06/2011 Deutschland € 14,90 Österreich € 16,40 Schweiz SFR 29,80
www.TecChannel.de

IDG

TECCHANNEL COMPACT

IT Experts Inside

Virtualisierung ★ Private Cloud

IT im UMBRUCH

Sicherheit

- Risiken beim Cloud Computing
- Identitätsmanagement in der Cloud

Ratgeber

- Was ist was bei der Virtualisierung
- Lizenzen bei virtuellen Servern
- Cloud-Dienste im Vergleich

Praxis

- Private Cloud aufbauen
- Small Business Server 2011 richtig einsetzen
- Virtuelle Umgebungen verwalten

Ausblick: Hyper-V 3.0 in Windows 8

TEC CHANNEL
SILBER-PAKET

Editorial

Alle schweben auf Wolke 7,

so könnte man mutmaßen, wenn man den aktuellen Studien von IDC und Gartner Glauben schenkt. Demnach nutzen bereits bis zu 70 Prozent der deutschen Unternehmen irgendeine Form von Cloud-Diensten. Doch die Bedenken, das moderne IT-Outsourcing weiter zu forcieren, bleiben weiterhin bestehen. Hauptkritikpunkt ist dabei die klare Definition der angebotenen Cloud-Services in Bezug auf Governance, Compliance und Performance. Ist einer der Aspekte nicht eindeutig geklärt, kann ein Unternehmen schnell in Bedrängnis kommen. Doch keine Panik, wer sich im Vorfeld ausführlich über mögliche Risiken und Hürden informiert, ist relativ gut gegen aufkommende Probleme gewappnet. Dabei sollte man die alte Weisheit "Zeit ist Geld" nicht unbedingt in den Vordergrund stellen.

Doch es gibt auch noch andere Baustellen, die den IT-Verantwortlichen in einem Unternehmen beschäftigen. An erster Stelle steht die kostenintensive Verwaltung der bestehenden IT-Infrastruktur. Diese sollte nach Möglichkeiten optimal ausgelastet sein. Dabei gilt es, Arbeitsprozesse und Ressourcen zu optimieren, zu verdichten und störungsfrei mit geeigneten Tools zu verwalten. Ein probates Mittel ist die Virtualisierungstechnologie. Sie offeriert eine Fülle von Lösungen, die vom Desktop über den Server bis ins Data Center reichen. So sind es oft die "kleinen" Virtualisierungslösungen, die ein großes IT-Problem aus dem Weg räumen.

Unser TecChannel-Compact greift aktuelle Themengebiete rund um Server, Virtualisierung und Cloud auf. In Ratgebern und Workshops zeigen wir Ihnen Lösungsansätze, die Sie sofort in die Praxis umsetzen können. Viel Spaß dabei!

Bernhard Haluschak

Impressum

Chefredakteur: Michael Eckert (verantwortlich, Anschrift der Redaktion)
Redaktion TecChannel:
Lyonel-Feininger-Straße 26, 80807 München,
Tel.: 0 89/3 60 86-897
Homepage: www.TecChannel.de,
E-Mail: feedback@TecChannel.de
Autoren dieser Ausgabe werden bei den Fachbeiträgen genannt
Verlagsleitung: Michael Beilfuß

Grafik und Layout:
stroemung GmbH (Michael Oliver Rupp, Oliver Eismann), Multimedia Schmiede, Twentyfirst Communications (Bernd Maier-Leppla)
Titel: Clemens Strimmer
Anzeigen: Anzeigenleitung: Sebastian Woerle
Tel.: 0 89/3 60 86-628
Ad-Management: Edmund Heider (Ltg.) (-127)
Anzeigenannahme: Martin Behringer (-554)
Druck: Sachsendruck GmbH, Paul-Schneider-Strasse 12, 08525 Plauen

Gesamtvertriebsleitung IDG Deutschland: Josef Kreitmair
Produktion: Jutta Eckebrecht (Ltg.)
Bezugspreise je Exemplar im Abonnement:
Inland: 12,30 Euro, Studenten: 10,95 Euro,
Ausland: 13,05 Euro, Studenten: 11,70 Euro
Haftung:
Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Veröffentlichungen in TecChannel-Compact erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt. Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: Alleiniger Gesellschafter der IDG Business Media GmbH ist die IDG Communications Media AG, München, eine 100-prozentige Tochter der IDG Inc., Boston, Mass., USA.
Verlag:
IDG Business Media GmbH
Lyonel-Feininger-Straße 26
80807 München
Tel.: 0 89/3 60 86-0, Fax: -118
Homepage: www.idg.de
Handelsregisternummer: HR 99187
Umsatzidentifikationsnummer: DE 811257800
Geschäftsführer: York von Heimburg
Mitglied der Geschäftsführung: Michael Beilfuß
Vorstand: York von Heimburg, Keith Arnot, Bob Carrigan
Aufsichtsratsvorsitzender: Patrick J. McGovern

TecChannel ist Mitglied der IDG Business Media GmbH und somit ein Teil der IDG-Verlagsgruppe. Darin erscheinen unter anderem auch folgende Zeitschriften:

Abonnement, Einzel- und Nachbestellung, Umtausch defekter Datenträger:
TecChannel Kundenservice, Postfach 81 05 80, 70522 Stuttgart, Tel: (+49) 07 11/72 52-276, Fax: -377, für Österreich 1/21 95 560, für Schweiz, 0 71/3 14 06-15, E-Mail: shop@TecChannel de

Inhalt

1 Server

Als zentrales Rückgrat der Unternehmens-IT sollen Server Informationen und Anwendungen zur richtigen Zeit am richtigen Ort und in bestmöglicher Verfügbarkeit bereitstellen. Dabei konkurrieren eigene Server-Unternehmenslösungen immer öfter mit Infrastrukturleistungen, bei denen Server-Hardware samt Storage übers Netz bereitgestellt und nach Bedarf bezahlt wird.

1.1 Die zehn größten IT-Herausforderungen

Wer als IT-Manager die Bereiche Server, Storage und Data Center verantwortet, steht vor einer Fülle von Herausforderungen. Sie reichen vom ungebremsten Datenwachstum über neue Server-, Storage- und Virtualisierungskonzepte bis hin zu Personalengpässen und den noch immer weitverbreiteten Legacy-Anwendungen im Rechenzentrum.

Gartner-Analyst Rakesh Kumar (www.gartner.com) erläutert die zehn wichtigsten Trends in der IT-Infrastruktur und wie IT-Manager darauf reagieren sollten. Kumar betreut bei Gartner die Themen Server, Storage und Data Center.

1.1.1 Trend 1: Virtualisierung erfasst alle IT-Bereiche

„Virtualisierung steht noch ganz am Anfang", lautet eine provokante These des Gartner-Experten. Eines Tages werde sich die gesamte Unternehmens-IT (Server, Storage, Netze, Desktops, Applikationen) nur noch als ein einziges logisches System darstellen. Allein die Anzahl virtualisierter PCs werde von weniger als fünf Millionen im Jahr 2007 auf rund 660 Millionen im Jahr 2011 steigen.

Damit einher gingen tief greifende Veränderungen in Business- und IT-Abteilungen. Sie beträfen sowohl die Art, wie IT beschafft, verwaltet und genutzt werde, als auch die Methoden für das Software-Pricing und die Lizenzmodelle. Die Vorteile einer umfassenden Virtualisierung liegen laut Kumar auf der Hand: weniger physikalische IT-Komponenten, bessere Auslastung, Energieeinsparungen und ein niedrigerer Kapitalbedarf. Hinzu kämen Verbesserungen bezüglich Hochverfügbarkeit, Management und Security in einer virtualisierten Infrastruktur.

To-Dos für IT-Manager

- Prüfen Sie Ihre IT-Konsolidierungspläne. Können Sie noch mehr tun?
- Haben Sie alle Virtualisierungsvarianten berücksichtigt?
- Haben Sie einen Plan? Virtualisierung ist ein Prozess, kein einmaliges Projekt!

1.1.2 Trend 2: Ungebremstes Datenwachstum

Die in Unternehmen gespeicherte Datenmenge wächst innerhalb der kommenden fünf Jahre um 800 Prozent, lautet eine weitere Gartner-Prognose. 80 Prozent der Steigerungen entfallen demnach auf unstrukturierte Daten, was die Verwaltung zusätzlich erschwert. Trotzdem müssen IT-Verantwortliche weiter mit knappen oder gar reduzierten Budgets auskommen. Die führenden IT-Anwenderunternehmen versuchen, Storage-Systeme besser auszulasten und zu managen, berichtet Kumar. Dabei spielen Virtualisierungs- und Deduplizierungstechniken eine wichtige Rolle, aber auch Tiering-Konzepte, die eine Klassifizierung der Datenbestände in wichtige und weniger wichtige Informationen zum Ziel haben.

To-Dos für IT-Manager

- Virtualisieren Sie Storage-Systeme. Nutzen Sie Deduplizierungstechniken.
- Bewerten Sie alle laufenden Daten-Inputs. Behalten Sie nur, was Sie wirklich brauchen.
- Segmentieren und priorisieren Sie die Datenbestände.

1.1.3 Trend 3: Energieeffizienz und Monitoring der IT

Data Center konsumieren 40-mal mehr Energie als die Büros, die sie mit IT-Diensten versorgen, hat Gartner ausgerechnet. Doch nicht nur aus diesem Verhältnis ergibt sich für IT-Verantwortliche ein erhöhter Handlungsdruck. Mit dem Trend zur IT-Konsolidierung und der höheren Packungsdichte von IT-Komponenten rückt auch der damit verbundene Stromverbrauch stärker in den Mittelpunkt.

IT-Verantwortliche haben erkannt, dass viele Systeme schlecht ausgelastet sind und trotzdem viel Energie verbrauchen. Ein durchschnittlicher x86-Server, der eingeschaltet ist, aber nur im Idle-Modus läuft, verursacht laut Gartner rund 65 Prozent des angegebenen Maximalverbrauchs. Wenn Unternehmen nicht messen, welche Workloads auf welchen Servern laufen, verschwenden sie womöglich sehr viel Energie, mahnt Kumar. Einen Hebel für mehr Effizienz bieten auch Automatisierungs- und Monitoring-Systeme.

To-Dos für IT-Manager

- Nutzen Sie Metriken wie PUE (Power Usage Effectiveness) und PPE (Power to Performance Effectiveness), um die Energieeffizienz Ihrer IT-Infrastruktur zu messen.
- Planen Sie eine kontinuierliche Verbesserung der Energieeffizienz in kleinen Schritten.
- Prüfen Sie, wie sich Automatisierung und Monitoring der IT mithilfe des Itil-Frameworks und von CMDB-Systemen verbessern lassen.

1.1.4 Trend 4: Unified Communications und Collaboration

Unternehmen müssen sich auf eine neue Generation von Mitarbeitern einstellen, die eine ganze Reihe unterschiedlicher Kommunikationsmöglichkeiten nutzt. Dazu bedarf es laut Gartner einer Roadmap für die Migration auf Unified Communications (UC).

Die meisten Organisationen nutzen in Sachen UC eine Mischung unterschiedlichster Produkte von mehreren Herstellern. Diese Insellösungen gelte es zu erfassen und einzudämmen. Gartner empfiehlt eine Konzentration auf einige wenige wichtige Anbieter und Produkte.

To-Dos für IT-Manager

- Recherchieren Sie, ob Ihre Softwarelieferanten die Potenziale von UC nutzen und welche Strategie sie verfolgen.
- Prüfen Sie, ob es noch andere Business-Szenarien als die bestehenden für den UC-Einsatz gibt.
- Denken Sie auch an die Kombination aus mobilen Plattformen und UC, um einen Business Case für UC zu finden.

1.1.5 Trend 5: Mitarbeiter halten und weiterbilden

In den meisten IT-Abteilungen finden sich Experten mit tiefen Kenntnissen auf einem oder mehreren technischen Fachgebieten. Ihr Erfolg und ihr Ansehen im Unternehmen beruhen auf diesem Know-how. Daneben gibt es Generalisten, die vor allem das Zusammenspiel unterschiedlicher Technologien und die Wechselwirkungen mit dem Business beurteilen können.

Prüfen Sie einmal objektiv, welche Mitarbeiter in Ihrer IT-Abteilung den größten Wertbeitrag bringen, empfiehlt Kumar. In den meisten Fällen seien es eher die Generalisten und die Business-affinen Kollegen, die regelmäßig auch komplexe Projekte erfolgreich zu Ende führten. Leider sind solche universell einsetzbaren Fachkräfte schwer zu finden. Unternehmen müssten darauf mit einer gezielten Weiterbildungskultur reagieren. Die effektivsten IT-Mitarbeiter seien stets darauf bedacht, Neues zu lernen.

To-Dos für IT-Manager

- Holen Sie die Mitarbeiter aus ihrer Komfortzone.
- Ermöglichen und belohnen Sie stetiges Lernen im Unternehmen.
- Erweitern Sie die Kenntnisse Ihrer IT-Experten sukzessive um weitere Disziplinen und geben Sie ihnen Gelegenheit, ihr Know-how im Business-Kontext im Rahmen von Projekten zu erweitern.

1.1.6 Trend 6: Social Networks – sind Sie bereit?

Man muss nicht erst die mehr als 500 Millionen Facebook-Benutzer bemühen, um die rapide wachsende Bedeutung von Social Networks zu belegen. Entscheidend für IT-Manager sollte sein: Facebook, Twitter, LinkedIn und Co. verändern die Gesellschaft und damit auch das Business vieler Unternehmen. Das trifft besonders auf die jüngeren Mitarbeiter zu, die jetzt in die Firmen drängen.

IT-Verantwortliche müssen darauf vorbereitet sein, warnt Gartner-Experte Kumar. Sein Rat: Denken Sie über mögliche „soziale" Dimensionen Ihrer Websites und Applikationen nach. Kategorisieren Sie etwa Geschäftsprozesse in eher strukturierte und eher unstrukturierte Abläufe. Prüfen Sie, inwieweit letztere Gruppe von sozialen Plattformen und Techniken profitieren kann und wie sich auf diese Weise deren Wertbeitrag im Unternehmen steigern lässt.

To-Dos für IT-Manager

- Beschäftigen Sie sich mit Nutzungsmustern von Social Networks.
- Entwickeln Sie einen Code of Conduct für das Nutzen von sozialen Medien.
- Beobachten Sie, welche Themen in den Social Networks diskutiert werden.

1.1.7 Trend 7: Legacy-Migrationen: Windows und Office

Dass Microsoft den Support für Windows XP zum April 2014 endgültig einstellt, ist mittlerweile hinreichend bekannt. Trotzdem haben längst noch nicht alle Unternehmen eine Migration auf Windows 7 in Angriff genommen. Gartner rät in diesem Kontext zu raschem Handeln. Etliche unabhängige Softwarehäuser (ISVs) hätten schon 2010 aufgehört, neue Softwareversionen für den Betrieb unter Windows XP zu testen. Bis zum Jahr 2012 werde dies der Normalfall sein.

Für IT-Verantwortliche bedeute dies, dass sie neue Releases geschäftskritischer Anwendungen womöglich schon lange vor dem offiziellen Support-Ende von Windows XP nur noch unter Windows Vista oder Windows 7 betreiben könnten. Eine konservative Planung sollte deshalb darauf abzielen, möglichst alle Anwender bis zum Jahresende 2012 auf Windows 7 migriert zu haben. Unternehmen, die über den April 2014 hinaus einen Custom Support für Windows XP benötigen, müssten mit Gebühren von mindestens 200.000 Dollar im ersten Jahr rechnen. Ähnliches gibt Gartner auch bezüglich Office 2003 zu bedenken, dessen Support ebenfalls im April 2014 endet.

To-Dos für IT-Manager

- Entwickeln Sie einen Fahrplan für die Migration.
- Machen Sie eine Bestandsaufnahme und klassifizieren alle Applikationen und Benutzer.

- Prüfen Sie, inwieweit Ihre wichtigsten Softwarelieferanten ältere Windows- und Office-Versionen unterstützen.

1.1.8 Trend 8: Packungsdichte – mehr IT auf immer weniger Raum

In modernen Rechenzentren werden Server-, Storage- und andere IT-Ressourcen immer dichter gepackt. Alle zwei Jahre verdoppelt sich beispielsweise die Anzahl der verfügbaren Cores auf einem Prozessor, berichtet Gartner. So lässt sich mehr Leistung aus einem gegebenen Raumangebot herausholen. Doch was Experten oft als vertikale Skalierbarkeit bezeichnen, birgt auch Nachteile. So steigt etwa die Hitzeentwicklung von immer dichter gepackten Serversystemen, was wiederum die Anforderungen an eine effiziente Kühlung erhöht. Ebenso wächst der Energieverbrauch. Eine Schlüsseltechnik in diesem Kontext ist die Virtualisierung, erläutert Gartner-Analyst Kumar. Sie ermöglicht es nicht nur, vertikal besser zu skalieren, sondern auch, Platz zu sparen und IT-Ressourcen schneller zur Verfügung zu stellen. Dabei erhöht sich zudem die Auslastung der eingesetzten Rechner.

To-Dos für IT-Manager

- Analysieren Sie die Auslastung Ihrer IT-Systeme und achten Sie dabei besonders auf Lastspitzen und Zeiten geringer Beanspruchung.
- Setzen Sie das Serverwachstum in Beziehung zu den daraus resultierenden höheren Anforderungen an Kühlung und Stromverbrauch.
- Installieren Sie ein „Facilities-Team“, das sich vorrangig mit solchen Aufgaben befasst.

1.1.9 Trend 9: Cloud Computing

Der Hype um den Begriff Cloud Computing verstellt bisweilen den Blick auf die eigentlichen Vorteile des Konzepts, moniert Gartner-Mann Kumar. Auch wenn Kostenersparnisse für kleinere Unternehmen ein schlagendes Argument sein mögen, lägen die größten Nutzenpotenziale eher in einem Zugewinn an Elastizität und Skalierbarkeit.

Eben diese Vorzüge sollten IT-Verantwortliche im Auge behalten, wenn sie Cloud-Services evaluieren. Etliche standardisierte IT-Dienste aus der Wolke sind heute marktreif und könnten durchaus auch in größeren Unternehmen dazu beitragen, die berüchtigten operativen Kosten des IT-Betriebs einzudämmen. Nichtsdestotrotz geht auch Gartner davon aus, dass die Private Cloud für einen längeren Zeitraum das dominierende Betriebsmodell bleiben wird.

To-Dos für IT-Manager

- Finden Sie heraus, welche Commodity-Services ihre IT erbringt und inwieweit sich diese auch aus der Cloud beziehen lassen.
- Evaluieren Sie Cloud-Modelle für die interne Nutzung.
- Kategorisieren Sie Anwendungen und IT-Services auf der Basis von SLAs, bevor Sie in Sachen Cloud aktiv werden.

1.1.10 Trend 10: Fabric Computing

Den Begriff Fabric Computing verwendet Gartner meist synonym mit der sogenannten Infrastructure Convergence. Dahinter steht die Idee einer vertikalen Integration von Server-, Storage- und Network-Komponenten mithilfe einer speziellen Managementsoftware.

Eine „Converged Infrastructure", wie sie inzwischen einige große IT-Anbieter propagieren, erlaubt es, einzelne hoch standardisierte „Building Blocks" rasch zu Ressourcen-Pools zusammenzusetzen oder zu verändern, um so schneller auf wechselnde Anforderungen reagieren zu können. Dabei kann es sich sowohl um physische als auch um virtuelle Pools handeln, die nur per Software verbunden sind. Unterm Strich sollen sich dadurch die im Data Center vorgehaltenen Ressourcen optimieren und effizienter nutzen lassen.

To-Dos für IT-Manager

- Evaluieren Sie die einschlägigen Konzepte der IT-Anbieter; seien Sie vorbereitet, wenn Ihnen entsprechende Systeme offeriert werden.
- Entwickeln Sie eine langfristige Data-Center-Strategie, die Fabric-Computing-Aspekte berücksichtigt.

Wolfgang Herrmann

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

TecChannel-Links zum Thema	Webcode	Compact
Die zehn größten IT-Herausforderungen	2036430	S.9
Vergleich – Microsoft SCOM gegen Nagios	2035098	S.15
Small Business Server 2011 Essentials installieren und einrichten	2036084	S.20
Small Business Server 2011: Clients sichern und wiederherstellen	2037146	S.28
Exchange Server 2010 und Lync Server 2010 gemeinsam betreiben	2034967	S.36

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

1.2 Vergleich – Microsoft SCOM gegen Nagios

Wer seine Entscheidung für eine Monitoring-Lösung fundiert treffen möchte, sollte den Blick auf die Lizenzkosten zunächst hintanstellen. Auch auf Basis einer ideologischen Meinung für kommerzielle oder Open-Source-Angebote sollte keine Auswahl getroffen werden. Relevant für einen Entschluss, den man auch Vorgesetzten gegenüber begründen kann, ist eine objektive Abwägung der Vor- und Nachteile inklusive der geschätzten Gesamtkosten für die Einführung und den Betrieb der Software. Den Ausgangspunkt für die Auswahl des Monitoring-Tools bilden immer eine Ist-Analyse der Umgebung und die Planung zusätzlicher Systeme für die Zukunft. Die anzufertigende Auflistung umfasst alle Serverarten und deren Betriebssysteme sowie andere Objekte im Netz wie Switches, Firewalls, die Unterbrechungsfreie Stromversorgung (USV), Türsteuerungen, Telefonanlagen oder Anlagensteuerungen. Bei dieser Untersuchung interessiert auch, über welche Schnittstellen ein System verfügt, um an die gewünschten Informationen zu gelangen. Die notwendigen Überwachungsparameter werden ebenso definiert.

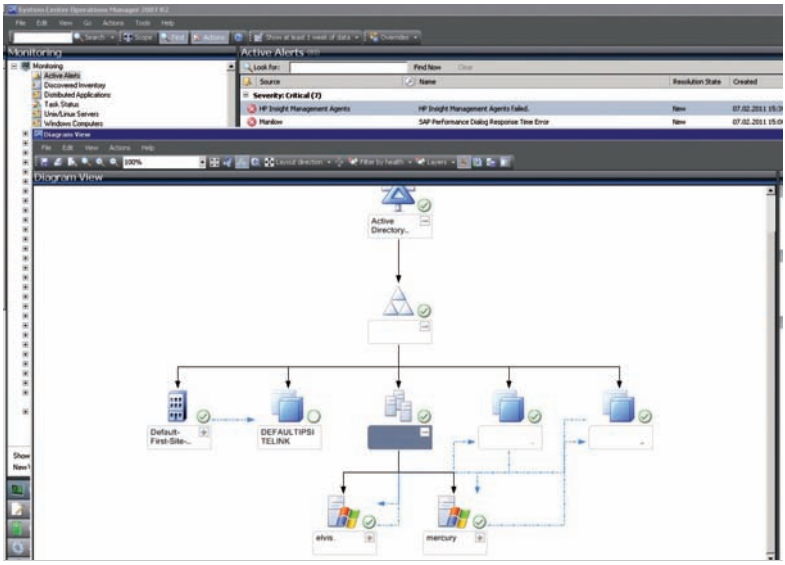
Zur Auswahl stehen dann zahlreiche Monitoring-Lösungen, die sich je nach IT-Landschaft sehr unterschiedlich für den individuellen Einsatz eignen. Oft stellt sich auch die Frage, ob man unter den Angeboten auf ein kommerzielles Produkt oder auf ein Open-Source-Werkzeug zurückgreifen soll. Um diese Entscheidung zu erleichtern, werden im Folgenden zwei namhafte Systeme exemplarisch gegenübergestellt: Das erste System ist Icinga, das im Jahre 2010 von einem Teil der Nagios-Community (www.nagios.org) ins Leben gerufen wurde und seitdem mit beeindruckendem Tempo weiterentwickelt wird. Die Grundfunktionen sind nach wie vor in beiden Open-Source-Systemen ähnlich, daher gelten die hier gemachten Aussagen gleichermaßen für beide Varianten. Bestärkt wird dies durch die uneingeschränkte und beabsichtigte Kompatibilität von Icinga zu Nagios (www.icinga.org) und all seinen Add-ons. Für die kommerzielle Seite sticht aus der Reihe der System-Center-Produkte von Microsoft der Operations Manager hervor, der häufig als Erzfeind von Open Source angesehen wird. SCOM liegt aktuell in Version 2007 R2 vor und verfügt mit den integrierten Cross Platform Extensions auch über eine Anbindung an Teile der Nicht-Microsoft-Welt (www.microsoft.com/systemcenter/en/us/operations-manager.aspx). Anhand dieser weit verbreiteten Lösungen sollen, was die kommerzielle Seite anbelangt, grundlegende Unterschiede und Gemeinsamkeiten zwischen Monitoring-Systemen aufgezeigt werden.

1.2.1 System Monitoring = Daten sammeln

Einer der Hauptunterschiede zwischen den beiden Monitoring-Systemen ist die Art und Weise, wie die Daten der überwachten Systeme gesammelt werden. Icinga verfolgt hier einen eher zentralistischen Ansatz und sammelt die Daten direkt vom

Icinga-Server aus ein, während SCOM dies von Agenten erledigen lässt. Beide Systeme erlauben aber auch die umgekehrte Vorgehensweise. So ist es beispielsweise möglich, auf Icinga-überwachten Systemen einen Dienst zu installieren, der das Sammeln und Versenden der Daten übernimmt (sogenannte passive Checks). Ebenso kann der SCOM-Server aktiv zum Sammeln von Daten bewegt werden, zum Beispiel bei Netzwerkkomponenten oder anderen agentenlosen Systemen.

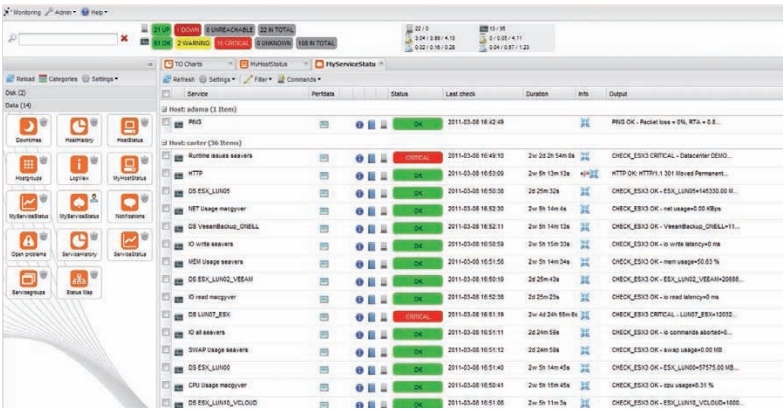
Beide Vorgehensweisen haben Vor- und Nachteile. Beim Datensammeln müssen alle Konfigurationen und Anpassungen lediglich am zentralen Server vorgenommen werden, da es keine dezentralen Agenten gibt. Beim Einsatz von Agenten wiederum können ein Teil der Sammellogik auf den Client verlagert und damit der Server entlastet werden. So reicht es, wenn der Agent den Füllstand einer Festplatte überprüft und beim Überschreiten eines Schwellenwertes einen Alarm auslöst (Modell SCOM), wohingegen ohne Agent (Modell Icinga) in regelmäßigen Intervallen eine entsprechende Kenngröße an den Server übermittelt wird und dieser dann entscheidet, ob der Alarmknopf gedrückt wird. Dies belastet nicht nur den Server, sondern auch die Netzverbindung. Ein einzelner SCOM-Server ist laut Microsoft für die Überwachung von bis zu 3.000 Agenten ausgelegt.



Struktur: Die Verwaltungskonsole des System Center Operations Manager. Im Vordergrund der automatisch erkannte Aufbau des Active Directory.

Natürlich gibt es Dienste, die besser „von außen“ überwacht werden, zum Beispiel ein Mail-Server. Ein Versuch der Verbindung mit dem entsprechenden Port muss erfolgreich sein, sonst erfolgt ein Alarm. Das allein reicht jedoch nicht aus: Han-

delt es sich nur um ein Mail-Relay, so wäre es interessant zu wissen, ob die angenommenen Mails auch zeitnah weitergeleitet werden konnten. Ein Webserver hingegen, der auf eine nachgelagerte Datenbank zugreift, sollte mit einer korrekt generierten Seite antworten und nicht nur mit einer beliebigen Seite. Oft ist demnach die Kombination beider Monitoring-Verfahren sinnvoll, also ein Agent, der den Service und abhängige Komponenten überwacht, im Zusammenspiel mit einem externen Verbindungsversuch, wie ihn auch ein Client vornimmt.



Details: Die Webschnittstelle von Icinga mit der Darstellung der zu einem Host zugehörigen Dienste und deren Status.

Microsoft löst das Problem der dezentralen Umkonfiguration seiner Agenten dadurch, dass der Administrator die einzelnen Konfigurationsänderungen zentral am Server vornimmt und diese dann automatisch an die Agenten übertragen werden. Icinga hingegen arbeitet mit passiven Checks, die es den Clients erlauben, einen Status an einen zusätzlichen Service auf dem Icinga-Server zu melden und diesen dann in die normale Ereigniskette einzusortieren. Bei diesem Entscheidungskriterium ist also interessant, wie und wo die Mehrzahl der benötigten Informationen gewonnen werden kann. Ein weiteres Kriterium wäre, ob der zu überwachende Server durch eine Firewall geschützt ist. In diesem Fall ist unter Umständen eine Abfrage „von außen“ per Icinga nicht möglich, aber ein Senden des SCOM-Agenten „von innen“ erlaubt.

1.2.2 Das Data Warehouse

Betrachtet man bei den beiden Systemen das „Data Warehouse“, also die Ablage der gewonnenen Daten, so werden gravierende Unterschiede sichtbar. Während SCOM auf den etablierten SQL Server setzt, sind die Ansätze bei Nagios, eine Datenbank wie MySQL zu verwenden, bisher eher von mäßigem Erfolg. Ein Großteil

der Nagios-Server setzt immer noch auf die Speicherung in Dateien. Dass dies zu Problemen bei der Performance etwa aufgrund von Größe und Locking führt, dürfte klar sein. Erfreulich ist allerdings, dass sich die Icinga-Entwickler insbesondere dieses Punkts angenommen haben. Eine Historie von Performance-Daten (Antwortzeiten, Füllstand etc.) kann mit Icinga nur sinnvoll über Add-ons erreicht werden, die einfach zu integrieren sind. Der SCOM sammelt die Daten per Agent und ermöglicht von Haus aus entsprechende Statistiken.

Relevant ist auch, wie die zu überwachenden Systeme erfasst werden. SCOM bietet hier ein Auto-Discover, sowohl (sub-)netzwerkbasiert als auch Active-Directory-integriert, wohingegen Icinga seine Informationen aus einer oder mehreren Textdateien bezieht. Diese werden zwar von einigen Administratoren automatisch generiert, in den meisten Fällen jedoch nach wie vor von Hand gepflegt, was recht fehleranfällig ist. Diese Fehleranfälligkeit lässt sich jedoch durch sinnvolle Vorlagendefinitionen für die einzelnen Überprüfungen erheblich reduzieren. Hintergrundinformationen über das System selbst, also etwa Hauptspeicher, Prozessortyp oder Betriebssystem, werden in Icinga über eine sogenannte Extended-Host-Information ebenfalls von Hand erfasst. Der SCOM liest diese Infos direkt aus und stellt sie zur Verfügung. Durch die seit einiger Zeit erhältlichen Cross Platform Extensions ist dies nicht nur auf Windows-Systeme beschränkt. Der Zugriff auf diese möglichst aktuellen Informationen kann eine wertvolle Hilfe bei einer Störungsbeseitigung oder Fehlersuche sein.

1.2.3 Wichtige Punkte bei der Einführung von Überwachungssystemen

- Klar definieren, was und wie tief überwacht werden soll;
- Lizenzkosten den geschätzten Aufwänden gegenüberstellen;
- Automatisierung von Problemlösungen vorantreiben;
- nicht als eigenständiges System betrachten, sondern als Komponente in einer Systemlandschaft (Tickettools);
- gegebenenfalls Produkte kombinieren, zum Beispiel über SCOM2Nagios.

1.2.4 Customizing und Pflege

Ein wesentlicher Aufwand beim Einrichten einer Überwachungssoftware entsteht durch das Customizing beziehungsweise die Pflege des Systems. Gerade das Einrichten neuer Überwachungen und Alarme sowie das Anpassen der Schwellwerte stellen den größten Aufwand innerhalb eines Einführungsprojekts dar. Es ist somit von Vorteil, wenn auf fertige Skripte zurückgegriffen werden kann. Für Nagios hat die sehr aktive Community bereits mehr als 390 nützliche Add-ons bereitgestellt. Auch im SCOM-Umfeld existiert eine starke Community, die Management Packs

(MP) vorhält. In diesen MPs werden alle Informationen hinterlegt, die für die Erkennung, Überwachung, Alarmierung und das Reporting der zu überwachenden Systemen benötigt werden. Das MP wird in SCOM importiert und automatisch an die Agenten verteilt. Durch Discovery Tasks entscheiden diese, ob die Überwachung für sie relevant ist. Dieser Aufbau ist ein großer Vorteil von SCOM in einer Microsoft-lastigen Umgebung, da umfangreiche und kostenlose Management Packs zu allen wesentlichen Produkten von Microsoft angeboten werden. In diesen ist zum Beispiel das fundierte Produktwissen der Exchange-Entwickler hinterlegt, die sinnvolle Schwellenwerte und mögliche Lösungen eines Problems in der integrierten Knowledge Base beschrieben haben. So beinhaltet das Active Directory Server 2008 Management Pack mehr als 850 fertige Regeln zu Überwachung des ADDS. Auch viele Drittanbieter offerieren MPs.

1.2.5 Alarmierung und darüber hinaus

Nachdem ein Fehler festgestellt wurde, kann eine bei beiden Produkten ähnliche Alarmierung erfolgen sowie eine automatisierte Problemlösung angestoßen werden. Ein einfaches Beispiel wäre ein SSH-Dienst, der auf einem Linux-System regelmäßig abbricht. Hier kann ein Administrator benachrichtigt werden, der den Fehler manuell behebt, oder man automatisiert die Aufgabe und lässt den Prozess durch das Managementsystem neu starten. In Icinga übernimmt das der sogenannte Event Handler, in SCOM sind dafür Diagnostic beziehungsweise Recovery Tasks zuständig. Der Wunsch nach einer fehlerfreien IT ist so zwar noch nicht erfüllt, durch die Automatisierung von Workarounds ist jedoch immerhin ein weiterer Schritt in diese Richtung getan. Ein Überwachungssystem steht im Allgemeinen nicht alleine da. Daher ist eine Ankopplung an andere Systeme von Bedeutung. Bestes Beispiel sind Konnektoren für Ticketsysteme. Hier bietet SCOM fertige Schnittstellen zu bekannten Lösungen wie Remedy AR Systems (www.bmc.com). Da die meisten Systeme auch E-Mail-Nachrichten in Tickets umwandeln können, ist über diesen Weg ebenso eine Verknüpfung mit Icinga möglich.

1.2.6 Hierarchien

Gerade in größeren Umgebungen ist ein hierarchischer Aufbau der Monitoring-Lösung wünschenswert. Denkbar sind standortbezogene Managementserver, die ihren Status an einen zentralen Server schicken. Dadurch wird auch die Last verteilt. Icinga unterstützt diesen Ansatz durch diverse Add-ons wie NSCA oder mod_gearman. Der Operations Manager lässt sich ebenfalls verschachteln. Alternativ ist auch der Einsatz von Gateway-Servern möglich, die die Meldungen von einem Standort sammeln und komprimiert weiterleiten.

Markus Bäker

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

1.3 Windows Small Business Server 2011 Essentials installieren und einrichten

Für kleine Unternehmen bietet Microsoft eine eigene Edition des Windows Small Business Server 2011 (SBS 2011) an, den Windows Small Business Server 2011 Essentials. Der Entwicklungsname dieser Version lautete Aurora. Der Server baut auf Windows Server 2008 R2 auf, unterscheidet sich vom SBS-2011-Standard aber deutlich. Die Essentials-Version richtet sich an Unternehmen mit bis zu 25 Benutzern; ebenso viele lassen sich an den Server anbinden. Die Standardversion spricht Unternehmen mit bis zu 75 Nutzern an.

SBS 2011 Essentials steht wie die anderen aktuellen Microsoft-Server nur als 64-Bit-Version zur Verfügung. Small Business Server 2011 Essentials bietet vor allem eine zentrale Datenablage und die Möglichkeit, über Connectoren die Daten auf Client-Computern zu sichern und diese zu überwachen. Im Folgenden haben wir für Administratoren beziehungsweise IT-Zuständige in entsprechenden Unternehmen die Installation und die ersten Schritte zusammengefasst.

1.3.1 Installation des SBS 2011 Essentials

Um SBS 2011 Essentials auf einem neuen Server zu installieren, legen Sie die Setup-DVD ein und booten mit dieser. Es startet der Installationsassistent. Im ersten Fenster wählen Sie aus, ob Sie den Server installieren wollen, oder ob Sie eine Systemreparatur durchführen wollen. Auf der nächsten Seite wählen Sie die Festplatte aus, auf der Sie den Server installieren wollen. Sie müssen auf dieser Seite auch bestätigen, dass der Assistent während der Installation die Festplatte formatiert. Reicht der Festplattenplatz für SBS 2011 nicht aus, erhalten Sie eine Fehlermeldung und die Installation bricht ab. Es müssen mindestens 160 GByte zur Verfügung stehen. Steht weniger Platz zur Verfügung, zum Beispiel durch eine falsche Partitionierung, müssen Sie die Installation neu beginnen, der Installationsassistent lässt sich nicht fortsetzen.

Findet der Installationsassistent keine Festplatte, benötigen Sie den Treiber des Serverherstellers für den Datenträgercontroller. Diesen können Sie anschließend mit der Schaltfläche *Treiber laden* im System integrieren. Am einfachsten kopieren Sie dazu den Treiber auf einen USB-Stick und verbinden diesen mit dem Server. Zeigt der Assistent die Festplatte an, müssen Sie zunächst die Option *Ich bin mir im Klaren, dass alle Dateien und Ordner auf der primären Festplatte gelöscht werden, wenn ich auf Installieren klicke* aktivieren. Erst dann können Sie mit *Installieren* die eigentliche Installation starten. Wollen Sie über diesen Weg SBS 2011 Essentials reparieren, müssen Sie auf der Startseite der Installation statt *Neuinstallation* die Option *Vorhandene Installation reparieren* auswählen.

Nach dem Start der Installation läuft diese ganz ähnlich wie bei anderen Windows-Betriebssystemen ab. Zunächst installiert der Assistent Windows Server 2008 R2

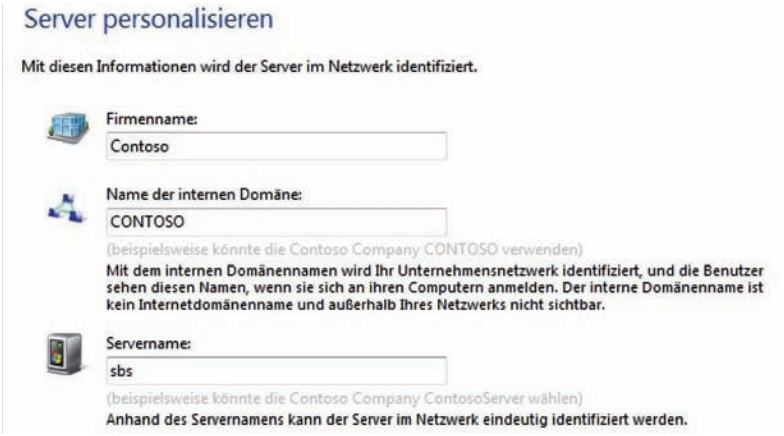
mit SP1 auf dem Server und anschließend die Komponenten von SBS 2011 Essentials. Die Installation dauert je nach System etwa 30 Minuten bis eine Stunde.

Während der Installation des Betriebssystems müssen Sie keine weiteren Eingaben vornehmen. Schließt der Assistent die Installation von Windows ab, findet eine automatische Anmeldung statt und die Integration der SBS 2011-Komponenten beginnt selbsttätig. Im Installationsassistenten wählen Sie als Nächstes das Land, die Zeit und Währung, sowie das Tastaturlayout. Anschließend können Sie die Uhrzeit und das Datum überprüfen und gegebenenfalls anpassen. Achten Sie darauf, dass die Zeit genau stimmt.

1.3.2 Lizenzbedingungen und Serverdaten

Der nächste Schritt besteht im Bestätigen der Lizenzbedingungen, bevor Sie die Installation fortsetzen. Auf der nächsten Seite geben Sie dann den Produktschlüssel für SBS 2011 Essentials ein. Sie müssen bei der Eingabe weder auf Groß- und Kleinschreibung achten noch die Bindestriche eingeben.

Weitere Lizenzen sind in SBS 2011 Essentials nicht einzutragen oder zu erwerben, es reicht aus, wenn Sie während der Installation einmalig den Produktschlüssel eingeben. Als Nächstes geben Sie den Namen Ihres Unternehmens ein sowie den Namen des Servers und der Domäne. Achten Sie darauf, Werte zu nehmen, die leicht einzugeben sind, da Anwender diese zum Verbinden mit dem Server benötigen. Verwenden Sie keinesfalls die Standardvorgaben. Am besten wählen Sie als Domänennamen Ihren Firmennamen oder eine Kurzform. Auch den Servernamen sollten Sie so kurz wie möglich halten. Sie können diese Eingaben nach der Installation nicht mehr ändern.



Fingerspitzengefühl: Bei der Personalisierung sollten Sie die Bezeichnungen sorgfältig auswählen.

Findet SBS 2011 Essentials einen DHCP-Server im Netzwerk, zum Beispiel einen DSL-Router, der IP-Adressen verteilt, bindet sich der Server über eine dynamische IP-Adresse in das Netzwerk ein. Generell ist das kein empfehlenswerter Weg.

Für den Fall, dass Windows keinen DHCP-Server für das automatische Zuweisen einer IP-Adresse erreicht, bestimmt der Server eine Adresse in der für Microsoft reservierten IP-Adressierungsklasse, die von 169.254.0.1 bis 169.254.255.254 reicht. Diese Adresse wird verwendet, bis sich ein DHCP-Server meldet.

1.3.3 Netzwerkkonfiguration für den Server durchführen

Sie sollten Server immer mit festen IP-Adressen konfigurieren, um sicherzustellen, dass sich die IP-Adresse nicht ändert.

```
Windows-IP-Konfiguration

Ethernet-Adapter LAN-Verbindung:

   Verbindungsspezifisches DNS-Suffix: fritz.box
   Verbindungslokale IPv6-Adresse  . : fe80::dd5a:4735:a540:1ef8%11
   IPv4-Adresse  . . . . . . . . . . : 192.168.178.51
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . : 192.168.178.4

Tunneladapter isatap.fritz.box:

   Medienstatus. . . . . . . . . . . : Medium getrennt
   Verbindungsspezifisches DNS-Suffix: fritz.box
```

Check: Rufen Sie die aktuelle IP-Adresse des Servers ab.

Bevor Sie den Namen der Active-Directory-Domäne und des Servers festlegen, sollten Sie daher die IP-Adresse des Servers auf eine feste IP-Adresse festlegen:

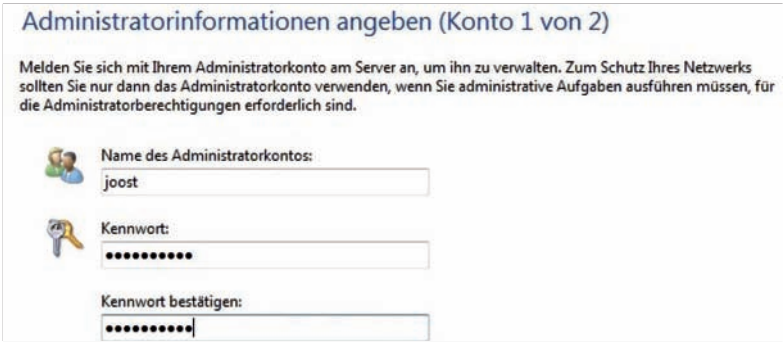
1. Drücken Sie auf der Seite *Server personalisieren* die Tastenkombination [Umschalt]+[F 10].
2. Geben Sie *ncpa.cpl* ein.
3. Rufen Sie die Eigenschaften der Netzwerkverbindung auf.
4. Klicken Sie doppelt auf *Internetprotokoll Version 4*.
5. Geben Sie eine freie IP-Adresse und das passende Subnetz ein.
6. Kennen Sie den IP-Bereich nicht, den Ihr DSL-Router oder DHCP-Server vergibt, geben Sie in der Befehlszeile den Befehl *ipconfig* ein.

Der Installationsassistent von SBS 2011 Essentials versucht, während der Installation immer eine IP-Adresse von einem DHCP-Server zu beziehen. Ist im Netzwerk kein DHCP verfügbar, verzögert das die Installation. In diesem Fall können Sie mit den vorangegangenen Schritten auch die Installation beschleunigen.

1.3.4 Administratorkonto

Auf der nächsten Seite des Assistenten geben Sie den Benutzernamen des Administrators ein, mit dem Sie sich anmelden. Verwenden Sie hier nicht den Standardnamen Administrator, sondern einen anderen Benutzernamen oder Namen wie superuser oder adminuser. Sie können der Einfachheit halber auch Ihr eigenes Benutzerkonto anlegen, wenn Sie den Server mit dem gleichen Konto verwalten wollen, mit dem Sie auch persönlich arbeiten.

Sollen aber andere Anwender den Server verwalten können, wenn Sie nicht da sind, besteht das Problem, dass diese auch auf Ihre persönlichen Daten zugreifen können, wenn sie Ihren Benutzernamen kennen.

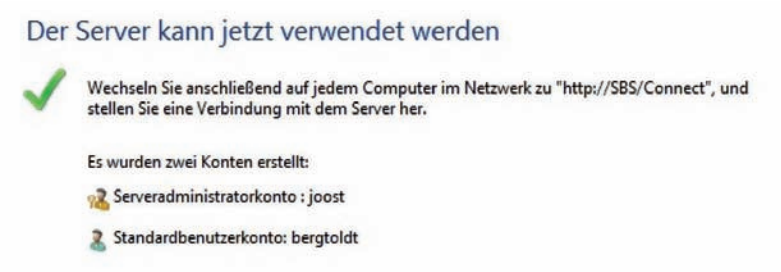


Zuweisung: Geben Sie die Benutzerdaten des Administrators ein.

Im nächsten Schritt legen Sie ein Benutzerkonto fest, das nur Standardrechte hat. Sie können später für jeden Benutzer ein eigenes Konto anlegen. Das erste Konto ist sozusagen das normale Benutzerkonto für den Administrator. Während der normalen Arbeit mit dem Server sollten Sie möglichst keine Administratorrechte verwenden, sondern nur dann, wenn Sie administrative Tätigkeiten vornehmen. Auf der nächsten Seite wählen Sie aus, ob sich der Server automatisch aktualisieren darf. Wenn Sie den Server mit dem Internet verbunden haben, sollten Sie die Option *Empfohlene Einstellungen verwenden* anklicken. Auf diesem Weg kann der Server automatisch wichtige Updates bei Microsoft herunterladen und installieren.

Sobald der Assistent seine Arbeit abgeschlossen hat, erhalten Sie eine entsprechende Meldung und können mit dem Einrichten des Servers beginnen. Die Installation ist an dieser Stelle abgeschlossen.

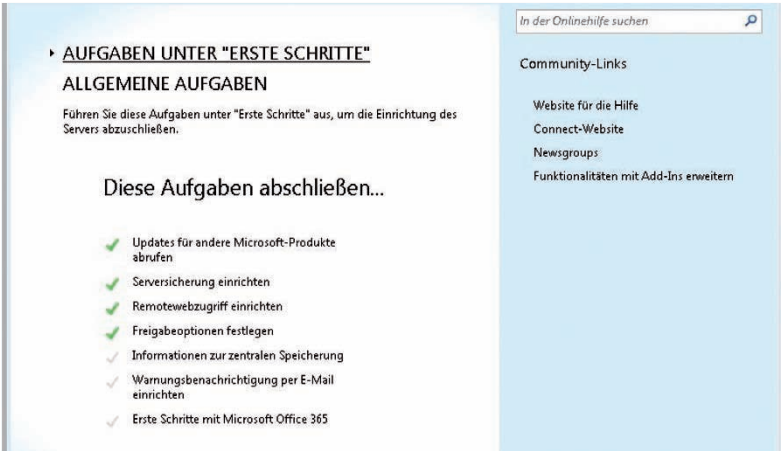
Nach der Installation ist der Server bereit. Melden Sie sich direkt am Desktop an. Sie können ebenso mit dem Remotedesktop arbeiten. Dazu rufen Sie auf einem Windows-7-Computer die *Remotedesktopverbindung* auf und geben die IP-Adresse oder den Namen des Servers ein. Die Remotedesktopverbindung starten Sie durch Eingabe von mstsc im Suchfeld des Startmenüs.



Alles ist gut: Die Installation des Servers ist erfolgreich abgeschlossen.

1.3.5 Erste Einrichtung des Servers

Nachdem Sie die Grundinstallation des Servers abgeschlossen haben, sollten Sie in den nächsten Schritten noch die notwendigen Patches installieren und die Einrichtung des Servers abschließen. Der erste Schritt besteht darin, den Server auf den neusten Patch-Stand zu bringen. Das Service Pack 1 für Windows Server 2008 R2 ist im Server bereits integriert, Sie müssen es nicht installieren. In SBS 2011 Standard ist das SP1 nicht integriert. Die Patches, die auf das SP1 aufbauen, installieren Sie über Windows-Update in der Systemsteuerung.

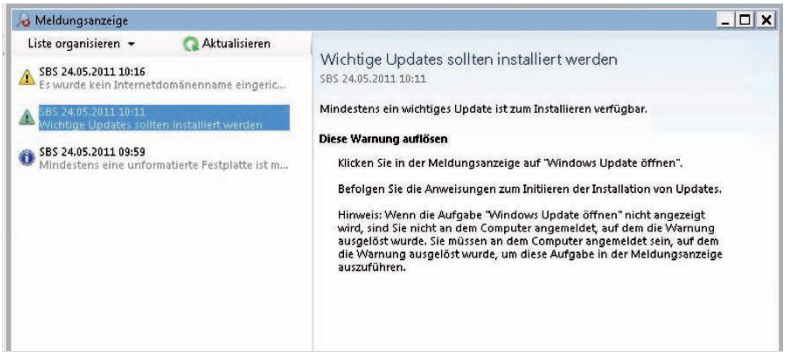


Erste Schritte: Es kann losgehen mit dem Einrichten des Servers.

Nach der Installation des Systems und der SBS-Komponenten müssen Sie SBS 2011 aktivieren. Aktivieren Sie Small Business Server 2011 nicht, stellt der Server den Betrieb nach 60 Tagen ein. Sie können Small Business Server 2011 entweder

über das Internet oder per Telefon aktivieren. Ist der Server mit dem Internet verbunden, finden Sie den Aktivierungs-Link von Small Business Server 2011 über *Start/Systemsteuerung/System und Sicherheit/System*.

Die komplette Verwaltung von SBS 2011 findet generell im Dashboard statt. Eine Verknüpfung zu dem Tool erhalten Sie nach der Installation auf dem Desktop. Hier erreichen Sie über Menüs alle notwendigen Einstellungen. Wenn Sie das Dashboard starten, sehen Sie zunächst eine Checkliste im Bereich *Diese Aufgaben abschließen*. Hier sind alle wichtigen Aufgaben für die erste Konfiguration hinterlegt.



Abschlussarbeiten: Im Dashboard sehen Sie die wichtigen Aufgaben für die erste Konfiguration.

Klicken Sie auf einen Link, öffnet sich das Konfigurationsfenster der entsprechenden Aufgabe. Bevor Sie den Server in Betrieb nehmen, sollten Sie alle diese Aufgaben durcharbeiten, damit der Server ordnungsgemäß zur Verfügung steht. Für viele Aufgaben, wie die Konfiguration der Updates oder des Remote-Webzugriffs, muss der Server eine Verbindung zum Internet haben.

1.3.6 Installation checken

Haben Sie den Server fertig installiert und eingerichtet, besteht der nächste Schritt darin, den Server zu testen und sicherzustellen, dass alles ordnungsgemäß funktioniert. Dabei helfen verschiedene Werkzeuge. Wenn Sie das eben erwähnte Dashboard starten, finden Sie im rechten oberen Bereich ebenfalls eine Überwachungsfunktion. Klicken Sie auf die Schaltfläche mit den Melde-Icons, öffnet sich ein neues Fenster, auf dem Sie ausführlichere Meldungen sehen und Fehler erkennen können. Mit der Taste F5 können Sie eine neue Überprüfung durchführen. Wollen Sie die Meldungen als E-Mail erhalten, können Sie über den Link *Warnungsbenachrichtigung per E-Mail versenden* einen E-Mail-Server und eine Adresse festlegen. Mit dem kostenlosen Windows Server Solutions Best Practices Analyzer (WSSBPA) 1.0 lässt sich eine Installation von SBS 2011 grundlegend testen.

Das Tool verwendet dazu von den SBS-Entwicklern vorgegebene Regeln und kann auch versteckte Probleme und Fehlerursache erkennen und diagnostizieren. Bevor Sie den BPA installieren können, benötigen Sie aber noch Microsoft Baseline Configuration Analyzer 2.0. Dieses Tool müssen Sie vor dem BPA installieren. Nach dem Start des Tools wählen Sie bei *Select a product* zunächst *Windows Server Solutions Best Practices 1.0* aus. Klicken Sie anschließend auf Start Scan. Daraufhin überprüft BPA die Installation des Servers.

1.3.7 Das Dashboard – SBS 2011 Essentials verwalten

Das Dashboard auf dem Desktop von SBS 2011 Essentials ist das zentrale Verwaltungswerkzeug des Servers. Sie benötigen keine weiteren Werkzeuge, alle Aufgaben lassen sich über die verschiedenen Menüs des Dashboards schnell und einfach durchführen. Über die Registerkarte *Start* konfigurieren Sie allgemeine Einstellungen. Alle Benutzer, die auf Daten des Servers zugreifen, verwalten Sie auf der Registerkarte *Benutzer*. Hier steuern Sie Benutzernamen, Sicherheit der Kennwörter, die Freigaben, auf die Benutzer Zugriff haben sowie den Remote-Webzugriff, und legen neue Benutzer an. Über einen Doppelklick auf den Benutzer rufen Sie dessen Eigenschaften auf und können so die Zugriffsebene (Administrator oder Benutzer), den Zugriff auf Freigaben und Computer sowie den Remote-Zugriff steuern. Außerdem können Sie hier Benutzerkonten zeitweise deaktivieren. Über *Computer und Sicherung* sehen Sie die angebundenen Client-Computer. In diesem Bereich können Sie auch Daten aus der Sicherung wiederherstellen.

