

administrator

Das Magazin für professionelle System- und Netzwerkadministration

Management virtualisierter Server

Im Test

**vSphere-Analyse mit
Icomasoft Opvizer 2.1**

14

Im Test

**Veeam Backup&Replication
v7 Cloud Edition**

24

Systeme

**Verwalten von Multi-
Hypervisor-Infrastrukturen**

38

Workshop

**Server mit Red Hat CloudForms
in die Cloud verlagern**

50

Know-how

**Lizenz-Management in
virtuellen Infrastrukturen**

72

Das IT-Administrator Komplettprogramm!!!

NEU!
Jetzt auch inklusive
E-Paper!

Sichern Sie sich jetzt das **IT-Administrator
Jahresabo All-Inclusive** mit allen Monats-
ausgaben im Print- und E-Paper-Format, zwei
Sonderheften pro Jahr und der Jahres-CD.

Automatisch bekommen Sie im März
und Oktober jeweils das IT-Administrator
Sonderheft und im Dezember die Jahres-CD
mit allen Monatsausgaben im PDF-Format
zugestellt. Ihre Abonnementnummer wird zum Login
für die E-Paper-Monatsausgabe – jetzt
auch mit App fürs iPad!



Als bestehender Jahresabonnent
können Sie hier upgraden:

[www.it-administrator.de/
abonnements/aboupgrade/](http://www.it-administrator.de/abonnements/aboupgrade/)

Oder Sie sind Neukunde? Hier können Sie bestellen:

[www.it-administrator.de/
abonnements/jahresabo/](http://www.it-administrator.de/abonnements/jahresabo/)

www.it-administrator.de



Heinemann Verlag
Im Dialog mit Spezialisten.

Verlag / Herausgeber

Heinemann Verlag GmbH
Leopoldstraße 87
D-80802 München

Tel: 0049-89-4445408-0
Fax: 0049-89-4445408-99
info@heinemann-verlag.de

Vertrieb, Abo- und Leserservice IT-Administrator

vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville

Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de

Software Defined Anything

Liebe Leser,

glaubt man den Zahlen des Anbieters, vertreiben sich derzeit rund zwölf Millionen Deutsche mit der App "Quizduell" die Zeit. Neben der Möglichkeit, sich im Wettstreit mit anderen als Schlaumeier ersten Ranges zu profilieren, nutzen viele auch die Option, eigene Fragen einzureichen. Meine Frage wäre: "Was wird 2014 zum IT-Buzzword des Jahres?" Als erlaubte Antworten gebe ich vor: Green-IT, Cloud Computing, Big Data und Software Defined Networking.



Wie lautet die Lösung? Green-IT lockt schon lange niemanden mehr hinter dem Ofen hervor, kein Hersteller würde einen neuen Server damit bewerben, dass dieser endlich mehr Strom zieht als sein Vorgänger. Die Cloud erscheint zwar nicht mehr ganz so diffus wie einst, mittlerweile aber arg überstrapaziert – uns Redakteuren ist es unter Androhung von Peitschenhieben verboten, das Wort "Wolke" in einer Überschrift zu verwenden. Big Data interessiert noch immer primär Marketing-Abteilungen (um zu verkaufen, was kein Mensch braucht) und Geheimdienst-Chefs (um herauszubekommen, was eigentlich keiner wissen will).

Bleibt also Software Defined Networking (SDN). Nachdem sich im Zuge der Virtualisierung viele Server in Luft aufgelöst haben, versprechen viele Hersteller quasi das Gleiche für das ganze Netzwerk, ja sogar das komplette Rechenzentrum. Dabei wird gerne vergessen, dass Daten ja letztendlich irgendwo liegen müssen und auf welchen Bahnen auch immer zu transportieren sind. Und das Versprechen, dass sich mit Hilfe von SDN heterogene Umgebungen einheitlich managen lassen, dürfte nicht immer einzuhalten sein. Dass wirklich alle Funktionen einer Storage-Appliance durch die Datacenter-Software eines anderen Herstellers nutzbar sind, glauben wohl selbst glühendste Enthusiasten nicht. Die Hersteller sollten deshalb darauf achten, mit der Fixierung auf Software keine falschen Erwartungen zu wecken – letztendlich müssen sie selbst bei Unstimmigkeiten beim SDN Support leisten.

Bis sich dieses Buzzword mit konkretem Inhalt gefüllt hat, bleiben wir bei alltäglicher Praxis und helfen Ihnen mit diesem Heft, das Management virtualisierter Server zu meistern. In unseren Tests nehmen wir Veeam Cloud Backup (Seite 24) und die Präventions-Plattform Opvizer (Seite 14) unter die Lupe. In der Praxis-Rubrik gehen wir darauf ein, was Sie bei der Nutzung mehrerer Hypervisoren beachten sollten (Seite 38). Und übrigens: Natürlich spiele auch ich Quizduell – wer ein Match wagen möchte, kann mich unter "travellermuc" gern herausfordern.

Stets die richtigen Antworten wünscht

Lars Nitsch

Redakteur

Management virtualisierter Server

Im Test: Splunk Enterprise 6



Windows protokolliert alle relevanten System- und Anwendungsmeldungen mit der Ereignisanzeige. Es gibt allerdings eine sehr große Anzahl vollkommen verschiedener Protokollierungstechniken. Diese Datenmenge im Überblick zu behalten, ist eine große Herausforderung, die das passende Werkzeug erfordert – beispielsweise Splunk Enterprise 6. Unser Test beleuchtet, wie sich virtuelle und physische Infrastrukturen damit überwachen lassen.

Seite 20

Im Test: Ocster Backup Business 8



Dass eine vor allem auf kleinere und mittelständische Unternehmen zugeschnittene Datensicherung für Desktops und Server nicht teuer sein muss, möchte die neue Business-Version 8 von Ocster Backup beweisen. Durch eine Reduzierung auf die wesentlichen Funktionen ist die Software leicht bedienbar. Zudem besteht die Möglichkeit zur schnellen Wiederherstellung im Katastrophenfall. Doch ganz ohne Abstriche ist die günstige Backup-Software nicht zu haben.

Seite 34

AKTUELL

- 06 **News**
- 10 **IT-Administrator Training: vSphere-Tuning und -Monitoring**
- 12 **IT-Administrator Training: Best Practices Hyper-V**

PRODUKTE

- 14  **Im Test: Icomsoft Opvizor 2.1**
Opvizor unterstützt VMware-Administratoren mit regelmäßigen Analysen und Hinweisen zur virtuellen Infrastruktur, um diese zu optimieren und Fehler proaktiv zu vermeiden.
- 20  **Im Test: Splunk Enterprise 6**
Es gibt in virtuellen und physischen Infrastrukturen eine große Anzahl an Protokollierungstechniken. Diese Datenmenge im Überblick zu behalten, ist eine Herausforderung, der sich Splunk Enterprise 6 stellt.
- 24  **Im Test: Veeam Backup&Replication v7 Cloud Edition**
Um Online-Storage einfach anzubinden, hat Veeam sein Backup-Tool um eine optionale Cloud-Anbindung erweitert. Genau diese Komponente haben wir uns angesehen.
- 30  **Im Test: Cloud Management mit Witsbits**
Witsbits geht gegenüber etablierten Anbietern wie VMware und Microsoft einen anderen Weg und bietet das VM-Management als Software-as-a-Service an.
- 34  **Im Test: Ocster Backup Business 8**
Dass eine vor allem auf KMUs zugeschnittene Datensicherung für Desktops und Server nicht teuer sein muss, möchte die neue Business-Version 8 von Ocster Backup beweisen.

PRAXIS

- 38  **Systeme: Verwalten von Multi-Hypervisor-Infrastrukturen**
Manchmal kann es sinnvoll sein, mehrere Hypervisoren einzusetzen. Der Artikel beschreibt die Erfordernisse einer solchen Konstruktion und nennt Werkzeuge, die beim Management helfen.
- 42  **Systeme: Optimierung von Virtual Desktop-Infrastrukturen**
Desktops wandern vermehrt ins Rechenzentrum. Wir zeigen, welches Optimierungspotential gerade beim Thema Storage schlummert und welche Tools dabei nützlich sind.
- 47  **Workshopserie: Datensicherung, Wiederherstellung und Livemigration mit Hyper-V 2012 R2 (1)**
Dieser Workshop zeigt die Sicherung und das Verschieben von virtuellen Maschinen mit Livemigration unter Windows Server 2012 R2.
- 50  **Workshop: Server mit Red Hat CloudForms in die Cloud verlagern**
CloudForms stellt ein einheitliches Management-Framework für unterschiedliche Hypervisoren dar, das öffentliche und private Clouds verbindet und Sicherheits- und Softwareverteilungsfunktionen bereitstellt.

