ist auch in diesen drei Editionen unbeschränkt.

Kommen wir nun zum vRAM. Die drei Editionen in der Enterprise-Klasse wurden von VMware mit ganz unterschiedlichen Leistungsbeschränkungen bedacht. In der Standard-Edition liegt der Schwellenwert bei 32 GB je Prozessor und Sockel. Die Enterprise-Edition erlaubt eine maximale Nutzung von 64 GB vRAM für den Betrieb von virtuellen Maschinen. Bei der Enterprise Plus Lizenz darf der maximale Verbrauch von vRAM bei 96 GB nicht überschritten werden.

Die Standard-Lizenzierung enthält über die Leistungsmerkmale der freien Version hinaus die im Folgenden gelisteten Leistungsmerkmale:

- vCenter Agent für VMware-Host
- Update Manager
- vStorage APIs für Data Protection
- Data Recovery
- High Availability
- vMotion

Interessant hierbei ist, dass die Leistungsmerkmale in dieser Version den Leistungsmerkmalen der Essential-Plus-Edition entsprechen.

Die Enterprise-Lizenzierung umfasst zusätzlich zu den Leistungsmerkmalen der Standard-Edition die im Folgenden gelisteten Leistungsmerkmale:

- Virtual Serial Port Concentrator
- Hot Add
- vShield Zones
- Fault Tolerance
- Storage-APIs für die Array-Integration
- Storage-APIs für Multipathing
- Storage vMotion
- Distributed Resources Scheduler
- Distributed Power Management

Die Enterprise-Plus-Edition ermöglicht darüber hinaus die folgenden Leistungsmerkmale:

- Storage I/O Control
- Network I/O Control
- Distributed Switch
- Hostprofile
- Auto Deploy
- Storage DRS
- profilgesteuerter Speicher

Also auch in vSphere 5 hat VMware durch Leistungsmerkmale deutlich gemacht, dass es sich bei Enterprise Plus um ein Lizenzierungsmodell für große Strukturen handelt.

Beim vCenter Server gibt es nach wie vor zwei unterschiedliche Methoden der Lizenzierung: Zum einen die Variante der Limitierung auf drei Knoten, wobei hier die Größe der drei

physischen Server nicht beschränkt ist. Setzen Sie zum Beispiel Acht-Sockel-Maschinen ein, die je Sockel und CPU 12 Kerne enthalten, kommen Sie bei der Lizenzierung bezüglich Foundation auf stolze 288 Kerne. Außerdem variiert natürlich auch die Menge vRAM je nach eingesetzter Edition deutlich. Zum anderen besteht die Möglichkeit, eine unlimitierte Version zu erwerben, die dann auch das Merkmal Linked Mode enthält und den Einsatz des Orchestrators gestattet.

Die auf drei Knoten limitierte Version wird, wie bereits erwähnt, als »Foundation« und die unlimitierte Version als »Standard« bezeichnet. Natürlich hat VMware auch hier keine Ausnahme beim Upgrade gemacht: Ein Upgrade von vCenter Server Foundation hin zu vCenter Server Standard ist ebenfalls problemlos möglich.

18.1.5 vSphere 5 – Standard, Enterprise und Enterprise Plus als Pakete

Wie Sie in Abschnitt 18.1.3, »vSphere 5 – Small Business«, bereits gesehen habe, können Sie auch im Paket lizenzieren und natürlich auch möglich, Standard-, Enterprise- und Enterprise-Plus-Pakete einzusetzen. Auch diese Pakete sind nachträglich beliebig in alle Richtungen zu ergänzen oder zu erweitern.

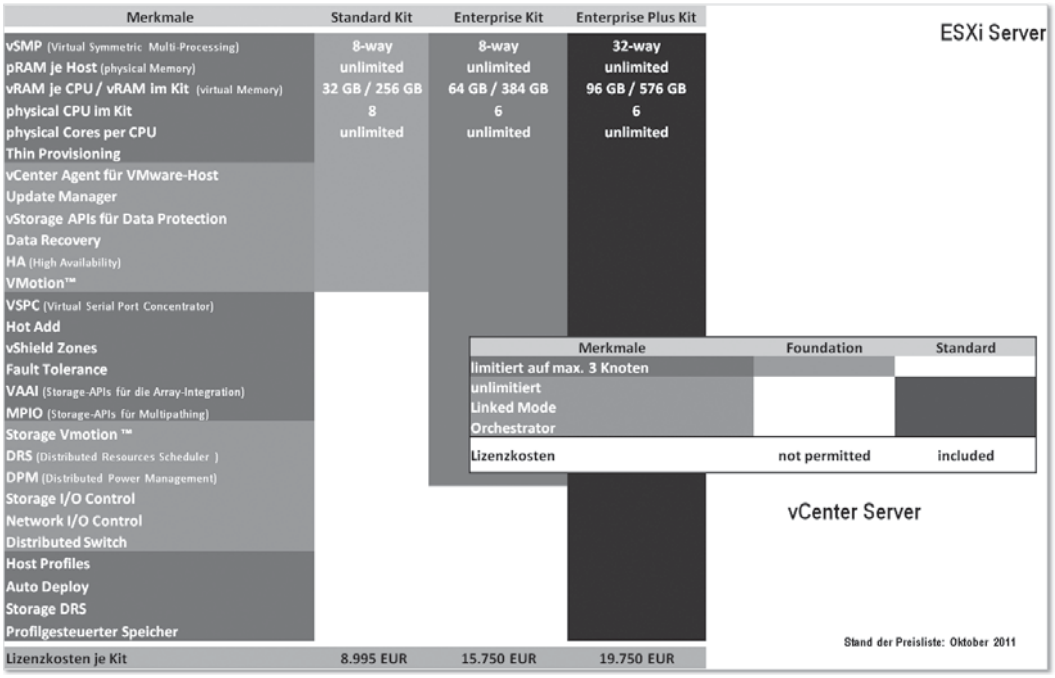


Abbildung 18.5 Die Leistungsmerkmale der Pakete innerhalb der Enterprise-Klasse

Entgegen den Small-Business-Paketen aus Abschnitt 18.1.3 wurde diesen Paketen eine vCenter-Server-Standard-Instanz beigelegt. Somit sind nicht nur Linked Mode und Orchestrator

enthalten, sondern es können so viele Hosts am vCenter-Server registriert werden, wie es das vCenter-Server-Maximum gestattet. In der aktuelle Version liegt das vCenter-Server-Maximum bei 1.000 Hosts je vCenter-Server (*http://www.vmware.com/pdf/vsphere5/r50/vsphere-50-configuration-maximums.pdf*).

Was den vRAM angeht, ist bei diesen Bundles einiges möglich. In Tabelle 18.1 finden Sie einige Werte und Merkmale im direkten Vergleich:

Version	vRAM-Pool	max. Wege	enthaltende Lizenz
Standard	256 GB	8	8
Enterprise	384 GB	8	6
Enterprise Plus	576 GB	32	6

Tabelle 18.1 vRAM: Werte und Merkmale im direkten Vergleich

18.1.6 Erweiterung einer Umgebung durch Hinzufügen von Funktionalität

Funktionserweiterungen sind auf jede der Versionen Standard, Enterprise und Enterprise Plus anwendbar. Bei der Version Enterprise Plus kann das Merkmal Distributed vSwitch um den Cisco Nexus 1000V erweitert werden. Die Versionen Standard, Enterprise lassen sich durch Upgrades in jede beliebige Version umwandeln, das heißt, Sie können durchaus auch Versionsstufen überspringen. So ändern Sie zum Beispiel eine Standard-Lizenz durch Upgrade direkt in eine Enterprise- oder Enterprise-Plus-Lizenz um.

18.1.7 SLES für vSphere-Lizenz-Besitzer

VMware und Novell sind schon seit längerer Zeit partnerschaftlich verbunden. Im Zuge dieser Partnerschaft wurde eine OEM-Version des SUSE Linux Enterprise Servers (SLES) für Kunden von VMware bereitgestellt. Damit Sie aber dieses kostenlose Betriebssystem in Ihren virtuellen Maschinen benutzen dürfen, sind einige Bedingungen zu erfüllen: Zum einen müssen Sie über einen gültigen Support-/Subscription-Vertrag mit VMware verfügen und zum anderen eine entsprechende vSphere 5-Edition besitzen. Ob Sie über eine berechtigte Editionen verfügen, können Sie unter *http://www.vmware.com/landing_pages/sles-for-vmware/eligible-products.html* nachprüfen. Wenn Sie berechtigt sind, den SUSE Linux Enterprise Server für VMware einzusetzen, dann können Sie ihn unter *http://download.novell.com/Download?buildid=gURHaoHcER0* herunterladen.

Damit Sie SLES dann auch lizenzieren können, müssen Sie noch einen Schlüssel, wie in Abbildung 18.6 nachzuvollziehen, registrieren, und zwar im VMware Portal für Complimentary Products unter der Adresse *https://www.vmware.com/partnerEval/secure/niagara/thirdParty-ProductHome.do*.

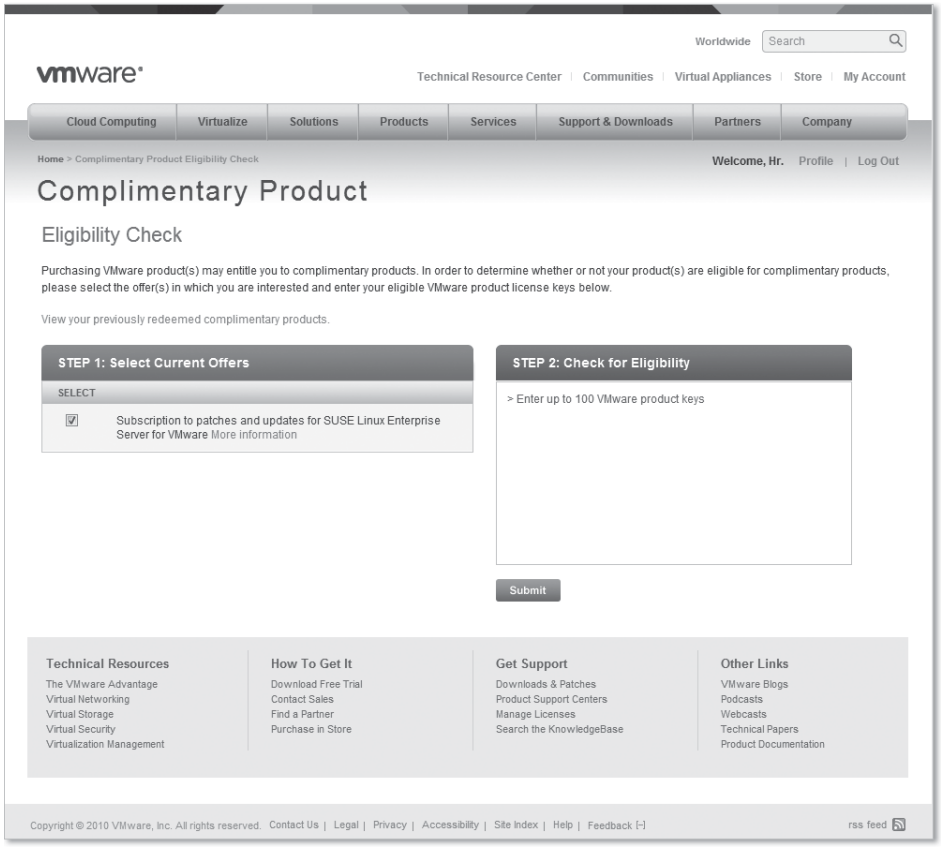


Abbildung 18.6 Im Portal für Complimentary Products kann der Schlüssel qualifiziert werden.

18.2 Support und Subscription

Generell ist es nicht möglich, im Umfeld der hier betrachteten Produkte Lizenzen bei VMware zu erwerben, ohne auch Support und Subscription – womit der Abonnement-Service gemeint ist – mitzukaufen. Allerdings müssen weder Support noch Subscription nach Ablauf der Laufzeit nachgekauft werden. In der Praxis ist es aber durchaus sinnvoll, Support und Subscription bei Ende des Support- und Subscription-Vertrages zu erneuern. Selbst wenn im Unternehmen Störungen ohne die Nutzung des VMware-Supports behoben werden, ist nicht immer gesagt, ob dies auch in Zukunft immer der Fall sein wird. Diese Frage muss aber jeder Administrator für sich selbst entscheiden. Bei der Subscription liegt die Sache etwas anders: Subscription bedeutet, dass Sie neue Versionen oder Updates bei Neuerscheinung herunterladen können und einsetzen bzw. benutzen dürfen.

VMware unterscheidet bei den Server-Produkten grundsätzlich zwischen zwei unterschiedlichen Arten von Support und Subscription, die Stufe *Basic* und die Stufe *Production*. Bei den

Laufzeiten für Support und Subscription können Sie zwischen einem, zwei und drei Jahren wählen. Falls Sie darüber hinaus größere Zeiträume für Support und Subscription wünschen, ist dies in der Regel auch möglich. Allerdings müssen Sie dies individuell anfragen. Für die Erreichbarkeit von VMware im Supportfall hier in Europa gilt für die Stufe Basic Montag bis Freitag in der Zeit von 7.00 Uhr bis 19.00 Uhr und für die Stufe Production 24 Stunden an sieben Tagen in der Woche und 365 Tagen im Jahr. Wenn Sie alle Einzelheiten zu Support und Subscription in Bezug auf die Stufen Basic und Production nachlesen möchten, empfehle ich das *basic.pdf (http://www.vmware.com/files/pdf/support/basic.pdf)* und das *production.pdf (http://www.vmware.com/files/pdf/support/production.pdf)*.

Eine sehr interessante Variante aus dem Bereich Support stellt der geschäftskritische Support von VMware dar. Dieser Support ist für alle gedacht, die Mission Critical Environments betreiben. Er ist als Ergänzung zum bereits erläuterten Production-Support zu sehen. Bei dieser Art des Supports wird eine enge Beziehung zwischen dem Hersteller und dem Kunden hergestellt. So stehen dedizierte Ansprechpartner und vieles mehr zur Verfügung. Auch hier verweise ich auf das entsprechende Datenblatt von VMware: *business_critical.pdf (http://www.vmware.com/files/pdf/support/business_critical.pdf)*

Eine ganz andere Art von Support – ohne enthaltene Subscription – steht mit dem Einzelfall-Support für ESXi und vSphere 5 Essential zur Verfügung. Der Einzelfall-Support ermöglicht es, VMware-Support auf Einzelfallbasis zu erwerben. Hier können Sie drei unterschiedliche Einzelfall-Supportpakete für einen, drei oder fünf einzelne Supportfälle (Incident-Packs) kaufen. Anfragen stellen Sie und Antworten erhalten Sie wahlweise über das Internet oder telefonisch. Eine Einzelfall-Supportanfrage ist in der Zeit von Montag bis Freitag von 7.00 Uhr bis 19.00 Uhr möglich. Detailliertere Informationen erhalten Sie im Dokument *perincident.pdf* (*http://www.vmware.com/files/pdf/support/perincident.pdf*) von VMware.

Sollte einmal Unklarheit darüber herrschen, ob ein vorhandenes VMware-Produkt noch unter Support ist, können Sie dies unter *http://www.vmware.com/de/support/support-resources/tools/* überprüfen (Abbildung 18.7).

Abbildung 18.7 Überprüfung von Supportberechtigungen

Eine weitere sehr gute Informationsquelle zum Thema Support stellt Ihnen VMware mit dem Dokument »Leitfaden für technischen Support von VMware« zur Verfügung. Sie finden es unter:

http://www.vmware.com/files/de/pdf/support/VMware-Technical-Support-Guide-GG-de.pdf

18.2.1 Die unterschiedlichen Schweregrade

VMware bietet die Möglichkeit, die Schweregrade der Supportanfrage zu klassifizieren. Grundsätzlich werden vier Schweregrade unterschieden. Im Wesentlichen werden diese Auswahlmöglichkeiten angeboten, um die relevanten Auswirkungen eines Problems auf die Systeme in einem Unternehmen zu erfassen. Die Einstufung eines Problems in den entsprechenden Schweregrad hat eine direkte Auswirkung auf die Reaktionsgeschwindigkeit des VMware-Support-Teams.

- *Schweregrad 1* liegt vor, wenn die Produktions-Server oder andere unternehmenskritische Systeme ausgefallen sind und eine Behelfslösung nicht unmittelbar zur Verfügung steht, wenn für wesentliche Teile der unternehmenskritischen Daten ein erhebliches Verlust- oder Beschädigungsrisiko besteht, die Services in unannehmbarem Umfang ausgefallen sind oder gar der Geschäftsbetrieb in erheblichem Umfang unterbrochen wurde.
- Um *Schweregrad 2* handelt es sich, wenn eine wichtige Funktion maßgeblich beeinträchtigt ist. In dieser Klassifikationsstufe kann der Betrieb mit Einschränkungen fortgesetzt werden, und eine vorübergehende Behelfslösung steht auch zur Verfügung.
- *Schweregrad 3* wird angegeben, wenn die Supportanfrage sich auf Situationen mit zum Teil unkritischem Funktionsverlust der Software bezieht. Es liegen Beeinträchtigungen bestimmter Komponenten vor, und der Anwender kann die Software weiterhin nutzen.
- Unter *Schweregrad 4* sind unkritische Probleme wie zum Beispiel ein Fehler in der Dokumentation oder Ähnliches zu verstehen. Dieser Schwierigkeitsgrad bezieht sich auf eher allgemeine Fragen, die keiner zeitnahen Reaktionen bedürfen.

18.2.2 Wie stellen Sie eine Supportanfrage bei VMware?

Eine Anfrage beim VMware-Support stellen Sie telefonisch oder über die Website von VMware. Bevor Sie eine Supportanfrage stellen, ist es ratsam, bereits einige Informationen zu notieren, die normalerweise vom VMware-Supportmitarbeiter grundsätzlich angefordert werden: der Name des Anfragenden, der Name der Firma und die Telefonnummer, unter der der Anfragende erreichbar ist. Falls Sie wegen einer früheren Supportanfrage anrufen, sollten Sie deren Referenznummer kennen. Natürlich ist eine kurze Beschreibung des Problems erforderlich. Im Anschluss teilt der VMware-Supportmitarbeiter Ihnen eine Referenznummer mit. Diese Referenznummer bleibt so lange erhalten, bis die Supportanfrage vollständig beantwortet oder das Problem behoben wurde.

Oftmals muss der Support weiterführende Informationen anfordern, um Probleme zu diagnostizieren und die Supportanfrage somit zügig bearbeiten zu können. Darum ist es unter Umständen extrem hilfreich, wenn die Umgebung gut dokumentiert ist. Diagramme und Dateien zur System-, Storage- und/oder Netzwerkkonfiguration sind für den Support bei der Problemerkennung und der damit verbundenen Problembehebung ausgesprochen hilfreich. Außerdem wird der Support nach Protokolldateien oder der Core-Datei (`vm-support`-Diagnosedatei) fragen.

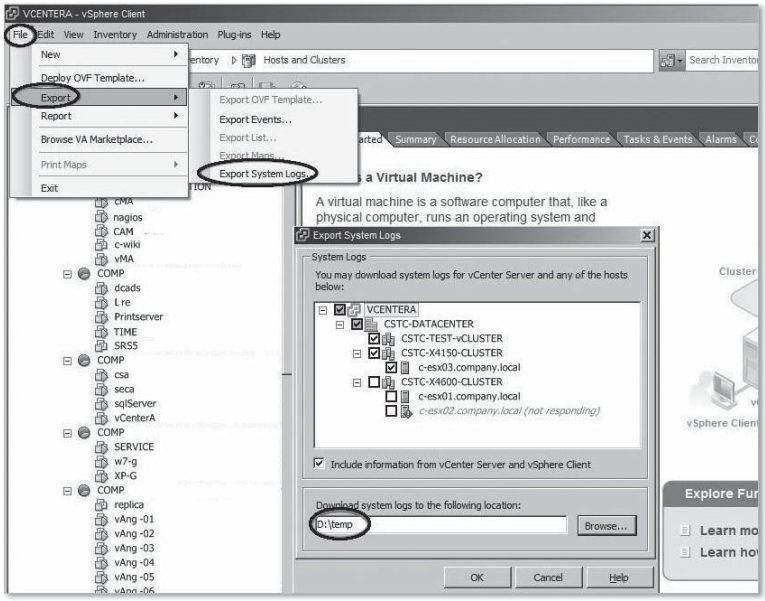


Abbildung 18.8 Erstellen der VMware-Supportinformationen

An dieser Stelle sollten Sie gut mit Ihrem System vertraut sein, um dem Support die geforderten Informationen geben zu können. Die Reaktionszeit des VMware-Supports ist je nach Supportstufe unterschiedlich, wie Tabelle 18.2 zeigt.

Klassifikation der Supportanfrage	Production-Reaktionszeit 24 × 7 – Telefon und Internet	Basic-Reaktionszeit 12 × 5 – Telefon und Internet	VMware-Support auf Einzelfallbasis Internet
Schwere 1	30 Minuten oder weniger	4 Stunden innerhalb der Hauptgeschäftszeit	4 Stunden (VMware EXSi) innerhalb der Hauptgeschäftszeit
Schwere 2	4 Stunden innerhalb der Hauptgeschäftszeit	8 Stunden innerhalb der Hauptgeschäftszeit	24 Stunden innerhalb der Hauptgeschäftszeit
Schwere 3	8 Stunden innerhalb der Hauptgeschäftszeit	12 Stunden innerhalb der Hauptgeschäftszeit	24 Stunden innerhalb der Hauptgeschäftszeit
Schwere 4	12 Stunden innerhalb der Hauptgeschäftszeit	12 Stunden innerhalb der Hauptgeschäftszeit	24 Stunden innerhalb der Hauptgeschäftszeit

Tabelle 18.2 Reaktionszeit des VMware-Supports

Telefonische Supportanfrage

Eine telefonische Eröffnung einer Supportanfrage stellen Sie in Deutschland unter *0800 1006711* oder *069 51709016*. Für andere Länder stehen ebenfalls derartige Support-Rufnummern zur Verfügung. Sie finden sie unter dem Link *http://www.vmware.com/de/support/phone_support.html*.

Der Telefonsupport wird in Deutschland ausschließlich innerhalb der Hauptgeschäftszeiten in Landessprache angeboten. Außerhalb der Hauptgeschäftszeiten erfolgt der Telefonsupport in englischer Sprache.

Die Hauptgeschäftszeit innerhalb von Europa beginnt montags bis freitags jeweils um 7.00 Uhr und endet um 19.00 Uhr Ortszeit. Auf der Internet-Site »Einreichen von Support-Anfragen« (*http://www.vmware.com/de/support/policies/file-sr/file-sr-phone.html*) können Sie weitere Informationen zum Thema »So stellen Sie eine telefonische Support-Anfrage« nachlesen.

Supportanfrage über die Website

Die andere Art, eine Supportanfrage zu stellen, ist die Anfrage über das Internet. Zu diesem Zweck hat VMware die Adresse *http://www.vmware.com/de/support* eingerichtet. Kontaktieren Sie den Support unter Support-Anfragen und Managementportale (Abbildung 18.9), indem Sie in der Auswahlbox Support Kontaktieren oder Supportanfrage einreichen auswählen und dann auf Go klicken.

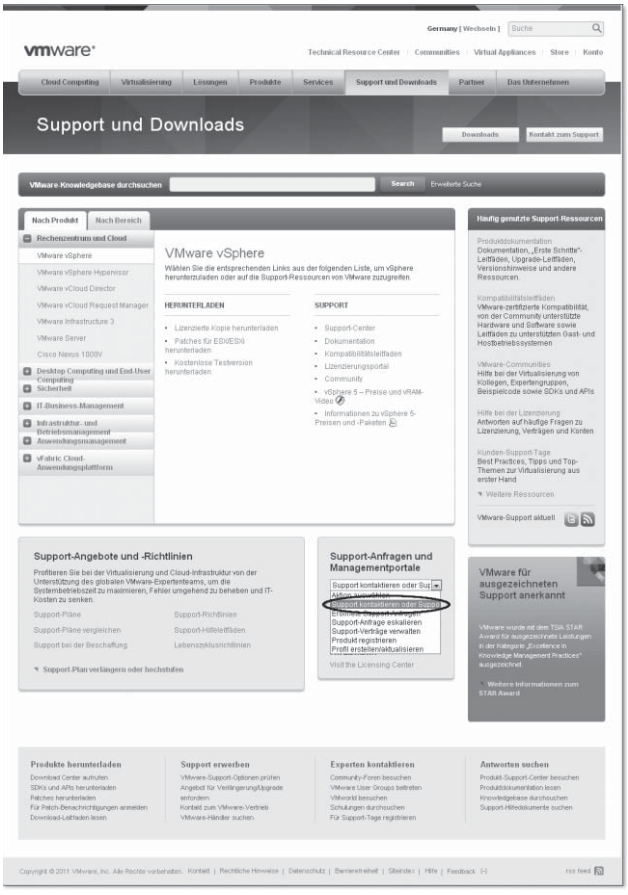


Abbildung 18.9 Der VMware-Internet-Support

Sie gelangen nun auf eine Site, auf der Sie unterschiedliche Möglichkeiten des weiteren Vorgehens angeboten bekommen. Ein Klick auf File a Technical Support Request führt zur Knowledge Base (Abbildung 18.11), und mit einem Klick auf View Support Requests gelangen Sie auf eine Seite, auf der Sie den aktuellen Status aller Ihrer Support-Requests abfragen können, wobei Sie Details zu den Supportverträgen unter Support Contract Details einsehen können.

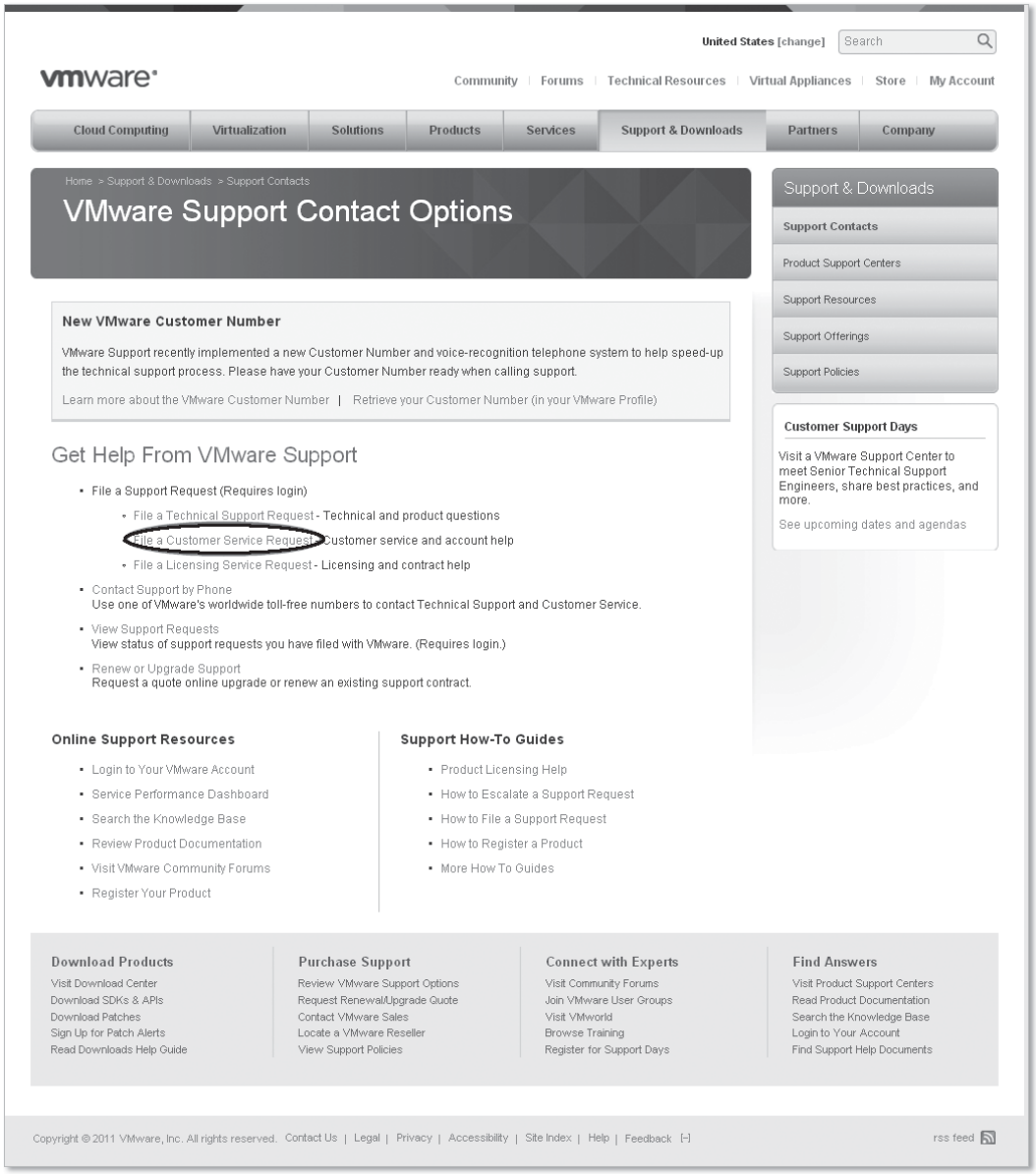


Abbildung 18.10 Auf dieser Seite entscheiden Sie sich für die Art des Supports, den Sie benötigen.

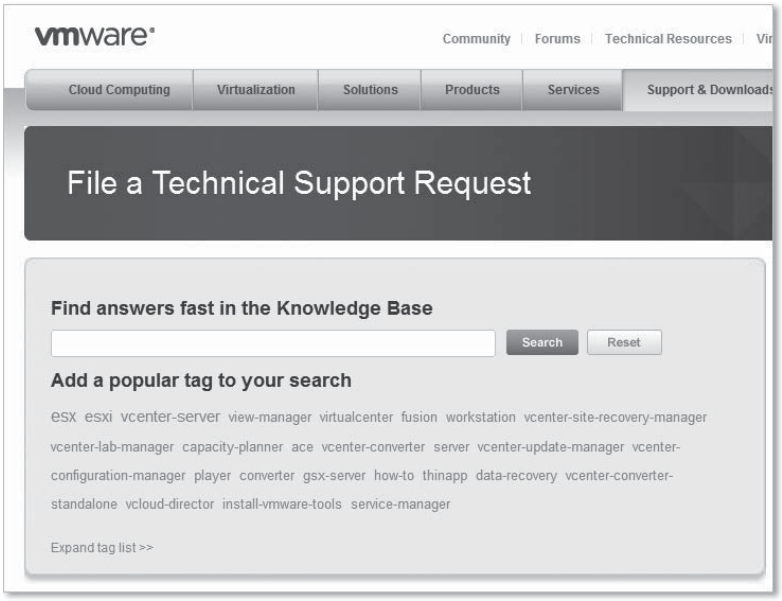


Abbildung 18.11 Suchen in der Knowledge Base

Über die Site *https://www.vmware.com/accounts/* erreichen Sie MANAGE SUPPORT CONTRACTS und sehen dort alle von Ihnen erworbenen Supports für sämtliche Produkte bzw. Lizenzen. Die Tabelle, die Sie nun angezeigt bekommen, können Sie mittels der Auswahlbox auf der rechten Seite zwischen den Status ACTIVE (noch unter Support) und EXPIRE (Support ist ausgelaufen) umschalten.

Wenn Sie eine Supportanfrage stellen möchten, klicken Sie auf FILE A CUSTOMER SERVICE REQUEST, und Sie gelangen auf eine Seite, an der Sie sich anmelden müssen. Loggen Sie sich mit Ihren Anmeldedaten ein, und füllen Sie das Formular unter CREATE A SUPPORT REQUEST (Abbildung 18.12) aus. Sollten Sie noch keine persönlichen Anmeldedaten besitzen, können Sie sich direkt unter *https://www.vmware.com/account/customerRegistration.do* bei VMware registrieren.

Abbildung 18.12 zeigt das Formular zur Supportanfrage. Nach dem Ausfüllen und Absenden dieses Formulars startet der Supportprozess, und je nach Art des Supports meldet sich ein Mitarbeiter des VMware-Support-Teams bei Ihnen.

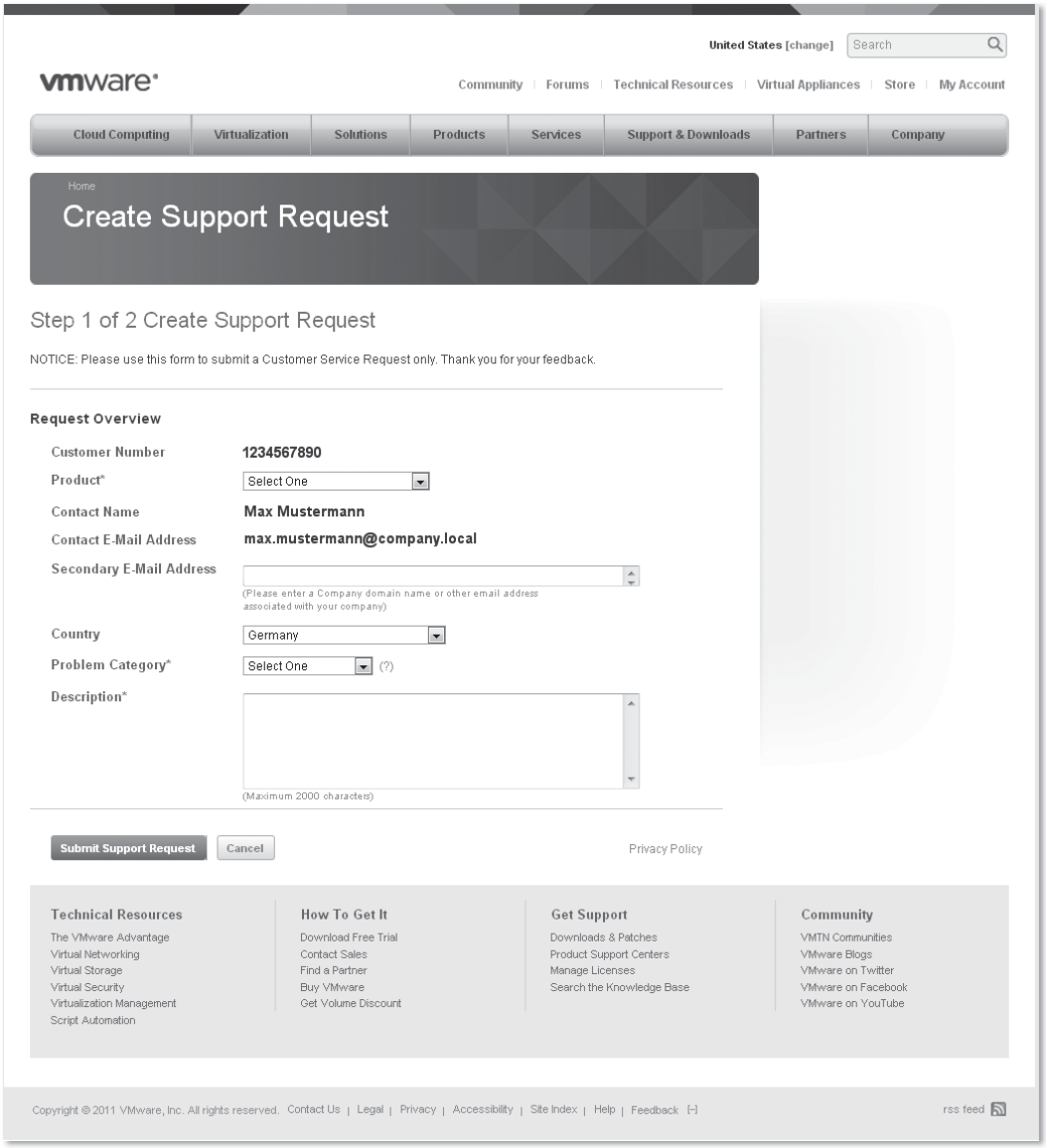


Abbildung 18.12 Eröffnung einer Supportanfrage über das Internet

Knowledge Base

Eine weitere wichtige Informationsquelle, die so manche Supportanfrage überflüssig macht, ist die bereits kurz erwähnte VMware Knowledge Base (Abbildung 18.11 und Abbildung 18.13), deren Adresse *http://www.vmware.com/go/sr* lautet.

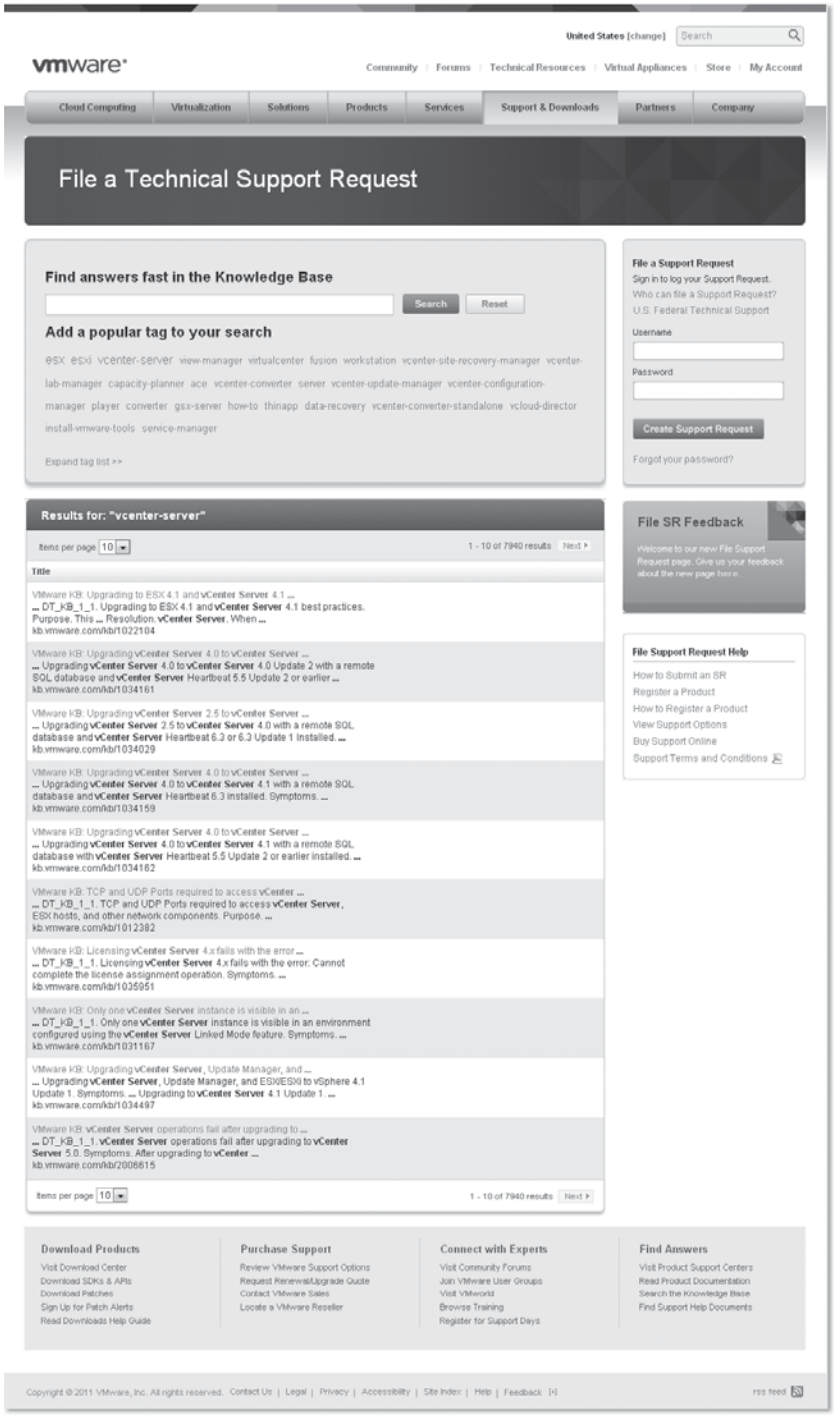


Abbildung 18.13 VMware Knowledge Base

Sie können die Dokumente, die in der Knowledge Base hinterlegt sind, durchsuchen und dadurch auf höchst effiziente Art und Weise an Informationen gelangen. Die Knowledge Base ist, wenn es nicht gerade um Support im Bereich von Schweregrad 1 oder 2 geht, eine durchaus geeignete Methode, sich selbst zu helfen.

Hinzu kommen weitere Selbsthilfe-Tools wie Dokumentation, technische Ressourcen (*http://www.vmware.com/de/support/pubs/*) oder Diskussionsforen (*http://communities.vmware.com/community/vmug/forums/emea/germany/germany_middle/*) und Anwendergruppen (*http://communities.vmware.com/community/vmtn/vmug/forums/emea/*). Ressourcen für Entwickler finden Sie unter *http://communities.vmware.com/community/vmtn/developer/*.

Das Schließen einer Supportanfrage

In der Regel wird eine Supportanfrage geschlossen, wenn der Anfragende bestätigt, dass eine Lösung erzielt wurde. Auch gilt eine Supportanfrage als geschlossen, wenn VMware nach drei Kontaktversuchen in einem Zeitraum von 10 Tagen keine Rückmeldung vom Anfragenden erhält. Es kommt natürlich auch vor, dass Supportanfragen aus bestimmten Gründen nicht gelöst werden können. In einem derartigen Fall wird die Supportanfrage dann ebenfalls geschlossen.

18.3 Die vSphere 5-Lizenzen

Die Version VMware vSphere läuft ohne Angabe einer Lizenz 60 Tage im Evaluierungsmodus (*https://www.vmware.com/try-vmware/*), mit vollem Funktionsumfang. Besitzen Sie bereits Lizenzen oder haben Sie Lizenzen bestellt, sind diese im VMware-Lizenzportal jederzeit abrufbar. Das Lizenzportal finden Sie unter der URL *http://www.vmware.com/support/licensing/*. Alternativ erreichen Sie das Portal über die VMware-Startseite unter Support und Downloads und dann Produktlizenzen verwalten. Nun werden Sie auf das VMware Licensing Help Center (Abbildung 18.14) verlinkt und können sich entscheiden, ob Sie vSphere 4- und vSphere 5-Lizenzen oder VI3-Lizenzen verwalten möchten.

Eine Verwaltung der Lizenzen von früheren Versionen verbirgt sich in der Rubrik Access by License Type hinter dem Link VI3 Licenses (Abbildung 18.14). Wenn Sie auf VI3 Licenses klicken, kommen Sie zu einer Abfrageseite, auf der Sie Ihre Zugangsdaten (Abbildung 18.15) eingeben. Anschließend werden Sie direkt in das Lizenzportal (Abbildung 18.24) weitergeleitet. Möchten Sie hingegen Ihre vSphere 5-Lizenzen sehen, wählen Sie an dieser Stelle den Link License Key aus. Ein weiterer Weg, in das Lizenz-Portal zu gelangen, führt über den Link *https://www.vmware.com/accounts/*. Geben Sie unter Login to VMware Accounts Ihre Anmeldedaten ein, und stellen Sie z. B. in der ersten Auswahlbox Manage Product Licenses ein. In der nächsten Auswahlbox wählen Sie dann die Art der Lizenzen, die Sie sehen wollen, aus. Wenn Sie nun auf Login klicken, werden Sie direkt in das Lizenzportal weitergeleitet (Abbildung 18.16).

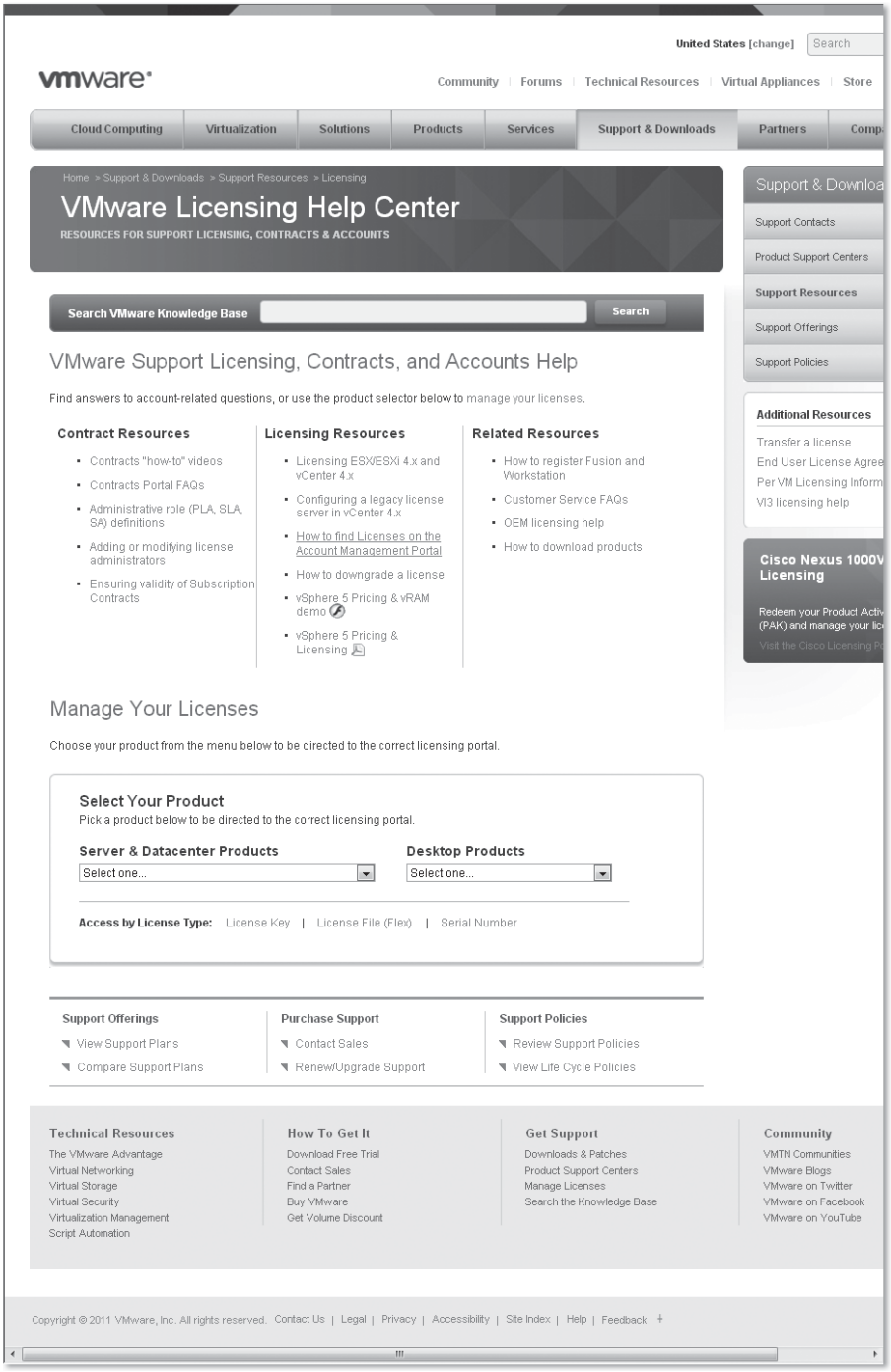


Abbildung 18.14 Die Lizenzen für vSphere 4 bzw. 5 und die Vorgängerversion VI3 sind getrennt anwählbar und in unterschiedlichen Portalen zu finden.

Der Umgang mit Lizenzschlüsseln

Nach der Auswahl der Produktgruppe, in unserem Fall LICENSE KEY (Abbildung 18.14), gelangen Sie auf die Anmeldeseite (Abbildung 18.15). Haben Sie die richtige Benutzerkennung mit Passwort eingegeben, werden Sie in Ihren Lizenzbereich weitergeleitet.

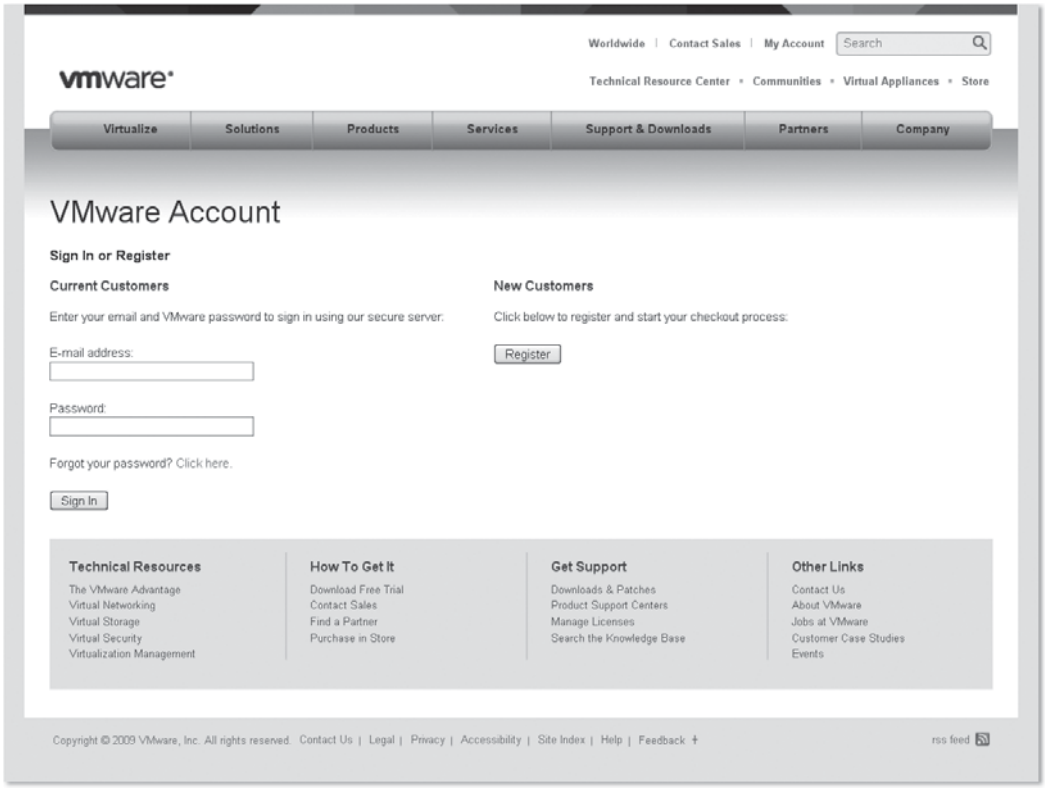


Abbildung 18.15 Anmeldeseite, die Ihnen den Zugang zu Ihrem Lizenzportal ermöglicht

Hier werden Ihnen nun Ihre Lizenzen angezeigt (Abbildung 18.16), die Sie eingepflegt haben. Sollte einer Ihrer Kollegen auch VMware-Lizenzen aktiviert haben, dann muss er diese explizit für Sie freischalten, damit Sie die Lizenzen ebenfalls sehen können.

Das Portal zeigt Ihnen nun in einer Übersicht, welche Lizenzen Sie in welcher Menge zur Verfügung haben und entsprechend nutzen können (Abbildung 18.16). Für jedes Produkt, das Sie besitzen, können Sie sich die Eigenschaften der Lizenzen anzeigen lassen, indem Sie auf das Pluszeichen vor der eingetragenen Lizenz klicken. Zu den Eigenschaften zählen die Ordernummer, das Bestelldatum und natürlich auch die bestellte Menge. Die Lizenznummer gehört ebenso dazu wie die Angabe, ob die Lizenz noch unter Support ist. Außerdem können Sie für Ihre Dokumentation hier auch einen Kommentar hinterlegen. Im Beispiel in Abbildung 18.17 wurde, wie Sie in der Umrahmung erkennen, ein Kommentar beigefügt. Haben Sie den Kommentar eingetragen, speichern Sie ihn mit SAVE.