1.3.8 Client-Computer anbinden

Client-Computer verbinden Sie direkt auf dem entsprechenden Client, indem Sie im Webbrowser den Befehl *http://<Servername>/connect* eingeben. Am besten verwenden Sie dazu den Internet Explorer. Neben Windows-Computern können Sie auch Mac-Clients ab Mac OS X 10.5 an SBS 2011 Essentials anbinden.

Klicken Sie auf den Link *Software für Windows herunterladen*. Es startet der Assistent, der Sie durch die Anbindung führt. Sobald Sie sich an der Domäne angemeldet haben, startet das Launchpad. Über dieses Launchpad starten Anwender die Sicherung des Client, können den Remote-Webzugriff starten und direkt auf die Freigaben auf dem Server zugreifen, für die sie berechtigt sind. Administratoren dürfen zusätzlich noch das Dashboard aufrufen und können Sie mit dem Administratorkonto direkt am Dashboard anmelden. Außerdem lassen sich Meldungen für den Client im unteren rechten Bereich des Launchpads anzeigen. Hier würden Anwender Fehler erkennen, die auf dem Client-Computer auftreten.

Arbeiten Anwender mit Windows 7 Home Premium, können sie zwar ebenfalls über den Connector mit den Freigaben auf dem Server arbeiten. Es ist aber keine Domänenanmeldung am PC möglich wie mit Windows 7 Professional oder Ulti-

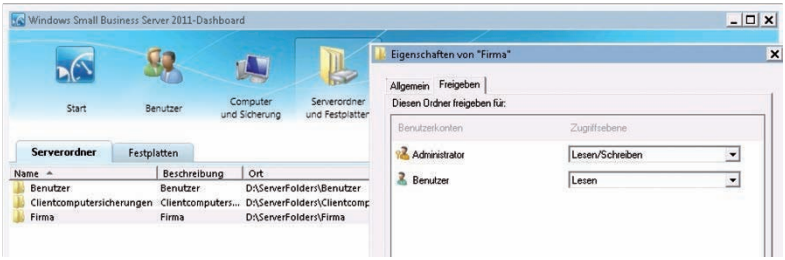
mate. In diesem Fall müssen sich Anwender am Launchpad nach der Anmeldung am PC noch einmal explizit anmelden. Über *Optionen* lässt sich diese Anmeldung auch speichern. Nach der Anmeldung stehen die Freigaben und Funktionen im Launchpad in Windows 7 Home Premium genauso zur Verfügung wie in Windows 7 Professional oder Ultimate.

Der Connector, mit dem der Client an den Server angebunden ist, hat ein eigenes Icon, das Sie über das Tray Icon sehen. Über das Kontextmenü dieses Icons starten Sie das Launchpad, zeigen Warnungen auf dem Computer an und können als Administrator das Dashboard öffnen. An der Farbe des Icons erkennen Anwender, ob der Computer Fehler meldet (rotes Icon), Warnungen findet (gelbes Icon) oder ob alles in Ordnung ist (grünes Icon). Standardmäßig blendet Windows 7 das Icon allerdings aus. Um es dauerhaft einzublenden, klicken Sie im Traybereich der Taskleiste auf den kleinen Pfeil und wählen Anpassen.

Wählen Sie im neuen Fenster dann für das Icon des Connectors die Option *Symbol und Benachrichtigungen anzeigen* aus. Sobald der Connector startet, zeigt er Fehler an, die auf dem Computer aufgetreten sind. Wenn Sie auf *Warnungen anzeigen* klicken, sehen Sie detaillierte Informationen zu den Fehlern.

1.3.9 Festplatten und Freigaben verwalten

Über den Menüpunkt *Serverordner und Festplatten* verwalten Sie den Speicherort Ihrer Daten auf dem Server und die Freigaben auf dem Server. Hier legen Sie in den Eigenschaften auch fest, welche Benutzer Zugriff auf die Daten haben sollen und ob die Benutzer nur lesen oder auch schreiben dürfen.



Zugriff: Über das Dashboard können Sie auch die Festplatten und Freigaben verwalten.

Neben den Freigaben verwalten Sie auch die physischen Festplatten in diesem Bereich. Dazu steht die Registerkarte *Festplatten* zur Verfügung. Für Administratoren sind die Statusmeldungen im Dashboard interessant, ebenso die Schaltfläche *Servereinstellungen*. Hierüber können Sie Einstellungen zum Remote-Webzugriff und zur Überwachung des Servers vornehmen und Fehler anzeigen lassen.

Thomas Joos

1.4 Small Business Server 2011: Clients sichern und wiederherstellen

Anders als die Standard-Edition des Windows Small Business Server 2011 erlaubt es Small Business Server 2011 Essentials Administratoren, die Client-Rechner in die Sicherung mit einzubeziehen. Das ist für die anvisierte Zielgruppe mit maximal 25 Client-Systemen durchaus ein Vorteil, denn es erleichtert dem IT-Zuständigen das Leben. Aus dieser Sicherung lassen sich die Daten sowie das komplette Betriebssystem auf den Clients wiederherstellen. Damit all dies funktioniert, sind eine eingerichtete Sicherung auf dem SBS und die Installation des SBS-Connectors auf den Clients Voraussetzung. Der folgende Praxisbeitrag erläutert detailliert die Sicherung der Clients und die möglichen Wege der Wiederherstellung.

1.4.1 Client-Computer verbinden

Neue Computer verbinden Sie am einfachsten über einen Webbrowser auf dem Client-Computer. Bevor Sie einen Client mit dem Small Business Server 2011 verbinden, erstellen Sie die Benutzerkonten, mit denen sich die Anwender anmelden sollen. Dazu verwenden Sie das Dashboard auf dem Small Business Server.

Kontaktaufnahme: Für die Anbindung des Clients müssen Sie zunächst Software herunterladen.

Um einen Computer an SBS 2011 anzubinden, gehen Sie folgendermaßen vor:

1. Öffnen Sie den Webbrowser auf dem Client-Computer.
2. Geben Sie *http://<Servername des SBS>/connect* in die Adressleiste ein.
3. Klicken Sie auf den Link *Software für Windows herunterladen*. Es startet der Assistent, der Sie durch die Anbindung führt.

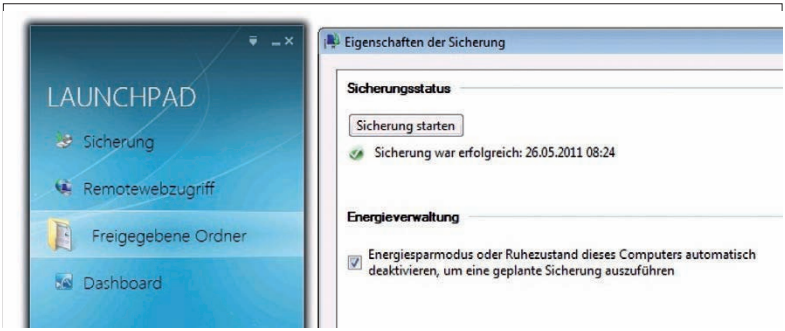
Haben Sie einen Client-Computer mit dem SBS-Netzwerk verbunden, sehen Sie diesen, wenn Sie im Dashboard auf *Computer und Sicherungen* klicken. Hier sind alle Computer des Netzwerks aufgelistet. In diesem Bereich können Sie in der

Spalte *Status* ablesen, ob der Computer eingeschaltet ist und ob Warnungen auf dem Computer gemeldet werden. Über das Kontextmenü oder den Bereich *Aufgaben* sehen Sie die verschiedenen Möglichkeiten zur Verwaltung des Clients.

Übersichtlich: Die Clients können Sie im Dashboard des SBS 2011 Essentials verwalten.

1.4.2 Client-Computer über das Dashboard auf den Server sichern

Sicherungen auf Client-Computern starten und verwalten Sie auf dem Server im Dashboard über *Computer und Sicherung*.



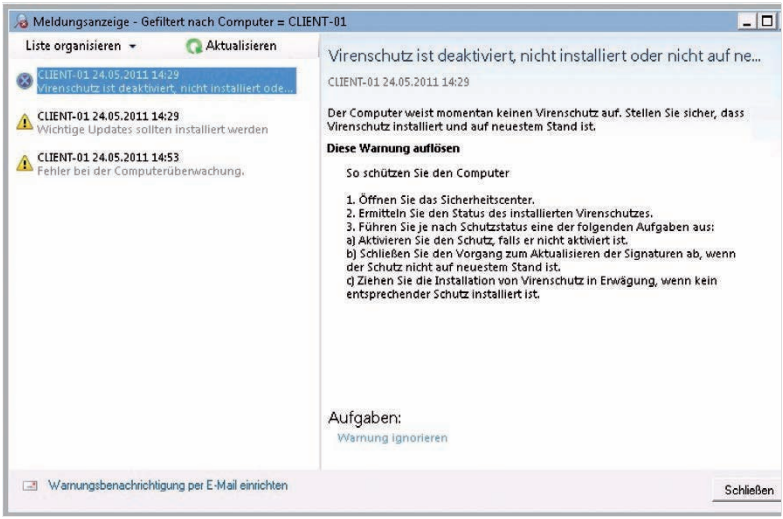
Unter Kontrolle: Sie können die Datensicherung auch auf dem Client überwachen.

Wenn Sie die Sicherung starten, sehen Sie über das Launchpad auf dem Client und der Auswahl von *Sicherung* den Status des Backups. Sie läuft im Hintergrund, sodass der Anwender weiter mit seinem Computer arbeiten kann.

Ist der Vorgang abgeschlossen, erkennen Sie dies an der gleichen Stelle. Über diesen Bereich starten Sie auch eine Sicherung vom Client aus auf den Server. In den Eigenschaften eines Computers sehen Sie auf der Registerkarte Sicherung auf dem Server die verschiedenen vorhandenen Sicherungen des Clients.

1.4.3 Warnungen auf den Clients anzeigen

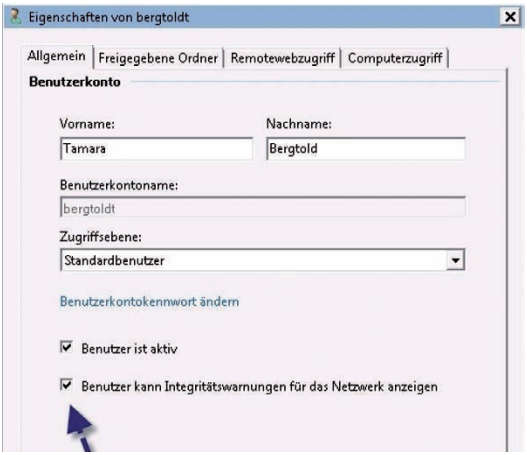
Anwender können sich aktuelle Warnungen des Clients über das Kontextmenü des Connectors oder direkt im Launchpad auf dem Client anzeigen lassen. Als Administrator können Sie im Dashboard über das Kontextmenü von Client-Computern ebenfalls die Warnungen anzeigen. Anschließend verbindet sich das Dashboard mit dem Client und zeigt vorhandene Fehler an. In diesem Fenster sehen Sie, wie Sie das Problem lösen können.



Sicherheitshalber: Die Warnungen der Clients können Sie im Dashboard sehen.

Für den Server existiert gleichfalls eine solche Meldeliste. Diese sehen Sie, wenn Sie auf die Schaltfläche mit den Meldungen klicken. In der Spalte Warnungen wird der aktuellen Status des Computers angezeigt und ob neben *Warnungen* auch Fehler aufgetreten sind. Durch diese Überwachung sehen Sie zum Beispiel, ob auf Client-Computern aktuelle Patches fehlen oder kein Antivirenprogramm installiert ist.

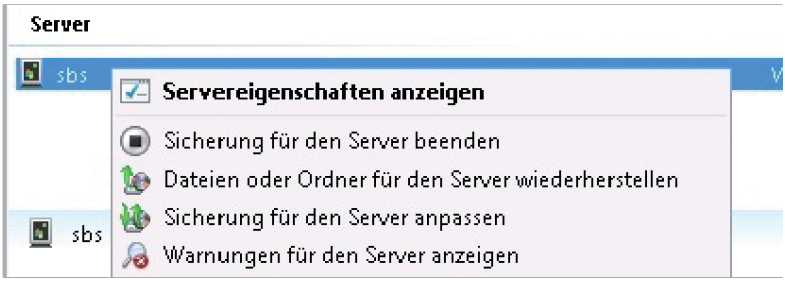
Erlaubnis erteilen: Entsprechend konfiguriert, können Benutzer die Warnungen für das Netzwerk sehen.



Standardmäßig zeigt der Connector jedoch nur Fehler auf dem lokalen Client an. Sie können für einzelne Benutzer aber festlegen, dass diese alle Warnungen im Netzwerk in der Meldungsanzeige sehen, auch die Fehler des Servers und der anderen Clients. Die Anwender benötigen keine Administrationsrechte, um die Fehler anzuzeigen. Damit der Connector auf Client-Computern sämtliche Fehler anzeigt, rufen Sie im Dashboard die Eigenschaften des Benutzerkontos auf. Anschließend aktivieren Sie die Option *Benutzer kann Integritätswarnungen für das Netzwerk anzeigen* auf der Registerkarte *Allgemein* in den Benutzereigenschaften.

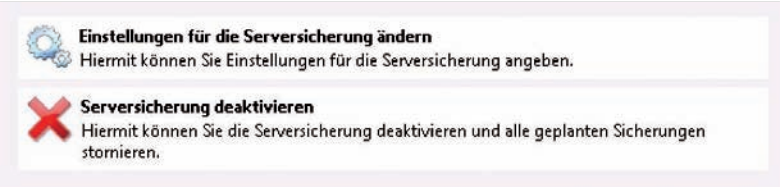
1.4.4 Datensicherung per Assistent

Um die Datensicherung mit dem Assistenten in Small Business Server 2011 Essentials durchzuführen, starten Sie das Dashboard und wechseln zum Menüpunkt *Computer und Sicherung*.



Einfach: Über das Kontextmenü des Servers konfigurieren Sie die Sicherung.

Über das Kontextmenü des Servers konfigurieren Sie die Sicherung. Nach deren erstmaligem Einrichten können Sie diese jederzeit an Ihre Bedürfnisse anpassen.



Flexibel: Sie können die Sicherung entsprechend anpassen.

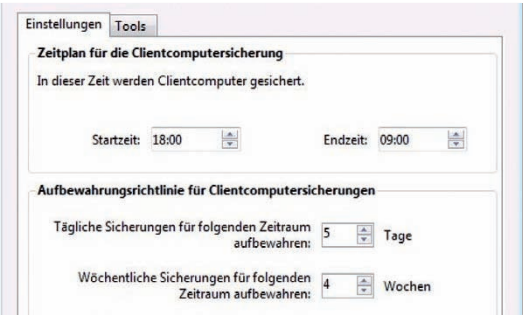
Über das Kontextmenü des Servers im Dashboard lassen sich verschiedene Aufgaben durchführen:

- Sicherung für den Server starten und Sicherung für den Server beenden
- Dateien oder Ordner für den Server wiederherstellen
- Sicherung für den Server anpassen

Nach der Installation des SBS 2011 Essentials müssen Sie die Sicherung zunächst mit *Serversicherung einrichten* auf der Registerkarte *Start* konfigurieren.

1.4.5 Client-Computer sichern und Sicherungen verwalten

Damit die Sicherung auf den Clients funktioniert, muss der Client eingeschaltet und korrekt an den Small Business Server angebunden sein. Bevor Sie Client-Computer sichern, sollten Sie über den Menüpunkt *Weitere Aufgaben* für diese Maßnahme zunächst allgemeine Einstellungen festlegen, die der Server für die Sicherung der Clients berücksichtigen soll. Die Einstellungen gelten nur für die Sicherung der Clients, nicht des Servers. Sie finden den Menüpunkt im rechten unteren Bereich des Dashboards auf der Registerkarte *Computer und Sicherung*.



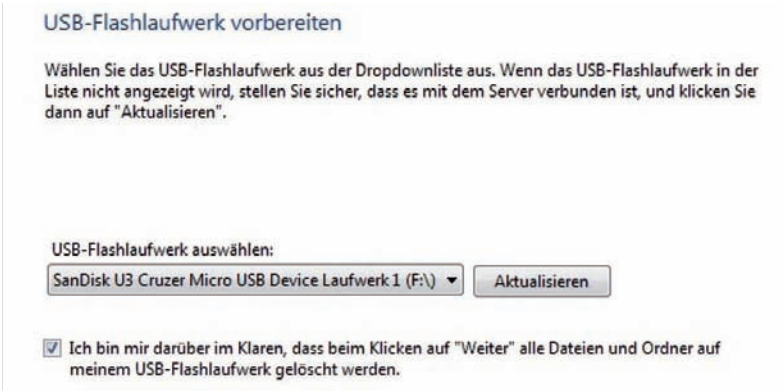
Allgemeine Einstellungen: Hier können Sie beispielsweise Zeitplan und Aufbewahrungsrichtlinien festlegen.

Nach der Auswahl des Menüpunktes öffnet sich ein neues Fenster, in dem Sie verschiedene Einstellungen vornehmen können. Auf der Registerkarte *Einstellungen* legen Sie zunächst fest, wann der Assistent die Client-Computer sichern soll und wie lange die Sicherungen auf dem Server verfügbar sein sollen. Über die Registerkarte *Tools* können Sie defekte Sicherungen reparieren, wenn sich aus diesen keine Daten wiederherstellen lassen. Lässt sich eine Sicherung nicht reparieren und daher auch nicht zur Wiederherstellung nutzen, kann der Assistent sie löschen.

1.4.6 USB-Stick für die Wiederherstellung von Clients erstellen

Über die Schaltfläche *Schlüssel erstellen* können Sie im Dashboard über den Bereich *Computer und Sicherungen* und die Auswahl von *Weitere Aufgaben für die Clientcomputersicherung* einen USB-Stick so konfigurieren, dass Sie Client-Computer über diesen USB-Stick wiederherstellen können – beispielsweise, wenn Windows nicht mehr startet.

Anschließend können Sie den entsprechenden Computer mit dem USB-Stick booten und so wiederherstellen – oder Sie verwenden für Wiederherstellungsvorgänge die Wiederherstellungs-CD, die zum Lieferumfang des Small Business Server 2011 Essentials gehört. Damit Sie den Stick erstellen können, müssen Sie diesen mit dem Server verbinden, nicht mit einem Client-Computer. Der Stick muss eine Mindestgröße von 512 MByte aufweisen. Der Assistent löscht alle Daten auf dem USB-Stick und formatiert ihn neu.



Simpel: Ein USB-Stick zur Wiederherstellung lässt sich recht einfach anfertigen.

Auf der ersten Seite erhalte Sie Informationen zu dem Vorgang. Als Nächstes wählen Sie den USB-Stick aus, den Sie verwenden wollen, und bestätigen die Meldung,

die auf das Löschen der Daten hinweist. Sobald Sie auf *Weiter* klicken, beginnt der Assistent den Stick vorzubereiten. Der Vorgang dauert einige Minuten. Sobald der Vorgang abgeschlossen ist, erhalten Sie eine entsprechende Meldung. Mit dem USB-Stick können Sie jetzt einen Client-Computer booten.

1.4.7 Client-Sicherung konfigurieren und manuelle Sicherungen starten

Manuelle Sicherungen für Client-Computer starten Sie im Dashboard auf dem Small Business Server über das Kontextmenü des Clients im Bereich *Computer und Sicherung*. Wählen Sie den Menüpunkt *Sicherung für den Computer starten* aus. Um die Datensicherung auf den Client-Computern zu konfigurieren, wählen Sie im Kontextmenü die Option *Sicherung für den Computer anpassen* aus. Im ersten Fenster können Sie die Sicherung für den Computer deaktivieren oder ändern, welche Elemente der Server im Rahmen der Sicherung alle mitsichern soll.

Generell ist es empfehlenswert, dass Sie alle Daten auf den Clients sichern. Dadurch ist auch sichergestellt, dass Sie komplette Client-Computer wiederherstellen können. Wenn Sie die Änderungen speichern, zeigt Ihnen der Assistent die Änderung an und wann die nächste Sicherung des Client-Computers stattfindet.

Den Status der letzten Datensicherung sehen Sie in der Spalte *Sicherungstatus des Clients*. Wenn Sie doppelt auf einen Client klicken, öffnen sich dessen Eigenschaften. Auf der Registerkarte *Sicherung* werden Ihnen die jeweiligen Zeitpunkte der Sicherung angezeigt. Ausführlichere Informationen zur Sicherung erhalten Sie über *Details*. Das kann vor allem bei auftretenden Fehlern hilfreich sein. Auf den Clients selbst können Sie sich ebenfalls Daten zu den Datensicherungen anzeigen lassen. Dazu klicken Sie im Launchpad auf den Link Sicherung. Sie sehen im Fenster den Status der letzten Sicherung auf den Server und können ebenfalls eine manuelle Sicherung starten.

1.4.8 Daten auf Client-Computern wiederherstellen

Um Daten auf den Clients wiederherzustellen, müssen Sie sich direkt mit dem entsprechenden Computer verbinden. Starten Sie auf dem Computer über das Launchpad das Dashboard und melden Sie sich als Administrator am Dashboard an. Nach dem Start des Dashboards klicken Sie auf *Computer und Sicherung* und dann mit der rechten Maustaste auf den Computer, für den Sie Dateien wiederherstellen wollen. Anschließend baut der Sicherungsassistent eine Verbindung mit dem Server auf, und Sie können die Datensicherung für den Client auswählen, aus der Sie Dateien wiederherstellen wollen. Nach der Auswahl des Sicherungszeitraums öffnet der Assistent die entsprechende Sicherung, und Sie können auswählen, welche Dateien Sie wiederherstellen wollen.

Haben Sie das Verzeichnis oder die Dateien ausgewählt, legen Sie als Nächstes fest, wo Sie die Dateien wiederherstellen wollen. Der Assistent zeigt dabei die lokalen Laufwerke direkt auf dem Client an, nicht die Laufwerke auf dem Server. Die Wiederherstellung erfolgt also direkt auf dem Client.

Als Nächstes stellt der Assistent die Dateien wieder her. Ist der Vorgang abgeschlossen, können Sie direkt den Speicherort öffnen, weitere Dateien wiederherstellen oder den Vorgang abschließen. Wollen Sie keine Dateien mehr wiederherstellen, schließen Sie das Dashboard auf dem Client-Computer.

1.4.9 Wiederherstellen eines Computers per USB-Stick

Nachdem Sie den Stick wie oben beschrieben erstellt haben, booten Sie den Client-Computer mit dem USB-Stick und wählen aus, ob Sie ein 32-Bit-System oder ein 64-Bit-System wiederherstellen wollen. Anschließend startet die Wiederherstellungsumgebung von Windows 7 über den USB-Stick. Im ersten Schritt initialisiert der Assistent verschiedene Systemkomponenten und ermöglicht die Auswahl der Sprache. Kann der Assistent keine Verbindung mit dem Server herstellen oder sind die lokalen Festplatten nicht verfügbar, können Sie die Treiber für die Geräte über die Schaltfläche *Treiber laden* integrieren. Dazu verbinden Sie den USB-Stick mit einem anderen Computer und kopieren die entsprechenden Treiber auf den Stick. Achten Sie aber darauf, dass Sie die Treiberdateien entpacken müssen, damit die .inf-Dateien der Treiber zur Verfügung stehen. In den meisten Fällen können Sie aber mit Weiter die Wiederherstellung fortführen. Im nächsten Schritt startet der Wiederherstellungsassistent. Zunächst müssen Sie einen Benutzernamen und ein Kennwort eines Administrators eingeben, mit dem Sie sich am Small Business Server anmelden können. Normale Benutzerkonten haben kein Recht, sich am Small Business Server für die Wiederherstellung anzumelden. Nach der erfolgreichen Anmeldung wählen Sie aus, welchen Client Sie wiederherstellen wollen.

Als Nächstes wählen Sie aus, welche Sicherung der Assistent für die Wiederherstellung verwenden soll. Über *Details* können Sie sich ausführlichere Informationen zur Sicherung anzeigen lassen. Sie können entweder den kompletten Computer mit allen Partitionen wiederherstellen lassen oder einzelne Partitionen für die Wiederherstellung auswählen. Der Assistent zeigt noch eine Zusammenfassung an und informiert Sie über die einzelnen Vorgänge der Wiederherstellung. In den nächsten Schritten stellt der Assistent den Computer aus der Datensicherung auf dem Small Business Server wieder her. Der Vorgang kann von wenigen Minuten bis zu mehrere Stunden dauern. Das System zeigt Ihnen zumindest eine Einschätzung der Dauer an. Nachdem der Assistent seine Aufgabe erledigt hat, erhalten Sie eine entsprechende Meldung und können den Client neu starten. Windows und alle Anwendungen sowie sämtliche Dateien zum Zeitpunkt der Sicherung sollten wieder zur Verfügung stehen.

Thomas Joos

1.5 Exchange Server 2010 und Lync Server 2010 gemeinsam betreiben

Wenn Sie im Unternehmen Lync Server 2010 parallel zu Exchange Server 2010 betreiben, können Sie die beiden Server auch miteinander verbinden. Der Vorteil dabei ist, dass Sie die E-Mail-Struktur über Exchange anbinden und Telefonate über Lync abwickeln. Outlook Web App können Sie als Webclient für Lync nutzen. Anwender sehen in Outlook in der Adressleiste, ob der Empfänger der E-Mail gerade in Lync online ist. Exchange kann über Lync Telefonate durchführen und Anrufe in Postfächer umleiten. Wenn Sie die Unified-Messaging-Funktion in Exchange einsetzen, müssen Sie spezielle Wählpläne erstellen, um Exchange mit Lync zu verbinden. Da die Verbreitung von Lync Server 2010 noch recht übersichtlich ist, ist der Erfahrungsschatz des gemeinsamen Betriebs mit Exchange Server 2010 auch noch begrenzt. Daher finden Sie bei Problemen aktuell nur relativ magere Informationen im Internet. Bei Schwierigkeiten mit der Konfiguration hilft dann oft nur der Weg zu Microsoft. Und wenn Sie die Telefoniefunktionen in Exchange und Lync nutzen, können Sie sich auf jede Menge Konfigurationsarbeit einrichten.

1.5.1 Lync Server 2010 mit Exchange Unified Messaging

Beim gemeinsamen Betrieb von Lync Server 2010 mit Exchange Server 2010 sollten Sie die Unified-Messaging-Rolle von Exchange installieren. Das ist allerdings nur dann notwendig, wenn Sie neben Instant Messaging, Audio-, Video- und Webkonferenzen auch die Telefoniefunktionen von Exchange und Lync nutzen wollen. Lync kann im Hinblick auf die Ausfallsicherheit mit mehreren Exchange-Servern eine Verbindung aufbauen. In diesem Fall müssen Sie auf den Exchange-Servern die Unified-Messaging-Serverrolle installieren. Beachten Sie, dass die Unified-Messaging-Rolle in Exchange Server 2010 Virtualisierung nicht unterstützt. Will heißen, diese Server können Sie nicht als Hyper-V oder VMWare-Gast betreiben, sondern Sie müssen physische Server zur Installation verwenden. Die Unified-Messaging-Rolle ist vor allem bei der Zusammenarbeit mit Lync Server 2010 nur dann sinnvoll, wenn Sie ein „echtes“ Zertifikat installieren und nicht das selbst signierte Zertifikat von Exchange verwenden. Optimal ist an dieser Stelle, eine interne Zertifizierungsstelle auf Basis der Active Directory-Zertifikatsdienste zu installieren. Mit dieser arbeiten Exchange und Lync optimal zusammen und können mit internen Assistenten Zertifikate beantragen und installieren.

1.5.2 Vorbereitende Maßnahmen

Wollen Sie den Exchange Server 2010 gleich mit der Unified-Messaging-Rolle installieren, so müssen Sie den Windows Server 2008 R2 vor der Installation von Exchange erst vorbereiten:

1. Für eine typische Installation oder die Installation der Serverrollen Hub Transport oder Mailbox benötigen Sie das Microsoft Filter Pack. Die Installation besteht aus wenigen Klicks und erfordert keinerlei Eingaben. Auch auf Unified-Messaging-Servern können Sie ohne Weiteres diese Erweiterung installieren.
2. Als Nächstes öffnen Sie die Windows PowerShell auf dem Server und geben den Befehl *import-Module ServerManager* ein. Unter Windows Server 2008 R2 ist die PowerShell standardmäßig bereits installiert. Wollen Sie die PowerShell ISE nutzen, müssen Sie diese als Feature nachinstallieren.
3. Möchten Sie zusätzlich zu Client Access, Hub Transport und Mailbox noch Unified Messaging installieren, verwenden Sie den Befehl:

```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,
➥ Web-Basic-Auth,Web-Windows-Auth,Web-Metabase,
➥ Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-Model,
➥ RSAT-Web-Server,Web-ISAPI-Ext,Web-Digest-Auth,
➥ Web-Dyn-Compression,NET-HTTP-Activation,
➥ RPC-Over-HTTP-Proxy,Desktop-Experience -Restart.
```

1.5.3 Erforderliche Erweiterungen installieren

Damit Sie die Unified Messaging-Rolle installieren können, müssen Sie auf dem Server noch folgende Erweiterungen installieren:

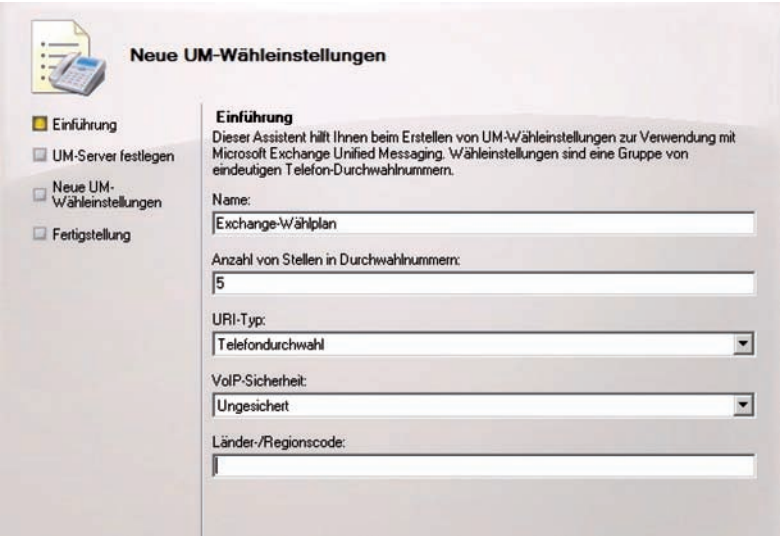
4. Unified Communications Managed API 2.0, Basis-Laufzeitkomponente (64 Bit) (http://go.microsoft.com/fwlink/?LinkID=180957)
5. Microsoft Server Speech Platform Runtime (x64) (http://go.microsoft.com/fwlink/?LinkID=180958)
6. Update zum Entfernen des Anwendungsmanifestablauf-Features von AD-RMS-Clients (http://support.microsoft.com/?kbid=979099)

Praktisch: Das Service Pack 1 kann fehlende Rollen automatisch installieren.

Erhalten Sie während der Installation der Unified-Messaging-Rolle die Fehlermeldung, dass eines oder mehrerer dieser Patches fehlen, laden Sie sich diese herunter und installieren Sie die Erweiterungen der Reihe nach. Klicken Sie anschließend im Exchange-Installationsfenster auf *Wiederholen*, um die Überprüfung erneut zu starten. Nach der Installation dieser Patches ist kein Neustart des Servers erforderlich. Anschließend können Sie die Installation von Exchange Server 2010 direkt über die SP1-Dateien starten. Installieren Sie einen neuen Server direkt mit dem SP1, haben Sie im unteren Bereich noch die Option *Für Exchange Server erforderliche Windows Server-Rollen und -Funktionen automatisch installieren* zur Verfügung. Aktivieren Sie diese Option, installiert der Setup-Assistent automatisch alle fehlenden Rollen nach.

1.5.4 Wählpläne in Exchange anlegen

Bevor Sie einen Unified-Messaging-Server unter Exchange Server 2010 einsetzen können, müssen Sie einen Wählplan erstellen und diesen Wählplan einem Server zuordnen. Das gilt auch dann, wenn Sie Exchange mit Lync verbinden wollen.



Hilfreich: Ein Assistent unterstützt beim Erstellen eines Wählplans.

Ein Wählplan legt fest, welche Durchwahlen die Anwender erhalten, um per Outlook Voice Access auf ihr Postfach zugreifen zu können. Mit UM-Wählplänen verknüpfen Sie die Telefondurchwahlnummer eines Empfängers mit einem UM-aktivierten Postfach. Bei der Erstellung können Sie die Anzahl der Stellen der

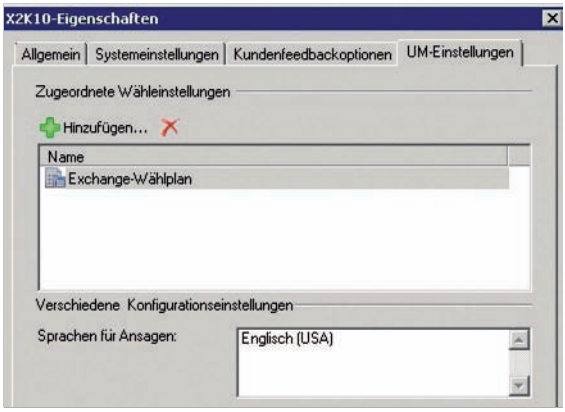
Durchwahlnummer, den URI-Typ (Uniform Resource Identifier) und die VoIP-Sicherheitseinstellung festlegen:

1. Starten Sie die Exchange-Verwaltungskonsole.
2. Klicken Sie auf *Organisationskonfiguration/Unified Messaging*.
3. Klicken Sie im Ergebnisbereich auf die Registerkarte *UM-Wähleinstellungen*.
4. Klicken Sie mit der rechten Maustaste in den Ergebnisbereich und wählen die Option *Neue UM-Wähleinstellungen*. Alternativ können Sie im Aktionsbereich auf diese Option klicken.
5. Im Anschluss startet der Assistent zum Erstellen eines neuen Wählplans.
6. Haben Sie Ihre Eingaben vorgenommen, klicken Sie auf die Schaltfläche *Neu*, um den Wählplan zu erstellen. Seit SP1 können Sie direkt nach der Erstellung den Wählplan einem UM-Server zuordnen.
7. Umfasst die vorhandene Telefonieumgebung Durchwahlnummern, dann müssen Sie eine Anzahl für die Stellen festlegen, die mit der Anzahl der Stellen in diesen Durchwahlen übereinstimmt.
8. Der Wählplan wird im Anschluss in der Exchange-Verwaltungskonsole angezeigt.

1.5.5 Wählplan zuweisen

Bei der Erstellung können Sie zudem verschiedene Einstellungen vornehmen, beispielsweise zur Verschlüsselung.

Zuordnung: Einen UM-Wählplan müssen Sie einem Exchange-UM-Server zuweisen.



Beim Erstellen von Wählplänen senden und empfangen die UM-Server unverschlüsselte Daten. Wählen Sie *SIP-gesichert*, verschlüsselt der Server SIP, aber keine

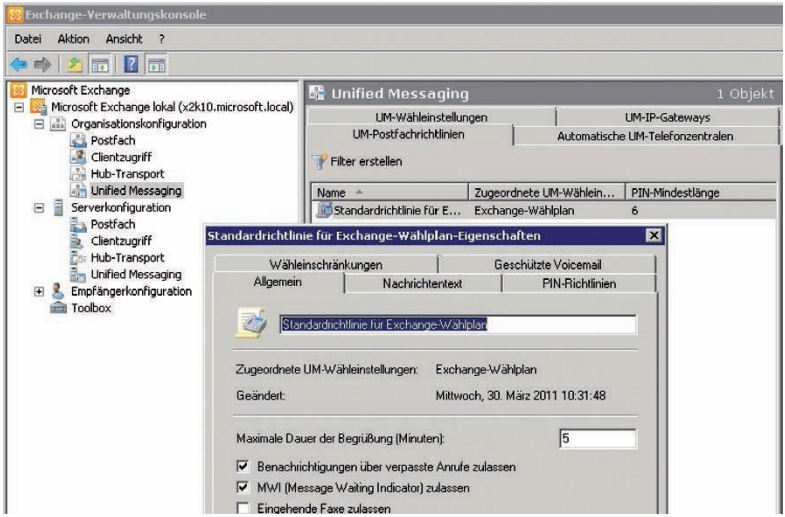
anderen Daten. Dazu verwendet der Server MTLS (Mutual Transport Layer Security). Bei Auswahl von *Gesichert* verschlüsseln die UM-Server SIP-Signale und den restlichen VoIP-Datenverkehr. Ein verschlüsselter Kanal, der SRTP (Secure Realtime Transport Protocol) verwendet, verschlüsselt ebenfalls mit MTLS (Mutual TLS).

Mit `New-UMDialplan -Name <Name>` erstellen Sie in der Exchange-Verwaltungs-Shell einen neuen Wählplan. Diesen müssen Sie anschließend einem UM-Server zuweisen; erst dann kann dieser Anrufe entgegennehmen und steht als Outlook Voice Access (OVA)-Server zur Verfügung. Um einen Wählplan zuzuweisen, gehen Sie folgendermaßen vor:

1. Starten Sie die Exchange-Verwaltungskonsole.
2. Klicken Sie auf *Serverkonfiguration/Unified Messaging*.
3. Rufen Sie im Ergebnisbereich die Eigenschaften des Servers auf.
4. Wechseln Sie auf die Registerkarte *UM-Einstellungen*.
5. Klicken Sie im Bereich *Zugeordnete Wähleinstellungen auf Hinzufügen*.
6. Wählen Sie im neuen Fenster den Wählplan aus, den Sie dem Server zuweisen

1.5.6 Erstellen und Verwalten von UM-Postfachrichtlinien

Mit Postfachrichtlinien können Sie eine gemeinsame Menge von Einstellungen für mehrere Postfächer anwenden.



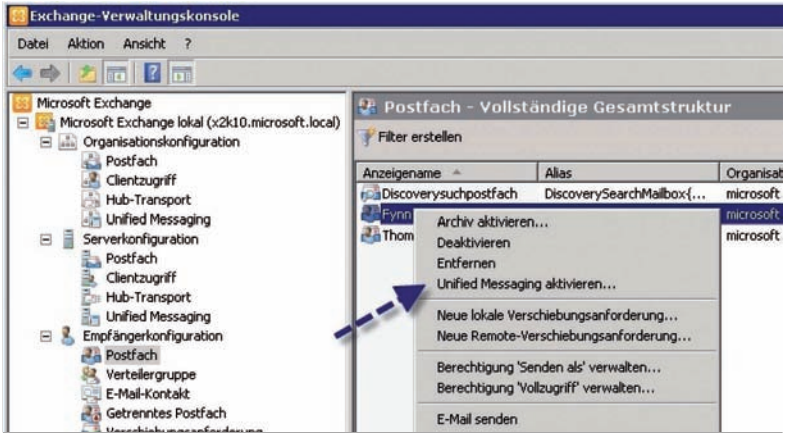
Basisarbeit: Sie können die vorhandene Richtlinie bearbeiten.

Sie müssen eine UM-Postfachrichtlinie erstellen, bevor Sie Benutzer für Unified Messaging aktivieren können. Haben Sie einen UM-Wählplan erstellt, wird auf dessen Basis eine standardmäßige UM-Postfachrichtlinie erstellt. Diese Richtlinie müssen Sie später bei der Aktivierung von Unified Messaging für ein Postfach bei dem entsprechenden Anwender hinterlegen. Sie können weitere UM-Postfachrichtlinien anlegen oder die standardmäßig vorhandene Richtlinie bearbeiten.

Die Erstellung und Verwaltung von UM-Postfachrichtlinien führen Sie am besten in der Exchange-Verwaltungskonsole über *Organisationskonfiguration/Unified Messaging* durch. Auf der Registerkarte *UM-Postfacheinstellungen* sehen Sie die Standardrichtlinie, die Sie bearbeiten können. Sie haben aber auch die Möglichkeit, weitere Richtlinien zu erstellen und den Anwendern zuzuweisen.

1.5.7 Benutzerverwaltung für Unified Messaging

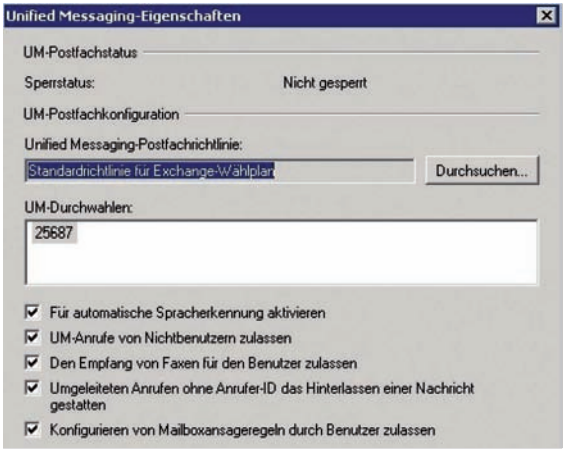
Um Benutzer an Unified Messaging anzubinden und in Lync zu integrieren, müssen Sie diese in Exchange erst für UM aktivieren. Verwenden Sie am besten die Exchange-Verwaltungskonsole. Navigieren Sie zum Menü *Empfängerkonfiguration*. Hier können Sie die Unified-Messaging-Funktion für Postfächer aktivieren, deaktivieren, PINs zurücksetzen und UM-Eigenschaften verwalten.s



Voraussetzung: Das Postfach muss noch für Unified Messaging aktiviert werden.

Um ein Postfach für Unified Messaging zu aktivieren, klicken Sie es mit der rechten Maustaste an und wählen *Unified Messaging aktivieren*. Haben Sie den Menüpunkt ausgewählt, startet der Assistent für die Benutzeraktivierung. Sie müssen zunächst eine UM-Postfachrichtlinie auswählen. In diesem Assistenten legen Sie auch die Durchwahl sowie die Zugriffs-PIN des Anwenders fest. Beide Informati-

onen können auch automatisch erstellt und müssen nicht manuell eingetragen werden. Haben Sie die Daten eingegeben, können Sie das Postfach über die Schaltfläche *Aktivieren* für Unified Messaging aktivieren. Beachten Sie, dass der Unified-Messaging-Zugriff eine Funktion der Premium-Version ist. Sie benötigen daher keine herkömmlichen Exchange-Server-CALs, sondern Exchange-Enterprise-Client-Zugriffslizenzen für Unified-Messaging-aktivierte Postfächer. Wenn Sie einen Benutzer für Unified Messaging aktivieren, erhält dieser eine E-Mail mit den wichtigsten Informationen automatisch zugestellt. Haben Sie ein Postfach für Unified Messaging aktiviert, können Sie dieses in der Exchange-Verwaltungskonsole wieder für Unified Messaging deaktivieren, indem Sie den entsprechenden Menüpunkt aus dem Kontextmenü oder dem Aktionsbereich auswählen.



Detailarbeit: Über die Unified-Messaging-Eigenschaften können Sie die Einstellungen für ein Postfach vornehmen.

Über diese Einstellung können Sie auch die PIN für den Zugriff anpassen. Wenn Sie in der Exchange-Verwaltungskonsole die Eigenschaften eines Postfachs aufrufen, können Sie auf der Registerkarte *Postfachfunktion* die Einstellungen für das Postfach ändern. Markieren Sie die Option *Unified Messagung* und klicken auf Eigenschaften. Es öffnet sich ein neues Fenster, in dem Sie die Unified-Messaging-Einstellungen spezifizieren können.

In der Exchange-Verwaltungs-Shell können Sie sich die UM-Eigenschaften Ihrer Benutzer über den Befehl

```
Get-UMMailbox -identity <E-Mail-Adresse> | fl
```

anzeigen lassen, mit

```
Set-UMMailbox
```

können Sie die Werte setzen.

1.5.8 Exchange und Lync per Skript verbinden

Nach der Einrichtung der UM-Funktionen in Exchange und Lync sowie der UM-Aktivierung der Benutzer in Exchange können Sie Exchange über das Skript *EXCHUCUTIL.PS1* an Lync anbinden und umgekehrt. Das Skript erteilt Berechtigungen an Lync, damit die Lync-Server die Benutzer verwalten können. Außerdem legt das Skript den Lync-Server als Gateway fest. Ausgehende Anrufe in Exchange laufen dann künftig über Lync. Sie finden das Skript auf den Exchange-Servern im Verzeichnis *C:\Program Files\Microsoft\Exchange Server\v14\Scripts*. Zur Ausführung wechseln Sie in dieses Verzeichnis. Geben Sie dann den Befehls

```
\ExchUCUtil.ps1
```

ein. Anschließend erstellt Exchange die entsprechenden Berechtigungen und Einträge. Den Lync-Server findet Exchange über die Einträge in Active Directory. Das heißt, Sie müssen vor der Integration von Exchange in Lync den Befehl erst ausführen. Wenn Sie in der Exchange-Verwaltungskonsole *Organisationskonfiguration\Unified Messaging* aufrufen, sehen Sie auf der Registerkarte *UM-IP-Gateways*, dass Exchange über das Skript den Lync-Server als Gateway eingetragen hat.

Lync mit Exchange verbinden – Exchange UM Integration Utility

Nach der Verbindung müssen Sie im *Microsoft Lync Server 2010 Control Panel* über *Voice Routing* einen neuen Wählplan (Scope User) zu Exchange Server 2010 einrichten. Achten Sie darauf, dass Sie den Namen als FQDN des Exchange-Wählplans anlegen.

Als Nächstes starten Sie auf dem Lync-Server das Exchange UM Integration Utility über *C:\Program Files\Common Files\Microsoft Lync Server 2010\Support\ocsumutil.exe*. Klicken Sie auf *Load Data* und wählen Ihre Domäne aus. Im Fenster müssen Sie jetzt den Exchange-Wählplan sehen. Über *Add* legen Sie neue Kontakte an.

1.5.9 Weiterführende Informationen

Die Anbindung von Exchange an Lync kann sich komplex gestalten. Sie finden im Internet verschiedene Quellen, die zum Thema hilfreiche Informationen bereithalten. Wir haben für Sie einige interessante Links zusammengestellt:

- http://blog.schertz.name/2010/11/lync-and-exchange-um-integration
- http://technet.microsoft.com/de-de/library/gg398193.aspx
- http://technet.microsoft.com/en-us/library/dd627240(office.12).aspx
- www.msxfaq.de/lync/lyncum.htm
- www.expta.com/2010/09/how-to-integrate-lync-server-2010-with.html
- http://social.technet.microsoft.com/Forums/de/ocsde

Thomas Joos

1.6 Workshop ntdsutil: Handwerkszeug fürs Active Directory

Die Microsoft-Ingenieure haben mit Windows Server 2008 und noch einmal mit dem Nachfolger-Update Windows Server 2008 R2 eine ganze Reihe von neuen Features, Erweiterungen und Verbesserungen rund um den Verzeichnisdienst Active Directory (AD) zur Verfügung gestellt (siehe auch Active Directory mit Windows Server 2008 R2).

Doch neben den oft beschriebenen neuen Fähigkeiten, wie etwa dem Einsatz eines Read-Only-Domänen-Controllers (RODC) sind es im täglichen Betrieb doch eher die erweiterten Fähigkeiten der kleinen Werkzeuge, die einen Systemverwalter interessieren und ihm helfen, seine Arbeit leichter zu bewältigen.

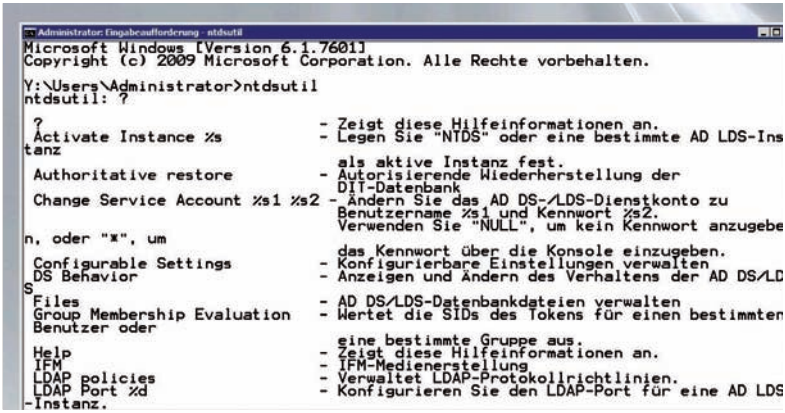
1.6.1 ntdsutil – mächtiges Befehlszeilenprogramm für den Profi

Mit dem Kommandozeilenwerkzeug ntdsutil steht ein mächtiges Programm zur Verfügung, mit dessen Hilfe viele Aspekte des Verzeichnisdienstes AD direkt verwaltet und betreut werden können. Es kann sowohl zu reinen Verwaltung der Active-Directory-Datenbank eingesetzt werden als auch zum Verwalten und Steuern von Einzelmaster-Betriebsfunktionen sowie zum Löschen von Metadaten auf Domänencontrollern, die ohne ordnungsgemäße Deinstallation aus dem Netzwerk entfernt wurden. Auch das Erstellen von Anwendungsverzeichnispartitionen ist mit diesem Programm möglich. Allerdings weist Microsoft auf den entsprechenden Seiten im Technet (http://technet.microsoft.com/de-de/) auch deutlich darauf hin, dass es sich hier um Werkzeug handelt, das nur von erfahrenen Administratoren angewendet werden sollte. Die Erweiterungen, die Microsoft diesem Programm mit Windows Server 2008 spendiert hat, können deshalb gerade dem IT-Profi wertvolle Hilfestellung bieten.

Dazu gehören insgesamt sechs Verbesserungen beziehungsweise Funktionalitäten: Snapshots einschließlich Activate Instance, die Installation von einem Medium (IFM – Installation from Media), das sogenannte DS Behavior (Verzeichnisdienstverhalten), lokale Rollen und das Partition-Management. Wir stellen diese Neuerung einzeln vor und zeigen auch, wie sie eingesetzt werden können.

1.6.2 Snapshot: auf dem Weg zur Wiederherstellung

Ganz neu ist in dieser Version die Snapshot-Funktionalität, die auch als „Active Directory Database Mounting Tool“ bezeichnet wird. Sie erlaubt es einem Administrator, zu einem bestimmten Zeitpunkt einen Snapshot der AD-Datenbank mit all ihren Objekten und Attributen zu erstellen.



Der erste Schritt zum Snapshot mittels ntdsutil: Durch diesen Aufruf wird zunächst die Instanz des Verzeichnisses angegeben, von dem dann daran anschließend der Schnappschuss erstellt werden soll.

Das Erstellen eines solchen Snapshots geht dabei ganz einfach von der Hand: Der Administrator muss nur ein Kommandozeilenfenster auf einem Domänen-Controller (DC) öffnen, wozu er auf diesem DC natürlich administrative Rechte benötigt. Danach ist ntdsutil zu starten, das dann als eigene Kommando-Shell arbeitet. Am ntdsutil-Prompt ist dann der folgende Befehl einzugeben:

```
activate instance ntds
```

Ein Snapshot wird auf dem Domänen-Controller erstellt: Solche Schnappschüsse können dann im direkten Zusammenhang mit der Wiederherstellung von gelöschten AD-Objekten verwendet werden.

Durch diesen Aufruf wird zunächst die Instanz des Verzeichnisses angegeben, von dem anschließend der Schnappschuss erstellt werden soll. Das Programm meldet dann auch, welche aktive Instanz festgelegt wurde. Nun folgt noch der Befehl

```
create
```

Danach wird ein entsprechender Snapshot auf dem Domänen-Controller erstellt. Solche Schnappschüsse können beispielsweise im direkten Zusammenhang mit

der Wiederherstellung von gelöschten AD-Objekten, die noch nicht aus der Datenbank des Verzeichnisdienstes entfernt wurden (sogenannte Tombstone-Objekte), verwendet werden.

1.6.3 Objekte wiederherstellen

Microsoft hat mit Windows Server 2003 die Möglichkeit der Reanimation von Tombstone-Objekten eingeführt, um so gelöschte Objekte aus dem AD-Container „DeletedObjects" an ihren ursprünglichen Platz zurückzuführen. Doch leider werden beim Löschen die meisten Attribut-Werte eines gelöschten Objekts ebenfalls ins Nirwana geschickt, weshalb die Wiederherstellung der Tombstones allein in den meisten Fällen nicht hilft.

Damit ein Objekt aus dem Active Directory wieder sinnvoll zum Einsatz kommen kann, müssen zunächst auch die Attribute wieder so hergestellt sind, wie sie vor dem Löschen vorlagen. Lesen Sie dazu auch unseren Workshop: Objekte aus dem Active Directory wiederherstellen (Webcode **2032334**). Da aber ein mit ntdsutil erstellter Snapshot alle Objekte und Attribute des Verzeichnisdienstes zu diesem Zeitpunkt enthält, bietet er dem Administrator eine Reihe von Möglichkeiten: Besitzt er einen Snapshot des Verzeichnisses, bevor das entsprechende Objekt gelöscht wurde, so kann er dessen Attribute komplett auslesen und auch extrahieren. Diese kann er dann wiederum dem wiederhergestellten Objekt zuweisen, womit das gewünschte Ergebnis erreicht wurde. Wichtig in diesem Zusammenhang: Der Administrator muss Mitglied der Gruppe der Enterprise- oder Domänenadministratoren sein, wenn er diese Arbeiten mithilfe eines Snapshots durchführen will.