- 54  **Workshopserie: Mobile Geräte mit Workplace Join und Web Application Proxy in Windows Server 2012 R2 anbinden (2)**
Nach der Grundkonfiguration binden wir in diesem Teil der Workshopserie ein iPad ein und veröffentlichen eine Beispielwebseite.
- 58  **Workshop: Mit TeamDrive eine Private Cloud betreiben**
Der Austausch von Daten zwischen Anwendern ist heute gang und gäbe. Um ungewollten Datenzugriffen einen Riegel vorzuschieben, bietet sich mit TeamDrive ein kostenloses Werkzeug an.
- 62  **Workshopserie: Dateiverwaltung mit dem Ressourcen-Manager für Dateiserver in Windows Server 2012 R2 (2)**
Für Unternehmen, die Dateiserver im Einsatz haben, Freigaben nutzen und eventuell auf SharePoint setzen, liefert Windows Server 2012 R2 den Rolldienst Ressourcenmanager als Bordmittel.
- 66 **Tips, Tricks & Tools**

WISSEN

- 70  **Reportage: Modernisierte IT-Infrastruktur bei Julius Kleemann**
Der IT-Dienstleister Controlware konzipierte und realisierte für das Fertigungsunternehmen Julius Kleemann eine virtualisierte IT-Infrastruktur und überführte die Daten und Anwendungen.
- 72  **Know-how: Compliance in virtuellen Infrastrukturen**
Virtualisieren Unternehmen Anwendungen oder Desktops, muss sich der IT-Verantwortliche seinen mit Lizenz-Fußangeln gepflasterten Weg zur gewünschten Infrastruktur bahnen.
- 75  **Know-how: Sicherer IT-Betrieb in der Cloud**
Viele Unternehmen beziehen mittlerweile Cloud-Dienste über das Internet. Wir beschreiben, welche Risiken es dabei genau gibt und wie sie sich beheben oder zumindest eingrenzen lassen.
- 78 **Buchbesprechung "Windows Server 2012 R2" und "Praxisbuch IT-Dokumentation"**
- 79 **Fachartikel online**

RUBRIKEN

- 03 **Editorial**
- 04 **Inhalt**
- 80 **Veranstaltungskalender**
- 81 **Das letzte Wort**
- 82 **Vorschau, Impressum, Inserentenverzeichnis**

Optimierung von Virtual Desktop-Infrastrukturen



Die Virtualisierungsrate steigt und steigt. Desktops wandern vermehrt ins Rechenzentrum. Die IT-Planer stehen beim Thema VDI vor gänzlich neuen Herausforderungen, etwa Flaschenhälsen besonders zu Stoßzeiten. Am Beispiel virtueller Client-Sitzungen zeigen wir, welches Optimierungspotential gerade beim Thema Storage schlummert und wie Atlantis ILIO, eine Software zur Optimierung von VDI-Landschaften, den Administrator unterstützen kann.

Seite 42

Mit TeamDrive eine Private Cloud betreiben



Der Austausch von Daten zwischen Anwendern ist in Unternehmen heute gang und gäbe. Public Cloud-Dienste aber haben das Problem, dass sich die Informationen nicht mehr in der Hoheit des Unternehmens befinden. Um ungewollten Datenzugriffen einen Riegel vorzuschieben, bietet sich mit TeamDrive ein kostenloses Werkzeug an. Wir stellen Ihnen die wichtigsten Funktionen vor und erklären, wie Sie die nötige Client/Server-Konstruktion aufsetzen und betreiben.

Seite 58

Themenübersicht



Server- und Systemmanagement



Netzwerkmanagement



Clientmanagement



Job/Weiterbildung



Storage



Virtualisierung



Sicherheit



Recht



Messaging



Anpiff, Anstoß, Tor!

Machen Sie Ihre IT zum Sieger

Mit Client-Management zum Erfolg: Sichern Sie sich umfassende Informationen und finden Sie heraus, wie Sie aktuelle Herausforderungen effizient meistern.

Die Plätze sind limitiert. Die Teilnahme ist kostenlos.

Agenda

- Anforderungen an ganzheitliches Management von Arbeitsplatzumgebungen
- Plattformübergreifendes Management der verschiedensten Endgeräte
- Compliance- und Schwachstellenmanagement
- Analysten-Ausblick auf IT-Trends



Termine und Orte

01.04. Dresden	08.05. München
08.04. Berlin	13.05. Dortmund
10.04. Leipzig	20.05. Hamburg
29.04. Frankfurt	22.05. Wolfsburg
06.05. Nürnberg	27.05. Sinsheim



Veranstalter ist die baramundi software AG. Es erwarten Sie Keynote Speaker von Samsung und techconsult!

Sichern Sie sich Ihre Eintrittskarte!

www.baramundi.de/focustour

Speicher stufenweise freischalten

Von **Quantum** kommt mit der Produktserie DXi4700 eine neue Reihe an **De-duplizierungsappliances** auf den Markt. Das erste Modell, die **DXi4701**, verfügt über eine nutzbare **Speicherkapazität von 5 bis 135 TByte**. Punkten will der Hersteller unter anderem mit einer **bedarfsgerechten Kapazitätserweiterung**: Die Geräte werden mit einer bestimmten Anzahl an selbstverschlüsselnden 4 TByte-Laufwerken ausgeliefert, die der Nutzer jedoch nicht gleich komplett bezahlen muss. Vielmehr lässt sich der nutzbare Speicher stufenweise auf Lizenzbasis freischalten. Quantum bewirbt die Appliance mit einer Inline-Performance von 5 TByte pro Stunde und

niedrigen Kosten pro TByte. Je nach Gesamtkapazität – der Listenpreis für die DXi4701 startet bei 16.000 US-Dollar – liege dieser zwischen 1.521 und 3.200 US-Dollar pro TByte. Wie die anderen Mitglieder der DXi-Familie bietet die DXi4700 einen Installationsassistenten, grafisches Reporting, terminierte Replikation, NAS- und VTL-Darstellung und 1/10GbE-Konnektivität. Das Gerät bietet zudem OpenStorage-Unterstützung. Auf NetBackup und Backup Exec basierende Features wie Auto Image Replication (AIR) und Granular Restore Technology (GRT) sollen sich so ohne Probleme nutzen lassen. (In)

Quantum: www.quantum.com/products/disk-basedbackup/



Die DXi4701 ist ab Werk mit selbstverschlüsselnden Festplatten ausgestattet, die hardwarebasiert mit AES 256-Algorithmus arbeiten

Storage mit hoher SSD-Auslastung

HP verleiht Software-definierten Speichersystemen Gestalt und bringt mit **HP StoreVirtual 4345** eine hybride Storage-Appliance auf den Markt, die **Daten automatisch und dynamisch zwischen Solid-State-Disks und herkömmlichen Festplatten verschiebt**. Das "Adaptive-Optimization" genannte Feature soll per Auto-Tiering für eine besonders effiziente Nutzung von wertvollem SSD-Speicherplatz sorgen. Eine **Software beobachtet Muster im Datenzugriff** mit einem Genauigkeitsgrad von 256 KByte und stellt diese transparent dar. Dann verschiebt sie die Daten, auf die besonders häufig zugegriffen wird, auf SSD-Medien. Dabei hält sie die leistungsfähigsten Speicherebenen für geschäftskritische Anwendungsdaten vor und speichert replizierte Daten (RAID 10, RAID 10+) sowie Paritätsdaten (RAID

5 und 6) auf günstigeren SAS-Laufwerken. Dadurch will der Hersteller eine nahezu einhundertprozentige Auslastung des vorhandenen SSD-Speichers möglich machen. Wie alle Appliances der StoreVirtual-Reihe nutzt das Modell 4345 als **Betriebssystem HP LeftHand OS**. Im aktuellen Release 11.0 lässt sich LeftHand OS nun auch über SMI-S mit Microsofts System Center 2012 R2 Virtual Machine Manager integrieren; das Plug-In HP Insight Control ermöglicht zudem die Anbindung an VMwares vCenter Server. Die Standard-Konfiguration des HP StoreVirtual 4345 umfasst sieben 10K-SAS-Laufwerke mit je 900 GByte in Small Form-Factor-Bauweise und drei Enterprise Mainstream-SSDs mit je 400 GByte. Der Einstiegspreis liegt bei rund 36.000 Euro. (In)

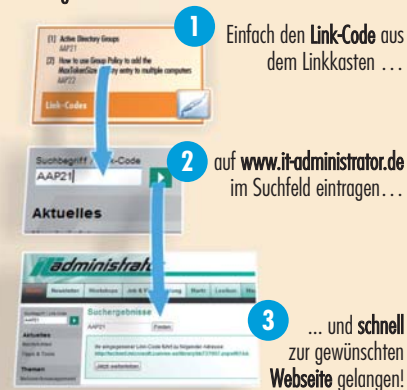
HP: <http://www8.hp.com/de/de/products/data-storage/>

Sicherer Briefverkehr

Norman hat die **E-Mail-Schutzsoftware Norman Email Protection** runderneuert. Neben dem **Schutz vor Malware, Spam und Phishing-Angriffen** ermöglicht sie die **Verwaltung von bis zu 500 Mailboxen**; ein optionales Add-On hilft bei der **Durchsetzung von Unternehmensrichtlinien** zu den Inhalten von E-Mails. Wichtigste Neuerung ist die Anpassung des Produktes an die **aktuellen Versionen der Microsoft-Plattformen** Windows Server 2012 (R2), Exchange Server 2013 und SQL Server 2012. Weiterhin wurde die **Datenbank für Absender- und Schadcode-Informationen** ausgebaut. Die **Umstellung auf SQL 2008** als Standard-Datenbank verspricht ferner eine bessere Leistungsfähigkeit der Schutzlösung. Auch die **Benutzeroberfläche** hat der Hersteller neu konzipiert. Sie kann jetzt unter den neuesten Browser-Versionen eingesetzt werden. Zusätzliche **Verwaltungs- und Monitoring-Funktionen** der Web-Schnittstelle sollen den Administratoren die schnellere Abwicklung von Routine-Arbeiten und den detaillierten Überblick über die genutzten Schutz-Funktionen, die System-Ressourcen und den Zustand des Mailservers ermöglichen. Die neue Version von Norman Email Protection ist ab sofort verfügbar. Die Jahreslizenz für bis zu 25 Mailboxen kostet ab 590 Euro, die Jahreslizenz für einzelne Mailboxen ab neun Euro. (dr)