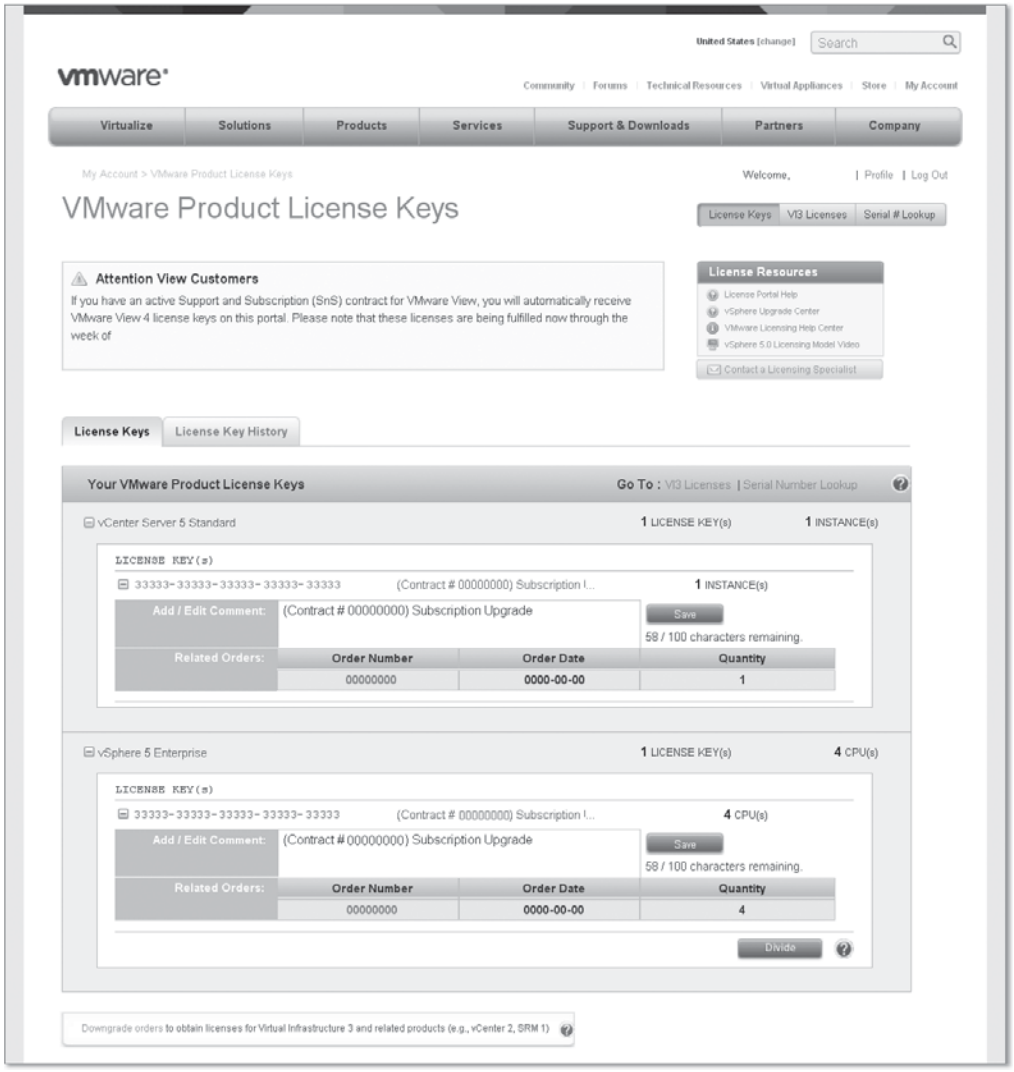


Abbildung 18.16 Hier können Sie die Eigenschaften Ihrer vSphere-Lizenzen einsehen und verwalten.

Abbildung 18.17 Ergänzende Informationen zur Lizenz hinzufügen

Bei der Anzahl der Lizenzen werden anfänglich Lizenzen für mehrere CPUs angezeigt. In unserem Beispiel steht im Portal ein Lizenzschlüssel für acht CPUs (Abbildung 18.18). Wenn Sie nun im vCenter diese Lizenz für einen Host einpflegen, der nur zwei CPUs besitzt, wäre eine derartige Vorgehensweise ineffizient.

Abbildung 18.18 Ungeteilter Lizenzschlüssel für acht CPU-Sockel

Damit der Host optimal lizenziert wird, können Sie im Portal zuvor einen neuen Lizenz-Key für eine Zwei-Prozessor-Maschine erstellen. Dazu teilen Sie die Lizenz über DIVIDE einfach in vier Zwei-Prozessor-Lizenzen (Abbildung 18.19 und Abbildung 18.20) oder eine Zwei-Prozessor- und eine Sechs-Prozessor-Lizenz auf.

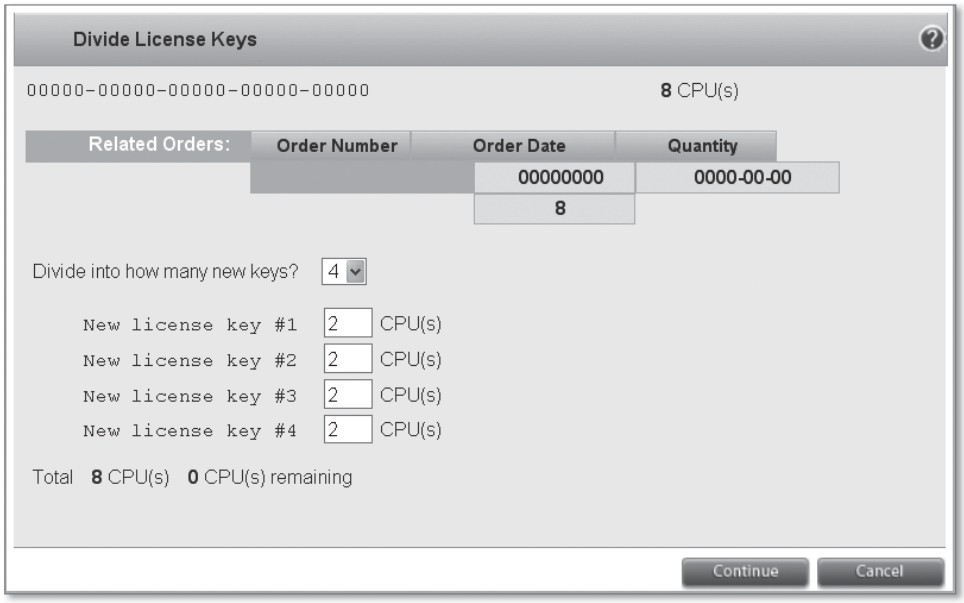


Abbildung 18.19 Aufsplittung einer Acht-Prozessor-Lizenz in vier Zwei-Prozessor-Lizenzen

Ersetzen Sie den Host mit den zwei Prozessoren nun durch einen mit z. B. vier Prozessoren, ist es notwendig, eine zur Hardwareausstattung des Hosts passende Lizenz zu erzeugen.

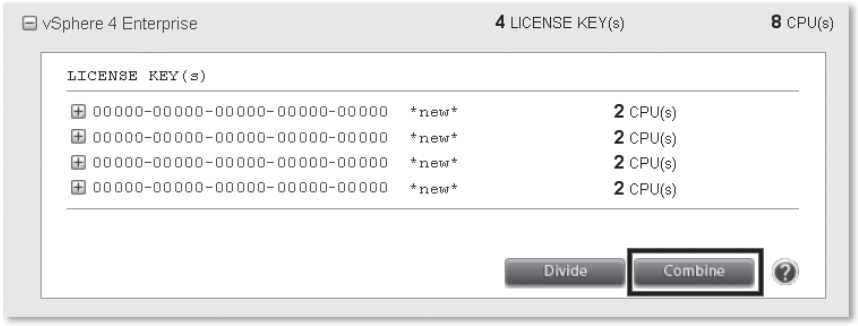


Abbildung 18.20 Vier Lizenzschlüssel für je zwei CPUs respektive Sockel nach der Aufsplittung

Sie benötigen also eine Vier-Prozessor-Lizenz. Dazu setzen Sie nun zwei Zwei-Prozessor-Lizenzen mittels der Funktion COMBINE zu einer Vier-Prozessor-Lizenz zusammen (Abbildung 18.21).

Abbildung 18.21 Zusammenführung von zwei Zwei-Prozessor-Lizenzen zu einer Vier-Prozessor-Lizenz

Hierbei legen Sie durch Anklicken der entsprechenden Checkbox die zu migrierenden Zwei-Prozessor-Lizenzen fest (Abbildung 18.21). Im Anschluss daran sind im Portal nur noch drei Lizenzschlüssel zu sehen: eine Vier-Prozessor-Lizenz und zwei Zwei-Prozessor-Lizenzen, also zusammen acht Prozessorlizenzen. Den erzeugten Vier-Prozessor-Lizenz-Key tragen Sie einfach in den vCenter-Server ein, und schon können Sie den Host oder das vCenter selbst lizenztechnisch aktivieren.

Die Historie der Lizenz-Keys

Selbstverständlich bietet VMware auch eine Historie der Lizenz-Keys an. Des Weiteren können Sie den Orderstatus aufrufen, Lizenzen downgraden oder ein Upgrade bestellen. Das gesamte Handling für die Lizenzen geschieht sehr anwenderfreundlich und transparent in diesem Portal.

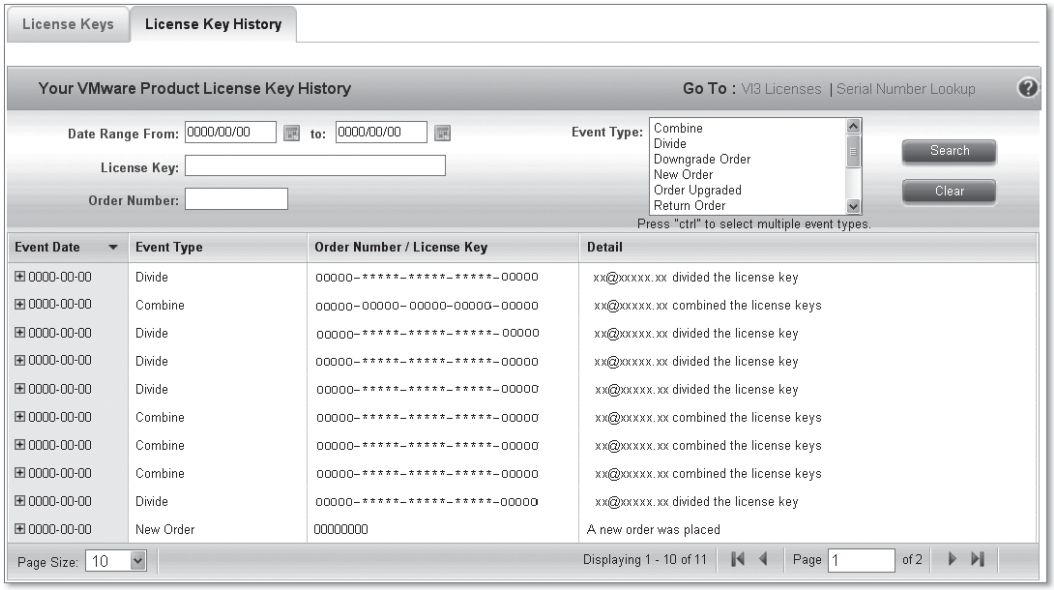


Abbildung 18.22 Die Historie der Lizenzschlüssel und des Orderstatus

18.4 Die VI3-Lizenzierung

Wenn Sie weiterhin ESX 3.x-Host-Systeme mit vCenter 5 verwalten möchten, kommen Sie an der Nutzung des »alten Lizenz-Servers« und der Anpassung des vCenters 5 zu dessen Nutzung nicht vorbei. Daher erläutern wir im Folgenden die Informationen zur VI3-Lizenzierung.

Abbildung 18.23 Umschaltung auf VI3-Lizenzierung

Lizenzdateien ansehen, anlegen, verändern und abrufen

Nach der Anmeldung mit dem Portal-Account, dem die Lizenzen zugeordnet sind, erscheint die Ansicht über alle verfügbaren und bereits aktivierten Lizenzen. Die VMware-Lizenzen sind modular in Komponenten aufgeteilt (Abbildung 18.24).

Im Falle eines Verlustes einer Lizenzdatei können Sie jederzeit im VMware-Lizenzportal eine neue erstellen (Abbildung 18.25) und sich diese entweder per E-Mail zusenden lassen oder direkt herunterladen.

Dies gilt natürlich auch für den Fall, dass die vorhandenen Lizenzdateien nicht korrekt angelegt sind oder aus dem einen oder anderen Grund verändert werden müssen.

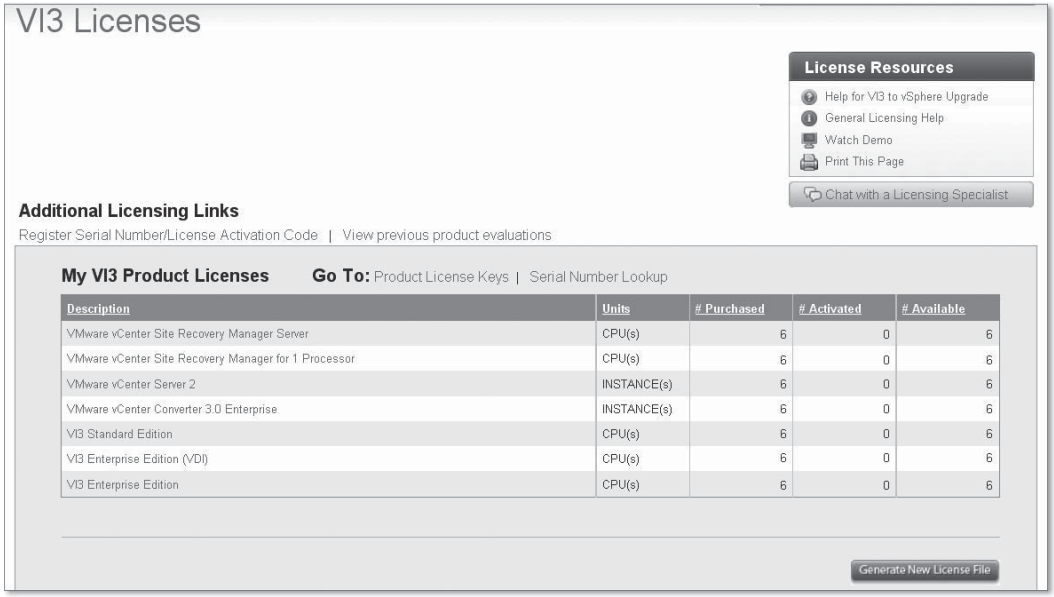


Abbildung 18.24 Übersicht über die verfügbaren und aktiven VI3-Lizenzen

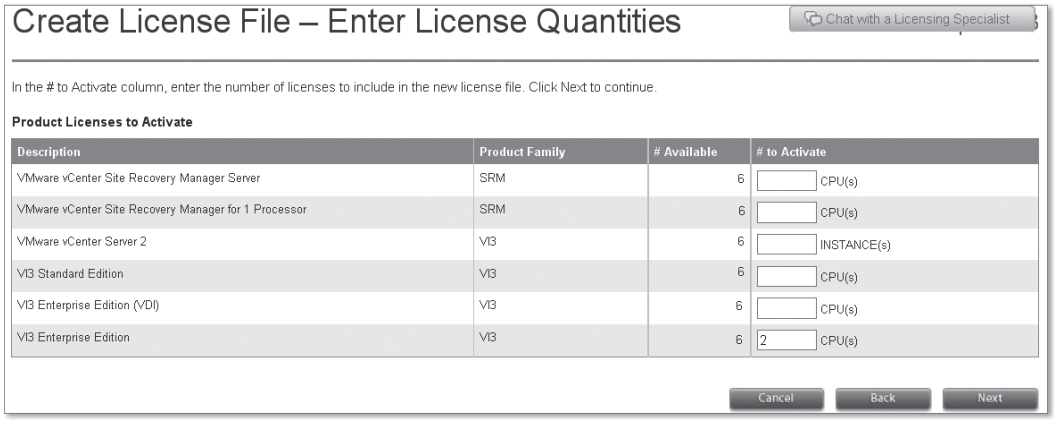


Abbildung 18.25 Erstellung einer Lizenz

Es kann natürlich auch vorkommen, dass die Art der Lizenzdatei verändert werden muss. Nach einem Klick auf GENERATE NEW LICENSE FILE zur Neuerstellung einer Lizenz wird nach dem Lizenzmodell gefragt (Abbildung 18.26). Es gibt grundsätzlich zwei Arten von Lizenzdateien im Lizenzmodell von VI3: die server- und die host-based Lizenzierung. Bei der server-based Lizenzierung wird die Umgebung unter Einbeziehung des VMware-Lizenz-Servers lizenziert. Bei der host-based Methode lizenzieren Sie einen oder mehrere Hosts direkt ohne Nutzung des Lizenz-Servers. Hierbei wird die Lizenzdatei direkt an den Host gebunden bzw. importiert.

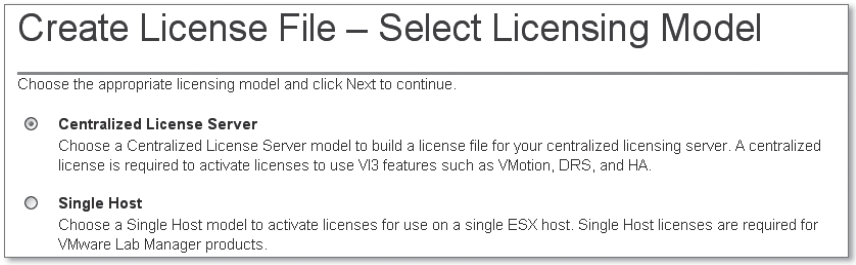


Abbildung 18.26 Das VI3-Lizenzmodell

Wie Sie in Abbildung 18.27 erkennen, gibt es drei unterschiedliche Spalten. Unterschieden wird nach insgesamt gekauften (❶), bereits aktivierten (❷) und noch verfügbaren (❸) Lizenzen. Die letztgenannte Spalte zeigt an, in welcher Menge Lizenzen noch zur Benutzung zur Verfügung stehen oder nicht in Benutzung sind. Aktivieren Sie verfügbare Lizenzen, werden diese unter ❸ abgezogen und dann unter ❷ gutgeschrieben.

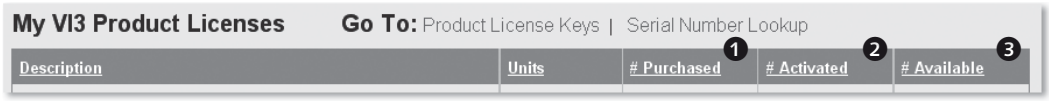


Abbildung 18.27 Es sind keine aktiven Lizenzen verfügbar.

Benötigen Sie eine Lizenzdatei nicht mehr, können Sie sie unter My License Files mittels Delete löschen (Abbildung 18.28). Das bedeutet aber nicht, dass sie tatsächlich gelöscht wird. Vielmehr wird sie lediglich innerhalb der Portalverwaltung verschoben. Das Delete bewirkt eine Verschiebung von Activated nach Available.

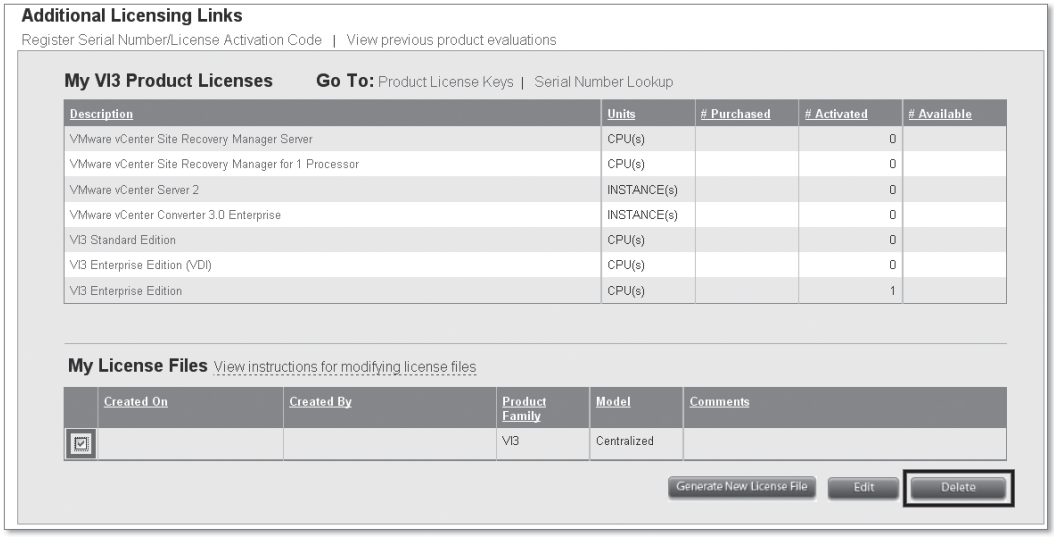


Abbildung 18.28 Löschen einer bereits erzeugten Lizenzdatei

Im Anschluss daran können Sie diese Lizenz wieder zur Generierung einer neuen Lizenzdatei benutzen.

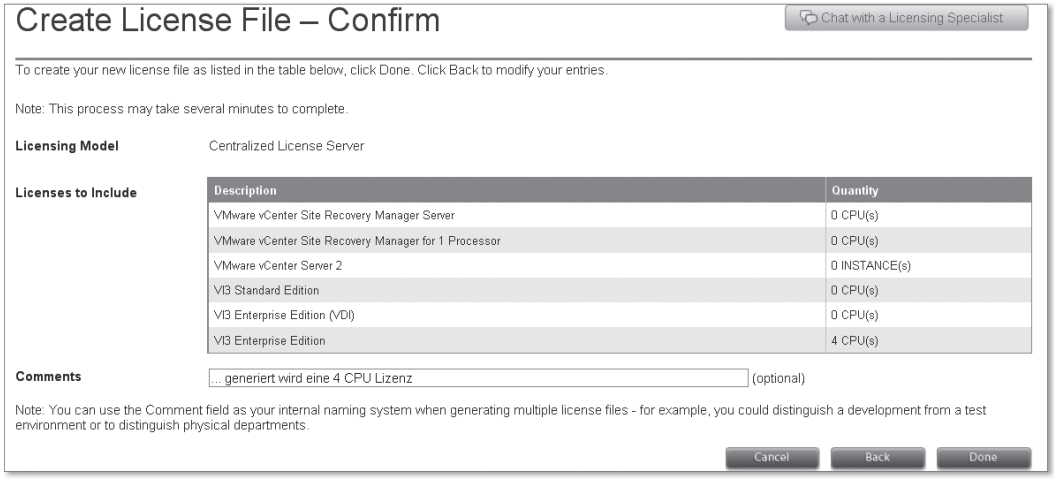


Abbildung 18.29 Erstellung einer neuen Lizenzdatei inklusive Kommentar

Nach optionaler Angabe eines Kommentars (Abbildung 18.29) können Sie eine Lizenzdatei herunterladen oder per E-Mail weiterleiten (Abbildung 18.30). Letzteres ist natürlich für Berater interessant, die so im Auftrag des Kunden vor der Installation bereits alles vorbereiten können.

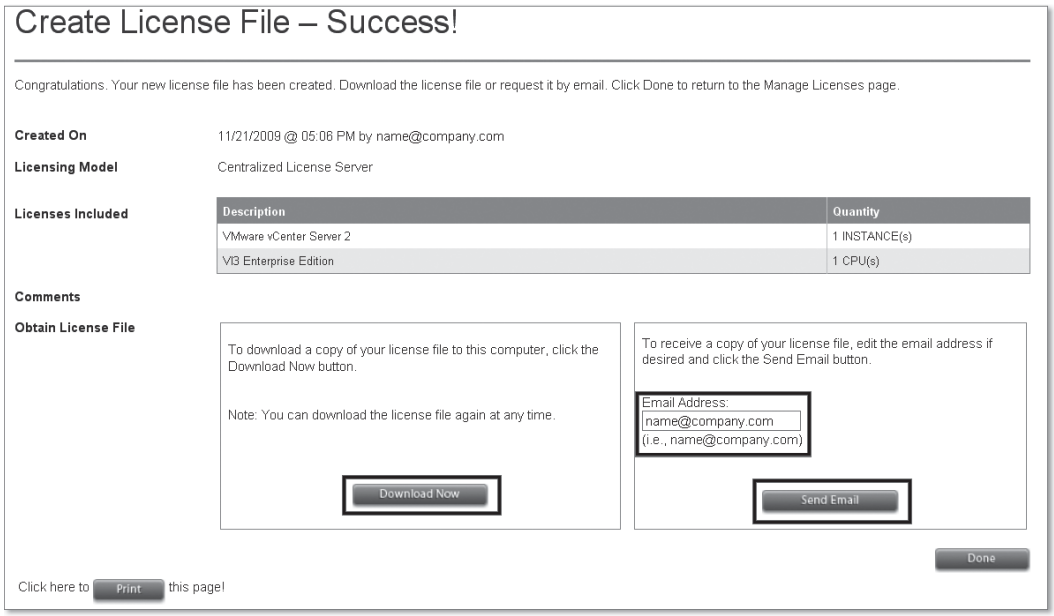


Abbildung 18.30 Versenden oder Herunterladen der Lizenzdatei

Leider existiert keine Möglichkeit, innerhalb des Lizenzportals ein Benutzerkonto für mehrere Personen freizugeben.

Lizenzdateien – Lizenz-Server

Eine Lizenzdatei hat immer einen bestimmten Aufbau, und Sie können mehrere Lizenzdateien miteinander kombinieren. Die Kombination der Lizenzen erfolgt entweder über das Portal oder auch manuell.

Aufbau der Lizenzdatei

```
SERVER this_host ANY 27000
VENDOR VMWARELM port=27010
USE_SERVER
INCREMENT PROD_VC VMWARELM 2005.05 permanent 1 \
   VENDOR_STRING=licenseType=Server ISSUED=19-Dec-2006 \
   NOTICE=FulfillmentId=214114 SIGN=" "
```

Die ersten drei Zeilen einer Lizenzdatei dienen der Zuordnung durch den Lizenz-Server. Erst danach folgen die eigentlichen Lizenzschlüssel, mit denen die Funktionen freigeschaltet werden können. Möchten Sie mehrere Lizenzdateien kombinieren, müssen diese ersten Zeilen am Anfang der Datei lediglich ein einziges Mal vorkommen. Alle weiteren mit `INCREMENT` beginnenden Teile dürfen Sie aus mehreren Dateien zusammenkopieren.

Sehen Sie sich die Zeile beginnend mit dem Wort `INCREMENT` näher an, können Sie das Produkt (`PROD_VC`; vCenter Server), die Gültigkeit (`permanent`), das Erstellungsdatum (`19-Dec-2006`) und den Lizenztyp (`licenseType=Server`) server-based auslesen. Die Zeile `VENDOR_STRING` kann die unterschiedlichsten Zusatzinformationen enthalten oder aus einer Lizenz eine bestimmte Funktion entfernen. Außerdem ist die Zahl hinter der Gültigkeit (`permanent`) sehr wichtig, da sie die Anzahl der Lizenzen dieses Typs beschreibt. Im vorliegenden Fall handelt es sich um eine Lizenz. Werden beispielsweise 20 ESX-Server-Sockel lizenziert, fänden Sie hier die Zahl `20` anstelle der `1`.

Folgende Produktlizenztypen werden derzeit verwendet:

Produktlizenz	String
Virtual Center Server	`PROD_VC`
ESX Server Starter	`PROD_ESX_STARTER`
ESX Server Standard	`PROD_ESX_FULL`
VMware Consolidated Backup	`ESX_FULL_BACKUP`
Virtual Center Agent VMware ESX	`VC_ESXHOST`
VMware vMotion	`VC_VMOTION`

Tabelle 18.3 Lizenztypen

Produktlizenz	String
VMware High Availability	VC_DAS
VMware DRS	VC_DRS

Tabelle 18.3 Lizenztypen (Forts.)

Alle Lizenzdateien werden im Programmverzeichnis des VMware Lizenz-Servers (*%programfiles%\VMware\VMwareLicense Server\Licenses*) abgelegt. Es ist ohne weiteres möglich, mehrere Dateien im gleichen Verzeichnis zu speichern. Der Lizenz-Server-Dienst liest diese entsprechend nacheinander aus.

Anhang

A **Automatisierung, Billing, Performance, vCenter Site Recovery Manager** 1077

B **VMware-vShield-Zones-Produktfamilie** 1099

C **Your Cloud** 1129

D **vCenter Operations** 1143

E **Die Virtualisierung des Desktops** 1147

In diesem Kapitel erfahren Sie, welche zusätzlichen Softwareprodukte VMware anbietet, um Ihnen als Administrator die Arbeit mit der virtuellen Infrastruktur zu erleichtern. Dabei geht es nicht nur um Server-, sondern auch um Desktop-Virtualisierung.

A Automatisierung, Billing, Performance, vCenter Site Recovery Manager

Autor dieses Kapitels ist Bertram Wöhrmann, Ligarion, bwoehrmann@ligarion.de

Durch das Studium der Anhänge A bis E erhalten Sie einen Überblick über die Softwarefamilie von VMware. Wir zeigen Ihnen, welchen Mehrwert die Produkte für Sie haben können. Eine Beschreibung der Installation und Konfiguration der einzelnen Softwarepakete ist nicht Bestandteil der Kapitel.

A.1 Automatisierung

In diesem Abschnitt finden Sie alle Add-ons der vCenter-Produktfamilie, die Sie bei der Automatisierung der Server-Landschaft unterstützen.

A.1.1 VMware vCenter Lab Manager

Hinweis

Die aktuelle Version des VMware vCenter Lab Managers unterstützt weder die Version 5.x des vCenter Servers noch die Host-Version vSphere 5.x (Stand Dezember 2011).

Mit dem VMware vCenter Lab Manager stellen Sie einem End-User Test- und Entwicklungssysteme in einer virtuellen Umgebung zur Verfügung. Durch diesen Self-Service-Ansatz entlastet der vCenter Lab Manager die Administratoren der virtuellen Infrastruktur. So richten Sie den Applikationsentwicklern eine virtuelle Entwicklungsumgebung für ihre Arbeiten ein. Zu diesem Zweck stellt der Administrator den Nutzern im Vorfeld eine Auswahl von virtuellen Maschinen als Templates zur Verfügung. Aus diesem Portfolio können sich die Nutzer dann ihre Testumgebung erstellen und anschließend ihre Applikation darauf installieren und weiterentwickeln. Die Entwickler haben es dabei selbst in der Hand, die Personen auf dem System zu berechtigen, die ihre Arbeit unterstützen sollen.

Der Zugriff auf den vCenter Lab Manager erfolgt dabei komplett über den Browser, so dass kein Endanwender einen weiteren Client installieren muss.

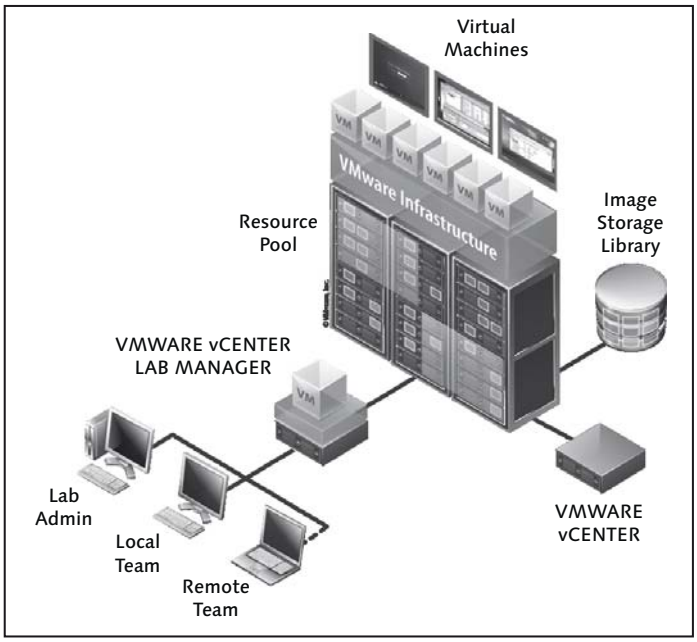


Abbildung A.1 Funktionsübersicht des Lab Managers

Die VM-Templates sind selbstverständlich jederzeit erweiterbar, so dass Sie den Anwendern auch neue oder aktuellere Systeme zur Verfügung stellen können. Der Vorteil liegt auf der Hand: Die Systeme kommen fertig »out of the Box«, und es ist keine weitere Konfigurationsarbeit seitens des Administrators mehr notwendig. Der Anwender selbst ist für seine Umgebung komplett eigenverantwortlich. Er baut aus den bestehenden Templates sein System oder seine Systemkette selbst auf.

Der Anforderer der VM wählt im Portal eine geeignete VM (❶). Anschließend sucht der vCenter Lab Manager, in Zusammenarbeit mit dem vCenter, den geeigneten Host aus (❷) und stellt den virtuellen Server zur Verfügung. Nach der Fertigstellung kann sich der Anwender direkt per Browser auf die Konsole des Systems verbinden (❸).

Sie können aber nicht nur neue Umgebungen aufbauen, sondern auch Duplikate von produktiven Systemen. Eine mögliche Anwendung wäre, die Verteilung von Patches zu testen, bevor Sie sie in der eigentlichen produktiven Landschaft ausrollen. In diesen Duplikaten können Sie selbstverständlich auch eine Fehlerbehebung verproben, wenn es Schwierigkeiten mit einem Server oder einer Applikationskette gibt. Alternativ nutzen Sie die Duplikate, um den Upgradepfad der Applikation zu erarbeiten. Verwenden Sie die Umgebung, um detaillierte Skalierungstests durchzuführen oder um die Lastverteilung über mehrere Applikations-Server zu testen.

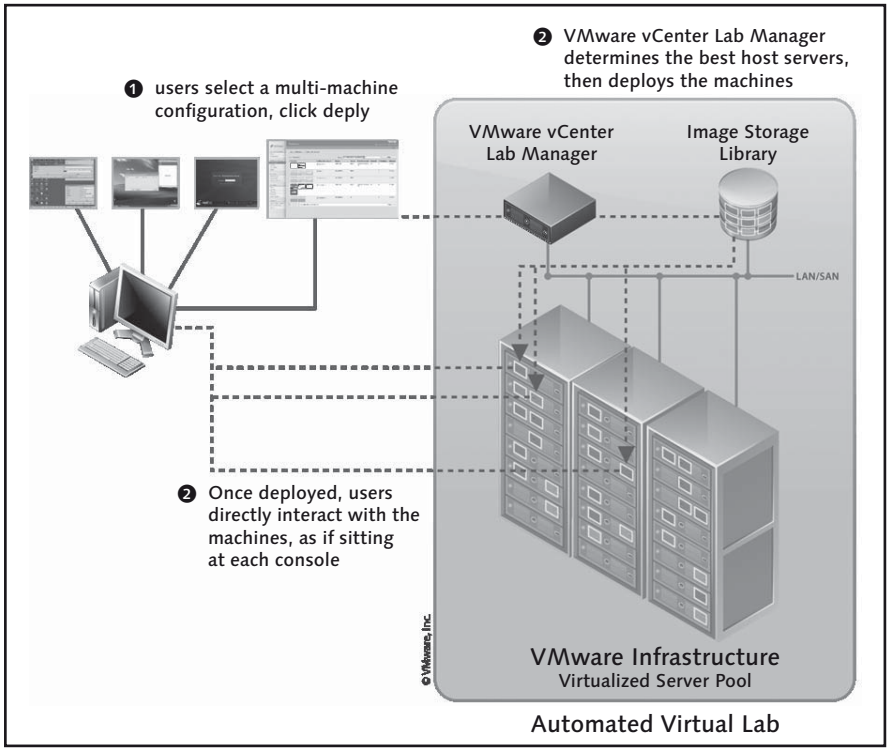


Abbildung A.2 Funktionsweise des Lab Managers

Durch den gezielten Einsatz von Resource-Pools lassen sich vCenter-Lab-Manager-Umgebungen vom produktiven Rechenzentrum abschotten. Sie machen sich so nicht gegenseitig die Ressourcen streitig. Selbstverständlich ist der vCenter Lab Manager skalierbar, so dass Sie im Bedarfsfall die unterliegende Umgebung erweitern können. Der vCenter Lab Manager wird auf einer bestehenden vSphere-Landschaft mit einem installierten vCenter-Server aufgesetzt. Das vCenter muss in der Version 4.x zur Verfügung stehen, als Host können Sie sowohl Systeme der Version 3.5 als auch Hosts der Version 4.x nutzen. Sowohl ESX- als auch ESXi-Plattformen werden unterstützt.

Nach der Installation bauen Sie nun einmalig eine Bibliothek von virtuellen Maschinen auf. Diese Maschinen erhalten ein Betriebssystem mit allen Tools, die installiert werden müssen, um einen reibungslosen und sicherer Betrieb zu ermöglichen. Über den fertig konfigurierten vCenter Lab Manager wird ein Webportal zur Verfügung gestellt, über das sich der potentielle Nutzer anmelden kann (Abbildung A.3).

Hier sieht er alle zur Verfügung stehenden Basis-Images und kann sich daraus »bedienen«, um sich einen Server oder eine Landschaft von Servern aufzubauen. Mit diesem Werkzeug kann er auch seinen Entwickler- oder Testkollegen Zugriffsrechte erteilen.

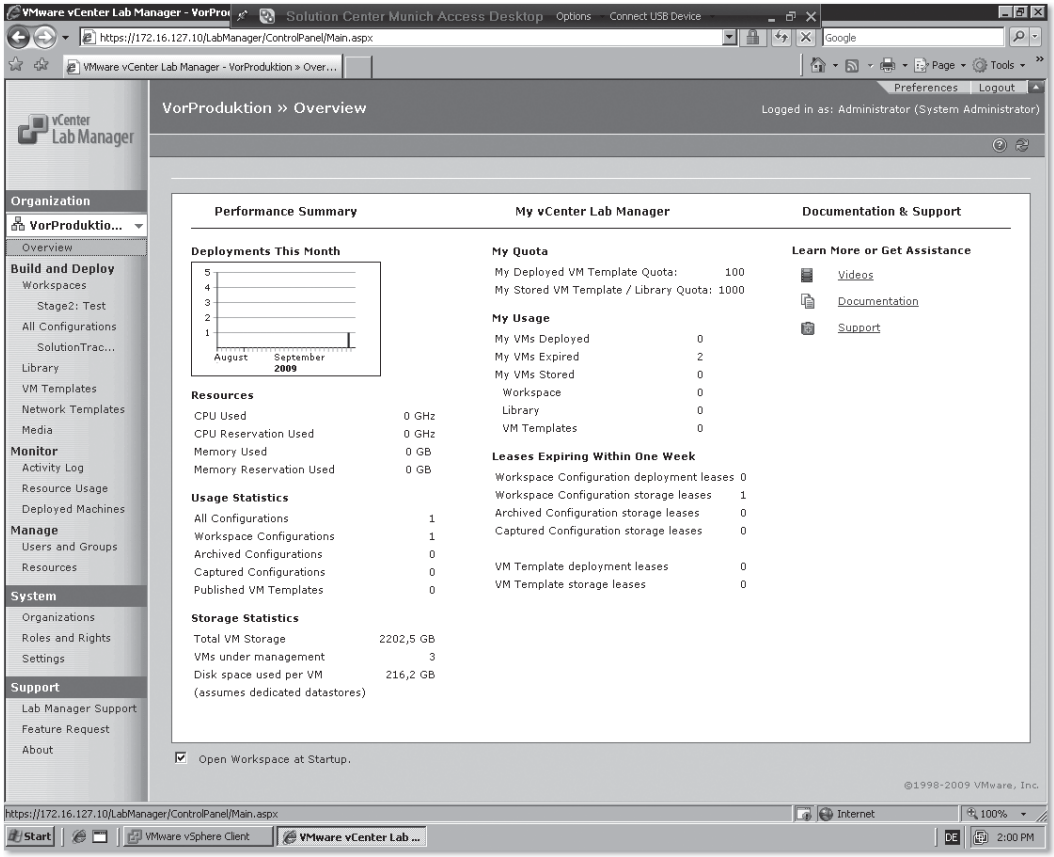


Abbildung A.3 Übersicht der Lab-Manager-Umgebung

Der vCenter Lab Manager bringt im Bereich Netzwerk besondere Fähigkeiten mit: Mit der Funktion *Network Fencing* erstellen Sie ein komplett isoliertes Netzwerk und hosten dort die Kopie einer produktiven Server-Landschaft. Selbstverständlich können Sie die virtuellen Server auch über mehrere Hosts verteilen. Somit vermeiden Sie z. B. einen IP-Adressen-Konflikt.

Eine weitere Funktion ist das Anlegen von Archiven. Eine einmal erstellte Testumgebung lässt sich archivieren und jederzeit wieder reaktivieren, um mit ihr weiterzuarbeiten. Das kann auch mehrfach und parallel geschehen, so dass sich der vCenter Lab Manager sehr gut für das Bereitstellen von Trainingsräumen eignet.

Zur weiteren Unterteilung richten Sie einfach mehrere Organisationen ein und konfigurieren so die gesamte Landschaft sehr granular. So machen Sie für die Anwender nur das sichtbar, was sie sehen sollen. Dabei hilft auch das ausgefeilte Berechtigungssystem, das über 50 verschiedene Berechtigungen kennt. Dieses Werkzeug entlastet Administratoren und überlässt dem eigentlichen Nutzer einen großen Teil der administrativen Aufgaben. Gerade in Entwicklungs- und Testumgebungen ist das auch sehr sinnvoll. Der Nutzer hat in Eigenverantwortung

zu entscheiden, wer wie wo berechtigt wird. Vorteile bietet auch hier die Funktion, mit Linked Clones zu arbeiten. Bei Linked Clones referenzieren sich die virtuellen Maschinen auf ein Masterabbild. Dies bietet eine Platzersparnis auf dem Storage und eine extrem schnelle Bereitstellung von neuen Maschinen.

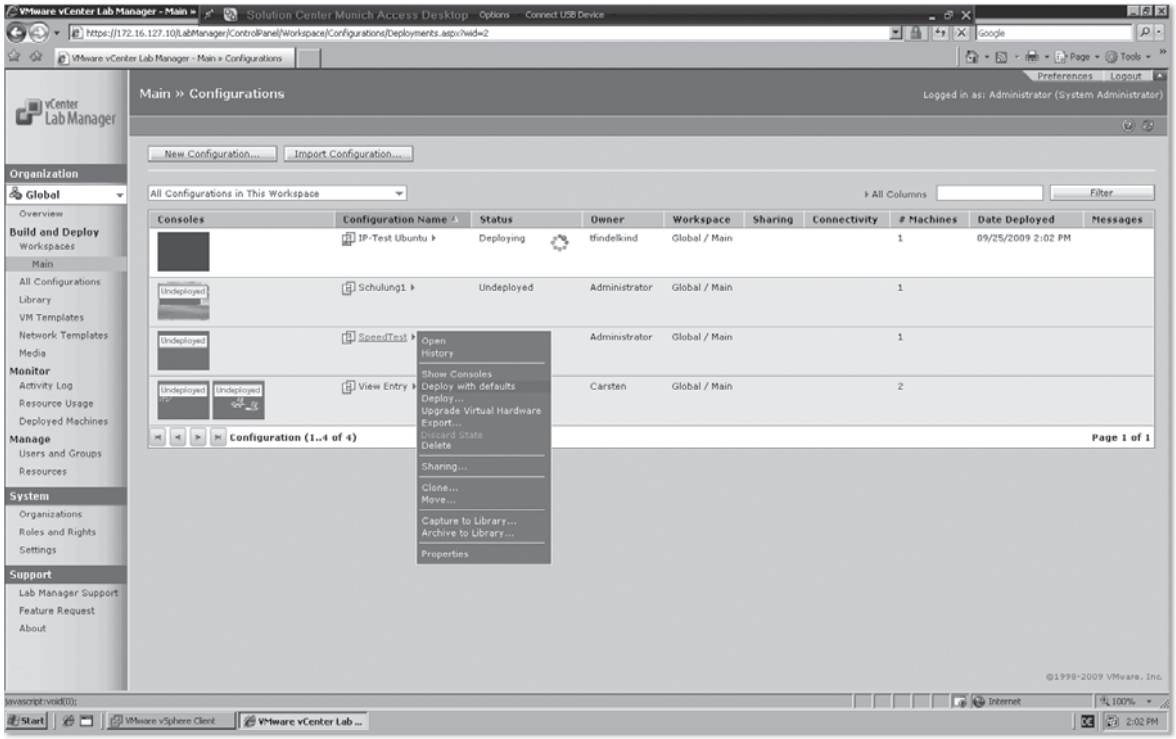


Abbildung A.4 vCenter-Lab-Manager-Konfigurationen

Seit der Version 4.0.1 des VMware Lab Managers sind die Funktionen des Lab Managers und des ehemaligen vCenter Stage Managers zusammengewachsen. Ein Video, das eine Übersicht über die Funktionen gibt, finden Sie unter: *http://www.youtube.com/user/VMwareDE*

A.1.2 VMware vCenter Orchestrator

Für die Erstellung von Workflows für Ihre täglichen Arbeiten können Sie den vCenter Orchestrator einsetzen. Es handelt sich um eine Erweiterung des vCenter Servers und ist auch Bestandteil von ihm.

Das System bringt eine Reihe von vorgefertigten Workflows mit, die Standardarbeiten abbilden und dem Nutzer zeigen sollen, wie man sich in der ganzen Thematik zurechtfindet. Die Aufgaben lassen sich in einem Designer anschauen und erstellen, damit Sie sich anhand der Beispiele mit der Funktionsweise der Anwendung vertraut machen können.

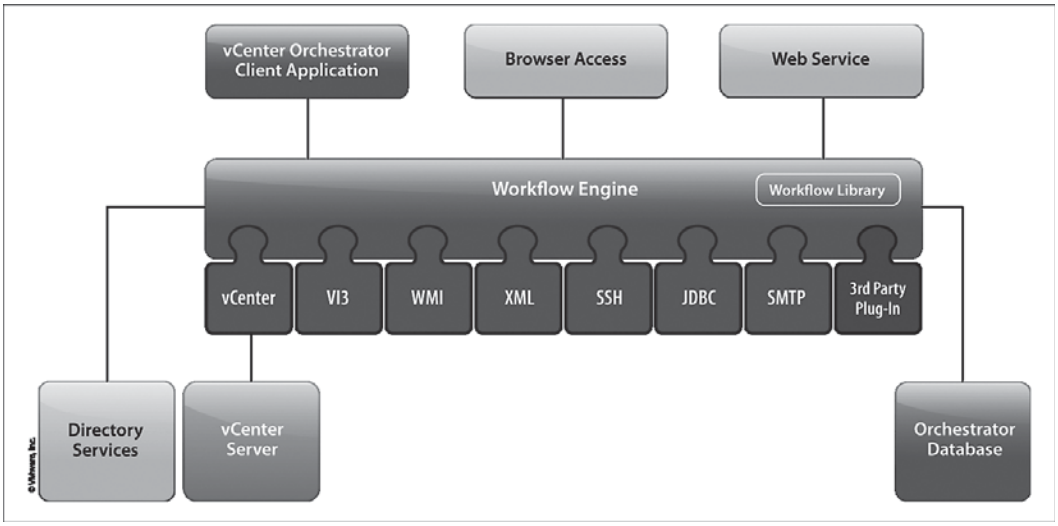


Abbildung A.5 Struktureller Aufbau des Orchestrators

Sie kombinieren verschiedene Aktionen, die sich auch in der Oberfläche durchführen lassen, miteinander und bauen sich somit einen Funktionsbaukasten. Dieser soll die Arbeit des Administrators unterstützen. Diese Workflows lassen auch Aktionen auf mehreren Objekten gleichzeitig zu. Was sich so einfach anhört, ist ein recht komplexer Vorgang, der nicht so einfach zu beherrschen ist. Macht man sich die Mühe, nach Beispieldateien zu suchen, findet man nur sehr wenige Administratoren, die sich intensiver mit der Materie auseinandergesetzt haben. Vielen VMware-Administratoren reicht es für ihre Arbeit aus, ihre Routineaufgaben über die verschiedenen vCenter-Schnittstellen durchzuführen. Als Beispiel sei die PowerShell genannt; sie ist zwar vom Umfang sehr komplex, aber recht leicht zu erlernen.

A.1.3 VMware vCenter CapacityIQ

Die Applikation vCenter CapacityIQ von VMware unterstützt den Administrator der virtuellen Infrastruktur in der Planung und der Erweiterung der VMware-Landschaft.

Das Add-on VMware vCenter CapacityIQ gibt Ihnen eine Übersicht über die Ressourcenauslastung Ihrer VMware-Infrastruktur. Es zeigt Ihnen an, wie viele Ressourcen derzeit genutzt werden und welche Reserven noch vorhanden sind. Neben der aktuellen Auslastung sind auch die historische und die zu erwartende künftige Auslastung dargestellt. Dadurch gibt das Tool Ihnen eine Planungsmöglichkeit an die Hand, rechtzeitig zu erkennen, wann die Ressourcen erweitert werden müssen. Eine Reporting-Funktion erstellt eine Liste von Möglichkeiten zur Optimierung der Landschaft. Mit dieser Funktion können Sie Engpässe sofort erkennen und darauf reagieren. Sie können sich auch darstellen lassen, wie sich die virtuellen Maschinen mit der Zeit entwickelt haben.

Die Applikation wird als virtuelle Appliance heruntergeladen. Die Appliance besteht vom Prinzip her aus vier Elementen: Der eigentliche vCenter-CapacityIQ-Server kommuniziert mit dem enthaltenen Datenbank-Server. Das Collector-Interface sammelt die Performancedaten aus der virtuellen Infrastruktur, sowohl von den Hosts als auch von den virtuellen Gästen. Dieses Interface liefert seine Daten im Minutenrhythmus direkt an die Datenbank.

Über alle Elemente legt sich das Administrations-Interface, mit dem Sie die Appliance konfigurieren. Die Administration erfolgt über ein vCenter-CapacityIQ-Plugin im vSphere-Client. Nach der Aktivierung der Applikation bietet sie Ihnen vier Schritte, um Ihre virtuelle Infrastruktur zu verstehen. Ist die initiale Sammlung der Performancedaten erfolgt, wird detailliert angezeigt, wie viele Ressourcen derzeit verbraucht bzw. genutzt werden. Sie sehen auch, welche Menge an Ressourcen noch für die Nutzung zur Verfügung steht.

Das Dashboard stellt aber auch Informationen zur Verfügung, die Ihnen helfen zu erkennen, wie viele VMs Sie noch aufbauen können, bevor die Landschaft erweitert werden muss. So liegen die nötigen Informationen vor, die Sie benötigen, um zur rechten Zeit zu investieren. Damit bleiben Ihnen Stresssituationen erspart, wenn zu kurzfristig zusätzliche Ressourcen benötigt werden. Als zusätzliche Funktion wird die Möglichkeit geboten, »Was wäre wenn«-Szenarien zu erstellen.

Für den Fall, dass größere Übernahmen anstehen oder Sie eine größere Anzahl von virtuellen Maschinen ausrollen müssen, stellt das Tool einen *Forecast Wizard* zur Verfügung. Dieser Wizard gibt Ihnen das Mittel an die Hand, die Anzahl, die Konfiguration und die Last von neuen virtuellen Maschinen als Simulation in die virtuelle Infrastruktur einzubinden. Mit diesen Informationen berechnet das Softwarepaket die benötigten zusätzlichen Ressourcen für die Abbildung der zusätzlichen virtuellen Systeme. Als Vorlage für die neue Berechnung können Sie auch Profile von bereits vorhandenen Systemen verwenden.

Was mit virtuellen Maschinen geht, ist selbstverständlich auch mit ESX-Hosts möglich. Durch das Hinzufügen von neuen oder das Ändern von vorhandenen Hosts berechnen Sie die vorhandenen Host-Ressourcen neu. So ist auf einfache Weise planbar, ob es sinnvoll ist, einen bestehenden Cluster zu erweitern oder einen neuen Cluster aufzubauen. Bevor jedoch neue Ressourcen angeschafft werden, ermöglicht vCenter CapacityIQ, zu ermitteln, ob VMs überdimensioniert sind oder ob VMs zwar laufen, aber eigentlich nicht von den Benutzern verwendet werden. Diese überflüssigen Ressourcenfresser können Sie so erkennen und eliminieren.

All diese Optionen erlauben in jedem Projekt eine optimale Planung. Die Informationen, die das System zur Auswertung nutzt, stehen ebenfalls zum Abruf von Server-Listen zur Optimierung der derzeit genutzten Ressourcen bereit. Es ist einfach, eine Liste mit Low- bzw. High-Performern zu erstellen. Diese Daten helfen, die Systeme gut zu gruppieren, so dass die Landschaft optimal genutzt werden kann.