1.6.4 IFM – von einem Medium installieren

Jeder Administrator, zu dessen Aufgabenfeld Verwaltung und Betreuung einer AD-Domäne gehören, kennt das Tool „dcpromo.exe", mit dessen Hilfe beispielsweise ein Domänen-Controller installiert werden kann. Microsoft bezeichnet es deshalb auch als „Assistent zum Installieren von Active-Directory-Domänendiensten". Die nun neu zur Verfügung stehende Funktionalität IFM (Install From Media) ist eine erweiterte Option dieses Assistenten. Wer jetzt auf seinem Windows Server 2008 nachschaut, wird allerdings interessanterweise feststellen können, dass der Begriff IFM weder bei der deutschen noch der englischen Version des Windows Servers innerhalb des Assistenten zu finden ist.

Trotzdem erlaubt die IFM-Funktionalität dem Systemverwalter, einen neuen Domänen-Controller unter Einsatz einer Sicherung des Systemzustands in eine Domäne einzuführen. Das Besondere daran: Die notwendigen Verzeichnispartitionen werden dabei aus dem Backup und nicht über das Netzwerk in die Datenbank des DC geladen – vor allem bei größeren Active-Directory-Datenbanken kann diese Option viel Zeit einsparen. Microsoft stellt in einem TechNet-Artikel mit dem

Titel „How to use the Install from Media feature to promote Windows 2003-based domain controllers“ (http://support.microsoft.com/kb/311078) detaillierte Informationen dazu bereit, wie ein Administrator mithilfe von IFM einen Domänen-Controller erstellen kann. Wie dem Titel zu entnehmen ist, stand die IFM-Funktionalität bereits auf Windows Server 2003 zur Verfügung, war damals aber noch nicht in ntdsutil integriert. Diese Funktionalität kam erst mit Windows Server 2008 ins Spiel, um NTBackup zu ersetzen, das ja schon seit NT 3.5 zusammen mit den Windows Servern ausgeliefert wurde.

Das bei den neuen Windows-Systemen vorhandene Windows Server Backup arbeitet nämlich anders beziehungsweise bietet andere Funktionalitäten als NTBackup: Systemverwalter, die eine festplattenbasierte Sicherung des Systemzustands ihrer Domänen-Controller bisher unter Zuhilfenahme von NTBackup ausgeführt haben, werden beispielsweise feststellen, dass dieses neue Tool viel länger braucht und zudem mehr Platz belegt. Das liegt unter anderem daran, dass ein Backup des Systemstatus unter Windows Server 2008 auch die Systemdateien beinhaltet, die unter der Windows File Protection (WFP) liegen. Diese werden dabei zusätzlich zur AD-Datenbank und zum SYSVOL-Datenträger abgespeichert.

1.6.5 IFM – die Optionen

Zusätzlich zu den anderen Funktionalitäten des Windows-Server-Backups sind es laut Microsoft auch die durch die Einführung der Read-Only-Domänen-Controller entstandenen Anforderungen, die eine Einführung dieser Option notwendig machten. Dabei soll IFM nur „so viel Sicherung“ durchführen, dass gerade genug Teile eines Domänen-Controller gesichert werden (nur die Datenbank und zwei Zweige der Registry), damit ein Windows Server 2008 DC von diesem Medium aus und nicht über das Netzwerk promotet werden kann.

Auf diese Weise ist die Arbeit mit IFM einfacher und schneller erledigt als unter Windows Server 2003: Schließlich muss der Systemverwalter nun nicht mehr zunächst eine Sicherung ausführen, um anschließend eine Wiederherstellung aus dieser Sicherung heraus zu starten, damit er die notwendigen Dateien bekommt.

Die Installation von einem Medium (IFM) stellt vier Optionen bereit:

- eine vollständige Sicherung (Create full backup name),
- eine vollständige Sicherung des SYSVOL (Create SYSVOL full backup name),
- die entsprechenden Aktionen für RODCs (Create RODC backup name) und
- Create SYSVOL RODC backup name.

Wer einen der beiden „full“-Befehle verwendet, kann mit ihrer Hilfe installierbare Medien erstellen, um einen vollständigen DC zu erzeugen. Die Optionen, die sich auf die Read-Only-Domänen-Controller beziehen, unterscheiden sich von den beiden ersten Optionen dadurch, dass sie andere Sicherheitsvorgaben beinhalten. So wird etwa die Active-Directory-Datenbank für einen RODC direkt beim Erstel-

len als Read-Only markiert. Gleichzeitig werden automatisch die Kennwortattribute entfernt. Fiele nämlich ein IFM-Mediensatz in die falschen Hände, bestünde ein Risiko, das dem Verlust oder Diebstahl eines kompletter DCs entspricht!

1.6.6 Eine IFM-Sicherung erstellen

Die RODC-Optionen garantieren hingegen, dass der entsprechende Mediensatz die gleiche Sicherheit besitzt wie ein Read-Only-Domämen-Controller. Entscheidet sich der Anwender für eine der Varianten mit SYSVOL, kommen auch die entsprechenden Inhalte dieses Verzeichnisses mit in den Datensatz auf das Medium.

Install from Media (IFM im Einsatz): Dieses Beispiel erzeugt eine komplette IFM-Sicherung (ohne SYSVOL) und legt diese dann im Verzeichnis „test" ab.

Auf diese Weise wird natürlich auf der einen Seite die Datenmenge größer, die auf den künftigen Domänen-Controller geschoben werden muss. Auf der anderen Seite wird die Menge des Replikationsverkehrs geringer, denn SYSVOL muss bei dieser Vorgehensweise anschließend nicht mehr über das Netzwerk repliziert werden. Wer Erfahrung mit dem Einsatz von Scripten hat, wird IFM gut in seine Werkzeugkiste einreihen können. So lassen sich die entsprechenden ntdsutil-Kommandos entweder nacheinander über die Kommandozeile oder über ein Script auf den Server bringen. Das folgende Beispiel erzeugt eine komplette IFM-Sicherung (ohne SYSVOL) und legt diese dann im Verzeichnis „test" ab:

```
ntdsutil „active instance ntds" ifm „create full test" quit
quit
```

Ein Beispiel für die Ausgabe zu diesem Befehl auf einem Windows Server 2008 R2 (mit SP1) ist im obigen Bild zu sehen. Hier wurde „test" als Name für das entspre-

chende Verzeichnis gewählt. In einem Script können hier beispielsweise durch Einsetzen des aktuellen Datums mittels einer Variablen die benötigten Verzeichnisse erzeugt werden.

1.6.7 Eine zusätzliche Schicht Sicherheit – DS Behavior

Auch die Sicherheit bei Windows Server2008 lässt sich mit ntdsutil besser kontrollieren. Hierzu wird am Prompt des Programms

```
DS Behavior
```

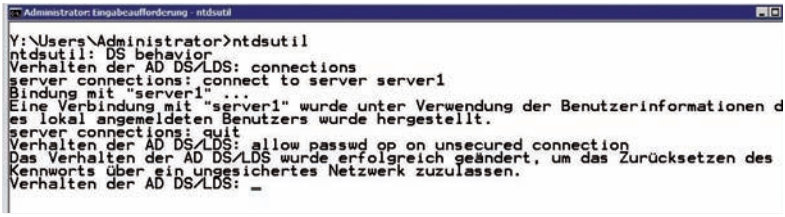
eingegeben, wodurch die Shell in eine weitere Unterebene verzweigt, in der das Verhalten der DS/LDS-Verbindungen (Directory Services/ Lightweight Directory Services) beeinflusst werden kann. Standardmäßig erlauben die Verzeichnisdienste ab Windows Server 2008 keine Operationen an Kennwörtern, wenn diese über eine ungesicherte Verbindung ausgeführt werden.

Will der Administrator dieses Verhalten ändern, so muss er unter ntdsutil zunächst eine Verbindung zum entsprechenden DC aufbauen; dies erfolgt, wenn er

```
connections
```

eingibt. In dieser weiteren Unter-Shell muss er dann angeben, auf welchem Server sich dieser Domänen-Controller befindet. Die Syntax hierzu lautet:

```
connect to server <Server-Name>
```



Ein Eingriff im Bereich der Sicherheit: Mit der Option „DS Behavior" kann das Zurücksetzen des Kennwortes über ein ungesichertes Netzwerk erlaubt werden.

Danach muss zunächst – das ist erfahrungsgemäß ein Punkt, der unerfahrenen Administratoren Schwierigkeiten bereitet – wieder in die darüberliegende Ebene der Shell verzweigt werden, was durch die Eingabe von

```
quit
```

möglich ist. Zuvor hat die Shell hoffentlich die Verbindung zu dem Server mit den richtigen Benutzerinformationen aufgebaut. Nun kann der eigentliche Befehl ein-

gegeben werden, der es erlaubt, das Passwort über ein ungesichertes Netzwerk zurückzusetzen:

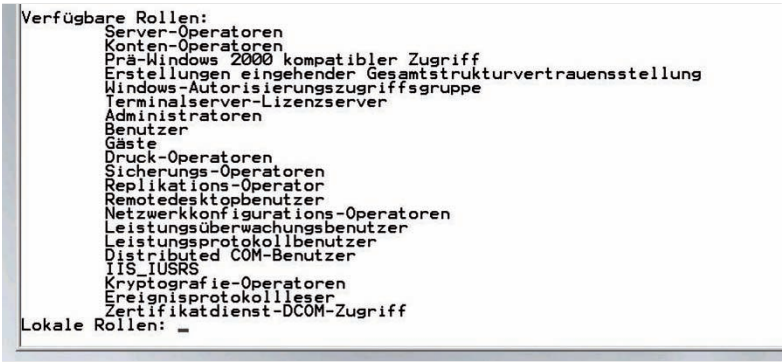
```
allow passwd op on unsecured connection
```

Damit wird diese Einschränkung ausgeschaltet. An dieser Stelle sollten Administratoren große Vorsicht walten lassen: Auch wenn diese Möglichkeit nun offensteht, sollte grundsätzlich immer die sicherere Variante zum Einsatz kommen und nur in Ausnahmefällen auf die hier gezeigte Version zurückgegriffen werden, die danach dann sofort mit dem folgenden Befehl wieder ausgeschaltet werden kann:

```
deny passwd op on unsecured connection
```

1.6.8 Speziell für den RODC: die lokalen Rollen

Mithilfe der lokalen Rollen (Local Roles) können Gruppenmitgliedschaften lokal auf einem Read-Only-Domänen-Controller (RODC) definiert werden.



Die „Local Roles"-Option: Mit ihrer Hilfe können auf einem Read-Only-Domänen-Controller lokale Rollen definiert und zugewiesen werden.

Auf diese Weise können die IT-Verantwortlichen dann auch dort eine echte Verteilung von Verwaltungsaufgaben und Zuständigkeiten erreichen. Ein Administrator kann so bestimmten Benutzern auf einem RODC höhere und/oder spezielle Rechte einräumen. Diese können dann auf dem lokalen RODC entsprechende Aufgaben ausführen, besitzen aber in übrigen Bereichen der Domäne keine höhere Rechte. Soll etwa HugoOfficeAdmin in die Gruppe der lokalen Administratoren auf einem RODC aufgenommen werden, muss der Administrator auf der Befehlszeile auf dem betreffenden Server das Kommando ntdsutil starten und danach

```
local roles
```

eingeben. Aus dem Menü zu den local roles folgt dann der Befehl

```
add HugoBranchOfficeAdmin Administrators
```

Damit wurde dem Nutzer „Hugo“ die Rolle des lokalen Administrators zugewiesen.

1.6.9 Partitionsmanagement – auch für Anwendungspartition

Das Partitionsmanagement stellt unter anderem Funktionen bereit, mit denen sich die Verzögerung bei Replikationsbenachrichtigungen („set replication notification delay“) für die Anwendungspartition in einer AD-Domäne oder Gesamtstruktur (Forest) bearbeiten lässt.

Eine weitere Funktion von ntdsutil: Mittels Partitionsmanagement können auch die sogenannten Anwendungsverzeichnispartitionen bearbeitet und verwaltet werden.

Diese Verzögerung kann dabei sowohl nur aufgelistet als auch erzeugt, gelöscht und entsprechend gesetzt werden. Die Applikationspartitionen werden auch als NDNCs („Non-Domain Naming Contexts“) bezeichnet. Weiterhin ist es mithilfe dieser Option möglich, sich diejenigen Domänen-Controller anzeigen zu lassen, die Replikate sind und eine solche Anwendungsverzeichnispartition unterstützen.

Zudem kann ein Administrator das Partitionsmanagement auch zum Verwalten von Partitionen im AD LDS (Active Directory Lightweight Directory Services) nutzen. Dazu ist es allerdings auch bei dieser Option nötig, zunächst über das Untermenü „connections“ die Verbindung zum entsprechenden Server herzustellen.

Frank-Michael Schlede

1.7 Workshop – Kontingentverwaltung mit Windows Server 2008 R2

Windows Server 2008 R2 bietet, wie das bereits bei den Vorgängerversionen Windows Server 2003 R3 und 2008 der Fall war, die Funktion der Kontingentverwaltung. Mit dem integrierten Ressourcenmanager für Dateiserver FSRM (Fileserver Ressource Manager) lässt sich festlegen, wer was auf Dateiebene darf. So können Sie Anwender mit dem Tool daran hindern, beispielsweise unerwünschte MP3-Dateien oder Bilder auf den Servern abzulegen.

Mit dem FSRM erstellen Sie zusätzlich detaillierte Berichte und auch Vorlagen für Quotas, die Sie mit wenigen Klicks Verzeichnissen auf den Servern zuweisen. Starten können Sie den Ressourcenmanager für Dateiserver über die Programmgruppe *Verwaltung* oder indem Sie *fsrm.msc* im Suchfeld des Startmenüs eingeben. Standardmäßig ist der Rollendienst *Ressourcen-Manager für Dateiserver* in der Rolle Dateiserver nicht installiert. Wollen Sie diesen nutzen, müssen Sie ihn erst über den Servermanager installieren.

Nachdem Sie das Programm gestartet haben, können Sie mit dem Befehl *Optionen konfigurieren* im Kontextmenü des Eintrags *Ressourcen-Manager für Dateiserver* detaillierte Benachrichtigungen und Berichte erstellen lassen und Grundeinstellungen vornehmen. Vor allem die E-Mail-Adressen der Administratoren sollten Sie konfigurieren, damit die später konfigurierten Berichte und Warnungen an die richtige E-Mail-Adresse gehen. Wenn Sie die Administratoren eingetragen haben, sollten Sie zunächst mit der Schaltfläche Test-E-Mail senden überprüfen, ob die E-Mail beim gewünschten Empfänger ankommt.

Wenn ein Benutzer mehrmals versucht, eine blockierte Datei oder eine Datei, die die Kontingentgrenze überschreitet, zu speichern, und wenn für dieses Dateiprüfungs- beziehungsweise dieses Kontingentereignis eine E-Mail-Benachrichtigung konfiguriert ist, sendet der Server für einen Zeitraum von 60 Minuten nur eine einzige E-Mail an den Administrator. Auf diese Weise wird verhindert, dass das E-Mail-Konto des Administrators mit Nachrichten überschwemmt wird.

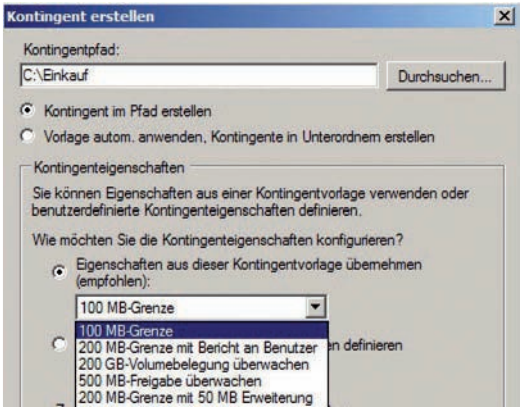
1.7.1 Kontingentverwaltung mit dem FSRM

Mit einem Kontingent lässt sich beispielsweise festlegen, dass ein Benutzer nur maximal 100 MByte auf seinem Home-Laufwerk speichern kann. Sie können mithilfe des FSRMs eine automatische E-Mail an Administratoren und den Benutzer senden, damit dieser rechtzeitig Daten auf seinem Laufwerk löschen kann.

Sie können auch Benachrichtigungen konfigurieren, ohne dass ein Kontingent gesetzt ist. Wenn Sie den Konsoleneintrag Kontingentverwaltung erweitern, stehen Ihnen die Konfiguration von Kontingenten und von Kontingentvorlagen zur Verfügung. An dieser Stelle können Sie für einzelne Freigaben oder ganze Datenträger

Speichergrenzen festlegen, die von den Anwendern nicht überschritten werden dürfen. Rufen Sie den Ressourcen-Manager auf, sehen Sie, dass der Server bereits Kontingente erstellt hat. Beispielsweise haben Sie die Möglichkeit, eine Grenze von 200 MByte für den persönlichen Ordner eines Benutzers auf einem Server festzulegen und zu bestimmen, dass Sie und der Benutzer eine E-Mail erhalten, wenn 180 MByte Speicherplatz überschritten sind.

Grenzen: Beim Verwalten der Kontingente gibt es mannigfaltige Optionen.



Für den gemeinsam verwendeten Ordner einer Gruppe kann wiederum ein flexibles Kontingent von 500 MByte festgelegt werden. Ist diese Speicherbeschränkung erreicht, benachrichtigt der Server alle Benutzer in der Gruppe per E-Mail.

Sie können festlegen, dass Sie eine Benachrichtigung erhalten, wenn die Auslastung eines Ordners 2 GByte erreicht, ohne jedoch das Kontingent dieses Ordners zu beschränken. Kontingente lassen sich aus einer Vorlage für mehrere Ordner oder individuell für einzelne Ordner erstellen. Wenn Sie Kontingente aus Vorlagen erstellen, ist es möglich, diese zentral zu verwalten, indem Sie statt der einzelnen Kontingente für verschiedene Ordner die Vorlagen konfigurieren. Sie können Änderungen damit auf alle Kontingente anwenden, die die entsprechende Vorlage verwenden. Um ein neues zu erstellen, klicken Sie im Knoten *Kontingentverwaltung* mit der rechten Maustaste auf den Eintrag *Kontingente* und wählen im Kontextmenü den Befehl Kontingent erstellen aus.

1.7.2 Kontingente bearbeiten

Bestehende Kontingente bearbeiten Sie per Doppelklick auf das entsprechende Kontingent: Wählen Sie bei *Kontingentpfad* den Pfad zu dem Ordner aus, für den das Kontingent gelten soll. Die Erstellung von Kontingentvorlagen läuft genauso ab wie die Erstellung eines Kontingents. Kontingentvorlagen können Sie als Vorla-

gen für verschiedene Kontingente verwenden. Um ein Kontingent basierend auf einer Vorlage zu erstellen, wählen Sie unter *Kontingentvorlagen* die Vorlage aus, auf der das neue Kontingent basieren soll. Klicken Sie dann mit der rechten Maustaste auf die Vorlage und wählen Sie im Kontextmenü den Befehl *Kontingent mithilfe einer Vorlage erstellen*.

Um eine Kontingentvorlage als Basis für das Kontingent zu verwenden, wählen Sie im Dialogfeld *Kontingent erstellen* die Option *Eigenschaften aus dieser Kontingentvorlage übernehmen* und dann über das zugehörige Listenfeld die Vorlage aus. Alle Vorlageneigenschaften werden unter Zusammenfassung der Kontingenteigenschaften angezeigt. Klicken Sie anschließend auf *Erstellen*. Nach der Erstellung wird das Kontingent im FSRM angezeigt, wenn Sie auf der linken Seite auf den Eintrag *Kontingente* klicken. Erstellen Sie ein neues Kontingent, können Sie bei der Erstellung die Option *Vorlage automatisch anwenden, Kontingente in Unterordnern erstellen* aktivieren. Sobald in dem konfigurierten Ordner ein neuer Unterordner erstellt wird, zum Beispiel wenn Sie mit servergespeicherten Profilen arbeiten, wird dieses Kontingent diesem Unterordner automatisch zugewiesen.

Durch Klicken auf die Schaltfläche *Hinzufügen* können einer Vorlage verschiedene Schwellenwerte und damit verbundene Aktionen zugewiesen werden, etwa die Ereignisprotokollierung oder das Senden von E-Mails. An dieser Stelle haben Sie die Möglichkeit, den Text der E-Mails zu konfigurieren, die vorhandenen Vorlagen zu bearbeiten oder neue Vorlagen zu erstellen.

1.7.3 Harte und weiche Grenzen definieren

Beim Erstellen von Kontingentvorlagen können Sie harte oder weiche Grenzen festlegen. Bei harten Grenzen hebt der Server beim Überschreiten der Grenze die Schreibrechte des Anwenders auf, sodass er keine weiteren Dateien mehr in diesem Verzeichnis speichern kann. Bei einer weichen Grenze ist das Speichern weiterhin möglich, der Ressourcenmanager benachrichtigt aber die Anwender und Administratoren per E-Mail. Benachrichtigungsschwellenwerte bestimmen, was passiert, wenn die Kontingentgrenze erreicht ist. Sie können E-Mail-Benachrichtigungen senden, ein Ereignis protokollieren, einen Befehl oder ein Skript ausführen oder Berichte generieren. Standardmäßig sendet FSRM keine Benachrichtigungen.

Um Benachrichtigungen zu konfigurieren, markieren Sie in der Liste *Benachrichtigungsschwellenwerte* den Schwellenwert und klicken auf *Bearbeiten*. Um E-Mail-Benachrichtigungen zu konfigurieren, legen Sie auf der Registerkarte *E-Mail-Nachricht* die folgenden Optionen fest: Aktivieren Sie das Kontrollkästchen *E-Mail an die folgenden Administratoren senden*, und geben Sie die E-Mail-Adressen der Administratorkonten ein, die Benachrichtigungen erhalten sollen. Trennen Sie mehrere Konten durch Semikola voneinander.

Um den Anwender selbst zu kontaktieren, aktivieren Sie das Kontrollkästchen *E-Mail an den Benutzer versenden*, der den Schwellenwert überschritten hat.

Der Text in eckigen Klammern fügt Variableninformationen zu dem Kontingentereignis ein, das die Benachrichtigung verursacht hat. Die Variable *[Source Io Owner]* etwa fügt den Namen des Benutzers oder der Anwendung ein. Klicken Sie auf die Schaltfläche *Variable einfügen*, um weitere Variablen in den Text einzufügen.

1.7.4 Ereignisprotokoll aktivieren

Um einen Eintrag im Ereignisprotokoll zu protokollieren, aktivieren Sie auf der Registerkarte *Ereignisprotokoll* das Kontrollkästchen *Warnung an Ereignisprotokoll senden*. Wollen Sie einen Befehl oder ein Skript auszuführen, aktivieren Sie auf der Registerkarte *Befehl* das Kontrollkästchen *Diesen Befehl oder dieses Skript ausführen* und geben Sie den Befehl ein. Wollen Sie die automatische Generierung von Speicherberichten festlegen, aktivieren Sie auf der Registerkarte *Bericht* das Kontrollkästchen *Berichte generieren* und wählen aus, welche Berichte der Server generieren soll. Nachdem Sie die Benachrichtigungstypen konfiguriert haben, klicken Sie auf *OK*, um den Schwellenwert zu speichern.

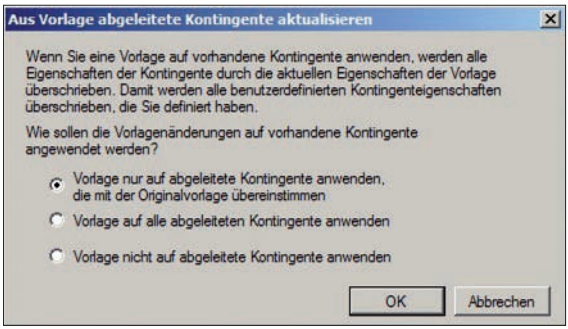
Wenn weitere Benachrichtigungsschwellenwerte konfiguriert werden sollen, klicken Sie im Bereich *Benachrichtigungsschwellenwerte* auf *Hinzufügen*. Geben Sie oben im Dialogfeld *Schwellenwert hinzufügen* den Prozentsatz der Kontingentgrenze ein, bei dem der Server Benachrichtigungen generieren soll. Der Standardschwellenwert für die erste Benachrichtigung liegt bei 85 Prozent.

1.7.5 Kontingentvorlagen konfigurieren

Sie können die Eigenschaften der vorhandenen oder von Ihnen erstellten Kontingentvorlagen jederzeit bearbeiten, wenn Sie auf der entsprechenden Vorlage einen Doppelklick ausführen. Wird eine Vorlage geändert und die Änderung abgespeichert, erscheint ein neues Fenster mit verschiedenen Optionen:

- *Vorlage nur auf abgeleitete Kontingente anwenden* – Überschreibt alle Kontingente, die diese Vorlage nutzen, mit den neuen Einstellungen der Vorlage, wenn die Kontingente noch den Optionen der Originalvorlage entsprechen.
- *Vorlage auf alle abgeleiteten Kontingente anwenden* – Mit dieser Option übernehmen Sie alle Änderungen der Vorlage auf die Kontingente, die Sie mit der Vorlage erstellt haben, unabhängig davon, ob Sie in den einzelnen Kontingenten nach der Erstellung noch Einstellungen geändert haben. Wenn Sie auswählen, die Änderungen an allen Kontingenten vorzunehmen, die von der Originalvorlage abgeleitet sind, werden alle von Ihnen erstellten benutzerdefinierten Kontingenteigenschaften überschrieben.
- *Vorlage nicht auf abgeleitete Kontingente anwenden* – Wenn Sie diese Option wählen, werden die Änderungen der Vorlage nicht auf die bereits erstellten Kontingente übertragen, sondern nur auf neue Kontingente angewendet, die Sie mit der Vorlage erstellen.

Die gleichen Optionen stehen Ihnen zur Verfügung, wenn Sie ein automatisch erstelltes Kontingent bearbeiten. Entsprechen die Werte *Verwendet* und *Verfügbar* für einige erstellte Kontingente nicht der tatsächlichen Einstellung für Grenze, könnte die Ursache ein verschachteltes Kontingent sein.



Aktualisieren: neue Einstellungen in Vorlagen auf Kontingente übernehmen, die die Vorlage verwenden.

Dabei handelt es sich bei dem Kontingent, das für einen Ordner gilt, um ein restriktiveres Kontingent, das von einem seiner übergeordneten Ordner abgeleitet ist. Wechseln Sie in diesem Fall im Knoten *Kontingentverwaltung zu Kontingente* und wählen Sie dann den Kontingenteintrag mit dem Problem aus. Klicken Sie im *Aktionsbereich* auf *Kontingente anzeigen*, die sich auf Ordner auswirken, und suchen Sie nach Kontingenten, die auf übergeordnete Ordner angewendet sind. So können Sie identifizieren, welche Kontingente restriktive Einstellungen für das ausgewählte Kontingent haben.

1.7.6 Datenträgerkontingente – wie viel dürfen Anwender speichern

Klicken Sie ein Laufwerk im Explorer von Windows 7 oder Windows Server 2008 R2 mit der rechten Maustaste an und wählen *Eigenschaften*, so steht Ihnen die Registerkarte *Kontingent* zur Verfügung. Aktivieren Sie die Kontingentüberwachung, können Sie festlegen, wie viele Daten die einzelnen Benutzer auf dem Computer speichern dürfen. Klicken Sie auf *Kontingenteinträge*, so kann festgelegt werden, für welche Anwender Sie besondere Grenzen ziehen wollen. Alle anderen Anwender können die maximale Datenmenge speichern, die Sie auf der Hauptseite des Fensters festlegen.

Thomas Joos

1.8 Sysinternals: Praktische Gratis-Tools liefern Systeminformationen

Microsoft gliedert seine kostenlosen Sysinternals-Tools (http://technet.microsoft.com/de-de/sysinternals) in verschiedene Kategorien, wir widmen jeder Kategorie einen eigenen Beitrag und stellen exemplarisch einige Programme praxisnah vor. Passt die eine oder andere Lösung aus einem anderen Bereich oder aus den Windows-Bordmitteln thematisch dazu, bleibt dies nicht unerwähnt. Mit den Sysinternals-Tools richtet sich Microsoft an IT-Professionals im Allgemeinen und Administratoren im Besonderen.

Die Werkzeuge sollen Admins die Verwaltung, Problembehebung und Diagnose von Windows-Systemen und -Anwendungen erleichtern. Diesmal haben wir einige Tools ausgewählt, die Administratoren unter anderem bei der Anzeige von Systeminformationen die tägliche Arbeit deutlich erleichtern können.

Bisher sind in dieser Artikelserie folgende Beiträge erschienen:

- Sysinternals – Gratis-Tools in Sachen Sicherheit (Webcode **2034515**)
- Sysinternals – Gratis-Tools für die Verwaltung von Dateien und Datenträgern (Webcode **2034453**)
- Sysinternals – mit Gratis-Tools Prozesse, Dienste und Ressourcen analysieren (Webcode **2034774**)
- Sysinternals – Gratis-Tools fürs Netzwerk (Webcode **2034556**)

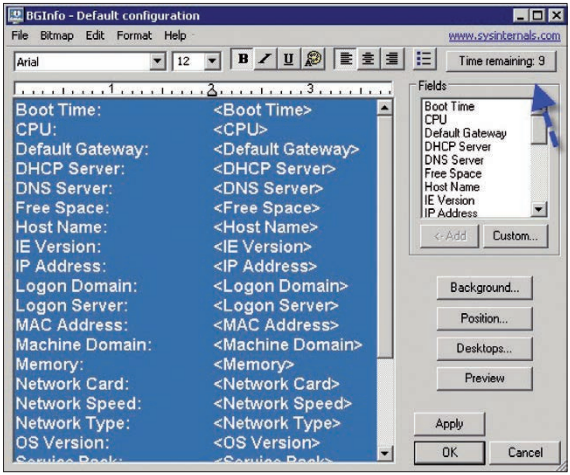
1.8.1 BGInfo – wichtige Informationen immer im Blick

Administratoren, die mehrere Server oder Computer von Anwendern im Netzwerk fernwarten, haben oft das Problem, dass nicht alle Informationen über den aktuell verbundenen Computer angezeigt werden, als da wären IP-Adresse, Informationen zu den Laufwerken, Rechnernamen oder Bootzeit beispielsweise. Es ist sicherlich hilfreich, die aktuelle IP-Adresse, den genauen Namen des Computers und weitere Einstellungen direkt auf dem Desktop zu sehen, vor allem wenn mehrere Server gleichzeitig in einer Diagnosephase sind oder Administratoren parallel mit mehreren Servern arbeiten. Wenn Anwender per Fernwartung unterstützt werden müssen, ist es ebenso hilfreich, wenn diese auf dem Desktop den Namen ihres Computers, die IP-Adresse und weitere Informationen auf einen Blick sehen.

Ein hilfreiches Tool für diese Zwecke ist BGInfo. Der Entwickler hält in einem eigenen Beitrag weitere Tipps zum Tool bereit (www.windowsitpro.com/article/desktop-management/bginfo.aspx). Im Sysinternal-Forum (http://forum.sysinternals.com/forum5.html) erhalten Sie ebenfalls hilfreiche Informationen zu BGInfo.

Eine Einarbeitung ist nicht notwendig, da das Tool sehr leicht bedienbar ist und keine Installation oder Konfiguration erfordert. BGInfo kann Informationen in

verschiedenen Schriftgrößen, Farben und anderen Formatierungen auf dem Desktop anzeigen. Neben vorgegebenen Feldern können Sie eigene Abfragen erstellen und Informationen einblenden lassen.



Alles auf Anfang: So sieht ein erster Start von BGInfo aus.

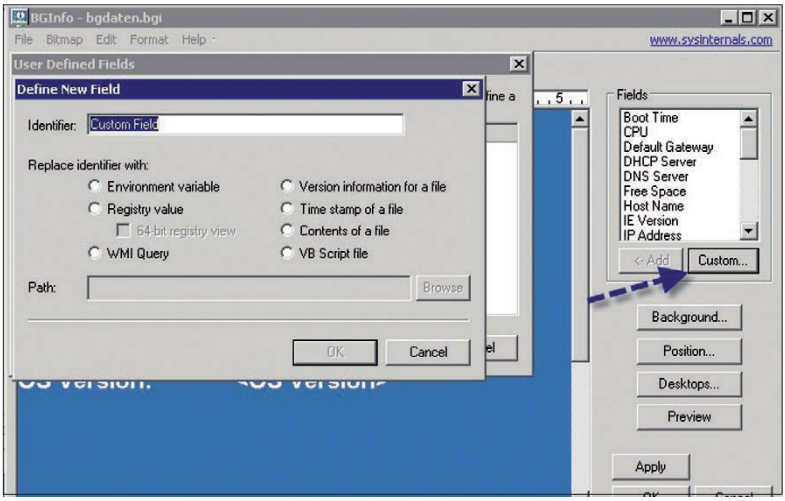
Diese Anzeige lässt sich vorkonfigurieren, als Konfigurationsdatei abspeichern und per Skript oder Gruppenrichtlinie an Computer im Netzwerk verteilen. Das Tool verbraucht keinerlei Systemressourcen, sondern erstellt beim Start aus den gewünschten Informationen eine neue Desktop-Bitmap und beendet sich danach wieder. Im laufenden Betrieb ist das Tool daher nicht gestartet.

1.8.2 Systeminformationen in BGInfo anpassen

Der Umgang mit dem Tool ist sehr einfach. Zunächst starten Sie die ausführbare Datei und wählen aus, welche Informationen Sie anzeigen wollen. Die wichtigsten Informationen sind bereits ausgewählt und im Fenster ersichtlich. Um Änderungen vorzunehmen, klicken Sie zunächst auf *Time remaining* oben rechts oder einen anderen Menüpunkt. Ansonsten bindet das Tool bereits automatisch nach zehn Sekunden die ausgewählten Informationen ein und beendet sich wieder. Nach dem Start können Sie konfigurieren, welche Daten Sie künftig anzeigen wollen, und diese als Konfigurationsdatei abspeichern.

Die Konfiguration ist sehr einfach. Im Feld *Field* sehen Sie, welche Daten Sie in das Hintergrundbild einbinden können. Klicken Sie auf ein Feld und dann auf *<-Add*, um es einzubinden. Verfügt ein Computer über mehrere Netzwerkkarten, bindet BGInfo diese automatisch mit ein, ebenso deren unterschiedliche Konfigurationen wie IP-Adressen, MAC-Adressen und weitere Daten.

Über die Schaltfläche *Custom* können Sie eigene Felder definieren, indem Sie mit *New* eine neue Abfrage starten. Sie haben im neuen Fenster die Möglichkeit, Umgebungsvariablen, einen Registry-Wert, eine WMI-Abfrage oder Daten einer Datei abzufragen. In den meisten Fällen ist das aber nicht notwendig, da die Standardfelder bereits viele Informationen umfassen.



Individuell: Sie können eigene Felder in BGInfo definieren.

Felder und Zeilen, die Sie nicht benötigen, können Sie im mittleren Fenster einfach löschen. Wenn gewünscht, können Sie wie in jeder Textverarbeitung Leerzeilen einfügen. Einzelne Zeilen bearbeiten Sie mit den Formatierungswerkzeugen des Tools, die Sie im oberen Bereich finden. Hier können Sie Schriftgröße und -art einstellen, Farben ändern und die Ausrichtung anpassen.

1.8.3 Anzeige der Systeminformationen mit BGInfo

Haben Sie ausgewählt, welche Felder Sie anzeigen wollen, und diese formatiert, können Sie über die Schaltfläche *Background* festlegen, welches Hintergrundbild Sie mit diesen Informationen anpassen wollen.

Standardmäßig verwendet BGInfo das aktuelle Hintergrundbild des Anwenders. Über die Schaltfläche *Position* bestimmen Sie, an welcher Stelle des Hintergrundbilds BGINfo die Informationen aufnehmen soll. Da das Tool auch mehrere Monitore unterstützt, können Sie festlegen, auf welchem Monitor die Informationen zu sehen sein sollen. Über die Schaltfläche *Compensate for Taskbar position* (Ausgleich für Taskleistenposition) legen Sie die Position so fest, dass die Taskleiste den

Text nicht überdeckt. Über die Schaltfläche *Desktops* bestimmen Sie, wo BGInfo die Informationen anzeigen soll. Standardmäßig sind die Daten erst zu sehen, wenn sich ein Anwender anmeldet. Sie können noch die Option *Update this wallpaper* innerhalb der Einstellung *Logon Desktop for Console Users* aktivieren. In diesem Fall werden die ausgewählten Informationen bereits am Anmeldebildschirm angezeigt, ohne dass sich Anwender anmelden müssen. Das ist zum Beispiel für Server sinnvoll, wenn an der Konsole kein Administrator angemeldet ist. Die Option zum Anzeigen des Hintergrunds ist auch für die Anmeldung an Terminal-Server-Bildschirmen möglich (in Windows Server 2008 R2 auch Remote-Desktop-Sitzungs-Host genannt) und lässt sich entsprechend aktivieren.

Wenn Sie auf *Preview* klicken, zeigt Windows eine Vorschau der Informationen an. Um diese wieder zu deaktivieren, klicken Sie noch einmal auf *Preview*. Um die Anzeige zu übernehmen, klicken Sie auf *Apply*. Mit *OK* übernehmen Sie die Einstellungen und schließen BGInfo.

1.8.4 BGInfo mit vorgefertigter Konfiguration per Skript starten

Natürlich ist es nicht sinnvoll, eine Konfiguration immer wieder neu zu erstellen oder für jeden Computer einzeln anzufertigen. Aus diesem Grund haben Sie in BGInfo auch die Möglichkeit, die von Ihnen angepassten Daten über File\Save als *.bgi-Datei abzuspeichern. Sie können anschließend BGInfo so starten, dass das Tool diese *.bgi-Datei als Konfigurationsdatei übernimmt und die ausgewählten Daten anzeigt. Dazu rufen Sie BGInfo wie folgt auf:

```
bginfo <Name der *.bgi-Datei> /timer:0
```

Geben Sie keine Konfigurationsdatei an, verwendet BGInfo die Standardkonfigurationsinformationen, die in der Registrierung im Pfad *HKEY_CURRENT_USER\Software\Winternals\BGInfo* gespeichert sind. Die Option */timer:0* bewirkt, dass das BGInfo-Konfigurationsfenster nicht erscheint, sondern sofort die Informationen übernommen werden. Sie können diesen Befehl in ein Anmeldeskript übernehmen und auf diese Weise auch Daten wie Anmeldezeit oder Boot-Zeit des Computers erfassen. Diese Zeiten sind natürlich immer nur dann aktuell, wenn Sie BGInfo bei jedem Systemstart oder jedem Anmelden starten lassen. BGInfo aktualisiert sich niemals dynamisch, sondern verwendet immer nur die Daten, die es beim Start vorfindet.

Nach der Erstellung des neuen Hintergrundbildes beendet sich BGInfo wieder. Neben Skripten können Sie BGInfo natürlich auch mit der Aufgabenplanung in Windows während des Systemstarts und im laufenden Betrieb ständig aktualisieren lassen. Das ergibt aber nur dann einen Sinn, wenn Sie auch Felder anzeigen lassen, deren Informationen sich im laufenden Betrieb ändern. Neben der Option timer stehen in BGInfo weitere Möglichkeiten zur Verfügung:

- /popup – Geben Sie diese Option an, zeigt BGInfo ein Pop-up-Fenster an, das die Informationen enthält. Dieses können Anwender schließen.
- /taskbar – Bei dieser Option blendet BGInfo ein Icon in der Informationsleiste der Taskbar bei der Uhr ein. Klicken Anwender auf das Symbol, erscheinen die gewünschten Informationen genauso wie bei der Option /popup.
- /all – Ändert die Daten für alle aktuell angemeldeten Benutzer, zum Beispiel auf Terminal-Server. Auf diese Weise erhalten also alle angemeldeten Anwender das neue Hintergrundbild.
- /log – Erstellt eine Logdatei über die Ausführung , in der das Tool auch Fehler schreibt. Diese Option ist sinnvoll, wenn Sie das Tool im laufenden Betrieb über den Aufgabenplaner des Öfteren starten lassen.
- /rtf – Erstellt eine RTF-Datei. Diese enthält auch die Formatierungen und die Farbe zur Protokollierung

Über ein Anmeldeskript oder eine Gruppenrichtlinie können Sie mit diesen Skriptoptionen das Tool ebenso über eine Freigabe starten lassen. Die Konfigurationsdatei kann dazu gleichfalls in einer Freigabe liegen. Sie können natürlich die Datei und das Tool per Gruppenrichtlinie auch direkt auf die einzelnen Computer kopieren lassen.

BGInfo als Inventur- und Überwachungs-Tool verwenden

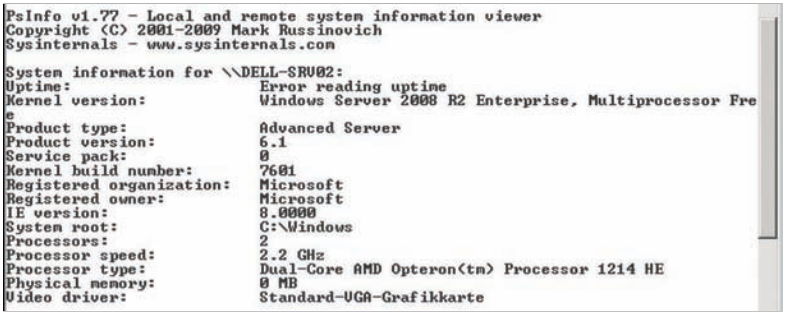
Über *File\Database* können Sie in der Konfigurationsdatei eine Verbindung zu einer Datenbank vorgeben, um die Daten eines oder mehrerer Computer zu erfassen, zum Beispiel für eine Inventur. In diesem Fall ändert das Tool nicht nur das Hintergrundbild, sondern erfasst die Daten in der Datenbank oder der ausgewählten Excel-Tabelle. Auf allen Computern, die diese Konfigurationsdatei nutzen, muss die gleiche Version von MDAC- und JET-Datenbankunterstützung installiert sein. Microsoft empfiehlt mindestens die Versionen MDAC 2.5 und JET 4.0. Sie können an dieser Stelle als Datenbank auch eine Excel-Tabelle verwenden (*.xls). Die Datei muss verfügbar sein, das Tool kann keine Excel-Dateien erstellen.

Wollen Sie mit BGInfo keine Hintergrundbilder ändern, sondern nur die Daten beim Systemstart abfragen und in die Datenbank oder Excel-Tabelle aufnehmen, können Sie in der Konfigurationsdatei festlegen, dass keine Änderungen stattfinden sollen. Dazu klicken Sie im Rahmen der Konfiguration auf Desktops und deaktivieren die Änderung der entsprechenden Desktops.

1.8.5 PSInfo – Systeminformationen in der Befehlszeile

Wollen Sie über einen bestimmten Computer Informationen in der Befehlszeile anzeigen, zum Beispiel zur eingebauten Hardware oder zu installierten Service Packs und Betriebssystemständen, können Sie das kostenlose Sysinternals-Tool PSInfo aus der PSTool-Sammlung nutzen

PSInfo kann nicht nur Daten des lokalen Computers abfragen – dazu könnten Sie zum Beispiel auch *msinfo32.exe* oder systeminfo in der Befehlszeile nutzen –, sondern auch Daten von Netzwerkcomputern.



Direkt: Mit PSInfo können Sie Systeminformationen auf der Befehlszeile ausgeben.

Um Daten des lokalen Systems abzufragen, geben Sie einfach *psinfo* in der Befehlszeile ein. PSInfo benötigt für die Abfrage von Remote-Informationen auch Remote-Zugriff auf die Registrierung des entsprechenden Computers, um Daten anzuzeigen. Das heißt, auf dem Computer muss der Systemdienst *Remoteregistrierung* gestartet sein. Außerdem muss das Benutzerkonto, mit dem Sie PSInfo ausführen, Zugriff auf den Remote-Computer haben.

Die Syntax des Tools lautet:

```
psinfo [[\\Computer[,Computer[,..] |
➥ @Datei [-u Benutzer [-p Kennwort]]] [-h] [-s]
➥ [-d] [-c [-t Trennzeichen]] [Filter]
```

- @Datei – Führt den Befehl auf allen Computern aus, die in der Textdatei angegeben sind. Schreiben Sie Computer in eine eigene Zeile.
- -u – Benutzernamen für den Remote-Computer
- -p – Kennwort für den Benutzer
- -h – Liste der installierten Patches
- -s – Liste der installierten Anwendungen
- -d – Zeigt Informationen zu Datenträgern
- -c – Ausgabe im CSV-Format

Mit der Option */filter* können Sie die Ausgabe nach Feldern filtern, die dem angegebenen Text entspricht.

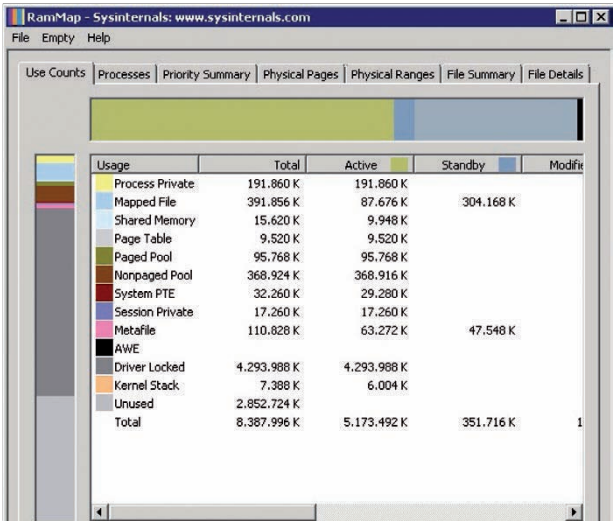
```
psinfo proc
```

zeigt zum Beispiel nur Informationen über die Prozessoren an.

1.8.6 RAMMap – Karte des Arbeitsspeichers

Für die Fehleranalyse oder Leistungsmessung eines Computers kann es sinnvoll sein, die aktuelle Auslastung des Arbeitsspeichers zu kennen. Das Sysinternals-Tool RAMMap zeigt die aktuelle Zuteilung des Arbeitsspeichers in einer grafischen Oberfläche an.

Übersichtlich: So verteilt sich beispielsweise der Speicher in Windows Server 2008 R2.



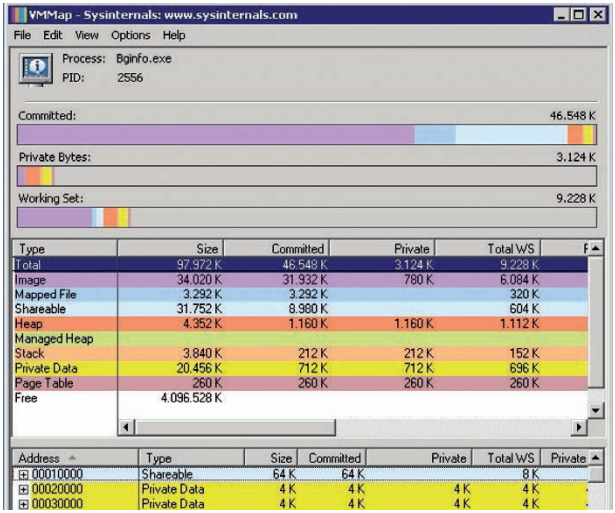
Mit dem Tool erkennen Sie, wie viel Arbeitsspeicher aktuell für den Kernel reserviert ist und welchen Arbeitsspeicher die Treiber des Computers verbrauchen. Auf verschiedenen Registerkarten zeigt das Tool ausführliche Informationen zum Arbeitsspeicher an:

- Use Counts – Zusammenfassung
- Processes – Prozesse
- Priority Summary – Priorisierte Stand-by-Listen
- Physical Pages – Seitenübersicht für den kompletten Arbeitsspeicher
- Physical Ranges – Adressen zum Arbeitsspeicher
- File Summary – Dateien im Arbeitsspeicher
- File Details – Individuelle Seiten im Arbeitsspeicher nach Dateien sortiert

Das Tool hilft vor allem Technikern und Entwicklern zu verstehen, wie die aktuellen Windows-Versionen den Arbeitsspeicher verwalten und an die verschiedenen Anwendungen, Treiber und Prozesse verteilen. Das Tool funktioniert ab Vista/Windows Server 2008, allerdings nicht in den Vorgängerversionen.

1.8.7 VMMAP – Arbeitsspeicher im Detail

Noch ausführlicher bei der Arbeitsspeicheranalyse ist VMMAP. Das Tool zeigt sehr detailliert die Arbeitsspeicherbelegung durch Prozesse an. Dank der ausführlichen Filtermöglichkeiten geht VMMap bei der Analyse wesentlich weiter als RAMMap. Beide Tools sind allerdings nicht nur für Administratoren geeignet, sondern richten sich ebenso an Entwickler oder Techniker, die genau das Aufteilen der Ressourcen analysieren wollen.



Tiefe Einblicke: Mit VMMAP können Sie eine Analyse der Arbeitsspeicherbelegung von Prozessen und Anwendungen durchführen.

VMMap hat die Möglichkeit anzuzeigen, ob ein Prozess Arbeitsspeicher durch den physikalischen Arbeitsspeicher erhält oder durch Windows in die Auslagerungsdatei ausgelagert wird. VMMAP listet sehr detaillierte Daten darüber auf, welche Daten eines Programms oder eines Prozesses in welchen Bereichen des Arbeitsspeichers oder der Auslagerungsdatei liegen. Das Tool ermöglicht das Erstellen von Snapshots und dadurch von Vorher-Nachher-Beobachtungen. Aufgrund der ausführlichen Analysemöglichkeiten kann das Tool in der grafischen Oberfläche genau anzeigen, wie viel Arbeitsspeicher einzelne Funktionen in einem Prozess benötigen. Über *View\String* lässt sich anzeigen, welche Daten ein einzelner Speicherbereich enthält. Gescannte Ergebnisse können Sie über File abspeichern. Neben dem Format, das VMMap kennt (*.mmp), beherrscht das Tool auch das *.txt-Format; zudem können Sie die Daten als *.csv-Datei abspeichern. Damit können Sie Analysen auch in Excel weiterführen. Anders als RAMMap unterstützt VMMAP ebenfalls in Windows 2000, XP und Windows Server 2003

Thomas Joos

2 Virtualisierung

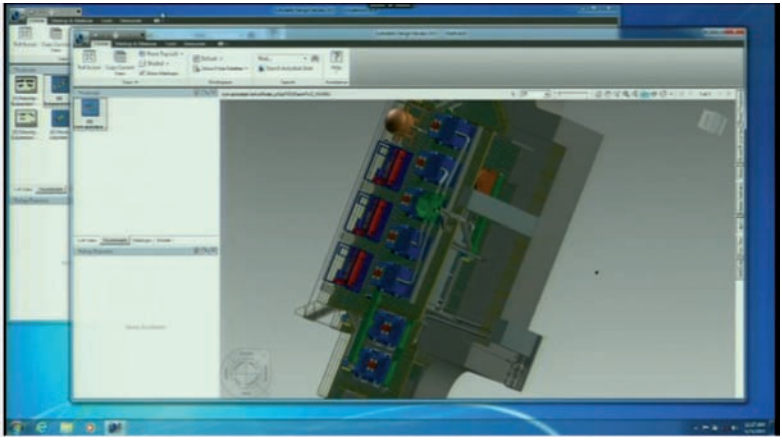
Virtualisierung hat sich im Serverbereich weitgehend etabliert und gewinnt bei der Neuausrichtung bestehender IT-Infrastruktur zunehmend an Bedeutung. Ziel ist es, die Kosten zu reduzieren und gleichzeitig die Flexibilität sowie Effizienz der Abläufe zu erhöhen. Vorteile für die IT-Organisationen sind mehr Flexibilität, eine höhere Verfügbarkeit und kürzere Reaktionszeiten.

2.1 Ratgeber: Was ist was bei der Virtualisierung

Durch die Virtualisierung von Servern wurden die Techniken der virtuellen Nachbildung von Umgebungen etabliert. Sie ist aber längst nicht mehr auf Server beschränkt, sondern wird auch in anderen Zweigen der IT-Nutzung angeboten und eingesetzt. Dabei hat jede der virtuellen Spielarten eigene Anforderungen, aber auch Einsatzzwecke. Worin diese liegen, wollen wir unter anderem in diesem Beitrag aufzeigen. Neben der Virtualisierung von Serversystemen ist heute die virtuelle Nachbildung von Applikationen, Desktops, Clients, der Präsentationsschicht oder auch Speichersystemen möglich. Dabei sind die prinzipiellen Konzepte so neu nicht. Die Nachbildung von physisch nicht realen Systemen durch virtuelle Ebenbilder ist so alt wie die Rechner selbst. In den folgenden Erläuterungen soll daher der Bogen über alle Möglichkeiten der virtuellen Nachbildung gespannt werden. Dies schließt die Servervirtualisierung ein, endet aber nicht bei ihr.

2.1.1 Client-Virtualisierung

Die Client-Virtualisierung ermöglicht die dynamische Bereitstellung von Client-Desktops. Sie ist, was die technische Umsetzung betrifft, der Virtualisierung von Servern ähnlich. Die Client-Virtualisierung zielt allerdings auf den Einsatz für Benutzer-Notebooks. Das System erlaubt den parallelen Betrieb von mehreren Anwendungssystemen auf einem Benutzer-Notebook. Damit lässt sich beispielweise ein Notebook sowohl für den geschäftlichen als auch für den privaten Einsatz verwenden. Neuester Spross aller Virtualisierungsmodelle ist die Client-Virtualisierung. Durch sie lassen sich die Konzepte von „Bring your own Device“ (ByoD) umsetzten. Bei ByoD sollen die Benutzer ihre eigenen Arbeitsgeräte in das Unternehmen mitbringen. Mithilfe der passenden Verwaltungssoftware, beispielweise eben die Client-Virtualisierung, werden diese dann an die jeweiligen unternehmensspezifischen Anforderungen angepasst. Durch die Trennung der Systems in den unternehmensspezifischen und privaten Anteil sind Sicherheitsübergriffe ausgeschlossen oder zumindest erschwert.



Workstation: Citrix hat die Grafikfunktionen im XenClient erneut verbessert und unterstützt auch Grafikverarbeitung.