Norman: www.norman.de

Unsere Link-Codes ersparen Ihnen mühsame Tipparbeit bei langen URLs:



So funktionieren Link-Codes



Dünn statt dick

TAROX erweitert sein Portfolio im Bereich Server-based Computing um den **Thin Client TC100R**. Ausgerüstet ist der Rechner mit dem **Betriebssystem Rango Linux** einschließlich einer eigenen TAROX-Oberfläche. Ein Dual Core VIA Eden X2 U4200 Prozessor, **2 GByte RAM und 8 GByte Flashspeicher** verrichten im Inneren des 195 x 42 x 145 mm messenden Gehäuses ihren Dienst. Optional ist ein WLAN-Anschluss per Stick, der sich zum Schutz vor Beschädigung oder Diebstahl hinter einer seitlichen Klappe sicher verschrauben lässt. Die Neuauflage verfügt über je einen **DVI-I- und DVI-D-Grafikausgang** und ist in Full-HD-Auflösung (1920x1200) im Dual-Monitorbetrieb einsetzbar. Dank der Unterstützung aller relevanten Übertragungsprotokolle (Microsoft RDP, Citrix ICA) können Unternehmen den Thin Client einfach in konventionelle als auch VMware-basierte Netzwerke integrieren. Die für die Wartung über den Server notwendige Konsole TCMS ist über den Hersteller

kostenlos erhältlich. TAROX liefert den Thin Client TC100R ab sofort zu einem Preis von rund 250 Euro aus. (In)

TAROX: www.tarox.de



Nutzer des TC100R können den Thin Client entweder mit einer VESA-Halterung an der Monitorrückseite montieren oder auf dem Schreibtisch platzieren

Unterwegs mit 4.000 ANSI-Lumen

Mit Modell **IN3138HD** hat **InFocus** ab sofort einen **Projektor** im Angebot, der **Full-HD-Auflösung von 1920 x1080 Pixeln auch bei der 3D-Darstellung** verspricht. Mit einer **Helligkeit von 4.000 ANSI-Lumen**, einem Sechsstufigen-Farbrad, BrilliantColor DLP-Imaging und einer Kontrastdarstellung von 5.000:1 soll der Beamer für einwandfreie, hochauflösende Bilder sorgen. Darüber

hinaus ist er mit integrierten 10 Watt-Lautsprechern ausgerüstet. Umfangreiche Anschlussmöglichkeiten sollen gewährleisten, dass das Gerät eine ganze Bandbreite unterschiedlicher Signalquellen mühelos verarbeiten kann. Über den integrierten HDMI-Anschluss, den DisplayPort sowie die NVIDIA 3DTV-PC-Konnektivität lassen sich **Inhalte direkt vom PC, Tablet oder Smartphone aus projizieren**. Als besonders praktisch führt der Hersteller ins

Feld, dass sich der Neuzugang **per Remote-Zugriff** komplett über das vorhandene Netzwerk steuern und konfigurieren lässt. Aufgrund der 144

Hz Triple-Flash-Funktionalität soll das Bild bei einer 3D-Wiedergabe komplett flimmerfrei sein. Für rund 975 Euro wirft der IN3138HD bis zu 10 Meter breite Full-HD-Bilder auf die Wände von Konferenzräumen. (In)

InFocus: www.infocus.de/projectors/



Mit Abmessungen von 285 x 261 x 122 mm und einem Gewicht von 3,15 kg gehört der Projektor InFocus IN3138HD zu den portableren seiner Art



Citrix lüftet den Vorhang für Version 7.5 der Virtualisierungswerkzeuge **XenDesktop** und **XenApp**. Die jüngsten Releases sollen vor allem die Integration in Cloud Umgebungen weiter verbessern. So kann XenDesktop nun Anwendungs- und Desktop-Workloads gleichzeitig an Private oder Public Clouds sowie an lokale virtuelle Infrastrukturen weiterleiten. Citrix betont dabei, dass XenDesktop die Nutzung verschiedener Public Clouds auf dem Markt erlaube, ohne bestimmte Anbieter vorzuschreiben. Mit XenApp 7.5 lassen sich in die Cloud ausgelagerte Applikationen jetzt auch dort weiterentwickeln. (In)

Link-Code: [E3A11](#)

regify bringt mit **regichat** ein sicheres und vertrauenswürdiges Chat-Werkzeug auf den Markt. Die Neuauflage richtet sich an professionelle Nutzer, die im Chat Vereinbarungen treffen und Verträge schließen wollen. Alle Teilnehmer erhalten dabei ein vollständiges Chat-Protokoll, das online auf seine Echtheit überprüfbar ist. Für die Nutzung des Chats reicht ein beliebiger Browser. Darüber können auch Dokumente hochgeladen und den Teilnehmern zugänglich gemacht werden. Das Werkzeug läuft auch auf Smartphones mit Android oder iOS. (In)

Link-Code: [E3A12](#)

Ab sofort bietet **Software602** mit **Long-Term Docs** eine Software an, die digitale Dokumente automatisch mit rechtsgültigen Zertifikaten sowie einer zukunftssicheren Formatierung versieht. Der Anbieter verspricht, dass so behandelte Informationen bis zu 30 Jahre später noch lesbar und rechtsgültig sind. Dazu bedient sich das Werkzeug des Dateiformats PDF/A. Die Dokumente lassen sich von jedem mobilen Gerät öffnen und vollumfänglich nutzen. Eine kostenlose Probeversion sowie die Pakete Start, Plus und Pro stehen für einen Preis ab 39 Euro pro 500 Dokumente zum Download bereit. (In)

Link-Code: [E3A13](#)

Red Hat gibt die Verfügbarkeit von **JBoss Data Virtualization 6** bekannt. Die Plattform bietet laut Hersteller eine schnelle, native Out-of-the-Box-Anbindung an verschiedene Datenquellen mit unterschiedlichen Zugriffsmethoden und Speichermodellen. Die Daten aus diesen Quellen werden gemäß Red Hat abstrahiert und so aufbereitet, dass Entwickler sich auf die inhaltlichen Aspekte ihrer Applikationen konzentrieren können. Mit Hilfe einer einheitlichen 360-Grad-Sicht soll das Werkzeug in Echtzeit ein vollständiger Überblick über Master- und Transaktionsdaten ermöglichen. (In)

Link-Code: [E3A14](#)

Online vorgestellt

Lenovo drängt nach vorn

Kurz nach der Übernahme der x86-Serversparte von IBM geht **Lenovo mit drei neuen Server-Modellen** an den Start. Die **Rack-Modelle ThinkServer RD340 und RD440** sollen selbst aufwendigste Infrastruktur- und Branchenanwendungen bewältigen und verfügen dazu über einen **Arbeitsspeicher von bis zu 192 GByte**. Zur Serienausstattung gehören unter anderem Massenspeicher, die sich während des laufenden Betriebs austauschen lassen, integriertes RAID sowie redundante Stromversorgung und Kühlung. Der ThinkServer RD440 unterstützt **bis zu 48 TByte internen Speicher**. Auf Wunsch sind weitere RAID-Adapter erhältlich, mit denen zusätzliche RAID-Level und andere leistungssteigernde Optionen möglich sind. Was die unterstützten Betriebssysteme betrifft, laufen auf den Maschinen Windows Server 2008 und 2012, Windows Small Business Server 2011, Novell SUSE Linux Enterprise Server, Red Hat Enterprise Linux Server, VMware ESXi sowie Citrix XenServer. Die beiden Rack-Server sind ab sofort zu einem Preis ab 1.030 Euro erhältlich. Wie die Rack-Varianten ausgestattet mit bis zu zwei Intel Xeon E5-2400 v2-Prozessoren, bietet der neue **ThinkServer TD340** im

Tower-Format laut Lenovo die Leistung eines vollwertigen Rack-Servers der Einstiegsklasse. Der Server soll sich für Unternehmen mittlerer Größe eignen, die neben Infrastruktur- und POS-Anwendungen noch Datenbanken und CRM nutzen. Features wie die Möglichkeit, HDDs oder SSDs im laufenden Betrieb zu wechseln, oder eine **sekundäre Stromversorgung** bieten Nutzern ein Plus an Sicherheit. Der TD340 unterstützt bis zu 192 GByte Arbeitsspeicher, bis zu 32 TByte Festplattenspeicher und hält **bis zu sechs PCI/PCIexpress-Slots** vor für unterschiedlichste Schnittstellen-Möglichkeiten wie etwa komplexe RAID-Systeme oder 10Gb-Ethernet. (ln)

Lenovo: <http://shop.lenovo.com/us/en/servers/thinkserver/>



Der ThinkServer RD440 von Lenovo misst zwei Höheneinheiten und bietet – je nach Bestückung mit HDs und SSDs unterschiedlicher Formfaktoren – bis zu 48 TByte Speicherplatz

Daten ausgeradiert

O&O Software stellt O&O Safe-Erase 7 Server und Workstation zur **sicheren Datenlöschung** vor. Durch die **native Unterstützung von Multikern-Prozessoren** und die **Beschleunigung der Löschalgorithmen** wurde etwa die Geschwindigkeit deutlich gesteigert. Dadurch sollen Unternehmen gerade bei großen Datenvolumen viel Zeit sparen können. Auch ist nun ein **Löschen des gesamten Rechners** ohne Start-Medium möglich. Dabei werden sämtliche Dateien, Einstellungen, Applikationen und das Betriebssystem derart gelöscht, dass eine Wiederherstellung ausgeschlossen ist. Außerdem listet die Software nun pro **Browser**

alle gespeicherten Informationen wie Cookies, Formulardaten oder Internet-Historien auf, die einzeln oder gebündelt sicher gelöscht werden können.