A.2 Billing: VMware vCenter Chargeback

Das sich direkt ins vCenter integrierende VMware vCenter Chargeback dient nicht nur der Kostenanalyse der virtuellen Infrastruktur, sondern auch einer verursachergerechten Abrechnung der Ressourcen anhand der Kundensysteme.

Der Aufbau und der Betrieb von virtuellen Infrastrukturen nimmt immer mehr zu. Im Gegensatz zu anderen Anbietern von Virtualisierungslösungen bietet VMware eine Applikation, VMware vCenter Chargeback, um die Ressourcennutzung der virtuellen Maschinen abzurechnen. Während der Installation wird die Applikation mit dem vCenter und dem Datenbank-Server verbunden. Eine Einbindung ins LDAP findet ebenfalls statt. So haben Sie die Option, granulare Rechte im System zu vergeben. Abschließend können Sie eine E-Mail-Adresse oder einen E-Mail-Verteiler für das automatische Versenden von Reports einrichten.

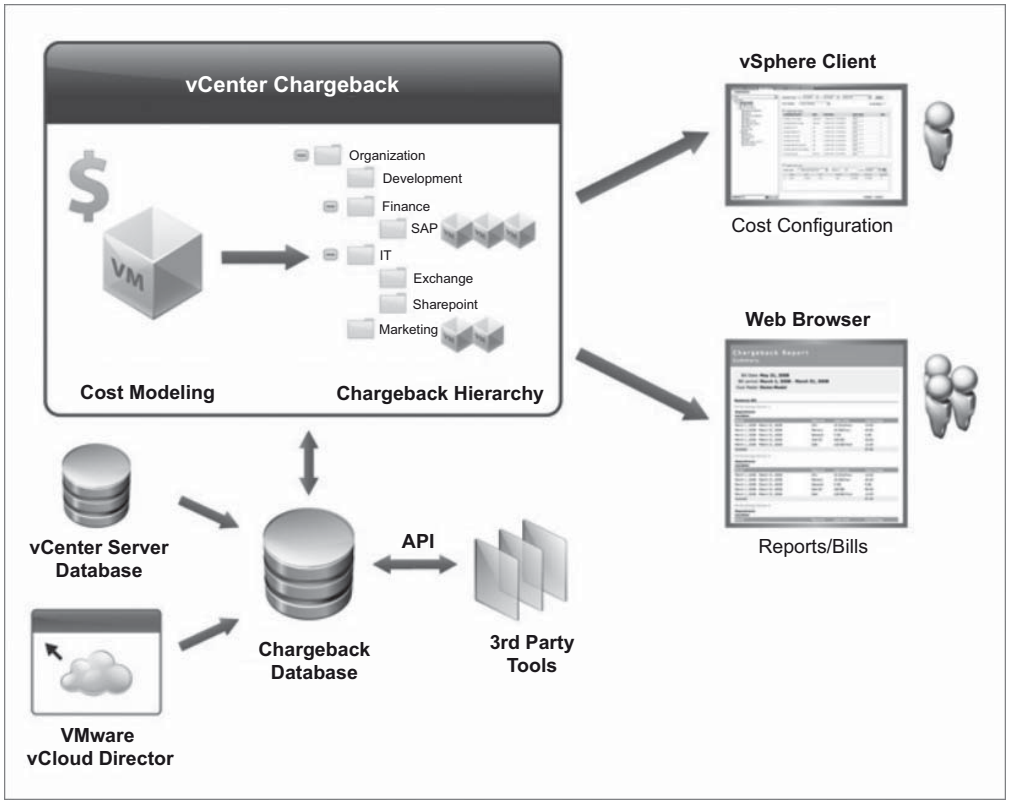


Abbildung A.6 Struktur von VMware vCenter Chargeback

Der wichtigste Punkt bei der Einrichtung der Anwendung ist das Definieren der Kosten für die Ressourcen. Die Werte sind dabei für jede benutzte Hardwareeinheit einstellbar. Bei der Hinterlegung der Kosten haben Sie einen hohen Flexibilitätsgrad. Sie können die Kosten verbrauchsabhängig oder als Fixkosten festlegen. Auch zusätzliche fixe oder periodische Kosten

können Sie berücksichtigen. Bei den Ressourcen wird entweder der Durchsatz als Berechnungsgrundlage herangezogen oder die vergebene Kapazität. Damit Sie die monetären Werte für die Abrechnung der Ressourcen richtig hinterlegen können, stellt VMware ein Excel-Sheet zur Verfügung. Mit dessen Hilfe können Sie berechnen, welche Kosten verrechnet werden müssen, um die Investition in die Infrastruktur zurückzuerhalten.

Dieses Sheet finden Sie unter:

http://www.vmware.com/support/vcbm10/doc/vCenter_Chargeback-Costing_Calculator.xls

	A	B	C	D	E	F	G	H	I	J
1	**Recovery Cost**		**3 Years**		Total Hours per Month					
2	Compute Cost	$ 139.136,00			**720**					
3	Storage Cost	$ 70.000,00								
4	Fixed Cost	$ 213.000,00								
5	**Recovery Total**	**$ 422.136,00**								
6										
7	**Compute Cost Calculation**	Hardware Cost Recovered %	Capacity	3 Year Cost	Annual Cost	Monthly Cost	Hourly Cost			
8	RAM (GB)	**70**	788,48	$ 123,52	$ 41,17	$ 3,43	$ 0,004766			
9	Processor Speed (GHz)	30	40,32	$ 1.035,24	$ 345,08	$ 28,76	$ 0,039940			
10										
11										
12	**Storage Cost Calculation**	Storage Cost Recovered %	Capacity	3 Year Cost	Annual Cost	Monthly Cost	Hourly Cost			
13	Tier 2 Storage (GB)	100	2048	$ 34,18	$ 11,39	$ 0,95	$ 0,001319			
14										
15										
16	**Total VMs**									
17	**500**									
18										
19	**Fixed Cost Calculation**	3 Year Cost	Annual Cost	Monthly Cost	Monthly Cost (Per VM)					
20	VMware License	$ 92.000,00	$ 30.666,67	$ 2.555,56	$ 5,11					
21	Microsoft License	$ 48.000,00	$ 16.000,00	$ 1.333,33	$ 2,67					
22	Network Connectivity	$ 19.200,00	$ 800,00	$ 66,67	$ 0,13					
23	Storage Connectivty	$ 28.800,00	$ 1.200,00	$ 100,00	$ 0,20					
24	vCenter License	$ 10.000,00	$ 3.333,33	$ 277,78	$ 0,56					
25	Database Cost	$ 15.000,00	$ 5.000,00	$ 416,67	$ 0,83					
26	**Total Fixed Cost**	**$ 213.000,00**	**$ 57.000,00**	**$ 4.750,00**	**$ 9,50**					
27										
28										
29	**System Sample**	RAM (GB)	Processor Speed (GHz)	Storage (GB)	Monthly Compute Cost	Monthly Storage Cost	Monthly Fixed Cost	Monthly Total	Hourly Total	Instantiation
30	Small	**1**	**2**	**20**	$ 60,94	$ 18,99	$ 9,50	$ 89,43	$ 0,12	$ 1.000,00
31	Medium	**2**	**4**	**80**	$ 121,89	$ 75,95	$ 9,50	$ 207,34	$ 0,29	$ 1.000,00
32	Large	**4**	**8**	**120**	$ 243,78	$ 113,93	$ 9,50	$ 367,21	$ 0,51	$ 1.000,00

Abbildung A.7 vCenter-Chargeback-Kostenkalkulationssheet

Auf dem ersten Sheet befindet sich eine kurze Anleitung für die Nutzung des Sheets. Der Reiter COSTS nimmt alle Kosten auf, die die Landschaft verursacht – die Server-Hardware, Lizenzkosten für die virtuelle Landschaft und die Gastsysteme, das Netzwerk, die Datenbank und den genutzten Storage. Beim CAPACITY-Reiter ist zu hinterlegen, welche Reserven in der Landschaft freigehalten werden, damit alle Anfragen bedient werden können. Der letzte Reiter, RECOVERY, berechnet die Kosten, die eine VM einer definierten Ausprägung verursacht. Die einmaligen Kosten für die Installation einer VM werden ebenfalls eingerechnet. Es fehlen nur die Beträge für die Betriebsaufwände des Gastes und der vSphere-Hosts.

In der Applikation hinterlegen Sie nun die Kosten für die zum Einsatz kommenden Ressourcen. Es wird ein Grundbetrag für jede Ressource manifestiert. Anschließend ist für jede virtuelle Maschine ein Faktor einzugeben. Durch die Ressourcengrundkosten und den Ressourcenfaktor einer jeden VM können Sie für jede virtuelle Maschine eine individuelle Rechnung erstellen.

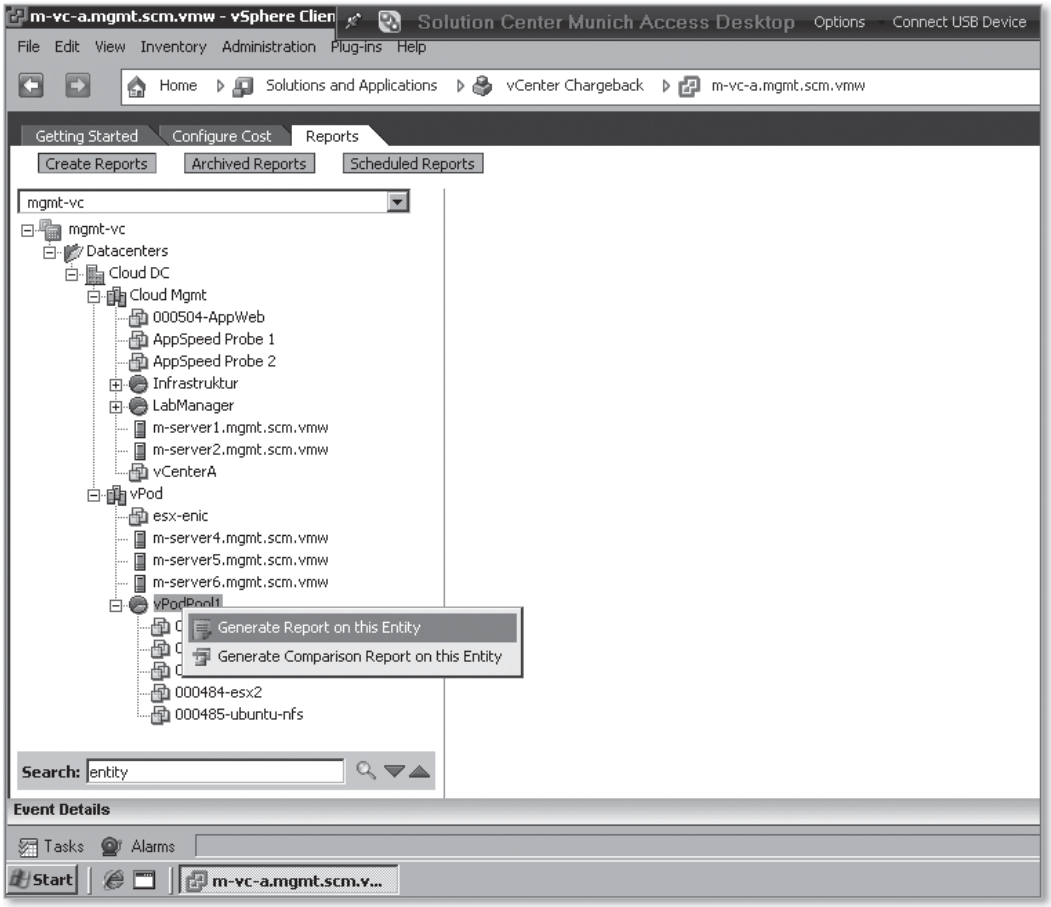


Abbildung A.8 Erstellen eines Reports

Über das Kontextmenü der einzelnen VM erstellen Sie einen individuellen Report (Abbildung A.8). Nach dem Aufruf wählen Sie die individuellen Verrechnungswerte aus, die zur Erstellung der Rechnung herangezogen werden sollen. Geben Sie den Zeitraum der Berechnung an und den Zeitpunkt des Rechnungslaufes. Eine Beispielrechnung für ein System sehen Sie in Abbildung A.9.

So können Sie für jeden virtuellen Server eine Rechnung einsehen. Dies bietet Ihnen eine Transparenz für die Kosten, die durch virtuelle Maschinen entstanden. Durch eine Gegenrechnung der erwirtschafteten Erträge und der Investition lassen sich die Kosten für eine virtuelle Infrastruktur optimieren.Selbstverständlich müssen Sie nicht jede Abrechnung manuell anstoßen, Sie haben natürlich auch die Option, den Rechnungslauf zu automatisieren und die Abrechnung periodisch zu verschicken. Alternativ rufen Sie die Verrechnung der Ressourcen über ein Webportal ab.

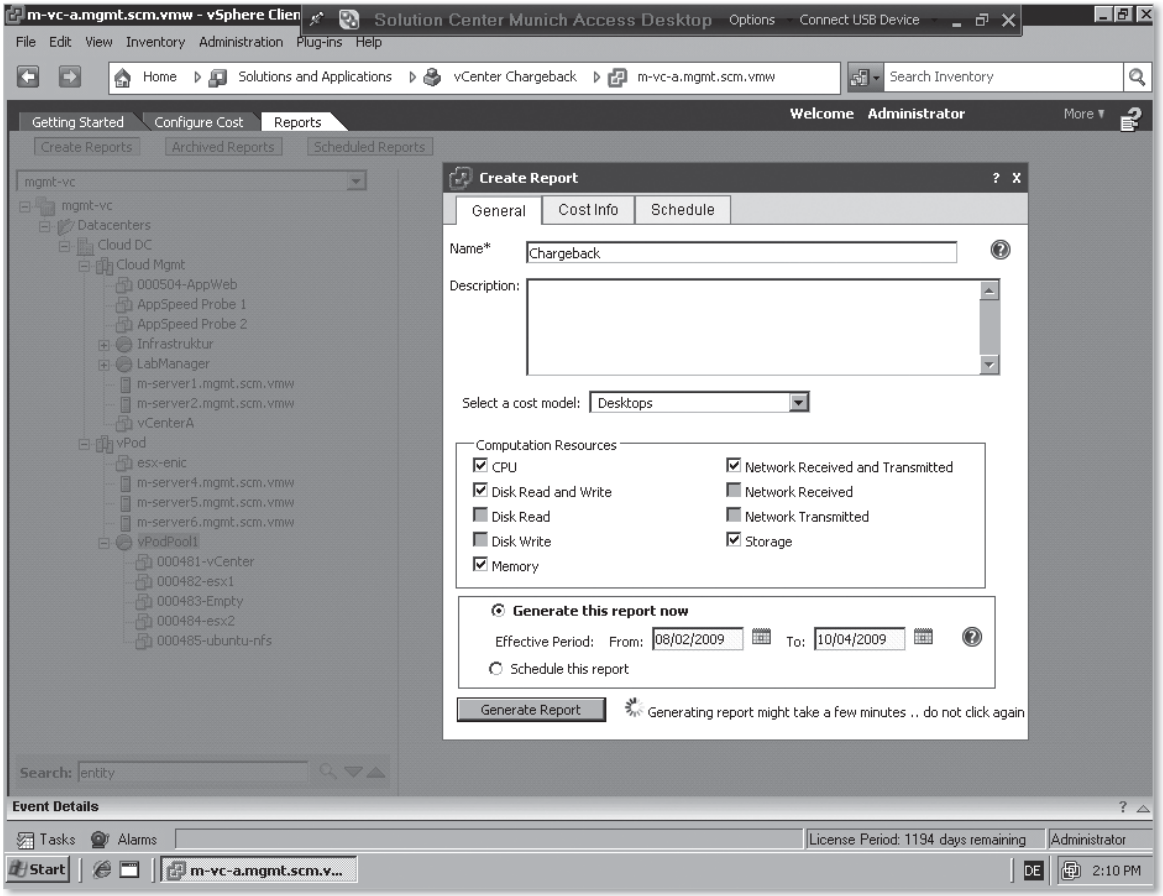


Abbildung A.9 Zusammenstellung einer Abrechnung

A.3 Performance: VMware vCenter AppSpeed

Auch wenn wir in diesem Buch fast durchgängig von virtuellen Landschaften sprechen, so gibt es doch Dinge, die virtuellen und physischen Systemen gemein sind. Es genügt nicht, dass diese Systeme zur Verfügung stehen, es wird von ihnen auch erwartet, dass sie performant arbeiten und definierten SLAs (Service-Level Agreements) genügen. Es stellt sich aber immer die Frage, wie und mit welchen Mitteln entsprechende Informationen zur Verfügung gestellt werden können. An dieser Stelle greift die VMware AppSpeed ein. Die Applikation kommt als Virtual Appliance und misst die Latenzzeiten einer Applikation. Es wird der gesamte Datenstrom gemessen, sowohl der eingehende als auch der ausgehende. Die erhaltenen Daten werden mit den SLAs abgeglichen. Auf der dann entstandenen Datenbasis wird ein Reporting erstellt. Unter Zuhilfenahme der Messdaten lassen sich den VMs die Ressourcen zuweisen, die benötigt werden, um die SLAs zu gewährleisten.

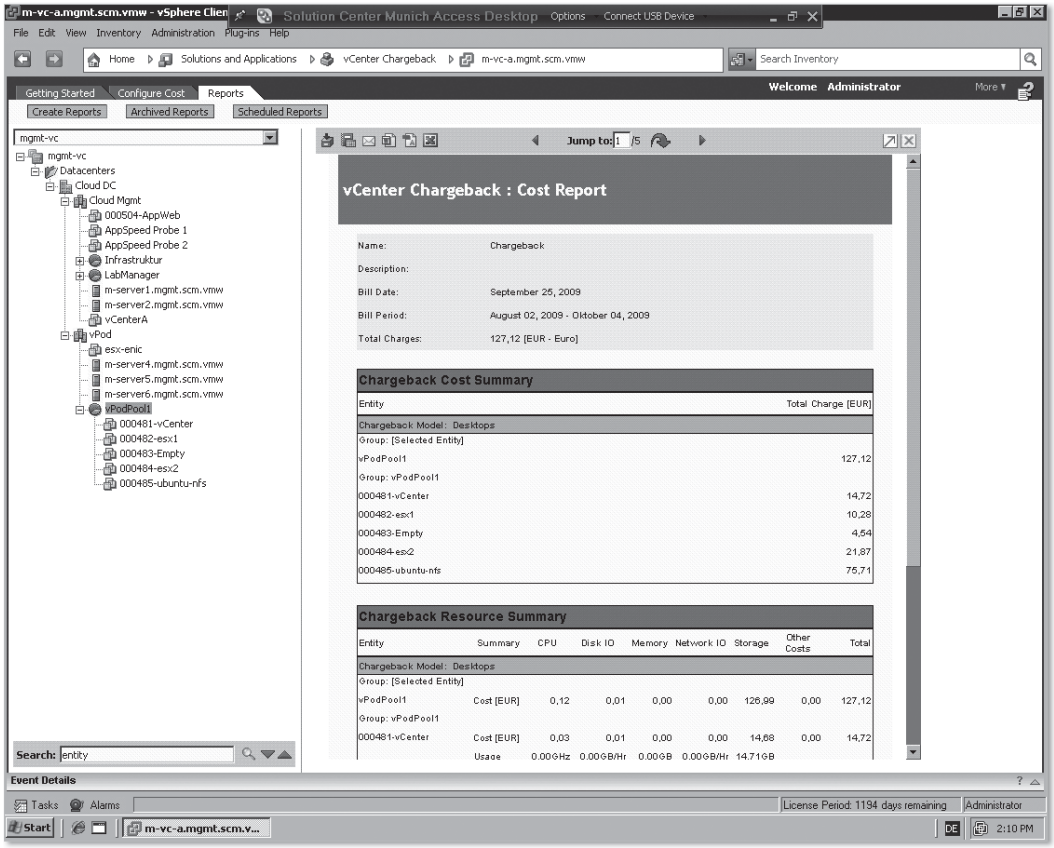


Abbildung A.10 Abrechnungsreport eines Server-Pools

Beleuchten wir zuerst einmal die Architektur von vCenter AppSpeed. Da ist zuerst einmal der eigentliche Applikations-Server, er integriert sich an den vCenter-Server. Als Client-Interface kommt ein vCenter-Plugin zum Einsatz, wie Sie das auch schon von anderen VMware-Applikationen kennen. Der AppSpeed-Server dient nur zur Verarbeitung von den Informationen, die von den AppSpeed-Messerfassungs-Servern, den sogenannten Probes, geliefert werden. Von diesen Probes benötigen Sie mindestens eine pro vSphere-Host.

Die VMware vCenter AppSpeed Probes überwachen den Datenstrom von MSSQL, Oracle, MySQL und Exchange. Des Weiteren tracken sie Webtraffic über HTTP oder HTTPS. Jede Probe kann Daten von bis zu 8 Switches sammeln, wobei es unerheblich ist, ob es sich um Distributed oder Standard-vSwitches handelt. In einer Landschaft können Sie bis zu 32 Probes in Betrieb nehmen.

Der vSphere-Administrator muss nicht unbedingt jede Applikation kennen. AppSpeed durchsucht das Netz und listet die gefundenen Applikationen in seinem Fenster auf. Zusätzlich werden die Server angezeigt, auf denen die Applikationen installiert sind. Über den Traffic im

Netzwerk werden die Applikations-Server gefunden und aufgenommen. Zur Darstellung gibt es zwei mögliche Ansichten, entweder serverbasiert oder applikationsbasiert. Selbstverständlich können die Abhängigkeiten der betroffenen Server untereinander auch grafisch aufbereitet werden. Es gibt auch hier verschiedene Darstellungsmodi, bei denen sowohl die Anwendung als auch die Server dargestellt werden.

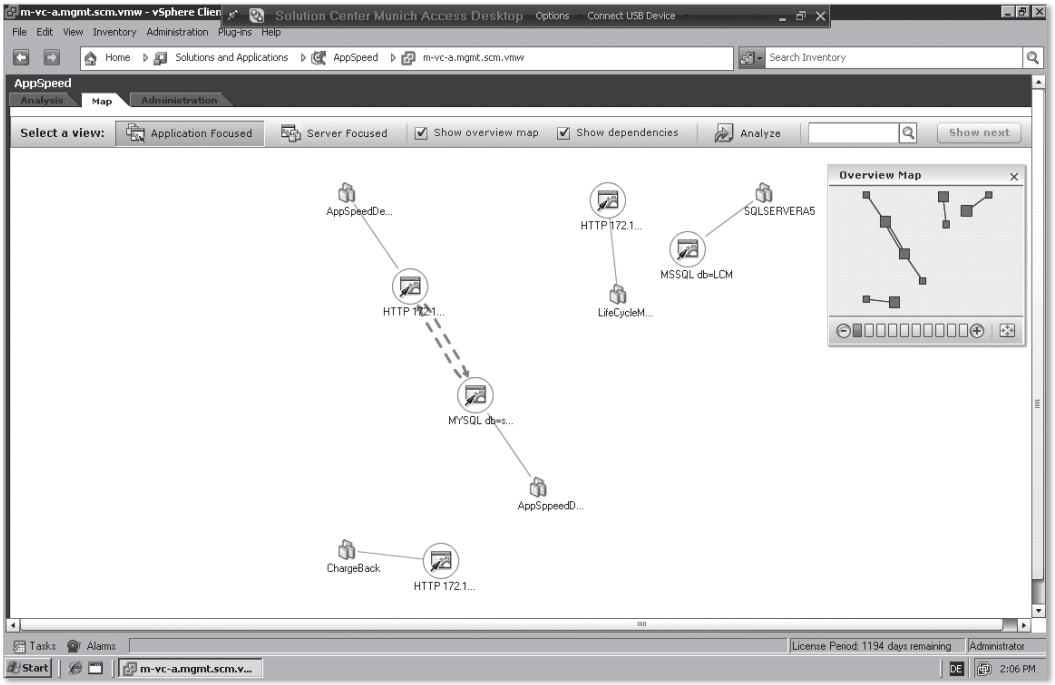


Abbildung A.11 Grafische Übersicht der überwachten Applikationen

Sind die Applikationen erkannt, werden die Zugriffszeiten gemessen. Die Latenzzeiten werden aufgenommen und für spätere Auswertungen gespeichert. Sind erst einmal Messdaten vorhanden, können Sie sich die Daten anschauen und bis auf Befehlsebene hinunter erkennen, welches Kommando welche Laufzeiten hatte. An der Charakteristik des Befehls lässt sich dann im Falle einer zu langen Abarbeitungszeit feststellen, wo der Engpass in der Applikationskette liegt.

Mit diesen Informationen schlagen Sie zwei Fliegen mit einer Klappe: Durch die agentenlose Datenaufnahme rund um die Uhr ist es möglich zu analysieren, wie optimal das Sizing der Server-Kette erfolgte. Eine genaue Auswertung der Daten fördert sofort zutage, an welcher Stelle die Systeme zu viele freie Ressourcen haben oder wo Sie die virtuelle Hardware zusätzlich erweitern müssen. So lassen sich an der einen oder anderen Stelle eine Menge Ressourcen einsparen oder optimieren. Der zweite Vorteil ist die Verwendung der Daten zum Nachweis der Einhaltung der SLAs.

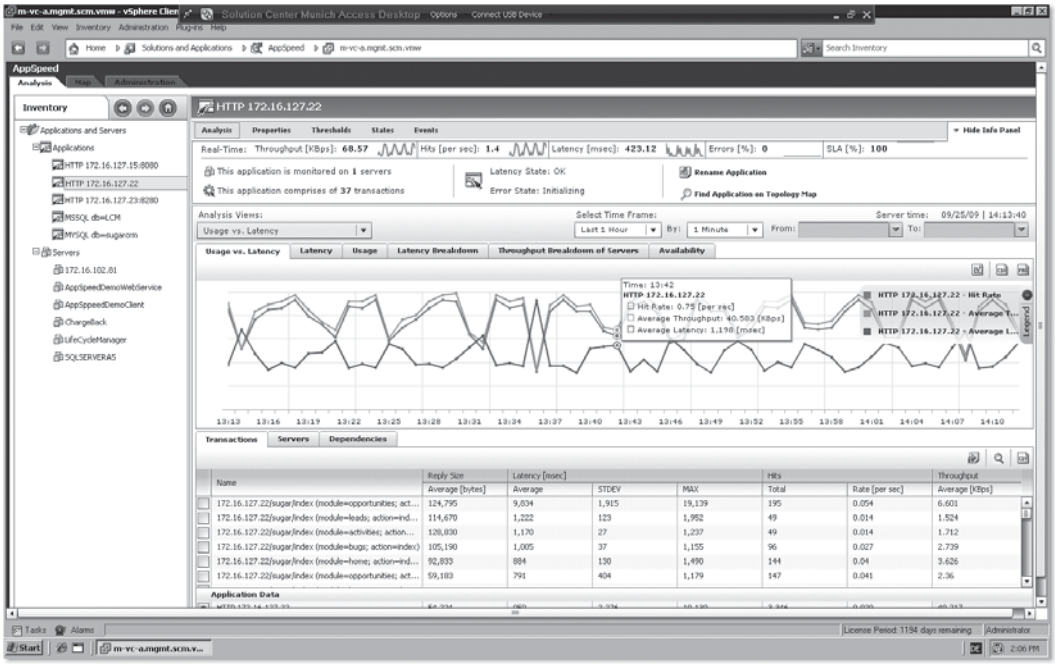


Abbildung A.12 Auflistung der Abarbeitungszeiten

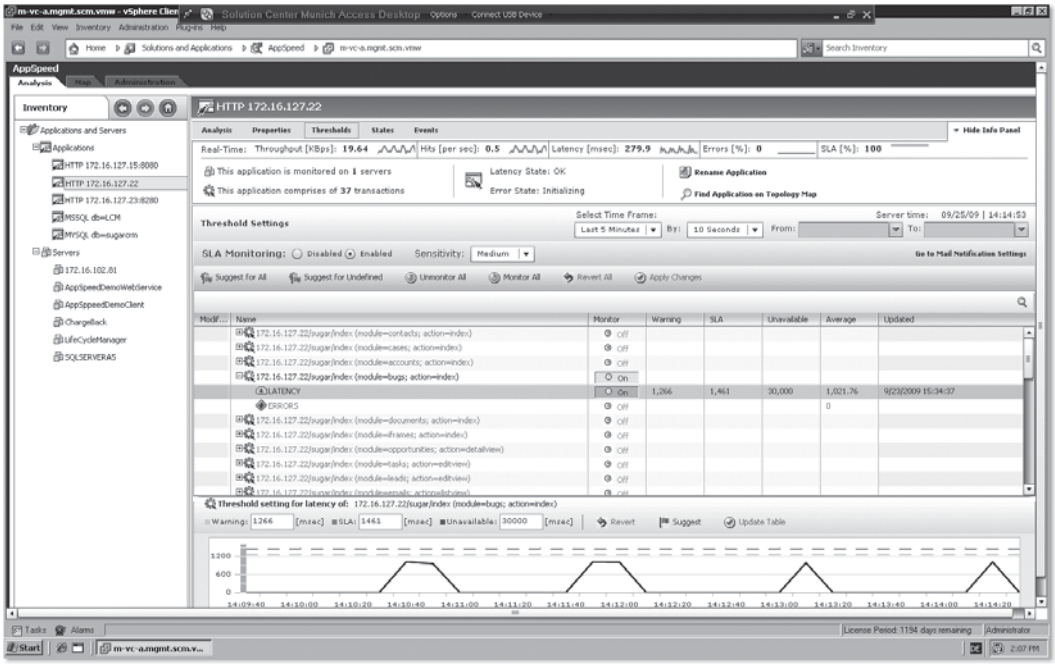


Abbildung A.13 Einhaltung der SLAs

Dabei lassen sich genau die Werte auswählen, die für die Überwachung der SLAs entscheidend sind. Selbstverständlich können Sie die Überschreitung der Schwellenwerte mit einem Alarm koppeln, oder Sie lassen sich einfach per E-Mail informieren.

Eine sehr granulare Analyse ermöglicht es Ihnen, genau festzustellen, welche der betroffenen Elemente den Performanceengpass verursacht hat.

Die Software greift hier an einem Punkt an, den jeder Administrator einer virtuellen Infrastruktur kennt: Für alle Probleme in den Gästen ist die Virtualisierung verantwortlich, und es wird vom Administrator erwartet, dass er alle Applikationen kennt, die auf den virtuellen Servern installiert sind. Hier hilft vCenter AppSpeed bei der Root-Cause-Analysis. Sie können genau analysieren und darstellen, welcher Befehl beim Zugriff auf die Datenbank Probleme verursacht hat. So gelangen Sie schnell zu einer Problemlösung und können die betroffene Betriebsabteilung gezielt auf die Unstimmigkeit ansetzen, ohne dass Sie selbst Kenntnis von der Applikation und deren Komponenten haben müssen.

Die gesamte Datenaufnahme erfolgt agentenlos. Es ist keine zusätzliche Software im Gast notwendig, um die Funktion von VMware AppSpeed zu gewährleisten. Auch hier gibt es einen Link zu einem Video: *http://blip.tv/file/2874476/*

A.4 vCenter Site Recovery Manager

Mit dem vCenter Site Recovery Manager (SRM) bietet VMware ein Produkt an, das im Desasterszenario unterstützen soll. Dabei wird nicht nur die Verwaltung der Sites unterstützt, sondern auch der Prozess der Automatisierung. Im Gegensatz zu anderen Funktionen zur Ausfallsicherheit, die in VMware vSphere bereits enthalten sind, deckt der SRM den Ausfall ganzer Sites ab. Es handelt sich hierbei also nicht um Szenarien wie den Ausfall einzelner Komponenten – z. B. eines Hosts, eines Controllers, eines Switches oder einer einzelnen virtuellen Maschine –, sondern um den kompletten Ausfall eines Rechenzentrums oder eines Standortes.

Bis zur letzten Version war der SRM nur eine Teilkomponente, die zu einem komplexen Konglomerat gehörte. Schließlich war es ebenfalls notwendig, den Plattenplatz über zwei Standorte mit storagebasierten Mitteln zu spiegeln. Die Version SRM 5.x bietet aber die Möglichkeit, selbst eine Storage-Spiegelung durchzuführen. Mit der Software kann nicht nur die endgültige Übernahme einer Site oder eines Rechenzentrums erfolgen, dieser Prozess kann auch verprobt werden, ohne dass dies für die produktiven Systeme eine Auszeit bedeutet. Damit kann regelmäßig ein Test erfolgen ohne eine weitere Beeinträchtigung anderer Komponenten und vor allem der Anwender. Auch an dieser Stelle hat sich mit der Version 5.x eine Änderung ergeben, denn der Rückweg in das Quell-Rechenzentrum ist nun genauso einfach möglich wie die Aktivierung der Recovery-Site.

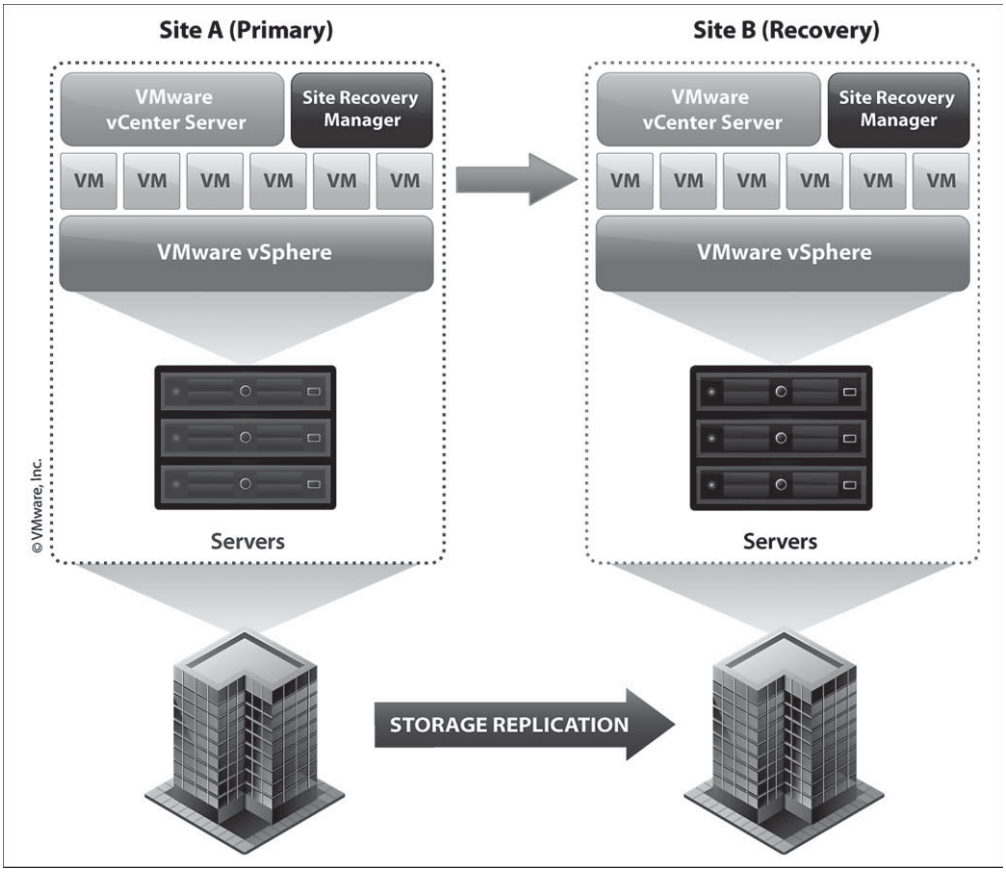


Abbildung A.14 Überblick VMware Site Recovery Manager

Den Site Recovery Manager gibt es in zwei unterschiedlichen Versionen. Die Standard Version eignet sich für kleinere Umgebungen und unterstützt den Schutz von maximal 75 virtuellen Maschinen. Bei der Enterprise-Version können Sie größere Umgebungen abbilden und haben zusätzlich die Option die Werte RPO (Recovery Point Objective) und RTO (Recovery Time Objective) zu parametrieren. Die beiden Werte definieren, wie groß der Datenverlust bei einem Umschalten sein darf. Eine genaue Definition an dieser Stelle ermöglicht die Optimierung der Bandbreiten für die Replikation. Das RTO legt fest, welches Zeitfenster Ihnen zur Verfügung steht, um die Recovery-Site zu aktivieren.

A.4.1 Der Katastrophenfall

Tritt der Katastrophenfall ein, ist das gleichbedeutend mit einem kompletten Neustart der IT-Landschaft an einem anderen Standort. Wer schon einmal eine Stromabschaltung in seinem Rechenzentrum miterlebt hat, versteht, wovon wir hier reden. Es ist nicht einfach mit dem Einschalten aller Komponenten getan, Sie müssen sich schon im Vorfeld Gedanken machen,

was in welcher Reihenfolge gestartet werden muss, damit alle Dienste ordnungsgemäß laufen. In der Regel gibt es sogenannte K-Fall-Handbücher, in denen ein solcher Prozess genau hinterlegt ist. Diese Informationen kommen Ihnen bei der Planung nun zugute. Dieses Handbuch hilft Ihnen, Schritt für Schritt die ausgefallene Umgebung an einem anderen Standort wieder hochzufahren. Aufgrund stetiger Änderungen im Rechenzentrum ist die Pflege eines solchen Handbuches häufig sehr schwer, der praktische Test eines solchen Schwenks meist unmöglich. Problematisch ist dabei, dass viele Ansätze in diesem Umfeld ein zweites Rechenzentrum benötigen mit nahezu identischer Hardwareausstattung, die für den eventuellen K-Fall bereitsteht. Man könnte fast sagen, es muss eine Investition getätigt werden, bei der man hofft, dass sie nie wirklich benötigt wird. Ein weiterer zu beachtender Faktor bei einem solchen Szenario ist der Mensch oder besser der Administrator. Zu den eventuell möglichen Tippfehlern, die beim Abschreiben der nötigen Kommandos aus dem Handbuch passieren können, kommt ein hoher Stressfaktor in dieser Situation hinzu. Eventuell muss der Administrator, gerade aus einem Gebäude vor dem Feuer geflüchtet, nun dafür sorgen, dass ein ganzes Unternehmen schnell wieder grundlegend arbeitsfähig wird. Zur Vereinfachung dieses Prozesses und der fehlerunanfälligen Abarbeitung der Inbetriebnahme des Backup-Rechenzentrums dient der SRM als Unterstützung.

A.4.2 Aufbau und Implementierung

Der Site Recovery Manager greift genau an diesen Punkten ein. Als Voraussetzung muss es auf der Storage-Ebene ein unterstütztes System geben. Dieses kann mit Replikationsfunktion ausgestattet sein, oder Sie nutzen die Replikationsmechanismen des SRM selbst. Mit Hilfe dieser Technologie werden die virtuellen Server der vSphere-Landschaft von der primären bzw. produktiven Seite auf die sekundäre, die Recovery-Site, übertragen. In der Regel erfolgt dies mittels asynchroner Spiegelung. Eine asynchrone Spiegelung bedeutet einen zeitlichen Versatz bei der Übertragung der Storage-Informationen. Ist die WAN-Bandbreite zwischen zwei Standorten nicht so performant, dann ist dies die Methode der Wahl. Natürlich können verschiedene Storage-Systeme auch synchron spiegeln. In diesem Fall sind die Daten an beiden Standorten identisch, mit einem minimalen Zeitversatz.

Auf der primären Seite findet man weiterhin die produktiven vSphere-Hosts, das vCenter und natürlich die gesamten virtuellen Maschinen.

Ähnlich wie andere Zusatzprodukte von VMware wird der Site Recovery Manager auf einem Windows-Server zusätzlich zum vCenter installiert. Die Entscheidung liegt beim Administrator, ob er die Software auf einem physischen oder einem virtuellen Server installiert.

Auf der sekundären Seite sind ebenfalls ein oder mehrere Hosts aufzubauen, um die virtuellen Server abbilden zu können, die im Desasterfall übernommen werden sollen. Die Anzahl und der Ausbau der Server müssen nicht der primären Seite entsprechen. Zusätzlich zu den ESX-Servern muss auch ein zweites vCenter und ein zweiter SRM-Server auf der sekundären Seite eingerichtet werden.

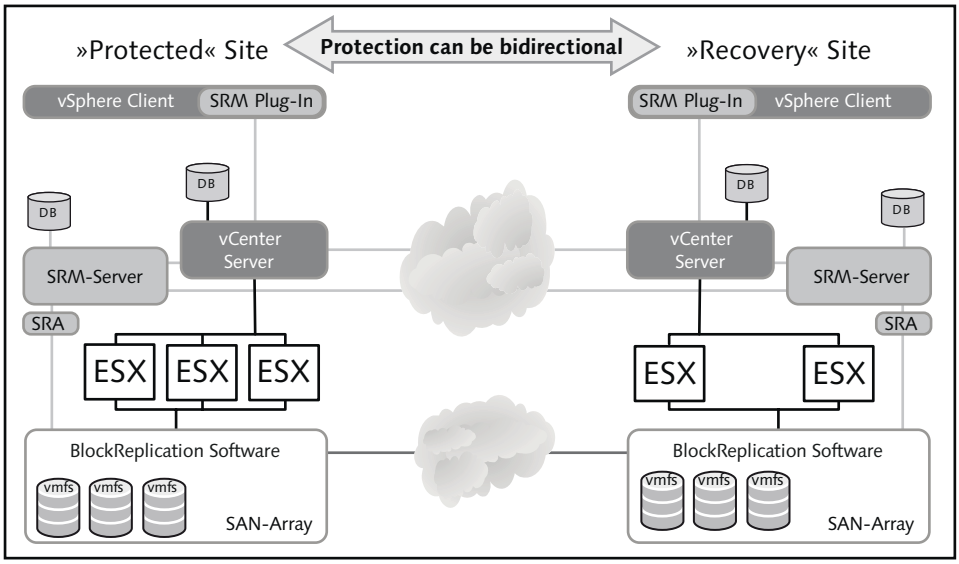


Abbildung A.15 Aufbau Site Recovery Manager im Detail

A.4.3 Storage-Replication-Modul (SRA)

Für die Kommunikation des vSphere Site Recovery Managers mit dem angeschlossenen Storage müssen Sie den entsprechenden Storage-Replication-Adapter (SRA) installieren. Die Replikation ist manuell einzurichten. Im Desasterfall muss der SRM-Server mit Hilfe dieses Moduls die Spiegelung aufbrechen. Das bedeutet, dass die Daten nicht weiter von dem primären Rechenzentrum auf die sekundäre Seite übertragen werden. Zudem wird der Lese- und Schreibzugriff auf den Speicher der sekundären Seite für die dort stehenden Hosts aktiviert.

Das SRA-Modul sorgt auch dafür, dass bei einem Test eines Recovery-Plans ein Clone der replizierten LUN oder des Volumes angelegt und nach Abschluss des Tests wieder gelöscht wird.

Für jeden Storage, den der vCenter Site Recovery Manager unterstützt, stellt VMware ein passendes SRA-Modul zur Verfügung. Nur mit diesem Modul ist die Funktion der SRM gewährleistet.

A.4.4 Site Recovery Manager Plugin

Der SRM integriert sich in das vCenter. Über den vSphere-Client installieren Sie die Client-Komponente. Über dieses Interface verknüpfen Sie die beiden vCenter-Server und die beiden Array-Manager vom primären und sekundären Standort miteinander.

Zur einwandfreien Funktion ist im Client ein Inventory-Mapping vorzunehmen. Dabei werden die Datacenter- und VM-Netzwerke miteinander verknüpft. Damit legen Sie fest, welches die primäre und welches die sekundäre Komponente ist. Die Datacenter haben immer unter-

schiedliche Namen, z. B. »DC-Primär« und »DC-Sekundär«, damit der SRM weiß, welches das primäre und welches das zugehörige sekundäre Datacenter ist. Beide werden dann in einem Folgeschritt miteinander verknüpft. Hier wird dem Umstand Rechnung getragen, dass in einem Rechenzentrum auch mehrere Sites gehostet werden können, weil dort beispielsweise unterschiedliche Kunden ihre Systeme stehen haben. So können unterschiedliche Umgebungen abgebildet und voneinander getrennt werden. Es muss ja nicht jedes Datacenter im SRM berücksichtigt werden.

Mit vSphere 5 brauchen Sie die produktive und die Recovery-Site nicht mittels Linked Mode im vSphere-Client zu verbinden.

A.4.5 Protection-Groups

Nach der Verknüpfung der beiden Seiten müssen Sie die *Protection-Groups* einrichten. Eine Protection-Group ist eine Gruppe von virtuellen Maschinen, die im Desasterfall auf der sekundären Seite neu gestartet werden. Die Anzahl der Protection-Groups ist nicht auf eine beschränkt.

In einer Protection-Group fassen Sie z. B. alle VMs auf einem gemeinsamen Datastore zusammen. Eine Protection-Group kann gebildet werden mit den virtuellen Maschinen der ersten LUN oder des ersten Volumes, eine andere mit den VMs der zweiten LUN. Alternativ füllen Sie eine mit den virtuellen Maschinen beider LUNs oder Volumes.

A.4.6 Recovery-Plan

Für eine oder mehrere Protection-Groups ist ein Recovery-Plan sinnvoll. In diesem legen Sie fest, wie bei einem Ausfall vorzugehen ist. Es kann einen Recovery-Plan für den kompletten Ausfall der primären SiteSeite geben oder auch für den Ausfall einer einzelnen LUN. So bereiten Sie schon jetzt für die unterschiedlichen Szenarien Pläne vor.

In einem Recovery-Plan können Sie verschiedene Aktionen festlegen, angefangen beim Herunterfahren der virtuellen Maschinen auf der primären Seite über die Startreihenfolge und Anpassung der virtuellen Maschine auf der sekundären Seite. Letzteres kann zum Beispiel nötig sein, um virtuelle Maschinen auf der sekundären Seite in ein anderes Netzwerk zu konfigurieren. In den Recovery-Plan können Sie auch individuelle Skripte, Befehle oder Abhängigkeiten einarbeiten. Eine Abhängigkeit kann zum Beispiel sein, dass erst, nachdem die VMware Tools der virtuellen Maschinen gestartet sind, mit dem nächsten Schritt begonnen wird. So werden unterschiedliche Gruppen von virtuellen Maschinen, die in Abhängigkeit voneinander stehen, nacheinander gestartet.

Ein weiterer Vorteil des SRM ist, dass auf der sekundären Seite auch virtuelle Maschinen betrieben werden dürfen. Sie können Testumgebungen aufbauen, die im Desasterfall einfach heruntergefahren werden, um so die Ressourcen für die produktiven VMs freizugeben. Der SRM wird auf Ebene der virtuellen Maschinen konfiguriert, so können nichtkritische VMs im

K-Fall ausgeschaltet bleiben oder erst später eingeschaltet werden. So wäre es möglich, zunächst den Domain-Controller zu starten. Nachdem dieser komplett gebootet ist, wird mit dem Mailserver fortgefahren. Erst dann würden die wichtigen Datenbank- und Applikations-Server folgen.

Wichtig ist aber, dass der Recovery-Plan stetig gelebt und an die Änderungen in der Umgebung angepasst wird. Sehr angenehm ist dabei die Möglichkeit des Tests, ohne dass die produktive Umgebung beeinflusst wird.

A.4.7 Testen des Desasterfalls

Für den täglichen Betrieb ist es sehr angenehm, dass Sie den Recovery-Plan jederzeit testen können. So überprüfen Sie regelmäßig ob der Plan noch aktuell ist. Beim Test des Recovery-Plans wird die Spiegelung nicht aufgebrochen, und die virtuellen Maschinen auf der produktiven Seite arbeiten normal weiter. Für den Test erstellen Sie nur einen Clone des Storage-Spiegels und versuchen, aus diesem Clone die benötigten virtuellen Maschinen zu starten. Damit es zu keinen IP-Adressen-Konflikten kommen kann, hängen Sie die gestarteten VMs in ein isoliertes Netz. So kann mit Hilfe der VM-Konsole im vSphere-Client auch in den VMs gearbeitet werden.

Den Test eines Recovery-Plans können Sie also auch dafür nutzen, kurzzeitig eine Testumgebung bereitzustellen. Diese basiert dann auf einem Datenbestand der Produktion zum Zeitpunkt der letzten Replikation, aber Sie können Tests an einer mit der Produktion fast identischen Umgebung durchführen. Dies wäre zum Beispiel vor einem größeren Patch-Vorgang interessant. Durch das Aktivieren eines Test-Recovery-Plans wird die sekundäre Seite isoliert gestartet. Jetzt können Sie dort die gewünschten Tests durchführen, ohne dass die produktive Landschaft beeinträchtigt wird. Am Ende löschen Sie die Testumgebung wieder. Auf dem Speichersystem wird dafür nur der Platz für die Änderungen der Storage-Daten benötigt, denn es darf auf dem Spiegel nur gelesen werden! Einzig die Änderungen werden in den Snapshot-Bereich geschrieben, der Plattenplatz wird nach dem Abschluss der Tests wieder freigegeben.

A.4.8 Der Desasterfall

Der SRM erkennt einen Desasterfall nicht automatisch, aber die Bereitstellung eines passenden Recovery-Plans erleichtert dem Administrator das Umschalten oder Neustarten der IT-Landschaft wesentlich. So muss anstelle der manuellen Arbeit nur noch das Desaster von einer autorisierten Instanz im Unternehmen erklärt werden. Dann kann der Administrator den Recovery-Prozess mit Hilfe des entsprechenden Plans starten. Wenn der Wunsch besteht, kann die Abwicklung des Recovery-Plans auch automatisch erfolgen.

Der grundlegende Ablauf ist also immer identisch: Zuerst wird das Desaster erklärt, dann startet der Recovery-Vorgang durch den Administrator. Jetzt übernimmt der SRM, entsprechend dem vorher erstellten Plan, die Wiederherstellung. Dabei kann der Administrator Schritt für

Schritt mitverfolgen, welche Aktion gerade durchgeführt wird – Herunterfahren der eventuell noch laufenden virtuellen Maschinen auf der primären Seite, Herunterfahren von eventuell vorhandenen und nichtkritischen virtuellen Maschinen auf der Recovery-Site; Aufbrechen der Replikation und Anbindung des Speichers an die ESX-Hosts auf der sekundären Seite. Anschließend werden die festgelegten virtuellen Server in der definierten Reihenfolge gestartet, bis alle benötigten Dienste wieder zur Verfügung stehen.

A.4.9 Neuerungen in SRM 5

Die Version 5 des Site Recovery Managers ist nach dem Release von vSphere 5 erschienen. Bei dieser Version stand nicht nur Kompatibilität mit vSphere 5 im Vordergrund, sondern auch die Erweiterung um zusätzliche Funktionen.

Zuallererst stellt VMware jetzt zwei unterschiedliche Versionen des SRM zur Verfügung: eine Standard- und eine Enterprise-Version. Die beiden Versionen unterscheiden sich nur durch die Anzahl der VMs, die geschützt werden können. Die Enterprise-Version hat hier keinerlei Einschränkungen, bei der Standard-Version werden pro Site und SRM Instanz nur 75 virtuelle Maschinen unterstützt.

Durch die Implementierung einer eigenen Replikations-Engine ist der SRM-Nutzer nicht mehr nur auf Storage angewiesen, der in der Supportliste des SRM steht. Es können nun über die eigene Funktion Replikationen eingerichtet werden. Das funktioniert selbstverständlich für alle von vSphere unterstützen Devices, egal, ob es sich um gesharten oder um lokalen Storage handelt. Der RPO kann dabei flexibel eingestellt werden zwischen 15 Minuten und 24 Stunden.

Eine Funktion, die bei den Anwendern ganz oben auf der Liste stand, hat auch ihren Weg in das aktuelle Release gefunden. Es handelt sich um den automatischen Failback, also der Weg zurück in das Original-Rechenzentrum nach Behebung des Fehlers. Hier müssen keine Konfigurationsorgien für den Rückweg durchgeführt werden.