Der Client-Hypervisor ermöglicht dabei den Betrieb mehrerer paralleler Clients auf einem einzigen Gerät. Der größte Unterschied zur Servervirtualisierung liegt in den Aspekten der Leistung, der Ausfallsicherheit, der Flexibilität und all der fortgeschrittenen Funktionen, die im Rechenzentrum benötigt werden. Bei der Nachbildung von Servern werden mehrere virtuelle Server in einem Host zusammengefasst. Bei der Client-Virtualisierung hingegen werden mehrere Client-Betriebssysteme gruppiert. Zu den bekanntesten Vertretern der Letztgenannten zählt XenClient von Citrix.

Client-Virtualisierung kurz und bündig

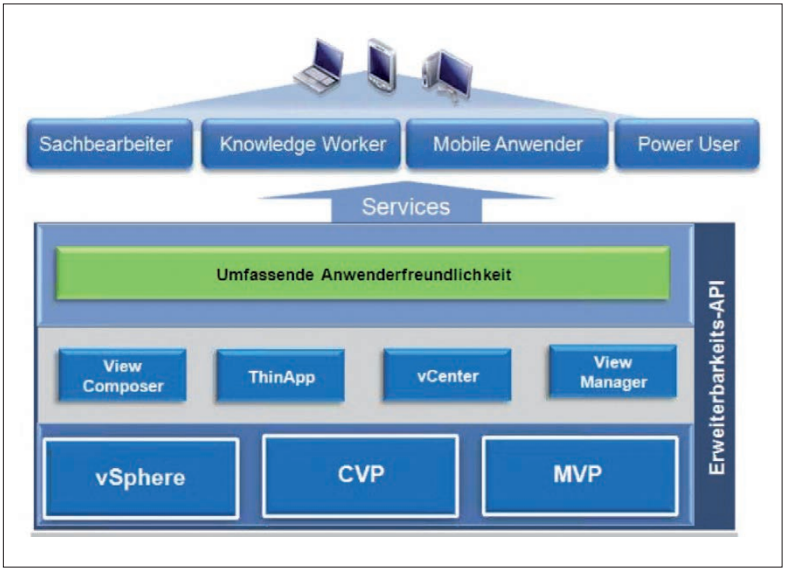
- Virtuelle Umgebung für mehrere parallele Betriebssysteme und Anwendungen
- Vergleichbar mit Multi-Boot-Umgebungen, aber einfacher und bessere Verwaltungsmöglichkeiten
- Ziel: Ein Notebook kann mit unterschiedlichen Betriebssystemen betrieben werden
- Produkte: Citrix XenClient, VMware Workstation, Oracle VirtualBox, Microsoft Virtual PC, VMware Player, Parallels Workstation

2.1.2 Desktop-Virtualisierung

Die Virtualisierung von Desktops zielt, wie auch die von Applikationen, auf den Benutzer-Desktop. Dieser läuft vollständig auf einem zentralen Server. Zum Benutzer hin übertragen werden nur die Bildschirmausgaben. Der Unterschied zu

Präsentationsvirtualisierung besteht darin, dass der Benutzer einen vollständigen Desktop zugewiesen erhält. Hierbei werden unterschiedliche Modelle angeboten.

Der Standard-Desktop etwa könnte über die Techniken der Präsentationsvirtualisierung abgebildet werden. Individuelle Desktops verlangen aber einen eigenen Rechner auf der Serverseite. Dieser Rechner wiederum kann bei hohem Leistungsbedarf durch einen Blade-Einschub im Rechenzentrum realisiert sein.



Grundlagen: Die Architektur der VMware-Desktop-Virtualisierung im Überblick.

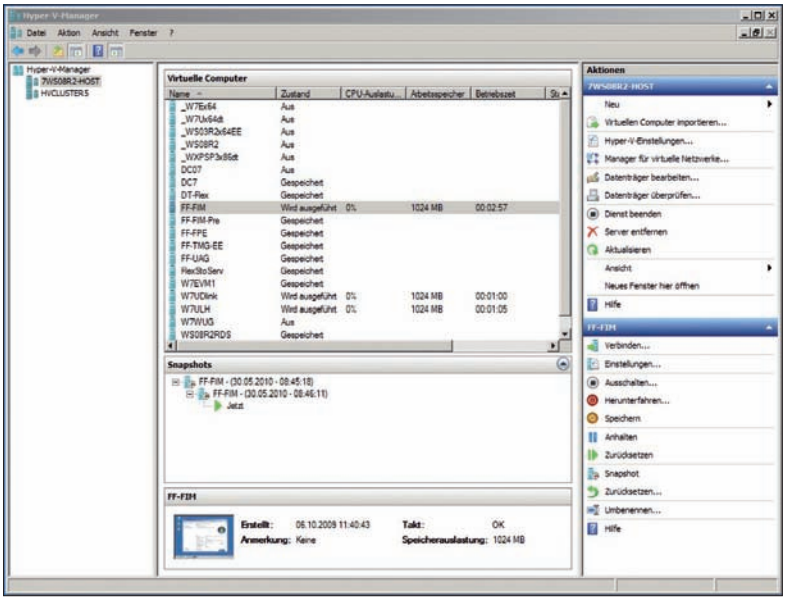
Bei weniger leistungshungrigen Umgebungen kann der Desktop wiederum in einer virtuellen Serverumgebung nachgebildet werden. Neben diese Variante der festen Zuordnung des Benutzers zu seinem zentralen Rechner existieren allerdings auch Mischformen. Durch Connection Broker erfolgt dann beim Verbindungsaufbau des Benutzers die Zuweisung eines virtuellen Desktops an den Benutzer. Dieser wiederum wird dann, wenn benötigt, aus einem vorbereiten Pool entnommen oder neu aufgebaut.

Desktop-Virtualisierung kurz und bündig

- virtuelle Laufzeitumgebungen für Benutzer-Desktops
- effizienter, weil zentrale Verwaltung der Benutzer-Desktops
- unterschiedliche Modelle mit oder ohne Streaming
- Produkte: Citrix XenDesktop, VMware View

2.1.3 Servervirtualisierung

Bei der Servervirtualisierung wird ein x86-Rechner weitgehend vollständig virtuell nachgebildet. Im Kontext dieser Emulation wird dann ein weiteres Betriebssystem ausgeführt. Hierbei handelt es sich meist um ein Serverbetriebssystem und die darauf laufenden Programme. Davon hat sich auch der Begriff der Servervirtualisierung abgeleitet, obgleich diese nicht auf einen Server eingeschränkt ist, sondern einen x86-Rechner nachbildet. Die Zielsetzung der Servervirtualisierung liegt in einer besseren Auslastung der physischen Server. Durch die Virtualisierung werden nun mehrere Serversysteme parallel ausgeführt. Somit steigt die Auslastung des physischen Gerätes, des Hosts.



Konkurrenz: Neben VMware und Citrix bietet auch Microsoft mit dem Hyper-V und dessen Manager eine Servervirtualisierungslösung an.

Die virtuellen Gäste beinhalten ihrerseits ein eigenes Betriebssystem und sind voneinander unabhängig. Die Grundlage dafür bildet ein Hypervisor. Er kümmert sich um die Speicher-, Prozess- und IO-Verwaltung, setzt direkt auf der Hardware auf und kontrolliert sie. Auch die virtuelle Nachbildung der Rechner für die Gäste gehört zu seinen Aufgaben. Dies aber kostet Zeit und Rechenressourcen. Um den Einsatz zu optimieren, sind die CPU-Hersteller dazu übergegangen Virtualisierungsfunktionen direkt in die CPUs zu integrieren. Die aktuellen Hypervisoren benötigen allesamt die Unterstützung der Virtualisierung durch die Host-CPU.

Servervirtualisierung kurz und bündig

- virtuelle Umgebungen für Serversysteme
- effizientere Nutzung der Serverhardware
- höhere Dynamik durch automatisches Deployment von Anwendungen
- Produkte: VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer, KVM

2.1.4 Applikationsvirtualisierung

Bei der Applikationsvirtualisierung wird, anders als bei der Servervirtualisierung, nicht ein Rechnersystem, sondern die Ausführumgebung für eine Applikation, also eigentlich ein Betriebssystem, virtuell nachgebildet. Die Applikationsvirtualisierung zielt damit in erster Linie auf die Client-Desktops und die dort ausgeführten Anwendungen. Prinzipiell könnte es sich auch um eine Serverapplikation handeln, denn auch hier ist die Abgrenzung weniger eine technische als eine, die durch den Einsatzzweck bestimmt wird. Die Grundlage aufseiten des Benutzers stellt, wie auch heute, ein Windows-Betriebssystem dar. Auf diesem Gerät können Applikationen fest installiert sein. Die virtualisierten Applikationen jedoch kommen immer von einem zentralen Server oder anderen Speicherstellen, auf die das Client-Gerät Zugriff hat. Der Benutzer erhält in der Regel lediglich einen Link auf den zentralen Speicherplatz und die Applikation auf seinem Desktop oder das Startmenü. Wenn er diesen Link aktiviert, so wird die Applikation geladen und ausgeführt. Hierfür hat sich auch der Begriff des Streamings etabliert.

Die Applikationsvirtualisierung hat eine Reihe von Vorteilen. Erstens entfallen all die Schritte, die bei einer festen Installation einer Software auf den Benutzergeräten notwendig sind. Die sind in vereinfachter Darstellung das Schnüren eines Installationspaketes, dessen Verteilung auf die Zielgeräte und der Anstoß der Installation aus diesen Paketen heraus. Zwar werden diese Prozesse durch eine Vielzahl an Client-Management-Suiten unterstützt, aber Aufwand verursachen die Abläufe dennoch. Zweitens treten bei den installierten Applikationen mitunter Inkompatibilitäten auf, die sich derart äußern, dass bestimmte Anwendung sich gegenseitig stören. Die gilt nicht nur für die reine Laufzeit, sondern generell. Sobald ein Applikation einmal installiert wird, kann es passieren, dass just eine andere Anwendung nicht mehr lauffähig ist und umgekehrt.

Der dritte Schwachpunkt der festen Installation von Anwendungen - und damit der dritte Vorteil der Virtualisierung - liegt darin, dass von einer Anwendung, obgleich sie wieder deinstalliert wurde, Reste in der Registry oder im Dateisystem zurückbleiben, die ihrerseits wieder zu Problemen führen können. Vorteile hat die Applikationsvirtualisierung auch im Hinblick auf die Sicherheit der Desktops und dessen Daten. Wie erwähnt, laufen die virtualisierten Applikationen in einer eigenen Betriebssystemumgebung. Dabei werden sowohl die Registry als auch das Dateisystem von Windows nachgebildet. Alle Änderungen, welche die virtualisierte Applikation vornimmt, betreffen ausschließlich diese virtualisierten Umge-

bung, deren Registry und Dateisystem. Handelt es sich bei der virtualisierten Applikation allerdings um eine zentrale Dateien oder etwa die Inhalte einer zentralen Datenbank, so gilt dies natürlich nicht. Die Nachteile der Applikationsvirtualisierung bestehen darin, dass sie eine gute Netzwerkanbindung an den zentralen Server, von dem sie die Applikation beziehen, aufweisen müssen. Dies gilt zumindest für den Zeitpunkt des ersten Aufrufs der Applikation, den sie muss ja schlussendlich erst geladen werden.

Um das Laden der Applikation zu optimieren, hat man sich jedoch diverse Techniken einfallen lassen. Durch die Pufferung muss die Applikation somit nur ein einziges Mal über das Netz transferiert werden. Mithilfe der etablierten Client Management Suiten lassen sich die virtualisierten Applikationen auch in größeren Mengen effizient verteilen. Ein weiterer Schwachpunkt kann in der Separierung der Laufzeitumgebung liegen - ein Aspekt, der weiter oben unter den Vorzügen erwähnt wurde. Ein virtualisierte Applikation kann daher keinen Datenaustausch mit anderen Applikationen vornehmen.

Applikationsvirtualisierung kurz und bündig

- virtuelle Laufzeitumgebungen für Client-Applikationen
- einfache Verwaltung der Applikationen, weil traditionelle Softwareinstallationen (Rollouts) entfallen
- erhöht die Sicherheit der Client-Desktops
- Produkte: VMware ThinApp, Microsoft App-V, Altiris SVS Symantec Endpoint Virtualization Suite, Landesk

2.1.5 Präsentationsvirtualisierung

Die Applikationsvirtualisierung ist für den Benutzer-Desktop gedacht. Sie führt damit zu einem ähnlichen Ergebnis wie die Präsentationsvirtualisierung, ist aber gänzlich anders umgesetzt. Bei der Präsentationsvirtualisierung wird nur die Darstellung der Bildschirminhalte, also die Präsentationsschicht einer Applikation, virtuell nachgebildet. Sie läuft dann getrennt von der Applikationslogik. Das Verfahren orientiert sich an der Aufteilung der Applikation in mehrere Schichten (3 Tier). Heute findet sich die Umsetzung der Präsentationsvirtualisierung vor allem in den Produkten von Citrix und deren XenApps (früher Presentation Server) und Microsoft und ihren Terminal Services wider. Die Applikationen laufen dabei auf einem zentralen Server, die oftmals in größeren Gruppen einer Farm zusammengeschlossen werden. Dabei teilen sich alle der Farm zugeordneten Benutzer einen gemeinsamen Rechner. Die größten Vorzüge diese Konzeptes liegen im vereinfachten Management: Die Verwaltung der Farm, ihrer Benutzer und Applikationen erfolgt ausschließlich serverseitig, Eingriffe auf dem Client sind, außer dem Einrichtern der Verbindung zur Farm, nicht notwendig. Die traditionelle Softwareverteilung entfällt beziehungsweise wird zu einer Zuweisung. Damit ist dieses

Verfahren unschlagbar in puncto Verwaltung und Zuweisung von Software für die Benutzer. Die Nachteile des Verfahrens liegen darin, dass eine Verbindung zur Farm für die gesamte Nutzungszeit der Applikation zwingend notwendig ist. Anders als bei der Applikationsvirtualisierung, bei der die Applikation ja auf dem Client gepuffert werden kann, muss bei der Präsentationsvirtualisierung das Benutzergerät immer eine Verbindung zum Server aufweisen.

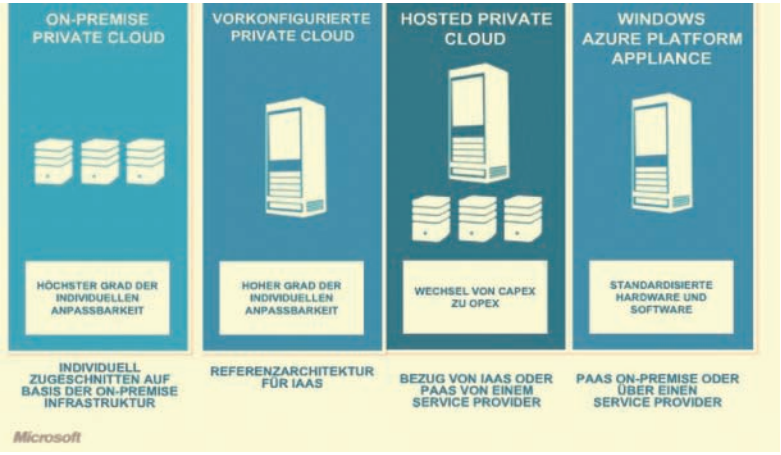
Minimalausrüstung: Die Präsentationsvirtualisierung begnügt sich als Anzeigegerät mit Thin Clients.

Präsentationsvirtualisierung kurz und bündig

- Gruppierung von mehreren Benutzer-Sessions in einer Farm
- sehr einfache Applikationszuweisung
- Thin Clients statt „Fat"-PC als Benutzergerät
- keine individuellen Anwendungen; alle Benutzer der Farm erhalten die gleichen Anwendungen
- Client-Geräte benötigen Anbindung an das Rechenzentrum
- Produkte: Citrix XenApp, Microsoft Terminal Services

2.1.6 Rechenzentrumsvirtualisierung

Bei der Rechenzentrumsvirtualisierung werden nicht nur einzelne Server virtualisiert sondern der gesamte Betrieb des Rechenzentrums; so nähert man sich den Cloud-Modellen an. Im Prinzip werden damit die Techniken der Servervirtualisierung weitergespannt und fortgeschrieben. In der Cloud werden die IT-Ressourcen in Pools gebündelt. Daneben stehen die Applikationsdienste. Wird ein Dienst (eine Anwendung) benötigt, so erhält dieser seine Ressourcen aus dem Pool zugewiesen. Diese Bereitstellung der Applikationen und der zum Lauf benötigten Ressourcen erfolgt dynamisch.



Vielfältig: Die Virtualisierung der Rechenzentren in den Cloud-Modellen ist in unterschiedlichen Varianten möglich.

Um den Prozess der Aktivierung und Deaktivierung von Anwendungenb schnell ausführen zu können, werden Skripte und Automatisierungs-Tools eingesetzt. Nicht mehr benötigte Anwendungen lassen sich auf diese Art und Weise auch wieder deaktivieren. Bei den Cloud-Modellen unterscheidet man nach folgenden Varianten: Beim Modell der Private Cloud werden die Ressourcen des eigenen Rechenzentrums genutzt; sie steht in der Regel nur für das eigene Unternehmen zur Verfügung. Bei der Public Cloud werden die Ressourcen im Internet angeboten beziehungsweise von dort genommen. Die hybride Cloud ist eine Mischform aus Private und Public Cloud.

Rechenzentrumsvirtualisierung kurz und bündig

- bessere Auslastung des Rechenzentrums
- höhere Dynamik durch automatisches Deployment der Anwendungen
- Self-Service-Portale für die Anwender
- aufwandsgerechte Verrechnung
- Produkte: diverse (Amazon, Apple, Google oder Microsoft) von Diensten für Public und Private Cloud

Johann Baumeister

Dipl. Inform. Johann Baumeister blickt auf über 25 Jahre Erfahrung im Bereich Softwareentwicklung sowie Rollout und Management von Softwaresystemen zurück und ist als Autor für zahlreiche IT-Publikationen tätig. Sie erreichen ihn unter jb@JB4IT.de

2.2 Was Datenbankvirtualisierung kostet

Die Auswirkungen der Virtualisierung auf die Lizenzierung von Datenbanken sind ein seit Jahren kontrovers diskutiertes Thema in der IT-Branche. Die klassischen Bezugsgrößen wie Server, CPU oder User-Anzahl sind in der virtuellen Welt nicht mehr so ohne Weiteres greifbar. Die Hersteller von Datenbanken halten oft an ihren alten, profitablen Lizenzmodellen fest und versuchen diese in die Welt von Virtualisierung und Cloud hinüberzuretten. Die Problematik hat es in sich, denn das ursprünglich aus der Mainframe-Welt stammende Konzept der Virtualisierung ist nicht mehr aus dem Unternehmensalltag wegzudenken und hat auch die Domäne der Datenbanken erfasst. So ergab eine Umfrage der Anwendervereinigung DOAG aus dem Jahr 2010, dass von 420 Oracle-Kunden etwa 90 Prozent Virtualisierungslösungen einsetzen, hierbei meist VMware.

Bei der Einführung neuer Lizenzmodelle sind unterschiedliche Aspekte zu berücksichtigen. Auf der einen Seite verlangen die Kunden flexible Lizenzmodelle, die dem Abruf der tatsächlichen Rechenleistung in virtuellen Umgebungen gerecht werden. In der Theorie wären verschiedene Modelle denkbar, zum Beispiel das aus der Mainframe-Welt stammende „Metering", bei dem die Nutzung der Hardwareressourcen durch die Anwendung protokolliert wird. Doch auf der anderen Seite benötigen die Kunden kalkulierbare Lizenzkosten, um das IT-Budget im Voraus planen zu können. Bei einem verbrauchsgerechten Lizenzmodell wissen die Kunden aber nicht, welche Lizenzkosten am Ende des budgetierten Jahres zu Buche schlagen werden. Insofern wäre bei der Einführung neuer Lizenzmodelle auch ein Umdenken bei der Budgetplanung notwendig. In der Praxis begegnen einem unterschiedliche Lizenz- und Abrechnungsmodelle. Diese werden bei Virtualisierungsprojekten oft zu spät berücksichtigt. Als Folge kann es zu einer signifikanten Reduktion der erhofften Einsparungen oder zu nachträglichen Einschränkungen bei der technischen Umsetzung von Virtualisierungsprojekten kommen. Einige Unternehmen geraten unwissentlich in eine Unterlizenzierung, was bei einem späteren Audit durch die Hersteller sehr teuer werden kann.

Im Folgenden werden exemplarisch die Lizenzmodelle von **Oracle** (www.oracle.com/de/), **IBM** (www.ibm.com/de/) und **Microsoft** (www.microsoft.com) gegenüber gestellt, um mehr Transparenz zu schaffen und um eine Entscheidungshilfe bei der Planung von Virtualisierungsprojekten zu bieten.

2.2.1 Das Lizenzmodell von Oracle

Bei der Lizenzierung virtueller x86-Umgebungen hält sich Oracle meist an altbekannte Partitionierungsregeln, die der technisch als sinnvoll erachteten Virtualisierung bei der falschen Planung kostenseitig Steine in den Weg legen können. Laut Oracle-Vorstand Jeb Dasteel wird es auch in naher Zukunft keine Änderungen in den Lizenzierungsregeln von x86-Virtualisierungslösungen geben. Grundsätzlich unterscheidet Oracle zwischen Soft- und Hard-Partitionierung.

2.2.2 Soft-Partitioning – alle im Server laufenden CPUs sind zu lizenzieren

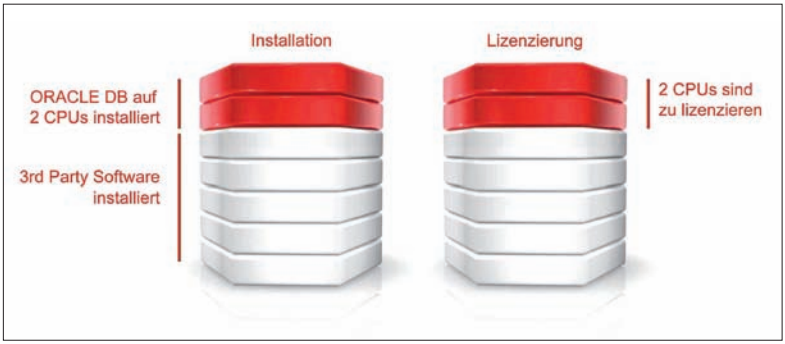
Virtualisierungslösungen, bei denen die Zuteilung der Prozessoren über Ressourcenmanager erfolgt, bewertet Oracle als Soft-Partitioning. Beispiele hierfür sind Solaris 9 Resource Containers, AIX Workload Manager, OracleVM oder VMware. Diese Lösungen haben keinen Einfluss auf die zu zählenden CPUs. Alle im Server installierten physischen CPUs müssen berücksichtigt werden. Die Anzahl der virtuellen Betriebsumgebungen und Instanzen auf dem physischen Server ist irrelevant. Im Bild „Soft-Partitioning“ ist ein soft-partitionierter Server mit acht installierten CPUs abgebildet. Eine Partition mit zwei CPUs wird von der Oracle-DB genutzt. Es sind alle acht CPUs im Server für die Oracle Datenbank zu lizenzieren. Die benötigte Anzahl an Lizenzen (Prozessor oder Named User) wird anhand der Kerne pro CPU kalkuliert (siehe auch Oracle Processor Core Factoring Table, www.oracle.com/us/corporate/contracts/processor-core-factor-table-070634.pdf).

Soft-Partitioning: Acht CPUs sind installiert, nur zwei werden von der Oracle-Datenbank genutzt. Zu lizenzieren sind trotzdem acht CPUs. (Quelle: ProLicense)

2.2.3 Hard-Partitioning – nur zugewiesene Prozessoren sind zu lizenzieren

Beim Hard-Partitioning wird der Server physisch in einzelne voneinander unabhängige Segmente aufgeteilt. Es sind in diesem Fall nur die dem jeweiligen Segment zugewiesenen Prozessoren zu zählen. Beispiele für von Oracle anerkannte Lösungen sind Solaris 10 Containers, LPAR, Micro Partitions, vPar, nPar und OracleVM (bei entsprechender Hard-Installation). Für ein Rechenzentrum, das bedarfsgerecht Rechenleistung für die Datenbank zur Verfügung stellen möchte, ergibt sich damit ein Problem: Nur die Soft-Partitionierung, zum Beispiel mit VMware, ermöglicht einen wirklich dynamischen und bedarfsgerechten Betrieb

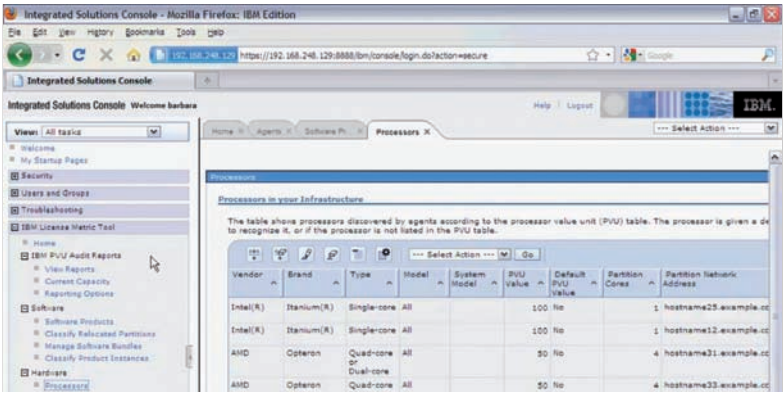
der Datenbank. Hierbei ist jedoch gemäß den Lizenzregeln von Oracle von Anfang an das gesamte System zu lizenzieren. Dies führt sofort zu hohen Lizenzkosten, die bei der Gesamtkostenanalyse berücksichtigt werden müssen.



Hard-Partitioning: Acht CPUs sind installiert, die Oracle-Datenbanken nutzen davon zwei Prozessoren. Zu lizenzieren sind zwei CPUs. (Quelle: ProLicense)

2.2.4 Das Lizenzmodell von IBM

Grundsätzlich besteht Ähnlichkeit zwischen den Lizenzmodellen von Oracle und IBM. Beide bieten User- und Rechenleistung-basierte Lizenzierungen an. Während bei IBM jedoch von PVUs (Processor Value Units – Basis ist hier die Gesamtanzahl der CPU-Kerne) gesprochen wird, lizenziert Oracle nach Prozessoren (wobei auch hier die Gesamtanzahl der Kerne ausschlaggebend ist).



IBM License Metric Tool: Die kostenlose Lösung bietet eine Dashboard-Ansicht mit regelmäßiger Berichterstellung. (Quelle: IBM)

Bei der Lizenzierung virtualisierter Systeme geht IBM jedoch einen etwas anderen Weg: Der Hersteller vereinbart zuvor mit seinen Kunden genau, welche Systeme virtuell aufgebaut werden sollen (Soft-Partitioning). Auf diesen Systemen wird dann das sogenannte IBM License Metric Tool (ILMT) installiert.

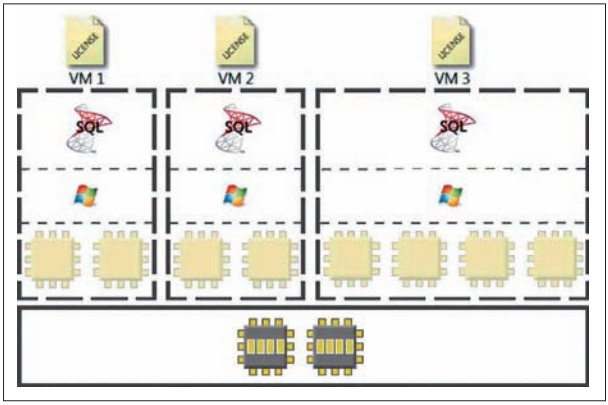
Hier zeigt sich ein Vorteil bei der Lizenzierung gegenüber Oracle: Nur die maximale Prozessornutzung wird lizenziert. Benötigt die Datenbank über einen bestimmten Zeitraum nur maximal vier CPUs, sind auch nur diese vier CPUs zu lizenzieren (auch wenn der physikalische Server mehr CPUs hat). Steigt die Nutzung zu einem Moment während des Betrachtungszeitraums etwa von vier auf sechs CPUs, so sind diese sechs CPUs zu lizenzieren. Ein Rückgaberecht der Lizenzen bei einer anschließend geringeren Nutzungstiefe gibt es hier jedoch ebenfalls nicht. Die Lizenzierung kann durch PVU-Lizenzen (Processor Value Units) oder Named-User-Lizenzen erfolgen. Auch hier ist wie bei Oracle die Anzahl der virtuellen Betriebsumgebungen und Instanzen auf dem physischen Server irrelevant.

2.2.5 Das Lizenzmodell von Microsoft

Grundsätzlich unterscheidet Microsoft zwischen der Server/CAL- und der Prozessor-Lizenzierung.

2.2.6 Das Server/CAL-Modell

In diesem Modell lizenziert der Kunde zum einen die User oder Devices mittels CALs (Client Access License) und zum anderen die notwendige Anzahl von Serverlizenzen. Je Serverumgebung werden dabei die virtuellen Betriebsumgebungen gezählt. Bei der SQL Server Standard Edition ist je virtueller Umgebung eine Serverlizenz notwendig.

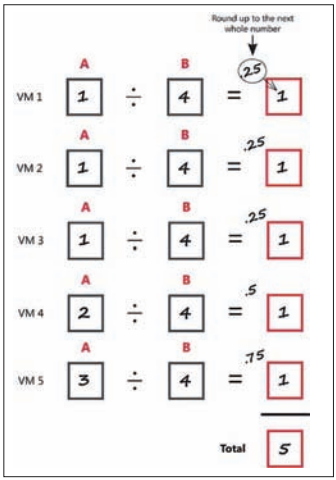


Microsoft SQL Server Enterprise Edition: Mit einer Lizenz können bis zu vier virtuelle Betriebsumgebungen innerhalb einer physischen Serverumgebung arbeiten. (Quelle: Microsoft)

Mit der SQL Server Enterprise Edition können mit einer Lizenz bis zu vier virtuelle Betriebsumgebungen innerhalb einer physischen Serverumgebung betrieben werden. Beim im Bild „Microsoft SQL Server Enterprise Edition“ gezeigten Beispiel mit drei virtuellen Umgebungen (VMs) lizenziert der Kunde demnach unabhängig von der Anzahl der Cores oder Prozessoren im Falle einer Enterprise Edition eine Serverlizenz und könnte in Zukunft noch eine weitere virtuelle Maschine (VM) ohne zusätzliche Lizenzkosten einsetzen. Oder er erwirbt bei der Standard Edition drei Lizenzen.

2.2.7 Das Prozessormodell

Beim Prozessormodell erfolgt die Lizenzierung auf Basis der physikalischen Prozessoren oder alternativ auf Basis der von den VMs genutzten virtuellen Prozessoren. Wählt der Kunde zum Beispiel die Enterprise-Edition im Prozessormodell, sind bei der oben dargestellten ersten Variante alle physischen Prozessoren zu lizenzieren. Je Lizenz können vier virtuelle Betriebsumgebungen genutzt und bei Bedarf weitere Lizenzen erworben werden, um zusätzliche VMs zu ermöglichen. Bei einem System mit vier physischen Prozessoren wären zum Beispiel vier Enterprise-Edition-Lizenzen notwendig und der Betrieb von 16 VMs möglich.



Aufgerundet: Die Anzahl der Lizenzen wird abhängig von der Anzahl der Cores und der virtuellen Prozessoren berechnet. (Quelle: Microsoft)

Die Lizenzierung mit der SQL-Server-Enterprise-Edition ist jedoch nur bis zu einer maximalen Servergröße von bis zu acht physischen Prozessoren möglich. Bei größeren Systemen ist eine Datacenter-Lizenz notwendig.

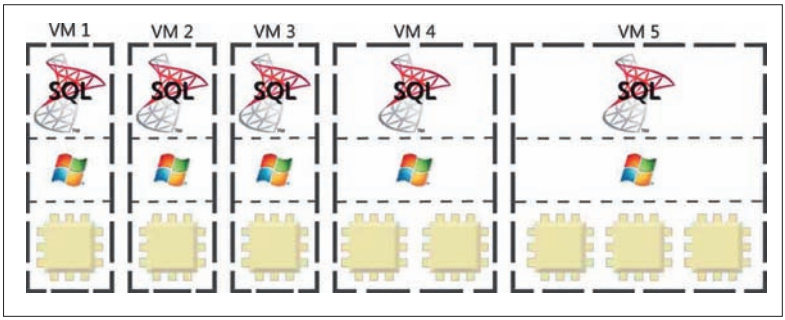
Das Modell auf Basis der physischen Prozessoren ist unattraktiv, wenn der Kunde zum Beispiel einen Server mit acht physikalischen Prozessoren betreibt, auf denen

VMs laufen, diese aber nur fünf virtuelle Prozessoren nutzen. In so einem Fall bietet sich die alternative Methode zur Berechnung der notwendigen Lizenzen an, bei der die Anzahl der tatsächlich von den VMs genutzten virtuellen Prozessoren lizenziert wird. Die Anzahl der Lizenzen wird hierbei in Abhängigkeit von der Anzahl der Cores und der Anzahl der virtuellen Prozessoren wie folgt berechnet:

Benötigte Anzahl der Lizenzen pro VM = Anzahl der virtuellen Prozessoren, die die VM unterstützen (A), geteilt durch die Anzahl der Cores im physischen Prozessor (B). Das Ergebnis ist bei nicht ganzzahligen Ergebnissen stets aufzurunden.

2.2.8 Beispielrechnung: Prozessormodell

Das Bild „Beispielkonfiguration" zeigt einen exemplarisch dargestellten Server mit zwei physikalischen Quad-Core-Prozessoren. Betrieben werden fünf VMs mit einer jeweils unterschiedlichen Anzahl von virtuellen Prozessoren.



Beispielkonfiguration: Server mit zwei Quad-Core-Prozessoren und fünf virtuellen Maschinen mit SQL-Server. (Quelle: Microsoft)

Wählt der Kunde die erste Variante (Lizenzierung nach der Anzahl der physischen Prozessoren), werden zwei Lizenzen für die SQL-Server-Enterprise-Editionen benötigt. Hierbei sind bis zu acht VMs zu betreiben. Im alternativen Berechnungsmodell müsste der Kunde zum Beispiel fünf SQL-Server-Lizenzen erwerben. Welches Modell am Ende das für den Kunden günstigere ist, hängt vom Nutzungsumfang (Enterprise versus Standard) sowie von der Anzahl der physischen Prozessoren, Cores und VMs ab.

2.2.9 Fazit

Es zeigt sich, dass keines der Modelle den dynamischen und bedarfsgerechten Betrieb von virtualisierten Umgebungen zu 100 Prozent abdeckt. Wenn weniger Rechenleistung im Laufe des Betriebs notwendig wird, wirkt sich dies bei allen drei

Anbietern nicht positiv auf die Lizenzkosten aus. Hier ein passendes Modell zu finden wird nach wie vor eine Herausforderung bleiben.

Allerdings lässt sich auch erkennen, dass zumindest teilweise Modelle angeboten werden, die eine Lizenzierung von einzelnen virtuellen Umgebungen ermöglichen, ohne den gesamten physischen Server lizenzieren zu müssen. Aber hierbei erhöht sich auch die Komplexität des Lizenzmodells.

2.2.10 Ausblick

Zunehmend werden auch Dienste angeboten, bei der Kunden ihre Anwendungen, Dienste sowie Speicherplatz in den Rechenzentren der Anbieter skalierbar betreiben lassen können (mit den einhergehenden Herausforderungen zum Thema Datenschutz oder Compliance). Hierbei erfolgt eine Abrechnung entsprechend dem tatsächlichen Bedarf, auch wenn dieser sinkt.

Bleibt zu hoffen, dass der Wettbewerb und die verstärkte Nachfrage der Kunden nach angepassten Lizenzlösungen für Virtualisierungsprojekte zu einer Weiterentwicklung der vorhandenen Lizenzmodelle führen.

Wie so oft steckt der Teufel im Detail. Die Welt der IT ist mit der Einführung von Multi-Core-CPUs, virtuellen Maschinen (VMs) und filigranen Cloud-Benutzungsmodellen nicht einfacher geworden. Eine genaue Prüfung der tatsächlichen Lizenzkosten bei Virtualisierungprojekten ist daher wichtig. Neben den Virtualisierungs- haben somit auch die Lizenzspezialisten zunehmend Konjunktur.

Hartmut Wiehr

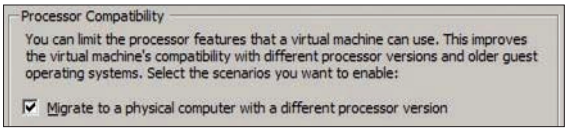
Dieser Beitrag basiert auf einem Artikel unserer Schwesterpublikation CIO.

TecChannel-Links zum Thema	Webcode	Compact
Was Datenbankvirtualisierung kostet	2036628	S.73
Ratgeber: Was ist was bei der Virtualisierung	2037095	S.65
Microsoft Hyper-V auf Intel Sandy Bridge erfordert SP1	2036033	S.80
Workshop – Dynamic Memory beim Hyper-V einrichten	2035020	S.82
Ausblick: Hyper-V 3.0 in Windows 8	2037302	S.86
Mit Parallels Desktop eine virtuelle Umgebung aufbauen	2036786	S.91
VMware vCenter Operations einfach konfigurieren	2036584	S.98
Mit VMware vSphere ein virtuelles Datacenter aufbauen	2037303	S.104

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

2.3 Microsoft Hyper-V auf Intel Sandy Bridge erfordert SP1

Windows Server 2008 R2 bietet in der ursprünglichen Fassung noch keine Unterstützung für AVX, da Sandy-Bridge-Prozessoren erst nach dem Erscheinen von Windows Server 2008 R2 verfügbar wurden. Mit dem Service Pack 1 wurde die Unterstützung von AVX nachgereicht, sodass jeder, der Software schreiben oder einsetzen möchte, die diese neuen Funktionen nutzt, SP1 installieren sollte. Ausführliche Informationen zum Service Pack 1 bietet Ihnen der Beitrag SP1 für Windows Server 2008 R2 und Windows 7.



Hilft ebenfalls nichts: Bei nicht installiertem SP1 auf Sandy-Bridge-Plattformen kann auch diese Option das Problem nicht lösen.

So lassen sich auf einem Hyper-V-Server, der auf einer Sandy-Bridge-Plattform läuft, keine VMs starten, solange nicht das Service Pack 1 installiert ist. Im Eventlog findet man die Fehlermeldung „<VM Name> could not initialize". Hyper-V verhindert korrekterweise zum Schutz der Datenintegrität den Start von virtuelle Maschinen mit unbekannten Prozessorfunktionen.

Die Funktion zur Beschränkung der Features von Prozessoren zum leichteren Verschieben von virtuellen Maschinen zwischen Servern mit unterschiedlichen Prozessoren ist davon unabhängig und hilft bei dem Problem nicht weiter.

Windows Server 2008 R2 und Microsoft Hyper-V Server 2008 R2 unterstützen erst nach dem Einspielen von Service Pack 1 vollständig die neuen Prozessoren. SP1 fügt dabei die Unterstützung von AVX für die Parent Partition und für Gast-Betriebssysteme in virtuellen Maschinen hinzu. Wer nicht in der Lage ist, SP1 auf dem Virtualisierungshost installieren zu können, kann alternativ den Hotfix aus You cannot start virtual machines on a computer that is running Windows Server 2008 R2 and on which a CPU is installed that supports the AVX feature installieren (http://support.microsoft.com/kb/2517374/en-us). Allerdings fügt dieser nur die Unterstützung für die Parent Partition hinzu, sodass sich dann VMs wieder problemlos starten lassen. Die Unterstützung für Gastbetriebssysteme erfordert die Installation des SP1.

Mit dem SP1 auf dem Hyper-V-Server kommen Sie zusätzlich in den Genuss des Features Dynamic Memory. Dynamic Memory gestattet es, dass virtuelle Computer, die nicht den gesamten zugewiesenen Arbeitsspeicher ausnutzen, den verbleibenden Speicheranteil anderen virtuellen Computern zur Verfügung stellen. Ausführliche Informationen dazu vermittelt Ihnen der Workshop: Dynamic Memory beim Hyper-V einrichten (Webcode **2035020**).

2.3.1 Problematik Speicherausbau

Ein zweites Problem kann beim Betrieb mit aktuellen Prozessoren und einem Hauptspeicherausbau von mehr als 32 GByte RAM auftreten. Die Geschwindigkeit eines solchen Systems ist womöglich schlechter als erwartet. Man kann dabei Dinge beobachten wie:s

- hohe CPU-Auslastung,
- lange Reaktionszeit des Servers unter Last,
- niedrige I/O Festplatten-Performance in VMs und
- langsames Starten von Windows.

Das Problem tritt auf, weil neue Intel-Westmere- und Sandy-Bridge-Prozessoren mehr als acht Memory Type Range Register (MTRRs) haben. Diese prozessorspezifischen Register kontrollieren das Caching für Speicherbereiche des physikalischen Hauptspeichers.

Hyper-V unterstützt jedoch maximal 8 MTRRs. Die neuen Prozessoren fügen zusätzliche MTRRs hinzu, um einen größeren Ausbau des Hauptspeichers zu ermöglichen. Da Hyper-V diese zusätzlichen MTRRs bisher nicht ansprechen konnte, werden einige Speicherbereiche als nicht-cachebar ausgewiesen, was die Systemleistung signifikant verringern kann.

Microsoft hat als Lösung für das Problem einen Artikel „Performance decreases in Windows Server 2008 R2 when the Hyper-V role is installed on a computer that uses Intel Westmere or Sandy Bridge processors“ veröffentlicht (http://support.microsoft.com/kb/2517329/en-us). Der darin beschriebene Hotfix kann auf Anforderung direkt heruntergeladen werden. Er ist kein Bestandteil von Windows Server 2008 R2 SP1, sondern muss zusätzlich installiert werden.

Daniel Melanchthon, Malte Jeschke

Dieser Artikel basiert unter anderem auf einem Beitrag aus dem German Virtualization Blog auf Microsofts TechNet (http://blogs.technet.com/b/germanvirtualizationblog/).

TecChannel-Links zum Thema	Webcode	Compact
Microsoft Hyper-V auf Intel Sandy Bridge erfordert SP1	2036033	S.80
Ratgeber: Was ist was bei der Virtualisierung	2037095	S.65
Was Datenbankvirtualisierung kostet	2036628	S.73
Workshop – Dynamic Memory beim Hyper-V einrichten	2035020	S.82
Ausblick: Hyper-V 3.0 in Windows 8	2037302	S.86
Mit Parallels Desktop eine virtuelle Umgebung aufbauen	2036786	S.91
VMware vCenter Operations einfach konfigurieren	2036584	S.98
Mit VMware vSphere ein virtuelles Datacenter aufbauen	2037303	S.104

2.4 Workshop – Dynamic Memory beim Hyper-V einrichten

Im Zuge der Servervirtualisierung werden mehrere physische Server in einem zusammengefasst. Die Ressourcen für den Host werden dabei auf die virtuellen Gäste verteilt. Was die CPU betrifft, so erfolgt diese Aufteilung durch einzelne Cores oder Zeitanteile (Zeitscheiben) der CPU. Das Netzwerk wird virtuell nachgebildet. In dieser Hinsicht sind alle Hypervisoren gleich. Bei der Zuweisung des Speichers gab es bis dato zwei Verfahren. VMware und Citrix haben mehr Speicher an die virtuellen Gäste zugewiesen, als physisch vorhanden war. Dies hat Vor- und Nachteile. Die Vorteile scheinen aber zu überwiegen, denn nun hat auch Microsoft mit einem vergleichbaren Konzept namens Dynamic Memory nachgezogen.

Durch die Funktion des Dynamic Memory wird die Speicherverwaltung des Hyper-V flexibler gestaltet. Der Microsoft Hypervisor kann nun auch mehr Speicher zuweisen, als physisch vorhanden ist.

Das Konzept von Dynamic Memory geht davon aus, dass der Hyper-V immer den optimalen Speicherbedarf des Gastes ermittelt. Diese ideale Speichermenge kann steigen oder auch sinken. Werden beispielweise zusätzliche Programme in der virtuellen Maschine gestartet, so erhöht das den Speicherbedarf; nach Beendigung dieser Programme sinkt er wieder. Infolgedessen erhöht sich oder sinkt auch der durch den Hyper-V zugewiesene Speicher für die virtuellen Maschinen. Dennoch verhält sich der Hyper-V anders als VMwares ESX-Server und seine Speicherverwaltung, die auch als Ballooning bezeichnet wird. Dahinter verbirgt sich – vergleichbar einem Ballon – ein „Aufblasen" des Speicherbedarfs. Herkömmliches Ballooning kennt aber nur eine Richtung: Der Speicher wird immer ausgeweitet, nicht reduziert. In dieser Hinsicht verspricht Hyper-V eine flexiblere Verwaltung.

2.4.1 Parameter und Funktionsweise des Dynamic Memory

Um in den Genuss von Dynamic Memory zu kommen, müssen Sie auf das Service Pack 1 des Windows Server upgraden, denn der Hyper-V ist auch Bestandteil von Windows Server. Alternativ kann man natürlich auch die um das SP1 erweiterte Version des Hyper-V Servers 2008 R2 bei Microsoft herunterladen. Nur bei diese beiden erneuerten Versionen kann der Administrator den Speicherpuffer dynamisch einstellt. Von Vorteil ist dabei die Tatsache, dass die Speicheranpassung auch im laufenden Betrieb der virtuellen Maschinen erfolgen kann. Es ist also nicht notwendig, die virtuellen Maschinen herunterzufahren oder zu „suspendieren", um deren Speicherzuweisung zu ändern.

Für das Einstellen des Dynamic Memory müssen Sie den Konfigurationsbildschirm der virtuellen Maschine des Hyper-V-Managers aufrufen. Unter dem Bereich der Speicherverwaltung findet sich nun die neue Option *Dynamisch*. Sie kennt zwei Grenzen: *Start-RAM* und *Maximaler RAM*. Durch diese beiden Werte

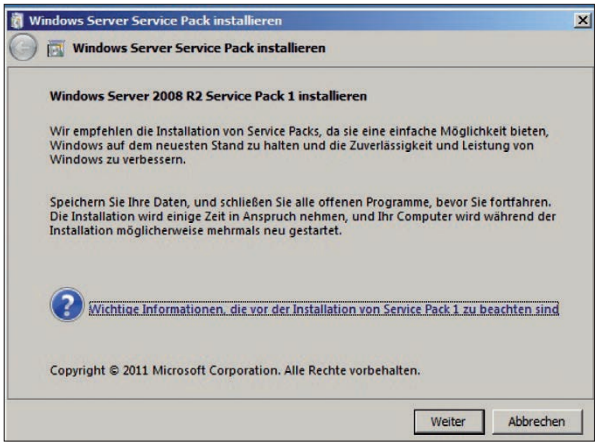
sind die Unter- und die Obergrenze des Speichers definiert. Darunter finden Sie einen weiteren Eintrag, der mit *Memory buffer* umschrieben ist. Dies ist die Menge, die der Hyper-V als Puffer reservieren soll. Der Standardwert ist auf 20 Prozent eingestellt, der Wert kann durch den Administrator aber beliebig verändert werden. Durch diese Einstellung ist nun festzulegen, wie viel an Speicher eine virtuelle Maschine vom System zugeordnet bekommt, wenn Speicher zwischen den Gästen angepasst werden soll.

Ferner erlaubt Windows Server beziehungsweise Hyper-V nun eine Gewichtung des Speichers der virtuellen Maschine im Vergleich zu allen anderen virtuellen Maschinen auf diesem Host. Dies erfolgt durch einen Schieberegler in der Verwaltungsmaske der virtuellen Maschine. Das ist immer ein relativer Wert, der ausschließlich im Verhältnis zu den weiteren virtuellen Gästen zu sehen ist.

2.4.2 Installation und Konfiguration

Um Dynamic Memory anwenden zu können, müssen Sie das Service Pack 1 des Windows Server 2008 R2 installieren, das Sie von der Microsoft-Website beziehen können. Microsoft stellt dabei unterschiedliche Module für die 32-Bit- und die 64-Version zur Verfügung. Dies sind die Dateien *KB976932-X86.exe* und *KB976932-X64.exe*. Sie können diese Service Packs auch für Windows 7 heranziehen, denn die Codebasis zwischen Windows Server 2008 und Windows 7 haben die Redmonder angeglichen. Wie bereits erwähnt, können Sie auch die um das SP1 erweiterte Version des Hyper-V Servers 2008 R2 herunterladen.

Start: Um Dynamic Memory nutzen zu können, muss zuerst das Windows Server Service Pack 1 installiert werden.

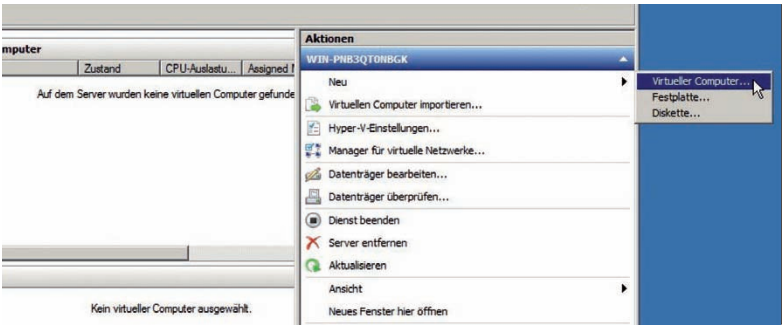


Starten Sie das Installationsprogramm für das Service Pack von Windows Server. Im Laufe der kommenden Dialoge werden Sie gefragt, ob Sie anschließend auto-

matisch einen Neustart des Rechners durchführen wollen. Die Konfigurationsdialoge sind schnell durchlaufen, ebenso das eigentlich Einspielen des Service Packs.

Details: Unter Serverrollen muss die Funktion Hyper-V explizit aktiviert werden.

Sofern Ihr Windows Server die Rolle Hyper-V noch nicht aktiviert hat, können Sie dies nun im Servermanager nachholen. Dazu rufen sie die Funktion *Serverrollen* auf. In der Übersicht müssen Sie bei *Hyper-V* einen Haken setzen.

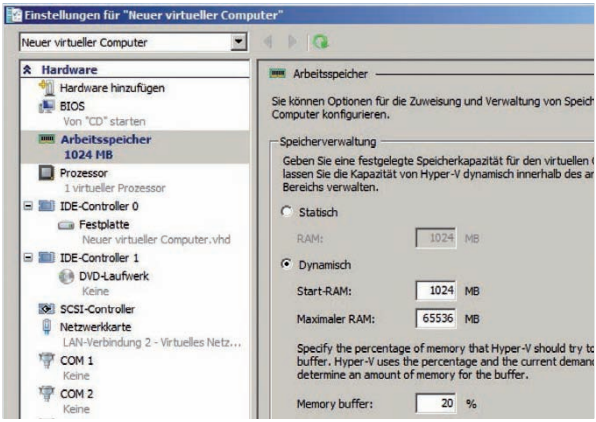


Fortsetzung: Mithilfe des Hyper-V-Managers muss ein neuer virtueller Computer angelegt werden.

Zur Konfiguration von Dynamic Memory starten Sie den Hyper-V-Manager und legen sie unter *Neu / Virtueller Computer …* einen neuen virtuellen Computer an. Vergeben Sie wie gewohnt alle notwendigen Parameter, die sie für dieses System geplant haben.

Standard: Die Größe des Arbeitsspeicher wird beim Einrichten einer virtuellen Maschine vergeben.

Der Assistent wird Sie, wie auch früher, nach der Speichermenge fragen, die Sie dem neuen virtuellen Computer zuweisen wollen. Dieser Werte ist in diesem Fall nur ein Basiswert, den die virtuelle Maschine benötigt. Die genaue Speicherparametrierung erfolgt im nächsten Schritt.



Zuweisung: In diesem Fenster werden die einzelnen Parameter des dynamischen Speichers einer virtuellen Maschine vergeben.

Um Dynamic Memory für eine bestehende virtuelle Maschine einzurichten, rufen Sie die Eigenschaften der virtuellen Maschine auf. Unter den Einstellungen für den virtuellen Computer können Sie nun unter der Rubrik *Arbeitsspeicher* alle weiteren Konfigurationen vornehmen. Sie müssen zuerst die Speicherverwaltung von *Statisch* auf *Dynamisch* wechseln. Danach können Sie die Größe von *Start-RAM* und von *Maximaler RAM* eingeben. Definieren Sie dann noch die Puffergröße und priorisieren Sie den Speicher für eingerichtete virtuelle Maschine. Damit ist die Vergabe des Dynamic Memory unter Microsoft Hyper-V abgeschlossen.

Johann Baumeister

2.5 Ausblick: Hyper-V 3.0 in Windows 8

Zwar stehen noch keine öffentlichen Beta-Versionen von Windows 8 und dem entsprechenden Serverbetriebssystem zur Verfügung, dennoch mehren sich die technischen Details zu den neuen Betriebssystemen. So soll Windows 8 die neue Version 3.0 der Virtualisierungstechnologie Hyper-V enthalten.

Zu Hyper-V sind gleichfalls schon einige Details bekannt, die zum Teil auch von Microsoft bestätigt sind. Mit der neuen Version will Microsoft Hyper-V auch für sehr große und leistungshungrige Serverfarmen und Private-Cloud-Infrastrukturen fit machen. Ganz offensichtlich möchte Microsoft mit Hyper-V einen entscheidenden Leistungssprung machen, damit auch anspruchsvolle Server wie SQL-Datenbanken problemlos und leistungsstark funktionieren.

Die grundsätzliche Verwaltungsoberfläche, der Hyper-V-Manager, sieht in aktuellen Builds von Windows 8 Server noch so aus wie bei Windows Server 2008 R2 und lässt sich offensichtlich auch so bedienen. Die neuen Funktionen hat Microsoft dazu in die Oberfläche integriert. Wir zeigen Ihnen die wichtigsten Neuerungen der neuen Version.

2.5.1 Verbesserte Wiederherstellung von virtuellen Servern – Hyper-V Replica

Hyper-V Replica ist mit Sicherheit die entscheidende Neuerung in Hyper-V von Windows 8 Server, wenn nicht sogar von Windows 8, und wurde bereits offiziell bestätigt. In Hyper-V 3.0 können Administratoren virtuelle Server sehr viel leichter zwischen Hyper-V-Hosts replizieren als bisher. Es ist kein Exportvorgang mehr notwendig, der die Maschine ausbremst, sondern asynchrone Replikationsvorgänge lassen sich schnell und leicht im laufenden Betrieb von virtuellen Servern durchführen. Dazu dient eine neue Funktion mit der aktuellen Bezeichnung Hyper-V Replica. Microsoft zeigt diese Funktion auch in einem Video (http://digitalwpc.com/Videos/AllVideos/Permalink/3cb3788c-5c47-4b9e-987c-0dec4194058b/).