Detaillierte Berichte sollen Auskunft über ausradierte Dateien geben. In der Server-Edition kostet die Löschoftware 167 Euro, in der Workstation-Variante sind 33 Euro fällig. (dr)

O&O Software: www.oo-software.com/de

Mehr Speed für Virtualisierung und Cloud

Unter dem Namen **OneConnect OCe14000** gibt **Emulex** den Startschuss für eine neue Generation von **Ethernet- und Converged Network-Adaptern**. Die 10Gb- und 40Gb-Ethernet Network-Adapter und

Converged Network-Adapter (CNA) basieren auf den Emulex Engine 100 I/O-Controllern. Die neuen Adapter nutzen skalierbare Hardware Offload-Technologien zur Übertragung des Overheads des virtuellen Networkings. Das soll für eine bis zu 50-prozentige Verbesserung der CPU-Auslastung im Vergleich zu üblichen NICs beim Betrieb etwa in einer VMware Virtual-Wire-Umgebung sorgen. Darüber hinaus ermöglicht der Adapter laut Emulex eine vierfache Leistungsverbesserung bei der Small Packet Network Performance, die zur Skalierung transaktions-schwerer und geclusterter Anwendungen notwendig ist. Die Technologien Generic Routing Encapsulation (NVGRE) und Virtual Extensible LAN (VXLAN)

werden unter Microsoft Hyper-V Network Virtualization beziehungsweise VMware NSX dazu benutzt, um die Beschränkungen bestehender Rechenzentrumsnetzwerke zu adressieren. Zudem widmet sich auch Emulex der Implementierung von Software-Defined Networking und stellt unter der Bezeichnung SURF eine entsprechende offene API vor. Nicht zuletzt soll der neue Adapter die Block-Protokoll-IOPS um 50 Prozent gegenüber früheren CNAs anheben. Single- und Dual-Port 10GbE SFP+-Modelle und Single-Port 40GbE QSFP+-Modelle der Emulex OCe14000-Familie sollen noch in diesem Quartal zum Preis ab 448 US-Dollar in den Handel kommen. (ln)

Emulex: www.emulex.com/products/



Emulex will es mit der Adapter-Serie OneConnect OCe14000 erlauben, die Performance in drei Dimensionen zu skalieren – nämlich höhere Bandbreite, reduzierte Latenzzeiten und mehr I/O-Vorgänge pro Sekunde

Rauer Tablet-Geselle

PENTA präsentiert mit dem **Ultra-10** einen **industriell nutzbaren, robusten Tablet-PC**. Der Neuzugang im **10,4-Zoll-Format** ist für den **Einsatz in rauen Umgebungen**, auch im erweiterten Temperaturbereich, geeignet – weder Stöße gegen das Gehäuse noch Stürze oder extreme Umgebungstemperaturen von -25°C bis $+50^{\circ}\text{C}$ sollen

das Gerät in seiner Funktionalität einschränken. Für Leistung sorgen der **Intel Atom-Prozessor D2550 mit 1,86 GHz**. Das passiv gekühlte System wiegt 1,65 kg und ist mitsamt der Schnittstellen rundum vor dem Eindringen von Staub und Wasser geschützt (Schutzklasse IP65) und frei von Lüftungsschlitzen. Betrieben wird der Ultra-10 über **zwei**

Lithium-Ionen-Akkus. Jeder davon soll selbst bei voller CPU- und Displayleistung bis zu vier Stunden halten und lässt sich dank Hot-Swap-Unterstützung im laufenden Betrieb austauschen. Die integrierte “intelligent Smart Touch Control” (iSMT) erlaubt außerdem, die Akku-Belastung jederzeit manuell zu regulieren. Funktionen, die der Nutzer nicht benötigt, können via iSMT abgeschaltet oder angepasst werden, um die Akkus zu schonen. Der Tablet-PC verfügt über ein Interface für eine fahrzeugtaugliche Docking-Station. Über diese stehen zwei USB 2.0- und eine GBit-Ethernet-Schnittstelle zur Verfügung. Zum kabellosen Datenabgleich verfügt der Rechner über integriertes WLAN 802.11a/g/n, Dualband Wi-Fi mit aktiver Antennenumschaltung (intern/extern), Bluetooth 4.0 und optional LTE, UMTS oder GSM. Für die Datenspeicherung setzt der Hersteller auf CFast SATA II-Speicherkarten. Das Tablet ist kompatibel mit Windows 7 sowie 8 und unterstützt kundendefinierbare Embedded Linux-Distributionen. Der neue PENTA Ultra-10 ist ab sofort zu einem Preis ab 2.300 Euro verfügbar. (In)

PENTA: www.penta.de



Das Multitouch-Display des PENTA Ultra-10 ist reflexionsarm und dank integriertem Lichtsensor auch bei einer Helligkeit von 800 bis 1000 cd/m² ablesbar

Verschlüsselung für Mac-Freunde

Origin Storage bietet die **externe, hardwareverschlüsselte Festplatte DataLocker 3** nun auch in für Mac-Rechner vorformatierten Varianten an. Durch die Verwendung des Dateisystems HFS+ können Apple-Anwender die Festplatten sofort ohne zusätzliche Anpassungen nutzen. Die Daten werden mit AES-XTS 256 Bit per Hardwareverschlüsselung geschützt. Die Authentifizierung des Berechtigten erfolgt durch Eingabe einer PIN mit bis zu 31 Stellen auf dem integrierten Touchscreen. Die Mac-Variante ist mit 320 Gigabyte oder ein Terabyte Kapazität sowie als SSD mit 256 Gigabyte verfügbar. Preislich startet die vorformatierte DataLocker 3 bei rund 185 Euro. (In)

Origin Storage: www.originstorage.com

Außen Storage, innen Windows

Buffalo Technology präsentiert die **TeraStation WSS 2012-Serie (WS5000R2)** – einen **iSCSI-basierten Windows Storage Server R2** für kleine und mittlere Unternehmen. Die voll bestückte Serie ist als **Rackmount- oder Desktop-Variante** mit Kapazitäten von **4 bis 24 TByte** erhältlich und ausgestattet mit einem Intel Atom Dual-Core Prozessor – entweder mit dem D2550 für zwei und vier Einschübe oder mit dem D2700 für sechs Einschübe und Rackmount. Die TeraStation lässt sich in das **Active Directory** integrieren, was den Zugang und die Verwaltung des Speichers wie bei einem Windows-Server ermöglicht. Zudem stehen zur Verwaltung die **PowerShell, Microsoft Systems Center** und eine breite Palette an **Speicherprotokollen** zur Verfügung. Der Wechsel der Fest-

platten ist im laufenden Betrieb möglich, während die Daten per RAID (RAID 0/1, Spanning, JBOD) vor Verlust gesichert sind. Die Preise liegen je nach Variante zwischen 714 und 2.345 Euro. (dr)

Buffalo Technology: www.buffalo-technology.de



Die TeraStation WSS 2012 arbeitet mit Windows Storage Server R2 und speichert bis zu 24 TByte



IT-Administrator Training vSphere-Tuning und -Monitoring

VMware-Administratoren kommen im Rahmen unseres kostengünstigen 1-Tages-Trainings voll auf ihre Kosten. Auf der Agenda: Die Überwachung und Leistungsoptimierung von vSphere-Infrastrukturen, um Performance-Engpässen vorzubeugen.

Das Ziel des neuen IT-Administrator Trainings "vSphere-Tuning und -Monitoring" ist es, IT-Verantwortlichen Methoden an die Hand zu geben, um Leistungsgengpässe in der VMware-Infrastruktur gezielt und im besten Fall proaktiv aufzuspüren und auszumerzen. Denn eine Reduzierung der Performance des Systems um beispielsweise 15 Prozent mag im Alltagsbetrieb unbemerkt bleiben, wird bei Spitzenlasten aber sehr schnell auf die Agenda des Systemverantwortlichen rücken. Ansatzpunkte für eine solche Systemüberwachung stellen wir den Teilnehmern etwa beim Sizing von VMs, den Snapshots und bei der Storage- und Netzwerkkonfiguration vor.

Hand in Hand mit diesen Methoden geht die Leistungsoptimierung der Umgebung. Denn nicht jede Umgebung arbeitet mit den gleichen Parametern auch gleich gut und wer sein Monitoring im Griff hat, kann an verschiedenen Stellschrauben drehen, um die Leistung zu optimieren.

So lassen Sie etwa mehr VMs pro Host fahren oder die Performance eines speziellen Systems lässt sich signifikant steigern. Hier werfen wir unter anderem einen Blick auf mögliche Memory-Engpässe – Stichwort Ballooning/Swapping – oder den Umgang mit hoher I/O-Last.

Unser neues Training wendet sich an VMware-Administratoren, die Leistungsprobleme in ihrer vSphere-Infrastruktur vermeiden oder gezielt aufspüren möchten – unabhängig von der Größe der jeweiligen Installation. Wir vermitteln dieses Wissen als Vortrag, der durch zahlreiche Demos des Dozenten unterstützt wird.