Ein Workflow für die geplante Durchführung der Arbeiten ist ebenfalls in Version 5 eingeflossen. Hier lassen sich alle Aktionen genau festlegen, damit Sie beim Übergang auf die jeweils andere Seite keinen Datenverlust erleiden. Des Weiteren die unterschiedlichen Konfigurationsfenster verbessert worden, damit der SRM sich leichter konfigurieren lässt.

A.4.10 Anmerkungen

Der Site Recovery Manager ist ein interessantes Produkt für die Realisierung von DR-Konzepten mittels Replikation auf Storage-Ebene. Die Hauptkosten entstehen durch die Anbindungen zwischen den beiden Standorten und Bereitstellung der Hardware und Software auf der zweiten Seite. Da der SRM aber nicht nur im Desasterfall genutzt werden kann, sondern auch bei anderen Anforderungen wie z. B. der Bereitstellung einer produktionsnahen Testumgebung,

nutzt er die zweite Umgebung auch aktiv. Außerdem darf und kann die zweite Seite auch für produktive virtuelle Maschinen verwendet werden. Damit nutzen Sie die Ressourcen effektiver.

Sollen wir Sie neugierig gemacht haben und möchten Sie sich näher mit dem Thema auseinandersetzen, dann können wir Ihnen das Buch von Mike Laverick zum Thema SRM empfehlen. Für die Version 4 ist es frei herunterladbar unter:

http://www.lulu.com/items/volume_71/11468000/11468233/1/print/8538123_colour_pages_inside.pdf

Für die Version 5 ist das Buch kostenpflichtig.

Sicherheitskonzepte virtueller und physischer Umgebung sind ein unerlässlicher Bestandteil der operativen Betriebssicherheit.

B VMware-vShield-Zones-Produktfamilie

Autor dieses Kapitels ist Stephan Bohnengel, VMware Global Inc., sbohnengel@vmware.com

In diesem Kapitel erläutern wir das Prinzip, den Nutzen und die Einsatzgebiete virtueller Firewalls am Beispiel der VMware-vShield-Zones-Produktfamilie in der Version 5.

B.1 Einleitung

Virtualisierungssicherheit der Plattform und die Isolierung der darauf befindlichen Cloud-Mandanten sind von großer Bedeutung für VMware, da das Unternehmen Hybrid-Cloud-Lösungen anbietet. Die größte Sorge der IT-Entscheider im Umgang mit Public-Cloud-Lösungen betrifft dabei immer die Datensicherheit. Dies zeigen viele Umfragen. Deshalb hat VMware hier ein massives Investment getätigt, um eigene Lösungen wie die vShield-Produktfamilie auf den Markt zu bringen und Lösungen von Partner-Softwareherstellern zu fördern.

Eine wesentliche Aufgabe im Security-Umfeld ist die Klassifizierung von Daten und damit die Bestimmung des Schutzbedarfs der VM, auf der sich die Daten befinden. Jeder von uns kennt dies. Dies kann je nach Firma und Anwendungsfall unterschiedliche Ausprägungen haben. Häufig sind Zertifizierungen zur Einhaltung rechtlicher Regularien, die durch Audits überprüft werden, und Haftbarkeit wesentliche Motivationsfaktoren, um personelle Verantwortlichkeiten und Sicherheitsrichtlinien innerhalb des Unternehmens zu definieren.

Diese Sicherheitsrichtlinien werden mittels eines Sicherheitskonzeptes unter Verwendung von Sicherheitsmaßnahmen umgesetzt. Dabei ist eine Risikoanalyse eine wichtige Grundvoraussetzung, um Restrisiken monetär zu bewerten und den Kosten einer neuen Sicherheitsmaßnahme gegenüberzustellen.

Ein Sicherheitskonzept folgt oft dem Zwiebelprinzip, also einem mehrschichtigen Ansatz, wie z. B. der Perimeterschutz durch Firewalls, interne Firewalls, IDS/IPS-Systeme und Maßnahmen auf VM-Ebene wie Antivirus mit Root-Kit-Detection sowie das Schließen von Sicherheitslücken des Gastbetriebssystems und dessen Applikationen mittels Patches. Überwindet ein

potentieller Angreifer eine Sicherheitsmaßnahme, können eventuell andere Schichten des Konzeptes den Angriff abmildern oder abfangen, um die Auswirkungen zu beschränken.

In den verschiedenen Compliance-Regularien wie ISO 27001/27002, an das sich auch der BSI-Grundschutz (Bundesamt für Sicherheit in der Informationstechnik) anlehnt, wird auch die Verwendung eines ITSM (IT Service Management) vorgeschrieben. Dort geht es unter anderem um das Change-Monitoring und die Änderungskontrolle. Virtuelle Sicherheit ist heute und in Zukunft ein sehr wichtiges Thema, dem sich VMware-Partner und VMware-Endkunden widmen müssen. Bei ITSM geht es vor allem um Prozesse und die Minimierung von Ausfallzeiten durch menschliches Versagen bei Änderungen im Rechenzentrum. Verfügbarkeit der Systeme ist ein wichtiger Unterpunkt der IT-Sicherheit im Allgemeinen.

Warum führe ich das bei dem Thema vShield an? Ganz einfach, weil sich viele Kunden berechtigterweise fragen: Was ändert Virtualisierung an meinen bestehenden Sicherheitskonzepten? Die Antwort lautet: Im Grunde genommen nicht viel; Sie müssen eine VM genauso patchen und gegen Viren schützen wie ihr physisches Pendant. Die meisten Fehler im IT-Betrieb entstehen durch fehlende Automatisierung, die menschliche Fehler vermeiden könnte, sowie die fehlende Implementierung von Prozessen, die definieren, was bei Änderungen zu tun ist. Oder mit den Worten von Neil MacDonald, einem renommierten Analysten bei Gartner im IT-Sicherheits-Research-Team: »Like their physical counterparts, most security vulnerabilities will be introduced through misconfiguration and mismanagement.« Es dürfte an dieser Stelle klar sein, dass nicht die Einführung von innovativen Technologien an sich – wie z. B. die Virtualisierung – das größte Risiko darstellt. Ihnen sollte immer bewusst sein, dass Fehlkonfiguration und Missmanagement das größte Einfalltor für Sicherheitslücken bilden.

Enterprise-Management-Tools wie der in Abschnitt A beschriebene VMware Configuration Manager schaffen hier Abhilfe, weil Sie Ihnen eine bessere Übersicht durch Berichte und Alarmierungen liefern. Vor allem helfen Sie bei Audits und bieten eine Änderungskontrolle für Administratoren. Sie finden hier auch *Compliance Dashboards*, mit denen Härtungsmaßnahmen von VMs gegen Auditierungsstandards wie ISO 27001 in ihrer Wirkung überprüft werden können.

Weitere positive Effekte lassen sich durch eine Automatisierung der Netzwerksicherheit erzielen. Beim Erstellen einer VM können die Firewall-Regeln für einen auszurollenden neuen Dienst im Rechenzentrum automatisch erstellt werden. Dies vermeidet Fehlkonfigurationen. Darüber hinaus ist ein Schutz durch Netzwerksegmentierung für die VM so wesentlich effektiver als durch die Übergabe des Change Request an das Sicherheitsteam. Dieses hätte ansonsten die zeitintensive Aufgabe, die erforderlichen Regeln oder die Einordnung in die Netzwerkzone manuell vorzunehmen.

Die Netzwerkisolierung unterschiedlicher Schutzbedarfsklassen durch Netzwerksegmentierung innerhalb des Rechenzentrums ist eine wesentliche Maßnahme. Man spricht hier auch von *Mikrosegmentierung*. Dies kann z. B. im Unternehmensumfeld das Abschotten der hochsensiblen Entwicklungsabteilung sein oder im Cloud-Umfeld die sichere Isolation der Man-

danten untereinander sein. Konzepte für virtuelle Firewalls bieten eine sehr gute Möglichkeit, Spezialhardware der Firewall-Hersteller einzusparen. Zudem besteht ein wesentlicher Vorteil darin, dass sich der Netzwerkdatenverkehr für die interne Netzwerksegmentierung drastisch reduziert. Dieser muss nicht mehr zu einem dedizierten physischen Firewall-Cluster gesendet werden, sondern wird bereits innerhalb des physischen ESX-Hosts inspiziert, ohne Netzwerkbandbreite in Anspruch zu nehmen. Dies wird durch die VMware VMsafeAPI möglich.

Konzepte für virtuelle Firewalls unterschiedlicher Hersteller haben mitunter unterschiedliche architektonische Ausprägungen. Generell kann man virtuelle Firewalls grob in verschiedene Kategorien unterteilen:

- auf Portgroups basierende Firewalls
- Layer-3-Gateway-Firewalls
- VMware-Kernel-Modul-Firewalls unter Verwendung der VMsafe API oder Cisco vPath

Hierbei arbeitet VMware mit namhaften Sicherheitsherstellern im Rahmen des VMsafe-Programms wie z. B. Cisco, Checkpoint, Trend Micro, Symantec, McAfee, Kasperski, Sophos, HP, IBM, Sourcefire etc. zusammen. Um die VMware-vShield-Produktfamilie zu verstehen, müssen Sie sich erst einmal mit der grundlegenden Architektur der VMware VMsafe API vertraut machen, einer Schnittstelle, die VMware führenden Sicherheitssoftwareherstellern an die Hand gegeben hat, damit diese Sicherheitsprodukte für den ESX Hypervisor auf den Markt bringen können.

Aktuelle Informationen zum VMSafe-Programm finden Sie unter:

http://www.vmware.com/technical-resources/security/vmsafe/security_technology.html

B.2 VMsafe-API

B.2.1 EPSEC-API

Die VMware VMsafe-API enthält die sogenannte EPSEC-API, die zum Scannen von Dateien innerhalb von VMs benutzt werden kann. Einsatzgebiet ist hier das *Antivirus Scan Offloading*, bei dem innerhalb des Gastes nur noch ein Thin-Agent installiert werden muss, nicht mehr ein vollwertiger Antiviren-Agent. Ein weiteres potentielles Einsatzgebiet stellen DLP-(Data Loss Prevention-)Lösungen dar. Der Thin-Agent kommt aus dem Hause VMware, ist auch als Bestandteil der VMware Tools erhältlich und umfasst nur wenige 100 KBytes. Der wesentliche Vorteil dieser Architektur besteht darin, dass z. B. im Antivirus-Bereich Real-Time-Scans und geplante Scans nicht mehr auf jedem einzelnen Gast durchgeführt werden müssen, sondern durch eine spezielle Sicherheits-VM eines Antivirus-Drittanbieters auf dem ESX-Host durchgeführt werden.

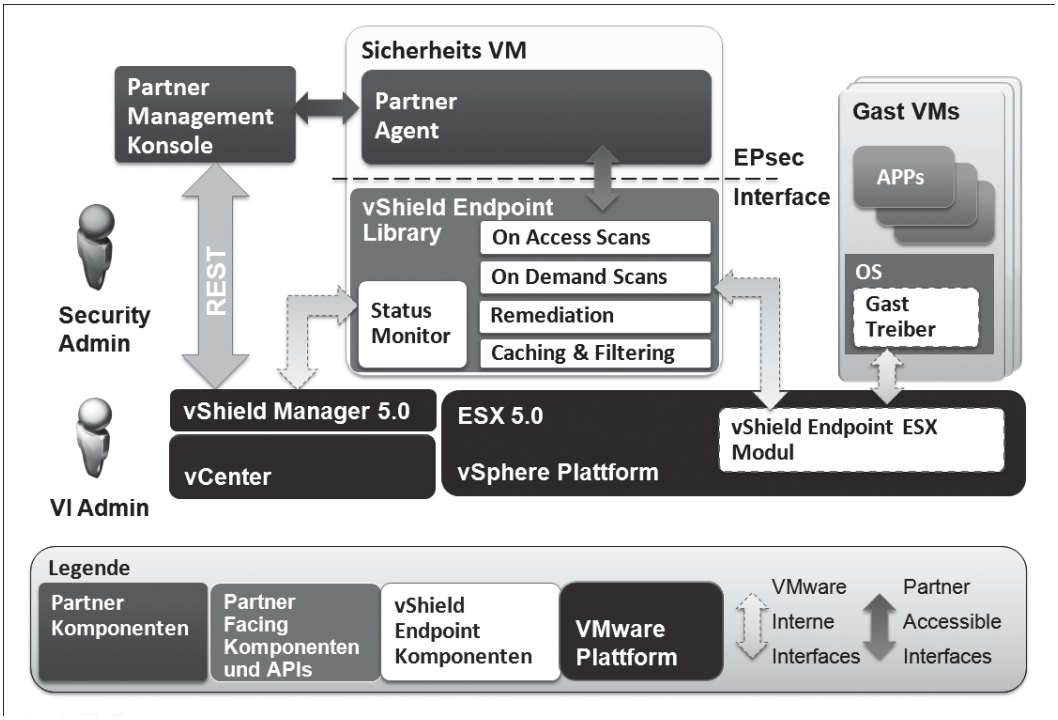


Abbildung B.1 EPSEC-Architektur

Durch Cache-Mechanismen und das Abgreifen der Daten durch das VDDK (VMware Disk Development Kit) direkt am Hypervisor mit Hilfe eines Kernel-Moduls schont dieses Modell Ressourcen. Damit kann eine Verbesserung der Konsolidierungsrate am ESX-Server erreicht werden. Dies haben auch Partneranalysen gezeigt.

Ein netter Nebeneffekt ist, dass sich durch das Fehlen eines kompletten Antivirus-Agenten die Gastbetriebssystem-Images verkleinern. Bei Migrationen wie z. B. dem Wechsel des Antivirus-Anbieters müssen keine Agenten getauscht werden. Zudem kann eine potentielle Schadsoftware nicht mehr versuchen, den Wächter innerhalb des Gast-OS auszuschalten, da diese eine Ebene darunter über den Hypervisor Dateizugriffe und Änderungen abgreift und diese an den Partner-Agenten innerhalb der Sicherheits-VM leitet. Pattern-Updates der Antivirus-Hersteller müssen nur einmal pro ESX-Host heruntergeladen und installiert werden. Dies schont die I/O-Ressourcen zum SAN, die aus Erfahrung bei klassischen Antivirus-Agenten zu massiven Performanceeinbußen im Storage-Bereich führen können, wenn z. B. bei VMware View 5.000 Antivirus-Agenten gleichzeitig das Pattern-Update installieren und damit die Storage-Systeme regelrecht in die Knie zwingen. Dies muss nicht der Fall sein, wenn der Antivirus-Hersteller die Pattern seriell installiert.

B.2.2 NetSec-API

Die NetSec-Komponente der VMsafe-API dient zum Scannen von Netzwerkverkehr auf dem ESX-Host. Damit können Intrusion-Detection-Systeme und Intrusion-Prevention-Systeme, aber natürlich auch virtuelle Firewall-Systeme von der VMware-VMsafe-Schnittstelle profitieren.

Bei Verwendung dieser Architektur wird wie in Abbildung B.2 dargestellt eine Sicherheits-VM pro ESX-Host installiert; auf jedem ESX 5.0-Server wird das NetSec-(dvFilter-)Modul installiert. Dieses sitzt nun im Netzwerkpfad mit den Data-Path-Agents zwischen virtueller Netzwerkkarte (vNic) und dem vSwitch-Port. Sämtlicher Netzwerkverkehr wird damit sichtbar und an die Sicherheits-VM des jeweiligen Hosts zur Überprüfung gesandt. Da diese Kommunikation lokal auf dem jeweiligen ESX-Server stattfindet, wird durch die Überprüfung nicht das LAN des Rechenzentrums beansprucht. Der Verkehr wird innerhalb des ESX-Servers über den physischen Server-Bus gehandhabt. Befinden sich virtuelle Maschinen, wie in der Abbildung dargestellt, auf dem gleichen ESX-Host in der gleichen Portgruppe und damit am gleichen VLAN, würde eine physische Sicherheitsmaßnahme bösartigen Verkehr gar nicht erkennen, da dieser Netzwerkverkehr den ESX-Host nicht verlässt. Sie hätten sozusagen einen potentiellen toten Winkel, auch *Blind Spot* genannt, den Sie beim Design der Sicherheitsmaßnahmen für virtuelle Umgebungen berücksichtigen müssen. Diese Sicherheitslücke könnten Sie durch eine Maßnahme, die die VMsafe-Schnittstelle verwendet, schließen. Die einzige aktuelle Ausnahme mit einem ähnlichen Effekt stellt das Cisco VSG (Virtual Security Gateway) dar, das in Verbindung mit dem Cisco-Nexus-1000v-Software-Switch und dem vPath-Modul das Gleiche erreicht.

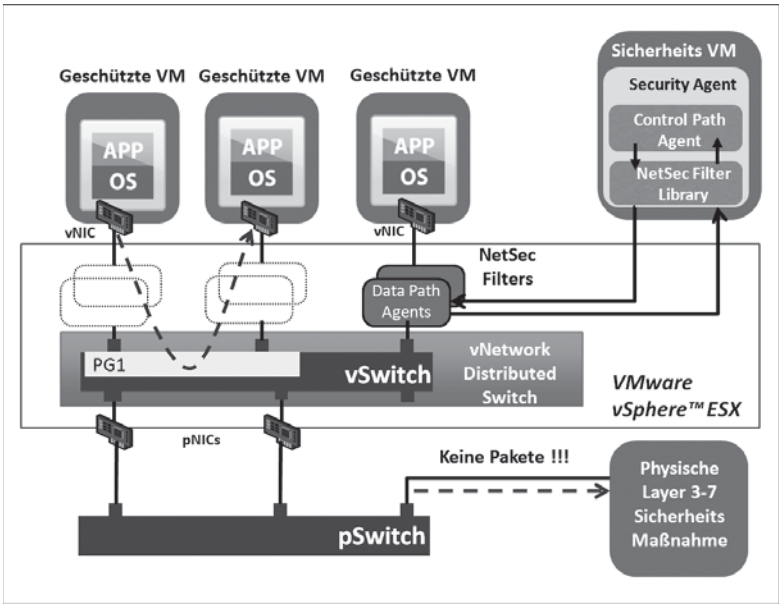


Abbildung B.2 NetSec-Architektur – Beispiel von Blind Spots

Hinzu kommt, dass sich Software-Firewalls schneller ausrollen lassen als physische, da sie nicht bestellt und auch nicht eingebaut werden müssen. Im Gegensatz zu klassischen physischen Firewall-Clustern vermindern sie große Teile Netzwerkverkehr durch Introspektion auf dem jeweiligen physischen Server. Die virtuelle Firewall muss nämlich nicht den kompletten Verkehr aller VMs überprüfen, sondern nur den Verkehr der jeweiligen VMs, die der ESX-Host zum entsprechenden Zeitpunkt beherbergt.

Wächst das Datacenter stark, stellt der physische Firewall-Cluster unter Umständen auch einen potentiellen Performance-Engpass dar, da er für einen bestimmten Netzwerkdurchsatz beschafft wurde und nicht horizontal mit den steigenden Anforderungen mitwächst. Ein Konzept mit virtuellen, verteilten Firewalls hingegen skaliert mit der Umgebung, da man die Scan-Aufgaben auf die jeweilige Sicherheits-VM pro ESX-Host portioniert.

Vorteile virtueller Sicherheitslösungen unter Verwendung von VMware VMsafe

Virtuelle Sicherheitslösungen bieten Ihnen wichtige Vorteile. Sie

- eliminieren Blind Spots am ESX-Host,
- skalieren durch den verteilten Ansatz mit der Umgebung horizontal mit,
- verhindern Performanceengpässe,
- lassen sich schnell ausrollen,
- benötigen keine Spezialhardware.

B.3 Die einzelnen vShield-Komponenten

Zur Drucklegung der vorliegenden Auflage (März 2012) besteht die vShield 5.0-Produktfamilie aus folgenden Komponenten, die Sie unabhängig voneinander beziehen können:

- vShield Manager – kostenfrei
- vShield App – lizenziert pro VM (alle VMs im Cluster)
- vShield App with Sensitive Data Discovery (SDS)
- vShield Edge – lizenziert pro VM (VMs hinter dem Edge Device)
- vShield Endpoint – lizenziert pro VM (alle VMs, die den Thin-Agent installiert haben)
- vShield Zones – kostenfreie Variante, ab vSphere Standard ist eine Produktlizenz enthalten (basiert auf vShield App 1.0 und verwendet nicht VMSafe). Diese Variante ist eine auf *portgroup* basierende Firewall – sie eliminiert unter Umständen keine *Blind Spots* auf dem ESX Host.)

In den nächsten Abschnitten sehen Sie genauer, was sich hinter den Produktnamen verbirgt.

B.3.1 vShield Manager (VSM)

Der vShield Manager (VSM) hat die Funktion des zentralen Managements und wird wie auch die anderen virtuellen Firewalls im Format einer virtuellen Appliance ausgeliefert. Er verteilt das Firewall-Regelwerk auf die ihm unterstellten anderen virtuellen Firewalls. Dies können vShield-App- und vShield-Edge-Firewalls sein. Die Administration erfolgt mittels Webinterface via HTTPS oder vSphere-Client-Plugin. Der vShield Manager kann aber auch über eine REST-API oder vSphere Power CLI (Powershell) von außen programmiert werden, so dass sich die Regelerstellungen, -änderungen oder -löschungen auch in Workflows integrieren lassen.

Damit kann die Firewall-Lösung durch andere VMware-Produkte wie den vCloud Director, den VMware Orchestrator oder den VMware Request Manager programmiert und gesteuert werden. Dies ermöglicht eine vollständige Automatisierung der Sicherheitskonfiguration durch höhere Applikationsschichten.

Der vCloud Director macht dies schon im Auslieferungszustand, Mandanten werden z. B. durch vollautomatisches Ausrollen von vShield-Edge-Devices sicher voneinander separiert. Dies ist auch der Grund, warum vShield Edge lizenztechnisch bereits mit dem vCloud Direktor mit minimiertem Funktionsumfang gebündelt ist.

B.3.2 Installation

Die Installation der Produktfamilie ist einfach zu handhaben:

1. Laden Sie den vShield Manager der virtuellen Appliance (OVA-Format) herunter.
2. Importieren Sie die OVA-Datei in das jeweilige vCenter (es besteht eine 1:1-Beziehung zwischen VSM und vCenter).
3. Öffnen Sie die vSphere-Console, und konfigurieren Sie die Grundparameter; danach ist ein Reboot erforderlich; Standard-User »admin«, Passwort »default«.

Grundkonfiguration

```
login as: admin
admin@172.16.0.60's password: default
manager> enable
Password:
manager# setup

Use CTRL-D to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

IP Address (A.B.C.D): 172.16.0.60
Subnet Mask (A.B.C.D): 255.255.255.0
Default gateway (A.B.C.D): 172.16.0.254
Primary DNS IP (A.B.C.D): 172.16.0.10
```

```
Secondary DNS IP (A.B.C.D):
Warning: Secondary DNS not set.
DNS domain search list (space separated): vpod.local
Old configuration will be lost, and system needs to be rebooted
Do you want to save new configuration (y/[n]): y
Do you want to reboot now (y/[n]): y
```

4. Ändern Sie nach Inbetriebnahme die Passwörter der CLIs (normaler und Expertenmodus).

Aus Sicherheitsgründen verpflichtend:

```
manager login: admin
password:
manager> enable (Notiz: priviligierten Modus aktivieren)
password:
manager# configure terminal (Notiz: Konfigurationsmodus an)
```

- Fügen sie einen neuen Benutzer hinzu. Dieses Beispiel erstellt den User »vshield« mit dem Passwort »vmware1!«.

```
manager(config)# user vshield password plaintext vmware1!
manager(config)# write memory (Notiz: Konfiguration speichern)

Building Configuration...
Configuration saved.
[OK]
```

- Geben Sie zweimal `exit` ein, um sich aus der CLI abzumelden:

```
manager(config)# exit
manager# exit
```

- Melden Sie sich nun noch einmal mit »vshield« an, um den Default-Admin-Account zu löschen. Wechseln Sie danach wieder in den privilegierten Modus, und aktivieren Sie den Konfigurationsmodus:

```
manager(config)# no user admin
```

- Um das Passwort des privilegierten Modus zu ändern, melden Sie sich im CLI an (nun mit »vshield« und »vmware1!«), wechseln in den privilegierten Modus und danach in den Konfigurationsmodus:

```
manager(config)# enable password abcd1234
manager(config)# write memory (Notiz: Konfiguration speichern)
manager(config)# exit
manager# exit
```

- Wichtig: Wenn Sie später mittels SSH dauerhaft auf die Konsole zugreifen müssen, dürfen Sie auf keinen Fall einen User namens »root« erstellen, da in der sshd_config »root«-Logins nicht erlaubt sind.

5. Die weitere Konfiguration erfolgt via Weboberfläche oder vSphere-Plugin (Login ist »Admin«, Passwort »default«).
   - Ändern Sie das Defaultpasswort auch hier.
   - Binden Sie das vCenter ein (legen Sie im vCenter einen Service-Account mit vollen Administratorberechtigungen für das vShield an).
   - Konfigurieren Sie die Zeitzone.
   - Konfigurieren Sie das vSphere-Plugin.

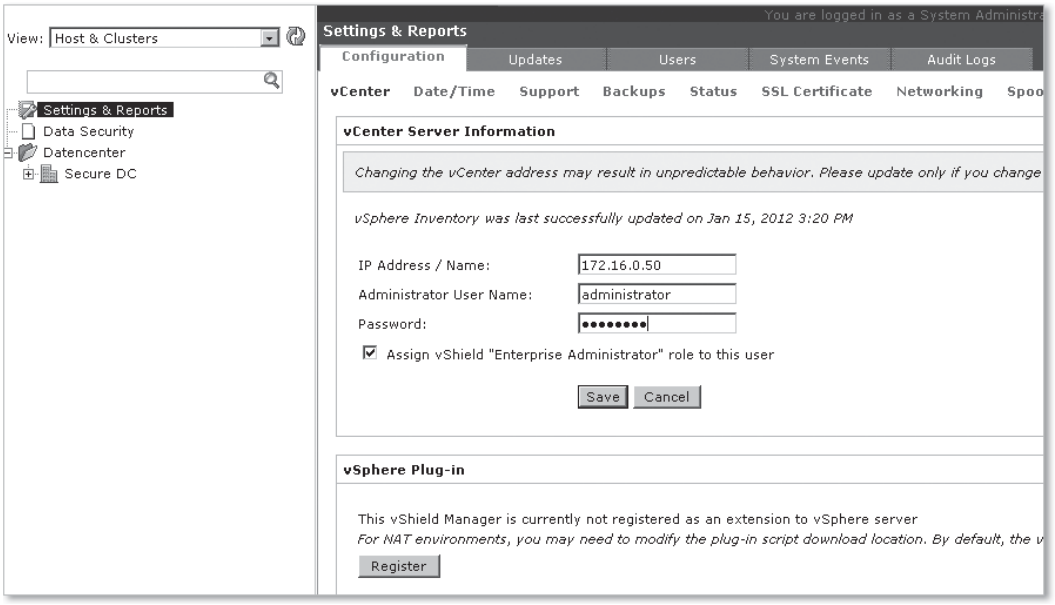


Abbildung B.3 Die vShield-Weboberfläche – Grundkonfiguration

6. Damit ist die Grundinstallation fast abgeschlossen; das vCenter wird kontaktiert, und die vSphere-Objekte werden mit denen des vShield Managers synchronisiert.
7. Fügen Sie vShield-Lizenzschlüssel im vCenter unter Lizenzierung hinzu, nicht im vShield Manager.

Der vShield Manager und die von ihm verwalteten virtuellen Firewalls installieren Sie am besten in das Managementnetzwerk-Segment, das wahrscheinlich bei größeren Unternehmen ein Sicherheitsabteilungsnetz sein dürfte.

Benötigte Netzwerkports vom und zum VSM

Bitte achten Sie darauf, dass die einzelnen vShield und VMware Management-Komponenten über die folgenden Netzwerkports miteinander kommunizieren können, und konfigurieren Sie eventuell vorhandene Netzwerk-ACLs und -Firewalls entsprechend:

- Zugriff auf ESX-Hosts: 902 TCP und 903 TCP
- REST-API: 80 TCP und 443 TCP, dies betrifft VMware Orchestrierungswerkzeuge, als auch Dritthersteller Management Konsolen
- GUI: 80 TCP und 443 TCP; diese Ports braucht auch der VSM, um die vCenter zu VSM-Kommunikation zu gewährleisten.
- SSH-Zugriff (falls gewünscht): 22/TCP

Alle weiteren Komponenten installieren Sie via Webinterface oder vSphere-Plugin. Bevor wir uns den Produkten vShield App und vShield Edge widmen und auf Design eingehen, noch ein Wort zu Benutzerrollen und Gewaltenteilung: Die Delegation von Benutzerrechten ist natürlich auch im vShield Manager möglich, und warum sollte ein vSphere-Infrastrukturadministrator in der Lage sein, Firewall-Regeln zu konfigurieren? Hier gibt es also keinen Unterschied zur alten physischen Welt.

Noch ein paar nützliche Tipps zum vShield-CLI

- Aktivieren Sie SSH, damit der Zugriff per vSphere-Client Konsolen–Umleitung entfällt. Diese hat den Charme eines deutschen Keyboardlayouts, wenn Sie mittels PuTTY darauf zugreifen.

```
manager#ssh start
Starting SSH Server…
manager# copy running-config startup-config
Building Configuration...
Configuration saved.
[OK]
```

- Der `list`-Befehl ist sinnvoll, um eine Übersicht über mögliche Kommandos zu erhalten. Der Befehl liefert unterschiedliche Ausgaben, je nachdem, in welchen Modus Sie sich befinden (normaler oder privilegierter Modus). Ein Auszug:

```
reset
show process (list|monitor)
show arp
show system memory
show log
show log last NUM
show log (follow|reverse)
write erase
show filesystems
show stacktrace
show ethernet
setup
show manager log
show manager log (follow|reverse|size)
show manager log last NUM
ssh (start|stop)
```

```
    show interface mgmt
    show slots
    show system log size
    purge log (manager|system)
    show interface
  manager# configure terminal
  manager(config)# list
    end
    exit
    hostname WORD
    interface mgmt
    ip route A.B.C.D/M A.B.C.D
    list
    web-manager
    no interface IFNAME
    no ip route A.B.C.D/M A.B.C.D
    no log syslog
    no user USERNAME
    user USERNAME password (hash|plaintext) PASSWD
    write memory
    reset
    enable password PASSWD
    no web-manager
```