Interessant wird es ab Minute 36:50. Auf diesem Weg lassen sich virtuelle Server auch sichern, da der Quellserver natürlich weiterhin aktiv bleibt. Die Übertragung mit Hyper-V Replica können Anwender entweder zeitgesteuert oder sofort durchführen. Hyper-V kann diese Replikation vollkommen unabhängig vom eingesetzten Speichersystem erledigen. Die einzige Voraussetzung ist, dass auf dem Quell- und dem Zielserver Hyper-V 3.0 läuft und die Server über eine Netzwerkverbindung verfügen, über die sie kommunizieren können. Im Gegensatz zur Live-Migration in Windows Server 2008 R2, bei der Sie Hyper-V-VMs in einem Cluster zwischen Knoten verschieben können, kann Hyper-V Replica auch ohne Cluster und ohne Zusatzkosten virtuelle Server replizieren, nicht nur verschieben.

2.5.2 Replikation mit Hyper-V Replica

Die Übertragung findet über einen leicht zu bedienenden Assistenten statt. Diesen starten Sie über das Kontextmenü von virtuellen Servern im Hyper-V-Manager. Zunächst wählen Sie im Assistenten den Zielserver aus, auf dem Sie den virtuellen Server replizieren wollen.

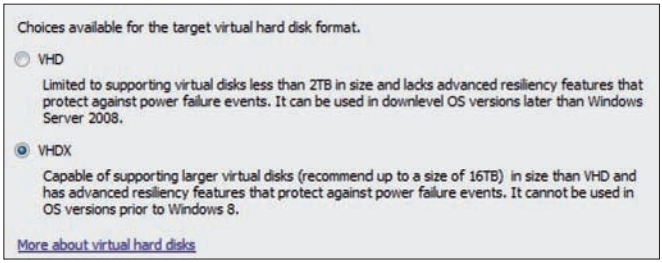
Weiterhin konfigurieren Sie die Verschlüsselung und die Authentifizierung für die Übertragung. Im Assistenten können Sie auch auswählen, welche virtuellen Festplatten Sie auf dem Zielserver replizieren wollen. Anschließend können Sie die Snapshots auswählen, die Sie mit auf den Zielserver replizieren wollen.

Im Assistenten legen Sie noch die Zeit fest, zu der Sie die Replikation starten möchten. An dieser Stelle bietet Hyper-V 3.0 die Möglichkeit, die virtuelle Maschine offline auf ein Medium wie eine externe Festplatte zu replizieren. Die Replikation lässt sich extrem einfach über den Assistenten durchführen. Sobald Sie alle notwendigen Konfigurationen ausgewählt haben, startet der Assistent mit der Replikation. Auch Serveranwendungen wie SQL-Server mit ausgelasteten Datenbanken lassen sich auf diesem Weg leicht replizieren, ohne auf komplexe Konfigurationen zurückgreifen zu müssen. Microsoft stellt die Funktion aller Voraussicht nach kostenlos in der Serverversion von Windows 8 zur Verfügung, zusammen mit Hyper-V 3.0. Allerdings ist bislang unklar, ob Microsoft hier Unterscheidungen zwischen der Standard- und der Enterprise-Edition von Windows 8 Server macht. Informationen und Screenshots zu der Funktion finden Sie auch in diesem Blog zu Windows (www.windowsblog.at/post/2011/07/28/Windows-Server-e2809c8e2809d-Sneak-Preview-Hyper-V-Replica.aspx). VMware bietet diese Funktion mit dem Site Recovery Manager (SRM) in vSphere 5.0.

2.5.3 Größere Festplatten, mehr CPU-Kerne

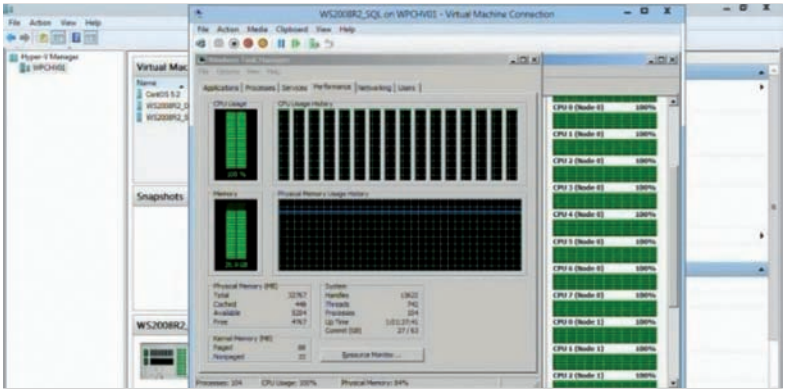
Hyper-V in Windows 8 unterstützt Festplatten mit einer Größe bis zu 16 TByte. Dazu ändert Microsoft das Format von .vhd zu vhdx. Platten im .vhd-Format unterstützen nur eine Größe von 2 TByte. Beim Erstellen neuer Harddiscs können Administratoren das Format auswählen.

Zugewinn: Das neue vhdx-Format unterstützt Festplatten mit bis zu 16 TByte.



In Hyper-V 3.0 steht dazu auch weiterhin das alte .vhd-Format zur Verfügung, um die Migration zu erleichtern. Das neue .vhdx-Format unterstützt nur Windows 8. Ob ein Service Pack für Windows Server 2008 R2 oder Windows 7 die neue Funktion auch dort integrieren wird, ist aktuell noch nicht bekannt. Das neue Format ist außerdem besser für Hyper-V Replica geeignet als die bisherige Version .vhd.

Ebenfalls neu sind die Möglichkeiten, mehr CPU-Kerne als virtuelle Prozessoren zuzuweisen. Hier bietet die neue Version mehr Möglichkeiten als die aktuelle Version in Windows Server 2008 R2. Im Internet kursieren bereits Gerüchte, dass sich mehr als 16 Kerne jeder virtuellen Maschine direkt zuweisen lassen.



Potenzial: In einem Demo-Video von Microsoft ist erkennbar, dass sich mindestens 16 CPU-Kerne einem virtuellen Server zuweisen lassen.

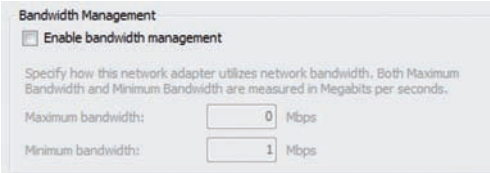
Genaue Informationen, wie viele Kerne Hyper-V unterstützt, gibt es aktuell noch nicht. Allerdings weist der Microsoft-Mitarbeiter in dem Demo-Video darauf hin (www.digitalwpc.com/Videos/AllVideos/Permalink/3cb3788c-5c47-4b9e-987c-0dec4194058b/), dass Hyper-V 3.0 wohl noch mehr Kerne unterstützt und diese auch durchaus bis zu 100 Prozent ausgelastet werden können. Im Film ist ein SQL-Server zu sehen, der 16 Kerne nutzt. Hyper-V 3.0 in Windows 8 bietet hier mehr Einstellungsmöglichkeiten als die Vorgängerversionen, um die CPU-Last zu verteilen. Das ist bereits im Menü des Hyper-V-Managers zu sehen. Die Einstellungsmöglichkeiten gelten ebenso für den Arbeitsspeicher: Auch hier erweitert Microsoft die Möglichkeiten von Dynamic Memory in Windows Server 2008 R2 SP1.

2.5.4 Bandbreitenverwaltung der Netzwerkverbindungen

Auch bei den Netzwerkverbindungen gibt es mehr Einstellungsmöglichkeiten. Administratoren können auf diesem Weg die Bandbreite der Netzwerkverbindungen genau justieren. Zusätzlich bieten die Einstellungen noch erweiterte Menüs, in de-

nen Administratoren zum Beispiel auch eine Hardwarebeschleunigung für Netzwerkverbindungen aktivieren können, sowie Offload-Einstellungen.

Einflussnahme: Administratoren können die Bandbreite regulieren.



Hyper-V 3.0 unterstützt anscheinend direkt TCP Chimney Offload. Bei dieser Technik lassen sich Berechnungen für den Netzwerkverkehr von den virtuellen Servern zu den Netzwerkkarten delegieren, was die Leistung des Rechners für Anwendungen und im Netzwerk erheblich beschleunigen kann. Das heißt, virtuelle Maschinen können künftig auch direkt auf Hardwarefunktionen der Netzwerkkarten zugreifen, was netzwerklastige Systeme beschleunigt. Zusätzlich ist eine Funktion integriert, die DHCP-Anfragen von virtuellen Servern blockieren kann, genauso wie Anfragen an die Router im Netzwerk. Alle diese Einstellungen finden sich im Konfigurationsfenster der virtuellen Maschinen im Hyper-V-Manager.

Ebenfalls neu ist die Möglichkeit, Ressource-Pools zu erstellen. In ihnen lassen sich Fibre-Channel-Verbindungen zusammenfassen und so leichter auf die virtuellen Server verteilen. Mit der Funktion können Sie zum Beispiel Speicherzugriffe auf SANs von virtuellen Servern einmal konfigurieren, zusammenfassen und mehreren Servern zuteilen. In Hyper-V 3.0 integriert Microsoft dazu virtuelle Fibre-Channel-Adapter. Auch diese Funktion ist im Hyper-V-Manager integriert.

2.5.5 Hyper-V auf dem Windows-8-Client

In neueren Windows-8-Versionen gibt es auch im Client-System eine Integration des Features Hyper-V-Core. Anscheinend bietet die Client-Version von Windows 8 ebenfalls die Möglichkeit, Computer mit Hyper-V zu virtualisieren. Die neue Funktion soll wohl den Windows-XP-Modus ablösen und Kompatibilität mit älteren Anwendungen ermöglichen, vor allem von 32-Bit-Anwendungen in Windows 8 x64. Diese laufen dazu als virtualisierte Anwendung oder als Anwendung in einem mit Hyper-V virtualisierten Computer im Windows-8-Client. Einige Spezialisten gehen davon aus, dass Hyper-V 3.0 direkt auch App-V-Anwendungen unterstützt, also virtualisierte Anwendungen ohne dazugehörigen Server.

Auch Windows Phone 7.5/8 soll sich auf diesem Weg emulieren lassen, was Entwickler und Administratoren sicher erfreut. Hier besteht zudem die Möglichkeit, dass sich auf diesem Weg nicht nur das komplette Smartphone-System emulieren, sondern auch einzelne Anwendungen starten lassen, die normalerweise nur für Windows Phone entwickelt wurden. In Hyper-V-Core, dem Ersatz von Virtual PC,

sollen wohl auch unterstützte Linux-Systeme laufen und sich direkt starten lassen, ohne selbst auf die Virtualisierungstechnologie zurückgreifen zu müssen. Für Anwender soll der Betrieb also noch transparenter sein als der aktuelle Windows-XP-Modus in Windows 7 oder Microsoft Enterprise Desktop Virtualization (MED-V) im Microsoft Desktop Optimization Pack (MDOP). Auch App-V wird anscheinend direkt in Hyper-V 3.0 übergehen, sodass sich Anwendungen direkt, also ohne Zuhilfenahme weiterer Techniken, virtualisieren lassen.

2.5.6 Virtualisierung neu geordnet

Im Bereich Virtualisierung bietet Microsoft aktuell noch sehr viele Produkte an, was die Transparenz gerade für Unternehmenskunden nicht erhöht, man zählt den Windows-XP-Modus, Microsoft Enterprise Desktop Virtualization, App-V, Hyper-V und Virtual PC. Künftig soll es nur noch Hyper-V geben, und zwar auf dem Server und dem Client. Allerdings sind dazu auf dem Client die Editionen Ultimate oder Enterprise notwendig. Weitere Gerüchte besagen, dass Hyper-V-Client auf Windows 8 auch 64-Bit-Systeme virtualisieren kann; Virtual PC ist dazu noch nicht in der Lage. Hyper-V in Windows Server 2008 R2 kann dagegen natürlich bereits problemlos auch 64-Bit-Betriebssysteme installieren.

In diesem Rahmen kursieren im Internet auch immer mehr Gerüchte, dass Anwendungen, die mit Hyper-V 3.0 auf dem Server virtualisiert werden, keine komplette Installation von Windows mehr benötigen, sondern in einem kleinen Windows-Kernel, auch MinWin genannt, laufen. Ähnlich wie bei Windows PE, über das aktuelle Rettungs-CDs funktionieren, sollen sich auf diesem Weg auch Anwendungen virtualisieren lassen. Der Vorteil des Systems ist, dass das Gastbetriebssystem keine unnötige Leistung verschwendet und auf diesem Weg mehr Ressourcen auf dem Hyper-V zur Verfügung stehen. Mit dieser Leistung können Administratoren dann entweder mehr virtuelle Server/Anwendungen zur Verfügung stellen oder den Anwendungen mehr Leistung gönnen.

2.5.7 Fazit

Es ist offensichtlich, dass Microsoft mit Hyper-V 3.0 in Windows 8 einen sehr großen Sprung machen will und vor allem Leistung und Kompatibilität im Auge hat. Techniken wie Hyper-V Replica gehören sicherlich zu den spannenderen Features in Windows 8, besonders für den Unternehmenseinsatz. In der kommenden Version 3.0 kann das kostenlose Hyper-V durchaus mit konkurrenzfähigen Funktionen punkten. Es bleibt abzuwarten, welche davon in die finale Version von Windows 8 einfließen, und was die Wettbewerber bis dahin zu bieten haben. Administratoren dürfen sich auf jeden Fall auf sehr interessante Features im Bereich Virtualisierung und Private Cloud freuen.

Thomas Joos

2.6 Workshop – Mit Parallels Desktop eine virtuelle Umgebung aufbauen

Virtualisierung wird überall genutzt, und es gibt inzwischen auch eine Vielzahl von Anbietern entsprechender Lösungen. Einer der bekanntesten Vertreter ist VMware mit View, Workstation oder Player (www.vmware.com). Doch auch für den Platzhirschen existieren verschiedene Alternativen. Unter Windows bietet Microsoft selbst die Freeware Virtual PC (www.microsoft.com), unter Linux gibt es Xen von Citrix (www.citrix.de) und andere, für Macintosh-Rechner ist Software von Parallels (www.parallels.com/de/) prädestiniert.

Während VMware Versionen für Linux und Windows anbietet, arbeitet VirtualPC von Microsoft nur unter Windows. Außerdem ist die Microsoft-Lösung bei den Gastsystemen eingeschränkt. VMware beherbergt hier fast alles, angefangen bei MS-DOS und Windows 3.1 über Linux und Novell Netware bis Oracle Solaris.

Was für VMware gilt, trifft größtenteils auch auf Parallels Desktop zu. Das Programm läuft ebenfalls auf Linux und Windows, aber auch auf dem Mac. Es unterstützt jedoch nicht so viele Gastsysteme wie VMware Workstation. Parallels Desktop lässt laut Waschzettel die folgenden 32- und 64-Bit-Versionen zu:

- Windows 7
- Windows Vista SP1, SP2
- Windows XP Pro SP3
- Windows XP Home SP3
- Windows XP Professional SP3, SP2, SP1, SP0
- Windows XP Home SP3, SP2, SP1, SP0
- Windows 2000 Professional SP4
- Debian 5.0
- Fedora 11
- Mandriva 2009
- OpenSUSE 11.1
- RHEL 4.7 und 5.3
- SLES 11
- Ubuntu 9.04

Später, wenn der Anwender im Programm eine virtuelle Maschine erstellen will, stellt er erfreut fest, dass mehr als 30 verschiedene Gastsysteme unterstützt werden. Hinzu kommt der Preis, der eindeutig für Parallels spricht: Während VMware Workstation 176 Euro kostet (www.vmware.com), sind für Parallels Desktop gerade mal 80 US-Dollar zu berappen (www.parallels.com/de/).

2.6.1 Anforderungen an das Host-System

Wer virtuelle Maschinen einsetzen will, sollte nicht am Host-System sparen. Denn da verlangen die Virtualisierungslösungen nach entsprechender Power. Wenn die Computerhardware nicht ausreicht, kann man Parallels Desktop nur eingeschränkt verwenden. Dann ist es zwar möglich, virtuelle Maschinen zu erstellen, aber das Ausführen muss auf anderen Rechnern geschehen. Als Minimalanforderung empfiehlt Parallels folgende Ausstattung:

- x86- und x64-Plattformen mit Intel-VT-x- oder AMD-V-Hardware-Virtualisierungsunterstützung
- Prozessor mit mindestens 1,5 GHz
- 2 GByte RAM (4 GByte oder mehr werden empfohlen)
- 30 GByte freier Festplattenplatz für die Installation der Parallels-Software und 30 GByte pro virtueller Maschine. Die Größe ist abhängig von den Programmen und Daten in der jeweiligen virtuellen Maschine
- Ethernet-Netzwerkadapter, gültige IP-Adresse

Die Anforderungen erfüllen heutzutage viele PCs. Auch ältere Rechner können da eventuell mithalten. Immerhin gibt es die Virtualisierungserweiterung der Prozessoren schon ein paar Jahre: AMD erste CPUs dieses Typs waren der Athlon 64, der 64 X2 und der 64 FX; sie kamen im Jahr 2006 heraus. Intel war mit den Modellen 662 und 672 des Pentium 4 ein halbes Jahr früher dran.

2.6.2 Das Gastsystem

Ist das Host-System noch anspruchsvoll oder ambitioniert zu nennen, so sind die Gastsysteme auf der anderen Seite Standard. Für die virtuellen Maschinen stellt Parallels Desktop folgende virtuelle Hardware zur Verfügung:

- CPU: bis zu 8-Core Intel-CPU
- Motherboard: Motherboard mit Intel-i965-Chipsatz
- RAM: bis zu 8 GByte
- Grafik: VGA- und SVGA-Unterstützung mit VESA-3.0-kompatiblem Videoadapter
- Grafik-RAM: bis zu 256 MByte Grafikspeicher
- Diskettenlaufwerk: 1,44 MByte-Floppy (einem Image oder einem real existierenden Diskettenlaufwerk zugeordnet)
- IDE-Geräte: bis zu vier IDE-Geräte; Festplatte als Image bis zu 2 TByte oder als CD/DVD-ROM-Laufwerk (einem realen Laufwerk oder einer Imagedatei zugeordnet)
- SCSI-Geräte: bis zu 15 SCSI-Geräte (Festplatten als Images bis zu 2 TByte sowie generische SCSI-Geräte)

- Netzwerk: bis zu 16 Netzwerkschnittstellen einschließlich einer virtuellen Netzwerkkarte mit RTL8029 (Bridging auf WLAN-Adapter wird unterstützt)
- Schnittstellen: vier serielle Ports (an Sockets oder Ausgabedateien) und drei bidirektionale parallele Ports, die einer Ausgabedatei, einem echten Port oder einem Drucker zugeordnet sind
- Sound: AC'97-kompatible Soundkarte mit Aufnahmeunterstützung
- Tastatur: generische PC-Tastatur
- Maus: PS/2-Radmaus
- USB: bis zu acht USB-2.0- und bis zu acht USB-1.1-Controller

Wichtig zu wissen: Ein 64-Bit-System kann nur auf einem 64-Bit-Host erzeugt werden. Steckt im Host-Rechner lediglich eine 32-Bit-CPU, geht virtuell auch nicht mehr. Umgekehrt hingegen schon: Ein 64-Bit-Host kann sowohl 64- als auch 32-Bit-Gastsysteme beherbergen. Die virtuellen Maschinen werden auf dem Host-System als ein Bündel von Dateien gespeichert. In den Dateien mit der Endung *.pvs* steckt die Konfiguration der virtuellen Maschinen. Die Festplatten-Images erkennt der Benutzer an der Endung *.hdd*, Diskettenlaufwerks-Images enden auf *.fdd*, Image-Dateien einer CD oder DVD folgen der Unix-Namenskonvention und enden auf *.iso*.

Wird eine virtuelle Maschine auf Stand-by geschaltet, erzeugt Parallels Desktop zusätzlich eine Datei mit dem aktuellen Zustand der Maschine (.sav) sowie ein Speicherabbild (.mem). Falls Sie außerdem noch .txt-Dateien innerhalb einer virtuellen Maschine finden: Das sind weder Release-Infos noch Installationshinweise, sondern die Ausgabedateien für serielle und parallele Ports.

2.6.3 Parallels Desktop unter Windows und Linux installieren

Die Installation von Parallels Desktop ist zumindest unter Windows mit keinerlei Anstrengungen verbunden. Nach wenigen Klicks ist das Programm installiert und lauffähig. Sollte die Hardware nicht ausreichend konfektioniert sein, weist das Programm schon während der Installation darauf hin. Unter Linux gestaltet sich die Installation ähnlich einfach, wenn der Administrator ein paar Dinge berücksichtigt hat: Zum einen werden die Kernel-Entwicklungspakete benötigt; diese heißen unter Red Hat *kernel-<kernel_version>-devel*, auf Debian-Systemen und Derivaten wie Ubuntu sind es die *linux-headers-<kernel_version>*. Außerdem ist der Gnu-C-Compiler erforderlich und dementsprechend auch make oder gmake. Von der Bibliothek glibc wird die 32-Bit-Version 2.3.6 oder höher benötigt. Schließlich benötigt man auf einem 64-Bit-Fedora-10-System noch die 32-Bit-Version des Pakets alsa-plugins-pulseaudio. Darüber hinaus sollte man auf 64-Bit-Linux-Systemen das 32-Bit-Paket alsa-lib (in Red Hat) oder lib32asound (in Debian und -Derivaten) installieren. Sollten die Pakete nicht vorhanden sein, versucht Parallels Desktop während der Installation, diese nachzuladen.

Bist du zu schwach, ist es zu stark: Wenn die Hardware des Host-Systems nicht ausreicht, weist Parallels Desktop bereits während der Installation darauf hin.

Für die Installation unter Linux sind root-Rechte erforderlich. Außerdem benötigen Sie das sogenannte RUN-Installationspaket aus dem Installationspaket von Parallels Desktop auf der Website oder von der Installations-CD. Ein Doppelklick auf das RUN-Paket startet die Installation von Parallels Desktop in einem Terminal. Zunächst sucht das Setup-Programm nach verfügbaren Updates. Tipp: Greifen Sie über einen Proxy-Server auf das Internet zu, und konfigurieren Sie diesen so, dass Parallels Desktop während der Installation nach verfügbaren Updates suchen darf. Einige Klicks später ist die Installation beendet.

Greift der Host-Computer nur über einen Proxy-Server auf das Internet zu, starten Sie die Installation von Parallels Desktop in einem Terminal. Dort suchen Sie das Installationspaket und führen folgenden Befehl aus:

```
sudo ./parallels-desktop-4.0.xxxx.xxxxxx.run --
➥ -p proxy_server_host_name:port
```

oder

```
sudo ./parallels-desktop-4.0.xxxx.xxxxxx.run --
➥ -p ip_address:port
```

Anstelle von *proxy_server_host_name* schreiben Sie den Host-Namen oder im zweiten Befehl anstelle von *ip_address* die IP-Adresse des Proxy-Servers sowie jeweils die Port-Nummer. Sollte für den Proxy-Server eine Authentifizierung erforderlich sein, fordert Parallels Desktop während der Installation noch Ihren Namen und Ihr Kennwort an. Nach der Installation ist nur noch der Aktivierungsschlüssel einzugeben, und schon kann Parallels Desktop gestartet werden; wer das Produkt lediglich testen möchte, kann für die Testversion auch einen kostenlosen Aktivierungsschlüssel anfordern.

2.6.4 Erste Schritte unter Windows und Linux

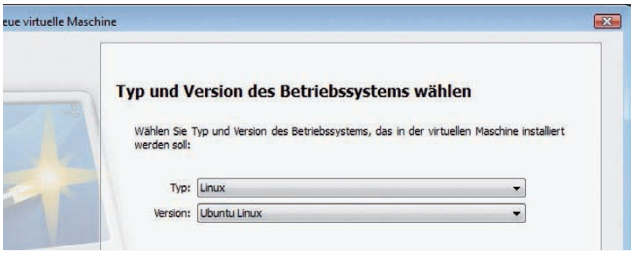
Parallels Desktop wird unter Windows direkt von der Arbeitsoberfläche gestartet, sofern diese Option während der Installation nicht explizit ausgeschaltet wurde. In Linux steht es entweder in einem der Menüs, oder Sie starten es in einem Terminal

mit „parallels-desktop“. Die wichtigsten Funktionen erreicht der Benutzer über die vier Schaltflächen des Programmfensters: virtuelle Maschine erstellen, vorhandene öffnen, virtuelle Maschinen von der Parallels-Website herunterladen und virtuelle Maschinen importieren von Fremdprodukten wie VMware, VirtualPC und VirtualBox.

Nach dem ersten Start: Sehr aufgeräumt präsentiert sich die Oberfläche des Parallels Desktop.

Rechts im Fenster hat man die sehr ausführliche Dokumentation im Zugriff. Leider führt der Link zu den Online-Ressourcen ins Leere; auch eine Suche auf der Parallels-Website bringt den Hilfesuchenden nicht weiter. Die Programmeinstellungen findet der Benutzer im Dateimenü, allerdings sind die Standardvorgaben schon ideal eingestellt und müssen nicht geändert werden.

Universell einsetzbar: Mehr als 30 Betriebssysteme unterstützt Parallels Desktop als Gastsystem.



Ein Klick auf Neue virtuelle Maschine erstellen startet den entsprechenden Assistenten. Im zweiten Fenster wählt der Benutzer das Betriebssystem und den Typ. Zur Wahl stehen *Windows*, *Linux*, *FreeBSD*, *OS/2*, *MS-DOS*, *Solaris* und Andere.

Aus der aufklappbaren Liste Version wählt man danach das gewünschte System. Hier bietet Parallels Desktop:

- elf verschiedene Windows-Version von 3.11 bis Windows 7
- neun Linux-Distributionen – Ubuntu, Fedora, Red Hat, Suse, Debian, CentOS, OpenSuse, Mandriva, Xandros – sowie andere mit 2.4er- oder 2.6er-Kernel
- FreeBSD 4.x bis 7.x
- OS/2 Warp 3 bis 4.5, eComStation 1.1 und 1.2
- MS-DOS 6.22
- Solaris 9 und 10

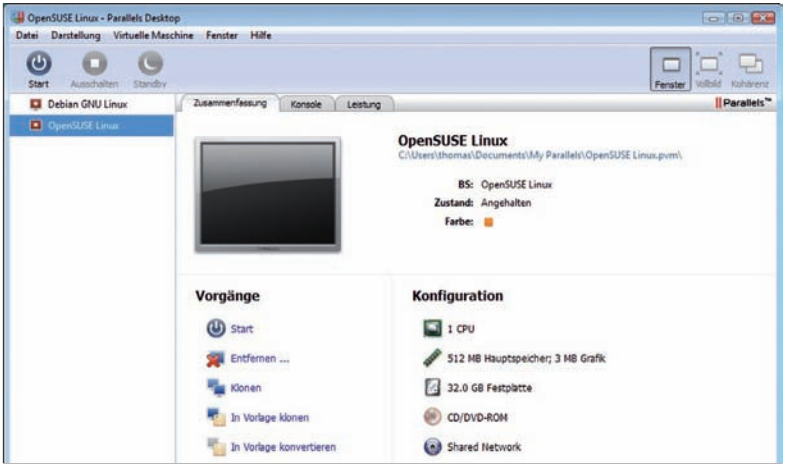
2.5.5 Virtuelle Maschine erzeugen

Im folgenden Schritt lässt der Benutzer eine typische virtuelle Maschine oder eine „Eigene" erzeugen. Wählen Sie Windows als Gastsystem, erscheint außerdem die Option *Windows Express*. Sie erstellt virtuelle Maschinen für Windows Server 2003, Windows XP, Vista oder Windows 7 und installiert das Betriebssystem automatisch; der Benutzer gibt im nächsten Fenster den Windows-Produktschlüssel ein, der während der Installation benötigt wird.

Netzwerkverbindung: Wie kommunikativ Parallels Desktop ist, legen Sie mit dem „Netzwerktyp" fest.

Unter *Eigene* wählt man stattdessen dann die Anzahl der CPUs und legt die Größe des Arbeitsspeichers fest. In Bezug auf die virtuelle Festplatte hat der Benutzer drei Möglichkeiten: Er lädt eine vorhandene, legt eine neue an oder arbeitet ohne Festplatte. Entscheidet er sich für eine neue Image-Datei, definiert der Benutzer im nächsten Schritt den Umfang der Platte und ob diese bis auf die vorgegebene Obergrenze mitwächst oder eine *einfache Dis*k erzeugt wird, die bereits den gesam-

ten Platz bis zur definierten Obergrenze belegt. Soll nicht die gesamte Datei auf einmal geladen werden, schalten Sie die Option *Festplatten-Image in 2-GB-Dateien aufteilen* ein. Das sollten Sie generell bei älteren Betriebssystem machen, die größere Daten nicht unterstützen, oder auch, um die Festplatte auf DVDs zu sichern.



Fertig: Die virtuelle Maschine ist erzeugt, und die Konfiguration wird im Hauptfenster angezeigt.

Nach der Entscheidung über die Festplatte erwartet den Benutzer eine komplexere Aufgabe: Hier wählt er einen Netzwerktyp aus. Zur Wahl stehen:

- Shared Network: Die virtuelle Maschine greift über die Netzwerkverbindungen des Hosts auf Netzwerk und Internet zu.
- Bridged Ethernet: Die virtuelle Maschine erscheint im Netzwerk als eigenständiger Computer.
- Host-exklusiv: Die neue virtuelle Maschine kann nur auf andere virtuelle Maschinen auf demselben Rechner sowie auf den Host zugreifen.
- Kein Netzwerk

Anschließend wählen Sie die Netzwerkschnittstelle und optimieren die Leistung entweder für die virtuelle Maschine oder den Host-Computer. Dann bekommt das Baby noch einen Namen und kann erstellt werden. Legen Sie auf Anforderung die Installations-CD oder -DVD des Gastsystems ein. Anschließend erscheint das Hauptfenster, in dem die Konfiguration des Gastsystems zusammengefasst ist. Mit Start starten Sie die Installation und später dann das Betriebssystem.

Thomas Hümmler

2.7 Workshop – VMware vCenter Operations einfach konfigurieren

Zur Verwaltung seiner virtuellen Systeme liefert VMware das vCenter. Bei diesem Produkt liegt der Fokus auf Infrastruktur und Technik. Das vCenter zeigt aber die virtuellen Systeme aus der Sicht der Server, der Netzwerke, des Speichers und der virtuellen Maschinen. Es liefert somit einen Einblick in die Infrastruktur der IT-Systeme in Hinblick auf die geschäftlichen Anforderungen. Hierzu liefert VMware (www.vmware.com/de/) nun eine Erweiterung: die vCenter Operations.

In den vCenter Operations lenkt VMware die Szenerie auf die geschäftliche Seite der IT-Nutzung und schlägt die Brücke zwischen der technischen Sichtweise der Infrastruktur und den Blick, den die Fachbereiche benötigen. So können beispielsweise alle virtuellen Maschinen, die einem bestimmten Bereich zugeordnet sind, zusammen überwacht und verwaltet werden.

In den Standardfunktionen des vCenters hingegen erfolgt die Gruppierung immer nach dem einzelnen Datacenter. In den vCenter Operations wird dieses „Manko" der Gruppierung aufgebrochen. Dies gilt allerdings nur für die Überwachung; die Position der virtuellen Maschinen bleibt davon unberührt.

2.7.1 Details zum Einrichten von vCenter-Operations

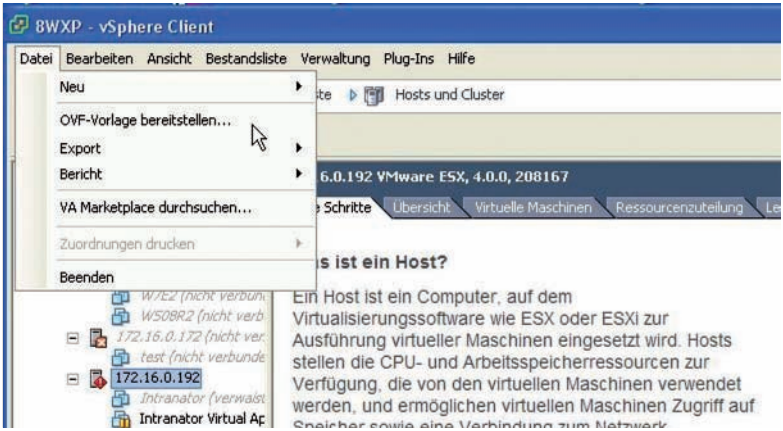
Für diesen Workshop haben wir die aktuelle Version der vCenter Operations auf einem bestehenden vCenter eingerichtet. Im folgenden Beitrag zeigen wir das Setup, die Konfiguration und die Bedienung der vCenter Operations.

Installationsdatei: Die vCenter Operations sind als OVA-Datei von der VMware-Website zu beziehen.

Die vCenter Operations werden von VMware als OVA-Datei angeboten. Die Dateierweiterung steht für Open Virtualization Appliance. OVAs beinhalten eine fertig konfigurierte virtuelle Maschine, die direkt in Betrieb gehen kann. Der von Windows bekannte Setup-Prozess entfällt somit. OVA-Files stellen eine Weiterentwicklung der OVF-Datei (Open Virtualization Format) dar. Das OVF-Format wurde von VMware entwickelt, um einen Standard für virtuelle Maschinen zu schaffen. Eine OVF-Datei besteht aus der virtuellen Maschine und der Beschreibung. Das OVA-Format geht weiter. Hier erhalten Sie bereits eine fertige virtuelle Maschine als Appliance. Da es sich dabei aber immer noch um eine virtuelle Maschine handelt, wird sie als virtuelle Appliance bezeichnet. Der Begriff Appliance soll dabei lediglich ausdrücken, dass diese virtuelle Maschine sofort in Betrieb gehen kann, vergleichbar mit einer entsprechenden physischen Appliance.

2.7.2 Die ersten Installationsschritte

Um die vCenter Operations Appliance in das vCenter zu integrieren, gehen Sie wie folgt vor: Rufen Sie als Erstes den *Virtual Infrastructure Client* auf. Hierzu bauen Sie zuerst eine Verbindung mit Ihrem vCenter Server auf. Dabei müssen Sie sich erst einmal authentifizieren. Selektieren Sie dann im *Virtual Infrastructure Client* die Zielumgebung mit dem ESX-Host, in dem Sie die virtuelle Appliance einhängen wollen. Rufen sie danach im *Virtual Infrastructure Client* die Option *Datei / OVF-Vorlage bereitstellen* auf. Über diese Option wird auch die OVA-Datei eingebunden. Bei der Frage nach der Quelle der OVF-Datei geben Sie den Pfad auf Ihre OVA-Datei an. Bestätigen Sie die weiteren Angaben im Assistenten und geben bei der Frage nach dem Netzwerk ihre Verbindung an.



Integration: Um die Hauptkonsole der VMware vCenter Operations aufzurufen, benötigen Sie den „Virtual Infrastructure Client". Unter „Lösungen und Anwendungen" befindet sich der Link auf „vCenter Operations Standard".

Anschließend präsentiert Ihnen der Assistent nochmals die gewählten Einstellungen. Diese können Sie bestätigen. Im Anschluss daran finden Sie eine neue virtuelle Maschine in der vorher gewählten Umgebung: die virtuelle Appliance mit den vCenter Operations. Die neue Appliance können Sie wie jede andere virtuelle Maschine starten, stoppen oder anhalten.

2.7.3 Virtuelle Appliance starten und konfigurieren

Wenn Sie die virtuelle Appliance starten, können Sie den Startvorgang in der Konsolenansicht der virtuellen Maschine verfolgen. Bei der Appliance handelt es sich um ein Suse-Linux-Derivat (Suse Linux Enterprise Server 11 SP1 für VMware).

Nach dem Start sehen Sie ein einfaches Kommandozeilen-Interface mit den drei Optionen zum Login, zur Konfiguration des Netzwerks sowie zu den Einstellungen der Zeitzone. Über das Login melden Sie sich bei der Appliance, dem Suse-Derivat, an. Sie können dann die von Linux bekannten Befehle absetzen. Ferner müssen Sie nun das Netzwerk für Ihre Appliance einrichtet. Rufen die dazu die Option *Configure Network* auf.

Im Rahmen des Workshops haben wir der Appliance eine statische IPv4-Adresse zugewiesen. Wenn Sie einen DHCP-Server im Einsatz haben, können Sie jedoch die IP-Adresse dynamisch zuweisen lassen. Über diese IP-Adresse ist die Appliance später zu erreichen. Sie müssen außerdem die Netzmaske, das Gateway, den DNS-Server und den Host-Namen angeben. Damit ist die Netzwerkkonfiguration der Appliance abgeschlossen. Für alle weiteren Aktionen können Sie einen entsprechenden Browser wie Firefox oder Internet Explorer verwenden.

2.7.4 Virtuelle Appliance konfigurieren

Für die weitere Konfiguration der Appliance der vCenter Operations öffnen Sie Ihren Browser. Geben Sie in der Adresszeile des Browser entweder den Namen oder die IP-Adresse ein. Der Zugriff erfolgt via https. Als Port geben sie *5480* ein:

```
https://IP-Adresse-Ihrer-Appliance:5480/
```

Beim Aufbau der Verbindung erhalten Sie einen Hinweis nach dem Sicherheitszertifikat der Website. Für einen ersten Test können sie diese ignorieren und das „Laden der Website fortsetzen". Anschließend sehen Sie eine Verwaltungsmaske, die mit „VMware vCenter Operations" umschrieben ist; hier können Sie sich nun anmelden. Die VMware-vCenter-Operations-Konsole ermöglicht eine generelle Verwaltung der Appliance mit allen Einstellungen, nun aber erstmals in grafischer Form. In der Konsole finden Sie drei Reiter, die mit *System, Network* und *Appliance Administration* umschrieben sind. Unter Network finden Sie beispielweise wieder die bereits vorher vorgenommenen Netzwerkeinstellungen, ebenso einen Statusbildschirm zum aktuellen Zustand der Appliance. Die Einstellungen in diese Konsole sind nicht komplex, sondern einfach und überschaubar. Trotzdem sollten Sie mit ihnen vertraut sein, entsprechende Vorkenntnisse besitzen oder sich solche aneignen. Wenn diese Basiskonfiguration abgeschlossen ist, müssen Sie die zu überwachenden vCenter-Server hinzufügen. Dies erfolgt im nächsten Abschnitt.

2.7.5 Die zu überwachenden Zielsysteme integrieren

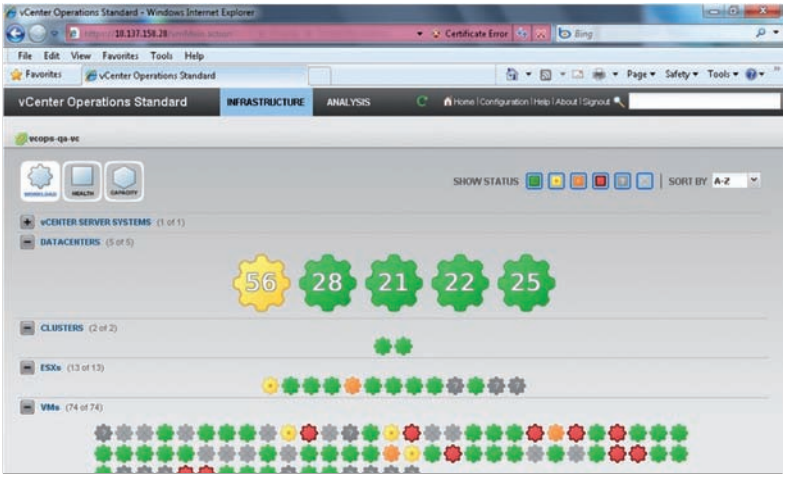
Nach der Basiskonfiguration der vCenter Operations Appliance müssen Sie der Anwendung die Zielsysteme bekannt machen, also die durch die Appliance überwachten vCenter Server. Dazu stellt Ihnen das Softwaresystem eine weitere Konsole bereit. Um in diese Konsole zu gelangen, verwenden Sie ebenfalls einen Browser.

Geben Sie in die Adresszeile die IP-Adresse der vCenter Operations Appliance ein – aber diesmal ohne die Port-Angabe. Besser geht es natürlich mit dem Namen des System und der Auflösung via DNS. Anschließend öffnet sich eine Maske, die als *vCenter Operations Standard* umschrieben ist. Melden Sie sich bei dieser Maske nun an und geben Sie ein wenig später die zu überwachenden vCenter-Server an.

Dabei müssen Sie auch die Berechtigungen für den Zugriff darauf bereitstellen. Das System meldet, wenn Sie Ihren vCenter Server erfolgreich hinzugefügt haben. Außerdem müssen Sie noch die entsprechende Lizenz bereitstellen, die Sie von der VMware-Website erhalten haben (www.vmware.com/de/). Wenn alles korrekt ist, können Sie die Konfiguration des Operations Center abschließen. Alle folgenden Arbeiten werden über die eigentliche Hauptkonsole, das Operations Center, vorgenommen. Dies erläutern wir in den folgenden Kapiteln.

2.7.6 Mit VMware vCenter Operations arbeiten

Um in die Hauptkonsole der VMware vCenter Operations aufzurufen, benötigen Sie den „Virtual Infrastructure Client". Sofern Sie diesen nicht vorher geschlossen haben, müsste er ohnehin noch offen sein. Über den „Virtual Infrastructure Client" erfolgt die Verwaltung des vCenters und der ESXi-Server. Bewegen Sie sich über die Navigationszeile des „Virtual Infrastructure Client" in den Bereich *Home*. Hier finden Sie die *Bestandliste*, einen Bereich *Verwaltung*, einen weiteren Bereich für das *Management* sowie ganz unten *Lösungen und Anwendungen*. Darunter befindet sich auch ein Link auf *vCenter Operations Standard*, den Sie nun betätigen sollten. Darüber gelangen Sie in die Überwachungskonsole.



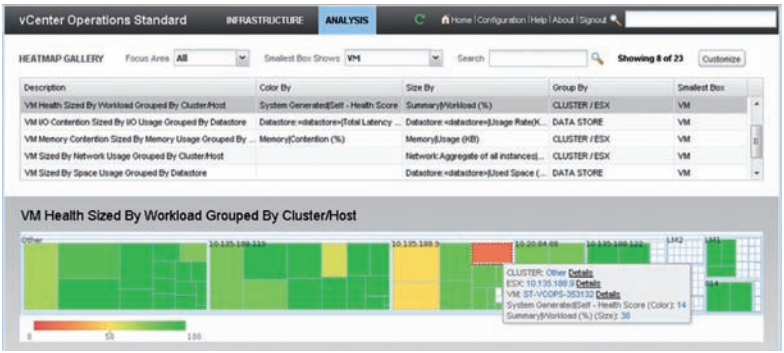
Übersichtlich: vCenter Operations umfasst eine grafische Anzeige der vSphere-Struktur.

Wenn Sie die vCenter Operations neu eingerichtet haben und erstmals aufrufen, sind die Inhalte noch leer. Das liegt daran, dass das System zuerst Daten sammeln muss, um diese dann zu präsentieren. Die vCenter Operations dienen in erster Linie der langfristigen Analyse, der Trendanalyse und der Überwachung der Kapazitäten, der Performance und der Konfiguration. All dies erfordert aber eine Datenbasis, die erst gesammelt werden muss. Gewonnen werden diese Daten aus den Informationen des vCenter-Servers, den Sie vorher angemeldet haben.

2.7.7 Die Konsole der vCenter Operations

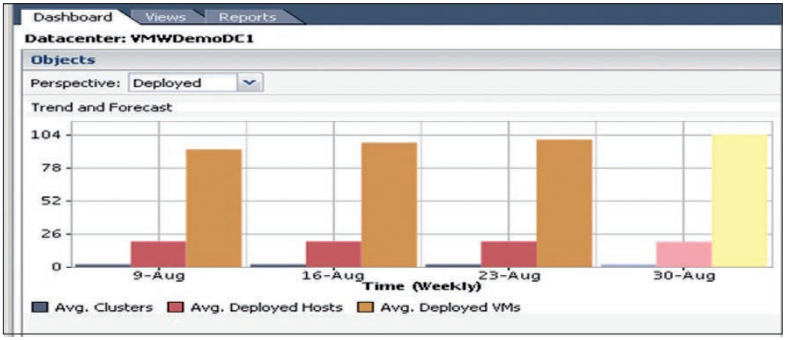
Die Konsole der vCenter Operations unterscheidet zwei zentrale Verwaltungsbereiche: den Blick auf die Infrastruktur und die Analyse der Daten. Analog dazu finden Sie zwei entsprechende Reiter im oberen Bereich der Konsole.

Bei der Wahl der Infrastruktur sehen sie im Hauptfenster die Einträge zu *vCenter Server Systeme*, *Datacenter*, *Cluster*, *ESXi* und *virtuelle Maschinen*. Diese Gruppierung ist der des vCenter Servers ähnlich. Der Bezug zu den Basisgruppierungen des vCenters und dessen Ansicht bleiben dabei ebenfalls erhalten.



Systemanalyse: Der „Analysis"-View liefert einen etwas anderen Blick auf die Systeme. Hierbei geht es um die Verfügbarkeit („Health") der virtuellen Systeme.

In der vCenter-Operations-Konsole sehen Sie links die Struktur der virtuellen Systeme in der vCenter-Darstellung. Es ist vor allem die Darstellung, durch die sich die vCenter Operations vom Standard-vCenter unterscheiden. Eine breite Palette an farbigen Schaubildern und Objekten liefert einen schnellen Überblick zur aktuellen Situation und Auslastung der Systeme. Die Anzeigen und das Dashboard der vCenter Operations sind auf schnelle und kompakte Übersicht getrimmt. Anzeigen in Ampelfarben zeigen den Ist-Zustand. Wenn notwendig, lassen sich aber auch die Details mit Zahlenwerten und Prozentangaben zur Auslastung der Systeme einblenden.



Systemauslastung: vCenter-Operations dient der Kapazitätsplanung und somit der Optimierung der Ressourcennutzung.

Die vCenter Operations umfassen drei zentrale Funktionsbereiche. Dazu gehört die Analyse der Performance einer vSphere-Infrastruktur. Eingeschlossen sind auch Anzeigen zur Auslastung der CPU, des Speichers, der Platten und des Netzwerks. Der zweite Funktionsblock der vCenter Operations soll die Konfiguration einer vSphere-Struktur vereinfachen. Der dritte Zweig der vCenter Operations dient der Kapazitätsplanung und somit der Optimierung der Ressourcennutzung und deren Zuweisung an die virtuellen Systeme. Zu den überwachten Parametern zählen die Auslastung der CPU und des Speicher sowie die Plattenzugriffe. Spitzenwerte (Peaks) werden erkannt und dargestellt. Die Grafiken liefern einen Überblick zur Auslastung der Platten oder der Netzwerk-Interfaces. Die Überwachungs- und Anzeigezeiträume lassen sich an die eigenen Anforderungen anpassen. Langzeitauswertungen ergänzen die Ad-hoc-Überwachung.

Hilfreich: Zur Analyse der Auslastung der Systeme und deren nachfolgenden Optimierung hat VMware auch ein Self-Learning-Verfahren implementiert. Durch Trendanalysen sollen künftige Engpässe erkannt werden.

Durch Automatismen und Policies sollen viele Verwaltungsaufgaben ohne Administratoreingriffe stattfinden. Zur Analyse der Auslastung der Systeme und deren nachfolgenden Optimierung hat VMware mehrere Techniken, wie etwa ein Self-Learning-Verfahren, implementiert. Durch Trendanalysen sollen künftige IT-Engpässe in einem Unternehmen erkannt werden, sodass der IT-Verantwortliche entsprechende Maßnahmen einleiten kann.

Johann Baumeister

2.8 Workshop – Mit VMware vSphere ein virtuelles Datacenter aufbauen

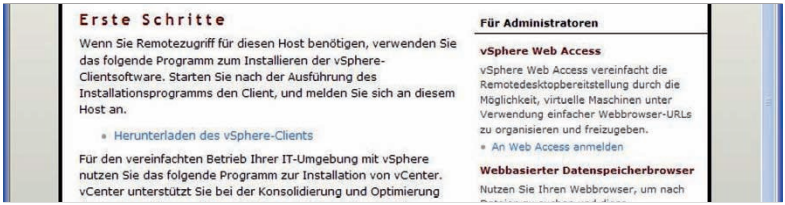
vSphere ist der Sammelbegriff von VMware (www.vmware.com/de/) für eine Reihe von Produkten zur Servervirtualisierung und der korrespondierenden Verwaltung. Zu diesen Produkten gehören all jene Tools und Hilfen, die für die Virtualisierung im Rechenzentrum notwendig sind. Die Zielsetzung von vSphere liegt in der Schaffung einer Infrastruktur für die Virtualisierung der gesamten IT und deren Geschäftsanwendungen. Diese Konzept ist gänzlich anders, als es bei der „punktweisen" Virtualisierung einzelner Anwendungen oder der virtuellen Nachbildung von Applikationen in Testumgebungen der Fall ist. Um das zu erreichen, integriert VMware in vSphere eine Reihe von Bausteinen, mit denen die Rechnerhardware in den Rechenzentren besser und umfassender verwaltet werden kann.

Die Basis dabei wird durch die Infrastruktur-Services gebildet. Dazu gehören alle Komponenten zur Virtualisierung der Rechenleistung, des Speichers und der Netzwerkanbindung. Die Virtualisierung der Rechenleistung erfolgt beispielsweise durch den ESX- oder ESXi-Server. vSphere bündelt all diese Ressourcen der Infrastruktur-Services in Pools. Aus diesen Pools werden die Ressourcen den Anwendungen nach Bedarf und geschäftlicher Priorität zugewiesen.

In diesem Workshop zeigen wir, wie Sie mithilfe von vSphere Datacenter schnell und unkompliziert ein virtuelles Rechenzentrum erstellen können.

2.8.1 vCenter als Managementzentrale

Als zentrale Verwaltungsinstanz für eine vSphere-Installation fungiert das vCenter, Es basiert auf dem zentralen Managementserver und einer Verwaltungskonsole, dem vSphere-Client. Der vCenter Server kommuniziert über eine API mit den überwachten ESX/ESXi-Hypervisoren. vSphere-Client und vCenter-Server können zusammen auf dem gleichen Server eingerichtet werden, müssen aber nicht.



Gut zu wissen: VMware liefert zur Verwaltung einer vSphere-Infrastruktur den kostenfreien vSphere-Client. Entweder nutzt man diesen, um damit direkt auf einen ESX-Host zuzugreifen, oder es wird der vCenter-Server dazwischengeschaltet. Sowohl der vSphere-Client als auch das vCenter können direkt von einem laufenden ESX-Server geladen werden. Dazu ist eine Verbindung zu ihm über seine IP-Adresse aufzubauen. Beim Einsatz des vCenters sind kostenpflichtige Zugriffslizenzen zu erwerben.

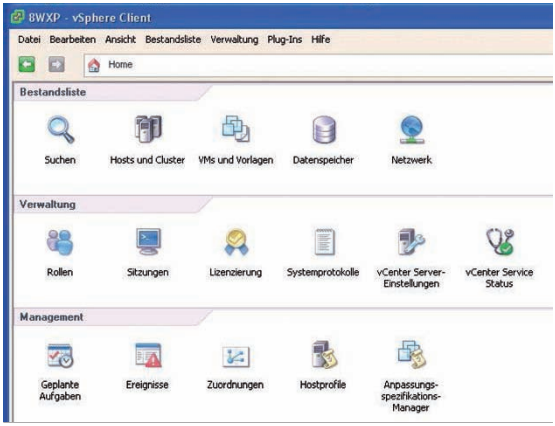
Der vSphere-Client benötigt als Laufzeitumgebung einen Browser. Er kann damit auf jeglichem Rechnersystem, das einen Browser aufweist, eingerichtet werden. Auch der vSphere-Client kommuniziert mit seinem vSphere-Server über eine VMware-eigene API. Der VMware vCenter Server bietet eine skalierbare und erweiterbare Plattform, die die Grundlage bei der Verwaltung von VMware-Szenarien bildet. Das vCenter ermöglicht dem Administrator ein einheitliches Management der Hosts und deren virtueller Maschinen über eine einzige Konsole. Eingeschlossen ist ferner die Überwachung der Rechenleistung und des Datendurchsatzes von Clustern, Hosts und virtuellen Maschinen. Darüber hinaus liefert der vCenter-Server einen Überblick über den Status und die Konfiguration von Clustern, Hosts, virtuellen Maschinen, dem Speicher, den Gastbetriebssystemen und vielen anderen Komponenten einer vSphere-Infrastruktur.

2.8.2 Die Verwaltungsobjekte von vSphere

Die Verwaltung einer vSphere-Infrastruktur hat VMware in mehrere Bereiche unterteilt. Dies sind etwa die Hardwareressourcen, die virtuellen Maschinen, Überwachungshilfen, Konfigurationsbildschirme oder die Ereignisse.

Etwas verwirrend mögen zu Beginn die unterschiedlichen Anzeigen und Gruppierungen in der vCenter-Konsole sein. So finden Sie beispielsweise in der obersten Menüzeile eine Gruppierung, die unter anderem die Einträge Datei, Bestandsliste und Verwaltung umfasst. Eine Zeile tiefer ist die Navigationszeile. Hier finden sich ähnliche Gruppierungen, aber auch andere Objekte wieder. Wenn Sie in der Navigationszeile auf Home klicken, so sehen Sie im Fenster darunter drei Bereiche mit den Begriffen Bestandsliste, Verwaltung und Management. Die Rubrik Bestandliste und Verwaltung ist auch in der Menüzeile zu sehen, nicht aber das Management. Hier sollten Sie sich zuerst einen Überblick verschaffen.