Zu jedem der vier Termine stehen 25 Plätze bereit, die unserer Erfahrung nach schnell vergeben sein werden – wie immer sichert eine schnelle Anmeldung Ihren Wunschtermin und -ort. Das Anmeldeformular und die detaillierte Agenda finden Sie auf unserer Homepage unter "Workshops". (jp)

Die Inhalte des Trainings

Performance-Killer gezielt identifizieren

- Ressourcenmanagement
- Sizing von VMs und Snapshots
- Storage- und Netzwerkkonfiguration

Tipps & Tricks zum Tuning der Umgebung

- Ressourcenlimits
- Memory-Engpässe vermeiden
- Umgang mit hoher I/O-Last

Monitoring der vSphere-Umgebung

- vCenter Performance-Ansichten und -Alarmer
- Externes Monitoring am Beispiel PRTG
- Integration von opvizor

Methoden

Vortrag mit Demo am Dozenten-Rechner.

Maximale Teilnehmerzahl

25

Termin & Ort

8. April 2014: München (10 bis 17 Uhr)
 Experteach Training Center München
 Wredstr. 10, 80333 München

14. April: Berlin (10 bis 17 Uhr)
 Fast Lane Institute for Knowledge Transfer GmbH,
 Oranienburger Straße 66, 10117 Berlin

22. April: Hamburg (10 bis 17 Uhr)
 Experteach Training Center Hamburg,
 Esplanade 6, 20354 Hamburg

6. Mai: Frankfurt/M. (10 bis 17 Uhr)
 Experteach Training Center Frankfurt, Dietzenbach,
 Waldstraße 10, 60128 Dietzenbach

Teilnahmegebühren

Für IT-Administrator Abonnenten 195,90 Euro inklusive 19% Mehrwertsteuer. Für Nicht-Abonnenten wird eine Gebühr von 254,90 Euro (inklusive 19% MwSt.) fällig.

Die Teilnahmegebühr umfasst das Training inklusive Dokumentation und das Mittagessen am Trainingstag.

Anmeldung und detaillierte Agenda

www.it-administrator.de/workshops

vSphere-Tuning und -Monitoring



Dozent



Der Dozent Jan Große arbeitet als Systems Engineer bei der opvizor GmbH. Neben der Beratung in technischen Belangen ist er mitverantwortlich für die Weiterentwicklung der opvizor-Lösung, welche die virtuellen Infrastrukturen analysiert und vorausschauend auf Probleme hinweist, bevor sie sich auf die virtuelle Infrastruktur negativ auswirken. Jan Große hat mehr als zehn Jahre Erfahrung bei der Planung und Umsetzung von Infrastruktur- und Virtualisierungsprojekten.

Der fachliche Leiter Dennis Zimmer hat mehr als 15 Jahre Erfahrung in der IT und sich auf Virtualisierung spezialisiert. Er gehört zu den führenden Meinungsbildnern in der Virtualisierungscommunity und ist ein weltweit bekannter Experte mit ausgezeichneten Kontakten zu Herstellern und der Community. Weiterhin ist er im fünften Jahr in Folge VMware vExpert sowie Inhaber und Geschäftsführer der opvizor GmbH.



Fachliche Leitung

1&1 SERVER

WELTNEUHEIT IN 1&1 QUALITÄT



BRANDNEU & SCHON BEI 1&1:

INTEL® ATOM™
1&1 DEDICATED SERVER A8i

ab **39,99** €/Monat*

NEU: 1&1 DEDICATED SERVER A8i MIT 30% MEHR PERFORMANCE!

- Intel® Atom™ C2750
- 8 Cores und 8 GB RAM
- 2x 1.000 GB SATA HDD
- Parallels Plesk Panel 11
- Linux-, Windows- oder Managed-Server
- 100 Mbit/s Netzwerk
- Voller 64 bit Support
- 30 % mehr Performance durch „System-on-Chip“ (SOC)



 0 26 02 / 96 91
 0800 / 100 668



1und1.info

* 1&1 Dedicated Server A8i nur 39,99 €/Monat bei 24 Monaten Vertragslaufzeit, 49,99 €/Monat bei 12 Monaten Vertragslaufzeit oder 59,99 €/Monat bei 1 Monat Vertragslaufzeit. 49,- € Einrichtungsgebühr. Preise inkl. MwSt. Intel, das Intel-Logo, Intel Atom und Intel Atom Inside sind Marken der Intel Corporation in den USA oder anderen Ländern.
1&1 Internet AG, Elgendorfer Straße 57, 56410 Montabaur

IT-Administrator Training

Best Practices

Hyper-V

Durch stete Verbesserungen seitens Microsoft hat sich Hyper-V mittlerweile zur ernsthaften Konkurrenz zu vSphere aufgeschwungen. Da der mittlerweile durchaus mit Enterprise-Funktionalitäten ausgestattete Hypervisor zudem kostenlos zu haben ist, findet er zunehmend Zuspruch in Rechenzentren. Sei es als Erseinstieg in die Virtualisierung, als Ersatz für einen bestehenden Hypervisor oder als zweite Virtualisierungsplattform – die Einführung und der Betrieb sollten Best Practices folgen. Diese kennt wie kein Zweiter Nils Kaczinski, MVP für Hyper-V, der in unserem neuen Training Hyper-V-Administratoren den optimalen Einsatz von Microsofts Hypervisor aufzeigt.

Grundlage jedes erfolgreichen IT-Projekts ist die solide Planung und Hyper-V macht hier keine Ausnahme. Ganz im Gegenteil: Ist eine Neueinführung vorgesehen, betreffen die notwendigen Anpassungen der Infrastruktur Server, Storage und auch das Netzwerk. Hier wird Nils Kaczinski typische Stolperfallen aus dem Weg räumen, um dann Best Practices bei der Installation und Grundkonfiguration vorzustellen.

Doch auch nach der Einführung lässt sich im laufenden Betrieb noch vieles optimieren, um die Leistungsfähigkeit von Features wie etwa der Livemigration vollständig auszunutzen. Hier lässt Sie der Dozent an seinem reichen Erfahrungsschatz aus der Praxis des Hyper-V-Betriebs teilhaben und stellt Best Practices für Clustering, Livemigration und Zuverlässigkeit des Systems

vor. Unser Training zeigt darüber hinaus, welche Optimierungen in der Konfiguration der virtuellen Maschinen erfolgen und wie Administratoren mehr Sicherheit und Stabilität in ihrer Hyper-V-Infrastruktur gewährleisten.

Unser neues Training wendet sich an Windows-Administratoren, die den Aufbau einer Hyper-V-Infrastruktur planen oder die bestehende Landschaft optimieren möchten. Wir vermitteln dieses Wissen als Vortrag, der durch zahlreiche Demos des Dozenten unterstützt wird. Zu jedem der drei Termine stehen 25 Plätze bereit, die unserer Erfahrung nach schnell vergeben sein werden – wie immer sichert eine schnelle Anmeldung Ihren Wunschtermin und -ort. Alle Details zur Anmeldung finden Sie im Kasten auf dieser Seite. (jp)



Dozent



Nils Kaczinski ist seit Mitte der Neunzigerjahre als Consultant für Windows-Netzwerke tätig und berät Firmen und Administratoren in technischen und strategischen Fragen. Für sein Engagement in Online-Communities hat Microsoft ihn seit 2003 regelmäßig als Most Valuable Professional (MVP) für Directory Services und Hyper-V

ausgezeichnet. Kaczinski leitet das Microsoft-Consulting bei einem hannoverschen Systemhaus. Seine Schwerpunkte sind die strategischen Themen Verfügbarkeit, Virtualisierung und IT-Sicherheit. Neben seiner beruflichen Tätigkeit ist er als Fachautor für Windows-Themen bekannt geworden und ist gefragter Sprecher auf Konferenzen und Community-Veranstaltungen. Das IT-Autorenblog faq-o-matic.net, das er mit über 80 Autoren betreibt, gehört seit 2005 zu den wichtigsten IT-Ressourcen der deutschsprachigen Community.



Quelle: digitalgenetics - 123RF

Die Inhalte des Trainings

- Der Plan macht das Projekt
- Hyper-V installieren und einrichten
- Clustering, Livemigration und Zuverlässigkeit
- Virtuelle Maschinen konfigurieren
- Tipps und Tricks für Sicherheit und Stabilität

Methoden

Vortrag mit Demo am Dozenten-Rechner.

Maximale Teilnehmerzahl

25

Termin & Ort

5. Juni 2014: Nürnberg (10 bis 17 Uhr)

New Elements,
Thurn-und-Taxis-Straße 10, 90411 Nürnberg

24. Juni: Essen (10 bis 17 Uhr)

PC-College,
Kruppstraße 96, 45145 Essen

15. Juli: München (10 bis 17 Uhr)

ExperTeach Training Center München,
Wredestr. 11, 80335 München

Teilnahmegebühren

Für IT-Administrator Abonnenten 195,90 Euro inklusive 19% Mehrwertsteuer. Für Nicht-Abonnenten wird eine Gebühr von 254,90 Euro (inklusive 19% MwSt.) fällig.

Die Teilnahmegebühr umfasst das Training inklusive Dokumentation und das Mittagessen sowie Kaffeepausen am Trainingstag.