- Überprüfen Sie das Management-Interface:

```
manager# show interface  mgmt
Interface mgmt is up, line protocol is up
  index 2 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:af:46:c1
  inet 172.16.112.96/24 broadcast 172.16.112.255
  Auto-duplex (Full), Auto-speed (1000Mb/s)
    input packets 7231493, bytes 2147483647, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 7865015, bytes 2147483647, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

B.3.3 Benutzerverwaltung

Der VSM hat eine lokale Benutzerdatenbank, kann aber auch auf Benutzer und Gruppen des verbundenen vCenter Servers zugreifen. Somit können Sie auch AD-Benutzern vShield-Rollen zuweisen. Es empfiehlt sich, eine eigene vShield-Admin-Rolle im Active Directory anzulegen, die Leserechte im vCenter bekommt. Der »admin«-User ist der einzige System-Administrator und kann nicht gelöscht werden, das heißt: Ändern Sie auf alle Fälle das Defaultpasswort.

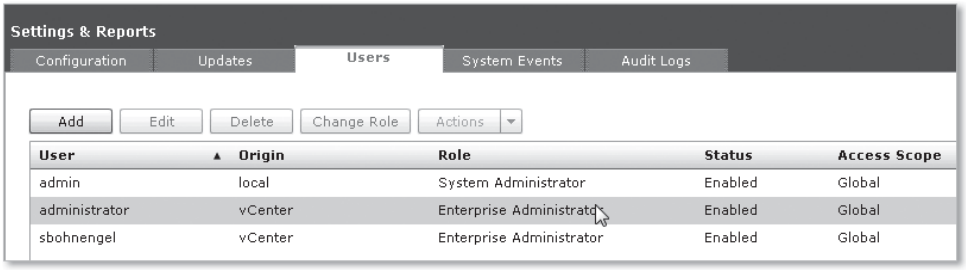


Abbildung B.4 Benutzerverwaltung in vShield

Abbildung B.5 zeigt, welche Rollen es im VSM gibt.

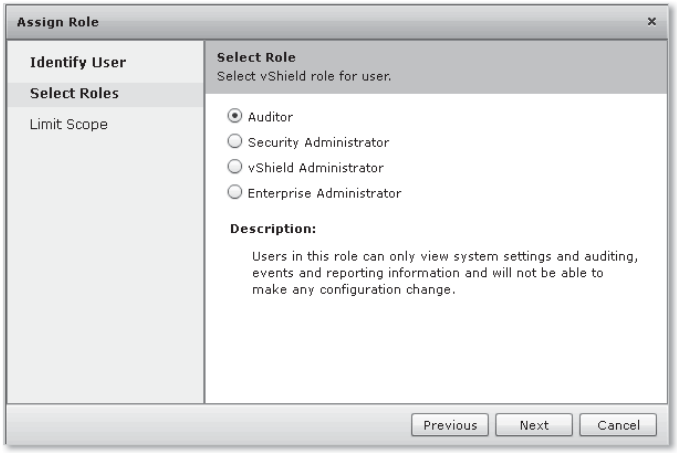


Abbildung B.5 vShield-Benutzerrollen

Als Enterprise-Administrator können Sie alle Änderungen im System vornehmen, also alle vShield-Produkte installieren und konfigurieren und die VSM-Grundeinstellungen administrieren. Dazu gehören auch Änderungen an der Firewall-Regelbasis. Als vShield-Administrator können Sie hingegen nur vShield-Komponenten ausrollen und verwalten. Sie können keine Regeln ändern. Dies wäre z. B. eine ideale Rolle für einen vSphere-Administrator. Zu seiner Standardaufgabe gehört es, Kernel-Module auf dem ESX-Server auszurollen, dort eine neue vShield-App-Instanz bereitzustellen, wenn ein neuer ESX-Server in den Cluster mit aufgenommen wird. Die Security-Administrator-Rolle hingegen verwaltet nur Sicherheitsregeln und deren Konfiguration, kann jedoch die globalen VSM-Einstellungen nicht ändern, wie das Verbinden zum vCenter. Die Auditor-Rolle hat nur Leseberechtigungen und darf nichts ändern.

Der Verwaltungsbereich kann wie in Abbildung B.4 dargestellt entweder global erfolgen, was für Enterprise- und vShield-Administratoren ohnehin gilt, aber auch auf Objektebene im vCenter weiter heruntergebrochen werden. Haben Sie mehrere Datacenter und Netzwerke, können Sie Rechte auf diese Objekte für Security-Administratoren und Auditors vergeben, so

dass ein Kollege z. B. für die Regelerstellung im vCenter-Objekt Datacenter A zuständig ist, während sein Kollege Datacenter B betreut.

B.3.4 Backup und Betriebshandhabung

Den VSM sollten Sie unbedingt regelmäßig sichern. Dazu verfügt der VSM über einen Backup-Reiter, aber auch durch REST-API Aufrufe lassen sich Regeln sichern und wiederherstellen. Der VSM protokolliert bei Bedarf Aktionen, und diese Log-Dateien lassen sich via Web-GUI oder Command-Line auswerten.

Der VSM kann außerdem problemlos vollautomatisch in einem DRS-Cluster verschoben werden, dies gilt auch für vShield Edge, nicht aber für vShield App.

Wichtig

Zur Drucklegung der vorliegenden Auflage (März 2012) empfiehlt VMware, den vShield Manager und auch das vCenter in einen gemeinsamen Management-Cluster zu installieren. Dieser wird losgelöst von der zu schützenden Umgebung von einem Ressourcen-Cluster betrieben. Er wird nicht von vShield selbst geschützt. Dadurch vermeiden Sie, dass durch die Fehlkonfiguration der vShield Komponenten die Management-Kommunikation an sich verhindert wird.

B.4 vShield App

Nachdem wir uns eingehend mit dem Manager beschäftigt haben, nun detaillierte Informationen zu vShield App, der VMsafe-Firewall von VMware, die *Blind Spots* am ESX-Server verhindern kann.

vShield App ist eine Stateful-Inspection-Firewall, die auch über eine gewisse Protokollinspektionsintelligenz verfügt, es ist jedoch keine Application-Level-Firewall oder eine Web-Application-Firewall. Prinzipiell arbeitet sie bis OSI-Layer 4. Sie können sie in zwei Ausprägungen beziehen, mit oder ohne Sensitive Data Discovery (SDS). Sensitive Data Discovery erfordert die zusätzliche Installation der vShield-Endpoint-Module über den vShield Manager.

B.4.1 Installation

Die Installation erfolgt über die Web-Console, die REST-API oder vSphere CLI. Pro ESX-Server wird eine vShield-App-Appliance benötigt, in Abbildung B.7 sehen wir vier ESX-Server und demzufolge auch vier vShield-App-Appliances. Die Installation erfolgt hierbei ohne Wartungsfenster für die virtuellen Maschinen vollkommen transparent. Jede vShield-App-Instanz benötigt 2 vCPUs und 2 GB RAM. Haben Sie diesen Schritt für jeden Host erledigt, werden pro VM in deren VMX-Dateien die VMSafe-API-Einträge automatisch eingefügt. Damit sitzt die virtuelle Appliance im Netzwerk-I/O-Pfad der VM.

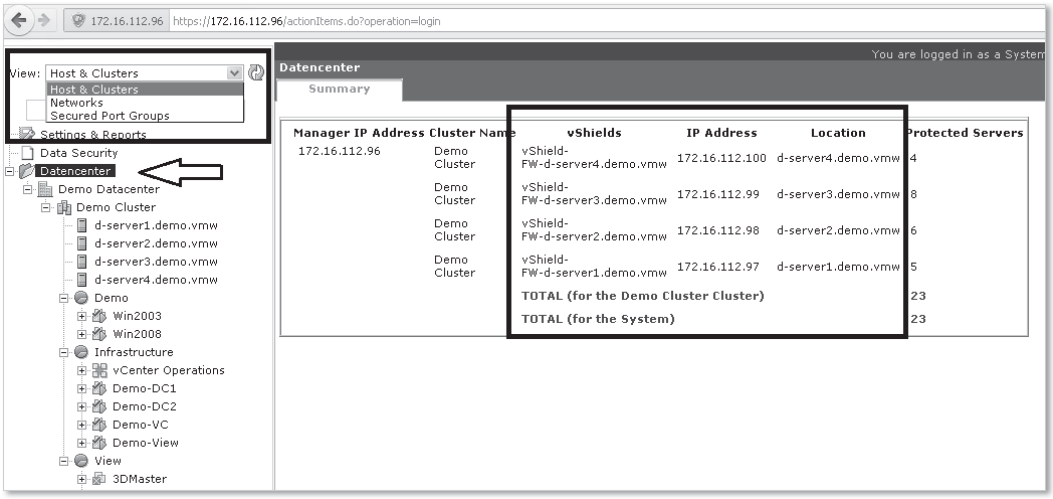


Abbildung B.6 Übersicht über verwaltete vShield-App-Instanzen und ihre Management-IP-Adressen

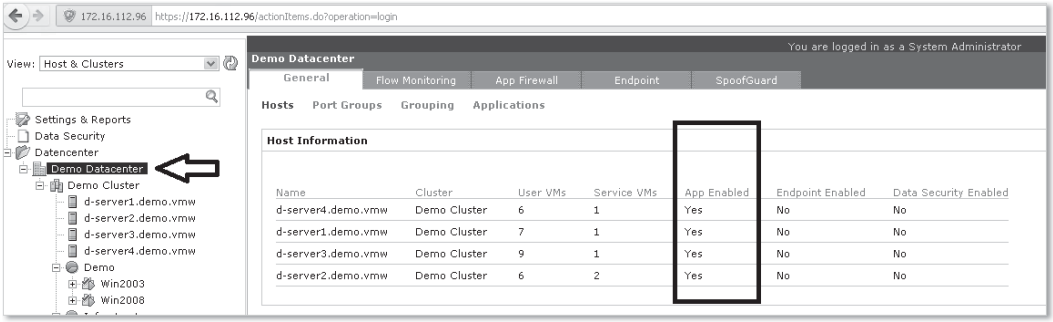


Abbildung B.7 Übersicht über eingeschaltete vShield-Komponenten im vShield-Web-GUI

Die Übersicht in Abbildung B.7 gibt Aufschluss darüber, ob vShield App installiert ist und wie viele Service-VMs sich auf dem jeweiligen ESX-Server befinden. Zu Service-VMs zählen natürlich auch andere Appliances wie der VSM oder vShield-Edge-Appliances. Auf der linken Seite sehen Sie die Grobansicht der vCenter-Objekte, die der VSM regelmäßig mit dem vCenter lesend synchronisiert. Auf der rechten Seite befindet sich die Detailansicht zu der jeweils im linken Bereich markierten Entität.

Bei der Installation müssen Sie eine Management-Interface-IP für das vShield angeben, die im gleichen Management-Segment liegen sollte wie die des VSM. Über dieses Interface empfängt das vShield Updates seines Managers und lässt sich auch zentral verwalten. Ist die Appliance erst einmal installiert, können Sie wie in Abbildung B.7 dargestellt einen Überblick über den Host-Preparation-Status gewinnen, um eventuell Module hinzuzufügen oder zu entfernen. Man bekommt einen Auslastungsgrad angezeigt haben auch die Möglichkeit, die Appliances

neu zu starten oder eine Synchronisation mit dem VSM zu erzwingen. Es lässt sich auch das Log-Level für bis zu drei Syslog-Server konfigurieren.

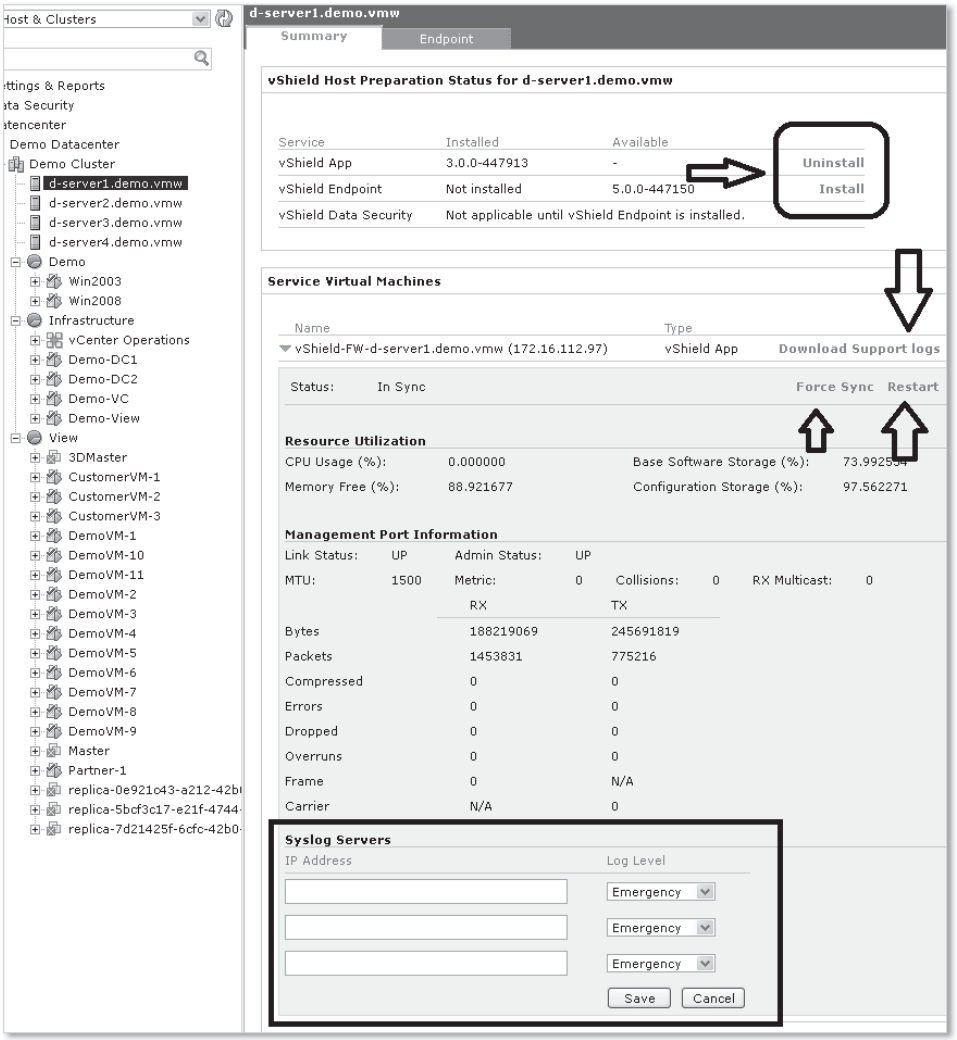


Abbildung B.8 Übersicht der vShield-App-Appliance nach der Installation

B.4.2 Überlegungen zum Betrieb

Die vShield-App-Appliances dürfen Sie nicht mittels DRS zwischen einzelnen ESX-Servern migrieren, und Sie müssen sie deshalb auch vom DRS ausschließen. Dies wird bereits von der automatischen Installationsprozedur konfiguriert. Deshalb können Sie durchaus die vShield-App-Komponente auf das lokale VMFS-Volume der ESX-Server installieren. Wird der ESX-Host gewartet und benötigt er einen Reboot, ist die vShield-App-VM die letzte VM, die am

Host heruntergefahren wird, und umgekehrt die erste, die nach dem Reboot des Hosts wieder gestartet wird.

Es empfiehlt sich deshalb, wie in Abbildung B.9 die vShield-App-Komponente in die automatische Start- und Shutdown-Sequenz der VMs aufzunehmen.

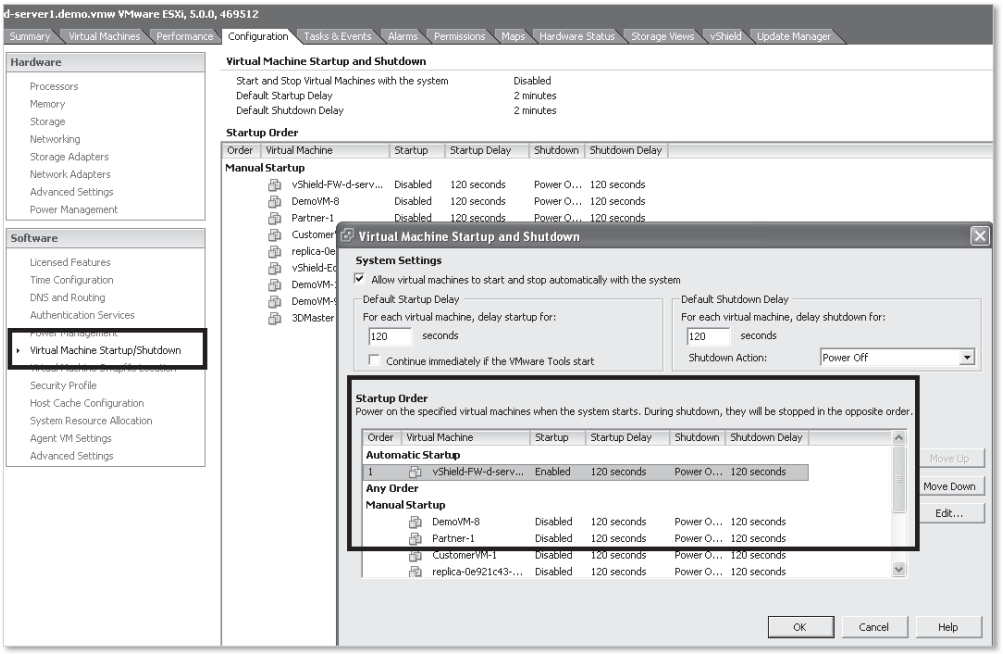


Abbildung B.9 vShield-App-VM in den automatischen Start einbeziehen

Alle ESX-Server müssen mit einer vShield App ausgestattet werden. Wird eine VM mittels DRS auf einen Host migriert, auf der sich keine vShield-App-VM befindet, konfiguriert das vCenter die VMSafe-Einträge aus der Konfigurationsdatei (**.vmx*) heraus, so dass die Maschine nach wie vor erreichbar bleibt. Jedoch ist damit kein Firewall-Schutz mehr durch vShield App gewährleistet.

Hätte die Firewall eine Kernel-Panic, könnten die VMs auf dem ESX-Host nicht mehr nach außen kommunizieren. Dies wird auch als *Fail-Close* bezeichnet. Dies ist kein Unterschied zu einer physischen Firewall-Maßnahme, die auch im Fail-Close arbeitet. In einem solchen Fall sind jedoch nur die VMs des jeweiligen Hosts betroffen, und eine Kernel-Panic kann so konfiguriert werden, dass sie mittels HA-VM-Monitoring über die installierten VMware Tools erkannt wird, was sofort zum Neustart der virtuellen Appliance führt.

Empfehlenswert ist auch das Einrichten von vCenter-Alarmen speziell für Infrastrukturmaschinen wie vShield App. Denkbar wären Alarm-Trigger wie VM-Heartbeat, die, bei Kommunikationsproblemen in einem Neustart münden. So können Sie VM-Heartbeat-Monitoring betreiben, auch ohne dies am Cluster-Level einschalten zu müssen.

B.4.3 Regelbasis und Funktionen von vShield App

Die Regelbasis von vShield funktioniert wie die einer jeden anderen Firewall. Sogenannte Fünf-Tupel-Regeln bestehen aus Netzwerkquelladresse, Quell-Port, Netzwerkzieladresse, Ziel-Port und Aktionen. Auch hier wird die Firewall-Regelbasis von oben nach unten abgearbeitet, und die Verarbeitung ist bei der ersten zutreffenden Regel für das Paket beendet. Regeln lassen sich bei Bedarf mitprotokollieren und können zu Troubleshooting-Zwecken aktiviert und deaktiviert werden. Wie in Abbildung B.10 dargestellt unterteilt man die Regeln in OSI Layer 3 oder OSI Layer 2 Regeln auf MAC-Adressen-Basis.

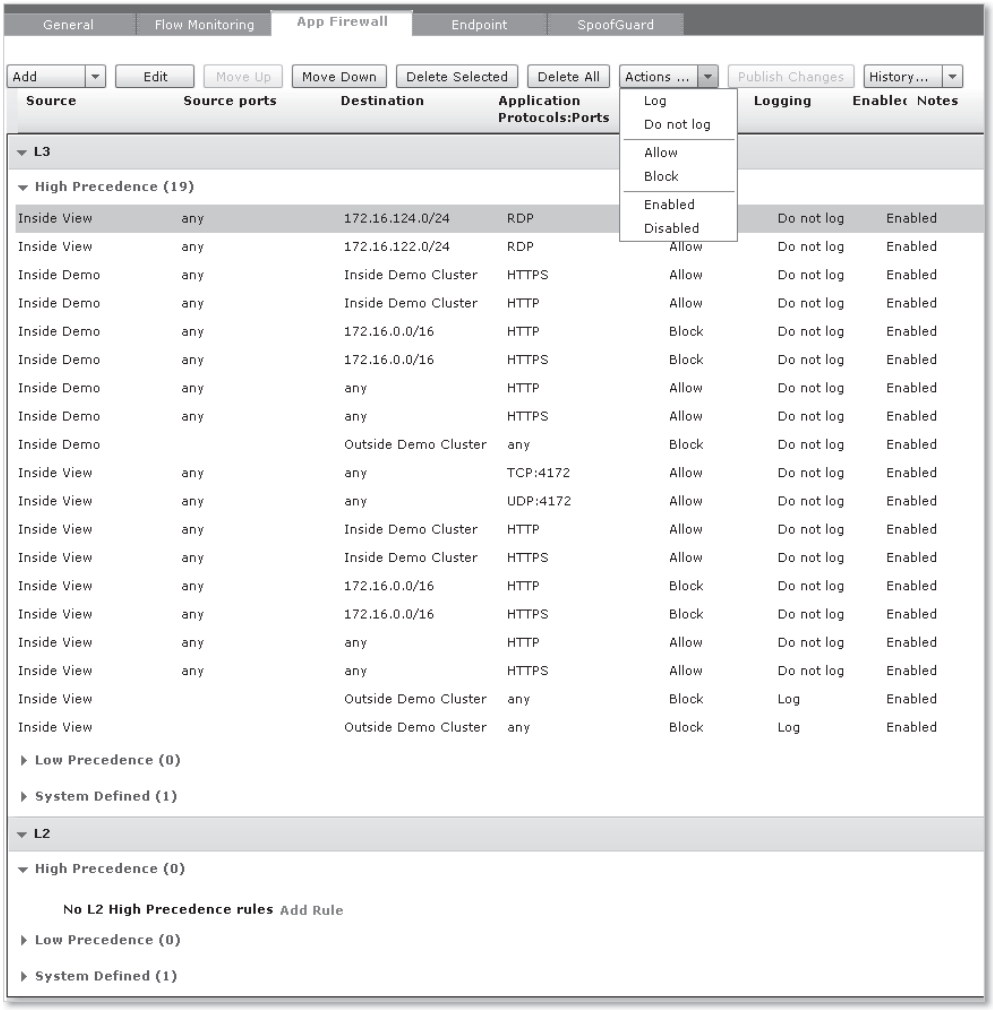


Abbildung B.10 Die vShield-App-Firewall-Regelbasis auf Datacenter-Ebene

Layer-2-Regeln haben Vorrang vor Layer-3-Regeln. Innerhalb der jeweiligen OSI-Ebene unterscheidet man zwischen High-Precedence-Regeln, die auf der Datacenter-Objekt-Ebene erstellt

werden, danach folgen Cluster-Level-Regeln (nicht in Abbildung B.10 dargestellt) und Low-Precedence-Regeln, die nach der Cluster-Ebene abgearbeitet werden, bevor die System-defined-Regel an der Reihe ist. Die System-Defined-Defaultregel lässt nach der Installation erst einmal allen Traffic zu, so dass Sie im laufenden Betrieb wichtigen Verkehr nicht blockieren. Dies garantiert eine unterbrechungsfreie Installation und Integration in ein bestehendes physisches Firewall-Konzept.

vShield App ist erst einmal transparent, das heißt, als Kunde müssen Sie nicht beim Einsatz der Lösung Ihr existierendes Firewall-Konzept von heute auf morgen ablösen, und es ist keine Gateway-Firewall, es sind also keine Anpassungen der IP-Adressierung oder der Routing-Definition notwendig.

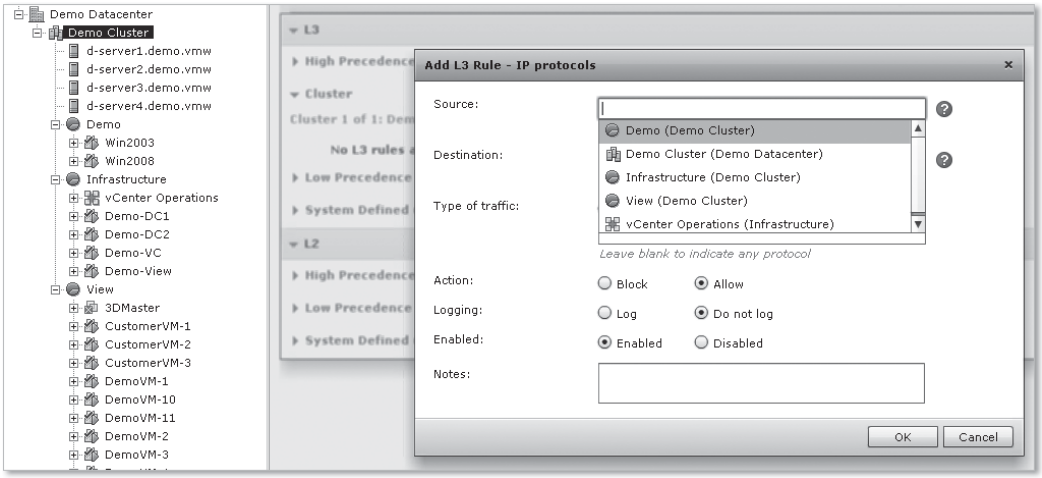


Abbildung B.11 Verwendung von vCenter-Objekten bei der Regelerstellung

Herausragend ist bei der Regelerstellung, dass Sie nicht nur CIDR-Adressen wie z. B. 192.168.1.0/24 als Quelle oder Ziel verwenden können, sondern vor allem logische vCenter-Objekte. Als Objekte lassen sich zum Beispiel aus dem vCenter »Datacenter«, »Cluster Level«, »vApp Level«, »Port Group» Objekte als Quelle oder Ziel heranziehen. Dabei können Sie bei dem jeweiligen Objekt immer den Geltungsbereich (SOURCE- und DESTINATION-Boundary) in der Quelle oder im Ziel angeben. Möchten Sie zum Beispiel nicht, dass ein Cluster-1-Objekt mit irgendetwas anderem spricht als Maschinen, die sich in selben Cluster befinden, sähe dies wie in Abbildung B.12 aus. Dies hat einen großen Vorteil gegenüber klassischen Firewalls: Die Objekte können unabhängig von definierten IPs oder IP-Ranges gelten und sind wesentlich dynamischer. Werden weitere VLANs in das Datacenter eingefügt, gelten die Cluster-Regeln nach wie vor unabhängig von physischen Gegebenheiten. Wenn ein vSphere-Admin zum Beispiel in der vSphere-Console falsch gepatcht hat und die Entwicklungsmaschine mit den hochsensiblen Daten in der DMZ hängt, würden Firewall-Regeln auf Objektebene immer noch gelten, Portgruppen- Regeln natürlich ausgenommen. Dies hat einen enormen Reiz, weil Netzwerkfehlkonfigurationen kein Sicherheitsloch erzeugen können. Eine weitere Möglich-

keit der Gruppierung bietet das Erstellen von vShield-Security-Groups, in denen Sie einzelne VMs unabhängig von Resource-Pools zu einer Entität für die Regelerstellung zusammenfassen können.

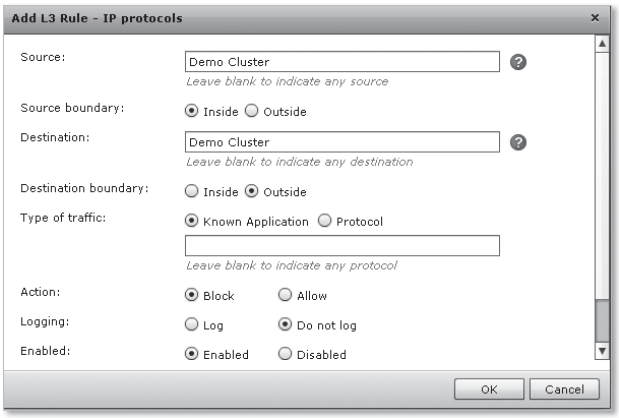


Abbildung B.12 Abbildung B.12:Boundary-Beispiel – der »Demo Cluster« darf nur intern kommunizieren.

Durch den Einsatz von Layer-2-Regeln erreichen Sie innerhalb eines Subnetzes eine virtuelle physische Layer-2-Trennung, was vor allem für die Richtlinienkonformität bestimmter Regularien wie z. B. PCI DSS (Payment Card Industry Data Security Standard) sehr interessant sein dürfte. Auch können Sie Verkehr auf Layer-3-Ebene voneinander isolieren, was an den Einsatz von Private VLANs erinnert, ohne diese auf den physischen Switches konfigurieren zu müssen. So lässt sich das Anwachsen der VLAN-Anzahl im Netzwerkbereich gut im Zaum halten.

Ein weiterer Vorteil der engen Integration mit vSphere, ist die Möglichkeit im z. B. Cloud Umfeld mit vShield App, überlappende IP Adressbereiche in der Regelbasis unterschiedlich abzuhandeln. Cloud Kunde A hat eine Maschine mit der IP Adresse 10.0.0.1, die leider auch der Cloud Kunde B hat. Eine Firewall Lösung muss nun die beiden VMs gleicher IP in der Regelbasis unterschiedlich handhaben. vShield App 5.0 beherrscht dies! Man legt in der Netzwerksansicht auf einer Portgruppe einen sogenannten Independent Namespace an. VMs die gleiche IPs im virtuellen Datacenter haben und in unterschiedlichen Portgruppen sind, können damit in der Regelbasis unterschieden werden.

B.4.4 Flow Monitoring

Verkehr zwischen virtuellen Maschinen können Sie im vSphere Plugin, das ein kongruentes Abbild der Webadmin-Oberfläche ist, auch sichtbar machen. Flow Monitoring hat nichts mit NetFlow-Monitoring zu tun, also bitte nicht verwechseln. Getreu dem Modell des hierarchischen Firewall-Konzepts können Sie auch hier unterschiedliche Ebenen für die Traffic-Analyse auswählen und betrachten. Möchten Sie die Gesamtheit Ihrer Daten sehen, die in den Cluster ein- und ausgehen, oder nur den Traffic des VLANs 123 oder des Webservers 1? Von wo kommt der Traffic? Welcher Traffic wurde erlaubt, und welcher wurde blockiert?

Es gibt beim Flow Monitoring zwei Ansichtsarten, die Chart-Ansicht und die Report-Ansicht. Die Chart-Ansicht gibt Aufschluss darüber, welches Protokoll in einem bestimmten Zeitraum wie oft aufgerufen wurde (Sessions/Stunde), wie viel Client- und Server-Kilobytes von z. B. HTTP- oder FTP-Traffic erzeugt wurde. Der Unterschied zwischen Client- und Server-Kilobytes besteht darin, wer die TCP/IP-Session initiiert hat, also eingehende Verbindungen im Gegensatz zu ausgehenden Verbindungen.

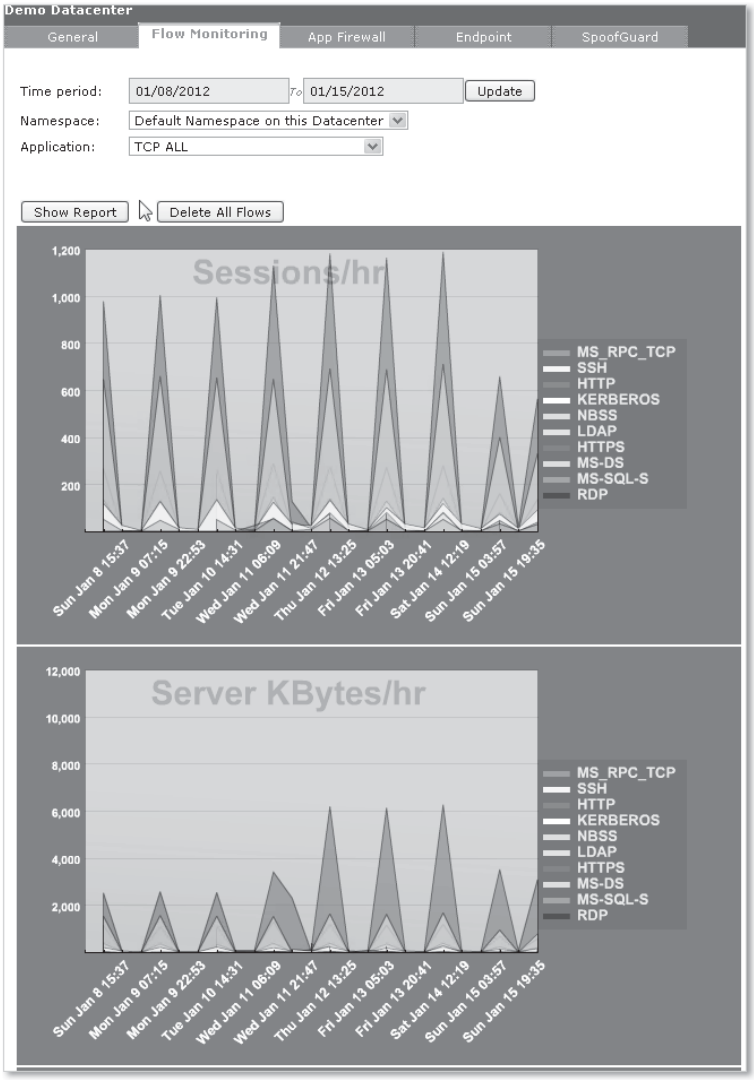


Abbildung B.13 Netzwerkverkehr auf Datacenter-Ebene (Chart-Ansicht)

In dem Dropdown-Menü Application können Sie zwischen verschiedenen Protokollen auswählen und sich dann zum Beispiel UDP-Traffic ansehen.

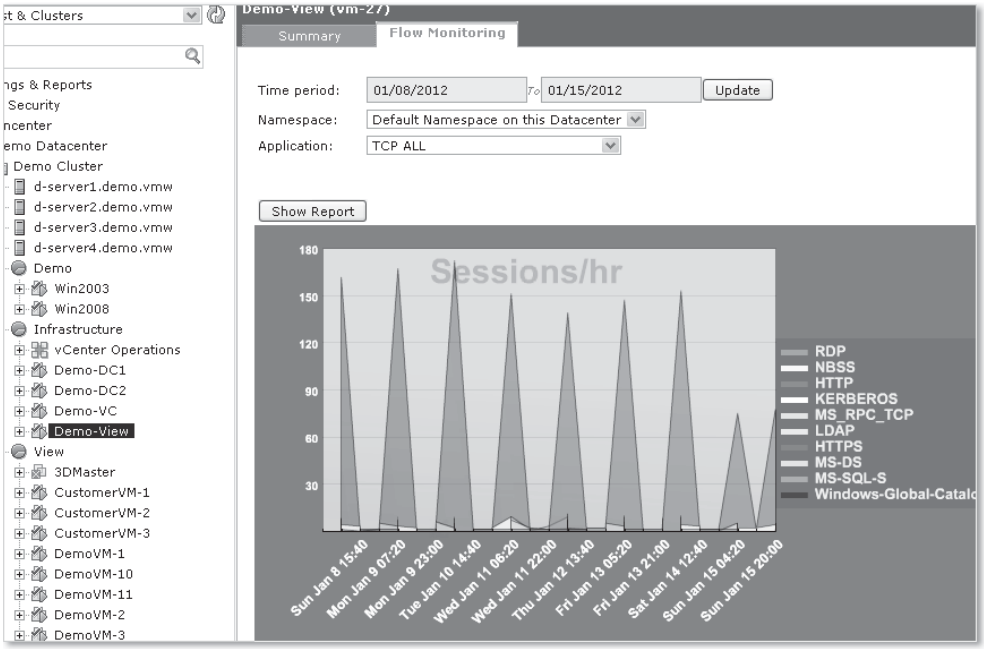


Abbildung B.14 Chart-Flows einer einzelnen VM

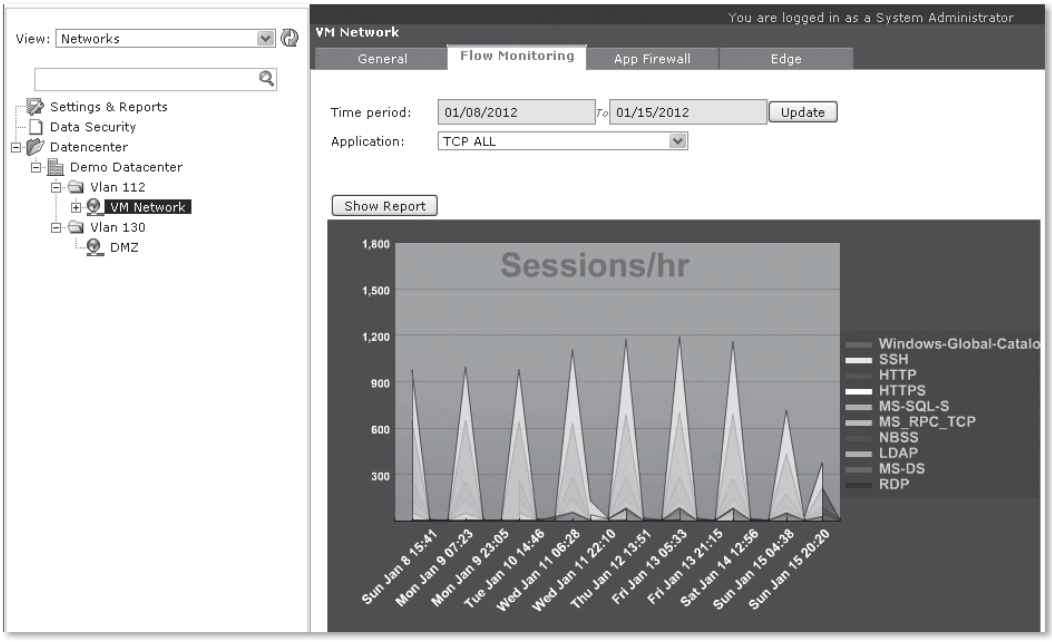
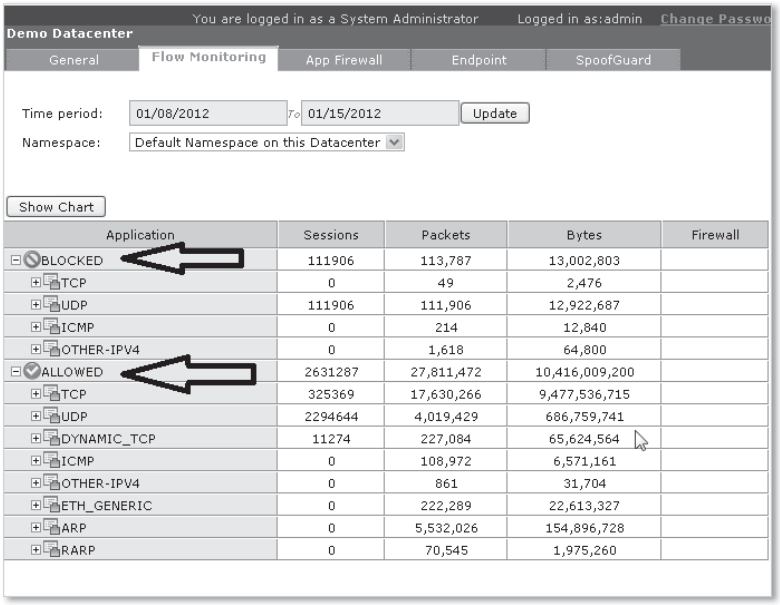


Abbildung B.15 Chart-Flow einer Portgruppe

Klicken Sie so wie in Abbildung B.13 bis Abbildung B.15 auf den Show Report-Button gelangen Sie in die Reportansicht der ausgewählten vCenter-Ebene.



Application	Sessions	Packets	Bytes	Firewall
BLOCKED	111906	113,787	13,002,803	
TCP	0	49	2,476	
UDP	111906	111,906	12,922,687	
ICMP	0	214	12,840	
OTHER-IPV4	0	1,618	64,800	
ALLOWED	2631287	27,811,472	10,416,009,200	
TCP	325369	17,630,266	9,477,536,715	
UDP	2294644	4,019,429	686,759,741	
DYNAMIC_TCP	11274	227,084	65,624,564	
ICMP	0	108,972	6,571,161	
OTHER-IPV4	0	861	31,704	
ETH_GENERIC	0	222,289	22,613,327	
ARP	0	5,532,026	154,896,728	
RARP	0	70,545	1,975,260	

Abbildung B.16 Report-Ansicht einer VM

In der Report-Ansicht sehen Sie sehr aussagekräftig, welche eingehenden und ausgehenden Verbindungen erlaubt oder blockiert worden sind. Außerdem lassen sich direkt aus dieser Ansicht Firewall-Regeln erstellen.

B.4.5 Spoofguard

Spoofguard ist eine vShield-App-Funktion ähnlich dem DHCP-Snooping von Cisco, die sich merkt und weiß, welche IP-Adresse für eine bestimmte MAC-Adresse und welche VM erlaubt ist. Das verhindert IP-Spoofing und geht über die Spoofing-Funktionen der virtuellen Switches von VMware hinaus, da diese nur ARP-Spoofing verhindert.

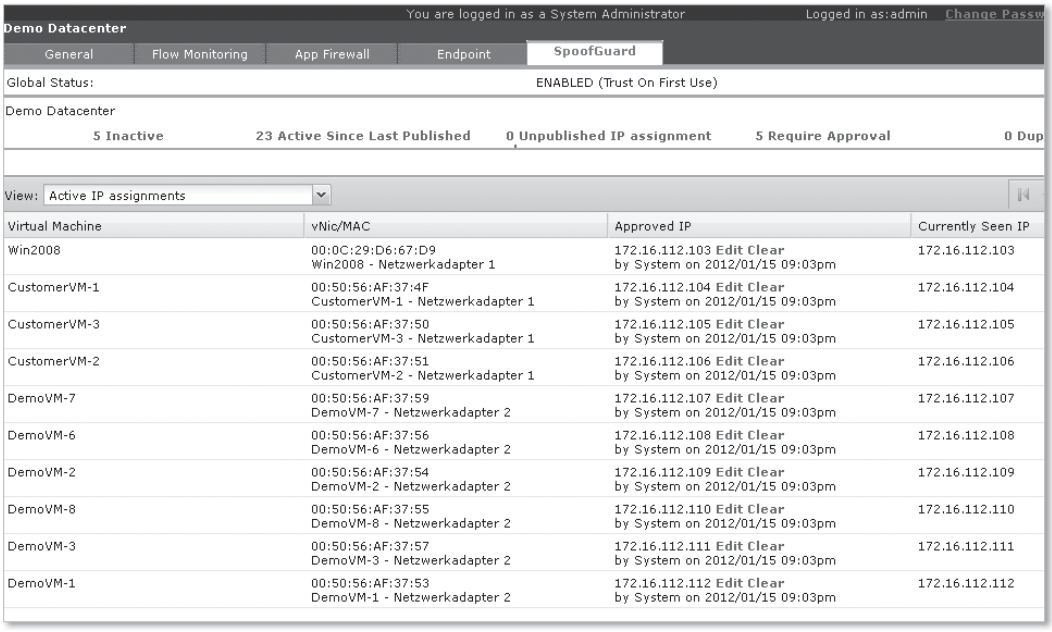


Abbildung B.17 Spoofguard

B.4.6 Sensitive Data Discovery

Sensitive Data Discovery (SDS) ist ein Add-on zur normalen vShield-App-Lizenz. Die Software ermöglicht es, unstrukturierte Dateien innerhalb von windows-basierten Gast-VMs agentenlos zu inspizieren, um sie gegen Regulatorien zu überprüfen. Es ist ein sehr gut geeignetes Audit-Tool, das zur Drucklegung jedoch noch kein vollwertiges DLP-Produkt ersetzt. VMware SDS verwendet technisch gesehen die VMSafe Endpoint-Komponente. Dies bedeutet, dass auf überwachenden VMs der Thin-Agent-Driver (Bestandteil der VMware Tools) installiert sein muss. Pro ESX-Host wird eine Appliance, wie in Abbildung B.18 dargestellt, ausgerollt (1 vCPU, 512 MB RAM).

Bei der Konfiguration von SDS können Sie aus Regularien wie PCI DSS, »Patient Health Information« etc., auswählen. Sie können auch mehrere Regularien auswählen. Die Definitionen der Regularien werden mittels Regular Expressions gegen Dateitypen und deren Inhalte innerhalb der Gast VM geprüft. Das heißt, die SDS Appliance sucht z. B. anhand von Pattern nach Sozialversicherungsnummern, Kreditkartennummern, Ausweisnummern etc. Welche Dateitypen innerhalb der zu überprüfenden Gast-VM gescannt werden, können Sie ebenfalls festlegen. Auch können Sie einzelne VMs vom SDS ausschließen. Was herauskommt, sind Auditierungs-Berichte von Policy-Verletzungen innerhalb der geprüften VMs, die dem Unternehmen sehr schnell einen Überblick verschaffen, ob Mitarbeiter fälschlicherweise sensitive Daten auf Ihren gehosteten VMware-View-Desktops speichern.

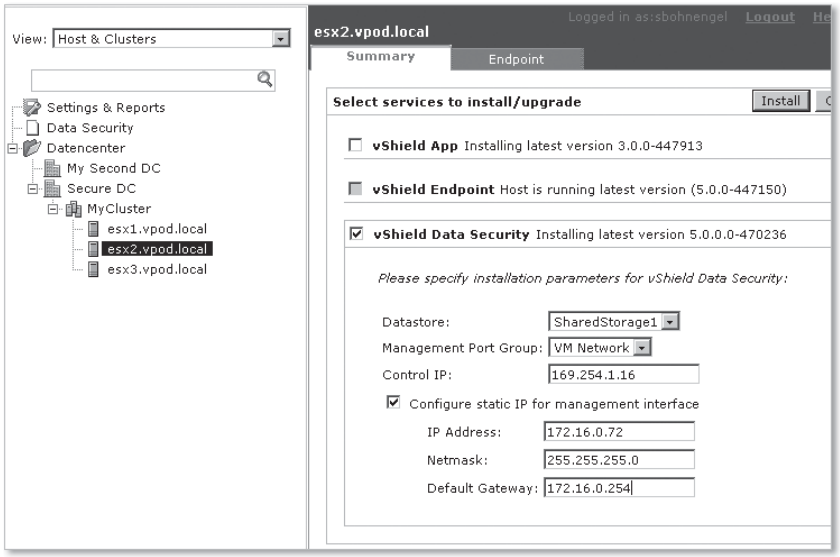
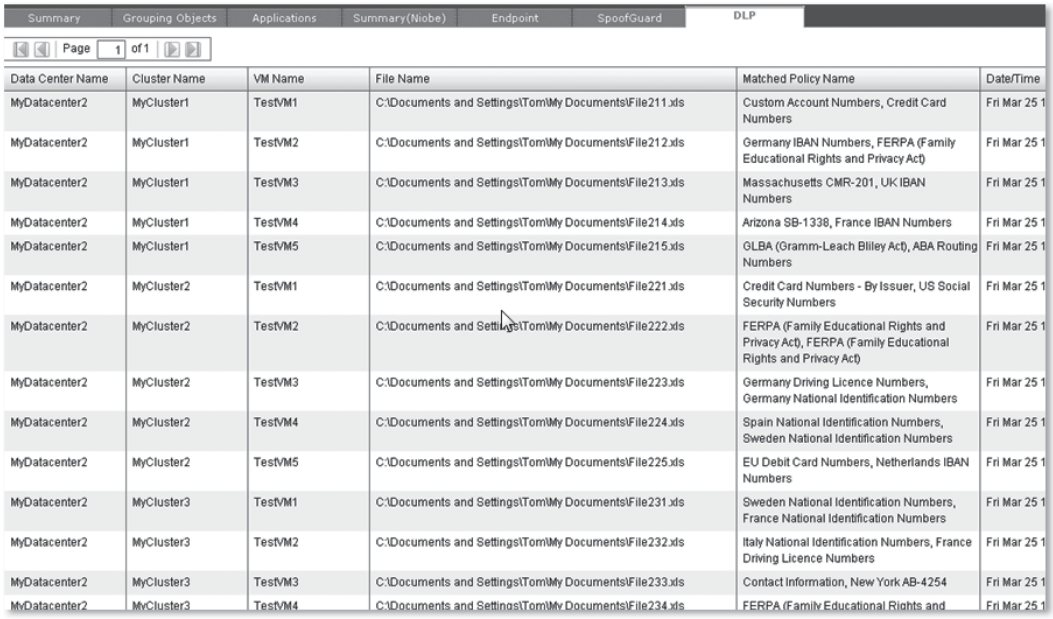


Abbildung B.18 Installation von Sensitive Data Discovery



Data Center Name	Cluster Name	VM Name	File Name	Matched Policy Name	Date/Time
MyDatacenter2	MyCluster1	TestVM1	C:\Documents and Settings\Tom\My Documents\File211.xls	Custom Account Numbers, Credit Card Numbers	Fri Mar 25 1
MyDatacenter2	MyCluster1	TestVM2	C:\Documents and Settings\Tom\My Documents\File212.xls	Germany IBAN Numbers, FERPA (Family Educational Rights and Privacy Act)	Fri Mar 25 1
MyDatacenter2	MyCluster1	TestVM3	C:\Documents and Settings\Tom\My Documents\File213.xls	Massachusetts CMR-201, UK IBAN Numbers	Fri Mar 25 1
MyDatacenter2	MyCluster1	TestVM4	C:\Documents and Settings\Tom\My Documents\File214.xls	Arizona SB-1338, France IBAN Numbers	Fri Mar 25 1
MyDatacenter2	MyCluster1	TestVM5	C:\Documents and Settings\Tom\My Documents\File215.xls	GLBA (Gramm-Leach Bliley Act), ABA Routing Numbers	Fri Mar 25 1
MyDatacenter2	MyCluster2	TestVM1	C:\Documents and Settings\Tom\My Documents\File221.xls	Credit Card Numbers - By Issuer, US Social Security Numbers	Fri Mar 25 1
MyDatacenter2	MyCluster2	TestVM2	C:\Documents and Settings\Tom\My Documents\File222.xls	FERPA (Family Educational Rights and Privacy Act), FERPA (Family Educational Rights and Privacy Act)	Fri Mar 25 1
MyDatacenter2	MyCluster2	TestVM3	C:\Documents and Settings\Tom\My Documents\File223.xls	Germany Driving Licence Numbers, Germany National Identification Numbers	Fri Mar 25 1
MyDatacenter2	MyCluster2	TestVM4	C:\Documents and Settings\Tom\My Documents\File224.xls	Spain National Identification Numbers, Sweden National Identification Numbers	Fri Mar 25 1
MyDatacenter2	MyCluster2	TestVM5	C:\Documents and Settings\Tom\My Documents\File225.xls	EU Debit Card Numbers, Netherlands IBAN Numbers	Fri Mar 25 1
MyDatacenter2	MyCluster3	TestVM1	C:\Documents and Settings\Tom\My Documents\File231.xls	Sweden National Identification Numbers, France National Identification Numbers	Fri Mar 25 1
MyDatacenter2	MyCluster3	TestVM2	C:\Documents and Settings\Tom\My Documents\File232.xls	Italy National Identification Numbers, France Driving Licence Numbers	Fri Mar 25 1
MyDatacenter2	MyCluster3	TestVM3	C:\Documents and Settings\Tom\My Documents\File233.xls	Contact Information, New York AB-4254	Fri Mar 25 1
MyDatacenter2	MyCluster3	TestVM4	C:\Documents and Settings\Tom\My Documents\File234.xls	FERPA (Family Educational Rights and	Fri Mar 25 1

Abbildung B.19 SDS-Audit-Reports

Zur Drucklegung dieser Auflage ist es bei der aktuellen Implementierung nicht möglich, Alerts zu konfigurieren, und deshalb ersetzt es noch nicht ein klassisches DLP-Tool.

Zusammenfassung SDS

- SDS benötigt die Installation des Endpoint-Kernel-Moduls.
- Pro ESX-Hosts läuft eine Appliance. Diese kann mittels Regular Expressions bestimmte Dateitypen in VMs scannen.
- SDS Appliance scannt seriell VMs. Es wird immer nur pro ESX-Hosts eine VM gescannt.
- Schont Ressourcen, da kein voller DLP-Agent innerhalb der VM gebraucht wird,
- Durch Thin-Agent so gut wie kein Installationsaufwand.
- Ist ein gutes Auditierungs-Tool und schützt damit vor dem Verlust sensitiver Daten.

B.4.7 Zusammenfassung

Fassen wir den Funktionsumfang von vShield App zusammen:

vShield-App-Funktionen

- schnelles Ausrollen der Appliances
- VMSafe-API-Firewall, eliminiert Blind Spots
- reduziert Anzahl der benötigten VLANs
- wird einmal pro ESX installiert
- skaliert parallel mit der Umgebung mit
- sannt innerhalb des physischen Servers, verhindert dadurch Netzwerkverkehr und Engpässe
- Stateful-Inspection-Firewall bis OSI Layer 4
- Spoofguard verhindert IP- und DHCP-Snooping.
- Überlappende IP-Bereiche können unterschieden werden.
- ist für VMs transparent, keine Änderungen an bestehenden Firewall-Konzepten notwendig, sanfte Migration
- kann die Anzahl der Firewall-Regeln in der Regelbasis durch Verwendung von vCenter-Objekten drastisch minimieren
- kann Netzwerkfehlkonfiguration seitens des vSphere-Admins verhindern, da Firewall-Regeln auf Objekten basieren können (Datacenter, Cluster, Resource-Pool, vAPPs, Security-Gruppe)
- Verwaltung mittels VSM oder Programmierung via REST-API oder vSphere Power CLI (Powershell)
- Automatisierung in Workflows und Cloud-Automatisierung möglich

Limitierungen:

- kann nur VMs oder teilvirtualisierte Dienste schützen
- keine Sichtbarkeit von physischen Services im Rechenzentrum

B.5 vShield Edge

Im Gegensatz zu VMware vShield App ist Shield Edge eine portbasierte Firewall. Damit hängt sie zwischen zwei Portgruppen und scannt nur Verkehr, der über sie hinweg muss. Dementsprechend eliminiert Sie keine Blind Spots am ESX-Host, die durch VMSafe-API-Firewalls abgedeckt werden. Sie können sie deshalb auch in Verbindung mit vShield App verwenden. Sie ist sehr klein und kann mittels DRS und vMotion überall im Cluster verschoben werden. Sie haben ja bereits erfahren, dass die App-Firewall-Lösung immer auf dem installierten Host bleiben muss und Sie dafür Sorge tragen müssen, dass diese VM nicht dynamisch die Hosts wechselt.

Die vShield Edge wird zum Beispiel mit dem Cloud Direktor gebündelt, jedoch nicht mit dem vollen Funktionsumfang. Sie ist auch eine Stateful-Inspection-Firewall. die bis auf Layer-4-Ebene arbeitet. Im Gegensatz zur vShield App ist sie für die Maschinen, die sie schützt, nicht transparent, sondern ist deren Default-Gateway. Zusätzlich bietet sie jedoch weitere Dienste an, die über die der vShield App hinausgehen. Diese finden Sie im Hinweiskasten.

vShield-Edge-Funktionen

- nicht transparent, sondern Default-Gateway
- kann im NAT-Modus betrieben werden oder statisch routen
- DHCP-Server
- Web-Load-Balancer für HTTP (Funktion nicht im Cloud-Director-Bundle enthalten)
- Site-to-Site-VPN mittels Pre-shared Key (Funktion nicht im Cloud-Director-Bundle enthalten)
- Verwaltung mittels VSM oder Programmierung via REST-API oder vSphere Power CLI (Powershell)
- Automatisierung in Workflows und Cloud-Automatisierung möglich
- schützt auch physische Hosts, da es ein Default-Gateway ist

Limitierung:

- eliminiert keine Blind Spots im Host

Idealerweise wird die vShield Edge als virtueller Perimeterschutz gesehen. Bitte verstehen Sie dies nicht falsch: Die Lösung ersetzt keinen physischen Firewall-Cluster, den Sie am Rande Ihres Rechenzentrums betreiben. Sie schottet vielmehr bestimmte Bereiche voneinander ab, indem sie entscheidet, welcher Verkehr überhaupt in einen Bereich hinein oder aus ihm hinaus kommunizieren darf. Als Beispiele wären Trennen von einer DMZ und dem internen LAN oder dem Entwicklungsbereich zu nennen oder das Abschotten von vCloud-Director-Mandanten untereinander. Wenn Sie in der virtuellen Umgebung ein Vorproduktions-Staging betreiben möchten, um Änderungen ITIL-konform (Information Technology Infrastructure Library) zu testen, hätten diese Produktionssysteme dieselbe IP-Konfiguration wie die Live-Systeme. IP-Adress-Konflikte wären die Folge. Hier liefert die Lösung mittels NAT eine ideale Funktion, um kongruente IP-Adress-Bereiche voneinander abzuschirmen. Der VMware Cloud Director

macht sich diese Funktion zunutze, schließlich kann man ja nicht verhindern, dass Mandanten unter Umständen gleiche Segmente in einem Self-Service-Portal verwenden. Auch innerhalb eines Mandanten ist dies der Fall, wenn er eine vApp, die aus mehreren VMs besteht. die in einer Netzwerkbeziehung zueinander stehen, mehrfach ausgerollt werden.

Die VPN-Funktion bietet dem Kunden die Möglichkeit, seine eigene private Cloud mit einem öffentlichen VMware-Enterprise-Cloud-Anbieter zu verbinden, bei dem er sich für einen bestimmten Zeitraum Server gemietet hat. Das Verbindungsstück zur Hybrid Cloud wird sozusagen über die vShield Edge realisiert.

Die manuelle Edge-Installation ist sehr einfach. Legen Sie im vCenter auf dem virtuellen oder verteilten virtuellen Switch eine zu schützende Portgruppe an. Im VSM oder vSphere Plugin wechseln Sie in die Netzwerk-Ansicht, wählen die Portgruppe aus und installieren einfach das Edge-Device wie in Abbildung B.20 dargestellt. In diesem Beispiel schützt das Edge-Device die innere Portgruppe DMZ.

Wichtig

Die vShield Edge kann mittels vMotion und damit VMware DRS den ESX-Hosts innerhalb eines Clusters wechseln. Die geschützten VMs innerhalb der Portgruppe können sich deshalb auf einem anderen ESX-Host befinden als deren vShield-Edge-Gateway. Damit müssen Pakete zum Gateway die physische ESX-Access-Switch-Infrastruktur überqueren. Die geschützte Portgruppe wird deshalb in den meisten Fällen einen VLAN-Tag benötigen, der nicht auf eine bestimmte Netzwerk-ID beschränkt ist.

Konfigurieren Sie die IP-Adressen des externen und internen Interfaces, und wählen Sie den Resource-Pool des initialen ESX-Servers sowie den Datastore aus, auf dem die Edge installiert werden soll. Dieser sollte ein gemeinsamer Datastore sein (NFS, iSCSI, FC, FCOE), damit DRS und vMotion Genüge getan ist. Ein Edge-Device nimmt eine vCpu, 256 MB RAM und 512 MB Plattenplatz in Anspruch.

Nach der Installation können Sie weitere Dienste wie NAT, DHCP, DHCP-Reservierungen, VPN und Load-Balancer konfigurieren (Abbildung B.21). In der Übersicht nach der Installation können Sie die Synchronisation mit dem vShield Manager erzwingen (Force Sync), Support-Logs generieren und bei Bedarf das Device deinstallieren. In der Services-Sektion lassen sich Dienste der Edge starten und stoppen, auch lassen sich bis zu zwei Syslog-Server pro Edge konfigurieren.

Auf dem externen Interface können Sie mehrere IPs via Proxy-ARP-Einträge binden, was durchaus sinnvoll ist. Dem wird auch im Firewall-Regelwerk der Edge Rechnung getragen, da Sie den Anwendungsbereich der Regel auf das jeweilige Interface legen können (VPN, internes oder externes Interface). Im NAT-Bereich können Sie sowohl Source- als auch Destination-NAT konfigurieren.

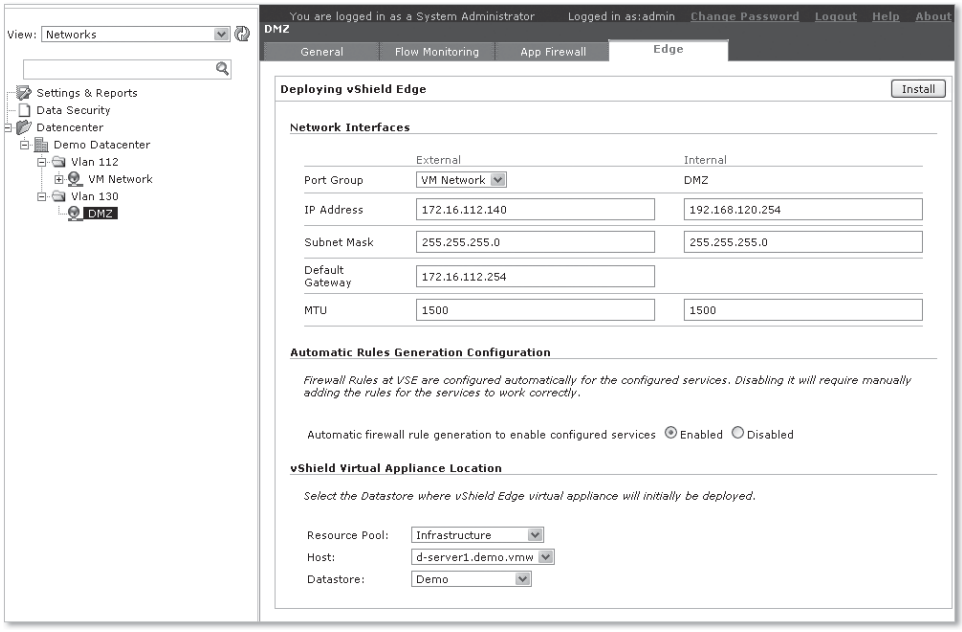


Abbildung B.20 Installation des Edge-Device auf einer Portgruppe

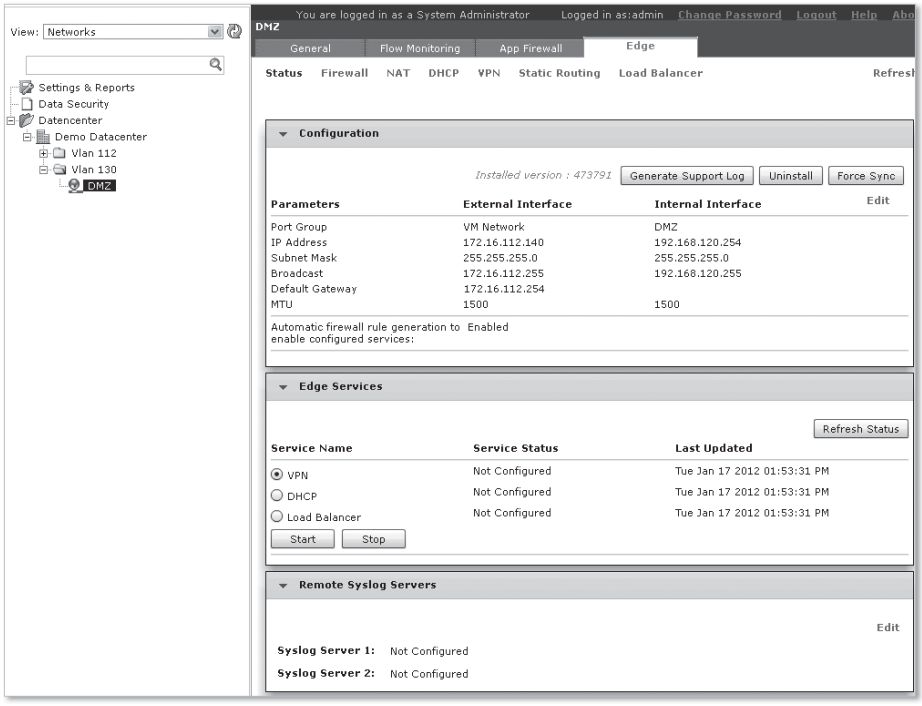


Abbildung B.21 Die Edge-Übersicht nach der Installation

B.6 vShield Endpoint

vShield Endpoint ist keine virtuelle Appliance, sondern bezeichnet die Schnittstelle zu Anti-Malware-Herstellern, die lizenziert werden muss; ihr haben wir uns bereits ausführlich in Abschnitt B.2.1, »EPSEC-API«, gewidmet. Trend Micro, Bitdefender haben bereits eine Lösung auf Markt (Stand März 2012). McAfee, Symantec und Kaspersky haben angekündigt, noch 2012 Produkte, die die VMsafe-Schnittstelle verwenden, auf den Markt zu bringen.

B.7 Versionskompatibilität und Links

Die aktuelle Version vShield 5.0 ist abwärtskompatibel mit vCenter Version 4.0 Upgrade 2 oder höher sowie mit ESX/ESXi Server 4.0 U2. Die einzige Ausnahme ist vShield Endpoint 5.0, das abwärtskompatibel mit VMware vCenter Server 4.1 und ESX/ESXi Server 4.1 ist.

Auf der VMware-Website gibt es unter *http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php* eine sehr gute Produktinteroperabilitätsmatrix

Produkt-Whitepapers finden Sie unter *https://www.vmware.com/support/pubs/vshield_pubs.html*:

- »vShield Quick Start Guide«
- »vShield Administration Guide«
- »vShield API Programming Guide«
- »die vShield Release Notes (wichtig, unbedingt lesen)«

Vor allem die Release Notes und die Admin Guides sind bei Upgrades bestehender vShield 4.1-Installationen unerlässlich.

Weiterführende Whitepapers finden Sie im »Technical Resource Center« zu VMware: *http://www.vmware.com/vmtn/resources/*

Filtern Sie einfach nach »vShield« in der Produktauswahl filtern. Aktuell (Anfang 2012) gibt es:

- vShield App Design Guide
- vShield Edge Design Guide
- The Technology Foundations of VMware vShield
- VMware vShield App protecting virtual SAP Deployments

Zum Thema Automatisierung der vShield-Produkt Familie sei noch ein Hinweis auf den hervorragenden vSPhere-CLI-Blog des Kollegen Alan Renouf, der auch Mitglied der Community vExpert ist, gestattet: *www.virtu-al.com.* Alan hat die REST-API der vShield-Aufrufe in ein leicht zu verwendendes Powershell Commandlet übersetzt.

Dieses Kapitel gibt Ihnen eine Übersicht über die vCloud Product Family. Sehen Sie was es hier gibt und für welchen Einsatz die Softwarepakete gedacht sind.

C Your Cloud

Autor dieses Kapitels ist Daniel Köck, VMware, dkoeck@vmware.com

Der Schwerpunkt dieses Buches lag bis jetzt auf der Bereitstellung von virtualisierter Infrastruktur. VMware ist aber längst mehr als ein Hersteller von Virtualisierungssoftware. Durch ständige Erweiterung der angebotenen Produkte ermöglicht es VMware, die komplette IT auf ein neues Niveau zu heben. Dabei werden Routineaufgaben wie etwa Bereitstellung, Monitoring, Kapazitätsmanagement und Performance-Monitoring innerhalb von vordefinierten Regeln automatisiert. Virtuelle Maschinen können dabei aus einem Katalog heraus bereitgestellt und zugehörige Nutzungsstatistiken und Reports abgerufen werden. Je nach Bedarf können virtuelle Maschinen zwischen Rechenzentren verschoben werden. Daraus resultieren völlig neue Betriebskonzepte, die eine Kombination aus *Private Cloud* (durch den Kunden selbst betrieben) und *Public Cloud* (externer Service-Provider) erstmals basierend auf einem Self-Service-Portal ermöglichen. Die Daten bleiben so immer in der Macht des Kunden. Dies stellt natürlich auch neue Anforderungen an Entwickler. Neuentwicklungen müssen portabel und cloudübergreifend programmiert werden. Um den steigenden Anforderungen gerecht zu werden, bietet VMware basierend auf dem branchenführenden Entwicklungs-Framework Spring ein Paket aus integrierten Anwendungs-Services wie einem schlanken Anwendungs-Server, globalem Datenmanagement, cloudfähigem Messaging, dynamischem Lastenausgleich und Performance-Management für Anwendungen.

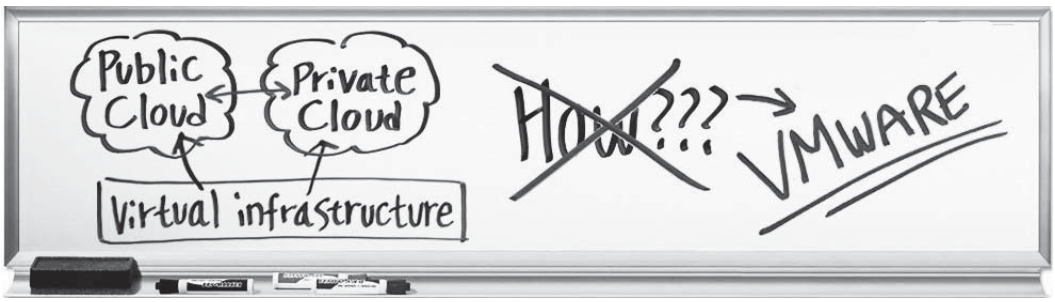


Abbildung C.1 VMware »Your Cloud«

Als Grundlage dient immer VMware vSphere, die Gesamtlösung wird dann darauf stufenweise aufgebaut. So haben Sie die Möglichkeit, schrittweise die IT von einem Modell mit individuellen Komponenten auf Standardisierung umzustellen. Die Bereitstellung von Standardinfrastruktur aus einem Vorlagenkatalog mit Anwendungen ist um ein Vielfaches schneller und einfacher als die komplette Neuerstellung einer Anwendung. Ähnliche Vorteile bringen die Zentralisierung und Standardisierung von Hochverfügbarkeit, Netzwerkverwaltung und Sicherheit. Diese Standards werden auch als führende Plattform für Serviceanbieter benutzt. Sowohl weltweit als auch in Deutschland, Österreich und der Schweiz existieren bereits Serviceanbieter, die Public Clouds basierend auf vSphere bereitstellen. Dies ermöglicht, einzelne Workloads flexibel am jeweils optimalen Ort bereitzustellen und Workloads jederzeit zwischen privaten und öffentlichen Cloud-Infrastrukturen zu verschieben. Unter dem folgenden Link finden Sie eine aktuelle Übersicht und mehr Informationen zu den in Ihrer Region verfügbaren Public-Cloud-Services: *http://vcloud.vmware.com*

Mit diesen modernen Konzepten kann sich die IT von der Vermeidung und Minimierung von Änderungen ab- und dem natürlichen Zustand der Anforderungen mit konstanten Änderungen zuwenden. In einer flexiblen Cloud-Infrastruktur können Sie für jede Anwendung genau die Ressourcen bereitstellen, die sie benötigt, und bei Bedarf auch wieder freigeben. Die wichtigsten Unterschiede zwischen herkömmlichen Management und morderner Bereitstellung in der Cloud im Verwaltungsansatz sind hier:

- **herkömmliches Management**
  - Es besteht eine feste Bindung zwischen Prozessen, Anwendungen und Infrastruktur
  - Änderungen erfolgen manuell, erfordern sorgfältige Planung, sind risikoanfällig und zeitaufwendig.
  - Heterogene Elemente und Prozesse sind in »Silo-Umgebungen implementiert.«
  - Die Ausführung der Verwaltungssoftware ist orientiert am kleinsten gemeinsamen Nenner.
- **Verwaltung der Cloud**
  - Dynamische Verbindungen bestehen über alle Ebenen hinweg.
  - Anfallende Änderungen werden regelmäßig und automatisch durchgeführt.
  - Es besteht eine hohe Standardisierung und Abstraktion.
  - Alltägliche Aufgaben werden automatisiert erledigt, dadurch sind Verwaltungstools verfügbar für wichtigere Aufgaben.

C.1 Cloud-Komponenten

Um solch eine Lösung aufzubauen, bietet VMware eine breite Palette an Produkten. Zur Bereitstellung von IaaS (Infrastruktur as a Service) dient als Kernkomponente der VMware

vCloud Director (vCD). Die vCD-Lizenz enthält auch grundlegende Funktionen für VMware vShield und vCenter Chargeback. Zusätzlich kann die Lösung um folgende Produkte erweitert werden:

- VMware vCloud Connector (kostenlos)
- VMware vCenter CapacityIQ