Details: Die Objektliste des vCenters ist bedeutend umfangreicher als jene eines einzelnen ESX-Servers. Das vCenter umfasst alle Möglichkeiten zur Verwaltung. Es kennt viele Verwaltungsobjekte und ist – verglichen mit dem direkten Zugriff des vSphere-Clients auf den ESX-Server – weitaus flexibler. In der Bestandsliste werden die zentralen Ressourcen einer vSphere-Infrastruktur zusammengefasst.



Ein zentraler Begriff beziehungsweise eine Option ist generell die *Bestandsliste*. Darunter fasst VMware die folgenden Objekte zusammen:

- **Host:** Dies sind die physischen Rechnersysteme, die durch den VMware-Hypervisor verwaltet und kontrolliert werden. Dabei kommen derzeit die Serversysteme ESX und ESXi zum Einsatz.
- **Cluster:** Ein Cluster ist ein Verwaltungsobjekt, das mehrere Hosts zusammenfasst. Es dient in erster Linie der Ausfallsicherheit der physischen Hosts und somit auch der darauf befindlichen virtuellen Gäste.
- **Virtuelle Maschinen:** Virtuelle Maschinen sind die Gäste des Hosts. Dabei werden die Rechner virtuell nachgebildet, weshalb man von der virtuellen Maschine spricht.
- **Vorlagen:** Vorlagen dienen der schnelleren Erzeugung von virtuellen Maschinen.
- **Datenspeicher:** Der Datenspeicher beschreibt den physikalischen Plattenspeicher. Er wird für die Ablage der virtuellen Maschinen, maber auch der Daten benötigt
- **Netzwerk:** Hiermit sind die Netzwerkverknüpfungen in den virtuellen Maschinen und nach draußen zu den weiteren physischen Servern gemeint.

2.8.3 Das Datacenter von vSphere

Datacenter ist ein Container für die von vSphere verwalteten Objekte. Dies sind in erster Linie die Hosts und virtuellen Maschinen. Aber auch Cluster und Ordner werden immer einem Datacenter zugeordnet. Datacenter werden immer unter dem Root-Ordnerobjekt der *Bestandsliste, Hosts* und *Cluster* im vCenter verwaltet.

Start: Nach dem Setup des vSphere-Clients erfolgt über diesen die Anmeldung am ESX-Server oder vCenter. Hierzu ist entweder die IP-Adresse oder der Name des ESX-Hosts beziehungsweise des vCenter bereitzustellen. Anschließend werden die Bestandsliste, die Plug-Ins und das Hauptformular für die Verwaltung geladen.

Um ein Datacenter zu erzeugen, gehen Sie wie folgt vor: Melden Sie sich am vCenter Server an. Datacenter stehen nicht zur Verfügung, wenn Sie direkt mit einem ESXi-Host verbunden sind, denn das Datacenter ist ein Verwaltungsobjekt des vCenters. Selektieren Sie den Root-Ordner in der *Bestandsliste* und klicken dann auf *Datei*, anschließend *Neu* und darunter *Datacenter*. Geben Sie zum Schmuss dem Datacenter einen Namen. Das Datacenter ist, wie erwähnt, nur ein Container,

es hat neben dem Namen keine weiteren Konfigurationsmerkmale. Sämtliche Attribute wie Ausfallsicherheit, Backup-Verfahren oder die Güte (Quality-of-Service), die man oftmals in SLAs niederschreibt und einem physischen Datacenter zuordnen würde, finden Sie hier jedoch nicht. All diese weiteren Eigenschaften des Datacenters müssen über zusätzliche Produkte von VMware oder von Drittherstellern separat verwaltet werden.

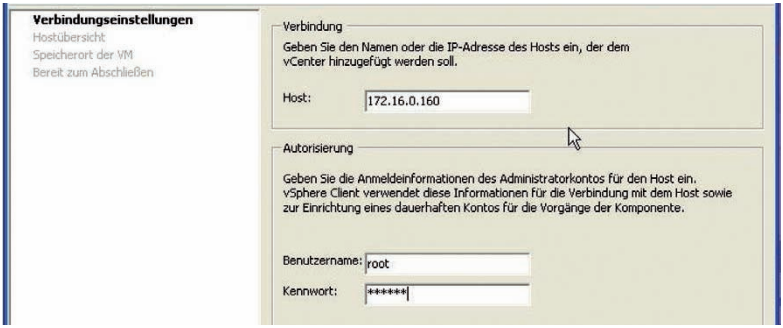
Die Anzeigen im Hauptfenster rechts unten sind kontextsensitiv. Sie ändern sich in Abhängigkeit vom gewählten Objekt. Wenn Sie beispielsweise ein Datacenter selektieren, sehen Sie unter dem Reiter *Übersicht* die wichtigsten Informationen und Verwaltungsaktionen dazu eingeblendet. Im Bereich *Allgemein* finden sich die Angaben zur Serverhardware, unter *Ressource* wird über die Auslastung der CPU, des Arbeitsspeichers und des Plattenspeichers informiert. Unter dem Reiter *Netzwerk* werden die Netzwerkverknüpfungen und virtuellen Switches verwaltet.

2.8.4 Integration der Hosts in das Datacenter

Das Datacenter ist, wie erwähnt, eine leere Verwaltungshülle. Zu den ersten Aufgaben, nach dem Einrichten des Datacenter gehört die Integration der vSphere-Hosts (der ESX- beziehungsweise ESXi-Server). Dies sollten Sie nun durchführen.

Wichtig: Das Datacenter ist die oberste Verwaltungsinstanz für alle vSphere-Objekte. In das Datacenter werden die Hosts eingefügt. Im Bild sehen Sie vier Hosts, die über ihre IP-Adresse identifiziert werden.

Um einen Host zur Verwaltung in den Kontext des vCenter hinzuzufügen, rufen Sie den Assistenten *Host hinzufügen* auf. Selektieren Sie dazu das Datacenter, in das sie den Host einfügen wollen, und klicken anschließend mit der rechten Maustaste. Nun öffnet sich das Kontextmenü des Datacenters. Darin finden Sie unter anderem die Einträge *Neuer Ordner, Host hinzufügen* und *Neue virtuelle Maschine*. Das bedeutet, dass Sie all diese Objekte direkt unter Ihr Datacenter einhängen können. Wenn Sie Ihr Datacenter durch einen Cluster gegen Ausfälle absichern wollen, sollten Sie zuerst einen Cluster erzeugen. Um einen Host in das Datacenter einzuhängen, rufen Sie die zugehörige Option auf. Daraufhin öffnet sich ein Assistent. Dieser fragt alle notwendigen Verwaltungsparameter in einer Dialogfolge ab.



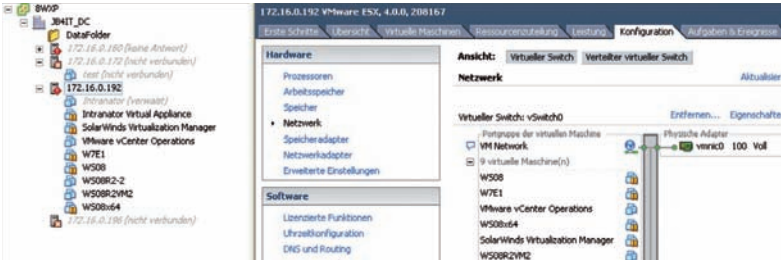
Unterstützung: vSphere vereinfacht die Verwaltung durch eine Vielzahl an Assistenten. Um beispielweise einen Host hinzuzufügen, ist der Assistent Host hinzufügen aufzurufen. Dieser fragt alle notwendigen Verwaltungsparameter in einer Dialogfolge ab.

Dazu gehören die IP-Adresse oder der Name des ESX-Hosts, die Zugriffsberechtigungen, die Lizenzangaben und der Cluster, in den der Host eingefügt werden soll.

Am Ende der Dialogfolge *Host hinzufügen* zeigt der Assistent nochmals alle gewählten Parameter des Hosts. Anschließend wird der Host in die Verwaltungsumgebung des vCenters eingefügt.

2.8.5 Netzwerkkommunikation intern und extern

Damit die virtuellen Maschinen untereinander und mit der Außenwelt kommunizieren können, benötigen sie eine Netzanbindung.



Kontaktaufnahme: Zur Netzwerkkonfiguration unter vSphere werden virtuelle Switches eingerichtet. Diese werden mit den virtuellen Maschinen auf der einen Seite und den physischen Netzwerkkarten auf der anderen Seite verbunden.

Dafür sind die Funktionen in vNetwork von vSphere zuständig. Die Dienste in vNetwork helfen bei der Bereitstellung, Administration und Kontrolle von Netzwerkfunktionen virtueller Maschinen in VMware-vSphere-Umgebungen. Um ein

Netzwerk im vCenter zu verwalten, müssen Sie zuerst einen Netzwerkadapter bereitstellen und anschließend ein Netzwerk konfigurieren. Bei dem Netzwerk handelt es sich im Grunde um einen virtuellen Switch.

Wichtige Details: Unter dem Reiter Konfiguration verbergen sich alle allgemeinen Einstellungen, die den Server betreffen, also eine allgemeine Statusüberwachung sowie Angaben zu Prozessoren, Arbeitsspeicher, Netzwerk, und Netzwerkadaptern.

Um einem Host ein Netzwerk zuzuordnen, müssen Sie ihn selektieren und dann den Reiter *Konfiguration* aktivieren. Unter dem Fenster Hardware sehen Sie dann die Einträge *Netzwerkadapter* und *Netzwerk*. Über diese beiden Links erfolgt die Konfiguration Ihrer Netzwerkkarte und des virtuellen Netzwerk-Switches.

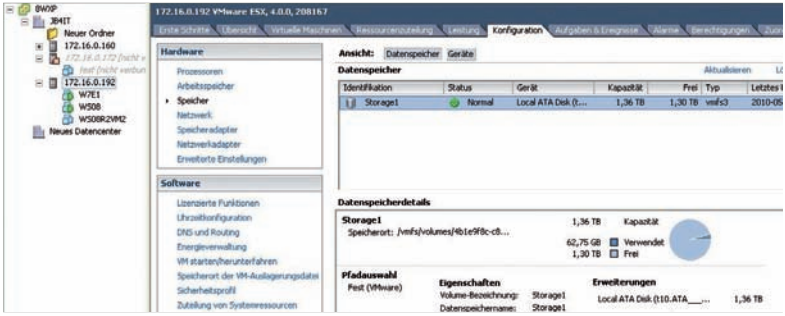
2.8.6 Zugriff auf den Plattenspeicher konfigurieren

Die Bereitstellung von Plattenspeicher läuft in zwei Schritten ab. Lokalen Plattenspeicher (Direct Attached Storage) verwalten Sie direkt unter der Rubrik *Storage*.

Storage-Anbindung: Die Verwaltung der Speicheranbindungen erfolgt im Bereich Konfiguration.

Um Ihrem ESX-Host-Plattenplatz zur Verfügung zu stellen, selektieren Sie den Host und dann den Reiter *Konfiguration*. Die Verbindung zu einem externen Speicher wird über den Link *Speicheradapter* konfiguriert. Die Verwaltung des Speichers und die Zuweisung zu vSphere erfolgen über den Eintrag Speicher. Unter

dem Fenster Hardware sehen Sie nun die Links *Speicher* und *Speicheradapter*. Über diese beiden Links erfolgt die Konfiguration Ihres Speichers.



Weitere Hinweise: Die Informationen zu den bereitgestellten Datenspeichern können unter der Konfiguration der Speicher ausgelesen werden.

Um externen Speicher wie iSCSI-Speicher oder Fibre-Channel-Speicher einzubinden, müssen Sie zuerst einen *Speicheradapter* konfigurieren.

2.8.7 Virtuelle Maschinen erstellen

Nach der Konfiguration des Speichers und der virtuellen Switches können Sie Ihre virtuellen Maschinen erzeugen. Dazu sollten Sie den Assistenten zur Erzeugen der virtuellen Maschinen aufrufen. Dieser verlangt unter anderem Angaben zu dem Betriebssystem der virtuellen Maschine, dem Speicherplatz für das Dateisystem (der VMDK-Datei), der Anzahl der CPUs, der Größe des Arbeitsspeichers, den die virtuelle Maschine erhalten soll, den USB-Schnittstellen und den vorher erzeugten Netzwerk-Interfaces. VMware vSphere unterstützt eine Vielzahl von virtuellen Gastbetriebssystemen. Dies umfasst alle gängigen Windows-Systeme, Novell Netware, Solaris und die meisten gängigen Linux-Derivate.

2.8.8 Fazit

Der vCenter Server umfasst alle Vorkehrungen, die erforderlich sind, um eine vSphere-Infrastruktur schnell und effizient zu verwalten. Das vCenter verwaltet die IT-Ressource, wie die Server, den Speicher und die Netzwerke. Es kennt darüber hinaus auch die virtuellen Strukturen mit den virtuellen Maschinen. Über Cluster werden diese Systeme gegen Ausfälle abgesichert. Als Rahmenwerk für all diese Objekte dient das Datacenter. Das vCenter erlaubt somit eine Verwaltung einer komplexen virtuellen IT-Struktur auf Basis von VMware vSphere.

Johann Baumeister

3 Cloud

Cloud Computing ist bei Unternehmenslösungen in aller Munde. Anwendungen, Rechenleistung und Speicherplatz wird von unternehmenseigenen Servern und PCs zu Providern verlegt. Durch die Verlagerung in die Cloud lässt sich die gebündelte Leistung einer dezentralen IT-Infrastruktur nutzen. Große Vorteile ergeben sich für die Bereitstellung und Skalierung von IT-Anwendungen.

3.1 Die Fallen bei Virtualisierung und Cloud

Die Analysten von Forrester (www.forrester.com) haben eine Studie mit dem Titel „2011 Top 10 IaaS Cloud Predictions For I&O Leaders" veröffentlicht (www.forrester.com/rb/Research/2011_top_10_iaas_cloud_predictions_for/q/id/58779/t/2). Darin sprechen sie davon, dass ein neuer Typ von hoch motivierten Spezialisten gebraucht wird, die mit ihrem Know-how und ihren Erfahrungen prädestiniert sind, bahnbrechende Entscheidungen für die Unternehmens-IT zu treffen. Denn die IT steht insgesamt vor einer Wende, wie sie zuletzt mit dem Übergang zu Client/Server-Netzen oder zum Internet stattfand.

Dienste	Angebote	Zielgruppe
	SaaS - Software as a Service	
Anwendungen	Microsoft Online Services (BPOS) Google Apps for Business CRM-Online (Salesforce, WebEx)	Konzerne, Großunternehmen, Mittelstand
	Microsoft Live Services Google Docs	Privatpersonen, Selbstständige
	PaaS - Platform as a Service	
Basis- Technologie	Microsoft Azure Service Google App Engine Force.com	IT-Planer, Integratoren, Entwickler
	IaaS - Infrastructure as a Service	
IT-Infrastruktur und Hardware- Komponenten	Amazon EC2 Micosoft Windows Azure Platform HP Cloud Enabling Computing Sun Cloud AppNexus	IT-Abteilungen, IT-Dienstleister

Cloud-Ebenen: Die drei Ebenen von Cloud-Services mit IT-Leistungen und adressierten Zielgruppen.

Immer mehr Unternehmen müssen sich nicht fragen, ob, sondern wann und wie sie ihre Infrastruktur auf neue Virtualisierungs- oder Service/Cloud-Konzepte umstellen wollen. Tun sie es gar nicht, laufen sie Gefahr, dass ihre IT nicht mehr konkurrenzfähig ist. Da der Wechsel zudem mit einigen technologischen Hürden und Gefahren aufwartet, steigt die Nachfrage nach Virtualisierungs- und Cloud-Spezialisten. Unternehmen sollten rechtzeitig nach Mitarbeitern Ausschau halten, die die neuen Technologien beherrschen, und damit die Unternehmens-IT um-

bauen. Dass IT-Verantwortliche in Sachen Cloud und Sicherheit eine gewisse Skepsis plagt, ist nur allzu verständlich.

Der Beitrag „Sicherheitsrisiken beim Cloud Computing reduzieren“ (Webcode **2031300**) beschäftigt sich eingehend mit der Problematik.

3.1.1 Interne Clouds bauen, auch wenn sie scheitern

Nach Ansicht von Forrester sind externe Cloud-Angebote zurzeit konkurrenzlos günstig. Dennoch sollten Unternehmen interne Serviceportale aufbauen, bei denen sich Abteilungen oder einzelne Mitarbeiter nach dem Utility-Abrechnungsmodell Applikations- und Rechenleistung für eine bestimmte Periode besorgen können. Die virtualisierten Server- und Storage-Ressourcen mit ihren leicht verschiebbaren und einfach zu klonenden Anwendungen erlauben schon jetzt solche Verfahren. Selbst wenn diese Infrastruktur erst teilweise gegeben und die Security- und Billing-Tools noch unausgereift sein sollten, werden sich die Anstrengungen langfristig lohnen, meint Forrester, frei nach dem Motto „Aus Fehlern lernen“.

Der Ansatz ist dennoch so revolutionär, dass sich die Unternehmen schon jetzt auf ihn vorbereiten sollten. Cloud verschiebt die IT von proprietären (und teuren) Silo-Architekturen in Richtung Standardisierung und leistungsbezogene Automatisierung. Alle bestehenden Ressourcen sollen in Pools zusammengefasst und auch intern nur nach wirklicher Nutzung verrechnet werden. Der notwendige Managementaufwand und seine Bewältigung ergeben sich laut Forrester aus der Erfahrung – „Trial and Error“.

3.1.2 Der Ausweg: gehostete Private Clouds

Wer nicht über genügend Zeit, Geld oder Geduld für den Aufbau einer internen Cloud verfügt, sollte auf eine Alternative setzen: sich bei einem Service-Provider einmieten, aber ohne die Risiken einer Public Cloud. Der Mittelweg besteht darin, eine geschützte private Cloud einzurichten, die von einem Provider gehostet und verwaltet wird. So kann ein Unternehmen in die Vorteile einer serviceorientierten eigenen IT-Infrastruktur kommen, erspart sich aber zugleich das mühevolle eigene Ausprobieren. Das Problem dabei: einen zuverlässigen Serviceanbieter zu finden, der sich wirklich auskennt, was in der gegenwärtigen Umbruchsituation keine einfache Aufgabe sein dürfte. Zumal, wenn es an der eigenen Kompetenz mangelt.

3.1.3 Community-Clouds und High Performance Computing

Forrester spricht in diesem Zusammenhang von „Cloud Washing“: Viele traditionelle Hosting-Anbieter hängen sich ein neues Mäntelchen um und geben sich als Virtualisierungs- und Cloud-Profis aus. Wer sich auf den Hosting-Weg begeben

will, kommt also doch nicht um das eigene Wissen herum. Nur so kann eine fundierte Auswahl getroffen werden. Ein Grund mehr, im eigenen Unternehmen Virtualisierungs- und Cloud-Experten heranzuziehen.

Öffentliche Clouds bergen Risiken: Wie steht es um die Sicherheit der Daten? Wer garantiert dafür? Können Compliance-Vorschriften eingehalten werden? Und interne Clouds sind noch zu kostspielig und erfordern einen langen Atem. Eine Alternative für viele Unternehmen könnten „Community-Clouds" sein, bei denen sich mehrere Firmen locker zusammenschließen und ihre IT-Infrastruktur gemäß eines Servicekonzepts gemeinsam nutzen.

In Deutschland kooperieren bereits einige Kommunen nach einem solchen Modell, indem man einen gemeinsamen Pool von Ressourcen, Anwendungen und Daten aufbaut. Universitäten und Unternehmen der Biotechnologie haben ebenfalls mit solchen Communities begonnen. So werden nicht nur die Cloud-Kosten gemeinsam geschultert, sondern es können die jeweils vorhandenen Strukturen über neue Portale weiterverkauft oder nach Nutzung abgerechnet werden.

Wie weit sich ein Unternehmen in solchen Cloud-Communities engagiert, hängt von der langfristigen Strategie ab. Diese kann von einer einfachen, mehr ideellen Unterstützung bis zu einer angestrebten totalen Kontrolle gehen. Je nach Option müssen die personellen und finanziellen Konsequenzen beachtet werden. Um eine Testumgebung für virtualisierte Cloud-Communities einzurichten, gibt es die kostenlose „Eucalyptus Community Cloud (ECC)" (http://open.eucalyptus.com/).

3.1.4 High Performance Computing (HPC) für alle

Grid Computing galt lange Zeit als der bestmögliche – und billigste – Zugang zu High Performance Computing (HPC). Zusammengebaut aus vielen No-Name-Rechnern und auf Basis des Linux-Betriebssystems, haben sich viele Universitäten, Forschungseinrichtungen und Unternehmen, die hohe I/O-Leistung zum Beispiel für geografische Berechnungen brauchen, solche Grid-Netze angeschafft. Die mit Supercomputern oder Mainframes verglichen niedrigen Anschaffungskosten werden allerdings konterkariert durch aufwendige Verwaltungsmechanismen und Monitoring-Vorrichtungen dieser PC-Landschaft. Und nur durch komplizierte Cluster-Konstruktionen kann der Ausfall einzelner Rechner abgefangen werden.

3.1.5 Cloud Computing und die Kosten

Cloud-Infrastrukturen sind im Begriff, dieses HPC-Modell abzulösen. Denn man muss ja nicht mehr solche Grid-Netze oder Supercomputer bei sich im eigenen Hause einrichten, sondern kann die benötigte Rechenkraft im gewünschten Ausmaß und für einen beliebig begrenzbaren Zeitraum kostengünstig anmieten.

HPC auf Cloud-Basis kann darüber hinaus der IT-Abteilung die Möglichkeit bieten, die Spielregeln für das Verhältnis von Business und IT zu verändern: Indem

hohe Rechenleistung nach Bedarf hinzugemietet wird, wird die IT vom reinen Cost Centre zum Treiber für das Geschäft. Auch in diesem Fall sind Know-how und Erfahrungen der eigenen IT-Mannschaft wichtiger denn je. Es besteht sonst die Gefahr, dass die Unternehmen von den Hosting- und Service-Anbietern über den Tisch gezogen werden. Der Einsatz von IT ist kein Selbstzweck. Dies gilt erst recht bei der Anwendung neuer Technologien, die sich lohnen müssen. Es muss nicht immer das Billigste eingekauft werden – wichtiger ist es, die Relation zwischen Aufwand und Ertrag im Auge zu behalten. Unternehmen sollten deshalb genau prüfen, welche Applikationen „reif" für eine Verlagerung in virtuelle und Cloud-Umgebungen sind. Auch müssen die Portal- und Abrechnungsmodalitäten auf diese Anwendungen abgestimmt sein. Unternehmen können hier schrittweise Erfahrungen sammeln und sich zu höheren Cloud-Niveaus vorarbeiten. Lehrreich ist es zum Beispiel, sich mit Amazon EC2 Spot Instances (http://aws.amazon.com/ec2/spot-instances/) oder mit Enomaly SpotCloud (www.economist.com/node/18185752) zu beschäftigen. Auch mit dem Cloud Price Calculator kann man die Cloud-Kosten in den Griff bekommen.

3.1.6 Auswertung von Daten

IT und ihre Auswertung in „realtime" versprechen Analyseprogramme, sei es als CRM-Durchforstung, als klassisches Data Warehouse oder als Business-Intelligence (BI)-Applikation, die heute fast alle großen Hersteller im Angebot haben. Doch Cloud-basierte Tools machen dieser Softwareabteilung nun Konkurrenz.

Aufwendige Installation und Verwaltung inklusive des nötigen Know-hows im eigenen Haus entfallen zumindest teilweise. Bereits 2008 starteten solche alternativen Programme wie AWS Elastic MapReduce (http://aws.amazon.com/elasticmapreduce/), 1010data (www.1010data.com) oder GoodData (www.gooddata.com). Es gibt auch die Open-Source-BI-Lösung Jaspersoft (www.jaspersoft.com).

Von Informationen und ihrer Bedeutung für die Unternehmenszwecke wird heute viel gesprochen – leider mehr in einem appellativen Stil, ohne dass die wirklichen Vorteile ersichtlich sind. In einer Cloud lassen sich auch Daten, die für andere Unternehmen von Interesse sein können, leichter vermarkten. Unternehmen, die sich auf diesem Feld versuchen, müssen natürlich genau abwägen zwischen Business-kritischen Daten und solchen, die von allgemeinem Interesse sein können.

3.1.7 Standards und Sicherheit

Schon Virtualisierungsansätze neigen dazu, proprietär zu sein und somit die Konkurrenz absichtlich auszugrenzen. Dies gilt in noch größerem Maße für den neu erkorenen Zukunftsmarkt Cloud Computing. Die sich abzeichnende Wende zieht viele Hersteller und Systemhäuser an, die sich alle ihren Anteil am zu verteilenden Kuchen sichern wollen. Für Anwender bedeutet diese Situation, sehr vorsichtig zu

sein, um nicht in eine Lock-in-Falle zu tappen. Gerade im eigenen Interesse sollten sie auf der Verabschiedung von Standards und allgemein zugänglichen Schnittstellen (APIs) insistieren. Nur so lassen sich zuverlässige Serviceanbieter und Hersteller herausfinden. Allein auf die gegenwärtigen Marktführer zu setzen wäre verkehrt. Allerdings genießen diese derzeit viel Vertrauen. In den USA gehen 39 Prozent der Unternehmen, die mit Cloud-Services experimentieren, zu Amazon Web Services, 31 Prozent wählen IBM und 30 Prozent Microsoft.

3.1.8 Cloud-Security

Sicherheit der Daten hat viel mit Compliance zu tun. Business-kritische Informationen müssen besonders geschützt sein, und wer sie in eine Cloud-Lösung mit virtualisierten Servern verlagert, muss auf besonderen Sicherheitsgarantien bestehen. Wer einen Deal mit einem Service-Provider eingeht, sollte auf genau ausformulierten SLAs (Service Level Agreements) bestehen. Eine finanzielle Entschädigung für den Fall, dass Daten verloren gehen oder beschädigt werden, kann nur ein Teil der Lösung sein. Unternehmen, die sich für externe Clouds interessieren, sollten deshalb genau abwägen, welche Applikationen sie nach außen vergeben wollen. Lesen Sie dazu auch unseren „Ratgeber: Cloud Computing und Datenschutz“ (Webcode **2033982**).

Hartmut Wiehr

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation CIO.

TecChannel-Links zum Thema	Webcode	Compact
Die Fallen bei Virtualisierung und Cloud	2034813	S.111
Cloud Computing – US-Behörden lesen Daten mit	2036922	S.116
Cloud Computing: Admin-Jobs in Gefahr	2036722	S.120
Sicherheitsrisiken in der Cloud vermeiden	2034755	S.122
Identitäts- und Berechtigungs-management in der Cloud	2034353	S.130
Private-Cloud-Lösungen im Überblick	2036787	S.133
Workshop – Verwaltungsumgebung für Private Clouds aufbauen	2036404	S.140
Workshop – Private Cloud mit Eucalyptus	2037292	S.147
Workshop – Aufbau einer Cloud mit VMware vCloud Director	2037250	S.154

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

3.2 Cloud Computing – US-Behörden lesen Daten mit

Keine guten Nachrichten für Cloud-Kunden – jedenfalls wenn sie Cloud-Services von einem US-amerikanischen Cloud-Provider beziehen. Ein Managing Director von Microsoft in England hat bei der Vorstellung der Microsoft-Cloud-Lösung Office 365 eingeräumt, dass sein Arbeitgeber auf Anforderung die Daten seiner Cloud-Kunden an das FBI oder andere US-Behörden weitergeben muss.

Im Ernstfall wird wohl nicht nur Microsoft die Daten seiner Kunden weiterreichen. Alle amerikanischen Cloud-Anbieter unterliegen dem USA Patriot Act und können sich dessen Regelungen nicht entziehen. Dazu kommt: Wenn die amerikanischen Behörden den Cloud-Provider zum Schweigen verpflichten, wird der Kunde nie davon erfahren, dass auf seine Daten zugegriffen wurde.

3.2.1 „Wir können diese Garantie nicht geben“

Damit wird jetzt eine Diskussion neu entfacht, die schon länger schwelte. Bisher hatten Marktkenner und Analysten vielfach dazu geraten, beim Abschluss von Cloud-Verträgen mit außereuropäischen Anbietern verbindlich zu vereinbaren, wo die Daten verarbeitet werden. So könnten sie sicherstellen, dass – zumindest personenbezogene – Daten in einem Rechenzentrum (RZ) in Deutschland oder doch in Europa verarbeitet werden. Das sollte im Hinblick auf die deutschen Datenschutzgesetze, die traditionell erheblich strenger sind als in anderen Ländern, rechtliche Sicherheit gewährleisten.

Thilo Weichert, Landesbeauftragter für den Datenschutz in Schleswig-Holstein, rät Unternehmen, sich bei der Nutzung von Cloud-Diensten für personenbezogene Daten ausschließlich auf rein europäische Service-Provider zu beschränken.

Diese Ratschläge dürften sich als nutzlos erweisen: Bei der Vorstellung der Microsoft-Cloud-Lösung Office 365 hatte Gordon Frazer, Managing Director von Microsoft in England, auf Nachfrage eines Journalisten eingeräumt, dass Microsoft letztlich keine Garantie dafür abgeben kann, dass die Kundendaten nicht weitergegeben werden. Skeptiker hatten immer wieder auf die unsichere Rechtslage hinge-

wiesen. Neu ist lediglich, dass erstmals ein hochrangiger Manager eines Cloud-Providers die Konsequenzen in dieser Deutlichkeit ausspricht. „Wir können diese Garantie nicht geben – und das kann auch kein anderes Unternehmen mit Hauptsitz in den USA", erklärte Frazer. Schließlich müsse Microsoft sich als US-amerikanisches Unternehmen an die amerikanischen Gesetze halten. Und das gelte auch für alle internationalen Niederlassungen – und die dort gespeicherten Daten ausländischer Kunden. Zwar versicherte der britische Microsoft-Statthalter, dass Kunden im Falle einer Datenweitergabe informiert würden, wann immer dies möglich sei. Aber auch das könne er nicht verbindlich zusagen. Wenn die amerikanischen Behörden Stillschweigen nach dem sogenannten „US National Security Letter" anordneten, müsse auch eine Information der Kunden unterbleiben.

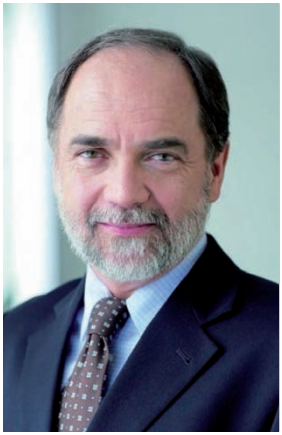
Nach Einschätzung von Thilo Weichert, Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein (ULD), stellt eine derartige Datenweitergabe aus dem Gebiet der EU einen Widerspruch zu europäischem Datenschutzrecht dar. Er schätzt die Rechtslage so ein, dass das Risiko der Datenweitergabe die Vertraulichkeit der – in diesem Fall – auf Microsoft-Servern gehosteten Daten und Anwendungen infrage stelle und bestehenden Verträgen zur Datenverarbeitungsdienstleistung die Grundlage entziehe. Das schließe nach seiner Einschätzung Anbieter wie den Office-365- und Windows-Azure-Anbieter Microsoft als Kandidaten für personenbezogene IT-Dienstleistungen aus und begründe sogar ein Sonderkündigungsrecht.

3.2.2 Amerikanische Cloud-Provider in der Zwickmühle

Kunden amerikanischer Cloud-Provider bringt das nicht nur im Hinblick auf die Einhaltung von Datenschutzbestimmungen in eine schwierige Situation. Die wenigsten wird es beruhigen, dass es ausschließlich amerikanische Behörden sind, die Zugriff auf ihre Daten erhalten. Dass der große amerikanische Bruder auch mitlesen kann, wenn es etwa um geistiges Eigentum wie Blaupausen und Konstruktionszeichnungen oder auch um Unterlagen für internationale Ausschreibungen geht, dürfte vielen Managern die Haare zu Berge stehen lassen. Amerikanische Cloud-Provider geraten damit in eine rechtliche Zwickmühle. Andreas Stein, Managing Director von Dells Services-Sparte, kommentierte dies gegenüber Heise-Online so: „Cloud-Anbieter befinden sich in einem Dilemma, sie können sich nur aussuchen, gegen welche Regelungen sie verstoßen: gegen die US-Bestimmungen oder gegen die hiesigen Datenschutzbestimmungen." Denn auf der einen Seite müssen sie ihren deutschen Kunden die Einhaltung der gesetzlichen Regelungen in Deutschland zusagen, auf der anderen Seite unterliegen sie dem USA Patriot Act, der sie im Ernstfalle zwingt, eben diese Regelungen zu verletzen.

Ist dies das Ende für Cloud Computing? Wohl nicht. „Den tatsächlichen Nutzen von Cloud Computing beeinträchtigt die amerikanische Rechtslage nicht", schreibt Joseph Reger, CTO von Fujitsu Technologie Solutions, in einem Kommentar (http://fujitsu.fleishmaneurope.de/statement-of-the-month/2011-07/).

„Allerdings ruft es uns nur einmal mehr ins Gedächtnis, dass bei aller berechtigten Euphorie für die Cloud eines nicht aus dem Fokus geraten darf: eine sorgfältige Prüfung im Vorfeld eines Servicevertrags." Dabei gelte es, sich ganz genau über den möglichen Provider und seine Bedingungen zu informieren und auch das Kleingedruckte zu lesen. Nur so könnten Unternehmen mögliche Folgen abschätzen – und Risiken entweder eliminieren oder eben in Kauf nehmen.



Joseph Reger, CTO bei Fujitsu Technologie Solutions: „Europäische Unternehmen, die ihre Daten vor dem Zugriff von US-Behörden schützen wollen, bleibt nur eine Möglichkeit: sich für einen Anbieter zu entscheiden, der eben nicht dem USA Patriot Act unterliegt."

Seine Schlussfolgerung: „Europäische Unternehmen, die ihre Daten vor dem Zugriff von US-Behörden schützen wollen, bleibt nur eine Möglichkeit: sich für einen Anbieter zu entscheiden, der eben nicht dem USA Patriot Act unterliegt." In diese Kerbe schlägt auch der schleswig-holsteinische Datenschutzbeauftragte Thilo Weichert: Auch er rät Unternehmen, sich bei der Nutzung von Cloud-Diensten für personenbezogene Daten ausschließlich auf rein europäische Service-Provider zu beschränken. Also das Aus für amerikanische Cloud-Anbieter in Europa? Zumindest kann zurzeit wohl niemand mit gutem Gewissen einem Unternehmen zu Cloud-Services eines amerikanischen Anbieters raten – jedenfalls wenn es um personenbezogene Daten oder geistiges Eigentum geht. Dabei sind es die amerikanischen Cloud-Provider, die zu allererst auf eine Klärung der Rechtslage und eine Lösung des Dilemmas drängen sollten. Denn für HP, Microsoft, IBM, Amazon, Google oder auch Salesforce.com, bei denen das gesamte Geschäftsmodell oder doch große Teile davon auf Cloud Computing basieren, dürfte es kaum eine Alternative sein, sich mit ihren Cloud-Services aus der EU zurückzuziehen.

Darüber, wie eine rechtlich saubere Lösung aussehen könnte, wird vielfach spekuliert. Ob es amerikanischen Unternehmen möglich ist, rechtlich unabhängige europäische Tochterunternehmen zu gründen, die nicht dem USA Patriot Act unterliegen ist ebenso umstritten wie vertragliche Regelungen, die Cloud Services als „Auftragsdatenverarbeitung" deklarieren.

3.2.3 Cloud-Standardverträge erfüllen nicht EU-Anforderungen

Rechtsanwalt Arnd Böken von der Berliner Kanzlei Graf von Westphalen etwa vertritt im Handelsblatt folgende These: Wird vertraglich die Auftragsdatenverarbeitung in einer „EU-Cloud" vereinbart – das heißt ausschließlich an europäischen RZ-Standorten – bleibe der Cloud-Kunde alleiniger Herr der Datenverarbeitung. Der Cloud-Provider werde dann lediglich im Auftrag und auf Weisung tätig. Ebenso wie die meisten europäischen Cloud-Provider böten auch einige amerikanische Cloud-Provider solche EU-Clouds an.

„Verfügt das deutsche Unternehmen über einen solchen Vertrag, ist eine Weitergabe von Daten durch den Cloud-Provider an US-Behörden ausgeschlossen", schreibt Anwalt Böken. Ein Zugriff von US-Behörden auf die Daten sei dann nur im Wege der Rechtshilfe über eine europäische Behörde möglich. Die Standardverträge vieler US-Anbieter erfüllten allerdings diese Anforderungen des deutschen Rechts an die Auftragsdatenverarbeitung nicht.

Rechtsanwalt Arnd Böken von der Berliner Kanzlei Graf von Westphalen: „Der deutsche Cloud-Kunde ist rechtlich nur dann auf der sicheren Seite, wenn er eine Auftragsdatenverarbeitung in einer EU-Cloud vereinbart."

Zwar mag dieses Vorgehen für europäische Unternehmen eine gewisse Sicherheit im Hinblick auf die deutschen und europäischen Gesetze bringen. Ob diese rechtliche Einschätzung im Ernstfall Bestand hat und amerikanische Behörden diese teilen, wird sich jedoch möglicherweise niemals erweisen. Denn ob Zugriffe auf die Daten europäischer Kunden stattfinden oder sogar schon stattgefunden haben, unterliegt eben auch der Geheimhaltung, wenn die amerikanischen Behörden das anordnen.

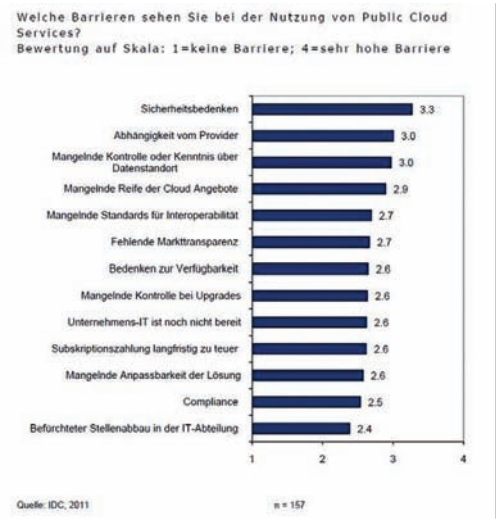
Holger Eriksdotter

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation CIO.

3.3 Cloud Computing: Admin-Jobs in Gefahr

Bernard Golden von unserer amerikanischen Schwesterpublikation CIO.com ist aufgefallen, dass in nahezu jeder Diskussion um Cloud Computing erwähnt wird, dass Cloud Computing Jobs kostet. Im Misstrauen, mit dem viele der Public Cloud begegnen, schwingt auch eine starke emotionale Komponente mit.

Golden mutmaßt, dass IT-Abteilungen sich vielleicht deshalb gegen Cloud Computing sträuben, weil sie den Jobverlust fürchten. In einer Umfrage unter IT-Verantwortlichen würden sich nur sieben Prozent für eine Public Cloud entscheiden. 47 Prozent der Befragten würden eine Private Cloud bevorzugen. Golden ist versucht, diese Umfrageergebnisse mit Selbstschutz zu erklären.

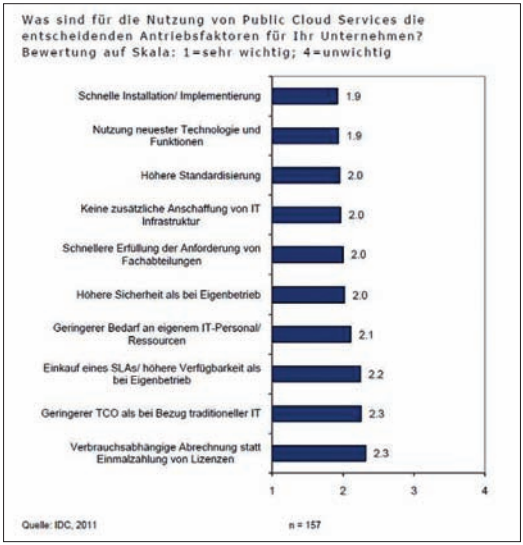


Kostensenkung: Einer IDC-Studie zufolge ist Personal durchaus ein Thema, denn hier könnte man mit Cloud Computing sparen.

Forrester-Analyst Ted Schadler wurde kürzlich in einem Infoworld-Artikel folgendermaßen zitiert: „Cloud Computing ist eine Gefahr für Blue-Collar-ITler, zum Beispiel Admins und Mitarbeiter im Bereich IT-Infrastruktur." Wer sich vor allem mit der Installation, Administration und Konfiguration von Softwarekomponenten in diesem Bereich beschäftigt, könnte durch Cloud Computing schon bald überflüssig sein, glaubt auch Bernard Golden. Das liegt seiner Meinung nach aber nicht an der Virtualisierung, sondern an der Automatisierung von Prozessen.

Dass durch die Automatisierung von Prozessen Arbeitsplätze redundant werden, ist nichts Neues, schreibt Golden. In vielen anderen Bereichen konnte man dieses Phänomen schon beobachten. In einer automatisierten Cloud-Umgebung seien nicht Tätigkeiten wie Installieren und Konfigurieren gefragt, sondern das Entwerfen und Implementieren solcher Cloud-Umgebungen.

Weniger wichtig: Die von IDC befragten IT-Verantwortlichen sehen beim Thema Personal und Cloud wenig Schwierigkeiten.



3.3.1 Alte Systeme versus SaaS

Hat diese Entwicklung denn auch Auswirkungen auf den CIO-Posten oder andere hochrangige IT-Manager? Ja und nein, glaubt Golden. Denn genauso wie Henry Fords Veränderungen die Arbeit in ganzen Fabriken umgekrempelt haben, glaubt er, dass Cloud Computing IT-Abteilungen verändern wird. CIOs müssen ihre Fabrik – die IT-Abteilung – so effizient wie möglich führen. Sie sollten ihre Dienstleistungen überdenken und erkennen, dass von ihnen Infrastrukturmanagement zu Marktpreisen gefordert ist. Golden glaubt aber, dass es ein noch bedeutenderes Thema gibt als die Debatte um Public und Private Clouds: alte Systeme versus SaaS. Denn schon jetzt fließt der größte Teil des IT-Budgets in alte Systeme, schreibt Golden – Systeme, die in vielen IT-Abteilungen als unantastbar gelten. Er hält es für nur schwer zu rechtfertigen, wie man an einem alten System festhalten kann, wenn die SaaS-Alternativen deutlich günstiger sind. Golden geht davon aus, dass sich die IT in den kommenden zehn Jahren stärker verändern wird als in den vergangenen 30 Jahren. Er geht davon aus, dass uns 2021 manche Prozesse von heute so vorkommen werden wie jemand, der in einem Schwarz-Weiß-Film ein Ferngespräch führen möchte.

Bernard Golden, Andrea König

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation CIO.

3.4 Sicherheitsrisiken in der Cloud vermeiden

Um bei der Nutzung von Cloud-Diensten nicht unerwartet im Regen zu stehen, scheuen große Unternehmen nach einer aktuellen Studie der amerikanischen Information Technology Intelligence Corporation (ITIC, www.itic-corp.com) den Schritt zum Cloud Computing. Die Marktforscher befragten international 300 Firmen mit bis zu 100.000 Mitarbeitern. Lediglich 15 Prozent von ihnen wollen in absehbarer Zeit entsprechende Technologien einsetzen, nur acht Prozent tun es bereits. Die größten Ängste existieren hinsichtlich der Sicherheit: Zum einen ist meist nicht genau bekannt, wo auf dem Erdball die sensiblen Daten gespeichert sind. Wie steht es da zum Beispiel mit der Compliance? Welchem Landesrecht unterliegen die Informationen? Zum anderen besteht die Sorge, dass das Geschäft durch einen längeren Netzausfall zum ruinösen Stillstand kommt. Wie so oft entstehen Ängste durch Skepsis vor dem Neuen: Gerüchte kursieren, und es herrscht mangelhafte Aufklärung. Wer aber weiß, welche Sicherheitslücken drohen und wie er sich schützen kann, muss sich weniger fürchten, denn die Risiken lassen sich auf ein Minimum reduzieren. Hier sind die Cloud-Computing-Provider in der Pflicht, ihren Kunden über die für ihn am besten geeigneten Sicherheitsmaßnahmen zu informieren. Welche davon er nutzt, bleibt jedem Anwender dann selbst überlassen. Aber nur wer das persönliche Sicherheitsniveau richtig einschätzen kann, entdeckt für sein Geschäft in der Wolke mehr als ominösen Nebel.

3.4.1 Privat versus öffentlich

Schon die von Anbieter zu Anbieter beziehungsweise Analyst zu Analyst unterschiedlichen Definition der Cloud führen zu gravierenden Missverständnissen: Meist geht es um ein Verlagern der ICT-Ressourcen von lokalen Rechnern ins öffentliche, unsichere Internet. Aber muss das zwangsläufig so sein? Hier gilt es, grundsätzlich zwischen öffentlichen („Public“) Clouds à la Amazon und Google sowie dedizierten („Private“) Clouds für Unternehmen zu unterscheiden. Erstere eignen sich primär für private Nutzer, um zum Beispiel Mails überall zu empfangen und zu versenden oder um Dateien und Urlaubsfotos bequem auf Festplatten im Netz abzulegen. Sie kosten meist nichts, ihre Betreiber verpflichten sich aber auch zu nichts. Bei einem Serverausfall müssen die Anwender eben warten. Geht ein Mail-Server oder eine Festplatte kaputt, sind die Daten weg. Sicherheit und Servicevereinbarungen – Fehlanzeige.

No risk, no fun? Was sich im privaten Umfeld mehr und mehr durchsetzt, widerspricht deutlich den Anforderungen der Geschäftswelt. Von der Datensicherheit, dem Schutz gegen Manipulationen und einer hohen Verfügbarkeit hängt oft das Überleben eines Unternehmens ab. Weltweit stünden die meisten Firmen nach gut einer Woche ohne ihre IT-Daten vor dem Ruin. Und neben einem hohen finanzi-

ellen Verlust leidet meist auch das Image, wenn Informationen über eine neue Produktentwicklung schon vor ihrer offiziellen Publikation nach außen dringen. Sollten Unternehmen also trotz der hohen Flexibilität und der rein verbrauchsabhängigen Bezahlung lieber auf die Wolke verzichten? Die Antwort liegt in der „privaten" Cloud, einem Kompromiss aus Wolke und eigener Anbindung an ein Data Center. Hier fließen die Daten nicht über das öffentliche Internet, sondern über das getunnelte Netz des Providers.

3.4.2 Dienstleister auswählen

Die wohl größte Herausforderung für Unternehmen beim Cloud Computing besteht darin, den geeigneten Dienstleister zu finden. Sie müssen sich hierzu intensiv mit den von ihm angebotenen Services und seiner tatsächlichen Leistungsfähigkeit befassen. Kann er zum Beispiel individuelle Bedürfnisse bedienen? Wie gut kennt er sich mit branchenspezifischen Anforderungen aus? Große ICT-Anbieter erbringen identische Leistungen für eine Vielzahl von Kunden. Durch die sich daraus ergebenden Skaleneffekte können sie Technologien einsetzen, die für ein einzelnes Unternehmen kaum erschwinglich wären.

Es müsste darüber hinaus Personal mit den richtigen Fachkenntnissen vorhalten und das Wissen der Mitarbeiter regelmäßig in Schulungen aktualisieren. Über den Provider kaufen Firmen das Fach- und Branchen-Know-how gleich mit ein. Das macht sich insbesondere bei der Sicherheit schnell bezahlt. Die Angreifer kennen sich meist mit den neuesten Werkzeugen perfekt aus. Hier mitzuhalten erfordert einen beträchtlichen finanziellen und personellen Aufwand.

3.4.3 Security-Anforderungen definieren

Gleichwohl sollten Unternehmen nicht sofort die komplette Sicherheit einfach auf den Provider schieben, sondern sich mit ihm zunächst intensiv über das nötige Schutzniveau auseinandersetzen. Der Dienstleister muss seinem Kunden die bestehenden Risiken erläutern und ihm sagen, was er konkret dagegen unternimmt. Erst aus einer gründlichen Gefahrenanalyse lässt sich eine individuelle Lösung ableiten, die sämtliche Sicherheitsanforderungen erfüllt.

Genauso wie bei klassischen ICT-Umgebungen reicht beim Cloud Computing einerseits das punktuelle Stopfen von Security-Lücken nicht aus. Andererseits braucht ein Unternehmen auch nicht zwangsläufig alle am Markt vorhandenen Sicherheitstechnologien einzusetzen, sondern kann diese von einem seriösen Provider modular ganz nach Bedarf beziehen. Spätere regelmäßige Risikobewertungen und Audits, etwa in Form von Penetrationstests, ergänzen diese ganzheitliche Sichtweise. So lassen sich neue Schwachstellen herausfinden und Maßnahmen schnell anpassen. Die genaue Auswahl und die kontinuierliche Aktualisierung der Sicherheitsmaßnahmen sind gerade beim Cloud Computing sehr wichtig, da mit

der hochgradigen Dezentralisierung und Verteilung von Anwendungen und Daten auch die Zahl der Angriffsvektoren und Gefahren steigt. Sind die Sicherheitsanforderungen exakt festgelegt, lassen sie sich über Service Level Agreements durchgängig vertraglich vereinbaren, also von der Produktion im Rechenzentrum über die Netze bis zum PC oder mobilen Endgerät beim Anwender im Unternehmen. Im eigenen Netz kann der Dienstleister das Einhalten der SLAs auch in der Cloud gewährleisten. So kann der Kunde die Qualität und die Verlässlichkeit des ICT-Service objektiv beurteilen.

Die Tatsache, dass eine spezialisierte, zentrale Stelle alle Vorgänge – beispielsweise Implementierung, Konfiguration, Release-, Update- und Patch-Management oder Backup – kontrolliert und steuert, erleichtert das Einhalten der Sicherheitsmaßnahmen zusätzlich. Erst dadurch können diese auf sämtlichen Ebenen wie Zahnräder wirksam ineinandergreifen. Das ermöglicht letztlich sogar das sichere Einbinden mobiler Endgeräte in die Wolke.

3.4.4 Anwendungen und Daten trennen

Trotz vieler Gemeinsamkeiten bei der Sicherheit stellt die virtuelle Wolke gegenüber dem klassischen Outsourcing einige besondere Anforderungen. Das betrifft zum Beispiel den Datenschutz: Da sich im Rechenzentrum mehrere Unternehmen Server teilen, die ihnen die jeweils benötigten Ressourcen zuweisen, muss sicher sein, dass niemand in die Daten des anderen Einblick nehmen kann. Hierzu kommt es auf eine saubere Trennung von Anwendungen und Daten der einzelnen Kunden an. Möglich machen das sogenannte virtuelle lokale Netzwerke (VLANs). Dabei erhält jeder neue Cloud-Kunde automatisch einen separaten Anschluss an den Server. Der Rechner verfügt somit am Ende über beliebig viele individuelle Zugangswege. Die Administration von VLANs erfolgt mit einer zentralen Weiche (Switch). Hier laufen alle Netzwerkkabel zusammen. Der Switch ordnet jedes VLAN automatisch einem bestimmten Kunden zu. Dieser darf nur in seinem eigenen Bereich arbeiten. Die VLANs sind komplett voneinander isoliert. Jemand mit bösen Absichten käme so über den Switch gar nicht auf einen anderen Zugang.

Die Rechner selbst sollten in mehrere Einheiten partitioniert sein, von denen jeder Kunde eine Scheibe mitsamt VLAN-Zugang bekommt. Sie können somit nicht von ihrer Partition auf die eines anderen Unternehmens springen. Dadurch ist es zum Beispiel möglich, dass SAP- und Oracle-Anwendungen gemeinsam auf einem Server laufen – strikt voneinander getrennt. Zudem sollten die Rechner vom öffentlichen Internet komplett entkoppelt sein. Webanwendungen, zum Beispiel für Online-Rechnungen, laufen dann in gesonderten Servicebereichen. Das unterbindet Angriffe übers Web auf geschäftskritische Anwendungen.

Letztlich sind die Informationen auch auf der Storage-Ebene voneinander zu isolieren. Sie lassen sich außerdem von der Technologie unveränderbar ablegen und sind damit revisionssicher archiviert.

3.4.5 Cloud-Systeme sicher integrieren

Einzelanwendungen liegen im Idealfall also im Data Center für jeden Kunden sicher voneinander isoliert vor. Gerade für Unternehmen kommt es aber oft darauf an, dass Applikationen miteinander kommunizieren. Die Mitarbeiter sollen beispielsweise E-Mails direkt aus SAP bearbeiten. Der Cloud-Provider kann hierzu getrennte Anwendungen eines Kunden in der Wolke wieder so zusammenführen, dass sie nach vorgegebenen Regeln gemeinsam funktionieren. Ein anderes Unternehmen bekommt hiervon nichts mit. Genauso ist auch eine Integration in die bestehende, nicht dynamische Anwendungslandschaft eines Kunden möglich, ohne dass für Angreifer Tür und Tor weit offen stehen. Selbst individuelle Einzelsysteme lassen sich einbinden, damit etwa unterschiedliche Fachabteilungen reibungslos miteinander arbeiten können. Doch nicht nur andere Unternehmen sollten keinen Einblick in vertrauliche Informationen erhalten. So sollte ein Cloud-Nutzer auch seinen Provider fragen, wie er es selbst mit Zugriffsrechten hält. Besonders kritische Daten sollten im Rechenzentrum so abgelegt sein, dass auch Mitarbeiter des Dienstleisters sie nicht einsehen, verändern oder löschen können. Lässt es sich für eine bestimmte Operation nicht vermeiden, auf die Informationen zuzugreifen, muss der Dienstleister seinen Kunden vorher um Erlaubnis fragen. Nur er besitzt den Schlüssel zu den Daten. Sollte der Kunde irgendwann aus der Wolke aussteigen wollen, müssen die Informationen lückenlos an ihn zurückfließen. Aus diesem Grund sollten Unternehmen vor der Auftragsvergabe auch auf die wirtschaftliche Stabilität des Dienstleisters achten. Unter Umständen leidet unter einer Insolvenz die Verfügbarkeit der Daten.