Anmeldung und detaillierte Agenda

www.it-administrator.de/workshops

Best Practices Hyper-V



4 NETWORKING PARTYS – ÜBER 100 SESSIONS – 120 PARTNER – 5.000 BESUCHER



In association with



VERISIGN™



The power to do more



Das Magazin für professionelle System- und Netzwerkadministration

1.-3. APRIL 2014 – EUROPA-PARK RUST

INFO & ANMELDUNG:

WWW.WORLDDHOSTINGDAYS.COM

KOSTENLOSE ANMELDUNG
FÜR IT-ADMINISTRATOR
LESER!
CODE: ME712NW

main.FORUM



WikiLeaks

Julian Assange
Live via Skype



Microsoft

Brad Anderson
Corporate Vice
President



Intel

Raejeanne Skillern
Director, Cloud
Computing Marketing



Parallels

Birger Steen
CEO



Flexiant

Jim Foley
SVP Market
Development



**Im Test: Icomasoft Opvizer 2.1**

Expertenbesuch auf Knopfdruck

von Jürgen Heyer



Eine stabile Virtualisierungsplattform ist eine wichtige Voraussetzung für den zuverlässigen Betrieb der virtuellen Maschinen. Potentielle Gefahrenpunkte sollten daher frühzeitig erkannt und beseitigt werden, möglichst bevor sie sich zu ausgewachsenen Problemen entwickeln. Genau hier greift das Expertensystem Opvizer an, indem es den Administrator mit regelmäßigen Analysen und Hinweisen unterstützt und so dessen Fachwissen ergänzt. IT-Administrator hat sich genauer angesehen, wie gut und zuverlässig das funktioniert.

Opvizer ist eine Software-as-a-Service-Dienstleistung in Form eines Expertensystems im Internet, das Administratoren bei der Analyse und Pflege ihrer Virtualisierungsplattform unter VMware vSphere unterstützt. Kernstück des Produkts ist eine ständig aktualisierte Wissensdatenbank mit momentan etwa 700 praktischen Hinweisen und Konfigurationsempfehlungen. Durch den Betrieb als SaaS-Dienstleistung kann die Datenbank vom Hersteller kontinuierlich gepflegt und ergänzt werden, ohne dass sich die Kunden darum kümmern müssen. So steht sie allen Nutzern immer in der aktuellsten Version zur Verfügung, sodass auch neue Erkenntnisse umgehend weitergetragen werden.

Für eine Analyse werden die notwendigen Daten von einem Online-Agenten über das vCenter erfasst, hochgeladen und analysiert, die Ergebnisse dann in einer Web-GUI dargestellt. Eine optionale Anonymisierung verschleiert die Informationen, die Rückschlüsse auf den nutzenden Kunden erlauben. Dazu ersetzt der Online-Client alle kundenspezifischen Informationen vor dem Upload durch Kürzel und legt für ei-

ne spätere De-Anonymisierung der Resultate eine lokale Zuordnungstabelle an.

Gegenüber der vor knapp drei Jahren im IT-Administrator 4/2011 betrachteten Version 1.5 wurde Opvizer umfassend erweitert, die Anzahl der hinterlegten Regeln fast verdoppelt. Neu ist eine optionale Bereitstellung als On Premise-Produkt für Unternehmen, die auf keinen Fall irgendwelche internen Daten in die Cloud stellen dürfen oder wollen. Neben der Analyse einer vSphere-Umgebung unterstützt Opvizer jetzt auch die Beobachtung von Net-App-Fileln.

Nur gucken, nicht anfassen

Ein großer Vorteil von Opvizer ist, dass in einer bestehenden Virtualisierungsumgebung keinerlei Änderungen oder Anpassungen erforderlich sind, um das Produkt zu nutzen. Der Einstieg beginnt mit einer Registrierung für einen Zugang zur Opvizer-Plattform inklusive Erwerb der Lizenz für die Opvizer-Applikation. Für die Kommunikation wird nur ein Windows-System mit einem Zugriff auf den vCenter-Server benötigt, um dort das Opvizer-Softwarepaket zu installieren. Es

kann auch der vCenter-Server selbst verwendet werden.

Die Voraussetzungen sind nicht besonders hoch. Lauffähig ab Windows XP sind 2 GByte Hauptspeicher erforderlich, beim Zwischenspeichern von Log-Dateien können bis zu 1,5 GByte Plattenkapazität belegt werden. Erforderlich ist eine aktuelle Java-Umgebung, zu beachten ist, dass bei einem 64 Bit-Betriebssystem auch ein Java 64 Bit JRE installiert wird.

Das Setup der Opvizer-Software richtet einen Dienst ein und zur Konfiguration einen Web-Server, der standardmäßig über den Port 7777 erreichbar ist. Betreibt ein Unternehmen mehrere vCenter-Server, können alle von einem Opvizer-Dienst abgefragt werden. Zu beachten ist nur, dass ältere Versionen als vSphere 4 nicht unterstützt werden. In unserer Testumgebung installierten wir das Opvizer-Paket

VMware-Umgebung mit vSphere 4/5,
optional auch für NetApp-Fileln.

Systemvoraussetzungen



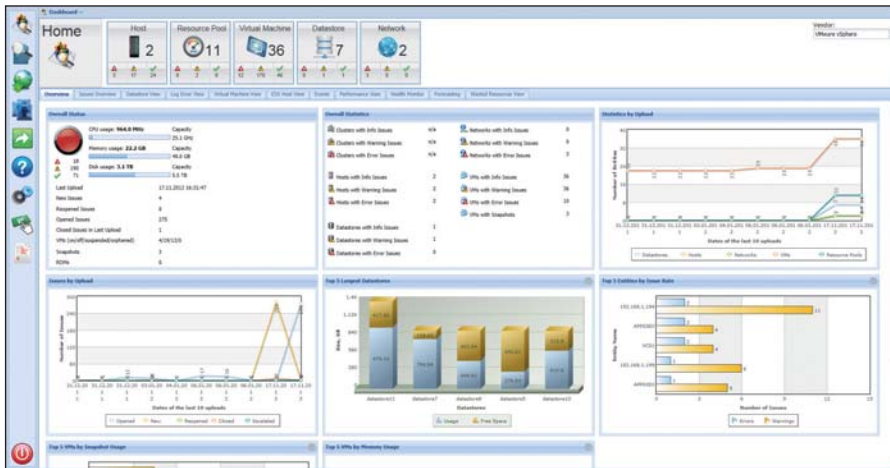


Bild 1: Das Opvizor-Dashboard liefert auf einen Blick umfassende Informationen zum Status der überwachten Umgebung und ist intuitiv bedienbar

auf einem unserer virtuellen Server, da wir in unserer vSphere-Farm die von VMware bereitgestellte vCenter-Appliance unter Linux nutzen, auf der sich die Software verständlicherweise nicht installieren ließ.

Der Opvizor-Dienst sammelt die Konfigurationsdaten und Log-Dateien über den oder die vCenter-Server ein, anonymisiert diese optional und lädt sie SSL-verschlüsselt auf die Opvizor-Server in der Cloud. Die Ablage dort erfolgt auf jeden Fall ebenfalls verschlüsselt mit AES 256 Bit sowie nach Kunden getrennt. Grundsätzlich nicht hochgeladen werden Informationen wie Benutzer, Passworte, Benutzerrechte, Daten von Gastapplikationen und Inhalte der virtuellen Festplatten. Um die Analyse regelmäßig durchzuführen, lässt sich ein Zeitplaner aktivieren, der mit dem installierten Dienst im Hintergrund die entsprechenden Abfragen durchführt. Opvizor empfiehlt je nach Größe der Umgebung unterschiedliche Abfrageintervalle als Mischung aus kompletten Abfragen aller Informationen und inkrementellen Ergänzungen. In einer kleinen Umgebung mit bis zu fünf ESX-Hosts werden eine volle Analyse alle zwei Stunden und halbstündliche Inkremente empfohlen, in sehr großen Umgebungen bei über 100 ESX-Hosts eine volle Abfrage täglich und Inkremente alle acht Stunden. Letztendlich liegt es auch in der Entscheidung des Administrators, geeignete Intervalle zu finden. Neben der Zeitplanung kann er noch einige weitere Einstellungen konfigurieren, so die Daten

eines SMTP-Servers hinterlegen und einen Proxy-Server eintragen, falls erforderlich. Sofern eine NetApp-Lizenz mit erworben wurde, sind auch die zu überwachenden NetApp-Filer einzutragen.

Ziel von Opvizor ist es, die Informationen zu lesen, auszuwerten und Hinweise zu geben. Opvizor ist aber nicht darauf ausgelegt, selbst irgendwelche Änderungen durchzuführen. Dementsprechend benötigt die Opvizor-Software für den Zugang auf das vCenter nur einen leseberechtigten Account und sollte auch nichts anderes bekommen. Allerdings verfügen die im vCenter hinterlegten Standard-Read-Only-Rollen (RO) nicht alle für Opvizor erforderlichen Leseberechtigungen. Das Opvizor-Handbuch beschreibt daher genau, wie eine RO-Rolle zu klonen und mit fünf zusätzlichen Rechten zu ergänzen ist.

Letztendlich obliegt es immer dem Administrator, die erhaltenen Hinweise nach zusätzlicher eigener Prüfung und Bewertung umzusetzen. Die ausschließliche Leseberechtigung hat unserer Einschätzung nach hinsichtlich der Bewertung der Datensicherheit sowie der Datenübergabe in die Opvizor-Cloud einen wichtigen Vorteil: Im schlimmsten Fall kann ein Unberechtigter bei Verzicht auf die Anonymisierung alle Auswertungen einsehen, es ist aber nicht möglich, durch Manipulationen bei der Analyse oder auf dem Datenweg etwas einzuschleusen, was dann eine virtuelle Umgebung lahmlegen kann. Der Verzicht auf Änderungen wurde von

**Windows XP
ist abgekündigt**

CeBIT

Beratung zur Migration
in Halle 3 am Stand G06



Windows 8

Migrieren Sie mit der
baramundi Management Suite
automatisiert auf eine aktuelle
Windows-Version!