- VMware vCenter Operations Manager
- VMware Service Manager
- vCenter Configuration Manager

Für die Anwendungsentwicklung werden folgende Produkte geboten:

- VMware vFabric
- VMware vFabric tc Server
- VMware vFabric GemFire
- VMware vFabric Enterprise Ready Server
- VMware vFabric Hyperic
- VMware vFabric RabbitMQ

In den folgenden Abschnitten finden Sie eine Beschreibung zu den angeführten Produkten.

C.1.1 VMware vCloud Director

VMware vCloud Director (vCD) ist die Kernkomponente für die Bereitstellung von IaaS. Er ermöglicht eine Konsolidierung der vSphere-Infrastruktur über mehrere Cluster hinweg, eine Kapselung von Anwendungs-Services als portable vApps sowie eine Bereitstellung dieser Services nach Bedarf mit Isolation und Kontrolle. Eine vApp ist ein Verbund aus einer oder mehreren virtueller Maschinen, die in virtuellen Rechenzentren laufen. Diese bestehen aus logischen Konstrukten von Rechen-, Speicher-, Storage-, und Netzwerkkapazitäten. Somit wird eine vollständige Abstrahierung zwischen der Nutzung von Infrastrukturservices und zugrundeliegender Hardware erreicht.

Mit der Hilfe von Organisationen können Sie Anwender gruppieren und so Richtlinien zuordnen. Jede Organisation verfügt über isolierte virtuelle Ressourcen, eine unabhängige LDAP-Authentifizierung, spezifische Richtlinienkontrollen und eigene Kataloge. Die Anwender können über ein webbasiertes Self-Service-Portal je nach Berechtigung verschiedene einfache Tasks wie das Erstellen, Starten, Stoppen, Kopieren und Löschen von vApps per Mausklick schnell und sicher ausführen, aber auch komplexe Aufgabenstellungen wie z. B. Site-to-Site-VPN, isolierte Netze und Betriebssystemanpassungen konfigurieren. Die angebotenen Infrastrukturen und Anwendungs-Services wie etwa virtuelle Appliances, virtuelle Maschinen, Betriebssystem-Images oder Medien können Sie in einem zentralen Katalog bereitstellen. Der vCD kann dabei sehr flexibel an bestehende Netzwerkanforderungen angepasst werden und

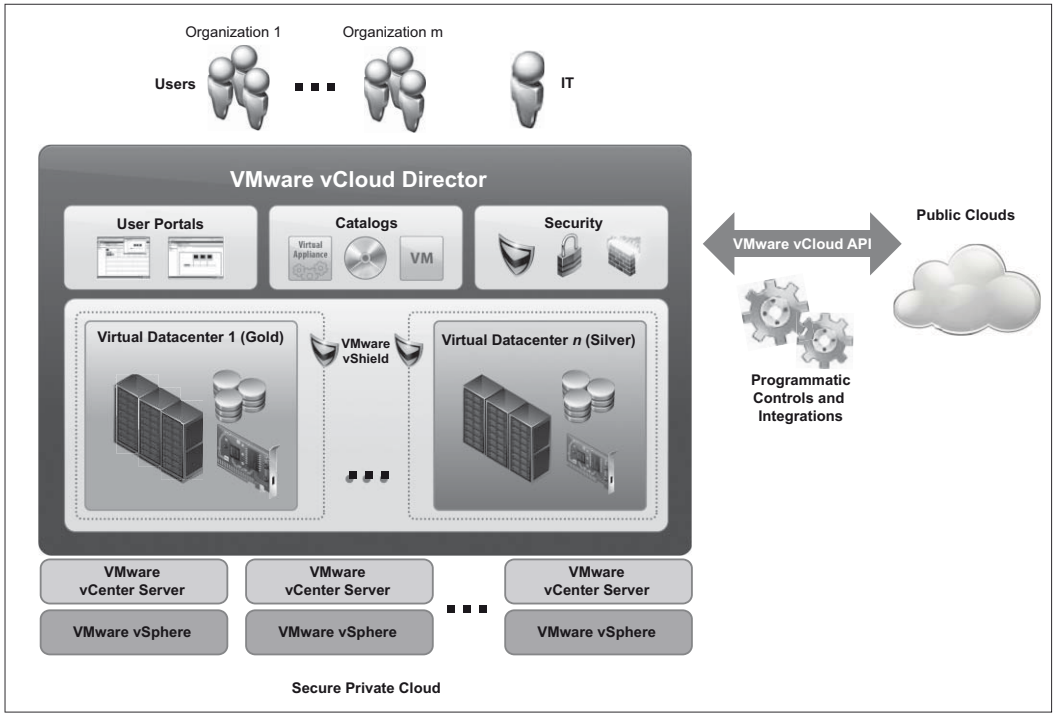


Abbildung C.2 Übersicht VMware vCloud Director

erweitert die Möglichkeiten der virtuellen Netze. Somit müssen Sie hier keinen Kompromiss in Bezug auf Sicherheit und Kontrolle eingehen. Zur sicheren Mandantentrennung können Sie Layer-2-Netzwerksegmente im laufenden Betrieb erstellen und mit externen Netzen verbinden, des Weiteren können Sie durch NAT/PAT und virtuelle Firewalls die Verbindung einschränken oder auch vollständig trennen. Zur schnellen Bereitstellung von vApps bietet vCD die Linked-Clone-Technologie. Dabei können die Anwender mehrere Kopien einer vApp erstellen, wobei aber immer nur die Änderungen gespeichert werden. Sämtliche kopierte vApps teilen sich eine Master-Kopie als gemeinsame Basis. So können neue vApps sehr schnell provisioniert werden, bei gleichzeitiger Einsparung des Storage-Bedarfs. Sämtliche Tasks können auch über die vCloud-API automatisiert werden. Dies ist eine REST-basierte API, die einen skriptgesteuerten Zugriff auf Cloud-Ressourcen und somit auch den einfachen Transfer von vApps zwischen Clouds ermöglicht.

Der vCloud Director speichert sämtliche Informationen in einer eigenen Datenbank. Derzeit werden Oracle und SQL unterstützt. Die vCloud-Software wird auf sogenannten *vCloud Cells* bereitgestellt. Eine Cell ist eine virtuelle Red-Hat-Maschine, auf der die vCD-Software installiert wird. Sämtliche Informationen werden in der zentralen Datenbank gespeichert, die vCD Cells sind stateless. Das heißt, um hier in die Breite zu skalieren, können Sie mehrere Cells

parallel betreiben, und bei Bedarf verwenden Sie davor auch noch einen (sticky-sessions-fähigen) Load-Balancer verwendet werden.

Damit Sie mit vCD schnell vertraut werden, bietet VMware eine fertige vCD-Appliance an; diese ist aber nur für Test- und Evaluierungszwecke und nicht für Produktionsumgebungen freigegeben:

https://www.vmware.com/tryvmware/?p=vcloud-director15&lp=default

In Produktionsumgebungen müssen Sie den vCD richtig installieren.. Die Komponenten sollten Sie in einen eigenen Management-Cluster, auf separaten oder bestehenden ESXi-Hosts installieren. Für die Cloud sollten eigene ESXi-Hosts und ein eigenes vCenter bereitstehen. Um eine funktionierende Umgebung zu erhalten, sind mindestens folgende Komponenten erforderlich.

- VMware vCenter (inklusive Datenbank)
- VMware ESXi
- VMware vShield Manager
- vCD Datenbank
- vCD Cell

Eine genaue Installationsanleitung finden Sie unter folgendem Link:

www.vmware.com/pdf/vcd_15_install.pdf

C.1.2 VMware vShield

vCD arbeitet sehr eng mit VMware vShield zusammen. Der vCD kommuniziert mit dem vShield Manager, der die Netzwerke für vApps bereitstellt. Dies ermöglicht eine sichere Mandantentrennung und die Einhaltung von Compliance-Standards. Die Basisfunktionen sind in der vCD-Lizenz enthalten, bei einem Upgrade auf die vollständige vShield Edge Suite stehen auch erweiterte Dienste wie z. B. Site-to-Site-VPN zur Verfügung. Weitere Informationen zu der kompletten VMware vShield Suite (Edge/App/Endpoint) finden Sie in Anhang B.

C.1.3 VMware vCenter Chargeback

VMware vCenter Chargeback kann in vCloud-Umgebungen als optionales Zusatztool verwendet werden. Es sammelt die genauen Daten zum Ressourcenverbrauch von virtuellen Maschinen, um sie in eine exakte Kostenabrechnung umzuwandeln. Diese können Sie dann direkt als PDF-Report versenden oder auch in anderen Formaten wie XML oder CSV an bestehende Kostenabrechnungsprogramme übergeben. Weitere Informationen zu VMware vCenter Chargeback finden Sie im Anhang in Abschnitt A.2.

C.1.4 VMware vCloud Connector

Wie bereits beschrieben ermöglicht vCD den Transfer von vApps zwischen verschiedenen Clouds. Workloads können in interne und externe Clouds verschoben werden. Diese neuen Betriebskonzepte, die eine Kombination aus Private und Public Cloud ermöglichen, nennt VMware *Hybrid Cloud*.

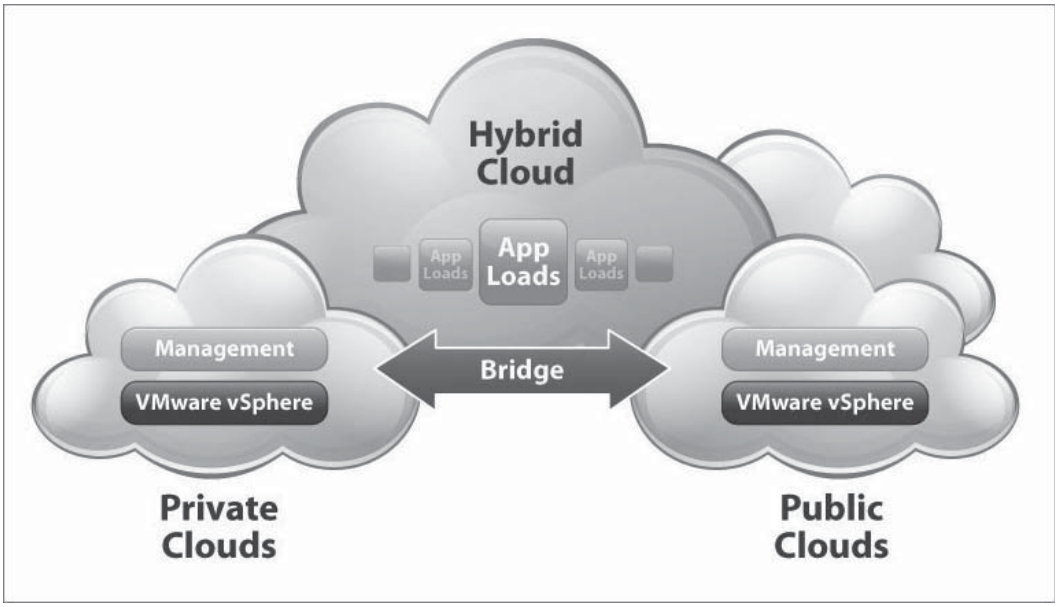


Abbildung C.3 VMware Hybrid Cloud

VMware vCloud Connector gewährleistet einen sicheren Transfer zwischen unterschiedlichen Clouds. Somit können Sie vApps in alle Richtungen (private – public, public – private, private – private, public – public) verschieben und auch von vSphere-Umgebungen in vCloud-Umgebungen importieren. vCloud Connector bietet eine zentrale Übersicht, von der aus Sie virtuelle Maschinen, vApps und Templates zwischen den verbundenen Umgebungen transferieren können.

Wie in Abbildung C.4 dargestellt besteht vCloud Connector aus mehreren Komponenten. Der vCloud Connection Server dient zur Verwaltung. Er wird in der internen Umgebung installiert und kommuniziert dann mit den vCloud Connector Nodes. Diese Nodes müssen Sie auch in jeder Cloud, in die Sie Workloads verschoben wollen, installieren. Ein Server kann mehrere Nodes verwalten und 1:1-Verbindungen zwischen den Nodes herstellen.

Der vCloud Connector und der zugehörige User-Guide sind kostenlos unter folgendem Link verfügbar:

http://www.vmware.com/de/products/datacenter-virtualization/vcloudconnector/overview.html

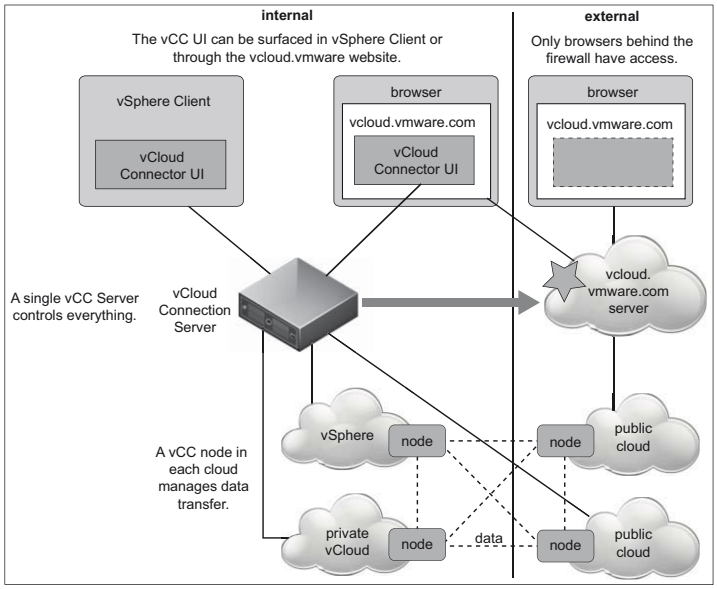


Abbildung C.4 vCloud-Connector-Architektur

C.1.5 VMware CapacityIQ

Durch die agile Bereitstellung, wird natürlich die Überwachung der Ressourcenauslastung der darunterliegenden Infrastruktur immer wichtiger. Anwendern kann die Freiheit gegeben werden, die Größe der virtuellen Maschinen selbst zu wählen. Auf den Administrator einer Cloud kommen neue Herausforderungen zu. Sorgfältige Planung wird immer wichtiger, um auf zukünftiges Wachstum vorbereitet zu sein. Des Weiteren soll die vorhandene Infrastruktur in Private Clouds natürlich optimal genutzt werden, um einen möglichst hohen Return on InvestmentI zu erzielen.

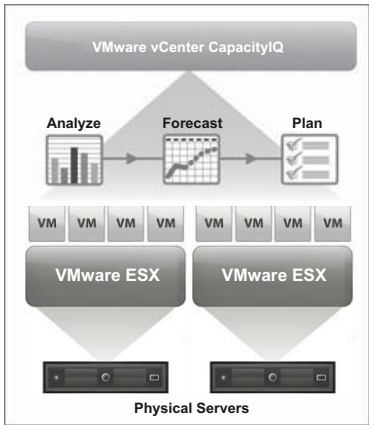


Abbildung C.5 VMware vCenter CapacityIQ

VMware CapacityIQ ist ein Kapazitäts-Monitoring-Tool. Es analysiert den aktuellen Ressourcenbedarf und Kapazitätsanforderungen und identifiziert dabei ungenutzte oder überbuchte Ressourcen. Außerdem können Sie Trendanalysen und Annahmen für zukünftige Anforderungen berechnen. Weitere Informationen zu VMware CapacityIQ finden Sie in Kapitel 16.

C.1.6 VMware vCenter Operations Manager

Traditionelle Programme zur Überwachung von Operations-Management stoßen in hoch virtualisierten, sich schnell anpassenden Umgebungen zumeist an ihre Grenzen. Sie wurden für das Monitoring von statischen Umgebungen entwickelt und sind nicht in der Lage, Clouds automatisiert zu überwachen. VMware vCenter Operations (vCOPs) wurde entwickelt, um Operations-Management in genau solchen Umgebungen zu vereinfachen. Ein integrierter und evolutionärer Monitoring-Ansatz verwendet neue patentierte Algorithmen, um proaktives Monitoring in virtualisierten Umgebungen zu bieten. Anwenderzufriedenheit hängt immer mehr von komplexen, verteilten, geschäftskritischen Anwendungen ab. Ohne eine umfassende Betrachtung der ganzen Umgebung können Probleme nicht mehr gelöst werden und wirken sich eventuell bis auf die Anwender aus. vCOPs ist ein automatisiertes Performance-Analyse-Tool für Geschäftsanwendungen und Prozesse. Es bietet Echtzeitanalysen, um Probleme proaktiv aufzuzeigen. Dies wird durch folgende Features erreicht:

- *Smart Alerts*: Informieren über bevorstehende Applikationsprobleme, lange bevor Anwender oder traditionelle Tools etwas bemerken.
- *Smart Alert Summary*: Diese Zusammenfassungen helfen Ihnen, bevorstehende Probleme zu verstehen, deren Auswirkungen und Auslöser zu identifizieren und mit reduzierten Aufwand zu vermeiden.
- *Automatic ›Health‹ Scores*: Zeigen Echtzeitinformationen über den derzeitigen Zustand der Umgebung aus zahlreichen Perspektiven.
- *Auto-Pilot Performance Dashboards*: Stellen eine kombinierte Performance-Ansicht aus allen Bereichen dar, um die Kommunikation zwischen einzelnen Abteilungen zu erleichtern.
- *On-Demand Analytics*: Kann objektive Empfehlungen basierend auf der Analyse von Kapazitäts- und Verhaltens-Trends und deren Abhängigkeiten erstellen.

vCOPs kann nicht nur als neues Monitoring Tool eingeführt werden, sondern es kann auch (historische) Daten aus bestehenden Systemen einlesen und analysieren. Der große Vorteil ist, dass vCOps keine statischen Grenzwerte verwendet, sondern diese mit der Zeit lernt. Es ist nicht notwendig, Grenzwerte für jede Applikation zu definieren, sondern diese werden selbst erlernt und auch dynamisch angepasst. Sobald vCOPs Daten sammelt, fängt es an zu lernen, wie sich die überwachte Umgebung verhält. Dabei markiert es keine Ereignisse als gut oder schlecht, sondern es benutzt Algorithmen, um eine Statistik über das Verhalten zu erstellen. Daraus errechnet es eine Metrik für den Normalbetrieb und setzt dynamische Grenzwerte. Der von vCOPs verwendete mathematische Algorithmus kann so Veränderungen sehr schnell feststellen und die Grenzwerte ständig anpassen. So kann vCOPs abnormales Verhalten sehr

sicher feststellen und Fehlalarme auch in dynamischen hoch-virtualisierten Umgebungen vermeiden. Die Ergebnisse können dann nicht nur in den vCOPs-Dashboards dargestellt, sondern auch an bestehende Tools zur weiteren Verwendung übergeben werden.

Weitere Information zu VMware vCenter Operations finden Sie unter:

http://vmware.com/de/products/datacenter-virtualization/vcenter-operations-management/overview.html

C.1.7 VMware Service Manager

VMware Service Manager ist ein Tool zur Automatisierung von IT-Service-Management. Es dient zur Darstellung von IT-Service-Workflows. So können Sie physische, virtuelle und cloudbasierte IT-Services mit einer standardisierten Methode verwalten. Die angebotenen Leistungen können dem Anwender in einem Katalog angeboten werden, und VMware Service Manager automatisiert den Anforderungs- und Freigabeprozess. In Kombination mit Cloud-Umgebungen werden dadurch vor allem folgende Vorteile geboten:

- Bietet Anwendern ein einheitliches Portal für alle Serviceanforderungen und vereinfacht dadurch die Bedingung.
- Anforderungsprozesse können verkürzt oder bei Bedarf auch vollständig automatisiert werden.
- Die strenge Einhaltung von Unternehmensrichtlinien kann sichergestellt werden.
- Dem Anwender kann eine große Auswahl an Services angeboten werden, der Zugang dazu wird eingeschränkt und überwacht.
- Vorhandene Schnittstellen zu VMware-Infrastruktur-Produkten bieten Integrationsmöglichkeiten zu bestehenden Komponenten.
- Die Kundenzufriedenheit steigt durch kürzere Prozesse und einfache Bedingung
- Änderungen für bestehende Services können beantragt werden (Change Management).
- Änderungen können zusammen mit vCenter Configuration Manager automatisiert werden.

Weitere Informationen zum VMware Service Manager finden Sie unter:

http://www.vmware.com/de/products/datacenter-virtualization/service-manager/features.html

C.1.8 vCenter Configuration Manager

VMware vCenter Configuration Manager automatisiert Konfigurations- Management für virtuelle und physische Server, indem er sämtliche Systemeinstellungen von vSphere sowie Windows, Unix, Linux-Server, Desktops und Templates überwacht und auch sehr tiefe Änderungen erkennt. Diese können Sie dann mit Industriestandards, Vorgaben oder selbstdefinierten

Einstellungen vergleichen, um Security- und Compliance-Vorgaben zu überwachen. Wird ein Verstoß erkannt, kann dieser automatisiert wieder behoben werden, oder es werden Aktionspläne zur Behebung vorgeschlagen. Gerade in dynamischen Umgebungen wird der Aufwand für die Verwaltung von verstärkten Compliance-Standards und erweiterten Security-Vorgaben immer größer. VMware vCenter Configuration Manager überwacht und sichert die Einhaltung sämtlicher Vorgaben. Dies können Sie jederzeit mit geringem Aufwand durch automatisierte Assessments kontrollieren. Als Vorlagen hierfür können Sie Industriestandards, gesetzliche Vorgaben oder auch Ihre Unternehmensstandards verwenden. Dies sichert den Betrieb und senkt den Aufwand und die Kosten für Audits erheblich.

Zusätzlich können Sie virtuelle und physische Systeme von einem zentralen Punkt aus automatisiert installieren und Softwarepakete inklusive der zugehörigen Richtlinien verteilen.

Weitere Informationen zu VMware vCenter Configuration Manager finden Sie unter:

http://vmware.com/de/products/datacenter-virtualization/configuration-manager/overview.html

Basierend auf der vCenter-Configuration-Manager-Technologie gibt es auch eine kostenlose kleine Version, den VMware Compliance Checker for vSphere. Mit ihm können Sie Ihre virtuelle Infrastruktur gegen die vSphere Hardening Guidelines oder PCI -Standards prüfen. Die aktuelle Version ist unter folgenden Links verfügbar:

- **vSphere Hardening Guidelines:**
  http://vmware.com/de/products/datacenter-virtualization/vsphere-compliance-checker/overview.html
- **VMware Compliance Checker for PCI:**
  http://vmware.com/de/products/datacenter-virtualization/pci-compliance-checker/overview.html

C.1.9 vFabric tc Server

VMware vFabric tc Server ist der Runtime-Server der VMware-vFabric-Cloud-Application-Plattform. Er bietet die Möglichkeit, Spring-Anwendungen mit Hilfe von mitgelieferten Spring-Entwicklungstools wesentlich schneller als im Vergleich zu herkömmlichen JEE-Servern zu entwickeln. Spring ist derzeit das weltweit am meisten genutzte Java-Framework. Entwickler werden mit vFabric tc Server sehr schnell vertraut sein, da er auf Tomcat basiert und zu 100 % kompatibel ist. Einen effizienten Betrieb ermöglicht seine reduzierte Arbeitsspeicherauslastung und »Elastic Memory for Java (EM4J)«-Technologie. Dabei kann Arbeitsspeicher dynamisch ohne Performanceeinbußen zwischen Java virtuellen Maschinen geteilt werden. Zusammen mit der »VMware vSphere Memory Balloon«-Technologie können so kleinere virtuelle Maschinen für den Betrieb von tc Server verwendet werden. Daraus ergeben sich höhere Virtualisierungsraten pro Host und verbesserter ROI der virtuellen Infrastruktur.

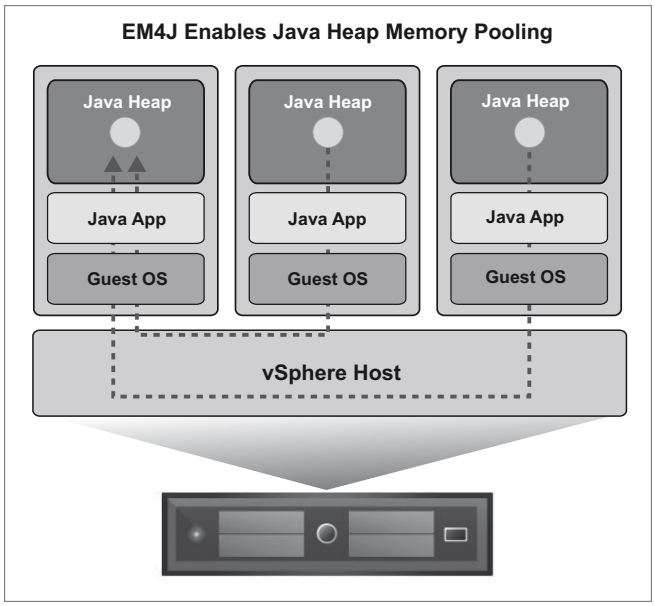


Abbildung C.6 VMware vFabric tc Server Elastic Memory for Java

Für den Betrieb bieten die mitgelieferten Tools auch die Möglichkeit, Anwendungen zu überwachen und ermöglichen tiefe Einblicke in die Ausführung. Dies ermöglicht es dem Anwendungsbetreuer, sicherzustellen, dass der ausgeführte Spring-Code die erwartete Performance erfüllt, oder bei Problemen einzelne Transaktionsabläufe zu isolieren, um den problematischen Code schnell zu analysieren.

Weitere Informationen zu VMware vFabric tc Server finden Sie unter:

http://www.vmware.com/products/application-platform/vfabric-tcserver/overview.html

C.1.10 Fabric GemFire

Die Bereitstellung moderner Applikation erfolgt immer öfter webbasiert. Zudem sind sie größtenteils sehr datenintensiv und werden in virtualisierten Cloud-Umgebungen betrieben. Daraus resultiert, dass Datenbanken immer mehr an Bedeutung gewinnen und dementsprechend verfügbar sein müssen, bei gleichzeitig hohen Performanceanforderungen. Es wird immer häufiger zu einem Problem, wenn Datenbanken mit wachsenden Anforderungen nicht dynamisch skalieren können. VMware vFabric GemFire liefert hohe Performance und dynamische Skalierung, verbunden mit den Datenmanagement und Zuverlässigkeit einer Datenbank. Eine verteilte Datenmanagement-Plattform bietet Funktionen wie Datenreplikation, Daten-aware-Routing und konstante Abfragen, und die erwartete Performance können Sie durch ein Scale-out-Design dynamisch erweitern. GemFire basiert auf einer neuen Architektur, die Daten partitioniert über einen Cluster verteilt. Kombiniert mit einem speziellen Fest-

platten-Logging-.Algorithmus, verteilten Anwendungsfunktionen, automatisierter Datenverteilung, und ständigem Client-Load-Balancing wird eine extrem hohe Performance erreicht. Ein eingebauter Wiederherstellungsmechanismus garantiert Datenkonsistenz und Verfügbarkeit, falls ein Cluster-Node ausfallen sollte.

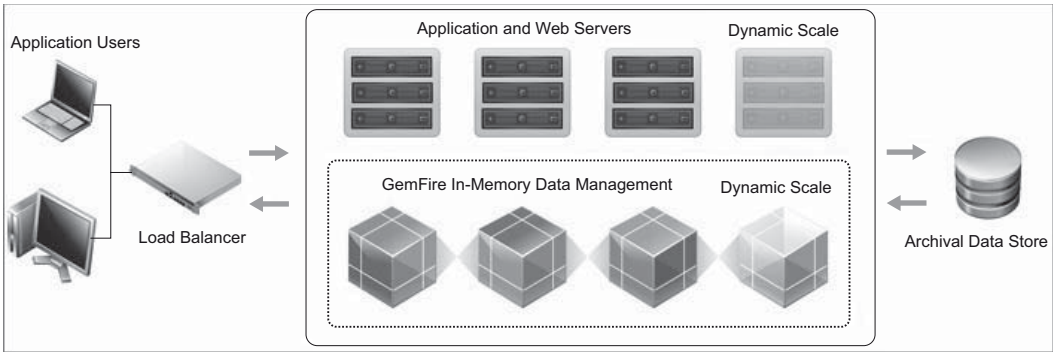


Abbildung C.7 VMware GemFire – Scale-out

Weitere Informationen zu VMware vFabric GemFire finden Sie unter folgendem Link:

http://www.vmware.com/de/products/application-platform/vfabric-gemfire/overview.html

C.1.11 vFabric Enterprise Ready Server

Enterprise Ready Server (ERS) ist das bekannteste und umfassendste Apache-Webserver- und Load-Balancing-Paket. Einfach bereitzustellen, optimiert für Performance und volle Unterstützung von VMware sind die wichtigsten Merkmale. ERS wird auch sehr oft für SSL-Entschlüsselung, PERL, PHP und C-Anwendungen, URL-Umleitung, FTP und Authentifizierung und Zugriffssteuerung verwendet. ERS wird auf den gängigsten Betriebssystemen bereits vorkompiliert und ist inklusive der zugehörigen Batches auch unterstützt. Dadurch es ist nicht mehr notwendig, eigene Module zu kompilieren und bereitzustellen. Hier auf standardisierte Komponenten zu setzen, erhöht die Sicherheit für Ihre Webanwendungen. Sicherheitslücken in aktuellen Systemen sind VMware schon oft vor der Veröffentlichung bekannt (ASF Security Community). Sie erhalten aktuelle Information zu möglichen Bedrohungen und auch die benötigten Updates, um Sicherheitslücken zu schließen.

Weitere Informationen zu vFabric Enterprise Ready Server finden Sie unter:

http://www.vmware.com/de/products/application-platform/vfabric-enterprise-ready-server/overview.html

C.1.12 vFabric Hyperic

vFabric Hyperic ist die führende Plattform für die Überwachung weborientierter und unternehmensspezifischer Anwendungen sowie für das Performance-Management. Der große Vor-

teil in Kombination mit Cloud-Umgebungen ist, dass neue VMs automatisch erkannt werden, über 75 gängige Webanwendungstechnologien automatisiert überwacht werden und erweiterte Warnmeldungsfunktionen Fehlalarme reduzieren. Dadurch erreichen Sie eine umfassende Transparenz, reduzierte Ausfallszeiten und die Einhaltung von SLAs.

Weitere Informationen zu vFabric Hyperic finden Sie unter:

http://www.vmware.com/de/products/application-platform/vfabric-hyperic/overview.html

C.1.13 RabbitMQ

Moderne Webanwendungen wie z. B. der VMware vCloud Director verwenden Messaging zwischen den Anwendungskomponenten und zur Verbindung mit anderen Services. Ohne Messaging laufen die Anwendungen mit der Geschwindigkeit der langsamsten Komponente. Durch die Entkoppelung der Anwendungskomponenten können Skalierbarkeit, Flexibilität der Anwendung gesteigert werden. vFabric RabbitMQ ist eine effiziente, hochgradig skalierbare und einfach bereitzustellende Queuing-Software, die für die Abwicklung von Messaging-Datenverkehr entwickelt wurde. Basierend auf offenen Standardprotokollen (AMQP) und einer bewährten Plattform ist RabbitMQ völlig unabhängig von spezifischen Bibliotheken. Durch breite Protokoll- und Plattformunterstützung ermöglicht es eine große Wahlfreiheit und Kosteneinsparungen bei der Integration. RabbitMQ bietet einen einheitlichen Messaging-Ansatz über mehrere Stacks und Plattformen hinweg.

Weitere Informationen zu vFabric RabbitMQ finden Sie unter:

http://www.vmware.com/de/products/application-platform/vfabric-rabbitmq/overview.html

VMware hat mit vSphere 5 und dem Wegfall des ESX Servers mit Service Console wesentliche Neuerungen im Sicherheitsumfeld eingeführt. Diese reichen von neuen Firewall-Funktionen bis hin zu Compliance-Software.

D vCenter Operations

Autor dieses Kapitels ist Dennis Zimmer, opvizor GmbH – opvizor.com, virtuellemaschinen@email.de – vmachine.de

vCenter Operations wurde 2011 von VMware in drei Varianten angekündigt, Standard, Advanced und Enterprise, wovon zur Drucklegung des Buches nur die Standard-Edition zum Download verfügbar ist. Außerdem ist eine VMware View Edition geplant.

vCenter Operations ist ein Realtime-Monitoring-Tool, das neben den erweiterten Überwachungsfunktionen auch Funktionen zur Analyse der Ressourcenkonfiguration bietet. Damit lässt sich direkt der Gesundheitsstatus von ESX-Hosts und virtuellen Maschinen abfragen und überwachen, aber auch eine Root-Cause-Analyse betreiben, d. h. untersuchen, welche Konfigurations- oder Performanceprobleme zu dem entsprechenden Gesundheitszustand beitragen. Außerdem erlernt vCenter Operations den »Normalstatus« und kann auf Anomalien hinweisen, was definitiv einen großen Vorteil darstellt.

Durch die Abstraktion von technischem Detailwissen auf leicht verständliche Anzeigen hilft vCenter Ops auch technisch weniger versierten Personen, Fehlkonfigurationen zu verstehen. Um die Schwachstellen jedoch zu beheben, muss man auf entsprechendes technisches Personal in Form von internen Administratoren oder externen Beratern zurückgreifen.

vCenter Operations bietet zusammengefasst folgende Funktionen:

- automatisiertes Performance-, Kapazitäts- und Konfigurationsmanagement
- in Drittanbieterlösungen integrierbare Managementkonsole ab Enterprise Edition
- fortlaufende Compliance-Analyse und Standardisierung

vCenter Operations setzt auf eines der modernsten Dashboards (Abbildung D.1) auf, die aktuell am Markt verfügbar sind. Allerdings wird größtenteils Flash eingesetzt, womit Apple iPad und andere mobile Geräte ein Problem haben. Farbige Kacheln zeigen die Zustände der Systeme an. Um auch eine Übersichtlichkeit bei sehr großen Infrastrukturen zu gewährleisten, werden die Systeme automatisch gruppiert und können gefiltert werden.

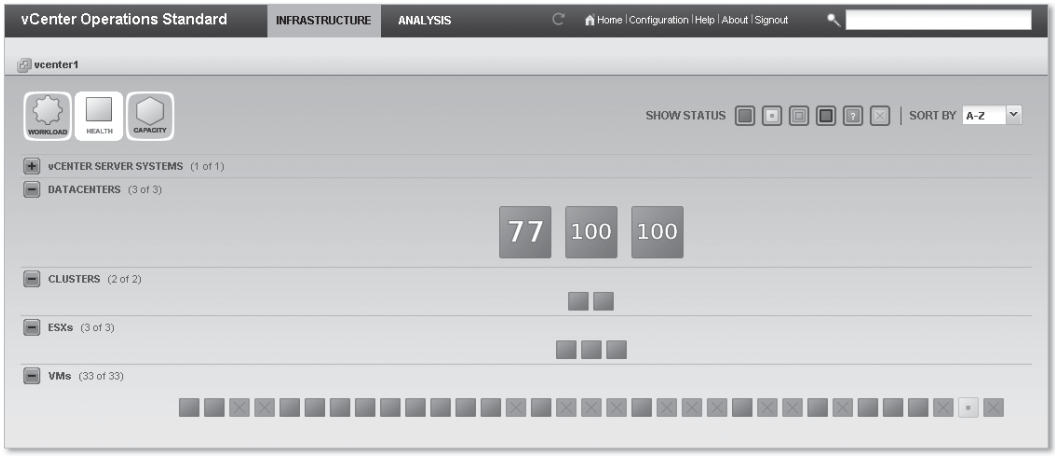


Abbildung D.1 vOps-Dashboard

Wählen Sie die DETAILS-Ansicht eines Objekts aus, z. B. einer virtuellen Maschine, erhalten Sie die aktuellen Leistungsdaten sowie relevante Events in einer Übersicht (Abbildung D.2).

Sind Sie auf ein Problem gestoßen, können Sie dieses in Echtzeit analysieren und werden durch sinnvolle Vorgaben und Statistiken sehr gut unterstützt (Abbildung D.3).

Unter folgenden URLs finden Sie Anleitungen und Informationen zu vCenter Operations:

- *http://virtualizationreview.com/articles/2011/05/04/how-vcenter-operations-can-help-you.aspx*
- *http://www.zdnet.com/blog/virtualization/second-take-on-vmware-vcenter-operations/2895*
- *http://www.zdnet.com/blog/virtualization/vmware-vcenter-operations/2834*
- *http://vninja.net/virtualization/installing-and-configuring-vmware-vcenter-operations/*

Echtzeit bedeutet leider immer, dass Sie sich mehr auf offensichtliche Probleme auf oberflächlichem Level beschränken müssen. vCenter Operations stellt daher eine ideale Kombination mit Analysetools wie Opvizor dar, da vCenter Ops in Echtzeit Schwachstellen anzeigen und analysieren kann, Opvizor allerdings deutlich mehr in die Tiefe von Konfigurations- und Protokolldaten zur Analyse geht, um eine proaktive Überwachung der Infrastruktur zu ermöglichen.

Dadurch steht vCenter Operations allerdings in direkter Konkurrenz zu Veeam-, vKernel- und SolarWinds-Produkten.

Abbildung D.2 Detailansicht einer VM mit Events und Storage-Informationen

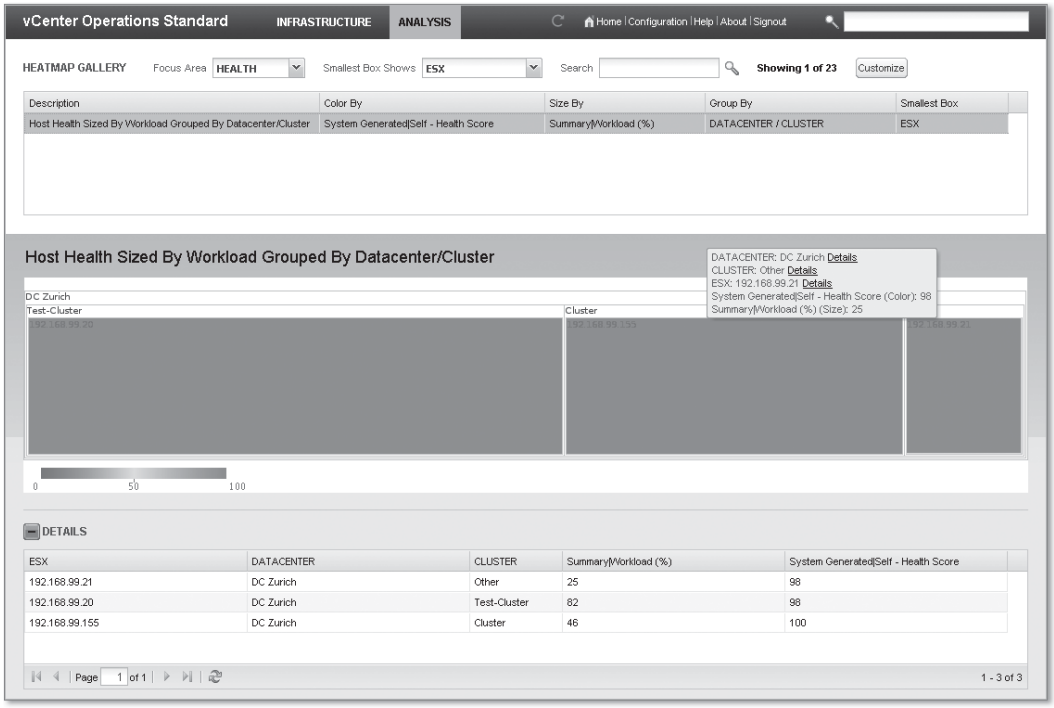


Abbildung D.3 Analyse eines Problems mittels vOps

D.1 Lizenzierung

vCenter Operations Standard wird pro virtueller Maschine berechnet und ist in 25er-Bundle verfügbar. Der Listenpreis beginnt bei 1.560,49 € pro 25 VMs und endet bei 2.111,34 € je nach Support-Level (Basic oder Production) und Anzahl der Wartungsjahre (1–3).

Die Virtualisierung von physischen Infrastrukturen hat sich im Bereich der Server-Landschaften bereits etabliert. Ein ähnliches Potential für die Virtualisierung steckt in den dezentralen IT-Infrastrukturen, also in den Clients an den Arbeitsplätzen der Anwender. Dabei kann das Verfahren der Desktop-Virtualisierung in Kombination mit Cloud-Computing zukünftig sogar so weit gehen, dass selbst ein Privatanwender – zu Hause – einen aus Software bestehenden Computer über das Internet nutzt.

E Die Virtualisierung des Desktops

Autor dieses Kapitels ist Günter Baumgart, guenter.baumgart@anmax.de

Wie im Anleser bereits deutlich wird, handelt es sich bei der Virtualisierung von Desktops prinzipiell um das gleiche Thema wie das bei der Virtualisierung der Server in den Rechenzentren. Bei dieser Art der Virtualisierung werden einfach die Desktop-Computer virtualisiert. Das bedeutet, dass in einem Host den Anwendern individuell konfigurierte Betriebssysteminstanzen zur Verfügung gestellt werden. Jeder Anwender arbeitet somit in seiner eigenen virtuellen Benutzermaschine. Bei dieser virtuellen Benutzermaschine handelt es sich nicht um eine Ressource, die sich mehrere Benutzer teilen müssen. Diese virtuelle Benutzermaschine, verhält sich genauso wie ein vollständiger lokaler Computer. In diesem Punkt unterscheidet sich diese Technologie grundsätzlich von der des Terminal-Servers. Es gibt viele Hersteller, die mit unterschiedlichsten Verfahren und Techniken mögliche Lösungsszenarien bereitstellen. Jedes dieser Verfahren zur Desktop-Virtualisierung bringt unterschiedlichste Funktionalitäten und Möglichkeiten mit. Auch sind die Ansichten, was der Hersteller unter Desktop-Virtualisierung versteht, höchst unterschiedlich.

Oftmals entscheiden aber auch die Anforderung aus den einzelnen Projekten darüber, welches der Verfahren oder besser gesagt welches Produkt sich im vorliegenden Fall am besten eignet. Selbst Kombinationen der einzelnen Produkte unterschiedlicher Hersteller sind nicht selten anzutreffen. In den einzelnen Unternehmen weichen die Anforderungen von Organisationseinheit zu Organisationseinheit oftmals so voneinander ab, dass Kombinationen verschiedener Produkte und Hersteller zwingend notwendig sind, um die gestellten Aufgaben zu lösen. In diesem Kapitel werden wir aber ausschließlich auf die Desktop-Virtualisierungs-Lösung des Herstellers VMware eingehen. VMware stellt zu diesem Zweck sein Kernprodukt View für die Virtualisierung von Desktops zur Verfügung. Da sich das Thema Desktop-Virtualisierung als enorm umfangreich darstellt und zu einer professionellen Desktop-Virtualisierung auch zwingend unterschiedliche Anrainerprodukte notwendig sind, können Sie sich in diesem Kapitel leider nur einen groben Überblick verschaffen. Möchten Sie allerdings tiefer in

dieses Thema einsteigen, empfehle ich Ihnen mein neues Buch zum Thema Desktop-Virtualisierung (ISBN 978-3-8362-1787-3), das für Anfang 2013 bei Galileo Computing geplant ist.

Bei allen Bemühungen, die Virtualisierung von Computern voranzutreiben und so weit wie möglich zu virtualisieren, stoßen wir unweigerlich an unterschiedliche Grenzen. Eine dieser Grenze ist das Endgerät, an dem der Anwender letztendlich seine Arbeitet verrichtet. Diese Schnittstelle zwischen Mensch und Maschine wird zwar für den Menschen immer komfortabler – denken Sie zum Beispiel an eine Microsoft Xbox mit Kinect-Sensor –, aber Sie werden immer an dieser Stelle noch ein Gerät benötigen. Wir werden dieses Gerät im weiteren Verlauf einfach »Device« nennen. Ein Device kann unterschiedliche Formen haben: Es kann ein normaler PC sein, aber auch ein Tablet, ein Thin-Client, ein System-on-Chip oder auch ein Zero-Client. Letzterer verfügt über kein integriertes Betriebssystem, sondern lediglich über eine Integration von einzelnen Diensten oder Protokollen direkt auf der Basis von Hardware. Derartige Devices vermitteln Ihnen unter anderem im Zuge des Anmeldeprozesses eine extreme Performanz.

E.1 Desktop-Management mit VMware View

Doch kommen wir zurück zur Desktop-Virtualisierung mit View. Die Desktop-Virtualisierung optimiert die Administration des herkömmlichen Desktops. Da sich der virtualisierte Desktop ja in Ihrem Rechenzentrum und nicht mehr in der dezentralen Infrastruktur befindet, werden die Wege natürlich erheblich kürzer für Sie. Themen wie Backup und Wiederherstellung, das Klonen von Desktops etc. sind dann vollständig innerhalb Ihrer Rechenzentrumsstruktur zu erledigen. Sie können sämtliche Funktionalitäten, die Ihnen die Virtualisierung mit vSphere bietet, nun auf den Desktop anwenden. Das Patch-Management, die Softwareverteilung und auch die Migration von Betriebssystemen werden so einfach und überschaubar wie nie zuvor. Da Sie Devices einsetzen, die nahezu wartungsfrei betrieben werden können, und der Aufwand von Seiten der Einrichtung eher als geringfügig einzustufen ist, vermeiden Sie mit derartigen Technologien erheblichen administrativen Aufwand.

Allerdings müssen Sie sich bei Einsatz dieser Technologie immer darüber im Klaren sein, dass die Verbindung bzw. der Kanal zwischen Device und der virtuellen Desktop-Maschine, also Ihrem Rechenzentrum, eine sehr hohe Verfügbarkeit benötigt. Diese Verbindung sollte immer mit einem Service-Level-Agreement (SLA) hinterlegt sein, unabhängig davon, ob es sich um LAN- oder WAN-Strecken handelt. Da View mittels PCoIP den Desktop aus dem Rechenzentrum zum Device hin übermittelt, ist bei Nichtverfügbarkeit der Strecke auch kein Arbeiten mit View möglich. Aber nicht nur die Anforderungen an Verfügbarkeit der Verbindung sind wichtig, sondern auch die Qualität der Verbindung muss stimmen! PCoIP stellt zwar Mechanismen wie dynamische Bandbreitenanpassung zur Verfügung oder kompensiert temporäre Leistungseinbrüche zum Beispiel in Form von erhöhter Latenz, aber grundsätzlich sollten die verwendeten Strecken den Anforderungen im Hinblick auf ausreichende Ressourcen genügen. Stimmen dann die soeben besprochenen Rahmenparameter, steht multimedia-

len Anforderungen wie Flash oder denjenigen, die im Umfeld von CAD-(Computer Aided Design-) oder GIS-(Geographisches Informationssystem-)Anwendungen entstehen, auch im WAN nichts mehr im Wege.

View wurde von VMware für den Betrieb innerhalb von vSphere konzipiert und dementsprechend optimal angepasst. Wie bereits erwähnt, stehen die Funktionen, die Sie aus der vSphere-Server-Virtualisierung her kennen, auch den Benutzer-Desktops respektive View zur Verfügung.

View kann auf einem Server mit Windows 2008 R2 64 Bit installiert werden und benötigt auch in dieser Version keine Schemaerweiterung des Active Directorys. Alle Daten werden in einer lokalen AD-LDS-Instanz (Active Directory Lightweight Directory Services) gespeichert. Die Datensicherung dieser AD-LDS-Instanz ist ebenfalls bereits in das Produkt integriert. Sollten Sie ein Update planen, schlagen Sie in jedem Fall im Dokument »VMware View-Upgrades« unter *http://www.vmware.com/files/de/pdf/view_5_upgrade_guide_de-de.pdf* nach.

Abbildung E.1 zeigt eine View-Umgebung. Diese sehr vereinfachte und auf die Grundelemente reduzierte Darstellung des Frameworks soll Ihnen einen ersten Einblick in das Thema ermöglichen.

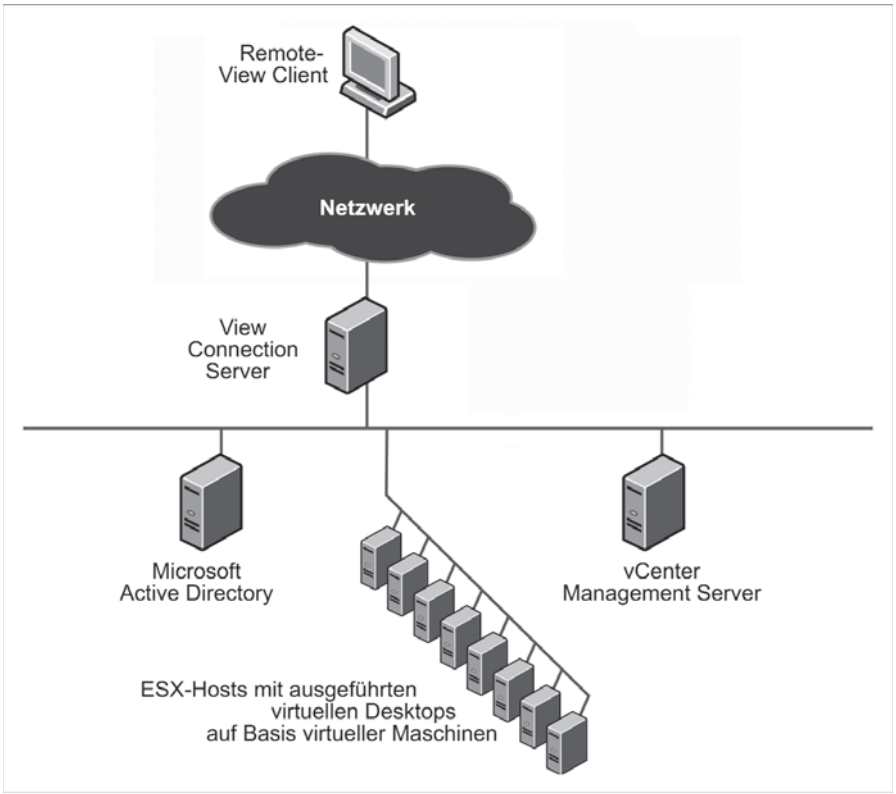


Abbildung E.1 Einfache Struktur einer VMware-View-Umgebung

In der einfachsten Form kann View mit sehr wenigen Elementen aufgebaut werden. Wenn Sie Abbildung E.1 betrachten, werden Sie feststellen – vorausgesetzt, Sie sind bereits mit vSphere vertraut –, dass Sie augenscheinlich bis auf zwei Elemente bereits alles kennen. Der Betrieb einer derartigen Umgebung ist zwar keinesfalls ratsam, aber zur Erläuterung für einen ersten Einstieg oder einen Test ideal geeignet. Sie benötigen also in jedem Fall einen View Client, einen View Agent, was aus dieser Abbildung nicht hervorgeht – dieser muss in jedem der virtuellen Desktops vorhanden sein –, und natürlich einen Connection-Broker bzw. View Manager, den View-Connection-Server.

In Abbildung E.2 sehen Sie eine bereits wesentlich umfangreichere Darstellung, wobei auch hier lediglich ein Server, der View Manager, als Connection-Broker schematisch dargestellt wurde. In einer professionellen Umgebung handelt es sich an dieser Stelle, ohne eine Lastausgleichsbetrachtung oder Redundanzen einzubeziehen, um bis zu vier Serversysteme.

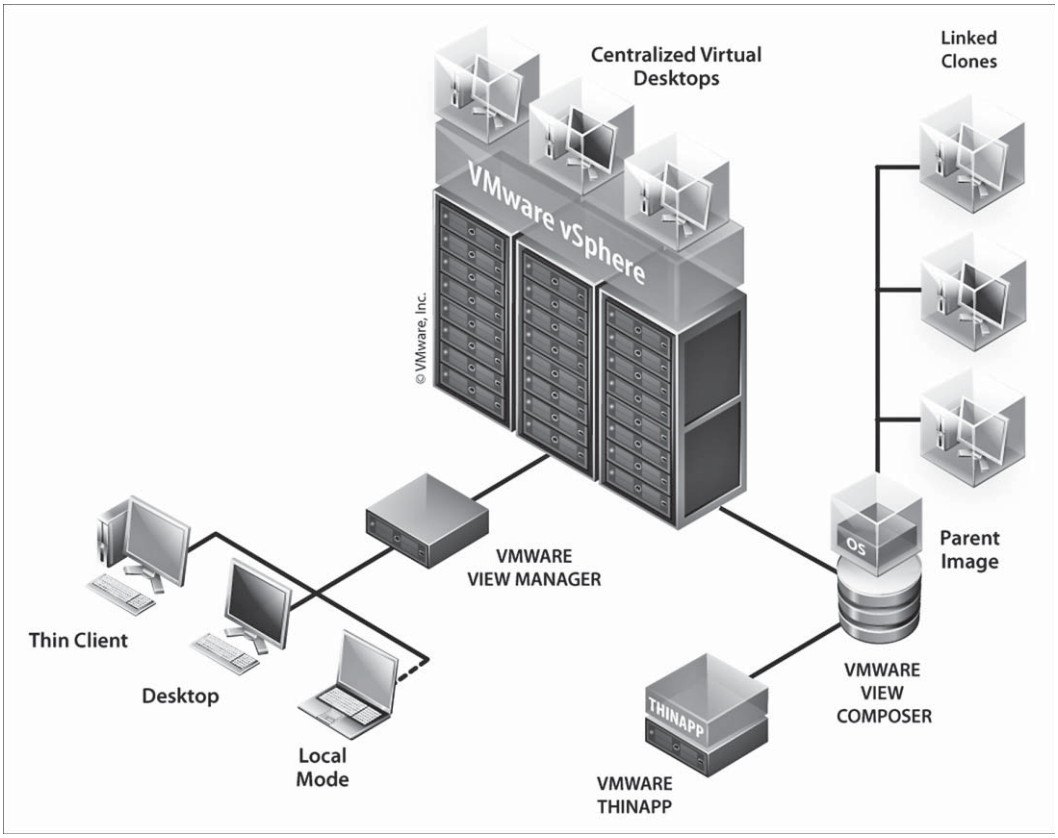


Abbildung E.2 Erweiterte Struktur einer VMware-View-Umgebung (Virtual Machine – VM)

An dieser Stelle können Sie bereits erahnen, dass mit einer zunehmenden Anzahl der zu betreibenden Desktops sowie einer Bereitstellung von erweiterter Funktionalität sehr schnell ein äußerst umfangreiches und komplexes Gebilde entsteht. Viele Großunternehmen verfü-