3.4.6 Identitäten prüfen und managen

Aber auch beim Kunden dürfen nach dem „Need-to-know"-Prinzip nur berechtigte Mitarbeiter die Informationen einsehen, die sie für ihre Arbeit tatsächlich brauchen. Aus dem klassischen Outsourcing bekannte Verschlüsselungs- und Zugangsmechanismen unterstützen solch ein Rollen- und Rechtemanagement. Public-Key-Infrastrukturen (PKI) stellen zum Beispiel sicher, dass sich der richtige Mitarbeiter am System anmeldet. Sie schalten den Zugang erst nach erfolgreicher Identifikation frei, zum Beispiel über Chipkarten mit Signaturfunktion, biometrische Verfahren oder über die mit einem Einmalpasswort versehene SIM-Karte (Subscriber Identity Module) im Handy. Damit verhindert eine PKI das Mitlesen oder Umlenken von Kommunikationsbeziehungen beziehungsweise das Einspielen von Schadsoftware ins Netz.

Große Cloud-Provider besitzen eigene Trust Center, die Zertifikate zur Authentisierung an einem System herausgeben. Erst mit diesen digitalen Ausweisen erhält der berechtigte Nutzer Zugang. Allerdings können sich Mitarbeiter mit den ihnen zugeteilten Zertifikaten auch gegenseitig zuverlässig erkennen. Nach dem Austausch der Ausweise weiß jeder, dass auf der anderen Seite tatsächlich der erwar-

tete Ansprechpartner mit ihm kommuniziert. So lassen sich auch in Cloud-Beziehungen sichere abteilungs- und unternehmensübergreifende Netzwerke für die Zusammenarbeit einrichten.

3.4.7 Wo liegen die Daten?

Zu großer Unsicherheit im Cloud Computing führt auch ein Faktor, der sich vom klassischen Outsourcing grundsätzlich unterscheidet: Der Nutzer weiß im Normalfall nicht, auf welchen Systemen, in welchem Rechenzentrum und – vor allem – in welchem Land der Provider seine Daten speichert. Diese Katze im Sack kann sich auf das Geschäft fatal auswirken. Überschreiten die Daten Ländergrenzen, erfüllen sie möglicherweise wichtige Anforderungen an die Sicherheit oder rechtliche und branchenspezifische Auflagen nicht. So ist es in Frankreich und Polen nicht erlaubt, Finanzdaten außerhalb des Landes zu betreiben. In den USA und anderen Ländern fallen Sicherheitstechnologien wie Verschlüsselung unter das Kriegswaffenkontrollgesetz und sind daher nur in Ausnahmefällen zulässig. Häufig ist auch nicht geregelt, wer im Fall eines Datenverlusts im Staat XY die Haftung trägt und wie diese aussieht. Weiterhin bestehen Risiken durch die unterschiedlich gestaltete Gesetzgebung, etwa beim Abhören oder bei unbemerkten Zugriffen. In einigen Staaten können Behörden ohne Vorwarnung die Herausgabe vollständiger Backups verlangen. Die Liste der Unterschiede in Bezug auf den Datenschutz lässt sich nahezu unendlich weiterführen. Manch ein internationaler ICT-Dienstleister verzichtet deshalb bewusst darauf, in bestimmten Ländern ein eigenes Rechenzentrum zu errichten. In der Private Cloud von T-Systems kann der Nutzer darüber hinaus selbst bestimmen, wo er seine Daten abgelegt haben möchte.

3.4.8 EU-Datenschutz erleichtert Cloud-Nutzung

Für Cloud-Services im geschäftlichen Umfeld eignen sich besonders Anbieter aus der Europäischen Union. Mit der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr hat die EU einen Mindeststandard für den Datenschutz und die Datensicherheit eingeführt. So setzt zum Beispiel jede Übermittlung personenbezogener Informationen die vorherige Einwilligung des Betroffenen voraus. Auftragsdaten dürfen nur in den Grenzen der EU beziehungsweise des Europäischen Wirtschaftsraums (EWR) verarbeitet werden. Öffentliche Institutionen verknüpfen Vergaben oft mit einer Datenverarbeitung im eigenen Land. Erstaunlicherweise gibt es selbst in den USA bislang keine festgeschriebenen Richtlinien zum Datenschutz. Dort sind nur spezielle Arten der Verarbeitung verboten. Behördenakten beispielsweise sind von jedem Bürger problemlos abrufbar.

Das Wissen, wo die Daten liegen, hat darüber hinaus noch einen anderen Aspekt: Manche Großunternehmen wollen ihre Daten und Anwendungen in einem ausfallsicheren Rechenzentrum wissen, das auch von der geografischen Lage her vor

Naturkatastrophen – Erdbeben, Stürme, Überschwemmungen etc. – gut geschützt sind. Ein internationaler Mineralölkonzern bezieht deshalb bereits bewusst Cloud-Computing-Services aus München.

3.4.9 Datentransport absichern

Das Rückgrat jeder Cloud bilden stabile, breitbandige Netze. Die Informationssicherheit lässt sich hier auf zwei Wegen gewährleisten. Den höchsten Schutz bieten dedizierte Punkt-zu-Punkt-Verbindungen vom Rechenzentrum zum Kunden. In MPLS-Netzen lässt sich für jeden Kunden eine vollständig isolierte Leitung einrichten. Die zweite Möglichkeit sind verschlüsselte Verbindungen, entweder über getunnelte Verbindungen im öffentlichen Internet (VPN, Virtual Private Networks) oder über SSL (Secure Socket Layer). Aber wie auch immer die Netzverbindung konkret realisiert wird, sie sollte genauso wie beim normalen Outsourcing doppelt ausgelegt sein und über zwei voneinander getrennte physikalische Verbindungen laufen. Fällt dann eine der beiden Leitungen aus, kann die andere nahtlos den Dienst der anderen übernehmen. Zudem empfiehlt es sich, alle Informationen gespiegelt in zwei verschiedenen Rechenzentren vorzuhalten. Das ist kein Widerspruch zur Cloud, wenn an beiden Standorten die Möglichkeit besteht, Server zwischen mehreren Unternehmen aufzuteilen.

3.4.10 Brandmauern schützen Netzsegmente

Dem Schutz der verschiedenen Netzsegmente dienen Firewalls. Sie kontrollieren den Datenverkehr und bestimmen regelbasiert, welche Pakete sie durchs Netzwerk schleusen und welche nicht. Das bietet Schutz vor unerlaubten Zugriffen. Zusätzlich erstellen sie Status- und Kontexttabellen aller Netzwerkverbindungen und erkennen so Korrelationen zwischen den Paketen (Stateful Inspection). Dadurch erkennen sie nach einem Verbindungsaufbau, ob ein System unaufgefordert Daten sendet, und blockieren diese. Viele Pakete gleichen Typs weisen etwa auf eine Denial-of-Service (DoS)-Attacke hin, die das Netzwerk lahmlegen soll. Firewalls sind damit auch ein wichtiger Erkennungsmechanismus, um die Verfügbarkeit von Daten und Anwendungen sicherzustellen. Sogenannte Computer Emergency Response Teams (CERT) achten im Rechenzentrum unter anderem darauf, dass sie jederzeit korrekt konfiguriert sind.

Einen Schritt weiter gehen Deep-Inspection-Firewalls, die Angriffe auf der Anwendungsebene erkennen. Sie blockieren Protokollverletzungen, Viren, Spam und weitere schädliche Inhalte wie etwa Trojaner. Das erschwert auch sogenannte Man-in-the-Middle-Attacken, bei denen Dritte die Kommunikation zwischen zwei Kommunikationspartnern abfangen und eine von beiden Parteien zu ungewollten Aktionen verleiten, indem sie sich als der vermeintliche Partner ausgeben. Mitarbeiter von Cloud-Providern führen solche Angriffe in regelmäßigen Abständen durch, um die Wirksamkeit der Firewall zu testen.

3.4.11 Monitoring und Frühwarnsysteme nutzen

Damit Sicherheit zu einem integralen Bestandteil aller Geschäftsprozesse im Cloud Computing wird, müssen sie kontinuierlich auf sicherheitsrelevante Komponenten überprüft und aktualisiert werden. In großen Rechenzentren sorgen spezielle Module auf den Servern automatisiert dafür, dass die vorgegebenen Sicherheitseinstellungen sich nicht verändern. Auch alle Firewalls, Virenscanner und Intrusion-Detection-Systeme (IDS) befinden sich unter ständiger automatischer Überwachung. Frühwarnsysteme spüren auf der Basis von Data-Mining-Verfahren Schwachstellen auf, bevor sie sich gefährlich auswirken. Angreifer nehmen sich oftmals viel Zeit, um über mehrere Stationen eine Lücke zu finden und einzudringen. Intelligente Analysesysteme (Security Information und Event Management) erkennen hierzu unter anderem anhand von Logfiles auffällige Muster und unterbinden solche Langzeitangriffe rechtzeitig.

Auch nach bestimmten Regularien lässt sich die IT-Infrastruktur im Rechenzentrum automatisiert überwachen, beispielsweise nach dem Sarbanes-Oxley Act (SOX). Dieses Kapitalmarktgesetz ist für an US-amerikanischen Börsen notierte Unternehmen relevant. Sie müssen ihr Internes Kontrollsystem (IKS) jährlich anhand seiner Richtlinien überprüfen, dokumentieren und von Wirtschaftsprüfern testieren lassen. Alle Passwörter des Systems müssen eine bestimmte Länge aufweisen. Ist das nicht der Fall, merkt das eine Lösung im Rechenzentrum, und Mitarbeiter des präventiven CERT-Teams können sofort nachsteuern.

3.4.12 Security beginnt in den Köpfen

Trotz aller Sicherheit, die ein großer Cloud-Provider bieten kann: Am Ende beginnt Security in den Köpfen der Mitarbeiter. Regelmäßige Workshops und Schulungen können die generelle Wachsamkeit im Umgang mit ICT-Lösungen steigern. Nur wer mögliche Sicherheitsprobleme kennt, kann sie durch richtiges Verhalten umgehen. Einige Dienstleister veranstalten interne und externe Programme, um das allgemeine Schutzniveau zu steigern und die richtige Sicherheitspolitik für ein Unternehmen zu entwickeln. Dass die Systeme anschließend alle so gestaltet sind, dass die Nutzer sie trotz aller Sicherheitsfunktionen noch sinnvoll einsetzen können, ist die Kunst des Cloud-Providers.

3.4.13 Mobile Cloud-Zugänge absichern

Bezieht ein Unternehmen alle Dienste und Daten über ein IP-Netz aus einem Cloud-Rechenzentrum, können Mitarbeiter mit einem beliebigen Endgerät überall und jederzeit sicher auf ihre persönliche Nutzeroberfläche zugreifen. Sie melden sich hierzu mittels eines USB-Sticks mit integrierter Smartcard am zentralen Server im Rechenzentrum an und können das Endgerät genauso nutzen wie einen klassischen Laptop – im Hotel, am Flughafen, beim Geschäftspartner oder im In-

ternetcafé. Stecken die Anwender den Stick in den USB-Anschluss des mit dem Internet verbundenen Rechners, stellt er über den integrierten Client automatisch eine verschlüsselte Verbindung zu einer Gegenstelle im Rechenzentrum her. Nach erfolgreicher Authentifikation erhält der Nutzer dann den Zugriff auf seine Daten und Applikationen. Zieht er den Stick wieder aus dem Desktop heraus, verbleiben auf dem Rechner keine Datenspuren.

Handys, PDAs und Smartphones, auf denen Applikationen installiert sind, lassen sich genauso zuverlässig verschlüsseln. Auch hier muss sich der Nutzer über eine Kryptokarte zunächst identifizieren. Kommt ihm das Endgerät abhanden, lässt es sich von Mitarbeitern im Rechenzentrum aus der Ferne in seinen Auslieferungszustand zurückversetzen. So gelangen Daten nicht in fremde Hände. Gleichzeitig gehen dem Unternehmen keine wertvollen Informationen verloren, da diese vollständig im Rechenzentrum gespeichert vorliegen. Während des normalen Betriebs findet automatisch eine regelmäßige Synchronisation aller Daten auf dem Endgerät mit den zentralen Servern statt.

Sicherheitsrichtlinien eines Unternehmens sind somit in der Wolke auch mobil umsetzbar. So lassen sich bestimmte Funktionen von Endgeräten in bestimmten Bereichen automatisiert abschalten, beispielsweise integrierte Kameras. Auf diese Weise gelangen in der Fertigungsindustrie keine Bilder von neuen Produkten ungewollt in fremde Hände oder ins Internet. Auch das Qualitätsmanagement erleidet keine Einbußen: Die Security-Experten im Rechenzentrum können neuen Patches in Ruhe prüfen, bevor sie sie auf die Rechner aufspielen. Ist für eine Sicherheitslücke, die eine akute Bedrohung für Laptops & Co bedeutet, noch kein elektronischer Flicken vorhanden („Day-Zero-Problem"), können sie die entsprechenden Zugänge kurzfristig per Knopfdruck aus der Ferne blockieren.

Rene Reutter und Thorsten Zenker, T-Systems

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

TecChannel-Links zum Thema	Webcode	Compact
Sicherheitsrisiken in der Cloud vermeiden	2034755	S.122
Die Fallen bei Virtualisierung und Cloud	2034813	S.111
Cloud Computing – US-Behörden lesen Daten mit	2036922	S.116
Cloud Computing: Admin-Jobs in Gefahr	2036722	S.120
Identitäts- und Berechtigungs-management in der Cloud	2034353	S.130
Private-Cloud-Lösungen im Überblick	2036787	S.133
Workshop – Verwaltungsumgebung für Private Clouds aufbauen	2036404	S.140
Workshop – Private Cloud mit Eucalyptus	2037292	S.147
Workshop – Aufbau einer Cloud mit VMware vCloud Director	2037250	S.154

3.5 Identitäts- und Berechtigungsmanagement in der Cloud

Ein modernes Identitäts- und Berechtigungsmanagement-System besteht aus verschiedenen Komponenten, die in der Identity-Management-Plattform zusammengefasst werden. Die tragenden Säulen dieses Systems sind die Authentifizierung, die Autorisierung von Identitäten und die Publizierung von Attributen. Die Sichtbarkeit, der Umfang und die Verwaltung von identitätsbezogenen Informationen, Daten und Berechtigungen erfordert in einem solchem Umfeld ein umfangreiches, flexibles und sicheres Identity und Access Management (IDA). Aufgrund unterschiedlicher Technologien und Verfahren (Software und Services) innerhalb einer Cloud zur Realisierung der geschäftlichen Anforderungen haben sich für das Cloud-Computing-IDA-System ein neuer Umfang und eine neue Komplexität entwickelt, die sich von klassischen IDA-Systemen unterscheiden. Die Herausforderung für diese IDA-Systeme besteht darin, eine integrativen Implementierung zu realisieren, die dem Konzept des Identity-as-a-Service Rechnung trägt.

3.5.1 Anforderungen an ein IDA-System

Ein effizientes Cloud Computing setzt ein IDA-System voraus, das administrative Aufgaben zusammenfasst und zusammenhängende Aufgaben administrierbar macht. Ein IDA-System muss in der Cloud die vollständige Kontrolle über jede Identität und jedes System haben. Dabei eingeschlossen sind die Administration von Identitäten natürlicher Personen, Servicekonten, physikalischer oder virtueller Computer und Server sowie Diensten (Identitäten). Diese Anforderungen kann ein herkömmliches IDA-System oft nur teilweise erfüllen. Idealerweise sollte das IDA-System alle relevanten Informationen speichern, auf deren Grundlage der Zugang oder die Verwaltbarkeit von Ressourcen innerhalb der Cloud gemäß den definierten Service Level Agreements (SLA) zu gewähren oder zu verweigern ist. Das IDA-System hält eine zusammenhängende Lösung für die Verwaltbarkeit des gesamten Lebenszyklus einer Identität und damit verbundenen Informationen, Anforderungen und Berechtigungen bereit. Funktional wird dabei in zwei Komponenten unterschieden: die Anlage und Löschung von Identitäten (Provisioning) und die Verwaltung von Identitäten (Administration). Die Verwaltbarkeit von Identitäten definiert die Durchführung und Übertragung (Delegation) von administrativen Tätigkeiten und den Zugang zu Self-Service-Komponenten.

3.5.2 Identitäten und Berechtigungen

In einer Cloud stellen die Anlage und Löschung von Identitäten einen Just-In-Time- oder einen On-Demand-Prozess dar. Dabei können Identitäten verteilt angelegt werden, ohne dass alle Informationen einer Identität in den angeschlossenen

Systemen oder Anwendungen verfügbar sind. Löschungen von Identitäten sollten sofort und unmittelbar, falls erforderlich, an alle Systeme und Anwendungen innerhalb der Cloud synchronisiert werden, da jede Verzögerung ein Sicherheitsrisiko beinhalten kann. IDA stellt innerhalb der Cloud sicher, dass auch verbundene Identitäten gemäß der Anforderung dysfunktional werden. Berechtigungen werden innerhalb des IDA durch eine Anzahl von Attributen dargestellt, die Zugänge und Berechtigungen für eine authentifizierte Identität (Authenticated Security Principal) beschreiben. Da Cloud-basierte Anwendungen oft eine eigene Verwaltung zur Autorisierung beziehungsweise Berechtigung beinhalten, ist hier unter Umständen die Hilfe von allgemeingültigen Autorisierungstechnologien gefragt.

Die Möglichkeit, dass eine Person innerhalb der Cloud mehrere Identitäten besitzen kann, macht eine übergeordnete Zuordnung notwendig. Mithilfe eines Synchronisationsautomats können verschiedene Identitäten über eine eindeutigen ID zusammengeführt und so die zentrale Administration sichergestellt werden.

3.5.3 Administration von Identitäten

Das zentrale IDA-System ermöglicht es, die Administration der verschiedenen Identitäten für unterschiedliche Anwendungen und Systeme (Service Provider) zusammenzufassen. Benutzer werden über eindeutige Werte oder Attributinhalte zentral identifiziert und definiert. Synonyme und sekundäre Identitäten (Discrete Identities) sollten dabei unterstützt werden. Um die Privatsphäre des Benutzers zu schützen, werden nur die Informationen für die unterschiedlichen Service Provider bereitgestellt, die zwingend erforderlich sind. Fragmentierte Benutzer-Logins für unterschiedliche Anwendungen und Systeme sind zu vermeiden. Authentifizierungsprozesse innerhalb der Cloud sollten für den Benutzer transparent sein.

In einem klassischem IDA-Modell werden beständige Beziehungen zwischen einer Identität und einer Organisation abgebildet. Innerhalb der Cloud können sich diese Beziehungen schnell und dynamisch ändern. Diese Veränderungen müssen durch das IDA-System abgebildet werden können. Herausforderungen wie die Publizierung von neuen Passwörtern oder Anmeldeinformationen bei den unterschiedlichen Service Providern stellen neue Anforderungen an das IDA-System.

Grundgedanken des Cloud Computings nach sollte ein IDA-System eine hohe Skalierbarkeit in der Qualität und Quantität der Verarbeitung von Identitätsinformationen haben. Single-Sign-On-Verfahren (SSO) erfordern eine schnelle und dynamische Verteilung von Informationen. Die unterschiedlichen Anforderungen an und von Ressourcen können die Verarbeitungsdichte innerhalb des IDA-Systems erhöhen. Das IDA-System sollte mit allen in der Cloud vorhandenen IT-Systemen, -Verfahren und -Prozessen direkt oder indirekt zusammenarbeiten. Dabei ist Ziel, die IDA-Prozesse so zu gestalten, dass für die Erfüllung aller Aufgaben ein Minimum an Aktionen mit geringem Umfang notwendig ist. Da Benutzer, Verfahren, Prozesse und geschäftliche Anforderungen unterschiedliche Anforderungen an Sicherheit und Funktionalität innerhalb der Cloud haben können, ist es not-

wendig, einen gemeinsamen Standard zum Schutz der IT-Infrastruktur mit den Service Providern zu definieren und diesen für die Bereitstellung und Publizierung von Anwendungen und/oder Informationen bereitzustellen. Sicherheits-Audits und Logging-Verfahren sind unverzichtbarere Bestandteile des IDA-Systems.

3.5.4 Sicherheit bleibt Sicherheit

Grundlegend unterscheidet sich die Informationssicherheit im Cloud Computing nicht von den Sicherheitsmaßnahmen in herkömmlichen IT-Infrastrukturen. Anforderungen, Richtlinien, Compliance und Governance sind identisch. Aus Sicht des IDA müssen die Definitionen für die Benutzeridentität neu überdacht und der Begriff erweitert werden. IT-Transaktionen werden zunehmend automatisiert. Die Interaktion zwischen Software und Systemen ähnelt immer stärker der Mensch-Maschine-Interaktion. Aus diesem Grund sind die Auswirkungen von Bereitstellung, Authentifizierung, Autorisierung und Administration von Identitäten für das Cloud Computing neu zu überdenken. Der Aspekt der Sicherheit wird für das Cloud Computing allerdings nicht ausschließlich durch die Bereitstellung von Sicherheitstechnologien definiert. Vielmehr ist das Auslagern von unternehmenskritischen Prozessen, Daten und Informationen eine Frage des Vertrauens. Da diese Aspekte aber bereits in heute bestehenden IT-Infrastrukturen durch Verfahren des Outsourcings und die Integration von Drittanbietern weit fortgeschritten sind, scheint ausschließlich eine Erweiterung dieser Überlegungen notwendig.

3.5.5 Vorteile des Cloud Computing

Wo immer Ressourcenbedarf mittelfristig kaum oder nur schwer abzuschätzen ist, wird der Nutzen des Cloud Computing für den Anwender deutlich. Die kurzfristige Bereitstellung zusätzlicher Ressourcen ist eines der unverzichtbaren Cloud-Paradigmen und somit von enormem Wert. Je nach Geschäftsmodell und benötigten Ressourcen lassen sich die Kosten für IT-Infrastrukturen reduzieren. Bedingt durch den Aufbau neuer Strukturen kann die Standardisierung vorangetrieben werden; somit lassen sich ebenfalls Kosten senken.

Verfügbarkeit und Zugang zur Cloud stellen je nach Architektur und Authentifizierungsmethode große Vorteile dar, die heute bereits für die Cloud sprechen. Sogenannte Time-To-Market-Zeiten können durch die dynamische Bereitstellung von IT-Infrastruktur reduziert werden mit der Folge, dass Cloud-Anwendungen schneller entwickelt, bereitgestellt und einsatzbereit sind. Heute ist Outsourcing in größeren IT-Infrastrukturen allgegenwärtig. Die durch Service Provider in der Cloud angebotenen Leistungen und Abrechnungsmodelle erleichtern die Möglichkeit des Outsourcings. Die Absprache der Service Level Agreements (SLA) vereinfacht sich dadurch, dass Standards bei der Bereitstellung einer Leistung durch den Provider verfügbar sind, und bietet dem Nutzer eine hohes Maß an Verlässlichkeit.

Andreas Bünseler

3.6 Private-Cloud-Lösungen im Überblick

Für die Nutzer von Public-Cloud-Diensten spielt die zugrunde liegende Cloud-Infrastruktur kaum eine Rolle. Sie obliegt in der Regel dem Anbieter. Wer jedoch im eigenen Haus eine Private Cloud aufbauen und betreiben will, sollte einen Blick auf die Komplettangebote der großen Anbieter werfen. Sie bündeln nicht nur Server-, Storage- und Netzwerk-Hardware, sondern auch eine Reihe von Tools, mit denen sich Cloud-Services im Unternehmen entwerfen, betreiben und verwalten lassen. Cloud Computing erfordert nicht nur eine deduzierte Hardware, die speziell an die neue Technologie angepasst ist, auch stellt auch besondere Anforderungen an die Ausfallsicherheit und die Skalierbarkeit. Zusätzlich müssen die Systeme leicht zu bedienen und zu verwalten sein.

Wir haben uns die wichtigsten Private-Cloud-Komplettsysteme von IBM (www.ibm.de), HP (www.hp.com), Fujitsu (www.fujitsu.com) und Cisco (www.cisco.com) angesehen und erläutern diese detailliert.

3.6.1 Hewlett-Packard: HP CloudSystem

Das Cloud-Angebot von HP umfasst fertig konfigurierte Cloud-Dienste sowie Tools zum Aufbau und zur Verwaltung von privaten und Public Clouds. Ein zentraler Baustein ist HP CloudSystem, eine komplette und integrierte IT-Umgebung, mit der Unternehmen IT-Services in hybriden Cloud-Umgebungen bereitstellen, verwalten und nutzen können. HP CloudSystem umfasst die Plattform HP BladeSystem Matrix und die Software HP Cloud Service Automation. Damit schafft der Anbieter eine einheitliche Steuerung, Sicherheit und Compliance für Anwendungen sowie für physikalische und virtuelle IT-Infrastrukturen.

Ein Schlüsselelement ist dabei die Konvergenz der IT-Komponenten in Form der Blade System Matrix. In der Matrix vereint HP alle wichtigen IT-Ressourcen in einem Verbund. Konkret sind das Blades als Rechenknoten (Compute), Speichersysteme (Storage) zur Ablage der Daten und Applikationen, das Netzwerk und die Verwaltungssoftware. HP bezeichnete die Blade System Matrix auch als Data-Center-in-a-Box, also als Rechenzentrum in einer geschlossenen Einheit. Die Marketiers des IT-Konzerns stellen sie zudem als Referenz für HPs Converged Infrastructure dar. Die Matrix umfasst auf engstem Raum alles, was für den Betrieb von Anwendungen notwendig ist.

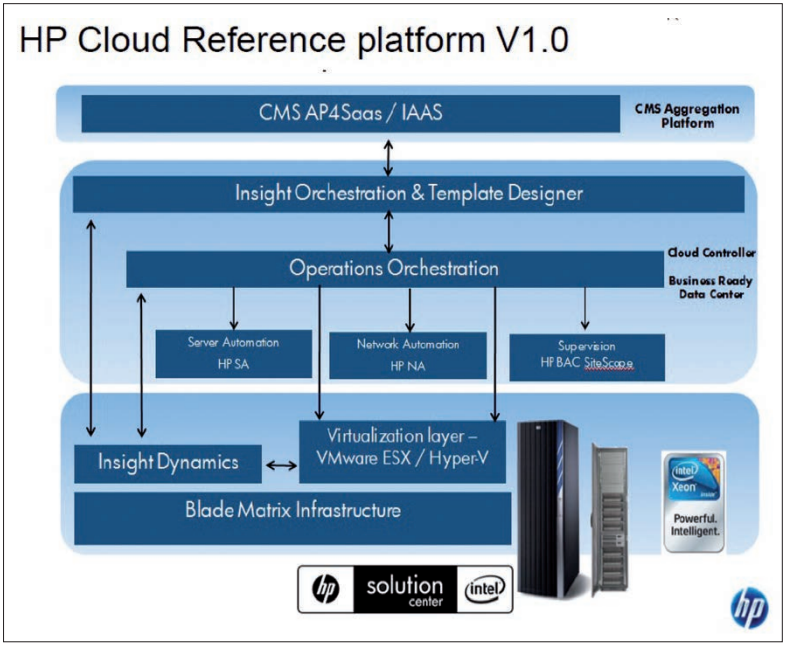
3.6.2 Die Blaupause der HP Cloud Reference Platform

Den architektonischen Unterbau des HP Cloud Computing bildet die „HP Cloud Reference Platform“. Die Software Insight Dynamics dient als darüberliegende Verwaltungsschicht. Hinzu kommen die Virtualisierungsdienste von VMware vSphere oder Microsoft Hyper-V. Die Orchestrierung erfolgt durch einen Cloud

Controller. Sie liefert die Vorlagen für die Virtualisierung. Zur Modellierung der Systeme stellt HP den Insight Orchestrator zur Verfügung. Da moderne IT-Dienste immer aus mehreren Serversystemen und Speichern bestehen, müssen auch die Beziehungen der einzelnen Serverdienste zueinander modelliert und abgebildet werden. Dies erfolgt in den „Cloud Maps". Sie legen die Architektur einer Anwendung fest. Einzelne Server werden in einem Template beschrieben. Die Cloud Maps führen die Konzepte fort, die VMware in den vApps festlegt. Eine vApp umfasst mehrere Serversysteme in einer vSphere-Applikation. Die Definition der Cloud Maps wiederum erfolgt durch spezielle „Architekten", die Cloud Map Designer.

3.6.3 Cloud Maps definieren die Applikationsumgebungen

Diese Cloud Maps werden dann den Anwendern bereitgestellt. Sie wiederum definieren dann anhand der vorkonfigurierten Cloud Maps ihren Dienst selbst. Dazu bedarf es noch eines weiteren Moduls, des Self-Service-Portals. Es stellt die oberste Schicht der HP Cloud Reference Platform dar. Im Self-Service-Portal wird ein Katalog der Private-Cloud-Services veröffentlicht. Der Katalog liefert damit die oberste Stufe eines Cloud-Dienstes.

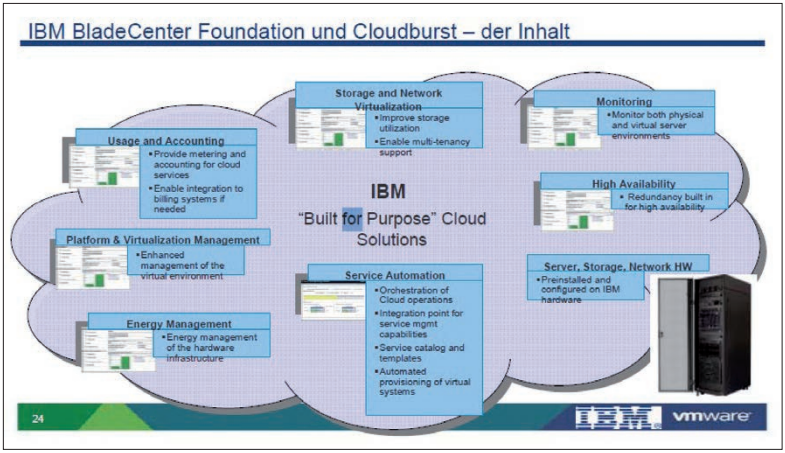


Details: So sieht der prinzipielle Aufbau einer HP Cloud Reference Platform aus. (Quelle: HP)

Die Umsetzung eines Cloud-Dienstes auf die Rechner-Blades erfolgt durch die dazwischenliegenden Module des Designers, des Orchestrators und aller weiteren Softwaresysteme. Hinzu kommen Skripte, Workflows und eine Reihe weiterer Automatismen.

3.6.4 IBM: System x und CloudBurst

IBM bietet mehrere Systeme für den Aufbau einer Cloud an. Das Unternehmen offeriert ein umfangreiches Angebot an Hardware, Software und Services, die es in unterschiedlichen Paketen auf den Markt bringt. Deren Ziel liegt in einer umfassenden Unterstützung aller heute verfügbaren Hardwaresysteme, den Softwareplattformen und Services. Dies reicht von x86-Servern über Power-Systeme bis hin zum Großrechner. Dabei lassen sich Workloads auf Mainframes, POWER7- und x86-Systeme verteilen und als gemeinsames virtualisiertes System verwalten.



Vielfältig: IBM liefert mehrere Cloud-Systeme. In CloudBurst fasst Big Blue Hardware, Software und Services in einer vorgefertigten Einheit für das Private-Cloud-Computing zusammen. (Quelle: IBM)

Das „IBM System X Privat Cloud Offering" besteht aus Standardhardwarekomponenten und Rack-Servern. Als Virtualisierungsplattform kommt Hyper-V von Microsoft zum Einsatz. Das System wird durch Partner vertrieben und adaptiert. Die Systemreihe „IBM System X und VMware" wird mit den Hypervisoren von VMware gebündelt. Die Hardwareplattform von IBM System X und VMware basiert auf Blade-Systemen und einem Blade-Chassis.

Das Flaggschiff der IBM-Cloud-Systeme ist CloudBurst / ISDM. Die Hardware basiert auf Rechner-Blades. Die Hypervisoren können von VMware, Microsoft, Citrix oder anderen wie etwa KVM stammen.

Die CloudBurst umfasst laut Hersteller sämtliche Hardware, die zum Betrieb von Anwendungen benötigt wird. Dazu gehören x86-Blades als Serversysteme, Speicher und die Netzwerktechnik. Die CloudBurst wird als vorkonfiguriertes Rechnersystem montiert und geliefert. Die Verwaltung erfolgt durch die Tivoli-Familie, wie etwa den Tivoli Provisioning Manager. Als Einsatzzweck für den CloudBurst sieht IBM vor allem dynamische Cloud-Strukturen. Durch ein Self-Service-Portal kann sich der Entwickler dabei eine Ausführungsumgebung selbst zusammenstellen. Die Grundlage dazu stellen Templates dar. Eingeschlossen dabei sind auch Workflows für die Freigabe und die Steuerung des Genehmigungsverfahren, der Verrechnung und des Deployments.

3.6.5 Weitere Details der CloudBurst-Architektur

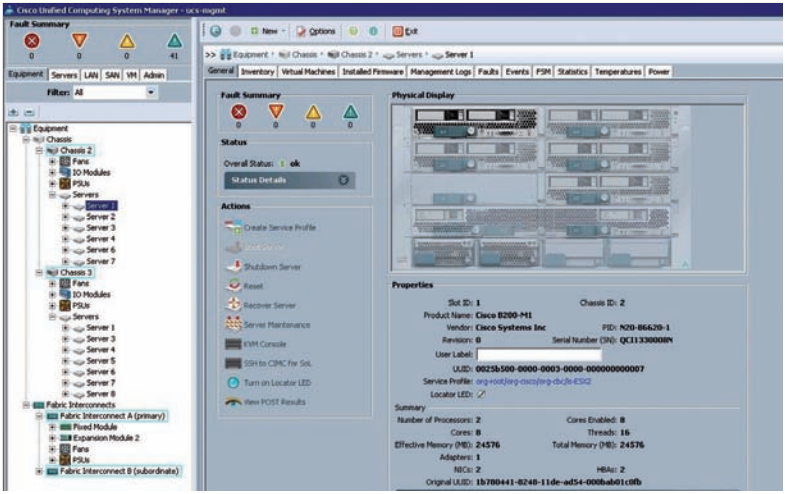
Die architektonische Grundlage der IBM-Blades ist in der Blade Server Foundation festgeschrieben. Spezifiziert sind darin die Hardwareverwaltung, das Monitoring der Hardware, die Virtualisierung des Netzwerks und der Speicher, das Energiemanagement und die allgemeinen Verwaltung der virtuellen Strukturen. Zusätzlich packt IBM bei der CloudBurst Software für „Usage und Accounting“ und „Service Automation“ dazu. Diese beiden Bausteine helfen bei der Verwaltung von Service-Templates sowie bei der Verrechnung der Nutzung an die Fachbereiche und ähnlicher fortgeschrittener Verwaltungsaufgaben.

Das Unternehmen adressiert mit seinem Angebot unterschiedliche Anwendungsszenarien der Fachbereiche. In vordefinierten „Workloads“ fasst IBM seine Ansätze zusammen. Diese Workloads sind beispielsweise für den Bereich „Analytics“ (Business Intelligence), Collaboration, Software Development, Test oder Desktop-Virtualisierung verfügbar. Bei den Workloads handelt es sich im Prinzip um die Beschreibungen von Diensten. Die Abbildung auf die notwendige IT-Plattform übernehmen die Tool-Sets der Tivoli-Familie, darunter etwa der Tivoli Service Automation Manager. Mit diesem will IBM Geschäfts- und IT-Prozesse miteinander verknüpfen und auf der Infrastruktur implementieren.

3.6.6 Cisco: Unfied Computing System für die Cloud

Der Netzausrüster Cisco ist erst seit wenigen Jahren als umfassender Anbieter von IT-Hardware aktiv. Sein Debüt als Systemlieferant gab das Unternehmen mit der Vorstellung des Unified Computing System (UCS). Darin bündelt Cisco seine Netzwerkbaugruppen mit Serversystemen und Verwaltungssoftware. Über Fabric Interconnect-Switche erfolgt dabei die Anbindung der Speichersysteme und des Datennetzwerks. In den Interconnect-Modulen werden somit Fibre Channel (FC)-SAN und LAN zusammengebracht. Im Chassis befinden sich dabei keine Switche mehr. Gleichzeitig wird damit die Anzahl der benötigten Netzbaugruppen reduziert. Die Anbindung der Systeme erfolgt über schnelle 10-GBit-Interfaces. Diese können durch Virtual Interface Cards in bis zu 128 logische Adapter für den

Server aufgesplittet werden. Diese logischen Adapter können Ethernet und Fiber Channel Adapter sein. Die Kommunikation der Speichersysteme erfolgt auf der Serverseite über Fabric-Interconnect-Switches durch Fibre Channel over Ethernet (FCoE). Im Switch erfolgt dann die Umsetzung von FCoE in das native Fibre-Channel-Protokoll. Als Server setzt Cisco auf Blades mit zwei Sockets und bis zu 384 GByte RAM. Es stehen aber auch Vier-Socket-Systeme zur Verfügung. Diese Systeme zielen auf den Einsatz in virtuellen Szenarien.



In der Praxis: Mittels Unified Computing System Manager bündelt Cisco seine Netzwerkbaugruppen mit den Serversystemen und der Verwaltungssoftware.

Die dritte zentrale Komponente, die für den Betrieb eines Applikationsdienstes notwendig ist – der Speicher -, bleibt dabei außen vor. Die Speichersysteme werden über Standardschnittstellen mit den Rechnersystemen verknüpft. Hierbei setzt Cisco auf die Speichersysteme von EMC und NetApp. Die Verwaltung erledigt eine integrierte Management-Applikation. Diese läuft direkt in den Fabric-Interconnect-Switches. Damit wird die Administration der gesamten Umgebung zentralisiert. Die Managementapplikation wird zur Verwaltung des Netzwerkes (LAN und SAN) und der Einstellungen der Server herangezogen. Zu diesen Basiseinstellungen der Server gehören die Angaben im Server-BIOS über die Netzwerkanbindung und die Boot-Reihenfolge.

Die Konfiguration der Server wird in Serverprofilen hinterlegt – XML-Dateien, die Hard- und Software eines Servers beschreiben. Durch das Laden eines Serverprofils auf eine Serverhardware wird auch das Boot-Image des Servers bestimmt. Booten kann ein Server vom SAN, vom LAN oder von einer lokalen DAS-Platte. Durch das Boot-Image werden anschließend die Rolle und die Funktion des Servers be-

stimmt. Durch eine Funktion, die Cisco als „Hardware-vMotion“ bezeichnet, lässt sich der Einsatzzweck eines Servers leicht ändern und anpassen. Hardware-vMotion ermöglicht die dynamische Neukonfiguration eines Servers. So kann beispielweise ein Server, der tagsüber als Träger von virtuellen Desktops eingesetzt wird, nachts kurzerhand zum Backup-Server werden.

Als Hypervisor zur Virtualisierung setzt Cisco auf die Software von VMware. Der Virtualisierungsspezialist steuert den Hypervisor bei und liefert mit vCenter und vCloud Director ein Tool-Set zur Verwaltung von Clouds.

3.6.7 Fujitsu: Building Blocks und Blade Systems für die Cloud

Fujitsu bietet mehrere Konstellationen seiner für die Cloud vorgesehenen Systeme. Im Zentrum der größten Cloud-Box steht Primergy CX 1000. Dieses System zielt in erster Linie auf den Einsatz bei Hostern oder großen Unternehmen. Die Blade-Systeme BX400 und BX900 sind kleiner und weisen eine feinere Skalierbarkeit auf. Durch die Nutzung von Rechner-Blades lässt sich die Leistung hierbei in kleinen Stückelungen anpassen. Vollständig der Cloud verschrieben sind die Systeme, die als DI-Block (Dynamic Infrastructure) bezeichnet werden. Alle Systeme sind oder werden als Referenzarchitekturen im Rahmen des Intel-Cloud-Builder-Programms zertifiziert.

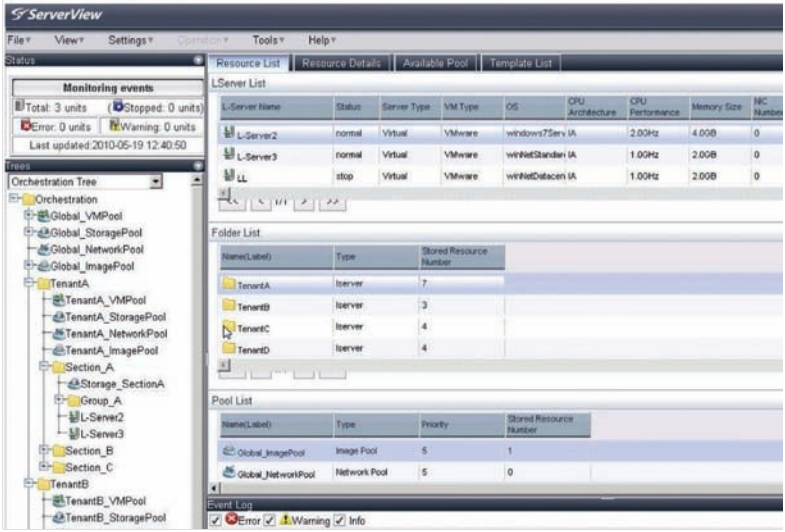
3.6.8 Für Hoster: CX 1000

Das Modell CX 1000 ist Rack-basiert. Es umfasst bis zu 38 19 Zoll-Servereinschübe. Die Netzwerkanbindung wird durch bis zu fünf integrierte Switches gebildet. Hierbei setzt Fujitsu auf die Modelle von Brocade. Das Storage-Subsystem wird extern angebunden. Die Kühlung des Racks erfolgt durch spezielle Ventilatoren an der Oberseite. Dadurch werden Kaltgänge überflüssig. Die Racks lassen sich so direkt aneinanderstellen. Der Zugang zum System erfolgt ausschließlich auf der Vorderseite. Fujitsu liefert das System vollständig und verkabelt es als eine Einheit. Der Cloud-Software-Stack wird dabei durch VMwares vCloud Director gebildet. Zur Verwaltung des Systems bietet Fujitsu seine Tools aus der Reihe „ServerView“ an. Die Managementsoftware von „ServerView“ besteht aus einer Sammlung von Tools unter anderem zum Server-Deployment und zum Fernzugriff.

3.6.9 Blades: BX400 und BX900

Die Private-Cloud-Infrastruktur der beiden Blade-Systeme BX400 und BX900 basiert ebenfalls auf den Spezifikationen des Intel-Cloud-Builder-Programms. Die BX400 kann auf zehn Blades ausgebaut werden, die BX900 auf 18. Dabei stehen

Blade-Server mit neun, zwölf oder 18 DIMM-Speicher-Slots zur Verfügung. Als Speicher kommt das Fujitsu-Produkt EternusDX 90 zum Einsatz. Das Management des Systems erfolgt durch einen Managementserver RX 300. Als Verwaltungssoftware zum Aufbau von Cloud-Strukturen nutzt der Hersteller den Microsoft Virtual Machine Manager und dessen Self-Service-Portal.



Tool: Der Resource Orchestrator hilft bei der Provisionierung und Orchestrierung einer Fujitsu-Cloud.

3.6.10 DI-Building-Blocks

Die dritte Systemreihe sind die DI-Building-Blocks, also Bausteine für Server, Storage und Netzwerkkomponenten. Diese werden für bestimmte Einsatzszenarien im Rechenzentrum vorspezifiziert, getestet und integriert, sodass sie schnell in bestehende Rechenzentrumsinfrastrukturen integriert werden können.

Für die Verwaltung von Cloud-Strukturen hat Fujitsu das ServerView-Tool-Set erweitert: Die neuen Module heißen Resource Coordinator Virtual Server Edition (RCVE) und Resource Orchestrator (ROR). Letzteres hilft bei der Provisionierung und Orchestrierung von Server-, Storage- und Netzwerk-Ressourcen. Fujitsu offeriert seine DI-Blocks ab dem vierten Quartal 2011.

Johann Baumeister

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

3.7 Workshop – Verwaltungsumgebung für Private Clouds aufbauen

Die Cloud-Technologie schickt sich an, die IT-Landschaft umzukrempeln. Doch dabei ist nicht alles neu, wie einige Protagonisten behaupten. Die Basis aller Cloud-Modelle, egal ob es sich dabei um die Private, die Public oder die Hybride Cloud handelt, bilden Serversysteme, wie wir sie auch heute kennen und verwenden. Microsofts Tool-Sammlung zur System- und Serververwaltung ist das System Center. Dessen Herzstück zur Verwaltung virtueller Strukturen ist der Virtual Machine Manager. Er adressiert vor allem den Aufbau einer Private Cloud. Der Virtual Machine Manager 2012 wird derzeit um Funktionen zum Aufbau und Verwaltung von Clouds erweitert und soll noch im zweiten Halbjahr 2011 verfügbar sein.

Unterlegt durch Assistenten sollen dabei Erzeugung und Verwaltung von Clouds zum Kinderspiel werden. Wir haben uns im Rahmen dieses Workshops den System Center Virtual Machine Manager 2012 Beta (SCVMM 2012) von Microsoft angesehen und erklären praxisnah, wie man mit dem neuen „Cloud Manager" eine Private Cloud erstellt.

3.7.1 Der Aufbau des System Center Virtual Machine Manager

Zum Umfang des System Center Virtual Machine Managers (SCVMM) gehören mehreren Komponenten: der Virtual-Machine-Manager-Server, die Verwaltungskonsole, die Agenten und ein Self-Service-Portal. Für diesen Bericht haben wir uns das aktuelle Pre-Release des Virtual Machine Managers geladen und installiert. Große Änderungen zur endgültigen Version sind nicht zu erwarten; die hier gemachten Aussagen werden also auch in der finalen Version gelten. Verfügbar ist die Software über das Abonnement beziehungsweise durch Registrierung bei Microsoft Technet (http://technet.microsoft.com) oder auch aus anderen Quellen.

SCVMM2012.EVALVHD.BETA.part01	25.03.2011 12:09	Anwendung	1.048.582 KB
SCVMM2012.EVALVHD.BETA.part02.rar	25.03.2011 12:10	RAR-Datei	1.048.576 KB
SCVMM2012.EVALVHD.BETA.part03.rar	25.03.2011 14:27	RAR-Datei	1.048.576 KB
SCVMM2012.EVALVHD.BETA.part04.rar	25.03.2011 14:25	RAR-Datei	1.048.576 KB
SCVMM2012.EVALVHD.BETA.part05.rar	25.03.2011 14:20	RAR-Datei	1.048.576 KB

Daten-Bundle: Die EXE-Datei erzeugt aus den geladenen Modulen eine VHD-Datei. Diese ist direkt als virtuelle Maschine zu verwenden.

Der SCVMM umfasst insgesamt sechs Dateien: eine EXE-Datei und fünf RAR-Anhänge. Zusammen ergeben diese etwas mehr als fünf GByte. Da eine Datei dieser Größe kaum einzeln geladen oder kopiert werden kann, hat Microsoft den

SCVMM in die genannten sechs Bausteine zerlegt. Um den SCVMM wieder „in einem Stück“ zu erhalten, müssen Sie nur die EXE-Datei starten. Diese generiert aus den sechs Einzelstücken eine einzige große VHD-Datei – vorher sollten Sie aber das Sixpack auf einen USB-Stick kopieren und dann auf ihr Testsystem übertragen. Dort starten Sie anschließend den Rebuild-Prozess. Dieser benötigt einige Minuten, daher müssen Sie ein wenig Geduld mitbringen. Das Ergebnis des Rebuild-Prozesses ist eine einzige große VHD-Datei. Sie umfasst circa 12 GByte und beinhaltet eine fertig konfigurierte virtuelle Maschine mit dem Windows Server, einem SQL Server und dem SCVMM 2012 Beta.

3.7.2 Arbeitsumgebung für SCVMM 2012 einrichten

Unsere Arbeitsumgebung bestand aus mehreren Rechnersystemen. Es beinhaltete einer Hyper-V-Computer, einem VMware-vCenter- und einem ESX-Server. Die Hyper-V-Server und der ESX-Server dienten als Ressourcen-Pool für unsere Private Cloud. Daneben stand eine weiterer Hyper-V zur Verfügung. Auf diesem haben wir eine virtuelle Maschine eingerichtet und darin den SCVMM als Gastsystem betrieben. Die erzeugte VHD-Datei können Sie nun direkt in Ihren Hyper-V-Server integrieren. Damit erhalten Sie sehr schnell eine lauffähige Version des SCVMM. Starten Sie dazu ihre Hyper-V-Verwaltung und rufen unter dem Menüpunkt *Aktion* und den Eintrag *Neu* die Option *Virtueller Computer* auf. Damit erzeugen Sie eine neue virtuelle Maschine im Kontext des Hyper-V. Es öffnet sich ein Assistent, in dem Sie alle Konfigurationseinstellungen eingeben müssen. Dies sind zuerst der Name der virtuellen Maschine und der Speicherort. Da Sie die virtuelle Maschine bereits als VHD-Datei vorliegen haben, legen Sie den virtuellen Computer am besten in das Verzeichnis, in dem auch die vorher erzeugte VHD-Datei liegt. Aktivieren Sie dazu die Checkbox *Virtuellen Computer an einem anderen Ort speichern* und selektieren anschließend die Position, an der Sie den neuen virtuellen Computer ablegen wollen.

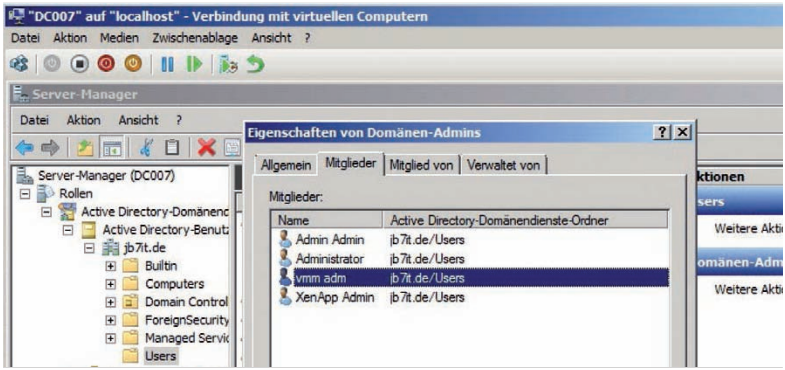
3.7.3 Virtuelle Maschine für den SCVMM erzeugen

Bei der Menge des Speichers für den neuen virtuellen Computer sollten Sie mindestens 4 GByte zuweisen. Wenn es um die Netzwerkkarten geht, müssen Sie Ihre bestehende Netzwerkkonfiguration berücksichtigen. Da unsere virtuelle Maschine weitere Hyper-V und vielleicht auch ESX-Server oder XenServer verwalten soll, muss sie natürlich über das Netzwerk mit all diesen Systemen eine Verbindung aufbauen können. Sie benötigen außerdem das Active Directory und müssen auch damit kommunizieren können. Es hängt nun letztendlich an Ihrem Netzwerkdesign, welche und wie viele Netzwerk-Interfaces Sie Ihrem virtuellen Computer zuweisen wollen oder müssen. Im Rahmen des Assistenten aber können Sie nur ein Netzwerk-Interface direkt zuweisen. Wenn Sie mehrere benötigen, müssen Sie diese später zuweisen und konfigurieren.

Bei der nächsten Frage nach der Lokation der virtuellen Festplatte geben Sie die VHD-Datei an, die wir vorher erzeugt haben – und damit ist die Konfiguration der VMM abgeschlossen. Bestätigen Sie anschließend den letzten Bildschirm. Nun finden Sie in der Übersicht der virtuellen Maschinen im Hyper-V Manager eine neue virtuelle Maschine. Diese können Sie nun direkt starten.

3.7.4 Die Konfiguration der virtuellen Maschine

Beim ersten Start der neuen virtuellen Maschine mit dem SCVMM werden Sie einige Meldungen erhalten. Das System passt zuerst die Registry an, konfiguriert Devices und das System. Nach der Auswahl der länderspezifische Einstellung und des Tastaturlayout müssen Sie die Lizenzvereinbarungen bestätigen. Anschließend erfolgt erneut ein Neustart des Rechners, und es erscheinen einige Meldungen zur weiteren Konfiguration der Systemumgebung.



Achtung: Der System Center Virtual Machine Manager 2012 benötigt einen Benutzer-Account. Sie sollten einen eigenen User dafür anlegen.

Der gesamte Vorgang aber ist fast vollständig automatisiert, und Sie brauchen hier kaum Eingaben zu machen. Nach etwa fünf bis zehn Minuten ist die Konfiguration ihrer neuen virtuellen Maschinen durchlaufen, und es erscheint der Hinweis, dass Sie bei der ersten Anmeldung zuerst das Passwort ändern müssen. An dieser Stelle ein Tipp: Die Windows Policies verlangen die Bereitstellung eines strengen Passwortes mit acht Zeichen Länge und Sonderzeichen. Verwenden Sie für den Anfang dennoch ein möglichst einfaches Passwort und achten Sie auf die Tastaturbelegung. Dieser Hinweis ist auch als allgemeiner Ratschlag zu verstehen. Der Autor dieser Zeilen hat schon viel Zeit wegen unklaren Passwortverhältnissen verplempert. Das Problem dabei ist: Wenn Sie ein Passwort mit Sonderzeichen eintippen und in diesem Moment eine US-Tastaturbelegung verwenden und später diese Tastaturbelegung beispielsweise auf deutsches Layout geändert wird, so

kennen Sie mitunter ihr Passwort nicht, denn wer hat schon alle Tastaturbelegungen im Kopf? Das Fatale daran ist aber eben, dass einem die Situation zuerst möglicherweise gar nicht bewusst ist. Um dennoch die Windows Policies zufriedenzustellen, sollten Sie daher auf die Unterschiede in der Tastaturbelegung für Passwörter am besten generell verzichten.