Testen Sie 30 Tage kostenfrei:
www.baramundi.de/einfach-migrieren

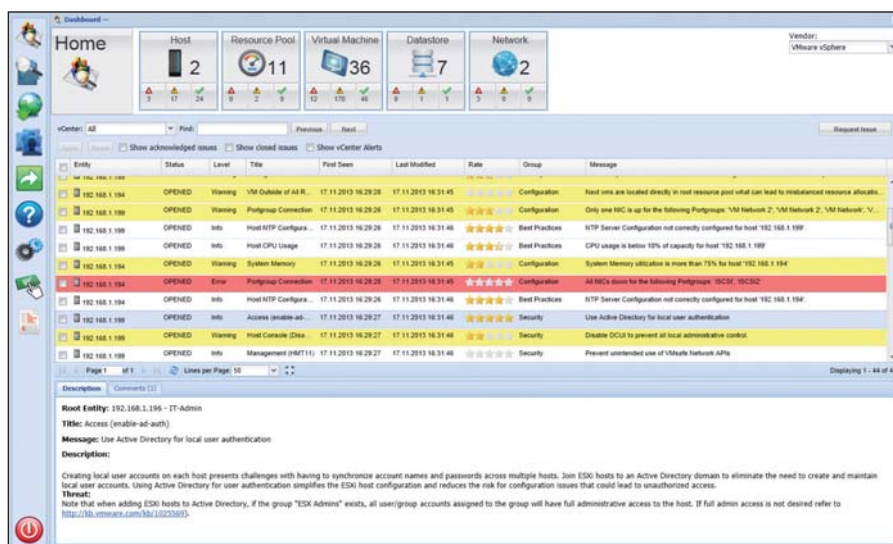


Bild 2: Die ermittelten Probleme und Ungereimtheiten werden von Opvizor bewertet und entsprechend unterschiedlich farbig unterlegt aufgelistet

Icomasoft bewusst so umgesetzt, da Administratoren in mittleren und größeren Umgebungen in der Regel sowieso keine Adhoc-Änderungen durchführen dürfen, sondern diese erst über ein Change-Management genehmigen lassen müssen. So entsteht erst gar nicht die Versuchung, schnell und womöglich doch unüberlegt etwas zu ändern.

Healthcheck mit 700 Regeln

Know-how und Intelligenz von Opvizor stecken in einer Datenbank mit einem Regelwerk, in dem aktuell rund 700 Regeln implementiert sind. Diese Regeln werden auf die erfassten Daten angewendet, um mögliche Engpässe, Sicherheitslücken und Fehlkonfigurationen aufzudecken oder auch Empfehlungen für Best Practice-Optimierungen auszusprechen. Icomasoft erweitert den Regelsatz kontinuierlich, die nächste Version 2.2 soll 715 Regeln enthalten. Da alle Daten in der Opvizor-Cloud analysiert werden, ist der auf Kundenseite installierte Dienst nicht betroffen, wenn neue Regeln aktiviert werden. Letztendlich muss ein Administrator nichts aktualisieren, solange keine Änderungen am Agenten notwendig sind.

Für die Darstellung nutzt Opvizor eine Java-basierte Web-GUI. Bei deren Aufruf erscheint die zentrale Ansicht, das sogenannte Dashboard, mit diversen statistischen Übersichten, viele davon in grafischer Form. In der Kopfzeile befindet sich eine Übersicht über die Anzahl der Hosts,

Ressourcenpools, VMs, Datenspeicher und Netzwerke des überwachten vCenters mit dem jeweiligen Alarmstatus (Fehler, Warnung, OK). Klickt der Administrator auf eines dieser Felder, erscheint die entsprechende Liste der Problemmeldungen, auf die wir noch genauer eingehen.

Darunter besteht das Dashboard aus insgesamt elf Registerblättern (Übersicht, Probleme/Issues, Datastore, Fehlermeldungen, VMs, ESX Hosts, Ereignismeldungen, Leistung, Gesundheit, Vorhersage und verschwendete Ressourcen), auf denen zu den genannten Themen in kleineren Fenstern und in zwei oder drei Spalten entsprechende Auswertungen und Übersichten zu sehen sind. So finden sich auf den Seiten diverse Top-n-Übersichten (etwa die fünf größten Datastores, die zehn VMs mit der größten Ressourcenutzung nach Speicher, CPU-Nutzung und Plattenkapazität) sowie Zusammenfassungen (durchschnittliche Speichernutzung aller VMs oder die durchschnittliche CPU-Nutzung). Während sich die meisten Übersichten jeweils auf die letzte Auswertung beziehen, gibt es auch einige Grafiken zum Vergleich der letzten zehn Uploads (Anzahl der VMs und Hinweise). Weiterhin zeigen Aufstellungen die Top 10 der VMs mit den meisten Fehlern und Warnungen sowie die letzten zehn aufgetretenen Hinweise.

Unter dem Registerblatt "Forecasting" zur Vorhersage ermittelt Opvizor das

mögliche Potential für neue VMs pro Cluster oder Host. Basierend auf der Speicher- und CPU-Nutzung von zehn Prozent der kleinsten oder größten VMs sowie dem allgemeinen Durchschnitt ermittelt das Tool, wie viele kleine, mittlere oder große VMs noch zusätzlich betrieben werden können. Das ist natürlich nur als grober Anhalt zu sehen. Als weitaus wertvoller fanden wir die Übersicht der verschwendeten Ressourcen "Wasted Resource View". Opvizor sucht hier nach verwaisten VMs und VMDK-Dateien, komplett ungenutzten Datastores, den größten ausgeschalteten VMs, den größten Snapshots und ungenutzten Netzwerken sowie LUNs. Werden in einer Umgebung irgendwelche Ressourcen knapp oder will ein Administrator grundsätzlich aufräumen, so lohnt sich ein Blick in diese Ansicht. Gelegentlich dürften hier auch freie Ressourcen gelistet sein, an die vorher keiner gedacht oder die keiner mehr gefunden hat.

Bei der Einrichtung eines Accounts startet Opvizor mit einer Standardanordnung der Fenster in der Web-GUI, diese ist jedoch nicht fix, sondern der Administrator kann die Fenster nach Belieben und Bedarf verschieben, sodass er sich beispielsweise die für ihn wichtigsten jeweils oben anordnet. Sofern bei einem Fenster oben rechts ein Zahnrad zu sehen ist, kann der Administrator hier die Kriterien verändern, also sich beispielsweise statt der fünf größten die sieben größten Datastores anzeigen lassen und dann nicht geordnet nach der Gesamtgröße, sondern anhand der freien Kapazität.

Zielgerichtete Fehlersuche

Opvizor nimmt seine Aufgabe, den Administrator proaktiv auf Probleme hinzuweisen, sehr ernst. Egal, ob er im Kopfbereich des Dashboards auf eine Zahl mit den ermittelten Problemen klickt oder in einem der Fenster auf einem der Registerblätter auf einen Balken, einen Eintrag oder ein Kuchenstück in einer Grafik, immer bekommt er als Resultat eine Übersicht der zu diesem Objekt anstehenden Probleme. Die Liste kann natürlich auch leer sein, wenn es gerade zu diesem Objekt kein Problem gibt. Gibt es welche, so sind diese entsprechend der Wichtigkeit

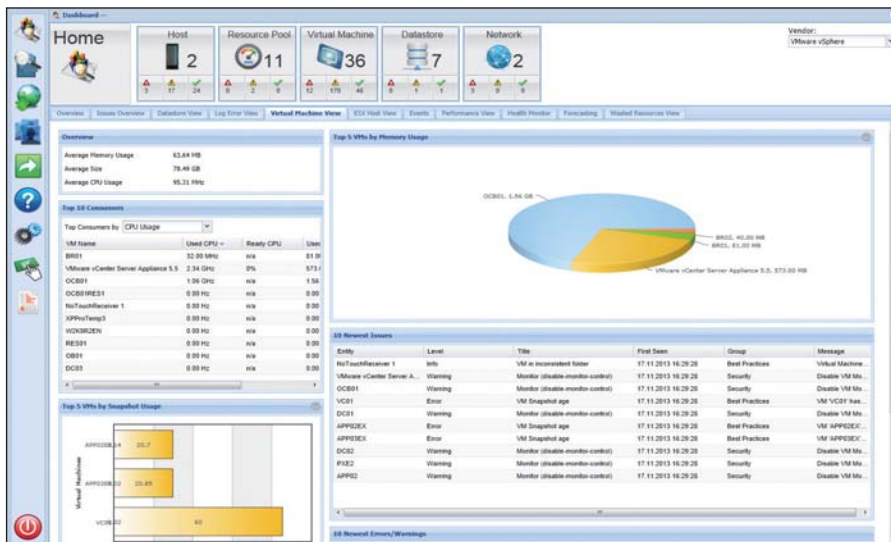


Bild 3: Innerhalb der Ansichten nutzt Opvizio unterschiedliche Darstellungsarten, um die Informationen möglichst einfach lesbar zu visualisieren

rot, gelb oder weiß unterlegt. Auf einen Blick sind Objekt, Titel, Status (offen, geschlossen, wieder eröffnet), Schweregrad (Info, Warnung, Fehler), Typengruppe (Konfiguration, Sicherheit, Best Practices), Zeit des ersten Auftretens und Zeit der letzten Aktualisierung erkennbar. Nach allen Spalten lässt sich sortieren.