gen bereits über eine Virtual Desktop Infrastructure (VDI), planen gerade eine solche oder bauen sie auf. Gerade die Vorteile, die diese Technologie im Umfeld von Unternehmenssicherheit und -Compliance bietet, sind ausgezeichnet. Das Thema Niederlassungsanbindung an die zentrale IT des Unternehmens lässt sich mit View sehr einfach gestalten. Auch können mittels Local Mode – ebenfalls ein Merkmal des View-Frameworks – mobile Desktops realisiert werden. Hierbei sind Offlinearbeitsplätze von Mitarbeitern, die beispielsweise mit Notebooks ausgestattet sind, in Übereinstimmung mit der Unternehmenssicherheit und -Compliance problemlos möglich.

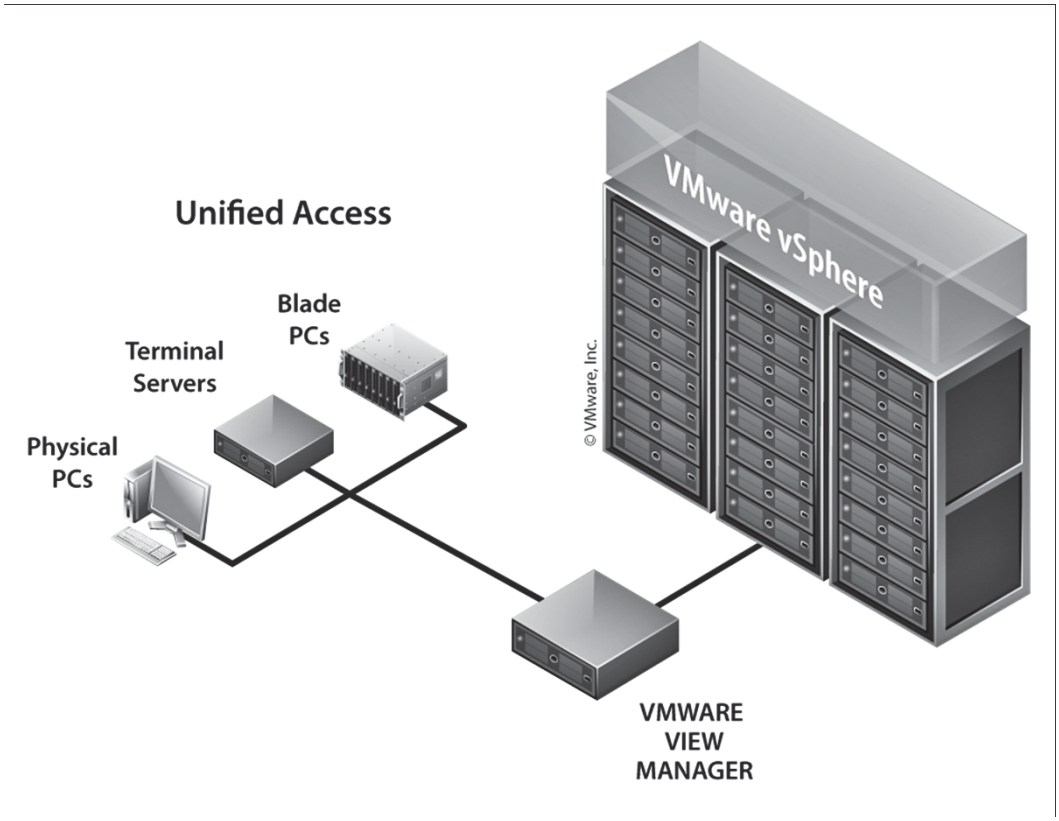


Abbildung E.3 Erweiterte Struktur einer VMware-View-Umgebung (Physical Machine – PM)

Handelte es sich bei den Desktops, die mittels View Client in Abbildung E.2 dem Benutzer zur Verfügung gestellt wurden, um Virtual Machines (VMs), so sehen Sie in Abbildung E.3, dass auch durchaus Physical Machines (PMs) dem Anwender mittels View Client bereitgestellt werden können. Des Weiteren können Sie Abbildung E.3 entnehmen, dass auch die Sessions eines Terminal-Servers dem Benutzer mittels View Client angezeigt werden können. Das Fazit dieser Aussagen ist, dass mittels View quasi ein einheitlicher Zugriff auf eine ganze Menge an unterschiedlichen Quellsystemen möglich ist.

Ebenfalls zum View-Framework gehört die Virtualisierung von Applikationen mit ThinApp. Auf dieses Thema werden wir in Abschnitt E.3, »Virtualisierung von Applikationen mit ThinApp«, noch eingehen.

VMware View steht in zwei unterschiedlichen Paketen zur Verfügung; Sie können eine Enterprise- und auch eine Premier-Edition erwerben, die die folgenden Merkmale aufweisen:

- **Premier-Edition**
  - ESXi Installable
  - vCenter Server
  - View Manager
  - View Composer
  - Local Mode
  - Workstation
  - ThinApp
  - vShield Endpoint
- **Enterprise-Edition**
  - ESXi Installable
  - vCenter Server
  - View Manager

Der Unterschied zwischen den Versionen liegt darin, dass bei der Premier-Edition eine Version der VMware Workstation und die Produkte ThinApp und vShield Endpoint enthalten sind. Für all diejenigen, die sich etwas genauer über vShield Endpoint Security informieren möchten, empfehlen wir einen Blick in das Datasheet von VMware, das Sie unter *http://www.vmware.com/files/de/pdf/VMware-vShield-Endpoint-Datasheet.pdf* finden.

Nachfolgend möchten wir etwas detaillierter auf die einzelnen Komponenten des View-Frameworks eingehen. Hierzu eine Auflistung der Komponenten, die wir im weiteren Verlauf dieses Kapitels ansprechen werden:

- View Manager
- View Client
- View Agent
- View Composer
- Local Mode
- ThinApp

E.1.1 Wichtige Begriffe

Im weiteren Verlauf dieses Kapitels werden wir unterschiedliche Begriffe verwenden, die wir zur besseren Verständlichkeit kurz erläutern möchten. Sind Ihnen diese Begriffe bereits bekannt, lesen Sie einfach bei Abschnitt E.1.2 weiter.

Individuelle Desktops sind bereitgestellte virtuelle oder physische Einzelmaschinen, die mittels View Client direkt als virtuelle Desktops genutzt werden können.

Pools bezeichnen mehrere Desktops, die zu einem Pool – also einer Einheit – zusammengefasst wurden. Hierbei ist es unerheblich, ob es sich bei dem Inhalt des Pools um Virtual Machines vom Type Linked Clone oder Individuell Desktop oder etwa um eine Physical Machine handelt.

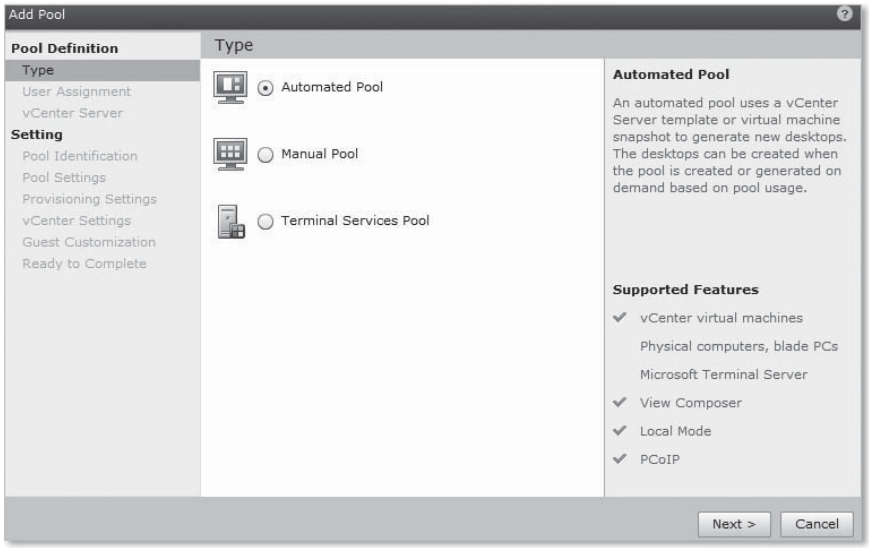


Abbildung E.4 Erstellung eines Automated Pools

Der Gestaltungsfreiraum bei der Erstellung von Pools ist immens. Fast jede erdenkliche Kombination zur Erstellung von Desktops in Pools ist möglich. Beim Anlegen des Pools können Sie neben dem Namen, der Anzahl der verfügbaren Arbeitsplätze und dem Verhalten bei Nichtbenutzung die unterschiedlichsten Parameter einstellen.

Ein *Automated Pool*, wie er in Abbildung E.4 angelegt wird, bedeutet, dass virtuelle Maschinen bereitgestellt werden. Diese Desktops werden entweder auf der Basis von Templates als Full Clone oder als Linked Clones eingerichtet. Ein Automated Pool erstellt die Desktops autark, also vollständig automatisiert. Ein Eingriff durch den Administrator ist während der Erstellung nicht erforderlich!

Ein *Manual Pool* umfasst eine Gruppe von bereits vorhandenen Virtual Machines, Physical Machines oder Blade-PCs, auf denen ein View Agent installiert ist. Die dritte Auswahl erlaubt

den Einsatz von Terminal Services in Form eines Pools. Die Anwender erhalten nach der Anmeldung dann ihre Session auf dem MS Terminal Server.

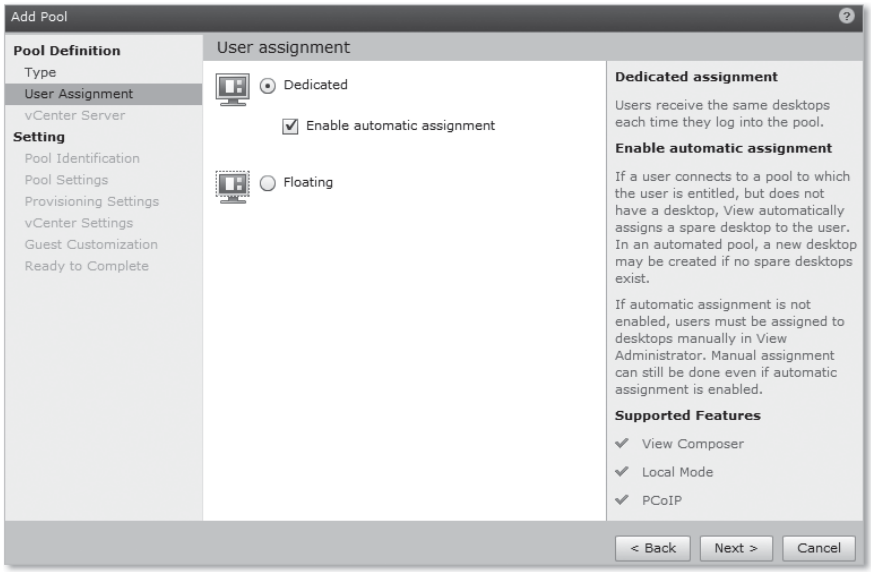


Abbildung E.5 Erstellung eines Dedicated Pools

Auf einen Pool haben entweder einzelne Benutzer oder Benutzergruppen Zugriff. Im Fenster aus Abbildung E.5 können Sie zum Beispiel festlegen, ob ein Benutzer sich immer mit dem gleichen Desktop verbinden darf, also eine so genannte DEDICATED-Zuweisung erhält. Möchten Sie allerdings genau das Gegenteil erreichen, weisen Sie stattdessen einfach FLOATING zu. Bei FLOATING würde der Benutzer bei jeder Anmeldung mit einem neuen Desktop verbunden.

In den vergangenen Versionen wurde zwischen persistentem und nichtpersistentem Pool unterschieden. Beziehen Sie nun die aktuellen Bezeichnungen ein, lautet die Definition: Bei der Auswahl der Option DEDICATED wird ein persistenter und bei der Option FLOATING ein nichtpersistenter Pool erstellt.

Im Fenster aus Abbildung E.6 wählen Sie aus, ob Sie einen Desktop einbeziehen möchten, der unter der Verwaltung von vCenter steht, oder nicht.

Blade-PCs: Der Formfaktor Blade ist auch bei den Clients möglich. Mit Blade-PCs oder Blade-Workstations lassen sich zentralisierte Infrastrukturen realisieren, die einfach zu verwalten sind. Anwender greifen mittels View darauf zu.

Terminal-Server werden seit geraumer Zeit in vielen Unternehmen zur zentralen Bereitstellung von Anwendungen eingesetzt. Wie bereits erwähnt können Sie diese Anwendungen ebenfalls durch den View Manager dem Anwender zur Verfügung stellen.

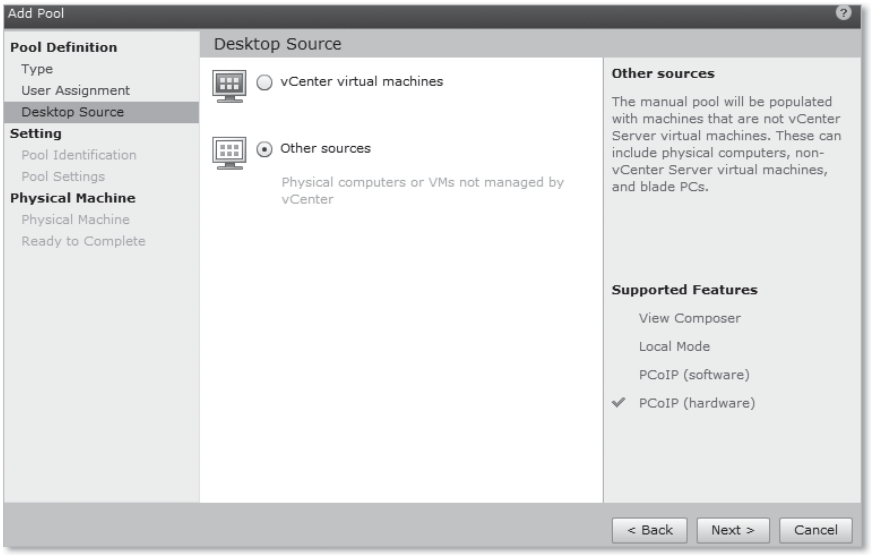


Abbildung E.6 Erstellung eines Pools gefüllt mit zum Beispiel PMs

Verfügbarkeit: Sie können 7 Connection-Server-Instanzen (5 + 2 Reserve) zusammenfassen, wobei die maximale Anzahl der gleichzeitigen Verbindungen bei 10.000 liegt. Durch diese Zusammenfassung wird einerseits die Verfügbarkeit erhöht und zum anderen die Skalierbarkeit verbessert. Für den Ausgleich der Belastungen zwischen den Connection-Server-Instanzen können Sie zum Beispiel den Microsoft Network Load Balancer (NLB) einsetzen. Natürlich können Sie aber auch andere Systeme zum Lastausgleich, wie beispielsweise Load Balancing Appliances von F5, verwenden.

E.1.2 View Manager

Eine Aufgabe der Server-Komponente namens View Manager, oftmals auch »Connection-Manager« oder »Connection-Broker« genannt, ist es, die Verbindungen zwischen dem Benutzer und dem Desktop zu ermöglichen. Bei erfolgreicher Authentifizierung des Anfragenden wird der Bildschirm des entfernten Desktops übertragen. Der View Manager gestattet es auch den Administratoren der View-Umgebung, über einen einzigen Kontrollpunkt virtuelle Desktops bereitzustellen, zu verwalten, zu kontrollieren und zu reglementieren. Integrierte Sicherheitsfunktionen sorgen dafür, dass alle Daten und Informationen im Rechenzentrum verbleiben. Der View Manager stellt Ihnen für Ihre Arbeit als administrative Schnittstelle die View-Manager-Verwaltungskonsole mit Dashboard-Anzeige, Abbildung E.7, zur Verfügung.

Auch bedient sich der View Manager der Funktionalität des vCenter-Servers, um die Benutzer-Desktops innerhalb der vSphere-Umgebung dem Benutzer zur Verfügung zu stellen. Wie in Abschnitt E.1, »Desktop-Management mit VMware View«, bereits erwähnt, wird der Verzeichnisdienst Active Directory zur Benutzerauthentifizierung und -verwaltung verwendet.

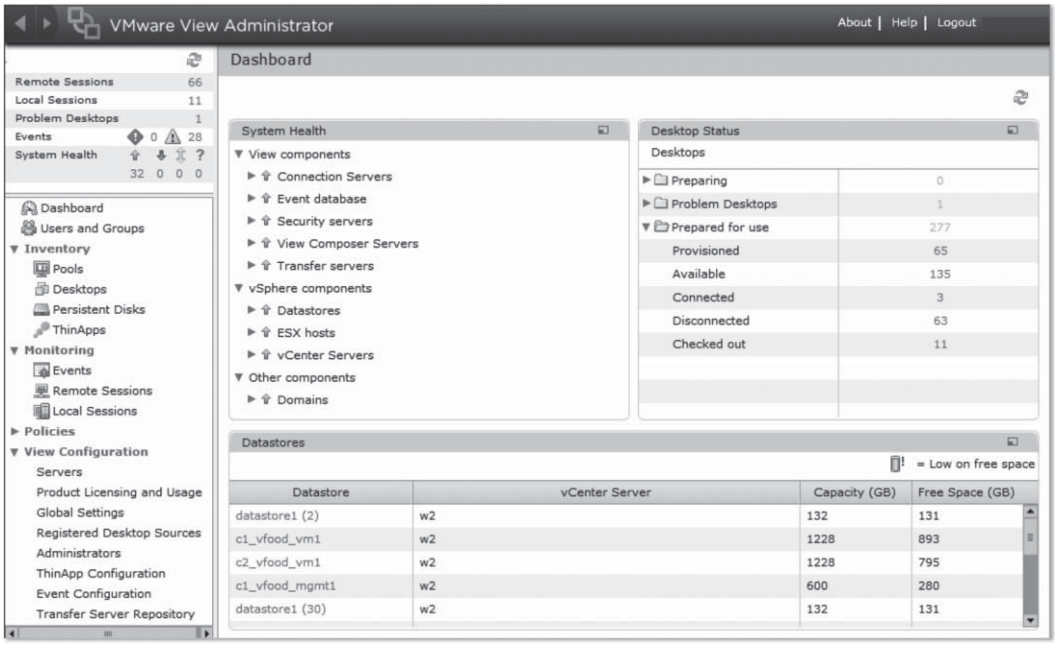


Abbildung E.7 View-Manager-Verwaltungskonsole mit Dashboard-Anzeige

An dieser Stelle sei noch kurz erwähnt, dass VMware ab der Version View 5 unter der Bezeichnung *Persona Management* ein eigenes User-Profil-Management in View integriert hat. Das Wesentliche daran ist, dass nun eine Abstraktion der Benutzerdaten und Benutzereinstellungen vom Betriebssystem möglich ist. Dadurch lassen sich Images wesentlich einfacher von mehreren Benutzern gleichzeitig nutzen.

E.1.3 View Client

Der View Client läuft auf einem Windows-PC mittels VMware View Client oder beispielsweise auf einem Linux-PC mittels VMware View Open Client. Auf einem iPad können Sie zum Beispiel mittels der App Wyse Pocket Cloud oder der VMware View App Ihren Desktop erreichen. Die Anzahl der Möglichkeiten, Ihren View-Desktop zu erreichen, sind sehr umfangreich. Fast jedes auf dem Markt erhältliche Device erlaubt Ihnen einen Zugriff auf Ihren View-Desktop. Prinzipiell kann zwischen einem Webzugriff und dem Zugriff über den View Client unterschieden werden. Der Webzugriff wird als *View Portal* bezeichnet und kann mittels Internet-Browser (aktuell nur Microsoft Internet Explorer) und einer implementierten ActiveX-Komponente genutzt werden. Die Clients unterscheiden sich teilweise erheblich in ihrem Funktionsumfang. So sollten Sie im Vorfeld immer überprüfen, ob sich der ausgewählte Client auch für Ihren Einsatzzweck eignet. Gerade im Umfeld von Linux gibt es unterschiedliche Varianten von View Clients. Ging es in den vergangenen Versionen lediglich um die Frage der Multimedia-Redirection, so kommt in der aktuellen Version die Frage der Protokollunterstüt-

zung hinzu. In der Regel können Sie aber davon ausgehen, dass die kommerziellen Linux-View-Clients, die die Hersteller von Thin-Clients in ihren Geräten anbieten, die größtmögliche Funktionsabdeckung bieten.

Starten Sie nun den View Client zum Beispiel auf einem Windows 7-PC, wird eine Verbindung zum View-Connection-Server aufgebaut. Nach einer erfolgreichen Authentifizierung werden Ihnen wie in Abbildung E.8 alle Ihre zugeordneten virtuellen Desktops als Auswahl angeboten. Nachdem Sie den entsprechenden Desktop ausgewählt haben, öffnet sich Ihr Desktop, und Sie können mit Ihrer Arbeit beginnen.

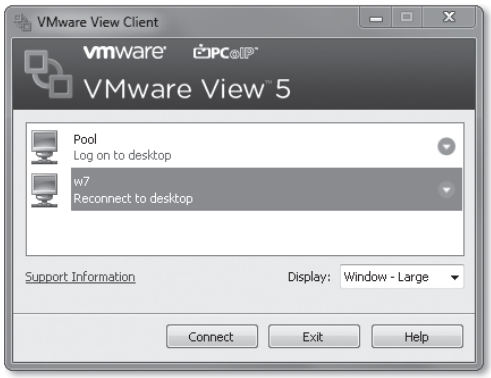


Abbildung E.8 View Client

E.1.4 Der View Agent

Der View Agent wird auf jedem virtuellen Desktop installiert bzw. ausgeführt und ermöglicht Sitzungsmanagement sowie Single Sign-on. Diese Applikation hat unter anderem die Aufgabe, den View Manager über den Status des Desktops zu informieren, das heißt, ob aktuell ein Benutzer angemeldet ist oder dieser sich bereits von der Remote-Sitzung getrennt oder abgemeldet hat. Die Installation des Agenten kann in die Vorlage bzw. das Template für virtuelle Maschinen integriert werden, so dass anhand dieser Vorlage erstellte virtuelle Desktops den Agenten automatisch enthalten. Bei individuellen Desktops hingegen muss der Agent in jeden Desktop installiert werden. Dies gilt selbstverständlich auch für PMs.

E.1.5 Der View Composer und die Storage-Optimierung

Die Komponente View Composer nutzt die Linked-Clone-Technologie zur schnellen Erstellung von Desktop-Images. Dadurch wird der Speicherbedarf für virtuelle Desktops um einen erheblichen Teil gesenkt und das Management von Images optimiert, siehe Abbildung E.9. Laut VMware können Sie hierbei mit Einsparungen von 50 % und wesentlich mehr des bereitgestellten Storages rechnen. View Composer arbeitet mit einem Desktop- bzw. Basis-Image und erstellt einen Pool mit bis zu 512 Virtual Machines bzw. virtuellen Desktops auf Basis von Linked Clones. Jeder dieser Linked Clones fungiert als unabhängiger Desktop. Ein weiterer

sehr wichtiger Aspekt in diesem Zusammenhang ist, dass die Erstellung eines neuen Desktops extrem schnell vonstattengeht. Durch das Linked-Clone-Verfahren, in dem eine Referenzierung auf einem Parent-Image erfolgt, ist ein Massen-Deployment von virtuellen Desktops gegenüber einem vollständigen Klonen von einzelnen Virtual Machines zeitlich gesehen extrem weit überlegen. Ein zusätzlicher Vorteil dieses Verfahrens ist: Auf diese Art können Sie die Desktops ganz einfach aktualisieren oder patchen, indem Sie lediglich das Parent-Image austauschen oder aktualisieren. Die Einstellungen, Daten oder Anwendungen der Anwender sind hiervon nicht betroffen.

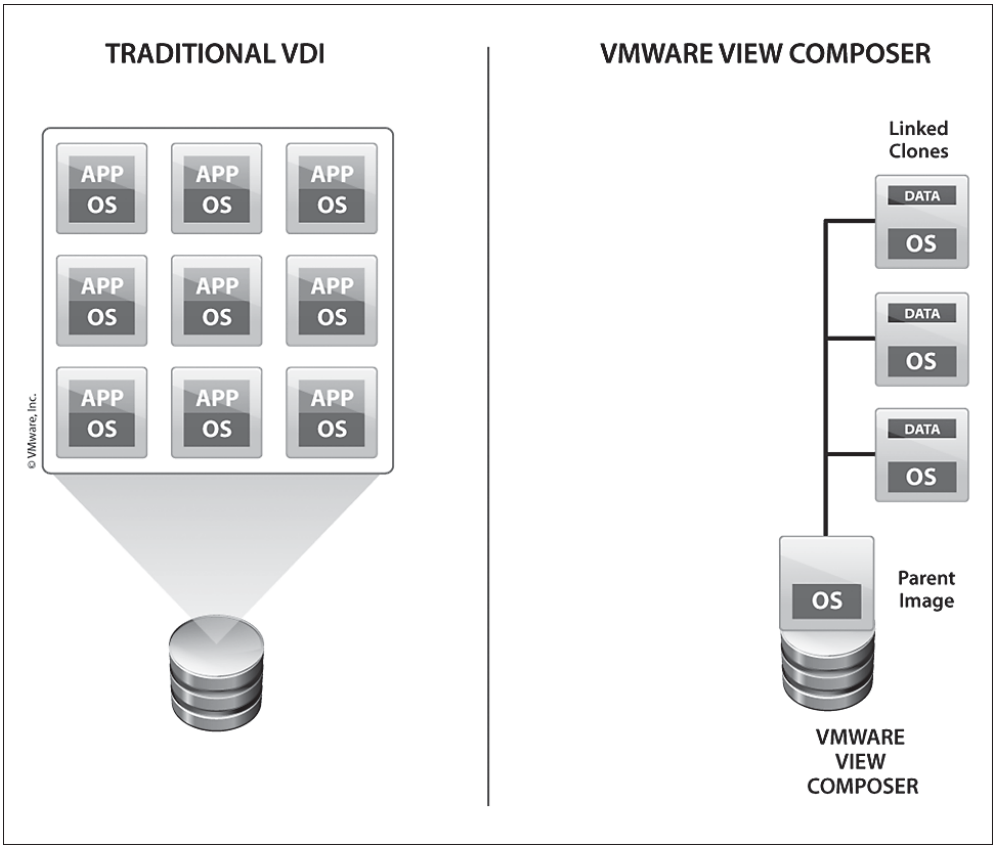


Abbildung E.9 Unterschied zwischen Full-Clone- (links) und Linked-Clone-Verfahren (rechts).

E.1.6 Der Local Mode schafft Mobilität

Mit dieser Funktion lässt sich ein Desktop-Image aus dem Rechenzentrum auf ein physisches Desktop-Gerät, zum Beispiel ein Notebook, unter Einhaltung aller Sicherheits-Policies herunterladen (auschecken) und ohne bestehende Netzwerkverbindung vollständig nutzen. Sobald das physische Desktop-Gerät wieder mit dem Unternehmensnetzwerk verbunden ist (einchecken), werden die Änderungen aus dem Offlinezustand zurückübertragen (Deltasynchonisa-

tion). Hierdurch wird die Mobilität des Anwenders auf eine ganz besondere Art und Weise verbessert. Denken Sie nur an Mitarbeiter im Außendienst, die aufgrund von nicht vorhandener Anbindung an das Internet nicht auf ihren Desktop im Rechenzentrum zugreifen können. Solange der Desktop ausgecheckt ist, kann die Kopie, die sich nach wie vor auf der zentralen View-Umgebung im Rechenzentrum befindet, nicht verwendet werden – sie ist für die gesamte Offlinedauer gesperrt. Der Local Mode ist nur in Verbindung mit individuellen Desktops möglich. Außerdem erfordert der Local Mode einen speziellen View Client. Mit dem Local Mode ist es möglich, administrative Reglementierungen sowohl auf Desktop- als auch auf globaler Ebene zu vergeben. So ist es auch möglich, das Einchecken nach einer bestimmten Zeit zu erzwingen. Wird dieser Zeitraum überschritten, wird das System beispielsweise unbenutzbar. Aktuell ist es erforderlich, dass auf dem physischen Desktop-Gerät noch ein Microsoft-Betriebssystem installiert sein muss. In einer der nächsten Generationen von View plant VMware angeblich, einen Desktop-Thin-Hypervisor einzuführen, der die Installation eines Betriebssystems auf dem physischen Desktop-Gerät erübrigt.

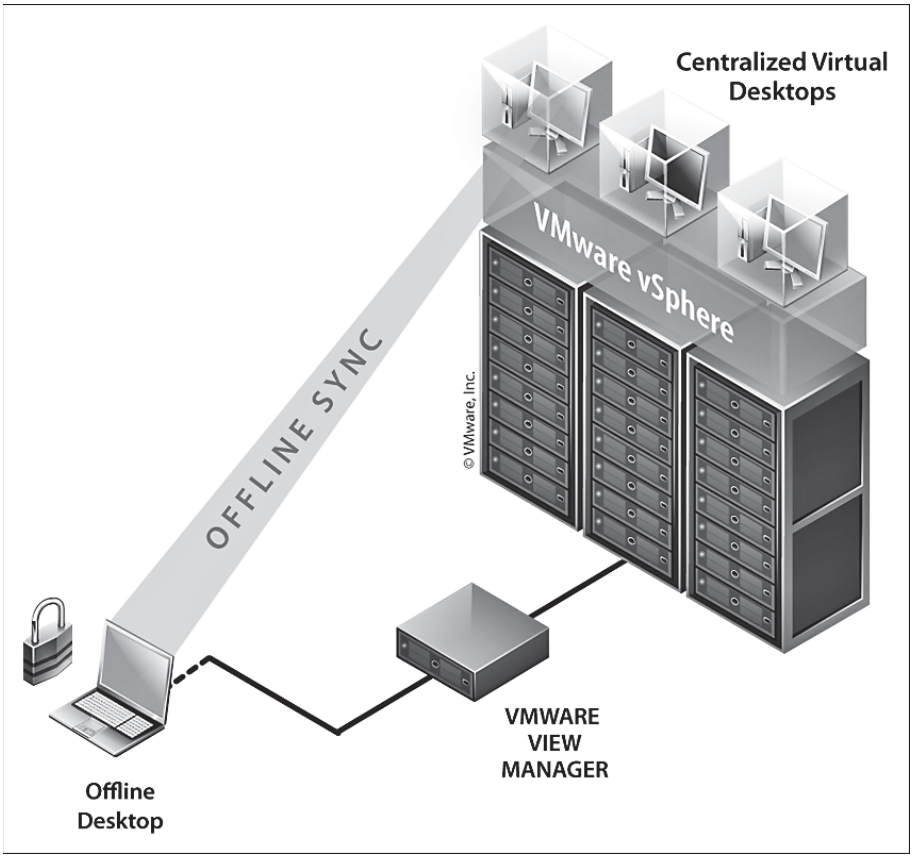


Abbildung E.10 Schema des Lokal Modes

E.2 Das Display-Protokoll – PCoIP

View enthält eine Softwarevariante des PCoIP-Protokolls. Die PCoIP-Komponenten werden mit dem View Client und dem View Agent installiert, wobei auf der virtuellen Maschine dadurch auch spezielle Grafikkarten- und Audiotreiber implementiert werden. Im lokalen Unternehmensnetzwerk (LAN) ist dank des PCoIP-Protokolls kein Unterschied zwischen einem herkömmlichen Arbeitsplatz und einem View-Arbeitsplatz zu bemerken. In Weitverkehrsnetzen (WAN) kann in Latenzbereichen von 150 bis 250 ms noch mit dem Desktop gearbeitet werden. Das PCoIP-Protokoll ist ein dynamisches Protokoll. Es passt sich in gewissen Maßen den aktuellen Bandbreiten respektive den Latenzen an. Das bedeutet: Ändern sich die Umgebungsbedingungen des Übertragungskanals, so wird die Qualität der zu übertragenden Daten – Bild und Ton – entsprechend angepasst. PCoIP nutzt unterschiedlichste Verfahren, um Kapazitätsengpässe bei der Übertragung zu kompensieren. Eines dieser Verfahren ist das Progressive Build, bei dem Bildschirminhalte bei geringeren Bandbreiten anfänglich mit geringer Qualität übermittelt und dann stetig nachgeschärft werden, wobei textuelle Informationen sofort zur Anzeige gebracht werden. Wenn Sie einen tieferen Einblick in derartige Verfahren bekommen möchten, empfehle ich Ihnen das Dokument »VMware View 5 Advances User-Centric Computing Model Enabling A Better Desktop«, das Sie unter *http://www.vmware.com/files/pdf/press-kit/vmw-view-vmworld.pdf* laden können.

Spezielle Arbeitsplatzkonfigurationen mit mehreren Monitoren sind mit PCoIP ebenfalls möglich. Auch unterstützt das Protokoll die Pivot-Funktion, also die Möglichkeit, einen Bildschirm um 90 Grad hochkant zu drehen, wobei der Display-Inhalt automatisch richtig ausgerichtet wird.

Die aktuelle Version von PCoIP beherrscht die folgenden Funktionen:

- Sie können 3D-Anwendungen wie Windows Aero oder Google Earth mit einer Bildschirmauflösung von bis zu 1.920 × 1.200 Pixeln verwenden.
- Mit dieser nicht hardwarebeschleunigten Grafikfunktion ist es möglich, Anwendungen wie DirectX 9 und OpenGL 2.1 ohne eine physische GPU (Grafikverarbeitungseinheit) auszuführen. Diese Funktion sorgt für akzeptable Leistung im WAN, nämlich bis zu 100 ms.
- Sie können bis zu vier Monitore einsetzen und die Auflösung jedes Monitors (bis zu 2.560 × 1.600) einzeln pro Anzeige festlegen.
- Wenn die 3D-Funktion aktiviert ist, werden bis zu zwei Monitore mit einer Auflösung von bis zu 1.920 × 1.200 Pixeln unterstützt.
- PCoIP unterstützt 32-Bit-Farben.
- Mit den für View 5 hinzugefügten Optimierungssteuerungen können Sie die Bandbreitenverwendung im LAN und WAN minimieren und bis zu 75 % Verbesserung bei der Bandbreite erzielen.

- PCoIP unterstützt die AES-Verschlüsselung (Advanced Encryption Standard) mit 128 Bit, die standardmäßig aktiviert ist.

View unterstützt in der vorliegenden Version sowohl die Software- als auch die Hardwareausprägungen des PCoIP-Protokolls:

- Software an Software
- Hardware an Hardware
- Hardware an Software
- Software an Hardware

Hierdurch wird ein Höchstmaß an Kompatibilität und Flexibilität erreicht, und es können alle Devices eingesetzt werden, die bereits den Teradici 1100-PCoIP-Portal-Processor eingebaut haben.

E.3 Virtualisierung von Applikationen mit ThinApp

Als letzten Punkt in diesem Kapitel möchte ich noch kurz das Thema ThinApp ansprechen. ThinApp dient zur Anwendungsvirtualisierung. Hierbei werden die Anwendungen vom Betriebssystem isoliert und voneinander gekapselt, so dass Regressionstests und Konflikte durch Anwendungsfehler vermieden werden können. Es wird kein Streaming-Server und auch kein Client zur Ausführung der Anwendung benötigt. Alles, was eine ThinApp-Applikation benötigt, befindet sich in der EXE- oder MSI-Datei. Zur Bereitstellung einer virtuellen Systemumgebung wird dann einfach dieses MSI-Paket oder diese EXE-Datei, die auch ThinApp-Package bezeichnet wird, geladen. Die Registrierungsschlüssel, DLL-Dateien, Bibliotheken von Drittanbietern und sämtliche Frameworks sind in den ThinApp-Packages enthalten. ThinApp-Packages können direkt auf einem virtuellen oder einem physischen Desktop ausgeführt oder über das Netzwerk gestreamt werden. Für den Einsatz im Umfeld des Streamings werden die Pakete auf einem zentralen Share abgelegt und über eine einfache Dateiverknüpfung, die auf die Anwendung zeigt, aufgerufen. Die mit ThinApp paketierte Anwendung wird nicht speziell für eine bestimmte Windows-Version erstellt. Da die Anwendungen isoliert und virtualisiert sind, können mehrere Anwendungen oder mehrere Versionen der gleichen Anwendung konfliktfrei auf den virtuellen Desktops der Anwender ausgeführt werden. Anwendungen werden zentral verwaltet und bereitgestellt, um sicherzustellen, dass alle Desktops über die neueste Anwendungsversion verfügen.

Die Funktionsweise des Streamings: Im ersten Schritt wird ein Streaming-Client aus dem ThinApp-Package extrahiert und dann in den Hauptspeicher des ausführenden Betriebssystems geladen. In Schritt zwei lädt sich der Client dann die aktuell benötigten Daten zur Ausführung der Anwendung aus dem ThinApp-Container.

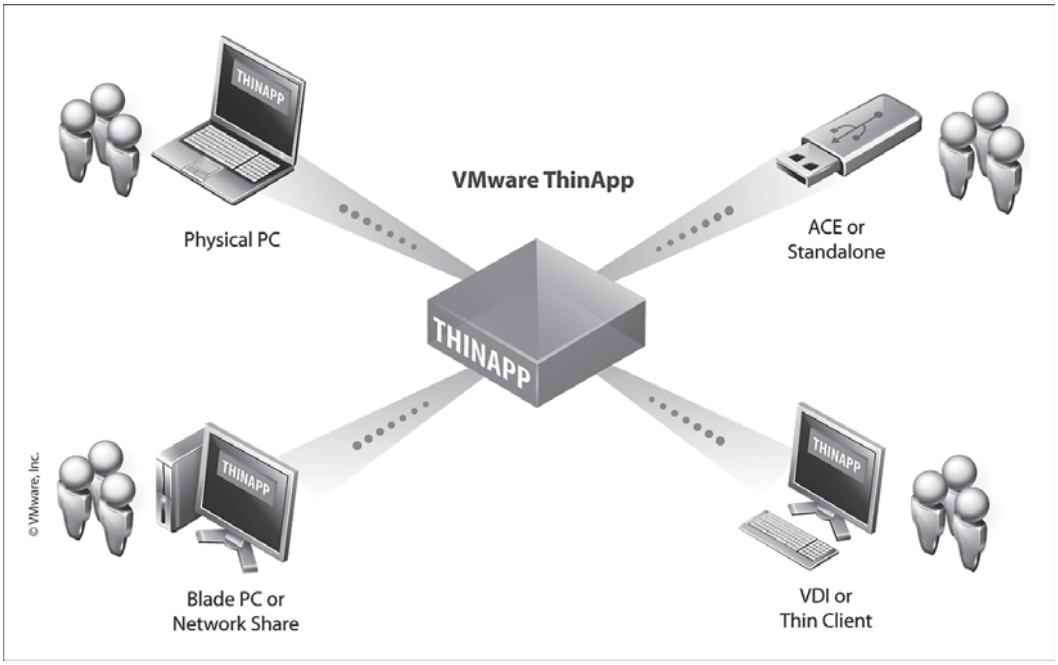


Abbildung E.11 Nutzungsmöglichkeiten eines ThinApp-Packages

Mit ThinApp ist es möglich, eine Applikation äußerst dynamisch sowohl in virtuellen als auch physischen Umgebungen einzusetzen. Die Applikation kann absolut isoliert betrachtet werden und lässt sich aus unterschiedlichsten Quellen bereitstellen. Ein weiterer sehr großer Vorteil dieser Technologie liegt darin, dass eine Anwendung zum Beispiel innerhalb eines fast beliebigen Windows-Betriebssystems virtualisiert werden und dasselbe Paket dann auf einer völlig anderen Version eines Windows-Betriebssystems oder sogar auf einem Windows-Terminal-Server betrieben werden kann.

Index

.NET Framework 258
/etc/exports 519
/etc/vmware/ssl 1029
10-GBit-Ethernet 402
10-GBit-Netzwerkkarte 427
10-Gigabit 321
1-Gigabit 321
2gbsparse 438
3D 1160
3PAR 411
3rd-Party-Multipathing-Module 414
3rd-Party-Plugin 436
64-Bit-Kernel 52
64-Bit-ODBC 241
802.1p 359
802.3ad 322

A

Acceleration-Kit 1043
Acceptance-Level 806
Account 721
  read-only 224
Active Directory 310, 677, 803, 978, 1025
  Einbindung 310
  Integration 88
Active und Standby-Adapter 323
Active Uplinks 340–341
Active/Active-Cluster 489
active/active-SP 409–410
active/passive-SP 410
Active/Unused-Konfiguration 110
ActivePerl 315
ADAM-Instanz 1149
AD-Controller 676
Add Role 717
AD-Integration 310
Administration 1001
Administratorengruppe 722
Admission Control 146–147, 158
Adobe Flash 261
Advanced Settings 300
Advanced-CPU-Funktion 136
AES-Verschlüsselung 1161
Agenten 85
Alarm 756
  Aktion 759
  Definition 757
  Reporting 759
  Thin Provisioning 593
  Trigger 758
Alarmierung 756
Alarmtyp 528
alicreate 492
Alignment 563
ALUA 413, 437, 496, 585, 590, 595
AMD Rapid Virtualization Index 118
AMD Tagged TLB 118
AMD-Opteron-Generation 139
AMDs Nested Page Tables 118
AMD-V 200
AMQP 1141
Analytical Engine 977
Analyze 993
Anforderungsprozesse 1137
Anomalie 994
Antivirus Scan Offloading 1101
AoE 408
API 1132
Appliance 86
Application Monitoring 165
Application Profile 994–995
Application Protection Suite 570
Applikationskonsistenz 857
AppSpeed Probes 1088
Arbeitsspeicher auslagern 711
Arbitrated Loop 403
Archiv 1080
Arista Networks 424
ASF Security Community 1140
A-SIS 542
Assessments 1138
Asset Information Report 999
Assign Role 311
Assign User-Defined Storage Capability 469
Asymmetric active/active 411
Asymmetric Logical Unit Access → ALUA
Asynchronous LUN Access → ALUA
Atomic Test & Set 450, 470
Audits 1138
Ausfallsicherheit 135, 230, 847
Ausgehende Verbindungen 695
Auslagerungsdatei 119, 433, 446
Auswertungsdaten 750
Authentication 762
Authentication Proxy 273, 803–804
Authentication Services 804
Authentifizieren im System 220
Auto Deploy 272, 811
  Add-DeployRule 814
  New-DeployRule 814
Auto-detect Method 980
Automated Pool 1153
Automatic ›Health‹ Scores 1136
Automation level
  fully automated 171
  partially automated 171

B

Backend-I/O 481
Backup 36, 281
  differentielles 854
  inkrementelles 854
Backup-Appliance 285–286
Backup-Datenstrom 855
Backup-Rechenzentrum 1093
Backup-Strategie 847
Ballooning 80
Bandbreite 321, 1160
Baseline 767, 780
  create 781
  dynamic 781
  fixed 781
  für Hostsysteme 234

Baseline (Forts.)
Status 787
Baseline-Gruppe 767, 784
Basic Consolidation Estimate → BCE
BCE 1009
Beacon Probing 340
Belastung 991
Belastungsprofil 977
Benchmarking 977
Benutzer
einrichten 718
exklusiver 243
Benutzer-Account 714
Benutzerdatenbank 719
Benutzerdefinierte Speicherfunktionen 926
Benutzerrolle 716
Benutzerschnittstelle, webbasierte 977
Benutzerverwaltung 1025
Berechnungsgrundlage 1085
Berechtigung 714
Gruppe 722
Berechtigungsstruktur 244
Berechtigungssystem 714
Bereitstellung 1129
Bereitstellungsreihenfolge 879
Betriebsaufgaben 722
Betriebssystem-Virtualisierung 38
Betriebsunterbrechung 1014
Bibliothek 1079
BIOS 215
Blade-PC 1154
Blade-Server 397
Blind Spot → Toter Winkel
Blockgröße 55, 503
Blocksize → Blockgröße
Boot Options 909
Boot vom SAN → Boot-on-SAN
Boot-Environment 228
Bootmenü 216
Boot-on-SAN 87, 230
Boot-Storms 541
Broadcast 416
Broadcom 55
Brocade 490
Bundle 1043
BusLogic Parallel 461, 888

C

Cache 538
Capacity Planner
Arbeitsweise 974
Betriebssystem 1006
Data Collectors 975
Data Manager 971
Framework 978
Nutzungsgrad 972
Server-Auslastung 972
Server-Landschaft 973
CapacityIQ 1135
CDP 342
CD-ROM-/DVD-Laufwerk 887
Cells 1132
cfgcreate 491–492
cfgenable 491–492
cfgshow 492
Change Management 1137
Changed Block Tracking 125
CHAP 421
Chargeback 1133
Chart Options 727
Checksumme 213
Child-Resource-Pool 163
CIFS 488, 821
Cisco 409
Discovery Protocol 342
Hot Standby Router Protocol 151
Nexus 1000V 1052
VSG 1103
CLI 87, 221, 313, 615, 634, 640
CLI-Befehle 313
Client-Device 837
Client-Tools 258
Clone 647, 946, 949
Clone Blocks 470
Clone to Template 947
Cloud 1129
Cloud-Komponenten 1130
Cluster 135, 307, 868
Administrator 875
freie Ressourcen innerhalb des Clusters 183
Cluster (Forts.)
Knoten 875
Konfiguration 868, 870
Landschaft 868
Name 875
Produkte 167
Service 877
Typ 880
Verbund 141, 877
Cluster Continuous Replication Environment 870
Cluster-aware 141
Clustering 416
Cluster-Objekt 135
Cold Migration 97
Cold Standby 282
Cold-Standby-Server 281
Collection-Job 976
Collector-Interface 1083
Collector-Modul 975
combine 1067
Command-Line Interface → CLI
Common Information Model 66
Community 354, 1039
Company-ID 983, 1005
Company-ID-Request 1004
Compare Systems 996
Compliance Checker 1138
Compliance Dashboards 1100
Compliance-Analyse 1143
Compliance-Check 786
Compliant 786
Configure Management Network 379
Congestion Threshold 474
Connection Manager 247
Connection-Broker 1150, 1155
Consolidated Backup 207
Consolidation 34
Content-based Memory-Sharing 433
Content-based Page-Sharing 80
Continuous High Availability 198
Convert to Template 947
Copy-on-Write-Verfahren 466
Coraid 408
Core Four 34
Co-Scheduling 72
co-started 72

co-stopped 72
CP-Admin 1018
CPU
Direct Execution Mode 68
Generationen 106, 136
Identification Mask 907
Identification Utility 102
Level-1-Cache 67
Level-2-Cache 67
Level-3-Cache 67
Privileigierungsstufen 68
Supervisor Mode 68
CPU Ready 729
CPU/MMU Virtualization 910
CPU-Affinität 70, 914
CPUID Mask 103, 137
CPU-Kompatibilität 101–102
CPU-Lastverteilung 70
CPU-Limit 913
CPU-Maskierung 102, 105
CPU-Reservation 914
CPU-Reservation, Best Practices 76
CPU-Ressourcen 912
CPU-Shares 913
CPU-Stopp 100
CPU-Virtualisierung 66
Crash-consistent 857
Create a Support Request 1059
Current Failover Capacity 158
Custom Port 1028
Custom Report 998

D

DAS 395, 487
das.allowNetwork 151
das.isolationaddress 150–151
Dashboard 977, 984–985, 987–988, 999, 1009, 1019
Account 984
Alarm 989, 993
Anomalie 989, 993
Belastungsdaten 996
Benchmark 993
Benutzer 984
Bericht 998
Business Hours 991
Dienst 1004
Dashboard (Forts.)
Durchschnittswert 988
E-Mail 1002
Enterprise Summary 986
Ergebnis 1013
Forecast Critical Processors 989
Hauptleistungsindikatoren 992
Hyperthreading 991
Indikator 990
Job History 1000
Konsolidierung 993
Konsolidierungsszenario 1010
Korrelation 1013
Leistungsdaten 985, 991
Leistungsindikator 988
Messwert 988
Messzeitraum 992
Modellsystem 1009
Nichtvirtualisierungs-empfehlung 1013
Notification 1002
Peak Hour 991
Phantom-Server 1013, 1015
Policy 984
Private 999
Processor Balance Table 991
Prozessorauslastung 991
Read-only-User 984
Remote 999
Schwellenwert 989, 994
Shared 999
Statistik 985–986
Szenariomodellierung 977
Template 977, 1009
Trend 992
Vorhersage 990
Zielsystem 985, 987, 994
Data Analyzer 977
Aggregation 977
Messwert 977
Trendanalyse 977
Data Collector 974
Agent 974, 1006
Analysierendes Environment 974
Anmeldeinformationen 978
anonymisiert 981
CPU-Statistik 981
Datensynchronisation 981
Data Collector (Forts.)
Discovery-Task 980
im Information Warehouse registrieren 983
Inv_*-Datei 981
Inventarisierung 982–983
Inventarisierungsdaten 984
Leistungsdaten 984
Linux 981
Memory, Auslastung 981
Message-Box 981
Messung 975
Messwerterfassung 982
Messzeitraum 1006
Messzyklus 1006
Network, Auslastung 981
Outbox 981
Ping 1006
Protokolldatei 980, 984
Prozessorauslastung 981
Redundanz 980
Stats_*-Datei 981
Synchronisation 981
Systemanalyse 979
Unix 981
Verbindungsaufbau 982
Verbindungstest 978
Zielsystem 975, 980, 982–983
Zugangsdaten 978
Data Loss Prevention 1101
Data Manager
Dienst 971
Rechenzentrum 971
Data Mover 125
Interface 629
Data Recovery 818
Lock 825
mark for delete 825
Restore 824
restore Rehearsal 825
zeitliche Einschränkungen 823
Data Recovery Client 287, 820
Destinations 821
Data Source Name → DSN
Data Warehouse 1009
Database Retention Policy 754
Database-ID 983, 999
Datacenter 307
Data-Collector-System-ID 983

Data-Manager-Modul 976
Benutzerschnittstelle 976
Verbindungstest 977
Data-Recovery-Appliance 867
Data-Recovery-Plugin 867
Datastore 293, 505, 524
assign a new signature 535
expand 528
extend 528
Extent 529
überbuchen 528
Datastore Maintenance Mode 186
Datastore-Browser 526
Datastore-Cluster 186, 192
anlegen 187
Datastore-Heartbeat 148
Datastore-UUID 121
Datastore-View 525
Dateiorientiert 425
Dateisystemblock 563
Datenaufkommen 236, 285
Datenbank 850, 1139
Datenbank-Agent 851
Datenbank-Server 236
Datenbanksicherung 851
Datenbanksoftware 240
Datenbanksystem 306
Datenbankverbindung 754
Datenbankwachstum 236
Datendurchsatz 537
Datengewinnung bei Unix und Linux, Methoden 979
Dateninkonsistenz 451
Datenkonzentration 855
Datenmanagement 1139
Datenpuffer 443
Datenquelle 240
Datenquellenname 242
Datensicherheit 852
Datensicherung 36, 285, 822, 847, 852
Richtlinien 850
Datensicherungsstrom 285, 852
Datensynchronisation 977, 984
Datensynchronisationsfunktion 982
Datensynchronisationsmodul 976
DB2 239
Dedicated Pool 1154
Deduplizierung 189, 285, 486, 524, 541, 543, 821, 866
Deduplizierungs-Storage 825
Delay-Zeit 693
Delete a Snapshot 960
Deltadatei 464
Denial-of-Service-Attacke 117
Deploy-Rule 815
Depot 271
Desasterfall 1096
Desasterschutz 856
Desktop-Firewall 1005
Desktop-Management 1148, 1155
Desktop-Virtualisierung 1147
Device-Treiber 836
devmgr_show_nonpresent_devices 837
df -h 518
DHCP-Server 273, 811
Diagnosedatei 1055
Diagnoselauf 285
Diagrammoption 726
Dienst, anzeigen 749
Direct Console UI 295
Direct-attached Storage → DAS
Disable Fault Tolerance 207
Disaster-Recovery 36
Diskettenlaufwerk 886
diskpart 453
Disk-Ressourcen 918
Disk-Shelf 538
Distributed Portgruppe 110
Einstellmöglichkeiten 356
Distributed Power Management → DPM
Distributed Resource Scheduling → DRS
Distributed Switche 45
Distributed vSwitch 110, 1052
DMZ 267
virtuelle Maschinen 1038
DNS 425, 680
Namensauflösung 680
DNS and Routing 301
DNS-Name 307
Domain-Zugehörigkeit 985
Domänenaccount 274, 311, 875
Domänenbenutzer 307
Double-Parity 409
DoubleTake 282
Download 212
Download Manager 266
downloadConfig.xml 776
DPM 183
DRS 135, 167, 276, 298
Affinity-Rule 170, 176
Automatisierungsstufen 168
Berechnungsprozess 169
Virtual Machine Options 180
DRS Aggressive 172
DRS Groups Manager 173
DRS-Automation-Level 170
DRS-Berechnung 181
DRS-Cluster 167, 310
Automatisierungsgrad 170
overcommitted 163
DRS-Empfehlungen 168
DRS-Gruppe 174
DRS-Konfiguration 142
DRS-Limitierungen 183
DRS-Prioritäten 170
DRS-Regelwerk 168
DRS-Resource-Pool 170
DSN 241
Dual-Port-SAS-Platte 396
Dump Collector 89, 268, 800
Dynamic binding 357

E

E1000 889
eagerzeroedthick 131
EDA-Appliance 272
EFD 399
Eingehende Verbindungen 695
Einzelfall-Support 1054
Elastic Memory for Java 1138
Embedded-Datenbank 761
EMC Atmos 569
EMC CLARiiON 413
EMC DMX 411
EMC Isilon 569
EMC PowerPath/VE 412
EMC Replication Managers 655
EMC Symmetrix 569

EMC VNX 569
ALUA 585
blockbasiert 576, 584, 592, 619
Dateisysteme 610
FAST Cache 576
FAST VP 573
Global Hot Spares 575
RAID-Groups 572
Storage-Pool 574
VPLEXTM 569
Enable Host Monitoring 145
Enduser License Agreement 217
Enhanced vMotion Compatibility 105
Enhanced vMotion Compatibility-Mode → EVC
Enter SDRS Maintenance Mode 197
Enterprise Flash Drive → EFD
Enterprise Plus Edition 49
Enterprise Ready Server (ERS) 1140
Environment-Variable 837
Ephemeral – no binding 357
EPSEC-API 1101
Ereignis, Export 738
Essential Plus 1047
Essential-Paket 1047, 1051
esxcfg
advcfg 1033
auth 1026
firewall 1028
esxcfg-advcfg 1033
esxcfg-firewall 1027
esxcfg-nics 120
esxcfg-volume 535
esxcli nmp satp 436
esxcli storage core 471
esxcli swiscsi 516
ESXCLI-Befehl 800
ESX-Host-Prozess 144
ESX-Hosts 1018
sechs Netzwerkports 389
Sicherung 847
vier Netzwerkports 388
zwei Netzwerkports 386
ESXi Deployment Appliance 229
ESXi Installable 1152
ESXi Server 1046
ESXi-Image 272, 813
ESX-Sicherheit 1021
esxtop 968
resxtop 600
etc, vmware/ssl 1029
/etc/exports 519
/etc/vmware/ssl 1029
Etherchannel 322, 383, 519
EULA → Enduser License Agreement
Evaluation 252
EVC 136
EVC-Cluster 105, 137, 310
Event 678, 737
Export 738
ExecutionPolicy 228
Export 312
exportfs 519
Extended Statistics 471
Extents 457, 472

F

Fabric 416, 489
Fabric GemFire 1139
Failback 341
Failover 340–341, 519
Failover Host 148
Failover Order 341
Failover-Aktivitäten 162
Failover-Kapazität 147
Failure Interval 882
FAST Suite 570
Fastpath-Authentifizierung 799
FAT 460
Fault Domain Manager 144
Fault Tolerance 135, 198, 384, 463, 870, 884
Fault Tolerance Logging 204
FC-/iSCSI-Datastore 524
FC-Broadcast 418
FC-Hub 403
FCoE 55, 408, 420, 488
FCoE-Hardwareschnittstellen 421
FCP 415
FCP Partner Path 496
fcp show initiator 494
FC-SAN 402, 606
FC-Switch 417
fdisk 561
FDM-Prozess 156
Fehlfunktion 883
Festplatte
2gbsparse 438
monolithic flat 439
monolithic sparse 439
Physical Compatibility 439
Virtual Compatibility 439
Festplattentyp 869
flat 832
thin 832
Fibre Channel NPIV 910
Fibre-Channel 55, 383, 401, 487
Fibre-Channel over Ethernet → FCoE
Fibre-Channel-Festplatte 396
Fibre-Channel-HBAs 230
Fibre-Channel-WWNs 902
File Allocation Table → FAT
File Level Restore 868
File-Clone 536
Filer 488
File-Server 1040
File-System-Checkpoints 649
Firewall 694, 1022, 1124
integrierte 1023
Protokollierung 1030
Startverhalten 698
Überwachung 1030
Firewall-Bedienung 1028
Firewall-Regeln anzeigen 1027
Firewall-Systeme 1103
Firmware 214, 229
Firmwareversion 405
Five Nines 1014
Fixed Multipathing 437
Flash-basierte PCI-Express-Karte 428
Flash-PCIe-Karte 399
FlexClone 535, 858, 865
Flexible 889
FlexVol 535
Flow Monitoring 1117
Forecast Alert 994
Forged Transmits 332
Foundation 1047
Fractional Reserve 547
Fragmentierung 443

Fremdherstellertool 827
Frontend-I/O 481
Fs3dm 126
Fs3dm Hardware Offload 126
Fsdm 126
FT sekundäre VM 206
FT-Funktionalität 202
FT-Lizenz 202
FT-Logging 202
Full Backup 855
Full file Backup 854
Full File Clone 470
Funktionsrollentrennung 91
Fusion-io 399, 428
Fusion-io ioDrive 430
Fusion-io ioMemory 430
Fusion-io ioTurbine 433

G

Gastbetriebssystem
anpassen 951
Ausfall 140
Gastdateisystem 465
Gateway 681
Generate New License File 1069
Geschwindigkeit vs. Kapazität 483
Grafted from ESX Host 170
Gratuitous ARP 144
Größenberechnung 236
Grundmetrik 751
Guest Customization Wizard 951
Guest SDK 166

H

HA 135
Advanced Options 149
Agent 155
Failover 158
Failover-Capacity 146–147
Host Isolation 160
Restart Priority 147
HA-Cluster 140, 307, 309
HA-DRS-Kombination 186