Nach der Änderung des Passwortes wird die virtuelle Maschine mit dem Windows Server, dem SQL Server und dem Virtual Machine Manager gestartet. Auf dem Desktop diese Systems finden Sie nun ein Icon mit der Bezeichnung *Configure VMM 2012*. Dieses Icon müssen Sie aktivieren, um die Konfiguration des SCVMM 2012 abzuschließen. Ein Assistent führt Sie auch durch diese Schritte

3.7.5 Netzwerkeinstellungen anpassen

Doch vorher sollten Sie noch die weitere Windows- und Netzwerkkonfiguration anpassen. Wie oben erwähnt, kann bei der Integration der virtuellen Maschine in die Verwaltung des Hyper-V durch den Assistenten lediglich eine Netzwerkkarte zugewiesen werden. Falls Sie nur eine Karte in diesem Rechner haben und über diese Verkabelung auch das Internet erreichen können, mag diese Verschaltung vollständig und passend sein. In unserer Arbeitsumgebung allerdings verwendeten wir zwei physikalische und eine logische (virtuelle) Netzwerkkarte für unsere virtuellen Maschinen. Durch die beiden physischen Exemplare erhielt unser Testrechner Zugang zum internen LAN und via DHCP zum Internet. Über die dritte virtuelle Netzwerkverbindung hatte die virtuelle Maschine mit dem SCVMM Zugang zum Host-System des Hyper-V.

Im nächsten Schritt müssen Sie nun Windows aktivieren. Andernfalls wird ihnen das System nach dem Ablauf der Testzeit den Dienst versagen. Dazu müssen Sie einen Produktschlüssel bereitstellen, den Windows Server mit dem SCVMM in eine bestehende Domäne einhängen und die DNS-Namensauflösung anpassen. Damit sind die Vorbereitungen abgeschlossen, und wir wenden uns dem SCVMM zu.

3.7.6 Grundkonfiguration des SCVMM 2012 durchführen

Nach der Richtigstellung der Netzwerkeinstelllungen und der Konfiguration von Windows starten wir die Konfiguration des VMM. Sie finden dazu den Link *Configure VMM 2012* auf Ihrem Desktop. Diesen sollten Sie nun aktivieren. Nach dem Eröffnungsbildschirm erscheint zuerst die Maske bezüglich der Registrierung der Software. Diese Angabe sollten Sie so, wie sie ist, bestätigen.

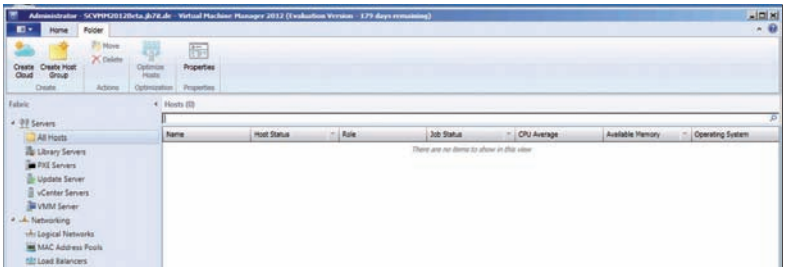
In der nächsten Maske werden Sie gefragt, ob Sie Updates aktivieren wollen. Wir haben dies ebenfalls bestätigt. Für die Updates wird der Zugang zum Internet benötigt, daher muss die Verbindung zum Microsoft-Website bereits möglich sein. Die dritte Maske fragt nach der Konfiguration der Datenbank. Wie eingangs erwähnt, umfasst die virtuelle Maschine auch einen SQL Server; er verwaltet die Da-

tenbank des SCVMM. Im unteren Bereich könnten Sie nun eine bestehende Datenbank angeben. Für unsere Testinstallation hingegen wählen wir eine *New Database*. Sie trägt den Namen „VirtualManagerDB“. Im nächsten Schritt müssen Sie einen Account für die Arbeit mit dem VMM bereitstellen. Wir haben dazu einen speziellen User „vmmadmin“ eingerichtet – er muss ein Domänenbenutzer sein. Geben Sie nun diesen Benutzer mitsamt seinem Passwort in der Maske *Account Configuration* an. Bei der Frage nach der *Library-Configuration* können Sie die bestehenden Angaben übernehmen und direkt zum abschließenden *Installation Summary* wechseln. Hier sehen Sie nochmals alle gewählten Einstellungen. Bei Bedarf können sie auch zurückkehren und noch Änderungen vornehmen. Wenn Sie jetzt die Eingaben bestätigen, fängt das System an, den SCVMM-Server und die VMM-Administrationskonsole entsprechend zu konfigurieren.

Wichtig: Den vorher erzeugten Benutzer müssen Sie bei der Konfiguration des SCVMM angeben.

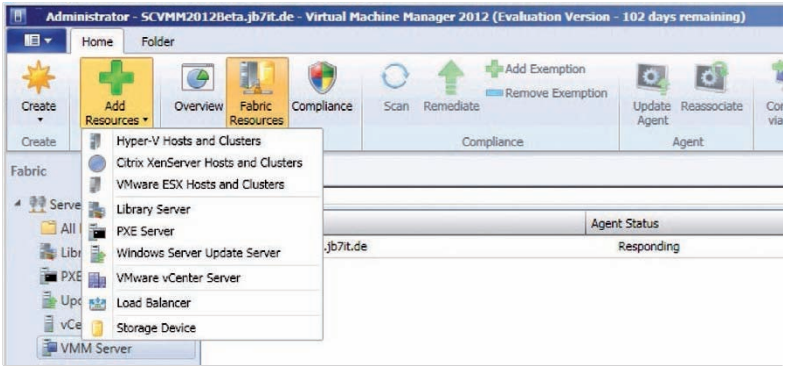
3.7.7 Private Cloud aufbauen

Damit sind alle Konfigurationsarbeiten abgeschlossen, und wir wenden uns dem Aufbau der Private Cloud zu. Um eine Cloud zu erzeugen, werden Ressourcen benötigt: die Server, die Speichersysteme und die Netzwerkanschlüsse. Diese drei Elemente stellen die Hardware der Cloud dar. Sie alle werden, ganz der Theorie folgend, vorher in Ressourcen-Pools zusammengefasst.



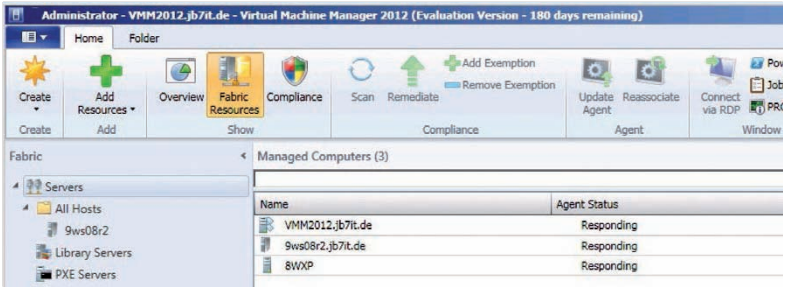
Start: Die Konsole des SCVMM ist nach dem Setup noch leer. Sie orientiert sich am Ribbon-Interface.

Starten Sie nun Ihren neu eingerichteten SCVMM 2012. Microsoft hat ihm als Verwaltungsoberfläche das Ribbon-Interface verpasst. Nach dem Setup und der Konfiguration des SCVMM auf dem Verwaltungsrechner müssen Sie zuerst Ihre Ressourcen bereitstellen.



Wahlfreiheit: Unter der Option „Add Resources" stellen sie die Ressource für Ihre Cloud bereit. Der VMM unterstützt sowohl Hyper-V-Server als auch VMware-ESX-Server und Citrix XenServer.

Dies passiert unter der Option *Add Ressources*. Ein Assistent hilft beim Einrichten und Konfigurieren und fragt alle benötigten Parameter ab. Als Ressourcen bezeichnet der SCVMM all jene IT-Baugruppen, die als Ausführgrundlage benötigt werden, also die Rechnersysteme mit Hyper-V, ESX-Hosts und XenServer.



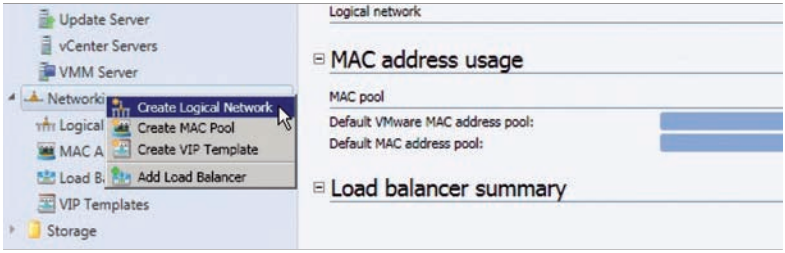
Details: Unter den „Fabric Resourcen" und darunter in der Rubrik der „Server" finden Sie die Ressourcen für Ihre Cloud. Im Bild haben wir zwei Hyper-V-Server und einen vCenter-Server integriert. Das vCenter stellt die Verbindung zu den ESX-Hosts her.

Im Rahmen des Workshops packen wir zuerst zwei Hyper-V-Rechner unter die Verwaltung des SCVMM. Grundlage des Hyper-V war eine Windows Server 2008 R2 mit SP1. Sie wurde von CD installiert, mit den aktuellen Updates versehen und

dann in unsere Domäne integriert. Bis dato sind das Standardprozesse, die bei jedem Windows-Server anfallen. Um ihn als Host-Ressource für den VMM verwenden zu können, muss dieser Rechner außerdem mit der Rolle des Hyper-V ausgestattet sein. Das erfolgt über die Rollenverwaltung des Server Manager. Nach der Integration der beiden Hyper-V-Server packten wir noch einen bestehenden ESX-Server unter die Verwaltung des VMM und stellten diesen als Cloud-Ressource bereit. Der VMM kommuniziert dabei aber nicht direkt mit dem ESX-Server, sondern benötigt hierzu das VMware vCenter. Daher müssen Sie an dieser Stelle das vCenter in den SCVMM integrieren. Über das vCenter erreicht und verwaltet der SCVMM dann die ESX-Systeme.

3.7.8 Netzwerke und MAC-Pools bereitstellen

Zum Umfang einer Cloud gehört auch die Anbindung an die Netzwerke. Hierzu erstellen Sie ein logisches Netzwerk und einen MAC-Adress-Pool. Aus diesem Pool werden dann die virtuellen Maschinen bedient.



Kontakt bitte: Die Verbindung der Systeme untereinander erfolgt über logische Netzwerke.

Die Konfiguration des Netzwerkes und der MAC-Pools finden Sie unter dem Bereich Networking in der SCVMM-Konsole. Falls gewünscht, können Sie außerdem noch einen zentralen (shared) Storage Pool zu der neuen Cloud dazupacken; ihn benötigen Sie unter anderem, wenn Sie das virtuelle System migrieren wollen.

Damit ist der Aufbau unserer Private Cloud abgeschlossen, und Sie können die virtuelle Maschine in Ihre Cloud legen. Dies erfolgt im Prinzip analog zu den bestehenden Deployment-Konzepten. Der größte Unterschied besteht allerdings darin, dass die Ressourcen für die virtuellen Maschinen aus unserer neuen Cloud genommen werden. Den Microsoft System Center Virtual Machine Manager (VMM) 2012 Beta können Sie bei Microsoft Technet als voll funktionsfähige 180-Tage-Version herunterladen (http://technet.microsoft.com/de-de/evalcenter/gg678609). Microsoft bietet außerdem kostenlose Private Cloud Online-Trainings (www.microsoftvirtualacademy.com/Studies/SearchResult.aspx) an.

Johann Baumeister

3.8 Workshop – Private Cloud mit Eucalyptus

Cloud Computing stellt IT-Infrastrukturen wie Datenspeicher, Netzwerk- und Rechenkapazitäten dynamisch über ein Netzwerk zur Verfügung. Weil der Nutzer diese Infrastruktur nicht direkt sieht und sie für ihn undurchsichtig erscheint, redet der Experte von einer „Wolke". Darin findet man aber nicht nur die Infrastruktur – gemeinhin als Infrastructure-as-a-Service (IaaS) bezeichnet –, sondern auch Software, die von einem oder mehreren Anbietern als Dienst gemietet wird (Software-as-a-Service, SaaS). Und auch Entwickler treibt es in die Wolken: Sie nutzen diese als Platform-as-a-Service (PaaS) und schreiben Anwendungen, die dann von einem PaaS-Provider beliebigen Nutzern via Internet zur Verfügung gestellt werden. Sinn und Zweck von Cloud Computing ist es unter anderem, zu Spitzenlastzeiten ein Vielfaches der Nutzeranzahl bedienen zu können. Das kann zum Beispiel im Weihnachtsgeschäft erforderlich sein, aber ebenso, wenn etwa nach einer Fernsehmeldung die eigene Homepage plötzlich massiv frequentiert wird. Der Internethändler Amazon etwa gibt an, dass die Spitzenlast im Jahr 2006 zehnmal höher war als die Grundlast im Tagesgeschäft. Das war der Anlass für das Unternehmen, aus der Architektur und den Diensten ein eigenes Produkt zu machen, das inzwischen auch nach außen angeboten wird: Das Produkt ist als Speicherdienst S3 und als Elastic Compute Cloud, kurz: EC2, bekannt.

Der Zugriff auf die Wolke erfolgt über das Netzwerk, meist das Internet. Neben öffentlichen wie EC2 kann es aber auch private Wolken geben, die über ein firmeninternes Intranet bereitgestellt werden. Sogar persönliche Wolken auf Laptops findet man inzwischen in der IT-Landschaft. Möglich machen das vor allem Open-Source-Systeme wie Eucalyptus (http://open.eucalyptus.com), Open Nebula (www.opennebula.org) und Openstack (www.openstack.org).

Eucalyptus steht für Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems. Die Open-Source-Infrastruktur ist kompatibel zu Amazons Speicherdienst S3 und zu EC2. Aktuell ist die Version 2.0.3 von Eucalyptus Open Source; in Ubuntu 11.04 ist noch die Version 2.0.2 enthalten. Neue Eucalyptus-Versionen erscheinen jeweils im März und im August. Es gibt auch eine kommerzielle Version: Die Eucalyptus Enterprise Edition (EE) basiert auf Eucalyptus Open Source. Sie wird seit der Version 1.5.2 von Eucalyptus Systems vertrieben, die das ursprünglich an der kalifornischen Universität in Santa Barbara entwickelte Forschungsprojekt übernommen hat.

In unserem Workshop zeigen wir Ihnen, wie Sie unter Ubuntu mithilfe der Open-Source-Cloud-Plattform Eucalyptus eine eigene Cloud aufbauen können.

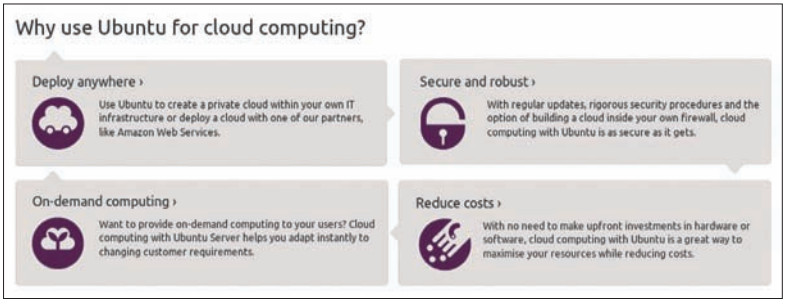
3.8.1 Aufbau einer Eucalyptus-Wolke

Eine Eucalyptus-Cloud besteht aus fünf Komponenten: Der Cloud-Controller (CLC) und der Speicherdienst Walrus stehen in der obersten Ebene und sind in jeder Cloud-Installation einmal enthalten. Der Cloud-Controller selbst ist ein Java-

Programm mit EC2-kompatiblen SOAP- und Abfrageschnittstellen sowie einem Web-Interface. Er übernimmt die Kontrolle über die gesamte Cloud. Walrus ist ebenfalls in Java geschrieben.

Der Walrus-Server speichert die sogenannten Buckets global; Buckets sind Behälter, in denen Objekte einer Cloud gespeichert werden. Um eine Anwendung in der Cloud rechnen zu lassen, müssen drei Buckets angelegt und beim Cloud-Controller registriert werden. Mithilfe des Cloud-Controllers wird eine Instanz davon erstellt und von Eucalyptus in der Cloud verteilt; ferner wird eine IP-Adresse vergeben, über die man auf diese Instanz zugreifen kann.

Beide Komponenten – der CLC und Walrus – können Ressourcen aus verschiedenen Clustern vereinen. Jeder Cluster oder Rechnerverbund benötigt zudem einen Cluster-Controller (CC) für die Netzwerkkontrolle und einen Storage-Controller (SC). Diese beiden Komponenten sind typischerweise im Hauptknoten eines Clusters untergebracht. Alle vier Komponenten bilden zusammen das sogenannte Frontend. Und schließlich braucht jeder Knotenpunkt mit einem Hypervisor einen Node-Controller (NC), um den Hypervisor zu kontrollieren. Der Cluster-Controller und der Node-Controller sind in der Programmiersprache C geschrieben und werden als Webservices innerhalb von Apache bereitgestellt.



Überblick: Das sind laut Canonical die Vorteile für Cloud-Computing mit Ubuntu.

Eucalyptus können Sie entweder aus den Quellen installieren, die Sie auf der Projektseite finden. Es gibt auch für einige Linux-Versionen (CentOS 5, Debian, Fedora 12, Opensuse 11) vorgefertigte Pakete. Außerdem wird Eucalyptus in einigen Distributionen mitgeliefert beziehungsweise im Repository vorgehalten. Das hat den Vorteil, dass es problemlos über die jeweilige Paketverwaltung installiert und aktualisiert werden kann. In Debian sind aktuell die Pakete der Eucalyptus-Version 1.6.2 integriert. Das bedeutet aber noch nicht, dass sie mit der nächsten stabilen Debian-Version ausgeliefert werden. Denn derzeit befinden sie sich noch im sid-Zweig (still in development) der Distribution.

Den größten Teil der Entwicklungsarbeit im Debian-Bereich hat übrigens Ubuntu gestemmt. Dort steht die Cloud-Infrastruktur bereits seit der Version 1.5 in den

Repositories. Aus gutem Grund: Eucalyptus bildet derzeit den Kern der Ubuntu Enterprise Cloud, eines der Geschäftsfelder von Ubuntu-Distributor Canonical.

3.8.2 Vorarbeiten für die Ubuntu-Installation

Um Eucalyptus unter Ubuntu (www.ubuntu.com) zu installieren, benötigen Sie mindestens zwei Maschinen: die eine mit dem Frontend, die andere für den Node-Controller. Der Frontend-Rechner sollte folgende Voraussetzungen erfüllen (in Klammern die Empfehlungen):

- CPU: 1 GHz (2 x 2 GHz)
- Arbeitsspeicher: 2 GByte (4 GByte)
- IDE-Festplatte mit 40 GByte freiem Speicherplatz (SATA mit 200 GByte)
- 100-Mbit-Netzwerk (1-Gbit-Netzwerk)

Der Rechner mit dem Node-Controller muss leistungsstärker sein, denn auf ihm laufen alle Instanzen. Auf diesem Rechner werden die virtuellen Maschinen installiert, die zuvor im Frontend heruntergeladen wurden.

- CPU mit VT Extensions (VT, 64 Bit, Multicore)
- Arbeitsspeicher: 1 GByte (4 GByte)
- IDE-Festplatte mit 40 GByte freiem Speicherplatz (SATA mit 100 GByte)
- 100-Mbit-Netzwerk (1-Gbit-Netzwerk)

Anschließend sollten Sie die aktuelle Serverversion von Ubuntu herunterladen. Sie finden diese unter www.ubuntu.com/download/ubuntu/alternative-download als Torrent sowohl für i386 als auch für amd64. Nach dem Download brennen Sie das Image auf eine CD und starten anschließend den für das Frontend geplanten Rechner mit dieser CD.

Wollen Sie mehr Rechner für die Cloud nutzen, werden die Frontend-Komponenten aufgeteilt. Bei drei Rechnern kommen CLC und Walrus auf die erste Maschine, CC und SC auf die zweite. Bei vier Rechnern werden auch noch CLC und Walrus voneinander getrennt. Ab fünf Rechner kann man bereits zwei Nodes nutzen; in dem Fall kommen CLC und Walrus wieder auf die erste Maschine:

- Maschine 1: CLC, Walrus
- Maschine 2: CC1, SC1
- Maschine 3: NC1
- Maschine 4: CC2, SC2
- Maschine 5: NC2 ...

Tipp: Sie können zu Testzwecken die gesamte Eucalyptus-Cloud auch auf einem Rechner installieren. Was Sie dabei beachten müssen, ist unter https://help.ubuntu.com/community/UEC/Topologies beschrieben.

3.8.3 Frontend und Node neu installieren

Die Installation von der Server-CD läuft ähnlich wie in den Desktop-Varianten von Ubuntu. Sie wählen zunächst die Sprache, dann aber den Eintrag *Ubuntu Enterprise Cloud installieren*. Danach werden die Tastatur und das CD-Laufwerk erkannt und die Komponenten für die Installation geladen. Nach der Hardwareerkennung wird das Netzwerk konfiguriert und dann nach dem Rechnernamen („ubuntu“) gefragt. Dann beginnt die Eucalyptus-Installation. Hier lassen Sie die Cloud-Controller-Adresse frei, weil es im Netzwerk noch keinen gibt – den wollen Sie ja erst noch anlegen. Im zweiten Bildschirm können Sie die zu installierenden Komponenten wählen; die fürs Frontend sind bereits markiert, sodass Sie mit Enter gleich weitergehen können.

Damit sind die Angaben für Eucalyptus zunächst beendet, und es beginnt die weitere Standardinstallation mit dem Partitionieren der Festplatten. Spannend wird es erst wieder, wenn die Setup-Routine nach dem Namen des Eucalyptus-Clusters fragt. Die Vorgabe cluster1 können Sie ändern oder übernehmen; der Name wird den Nutzern später als verfügbare Zone angezeigt. Danach müssen Sie einen Adressbereich Ihres Netzwerks angeben, den Eucalyptus virtuellen Maschinen als öffentliche IP-Adressen dynamisch zuweisen kann. Um den Adressbereich einzugeben, benötigen Sie das Minuszeichen. Sie finden es auf der US-amerikanischen Tastatur auf der *ß-Taste*.

Anschließend installieren Sie den Node-Rechner. Benutzen Sie dasselbe Image und wählen ebenfalls den Eintrag *Ubuntu Enterprise Cloud installieren*. Achten Sie darauf, dass der Node im selben Netzwerk angeschlossen ist. Dann wird der Cluster von selbst erkannt, und die Installation des Node-Controllers wird angeboten. Der Rest funktioniert wie oben bereits beschrieben.

3.8.4 Installation auf bestehendem System

Falls Sie bereits Ubuntu auf den Rechnern installiert haben, müssen Sie es nicht erst wieder löschen. In dem Fall installieren Sie die Eucalytus-Pakete entsprechend. Auf dem Frontend-Rechner geht das ziemlich einfach mit dem Befehl

```
sudo apt-get install eucalyptus-cloud eucalyptus-cc
➥ eucalyptus-walrus eucalyptus-sc
```

Danach können Sie sich dem Node-Rechner zuwenden und dort den Node-Controller installieren mit

```
sudo apt-get install eucalyptus-nc
```

Das sieht zunächst noch einfacher aus. Doch während für das Frontend bereits alle Arbeiten erledigt sind, müssen Sie bei dieser Art der Installation noch einiges auf dem Node-Rechner anpassen. Zunächst müssen Sie die Bridge konfigurieren.

Dazu laden Sie die Datei */etc/network/interfaces* in einen Editor und kommentieren alle Einträge für vorhandene Schnittstellen wie *eth0*, *eth1* und so weiter aus. Fügen Sie zum Beispiel den folgenden Bridge-Eintrag hinzu, um die Bridge an alle physikalisch vorhandenen Ethernet-Geräte zu binden und per DCHP eine IP-Adresse zu erhalten:

```
auto br0iface br0 inet dhcp bridge_ports all
```

Sollte das nach dem Netzwerkneustart mit „/etc/init.d/networking restart“ nicht funktionieren, versuchen Sie stattdessen folgende Konfiguration:

```
auto br0iface br0 inet dhcp bridge_ports eth0 bridge_fd 9
➥ bridge_hello 2 bridge_maxage 12 bridge_stp off
```

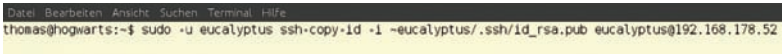
Wichtig: Achten Sie darauf, dass die *bridge_ports* an die richtige eth-Schnittstelle gebunden werden. Wollen Sie die IP-Adresse statt per DHCP statisch zuweisen, dann erledigen Sie das mit einem Eintrag in der Art:

```
auto br0iface br0 inet static address 192.168.12.20
➥ netmask 255.255.255.0 network 192.168.12.0
➥ broadcast 192.168.12.255 gateway 192.168.12.1
➥ dns-nameservers 192.168.12.1 dns-search foobar
➥ foobar.com bridge_ports eth0
```

Denken Sie daran, bei den Angaben von *address* bis *dns-search* Ihre eigenen IP-Adressen und Parameter einzugeben. Anschließend starten Sie das Netzwerk neu.

Im Anschluss kontrollieren Sie, ob in der Datei */etc/eucalyptus/eucalyptus.conf* in der Zeile *VNET_BRIDGE* die zuvor definierte Brücke eingetragen ist. Danach starten Sie den Node-Controller neu mit

```
sudo /etc/init.d/eucalyptus-nc restart
```



Ziemlich lang: Mit diesem Befehl übertragen Sie den öffentlichen SSH-Schlüssel des Benutzers eucalyptus auf den Node-Rechner.

Als Nächstes müssen Sie den öffentlichen SSH-Schlüssel des eucalyptus-Nutzers vom Frontend auf den Node-Controller installieren. Das ist am einfachsten, indem Sie zunächst dem Nutzer *eucalyptus* ein Passwort zuweisen:

```
sudo passwd eucalyptus
```

Anschließend übertragen Sie dieses am Frontend hinüber zum Node-Rechner mit

```
sudo -u eucalyptus ssh-copy-id -i ~eucalyptus/.ssh/
➥ id_rsa.pub eucalyptus@<IP-ADRESSE-DES-NODES>
```

Den Schlüssel finden Sie danach in der Datei */var/lib/eucalyptus/.ssh/authorized_keys*. Nun können Sie das Passwort wieder entfernen mit

```
sudo passwd -d eucalyptus
```

Nun starten Sie auf dem Frontend die Publication-Services von Walrus, Cluster- und Storage-Controller:

```
sudo start eucalyptus-walrus-publicationsudo
➥ start eucalyptus-cc-publicationsudo
➥ start eucalyptus-sc-publication
```

Anschließend starten Sie den Service auf dem Node-Rechner:

```
sudo start eucalyptus-nc-publication
```

Wechseln Sie wieder zum Frontend-Rechner und starten den Listener für den Cloud- und den Cluster-Controller (sind diese auf unterschiedlichen Maschinen, müssen Sie den Befehl an beiden ausführen):

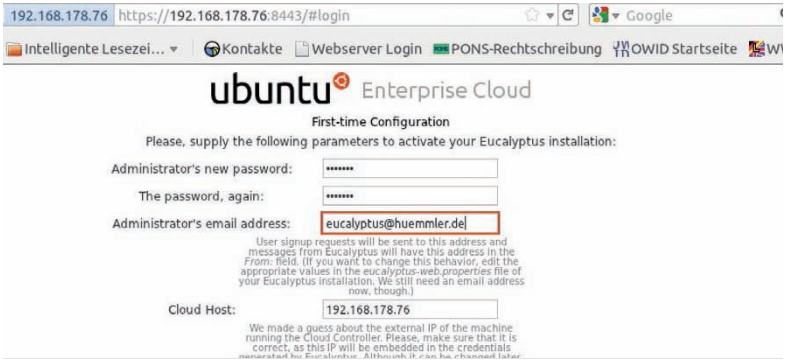
```
sudo start uec-component-listener
```

Im letzten Schritt können Sie sich in der Logdatei */var/log/eucalyptus/registration.log* davon überzeugen, dass die Registrierung der Komponenten erfolgreich war.

3.8.5 Credentials holen

Jetzt kommt der große Augenblick. Starten Sie einen Webbrowser und loggen sich auf dem Cloud-Controller ein. Dazu geben Sie in die Adresszeile des Browsers ein:

```
https://192.168.178.76:8443/
```



Erstkonfiguration: Zunächst muss ein neues Passwort und eine E-Mail-Adresse eingetragen werden.

Wichtig: Achten Sie darauf, das sichere HTTPS-Protokoll zu verwenden. Als Benutzernamen und Passwort geben Sie jeweils admin ein. Danach erfolgt die Erstkonfiguration der Cloud, und Sie werden aufgefordert, ein neues Passwort für admin festzulegen.

Danach erscheint der Konfigurationsbildschirm. Hier müssen Sie zunächst nichts ändern. Wechseln Sie oben links im Menü zu *Credentials* und klicken auf *Download Credentials*, um die Zertifikate von Cloud-Controller herunterzuladen. Entpacken Sie diese anschließend mit

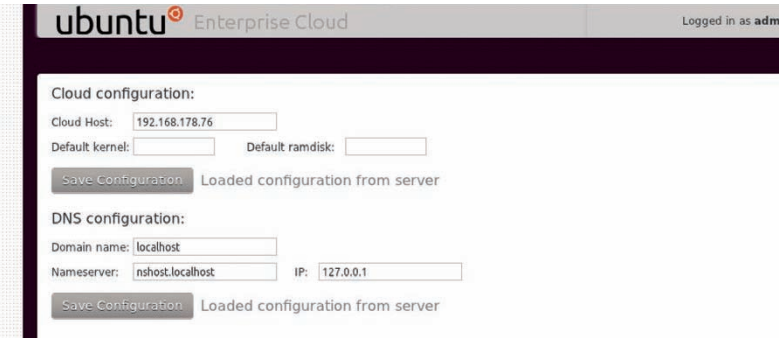
```
unzip -d ~/.euca /Pfad_zu/euca2-admin-x509.zip
```

in den versteckten Ordner *.euca* in Ihrem Home-Verzeichnis. Jetzt benötigen Sie noch die Euca-Tools für den Cloud-Nutzer, die zum Verwalten der Eucalyptus-Instanzen dienen. Installieren Sie diese mit

```
sudo apt-get install euca2ools
```

Das alles funktioniert, prüfen Sie abschließend, indem Sie die Verfügbarkeitsdetails der virtuellen Maschinen des lokalen Clusters abrufen:

```
. ~/.euca/eucarceuca-describe-availability-zones verbose
```



Geschafft: Die Cloud kann über ein Web-Frontend konfiguriert werden.

Die Cloud-Infrastruktur ist jetzt fertig und betriebsbereit. Nun können Sie die Cloud befüllen und entsprechende Images installieren. Klicken Sie auf Extras und laden eines von der Eucalyptus-Homepage herunter. Die Images enthalten jeweils ein XEN- beziehungsweise KVM-kompatibles Kernel- und Ramdisk-Paar sowie ein Image für die virtuelle Maschine. Wie Sie das Image installieren, ist auf der Eucalyptus-Homepage beschrieben (http://open.eucalyptus.com/wiki/EucalyptusUserImageCreatorGuide_v2.0).

Thomas Hümmler

3.9 Workshop – Aufbau einer Cloud mit VMware vCloud Director

Die Verwaltung eines Cloud-Dienstes hat mit dem traditionellen IT-Management nur wenig gemeinsam. Die feste Zuordnung eines Applikationsdienstes zu einem Server wird bei den Cloud-Techniken und deren Basis, der Virtualisierung der IT-Dienste, durch dynamische Deployment-Techniken abgelöst. VMware ist mit vSphere Marktführer bei der Virtualisierung.

Nun trimmt der Hersteller von vSphere und ESXi-Server (www.vmware.com) sein Produktportfolio konsequent in Richtung Cloud und positioniert es als „Cloud-Betriebssystem". Noch in diesem Quartal soll ein Großteil der VMware-Werkzeuge in einem neuen Release kommen. VMware fasst seine Cloud-Funktionen in einem vCloud Stack zusammen. Dazu gehören der vCenter-Server, die Funktionen des Dynamic Resource Scheduling, vMotion, die Sicherheitsmodule von vShields und vor allen der neue vCloud Director. Der vCloud Director ist ein zentraler Baustein für die IT-Verwaltung im Sinne der Cloud. Zu den wichtigsten Neuerungen der aktuellen Version zählt Fast Provisioning durch Linked Clones und das Customizing der Applikationen. Begleitend dazu wurden die Sicherheitseinstellungen, die in den vShield-Produkten gebündelt sind, überarbeitet. Und schließlich kann als Backend-Datenbank zur Ablage der Konfigurationsinformationen in Zukunft auch der Microsoft SQL Server verwendet werden. Bis dato wurde nur das Oracle-Datenbanksystem unterstützt. Wir haben uns den neuen VMware vCloud Director in Version 1.5 angesehen und zeigen in einem Workshop, wie Sie mit dieser Software schnell und komfortabel eine Cloud-Infrastruktur aufbauen können. Darüber hinaus erläutern wir detailliert den praktischen Einsatz und die verschiedenen Möglichkeiten des vCloud Directors.

3.9.1 Von der Virtualisierung zur Cloud

Wer selbst eine Cloud aufbauen möchte und in Zukunft sein Data Center als „private Cloud" betreiben will, sieht sich mit neuen Anforderungen konfrontiert. Wie aber sehen diese Anforderungen aus und was ändert sich gegenüber den bestehenden Konzepten? Auf dem Weg zur Cloud sind mehrere Stufen zu beschreiten. Die Marktforscher von Gartner beispielsweise unterscheiden drei Phasen. Phase I hat die Virtualisierung der Server im Fokus. Dies erfolgt durch die Hypervisoren VMware ESX und VMware ESXi. Mittels Virtualisierung werden physische Server reduziert. Bei einer Konsolidierungsrate von 10:1 werden zum Beispiel zehn Serversysteme auf einen Host zusammengefasst. Neuere Serversystem erlauben aber auch Konsolidierungsraten mit Hunderten von virtuellen Maschinen auf einem physischen Server. Damit lassen sich ganze Serverschränke auf eine einzige leistungsfähige „Serverbox" reduzieren. Die Konsolidierung der IT-Infrastruktur ist damit vor allem ein Mittel zur Reduzierung der IT-Ressourcen und zur damit ein-

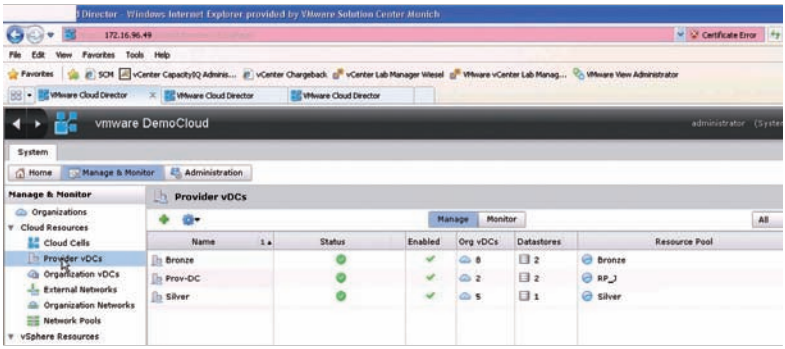
hergehenden Kostensenkung. Phase I ist in vielen Unternehmen derzeit in der Umsetzung oder bereits abgeschlossen. Phase II erhöht die Flexibilität (Agilität) der IT. Durch flexiblere IT-Betriebsmodelle sollen die Unternehmen rascher auf die Anforderungen des Marktes reagieren können. Dies bedingt die schnellere Inbetriebnahme von IT-Diensten, mitsamt ihren Applikationen und begleitenden Verwaltungsprozessen. Erreicht wird dies durch die erweiterten technischen Funktionen der Virtualisierung, etwa die schnellen Provisionierung einer virtuellen Maschine, die dynamische Lastverteilung von bestehenden Anwendungen auf weniger belastete Serversysteme, Funktionen für Fehlertoleranz und Ausfallsicherung sowie die besseren Möglichkeiten des Disaster Recovery. Durch VMware Fast Provisioning wird die Inbetriebnahme der virtuellen Maschinen beschleunigt. Anstatt die Images von virtuellen Maschinen zu kopieren, werden lediglich Zeiger auf die ursprünglichen Images erzeugt und verwaltet. VMware setzt dabei auf seine Linked-Clone-Technik. Änderungen zwischen dem Original und der Kopie (dem Clone) werden in Delta-Files zusammengefasst. VMwares Fast Provisioning ist damit ein weiterer und zentraler Baustein für den Betrieb der IT nach den Cloud-Modellen. Das Eigentliche Deployment der Cloud-Dienste, also die Bestückung des Servers mit dem Betriebssystem, den Patches und den Applikationsdiensten, sollen dabei ohne Eingriffe eines Administrators erfolgen. Automatismen und vorbereitete Skripte ermöglichen eine weitaus raschere Aktivierung von virtuellen Maschinen, als dies durch manuelle Eingriffe erfolgen könnte.

3.9.2 Erweitertes Customizing und Pool-Verwaltung

Die erzeugten Anwendungen und Dienste müssen aber in der Regel noch personalisiert werden. Dazu gehören beispielsweise die Namen der virtuellen Maschinen, deren IP-Adressen oder URL-Links, um die Anwendungen den Benutzern zur Verfügung zu stellen. Diese Konfiguration erfolgt im Rahmen der „Personalisierung" der virtuellen Instanz der Anwendung. Ein Automatismus kann aber nur dann seine Vorzüge ausspielen, wenn auch diese begleitende Personalisierung des Applikationsdienstes automatisch erfolgt. Dies ist eine weitere Neuerung des vCloud Director. Nunmehr bestehen im vCloud Director mehrere und bessere Möglichkeiten, die Personalisierung der Anwendungen vollständig zu automatisieren. VMware spricht dabei von Applikations-Customizing. Des Weiteren können mit Version 1.5 des vCloud Directors mehrere identische Kopien einer virtuellen Maschine oder vApp gleichzeitig ohne jegliche Anpassung betrieben werden.

Eine vApp fasst einen oder mehrere virtuelle Maschinen in einem Container zusammen. Diese Sammlung an virtuellen Maschinen bildet dabei einen gemeinsamen Dienst ab. Ein Beispiel dafür ist ein Webangebot eines Unternehmens. Hierbei kommen in der Regel einer oder mehrere Webserver, Applikationsserver und Backend-Datenbanken in Betracht. Sie alle zusammen bilden den Webdienst für die Anwender im Internet ab. Um vApps besser zu unterstützen, hat VMware die Technik des „Cross Host Fencing" in seinen Systemen integriert.

In der dritten Phase schließlich erfolgt eine vollständige Entkopplung der IT-Dienste von den benötigten IT-Ressourcen. Als Ressourcen einer Applikation zählen dabei die Server, der Plattenspeicher, die Netzwerkkomponenten und weitere Infrastrukturbaugruppen. All diese IT-Ressourcen werden stattdessen in einem Pool zusammengefasst. Parallel dazu steht der Softwarekatalog. Er umfasst alle verfügbaren Anwendungen, die dem Benutzer angeboten werden. Durch Automatismen und Skripte werden dann die Programme des Katalogs aktiviert. Die Ressourcen dazu werden aus dem Pool entnommen.



Details: Beim vCloud Director bündeln die Ressourcen-Pools die Ressourcen der Cloud. Aus diesen werden die Dienste versorgt.

Die Verwaltung des Resource Pools und des Katalogs sowie die Automatismen sind im vCloud Director gebündelt. Die wahlfreie Zuordnung einer Applikation zu den Pool-Ressourcen führt somit zu einer vollständigen Abstraktion der Dienste. Die Entkopplung der Dienste von den Ressourcen mündet schlussendlich in die Verfahren, die als Cloud Computing bezeichnet werden können.

3.9.3 Die Anforderungen für den vCloud Director

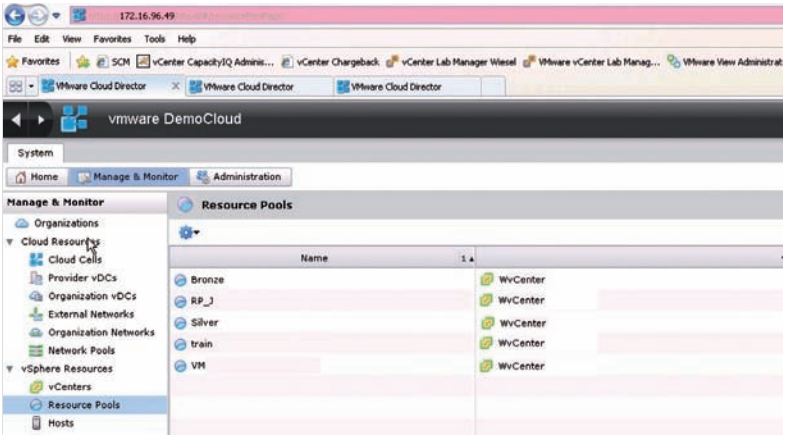
Nach diesen allgemeinen Anmerkungen zum Aufbau von Clouds und zum vCloud Director wenden wir uns nun dem praktischen Einsatz zu. Dazu haben wir das aktuelle Pre-Release des vCloud Director Version 1.5 verwendet. Wie erwähnt, soll das finale Produkt im dritten Quartal 2011 verfügbar sein. Auf die Betrachtungen im Rahmen diese Workshops hat das aber keinen Einfluss. Die zu erwartenden Änderungen betreffen laut VMware eher die Leistungsoptimierungen und sind ansonsten „unter der Haube".

Die finale Version des vCloud Directors soll als vApp verfügbar sein. Für das aktuelle Pre-Release gilt dies allerdings noch nicht. In vApp (virtual Appliance) paketiert VMware fertig konfigurierte Anwendungssysteme. Eine vApp fasst einen oder mehrere virtuelle Maschinen, die gemeinsam einen Dienst abbilden, in einem

Container zusammen. Diese werden als virtuelle Maschine im Kontext des ESX-Servers ausgeführt. Die Betriebssystemgrundlage für den vCloud Director ist ein Red-Hat-Linux-Derivat. Im normalen Umgang mit dem vCloud Director wird man das Linux-Betriebssystem aber kaum zu Gesicht bekommen. Der vCloud Director weist stattdessen eine grafisch ansprechende Verwaltungskonsole auf.

3.9.4 Acht Schritte zur vSphere-Cloud

Der Aufruf der vCloud Director-Konsole erfolgt über einen Browser. Nach dem Login am vCloud Director können Sie auch schon loslegen und eine Cloud erstellen. Die Konsole der Version 1.5 hat sich gegenüber der derzeitigen Version 1.0 kaum verändert.



Übersichtlich: Unter „Manage & Monitor" finden Sie die Verwaltungsobjekte der Cloud.

Im oberen Bereich finden Sie drei Reiter, die mit *Home, Manage & Monitor* und *Administration* benannt sind. Unter *Administration* erfolgt die allgemeine Verwaltung und Konfiguration des vCloud Director. Die eigentliche Überwachung und Verwaltung der Cloud, der Rossourcen-Pools und aller anderen Cloud-Objekte sind unter Manage & Monitor zusammengefasst.

Im Zweig *Home* findet sich eine Reihe von Assistenten, die den Einstieg und Aufbau einer Cloud vereinfachen sollen. Diese haben wir uns zuerst angesehen. VMware stellt im vCloud Director insgesamt acht Assistenten bereit. Diese sind im unteren Teil unter Guides Tasks eingeblendet. Nach der Abarbeitung dieser acht Assistenten haben sie eine fertig konfigurierte und lauffähige Cloud erzeugt. Die Grundlage dafür bilden vSphere, eines der ESX-Derivate, das vCenter und die weiteren VMware-Verwaltungs-Tools wie vShield.

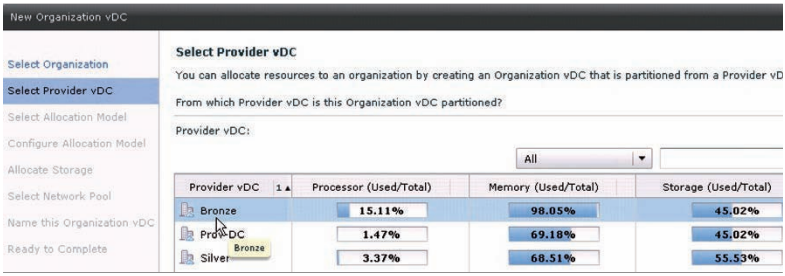
3.9.5 Assistenten helfen beim Aufbau der Cloud

Mithilfe der ersten vier Assistenten stellen Sie die Cloud-Ressourcen bereit. VMware hat folgerichtig diesen Zweig mit *Provision additional Cloud Resources* umschrieben. Zu diesen Ressourcen gehören die oben erwähnten IT-Baugruppen, wie die Hypervisoren, die Netzwerke und der Speicher. Ferner erfolgt hier die Pool-Bildung der Ressourcen.

Die Schritte fünf bis acht fasst der vCloud Director unter der Bezeichnung *Allocate addtional organization resources* zusammen. Hier erfolgt die Zuweisung der unter Schritt eins bis vier definierten Dienste an die Benutzer. Die acht Assistenten leiten den Anwender intuitiv und komfortabel durch die einzelnen Installationsschritte. Wenn später Änderungen an der Konfiguration, der Cloud oder den Pools vorgenommen werden müssen, erfolgt dies unter dem Reiter *Manage & Monitor*.

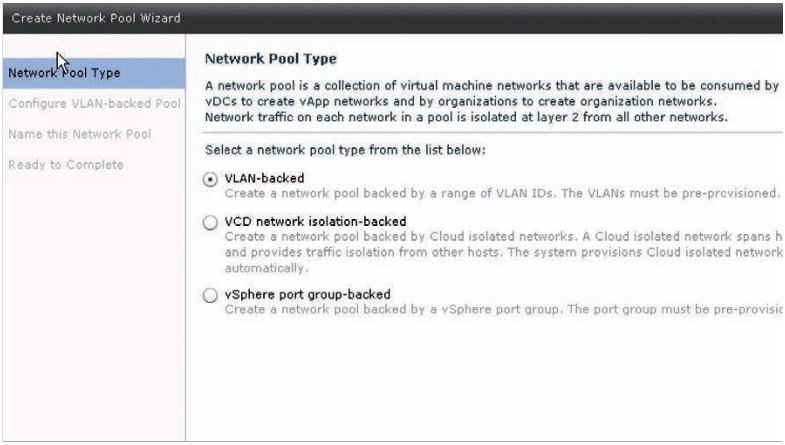
3.9.6 Der Aufbau einer Cloud

Das vCenter ist das zentrale Verwaltungswerkzeug für eine vSphere-Infrastruktur. Es wird auch bei Aufbau einer VMware-Cloud benötigt. Im ersten Schritt müssen Sie eine Verbindung zwischen vCloud Director und vCenter-Server herstellen. Für größere virtuelle Szenarien können auch mehrere vCenter-Server parallel existieren. Der Assistent verlangt lediglich die Angaben des oder der vCenter-Server. Über den oder die vCenter-Server greift der vCloud Director auf die Verwaltungsdaten der vSphere-Infrastruktur zu.



Los geht's: Die Ressourcen werden in einen virtual Data Center (dem Provider DC) gebündelt. Durch die Provider DCs lassen sich auch unterschiedliche SLA abbilden.

Anschließend, im Step 2 (2. Create another Provider vDC), erzeugen Sie ein Provider-vDC (virtual Data Center); hier werden die verfügbaren Ressourcen gebündelt. Im praktischen Einsatz wird man mehrere Provider-DCs aufbauen. Sie lassen sich auch einfach anhand der SLA-Anforderungen erstellen. So können beispielsweise Provider-DCs mit geringen (Bronze), mittleren (Silber) oder hohen (Gold) Anforderungen parallel verwaltet werden.



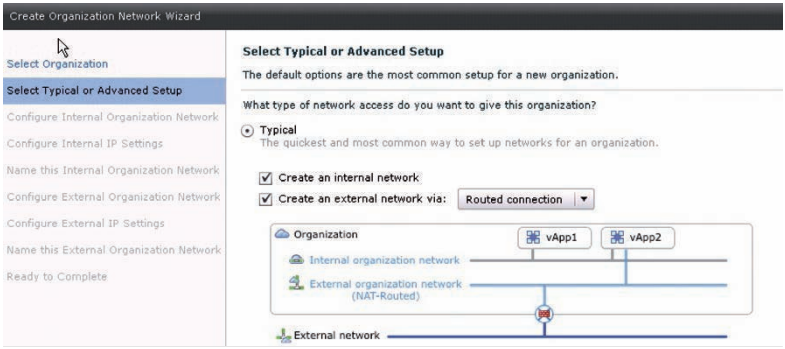
Kontakt bitte: Durch den Netzwerk-Pool erfolgt die Verknüpfung der virtuellen Maschinen in der Cloud.

Die Ressourcen eines virtual Data Centers wiederum werden durch die vSphere-Infrastruktur gebildet. Damit das virtual Data Center mit weiteren Systemen kommunizieren kann, sind externe Netzwerkverbindungen erforderlich. Durch das externes Netzwerk erhalten das virtuelle Datacenter und dessen Anwendungen den Zugang zur Infrastruktur außerhalb der vCloud Director. Dessen Aufbau erfolgt im nächsten Schritt (Schritt drei). Die Kommunikation mit weiteren Diensten innerhalb des virtuellen Data Centers der Cloud erfolgt durch einen internen Netzwerk-Pool, der vom vierten Assistenten aufgebaut wird. Nach der Durchführung der ersten vier Assistenten sind die Cloud und ihre Ressourcen eingerichtet. Unter *Manage* & *Monitor* finden Sie nun Ihre erzeugten Cloud-Objekte.

3.9.7 Die Nutzer der Cloud-Dienste

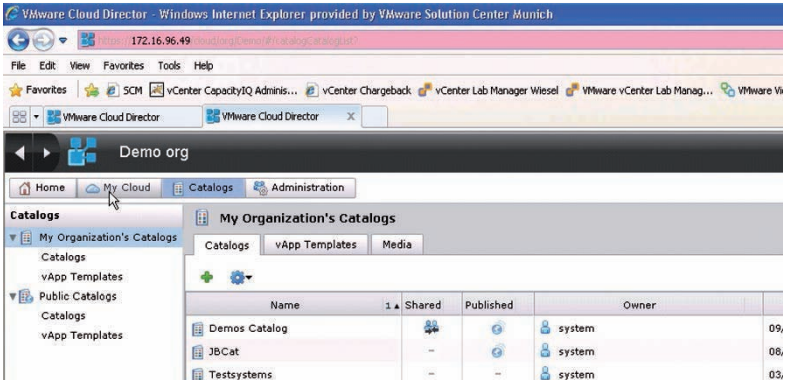
Durch die ersten vier Assistenten wurde die Cloud mit ihren Ressourcen definiert. In den nachfolgenden Schritten müssen Sie die Nutzer der Cloud und deren Dienste (Applikationen) aufbauen.

Zuerst müssen Sie unter 5. *Create another organization* die Organisationseinheit, die die Cloud nutzen soll, definieren. Sie umfasst die Anwender und die Richtlinien für die Benutzer des Cloud-Dienstes. Im Schritt sechs wird das „Allocation Model“ bestimmt; es legt die Servicequalität beispielsweise vom Netzwerk-, CPU- oder Speicher fest. Anschließend müssen Sie ein Netzwerk definieren, über das die Anwender der vorher erzeugten Organisationseinheit den Cloud-Dienst ansprechen können. Im letzten Schritt schließlich legen Sie den Dienste-Katalog fest. Hierin sind die Anwendungen abzulegen. Die Verwaltung des Kataloges kann dann aber auch durch Fachbereichsadministratoren erfolgen.



Verbindung: Benutzer der Organisation erhalten einen eigenen Netzwerkzugriff auf ihre Cloud-Dienste.

Damit ist der Aufbau Ihrer Cloud auf der Grundlage des VMware-Cloud-Stacks abgeschlossen. Sie können jetzt die Anwendungen ihren Nutzern dynamisch, so wie es die Cloud-Mechanismen vorgeben, zur Verfügung stellen.



Gemeinsamkeiten: Die Anwendungen (Dienste) werden in Katalogen zusammengefasst und verwaltet.

3.9.8 Fazit

Die Techniken und Methoden zum Aufbau eine Cloud waren bis dato oftmals noch relativ nebulös. Es dauerte eben seine Zeit, bis die Hersteller die passenden Verwaltungswerkzeuge dafür erstellten. Doch nun scheint die Cloud konkret zu werden. VMware liefert mit dem vCloud Director ein Tool-Set, das den Aufbau einer privaten Cloud vereinfacht und in acht Schritten aufzeigt, wie unser Workshop veranschaulicht hat.

Johann Baumeister

4 Anhang: Die beliebtesten Netzwerk-Artikel (QR-Codes)

Zum Thema dieses TecChannel-Compacts finden Sie hier die QR-Codes zu den meist geklickten Artikeln auf TecChannel.de. Mit einer entsprechenden App für Ihr Smartphone oder Tablet-PC gelangen Sie so schnell und ohne Tippen zu noch mehr Informationen.

Die schnellsten Prozessoren im Benchmark ... (Webcode 2016541)

Die wichtigsten Cloud-Anbieter im Vergleich (Webcode 2029069)

Vergleich: Google Apps und Microsoft Office 365 (Webcode 2035660)

Die beliebteste Virtualisierungs-Software (Webcode 2033403)

Gruppenrichtlinien in Windows Server 2008 R2 (Webcode 2022544)

Cloud Computing – SaaS, PaaS, IaaS, Public und Private (Webcode 2030180)

Die Nachteile der Server-Virtualisierung (Webcode 2036655)

Tools zum Monitoring virtueller Umgebungen (Webcode 2035806)

Virtualisierungs-Grundlagen – Varianten und ... (Webcode 2029842)

Cloud Computing – SLA, Kostenberechnung ...
(Webcode 2030342)

Mehr Sicherheit trotz Botnetze, Cloud- und ...
(Webcode 2034953)

Sicherheitsrisiken in der Cloud vermeiden
(Webcode 2034755)

Virtualisierung verlangt nach dedizierten ...
(Webcode 2032623)

Energiespartipps für die Unternehmens-IT
(Webcode 1785486)

Rechenzentren mit besonders effizienter ...
(Webcode 2035041)

Tipps: Mehr Sicherheit im Serverraum ...
(Webcode 2033076)

Cloud Computing – Anwender misstrauen ...
(Webcode 2028816)

Top-Gründe für/gegen Cloud Computing ...
(Webcode 2033156)

KVM gegen Xen – Open-Source-Hypervisoren ...
(Webcode 2029529)

Workshop: Linux-Hardeningn
(Webcode 2034441)

Benutzerverwaltung unter Linux
(Webcode 2033921)