HA-Knoten 142
HA-Logik 162
HA-Master und Slave-Agenten 159
HA-Priorität 157
Hardware
erweiterte Konfiguration 706
vereinheitlichen 36
virtuelle 886, 898
Hardware Compatibility Guide 209
Hardware Compatibility List 94
Hardware Interface Layer 66
Hardware Status 309, 748
Hardwareinstrumentierung 88
Hardware-Management-Schnittstelle 1022
Hardwarevirtualisierung 38, 82, 200
HA-Slot-Berechnung 158
Hauptadministrator 984
Hauptspeicher-Checkpoint 98
Hauptspeicherreservierung 448
HBA 404
HBA-Controller 229
HCA 404
HCL 53
HDS USP 411
Heartbeat 282, 881
Paket 146, 160
Traffic 872
Hersteller-Benchmarks 993
Hexa-Core-Systeme 68
Hitachi-AMS2000 412
Hochverfügbarkeit 97, 281
Home-Verzeichnis 129
Host
Failures Cluster Tolerates 148
Isolation Response 154
standardisieren 234
Utilities 551
Host and Clusters 293, 829
Host Channel Adapter → HCA
Host Isolation Response 154
Host Monitoring 145
Host-based Lizenzierung 1069
Host-Bus-Adapter 230
Host-Cache 400, 429, 433
hostd 100
Host-Ids, Best Practices 588
Hostprofil 46, 665, 847, 1021
assoziieren 668
Editiermodus 667
erstellen 666–667
exportieren 667
importieren 666–667
Konfigurationscheck 670
Konformität 666
nicht compliant 669
verknüpfen 666
verteilen 666
zuweisen 670
Host-Ressourcen 1083
Host-Systemressourcen, CPU-Reservierung 712
Hot Add 934
Hot Migration 97
Hot Plug 908
Hot-Add-Funktion 461
Hotclone 826
Hot-Remove-Funktion 461
HP EVA 413
HP iLO 183
HP-EVA-Levelling 486
HPs MC/ServiceGuard 140
Hybrid Cloud 1099, 1134
Hyperthreading 70, 914
HypertTransport Technology 68
Hypervisor 39, 83, 712
Typ 1 37
Typ 2 38
HyTrust Appliance 1033

I

I/O Imbalance Threshold 191
I/O-Durchsatz 429
IaaS 1130–1131
iBFT 506
IBM DB2 240
IBM DS8000 411
icomasoft Opvizor 1036
IDE-Adapter 461
IDE-Unterstützung 397
Idle-Zyklus 676
IDS/IPS-Systeme 1099
IEEE 802.3ad 322
igroup create 511
igroup show 495, 511

IIS-Server 274
IIS-Version 803
Image 827
Image Builder 270, 805
Individuell Desktop 1153
Industriedurchschnittswerte 989
Industriestandards 1137
Infiniband 404
Information Warehouse 974, 982–983, 988, 1005
Infrastructure Agents 66
Infrastruktur as a Service 1130
Initial Placement 187
Initiator-Group 494
Inkonsistenz 851
Installation 209
SD-Karte 219
USB-Medium 215
Installations-Appliance 847
Installationsimage 270
Installationsmedium 219
Installationsoptionen 249
Installationsroutine 217
Installationstools 229
Installationszustand 987
Integrierte Firewall 1023
Integrität 981
Intel VT 200
Intelligent Platform Management Interface → IPMI
Intitiator, Target-Portverbindung 409
Inventarisierung 977
manuelle 979
Inventarisierungs- und Performancedaten 974
Inventarisierungsdaten 986
Inventarisierungs-Task 979
Inventory 297
IOPS 396, 537
IP Allocation Policy 795
iPad 302, 1156
iPad-App 302
IP-Einstellungen 819
IP-Hash 322, 390, 520
IP-Hash-basiertes Load-Balancing 427
IPMI 748–749
IP-Netzwerk 423
IP-Pool 298, 731–732
IP-Port 264
IP-Range 978
IP-SAN 402, 606
IPsec 421
IP-Spoofing 1120
IQN 509
iSCSI 55, 401, 487, 505–506
Ausfallsicherheit 514
iSCSI Boot Firmware Table → iBFT
iSCSI Qualified Name → IQN
iscsi start 509
iSCSI-HBA 230
iSCSI-Load-Balancing 516
iSCSI-Netz 383
iSCSI-Speichernetzwerk 421
iSCSI-Storage 387
ISO 27001/27002 1100
ISO-File 234
Isolated 354, 1039
Isolation Response 145
Isolationsvorgang 161
Isolierte Netze 1131
IT-Service-Management 1100, 1137
ITSM → IT-Service-Management

J

JEE 1138
Job, automatisiert ausführen 982
Job-Planer 976
Join Domain 804
Jumbo-Frame 88, 426, 508
JVM Memory 256

K

Kapazitätsmanagement 1129
Kapazitätsmessung 1005
Kapazitäts-Monitoring 1136
Kapazitätsplanung 971
Kapazitätsplanungsprojekt 984, 1002, 1004
Katalog 1129, 1131
Katastrophenfall 1092
Keep Virtual Machines Together 176
Kennwortänderung 242, 245
Kerberos 1026
K-Fall-Handbuch 1093
Klimabedarf 880
Klonen von Desktops 1148
Kommandozeile 312, 315
Kommunikationszone 491
Kompatibilitätsliste 209, 237
Kompatibilitätsprobleme 258
Konfigurationsdatei 853
Konfigurationsgröße 255
Konfigurationsmenü 221
Konfigurationsnacharbeiten 96
Konfigurationsschritte 307
Konsole 295
Konsolidierung 34, 1017
Konsolidierungsratio 1017
Kontextmenü 277
Konvertierung 826
Kostenabrechnung 1133
Kostenanalyse 1084

L

LACP 322, 388, 520
LAN-Frame 508
LAN-free 853
LAN-Kommunikation 424
LAN-Manager 978
Lastausgleich 1000
Lastausgleichsbetrachtung 1150
Lastenausgleich 135
Lastspitze 855
Lastverteilung 424
Latenzzeit 114, 132, 190, 408, 429
Leistungs- und Inventarisierungsdaten 1009
Leistungsaufnahme 1017
Leistungsdaten
Bericht 981
ermitteln 980
Ermittlung 983
manuell ermitteln 980
Messung 982
Leistungsengpass 423
Leistungsindikator 726
Lese-Cache 434
license add 518
Licensed Features 300

Limits, Best Practices 76
Link Aggregation 519
Link Aggregation Control Protocol → LACP
Link Layer Display Protocol 342
Link status only 340
Linked Clone 430, 565, 1153, 1157
Linked Mode 253, 278, 790, 1051
Linked vCenter Server 58
Linked-Clone-Technologie 1132
Linux 677
Live-Migrationsfunktion 97
Lizenz 37, 88
Asset-Satz 701
einpflegen 701
Server Diags 705
Lizenzbereich 1064
Lizenzdatei 703, 1068
Lizenzen prüfen 283
Lizenzierung 59, 88, 282
Lizenzierungsmodelle 1043
Lizenz-Key 700, 1067
Lizenzmanager 700
Lizenzportal 283
Lizenzschlüssel 1064, 1072
Lizenz-Server 249, 276, 283, 699
DNS 706
integrierter 282
Umzug 706
LLDP 342
Load Balance Collector 1000
Load-Balancing 322, 336, 347, 357, 412, 496, 519
IP-Hash-basiertes 427
Local Mode 1158
Local Protection Suite 570
Lockdown Mode 295, 1021
Locking-Mechanismus 517
Log on as a service 253
log.rotateSize 1032
Log-Datei 294, 893
Logical Unit Number → LUN
Log-Level 312, 753
Lokale Installation 214
Lokale Medien 393
Long Distance vMotion 122
LSI Logic Parallel 888
LSI Logic SAS 461, 888
LSI-Logic-Parallel 461
LUN 55, 230, 410
Alignment 562
Clone 532, 865
ID 410, 419, 502
Queue Length 494
Space Reservation 547
vergrößern 529
lun clone create 533
lun create 493, 509
lun map 496, 512
LUN-Größe 485
LUN-ID0 419
LUN-Konfiguration 585
LUN-Mapping 230, 419
LUN-Owner 413
LUN-Ownership 628
LVM.Resignature 534

M

MAC Address Changes 331
MAC-Adresse, statische 936
Machine Memory Pages 78
Mail-Einträge 751
Maintenance-Modus 94, 135, 182, 302, 786
Maintenance-Status 182
Management Information Base → MIB
Management-Appliance 223, 315
Management-Homepage, vCenter 700
Management-Interfaces 91
Management-Netzwerk 155, 382
Wiederherstellung 378
Managementoberfläche 294
Management-Server 281
Managementskripte 85
Managementumgebung 231
Mandantentrennung 1132–1133
Manual Pool 1153
Manuelle Inventarisierung 979
Manuelle Leistungsdaten-ermittlung 980
Mapping 494
Maps 309, 736
Masking 494
Master 155
Maximum resets time window 883
mbralign 564
mbrscan 564
MD5 213
Medium, lokales 393
Mellanox 408
Memory
Limit 915
Overcommitment 79, 433, 463, 711, 729
Reservation 158, 916
Ressourcen 915
Shares 915
Memory Management Unit 69
Memory-Ballooning 433
Memory-Compression 79, 433
Memory-Overhead 78
Memory-Swapping 81
Messaging 1141
Messung überwachen 1008
Metadaten, Schreibzugriff 518
Metro-Cluster 144
mgmt-vmware 1029
MIB 678
Microsoft
Cluster 282
Cluster-Lösung 140
NLB-Verbund 177
Windows Installer 249
Microsoft NLB 341
Microsoft SQL 2005/8 240
Microsoft SQL 2008 Express 237, 240, 306
Microsoft SQL Server
Datenbankberechtigung 244
Kennwortänderung 245
Recovery-Modell 244
Migrate 114
Migration 89, 93, 101, 351, 354, 370
Migrationsprojekt 972
Mikrosegmentierung 1100
Minimum Uptime 882
Misalignment
ÜBERAlign 651
vAligner 651
Volume-Alignment 651

Mischumgebung 257, 282
mkfile 543
MLAG 519
MLC-SSD 399
MMU 69
Mobile Desktops 1151
Mobile Geräte 302, 304
Modellszenario 977
Monitoring 1129
Monitoring Sensitivity 164
Monolithic-flat-Festplattendatei 439
Monolithic-sparse-Festplatte 439
Most Recently Used → MRU
MPIO-Multipathing 407
MRU 413, 437
MSCS 868
Einschränkungen 870
MSDE 237
msinfo32.exe 563
MTU 426
MTU-Size 347
Multichassis Link Aggregation → MLAG
Multikernsystem 991
Multimedia Appliance 302
Multi-NIC vMotion 107
Multi-NIC-Support für vMotion 108
Multipathing 383, 435, 591
Einstellen 633
Installation PowerPath 642, 652
NMP 609
NMP Round-Robin 595
PowerPath 595, 609
Multi-Path-Plugin 436
Multiple Connections per Session 511
Multiprotocol 562
Multiprozessor 991
Multiprozessorfähig 72
Musterrolle 717

N

NAA 410
Nacharbeiten 95–96
Nagios-Plugin 549
Namensauflösung 791
NAS 395, 517, 821
Native Client 241
Native Snapshot Support 471
Native-Multipathing-Plugin 436, 500
Nearline 542
Nested Page Tables 118
.NET Framework 258
NetApp 409, 489
FAS2050 523
Snapshot 531
Volume 518
WAFL File-System 560
NetApp Filer 425
NetApp PAM 400
NetApp-Storage 855
NetFlow 363
NetSec-API 1103
Network 293
Adapter 300
Fencing 1080
File System 517
Network Address Authority → NAA
Network Failover Detection 340
Network I/O Control 45, 359
Network resource pool 360
Network-attached Storage → NAS
Netzwerk 319
Installation 228
Netzwerkanbindung 319
Netzwerk-Design 319
Netzwerkeinstellungen 294
Netzwerkkarte 324, 326, 889
Netzwerkkartentyp, vlance 888
Netzwerkport 1023
Netzwerkports (Sechs) 389
Netzwerkports (Vier) 388
Netzwerkports (Zwei) 386
Netzwerk-Resource-Pools 362
Netzwerkschichten 323
Netzwerkstack 435
Neuformatierung 459
Neuinstallation 94, 232
Neverfail 282
NewSID 951
NFC Copier 125
NFS 55, 401, 425, 487, 517, 623
NFS-Client 425, 518
NFS-Datastore 382, 628, 865
NFS-Export 522
NFS-Netz 382
NFS-Protokoll 425
NFS-Speicher 143
NIC-Teaming 336, 347, 357
Niederlassungsanbindung 1151
NIS-Dienst 762
NMP-Modul 436
Non-blocking 424
Non-Execution-Bit 103–104
Non-persistent Mode 897
Non-uniform Memory Access 73
Notification-Template 995
Notify Switches 99, 340
Notstromversorgung 1006
NPIV 419, 870
NPIV-Funktion 420
N-Port-ID-Virtualisierung 419, 910
NTP 672
NTP-Server 674
NUMA 73
NUMA Memory Affinity 917
NUMA-Knoten 74
Nutzerrecht 719
NVRAM-Datei 893
NVSAVE 858
NX/XD Flag 103
NX-Flag 69

O

ODBC 91, 239–240
ODBC auf 64-Bit-Systemen 241
ODBC-Datenquelle 243
ODBC-Einstellungen 267
Offline-Migration 117
On-Board-USB-Controller 400
On-Demand Analytics 1136
Open IPMI 748
OpenGL 1160
Operations Manager 549
Operations-Management 1136
Optimization Report 998
Optimize 999
opvizor 467
Oracle 237

Oracle 10g 239
Oracle 11g 239
Oracle-Datenbanken 278
Oracle-Raw-Daten 462
Oracle-Treiber 248
Orchestrator 1051
Originating Port-ID 388
Outstanding I/O 494
Overhead 52, 78

P

P2V 826
Paketverlust 132
PAM-Karte 539
Paravirtualisierung 83
Paravirtualized SCSI 461
Partition-Alignment, konsistentes 561
Partitioned 162
Partitionierungsmöglichkeit 217
Partitionstabelle 501
Partitionstartoffset 563
Passthrough 707
Passwortgültigkeit 1025
Passwortkomplexität 1025
Patchaufwand 85
Patch-Baseline 767
Patch-Datenbank 264
Patchen 983
Patch-Manager 235
Patch-Repository 233, 767
Path Selection Policy 500
Path-Selection-Plugin 436
Path-Trashing 412
Pattern-Update 1039
PCI DSS 1121
PCI-Device 708
PCI-ID-Plan 215
PCoIP 1148, 1160
Performance 275, 298, 309, 722, 988
Analyse 600
Clones 647
Defragmentation 592
FAST VP 573
FC-SAN 606
Festplatten 584
IP-SAN 607
Performance (Forts.)
Netzwerk 606
Optimierung für NAS 625
Queue-Depth 600
Storage Pool 574
Stripe-Size 594
TCP/IP Heap 620
Thick Virtual Disk 622
Trespassed LUN 662
VASA 597
Performance Accelerator Module 537
Performance Counter 1000
Performance-Analyse-Tool 1136
Performancedaten 974
Performance-Messung 977
Performance-Monitoring 1129
Performance-Studie 435
Performance-Tab 525
Perimeterschutz 1099
Permissions 298, 309
Persistent Mode 897
Pfad verwalten 498
Phantom-Server 1009–1010, 1014
Phantomszenario 977
Physical Mode 462
Physische Switches, Links 323
Pillar Data Systems 414
Ping 979
Planungsmöglichkeit 1082
Platinum-Support 1053
Plattentyp 832
Pluggable Storage Architecture → PSA
Plug-in 266, 276
Manager 277, 766
Schnittstelle 51
Pool 1153
Port 324, 330, 347, 357–358
Freischaltung 699
Port-Aggregation 425
Portal 1064, 1078, 1137
Portal-Account 1068
Portangabe 792
Portbasierte Firewall 1124
Portfast 341
Portfreigabe 276
Portfreischaltung 699
Portgruppe 45, 54, 324, 328, 330, 356, 358, 372
Ebene 385
migrieren 374
Port-Mirroring 366
Portübersicht VMware ESX 4 und 5 1027
Portübersicht VMware ESX 5 1027
Port-Zoning 417
Post-Processing-Mode 542
Power-Aktivitäten 904
PowerCLI 86, 227, 317, 805, 1028
Voraussetzungen 227
Power-Management 183, 300, 906
Power-Management-Funktion 184
PowerPath/VE 438
PowerShell 317
PPVE 644
Pre-Installation-Tasks 241
Private Cloud 1129
Private VLAN 354, 1039
Produktlizenzentypen 1072
Profil 271, 814
Profile Compliance 299
Profile Driven Storage 46
Profile-Ordner 265
Project Data Range 999
Projektmanagement
Außerbetriebnahme 1009
Contact-Info-Sheet 1003
Ergebnisbesprechung 1002
Gantt-Diagramm 1004
Initial Workshop 1002
Meilenstein 1003
Migration 1003
Pre-Screen Phone Interview 1003
Projekt 1002
Schlussmeeting 1002
Timeline 1003
Zielsystem 1003
Promiscuous 354, 1039
Promiscuous Mode 331
Protection-Group 1095

Protokollierung 1032
externe 1032
Protokolllevel 236
Proxy-Konfiguration 732
Proxy-Server 264, 820
Prozessorauslastung 991
Prozessoren 53
AMD Opteron 53
Intel Xeon 53
PSA 435
Pseudo-active/active 411
PSP-Modul 436
Public Cloud 1129
PVLAN 354
PVSCSI 84
PXE 228

Q

QFULL 599
QlLogic 55
QoS 359, 361
qtree security 519
Quality of Service 359, 459
Quellmaschine 828
Queuing 1141
Quick Assessment 1012
Quick Resume 107
Quorumdisk 875

R

RabbitMQ 1131, 1141
RAID 219, 287, 501
RAID-5 574
RAID-6 575
RAID-Größe 482, 485
RAID-Group-LUNs 575
RAID-Konfiguration 482
RAID-Rebuild 486
RAID-Verbund 395
Random-Read-Muster 537
Random-Workload 537
Random-Zugriff 395
Rapid Cloning Utility 536
now.netapp.com 537
Rapid Deployment Pack 229
Rapid Virtualization Index 118
RARP-Paket 121
Raw Device Mapping → RDM
Raw LUN 877
RDM 129, 229, 410, 460, 462, 466, 628, 877, 879, 897
RDM-Größe 55
RDM-Mapping-Datei 132
Read-Cache 544
Rechenzeit 676
Recht, durchpropagieren 722
Reconfigure for HA 156
Record- und Replay-Funktionen 199
Recovery Point Objective → RPO
Recovery Time Objective → RTO
Recovery-Modell 244
Recovery-Plan 1095
Recovery-Prozess 1096
Recovery-Site 1097
Red Hat Enterprise Linux 5 1021
REDO-Log 128
Referenznummer 1055
Refresh-Intervall 721
Regelwerk 1027
Registrierung 261
neue VM 527
Registry Editor 677
Registry-Angaben 243
Remote CLI 123, 313
Installation 313
Remote Command-Line
Installation Linux 313
Installation Windows 315
Remote Protection Suite 570
Remote-Konfiguration 982
RemoteSigned 228
Remote-Steuerung 977
Replikationsfunktion 1093
Replikationsmechanismus 856
Report 998
Report-Template 998
Repository 268, 273
Rescan SAN 524
Reserve Space 470
Reservierung 298
Reservierungswert 81
Resource Allocation 298
Resource Management 66
Resource-Distribution-Chart 172
Resource-Pool 298, 308, 681
erstellen 681
expandable 683
Kontextmenü 681
Limit 683
Reservation 683
Shares 684
Übernahme 170
Ressourcenauslastung 168–169
Ressourcen-Management 82, 912
Ressourcenreservierung 98
Restart Management Agents 295
REST-basierte API 1132
Restore Network Settings 379
Restore-Prozess 855
Restore-Zeiten 493
Revert to Snapshot 960
Rich Client 1016
root 519, 1025
Root-Cause-Analyse 1143
Root-Kit-Detection 1099
Root-Resource-Pool 170
Root-Zugriff 1024
Round-Robin 436–437
Round-Robin-Mechanismen 425
Round-Robin-Verfahren 383
Route based on IP hash 336, 338
Route based on physical NIC load 336, 339
Route based on source MAC hash 336, 339, 341
Route based on the originating virtual port ID 336–337, 341
RPO 856
RTO 493, 856
Rücksicherungsoption 854
Run-Level-Informationen 817
Runtime Settings 751

S

SAN 395, 821
Installation 229
Rescan 498
SAN-Boot 406
SAN-Speicher 143
SAS, Expander 396
SAS-Festplatte 394, 537

SATA im professionellen Umfeld 395
SATA-Festplatten 393
Scheduled Task 738
Scheduler 518
Schreib-/Lese-Belastung des Storage-Systems 128
Schwellenwert 1013
SCSI2-Sperrmechanismus 455
SCSI-Bus-Sharing 898
SCSI-Bus-Sharing-Mode 875
SCSI-Controller 888
SCSI-Festplatten-Controller 873
SCSI-Inquiry 451
SCSI-Reservation 443, 455
SCSI-Reservation-Conflicts 118
SCSI-Timeout 438
SDelete 446
SD-Karte 219
SDPS 107
SDRS 584
Cluster Datastore 193
I/O Metric 595
Maintenance Mode 197
Round-Robin-DNS 622
Scheduling 197
Storage I/O Control 595
VNX-Technologien 596
SDRS-Berechnung 190
SDRS-Regelwerk 194
SDRS-Zeitsteuerung 195
SDS 1104, 1111, 1121
Sechs-Prozessor-Lizenz 1066
Secondary VLAN 354
Secure Shell 980
Security and Compliance Suite 570
Security Identifier → SID
Security-Policies 331
Security-Profile 697, 1022
Self-Service-Portal 1129, 1131
Self-vMotion 123
Send Targets 512
Sensitive Data Discovery → SDS
Separate Virtual Machines 177
Serial-attached SCSI 396
Serielle Konsole 87
Server Heartbeat 278
Server, Auslastung 36
Server-based Lizenzierung 1069
Server-Deployment 35
Server-Farm 665
Server-Management 385
Server-Management-Controller 385
Server-Virtualisierung 33
Service Console 85, 87, 209, 382, 423, 446, 1024
Service Manager 1137
Serviceanbieter 1130
Service-Console-Verbindung 144
Service-Level Agreement → SLA
Session 742
SHA1 213
Shared Storage 494
Shares 298, 361
Best Practices 76
Custom 684
High 684
Low 684
Normal 684
Sharing-Modus 877
Shell 317
Sicherheit 1021, 1032, 1099
Komponenten 1032
Sicherheitspatches 85
Sicherung 847
Sicherungsdaten 852
Sicherungszeiten 825
Sicherungsziel 821
Sicherungszyklus 823
SID 721
Simple Network Management Protocol → SNMP
Simple-Recovery-Mode 244
Single Point of Failure 36
single_image-Cluster 495
Single-Initiator-Zoning 418
SIOC 45, 190, 472–473, 584, 601
Congestion Threshold 601
NFS 621
nicht unterstützt 602
ungeeignete Fälle 621
Site Recovery Manager Plugin 1094
Site Survey Tool 202
Site-to-Site-VPN 1131
Skalierbarkeit 1016
Skalierungstest 1078
SLA 1087, 1148
Slow Down During Page Send → SDPS
Small Business 1047
Smart Alert Summary 1136
Smart Alerts 1136
SMVI 857, 859
snap create 533
snap reserve 509
SnapCreator 857
SnapManager for Virtual Infrastructure → SMVI
SnapMirror 856
Snapshot 132, 450, 494, 518, 647, 853, 856, 867, 956
Beschreibungsdatei 467
löschen 960
Snapshot Consolidator 467
Snapshot Manager 466
Befehle 957
Snapshot-Datei 957
Snapshot-Reserve 493
SnapVault 856
Integration 858
SNMP 87, 678–679, 752
Softservice Installer 229
Software
erweiterte Konfiguration 711
systemspezifische 837
Software-FCoE-Initiator 421
Software-Initiator 404
im Gastbetriebssystem 407
Software-iSCSI 510
Initiator 422
Softwarekonfiguration, erweiterte 711
Softwarepakete 1138
Solid State Disk → SSD
Solutions Manager 742
Source Volumes 831
Source-MAC 387
Spanning Tree Protocol 328
Specification Manager 747
Speicher hinzufügen 501
Speicheransichten 733
Speicherbereich 77
Speicherfunktion, benutzerdefinierte 926

Speicherprofil 198, 467, 925
Spiegelung, asynchrone 1093
Split-Brain 162
Spoofguard 1120
Sprachen 297
Sprachenmix 294
Spring 1138
Spring-Framework 1131
SQL 2005 239
SQL 2008 239
SQL 2008 R2 239
SQL 2008 R2 Express 239
SQL 2008-Express 306
SQL-Benutzerauthentifizierung 243
SQL-Express-Datenbank 263
SQL-Server-Name 242
SRA 1094
SRM 1091
SSD 397
SSD-Festplatte 428
SSE3-Funktion 104
SSH Service 295
SSH-Client 91
SSH-Sicherheitsschlüssel 979
SSL-Fingerprint 261
SSL-Zertifikat 202, 755, 1029
Standalone-Download-Manager 266
Standardinstallation 279
Standard-SCSI-Adapter 461
Standby Uplinks 341
Start Order 691
Startpriorität 276
Startup-Level 276
Stateful-Inspection 1111
Static binding 357
Statistics 750
Status des erworbenen Supports 1059
Stellplatz 880
Storage Adapter 300
Storage Appliance 278, 287
Storage Area Network → SAN
Storage DRS 186
VASA 596
Storage I/O Control → SIOC
Storage Profiles 744
Storage Views 298, 309, 733
Storage vMotion 44, 97, 123
Belastung 127
Storage-Alert 527
Storage-Architektur 393
Storage-Array-Type-Plugin 436
Storage-Awareness 186
Storage-Capability 468
Storage-DRS-Lastverteilung 187
Storage-Groups, Best Practices 589
Storage-Konfiguration 569
Storage-Probleme 393
Storage-Providers 743
Storage-Prozessor 409
Storage-Prozessor-Port 409
Storage-Replication-Modul 1094
Storage-Virtualisierung 409
Storage-vMotion-Mirror-Treiber 125
Storage-vMotion-Plugin 123
Storage-vMotion-Prozess 124
Storage-vMotion-Timeout 132
Streaming-Client 1161
Streched Cluster 144
Strict Admission Control 141
Striping 457
Stun During Page Send → SDPS
Stun Mode 107
Sub-Block 449
Sub-LUN-Clon 536
Subscription 1053
sudo 224
Summary 298, 308
Support 1053
Supportanfrage, Schweregrad 1055
Support-Calls 92
Supportmatrix 415
svmotion 315
svMotion vSphere-Client 129
Swap-Datei 448
Swapfile Location 912
Switch 324
Ausfall 388
Einstellungen 346
unmanaged 384
Switched Fabric 402–403
Switch-Port überbuchen 506
Synchronisierung 672
Syntax 315
sysconfig -v 540
Syslog 1030
Syslog Collector 269, 801
Syslog-Dienst 1030
Syslog-Ziel 801
Sysprep 827–828, 951
System Processors Load 991
System Resource Allocation 301
System-Account 253
System-DSN 241, 253
System-ID 983
System-Log 739
System-Resource-Pool 713
System-Rolle 717
Systemsteuerung 240
Systemtools 834
Systemvoraussetzungen 237
Systemwiederherstellung 836

T

T10-Namespace 410
Tagged TLB 118
Take a Snapshot 960
Taktsignal 884
Target 409
Target-Port 489
Task anlegen 738
Task-Planer → Job-Planer
Tasks & Events 309
TCP/IP Offload Engine 406
TCP/IP-Protokoll 404
Teaming 340
Teaming and Failover 337
Template 946, 1077
Teradici 1161
Terminal-Server 1151, 1154
Test-Trap 679
Testumgebung 35, 1016
Texas Memory 399
TFTP 228
TFTP-Dienst 817
TFTP-Server 272, 811
Thick-Format 830
Thin Provisioned VM 444
Thin Provisioning 43, 189, 442, 457, 470, 527, 546
Thin-Agent-Driver 1121

ThinApp 1152, 1161
Thin-Clients 1157
Thin-Festplatte 438
Thin-Provisioned-Format 131
Thin-Provisioning-Modus 425
Threshold 994
Time Configuration 301, 673
Timeout-Wert 552, 753
Timer 676
Time-Service 677
Tip of the Day 742
TLUs 575
tnsnames.ora 247
TNS-Profil 247
Toter Winkel 1103, 1111
Traffic-Shaping 332
Transaktion 676
Transparent Page-Sharing 433, 463
Trend Deviation 994
Trendanalysen 1136
Trendanzeige 993
Trespassed LUNs 662–663
Trespassing 412
Triggered Alarm 757
Trivial File Transfer Protocol 228
Troubleshooting Options 295
Troubleshooting-Modus 1025
Trunk-Port 334
Trust 791
Turn on Fault Tolerance 204

U

Überbuchung 423
Übertragungsstatistik 1008
Überwachungsinformationen 678
Umsteiger 85
Unified Storage 488
Universale Installation 217
Unix
Hardlink 542
Rechte 519
Unterbrechungsfreies Upgrade VMFS-5 449
Unused Uplinks 341
Update Manager 92, 232, 262, 264, 278, 299
Download 775
Download-Frequenz 770
Download-Server 776
Einstellungen 771
Export 779
Export der Patches 779
Kommandozeile 777
Metadaten 780
Network Connectivity 767
Sicherheitsrichtlinien 770
smart Reboot 773
Snapshot 770
vApp 772
Zeitplaner 769
Upgrade 231
ESX 3.x/ESXi 3.x 231
ESX 4.x/ESXi 4.x 231
vSphere 5.x 231
Upgrade Checker 250
Upgrade-Baseline 233
Upgradeschritte 91
Uplink 326, 386
Uplink-Port 506
USB-Arbitrator 919
USB-Autoconnect 920
USB-Controller 919
USB-Gerät 919–920
Controller-Typ EHCI+UHCI 921
Controller-Typ xHCI 921
entfernen 925
verbinden 921
vSphere vMotion 920
USB-Medium 215
USB-Memory-Stick 215, 397
USB-Passthrough 919
Use explicit failover order 336, 340–341
Use Shared Repository 769
User-DSN 241
User-ID 0 519

V

VAAI 443, 602, 633
Fast Clones 623
NFS aktiviert 622
Status 603
VAAI (Forts.)
Thick Virtual Disks 622
UNMAP 603
VAAI for NFS 622, 640
VAAI UNMAP DISABLE 605
VAAI UNMAP 605
VAAI-Storage-Kommunikation 123
VAAI-Unterstützung 126
vApp 685, 1131
Abarbeitungsreihenfolge 692
anlegen 685
Edit Settings 689
IP Allocation Policy 690
Längenbeschränkung des Namens 685
Manual Startup 694
Optionen 689
Ressourcen 686
Start Order 689
transient 690
Verknüpfung 687
vServices 689
VASA 186, 469, 637
Compliance 598
Installation 597, 637, 655
Konfiguration 638
Speicherprofil 597–598
Storage DRS 597
VNX-LUN-Typen 597
VASA-Provider 472
VCB 132, 281, 445, 716, 852
VCB-Proxy 853
vCD 1131
vCD Cell 1132
vCenter
Advanced Settings 755
Management-Homepage 700
Unisphere-Anbindung 577
vCenter CapacityIQ 1082
vCenter Chargeback 1084
vCenter Converter 275
Advanced options 834
Data to copy 831
Devices 832
Dienste 833
Nacharbeiten 837
Networks 833

vCenter Converter Standalone 279
vCenter Host Agent Pre-Upgrade Checker 250
vCenter Lab Manager 1077
vCenter Mobile Access → vCMA
vCenter Operations 1136, 1143
Lizenzierung 1146
vCenter Ops → vCenter Operations
vCenter Orchestrator 1081
vCenter Server Heartbeat 282
vCenter Server-Appliance 278, 760, 763
vCenter Site Recovery Manager → SRM
vCenter Update Manager 261, 765
vCenter Web Client 258
vCenter-Oberfläche 297
vCenter-Protokolldateien 277
vCenter-Server 56, 89, 232, 235, 305–307, 522, 1152
Administration 306
Editionen 57
EXXi-Hosts hinzufügen 307
HA-Cluster 309
Homepage 306
Inventory 306
Management 306
Solutions and Applikations 306
Starten 307
Troubeshooting 312
vCenter-Server-Datenbank, Sicherung 851
vCenter-Verwaltung 1026
vCLI 89, 1028
vCloud Cells 1132
vCloud Connector 1134
vCloud Director 1105, 1131
vCMA 302
vCOPs 1136
VCVA 761
VDDK 1102
VDI 425, 1016, 1151
vDisk 55
vDS 327–331, 348–349, 351, 353, 363, 370
Verbindungsaufbau zu den Zielsystemen 978
Vererbungsreihenfolge 717
Verfügbarkeit 1014
Verlinkung 235
Vertraulichkeit 981
Verwaltungsmöglichkeiten 291
Verwaltungsnetz 382
Verwaltungssicherheit 275
vFabric Hyperic 1140
vFabric tc Server 1138
VI3-Lizenzierung 1068
VIB 271, 806
VIBE 857, 865
vicfg-authconfig 1026
vicfg-ntp.pl 673
vicfg-snmp 679
vicfg-snmp.pl 1030
View Agent 1150, 1157
View Client 1150–1151, 1153, 1156
View Composer 1157
View Manager 1150, 1155
View Open Client 1156
View Portal 1156
View-Connection-Server 1150
vi-fastpass 316
vihostupdate 295
Virtual Appliance 223
Ausführen 316
Virtual Compatibility Mode 126
Virtual Desktop Infrastructure → VDI
Virtual Disk 623
Kapazität 623
Virtual Infrastructure Backup Engine → VIBE
Virtual Machine 298
Startup/Shutdown 693
Virtual Machine File System → VMFS
Virtual Machine Manager 37
Virtual Machine Memory 78
Virtual Machine Monitoring → VMM
Virtual Machine Options 153
Virtual Machine Support 66
Virtual Mode 462
Virtual Security Gateway 1103
Virtual SMP 71
Virtual Storage Console → VSC
Virtual Storage Integrator 627
Virtual Symmetric Multi Processing 43
Virtual-Disk-Mode 896
Virtualisierung
Applikationen 1152, 1161
hypervisor-basierte 37
Virtualisierung der MMU 902
Virtualisierungs-Overheads 78
Virtualisierungstechnologien 52
AMD-V 52
Intel VT-x 52
Virtual-Machine-Netzwerke 385
Virtual-Machine-Netzwerkverbindungen 141
Virtuelle Hardware 886, 898
Virtuelle Maschine 34, 885
Bestandteile 891
Deployment 948
Eigenschaften 902
Erstellung 893
Festplattenkonfiguration 896
Grundlagen 885
in der DMZ 1038
Migration 945
Netzwerkkarten 889
Netzwerkkonfiguration 896
Optimierung 938
USB-Geräte 919
Virtueller getunnelter Interconnect 495
Virtueller Server, Rechnung 1086
VLAN 321, 333, 383, 1117
privates 1039
VLAN-ID 333
vLockstep-Technologie 199
VM
Killen einer hängenden 967
neue registrieren 527
VM Application Monitoring 166
VM Storage Profile → Speicherprofil
VM's and Templates 293
vMA 89, 225, 313, 316, 793
vMA 5.0 315
VMDirectPath 54, 300, 430
VMDirectPath I/O 407, 463

VMDK-Alignment 552
VMDK-Datei 875, 891
VMFS 449, 492
Migration 454
Skalierungsprobleme 428
Upgrade 449
UUID 450
VMFS Volume Grow 529
VMFS-5 449
VMFS-Blockgröße 459
VMFS-Datastore 218, 626
Komprimierung 632
VMFS-Extents 456
VMFS-Metadaten 410
VMFS-Partition 485
VMFS-Partition-Alignment 452
VMFS-SCSI-Errorcodes 460
VMFS-Signatur 534
VMFS-UUID 450
VMFS-Version 5 Migration 454
VMHA 163
VMI-Paravirtualisierung 902
VMkernel 65, 422
Swapspace 447
VMkernel-Adapter 109
VMkernel-Port 101
VMkernel-Protokoll 119
vmkfstools -L lunreset 456
vmklogger 199
VMM 37, 70, 80, 163, 310, 881–882, 884
vmmemctl 80
vmnic-Nummerierung 326
vMotion 97, 272, 310, 463, 1026
Auslagerungsdatei 119
Datenübertragung 116
Iterationskopie 118
lokale Geräte 117
SCSI-Reservation-Conflicts 118
Sicherheit 116
über Datacenter-Grenzen 117
vMotion-Abbrüche 121
vMotion-Interface 101
vMotion-Migration 144
vMotion-Migrationen pro VMFS-Datastore 116
vMotion-Modul 100
vMotion-Netz 384
vMotion-Netzwerk 384
vMotion-Plugin 123
vMotion-Priorität 115
vMotion-Prozess 98
vMotion-Vorgang 164
VMs and Templates 829
VMsafe-API 1041, 1101
VMSD-Datei 893
VMSN-Datei 893
VM-Speicherprofil → Speicherprofil
VMSS-Datei 893
vm-support 1055
VM-Swapfile 711
VMT 335
VMware 209
VMware Auto Deploy 229
VMware Backup 127
VMware Compatibility Guide 238
VMware Configuration Manager 1100
VMware Consolidated Backup → VCB
VMware Converter 826
VMware Data Recovery 46, 285, 866
Managementoberfläche 818
VMware Data Recovery Clients 287
VMware Disk Development Kit → VDDK
VMware DRS 310
VMware ESXi 42, 1021
VMware EVC 310
VMware Fast Server Recovery 141
VMware Fault Tolerance 208
VMware Fusion 41
VMware High Availability (HA) 140, 198, 309
VMware Management Framework 65
VMware Paravirtual 888
VMware Player 41
VMware Scripts 941
VMware SDK 123
VMware SDK for Perl 47
VMware Server Linked Mode 47
VMware Service Manager 1131
VMware Tools 445, 675, 939–940
aktualisieren 943
Automatische Aktualisierung 905
VMware Tools Service 940
VMware Tools Toolbox 941
VMware vCenter Chargeback 1084
VMware vCenter Lab Manager 1077
VMware vCenter Orchestrator 46
VMware vCenter Server 42, 235
standalone 253
VMware vCenter Server Heartbeat 47
VMware vCloud Connector 1131
VMware vCloud Director 1131
VMware vFabric Enterprise Ready Server 1131
VMware vFabric GemFire 1131
VMware vFabric Hyperic 1131
VMware vFabric tc Server 1131
VMware View 4 1148
VMware View Edition 1143
VMware View, Verfügbarkeit 1155
VMware View-Upgrades 1149
VMware Virtual Infrastructure, Administration 317
VMware VMsafe-API 1101
VMware vShield Zones 46, 1038
VMware vSphere 42
Einführung 42
Installation 209
Systemvoraussetzungen 209
VMware vSphere 5.0 209
Download 212
Lokale Installation 214
VMware vSphere CLI 47
VMware vSphere Client 42
VMware vSphere for SMBs 50
VMware vSphere Hypervisor 41
VMware vSphere Management Assistant 48
VMware vSphere PowerCLI 47
VMware vSphere SDKs 47
VMware vSphere Storage Appliance → VSA

VMware vSphere Web Client 42
VMware vSphere Web Services SDK 47
VMware vStorage APIs for Array Awareness 472
VMware vStorage APIs for Array Integration 470
VMware Workstation 40, 231
vmware.log 1032
VMware-Editionen 48
Enterprise Edition 48
Standard Edition 48
VMware-Gerätetreiber 941
VMware-HA-Cluster 382
VMware-Lizenz 1043
VMware-Lizenz-Server 703
VMware-Maps-Funktion 203
VMware-Snapshot 464
VMware-SNMP-Dienst 1030
VMware-Storage 435
VMware-Tools-Shrink-Funktion 445
VMware-Tools-Skript 904
vmware-umds.exe 776
VMware-User-Prozess 941
VMX-Datei 891
VMXF-Datei 893
VMXNET 2 (Enhanced) 889
VMXNET 3 84, 889
vNetwork Distributed Switch 328, 348
vNetwork-Standard-Switch → vSS
VNX Installation Assistant 577
VNX Virtual Storage Appliance, VSA 658
VNX, Festplattentypen 572
VNX-Speichergruppen 572
vol autogrow 548
vol create 493, 509
Volume Shadow Copy 285
Volume Space Guarantee 548
Volume, flexibles 522
Vorher-Nachher-Betrachtung 1017
Vorlagenkatalog 1130
VPN 1125
VPN-Verbindung 1008
vpxa 100
vpxuser 1025
vRAM-Pool 1044
VSA 287, 475, 478
Konfigurationsarbeiten 842
VSA Cluster Service 478
VSA-Architektur 477
VSA-Cluster 287, 289, 840
Installation 289
VSA-Manager 288
Installation 288
Plugin 289
VSC 532, 551, 554
vShield 1100, 1133
Automatisierung 1127
Powershell Commandlet 1127
Versionskompatibilität 1127
vShield App 1104, 1111
Betrieb 1113
Funktionen 1115
Installation 1111
Regelbasis 1115
vShield App with Sensitive Data Discovery → SDS
vShield Edge 1104, 1124
vShield Endpoint 1104, 1127, 1152
vShield Manager (VSM) 1104–1105, 1109
Backup und Betriebshandhabung 1111
Benötigte Netzwerkports 1107
Benutzerverwaltung 1109
Installation 1105
vShield Zones 1104
vShield-CLI, Tipps 1108
VSI 626–627, 652
Access-Profile 653
Compress 632
DHSM 653
Discover New VNX 653
Erweitern von Datastores 629
Fast Clone 630
Full Clone 630
Import Access Profile 654
Installation 652
Konfigurieren 653
Multipathing Policy 633
Network File Systems 628
Provision Storage 626
RDM Volume 628
VSI (Forts.)
Solutions Enabler 653
VSI for VMware vSphere Path Management 652
VSI und Netzwerke 652
VSM 1109
vSMP 71, 76
vSphere 4-Lizenzen 1062
vSphere 5.0, Update 231
vSphere 5i
Erststart 220
Installation 216
vSphere CLI 86, 221
Ausführen 315
Installation Linux 222
Installation Windows 223
vSphere DirectPath I/O 900
vSphere Distributed Power Management 44
vSphere Distributed Resource Scheduling 44
vSphere Enterprise 1049
vSphere Enterprise Plus 1049
vSphere ESXi 5.0 657
vSphere Fault Tolerance 44
vSphere HA Protection 165
vSphere High Availability 44
vSphere High Availability Agent 155
vSphere Image Builder
Add-EsxSoftwareDepot 805, 809
Export-EsxImageProfile 811
Get-EsxImageProfile 805
New-EsxImageProfile 806
Remove-EsxSoftwarePackage 807
vSphere Management Assistant → vMA
vSphere SDK for .NET 47
vSphere Standard Switches 45
vSphere Storage DRS 45
vSphere Virtual Machine File System 43
vSphere vMotion 44
vSphere4 Essential 1054
vSphere4 Standard 1049
vSphere-Architektur 51

vSphere-Client 257, 296, 304–305
herunterladen 296
iPad 304
vSphereESX 5, Voraussetzungen 88
vSphere-Host 52
Advanced Settings 713
Verwaltung 308
vSphere-Security 694
vSphere-Server, Installation über das Netzwerk 228
vSphere-SNMP-Agent 1030
vSS 327–330, 344–345, 351, 354, 370
VST 333
vStorage API for Storage Awareness 191
vStorage-API 537
vSwitch 327, 385
vSwitch-Typen 328
Cisco Discovery Protocol 342
Load-Balancing 336
NIC-Teaming 336
VLAN-Einstellungen 333
VSWP-Datei 892
VTIC 495

W

w32tm 677
WAFL-Dateisystem 546
Wake on LAN → WOL
Wartungsmodus 186
Wartungsplan 851
Watchdog-Prozess 156
Web Zugriff 88
WebAccess 526
Webbasierte Benutzerschnittstelle 977
Web-Client 293
Weboberfläche 291–292
Webzugriff 292
Wechselmedien 837
Wiederherstellbarkeit 275
Windows 315
Windows Aero 1160
Windows Management Instrumentation 979
Windows-Registry 983
WOL 326
Workflow 1081
World Wide Number → WWN
WWN 410
WWN-Zoning 417
WWPN 491
Wyse Pocket Cloud 1156

X

X.509 (CER) 804
XCOPY 470
XML-Datei 667

Z

Zeitdienst 677
Zeitfenster 721
Zeitsynchronisation 675–676, 905, 941
Zeitzone 818
Zertifikatsart 803
Zertifizierung 406
Zieldatenbank 262
Ziel-Server, Merkmale 980
Zielsystem 1013–1014
auffinden 978
zonecreate 492
Zoning 417, 490
Zugriffsport 752
Zugriffsrecht 307, 719
Zwei-Prozessor-Lizenz 1066