Über einen Haken lassen sich auch bereits bestätigte Hinweise einblenden, diese werden dann im Status "CLOSED" durchgestrichen dargestellt. Aufgabe des Administrators ist es nun, die Hinweise abzuarbeiten, indem er entweder den Punkt löst oder die Meldung als solche bestätigt, damit sie im weiteren Verlauf nicht mehr angezeigt wird. Bei der Bestätigung einer Meldung kann er diese entweder nur für diesen speziellen Hinweis oder für alle identischen Hinweise auch bei anderen Objekten wirksam werden lassen.

Überaus wertvolle Lösungshinweise

Ausgesprochen gut gefallen haben uns der Umfang und der Detailgrad der Hinweise. So lieferte Opvizio im Test erstaunlich viele Tipps in der Rubrik "Best Practices", um Hinweise zu geben, wo sich gegebenenfalls etwas optimieren lässt oder Empfehlungen nicht eingehalten werden. Beispielsweise hatten wir bei den ESX-Hosts nur einen NTP-Server angegeben, es sollten aber zur Sicherheit mehrere sein. Auch bekamen wir Hinweise hinsichtlich einer

sehr niedrigen CPU-Auslastung sowie kaum belegter Datastores als Zeichen dafür, dass hier Ressourcen nicht optimal genutzt wurden.

Hinsichtlich der Detailliertheit liefert Opvizio zu jedem Hinweis eine genaue Beschreibung, dann die eventuell bestehende Bedrohung und gegebenenfalls eine exakte Anleitung, wo eine Einstellung geändert werden kann und welches Werkzeug sich dazu eignet. Sobald Opvizio zusätzlich auf die Dokumentation von VMware verweist wie auf den "vSphere Security Hardening Guide", so ist der Link hinterlegt und auch der Code angegeben, mittels dessen sich die entsprechende Stelle im Handbuch leichter finden lässt. Wir haben im Test aufgrund der Hinweise einige Fehler beseitigt und Tipps umgesetzt. In keinem Falle hatten wir Schwierigkeiten, diese aufgrund der Beschreibung auch zu finden.

Bei der nächsten Analyse nach der Beseitigung von Fehlern erkennt Opvizio dieses und setzt den Hinweisstatus auf "CLOSED", löscht ihn aber nicht vollständig, sodass er sich auch später wieder wie schon erwähnt optional anzeigen lässt. Um auch später eine Entscheidung nachvollziehen zu können oder anderen Administratoren zusätzliche Tipps zu geben, lassen sich zu jedem Problem mit Lösungshinweis zusätzlich eigene Kommentare hinterlegen, wieder bearbeiten und auch zu einem Kommentar wieder eine

Worüber Administratoren morgen reden

Sichern Sie sich den E-Mail-Newsletter des IT-Administrators und erhalten Sie Woche für Woche die

- neuesten TIPPS & TRICKS
- praktischsten TOOLS
- interessantesten WEBSITES
- unterhaltsamsten GOODIES

sowie einmal im Monat die Vorschau auf die kommende Ausgabe des IT-Administrators!

Jetzt einfach anmelden unter:



www.it-administrator.de/newsletter



Antwort schreiben. So kann ein Administrator beispielsweise zu dem Problem mit dem Titel "VMware Tools Outdated" eine eigene Handlungsanweisung als Kommentar hinterlegen, die dann immer mit angezeigt wird, wenn Opvizor dieses Problem irgendwo erkennt.

Gegenüber der früher getesteten Version wurde der Umfang der Hinweise enorm erweitert. Viele Hinweise enthalten jetzt auch komplette PowerShell-Skripte, um Einstellungen mittels PowerCLI oder vCLI zu ändern. Die Verwendung dieser Skripte ist vor allem dann sinnvoll, wenn es nicht nur darum geht, eine Einstellung für eine VM zu ändern, sondern über eine Schleifendefinition systematisch für alle Maschinen, um einen Serienfehler zu beseitigen.

Auswertungen anonym, lokal oder On Premise

Der Zugriff auf die Resultate der Analysen in der Opvizor-Cloud kann auf zwei Wegen erfolgen. Der eine ist die Nutzung der "Opvizor Management GUI" direkt auf dem System, auf dem der Agent installiert wurde, also über den dortigen lokalen Webserver. Die andere Möglichkeit besteht in der Anmeldung direkt auf der Opvizor-Homepage. Bei nicht genutzter Anonymisierung sind beide Ansichten identisch. Anders stellt sich das allerdings bei aktiver Anonymisierung dar. Dann sind über die Managementoberfläche nach wie vor alle Namen und Bezeichnungen im Klartext zu lesen. Beim Zugriff über die Opvizor-Homepage dagegen sind stattdessen nur Zahlenkürzel wie "^^212^^" zu sehen.

Wie führt nun Opvizor die Anonymisierung durch? Das Tool legt im Rahmen der Softwareinstallation auf diesem System lokal eine XML-Datei an, verknüpft in dieser jede kundenspezifische Bezeichnung mit einer Zahl nach obigem Muster und ersetzt vor dem Upload die Bezeichnungen durch diese Kürzel. Gleiche Kürzel deuten also stets auf das gleiche Objekt hin. Der Administrator kann die XML-Datei über die Management GUI einsehen. Im Web sind nun nur die Kürzel sichtbar, während bei der Ansicht über die GUI vorher eine De-Anonymisierung

stattfindet, indem die Kürzel wieder durch die ursprünglichen Bezeichnungen ersetzt werden. Genau dies ist bei der Betrachtung auf der Opvizor-Homepage nicht möglich, da die XML-Datei nur lokal beim Kunden verfügbar ist.

Laut Icomasoft verzichten viele Nutzer auf eine Anonymisierung, wenn sie geplant haben, die Daten beispielsweise dem betreuenden Systemhaus für Supportzwecke zur Verfügung zu stellen, damit alles besser lesbar ist. Auch zeigte uns ein Blick auf die anonymisierten Daten, dass sich trotzdem noch diverse Informationen herauslesen lassen wie die Leistungsdaten der ESX-Hosts und der angelegten VMs, Größe und Belegung der Datastores. Letztendlich sind nur die Objektbezeichnungen verschleiert.

Wichtig ist es bezüglich der Anonymisierung, sich einmalig zu entscheiden, ob diese genutzt werden soll oder nicht, da andernfalls ein unübersichtlicher Darstellungsmix entsteht. Im Zweifelsfall beziehungsweise bei einer Änderung der Entscheidung sollten alle bisher erfassten Daten gelöscht werden, was innerhalb von Opvizor recht einfach zu realisieren ist.

Nicht unerwähnt bleiben darf in diesem Zusammenhang, dass Opvizor mittlerweile auch in einer On-Premise-Version verfügbar ist, bei der die Auswertung nicht in der Cloud erfolgt, sondern auch die gesamte Basis im Kundennetz installiert ist. Dies zieht für den Kunden verständlicherweise einen größeren Aufwand nach sich, lohnt sich aber für größere Unternehmen, die keine Informationen in eine Cloud stellen dürfen oder wollen, durchaus.

Sehr umfassendes Reporting

Für regelmäßige Auswertungen und Benachrichtigungen beinhaltet Opvizor ein umfassendes Reporting. So sind für den VMware-Bereich 13 Berichte (unter anderem für die Rubriken Netzwerk, Probleme, Sicherheit, Inventarisierung oder Schnappschüsse) hinterlegt, wobei der Administrator bei den meisten Berichten noch eine eigene Filterung vorgeben kann, die entspre-

chend des Inhalts der Berichte variiert. Die Ausgabe kann wahlweise in HTML und PDF erfolgen. In beiden Fällen wird automatisch ein Inhaltsverzeichnis erstellt, sodass sich einzelne Punkte einfach anspringen lassen.

Die automatisierte Erstellung ist mit einem Mailversand gekoppelt. Dazu trägt der Administrator die Empfänger ein und

Produkt

Programm zur Analyse von Schwachstellen, Konfigurationsfehlern und Engpässen innerhalb einer virtuellen Infrastruktur sowie auf NetApp-Filem.

Hersteller

Icomasoft
www.opvizor.com

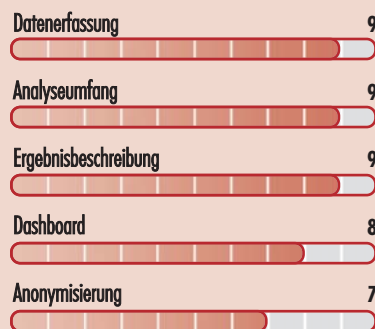
Preis

Die Lizenzierung erfolgt anhand der Anzahl der ESX-Hosts. Pro Jahr kostet die Nutzung des Dienstes 990 Euro pro ESX-Host.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für VMware-Umgebungen mit komplexem Aufbau in Unternehmen jeder Größe, die Wert darauf legen, dass die Konfiguration hinsichtlich Stabilität und Sicherheit möglichst optimiert ist. Durch die On Premise-Variante ist Opvizor auch für Unternehmen geeignet, die keine Daten in eine Cloud übergeben wollen.

bedingt für Unternehmen, die bei der Virtualisierung nicht nur auf vSphere setzen. Hier kann Opvizor nur einen Teil beaufsichtigen, für andere Plattformen sind eigene Tools erforderlich.

nicht für Umgebungen, die nicht auf Basis von VMware vSphere virtualisieren. Eine Version für Hyper-V soll Ende 2014 erscheinen.

Icomasoft Opvizor 2.1

bestimmt den Sendezeitpunkt als Wochentag und Uhrzeit. Er kann dabei einzelne Wochentage angeben, sodass er das Intervall zwischen täglich und einmal wöchentlich variieren kann. Natürlich lässt sich ein Bericht auch adhoc erzeugen, um innerhalb kürzester Zeit ein Ergebnis in der Hand zu halten.

Im Test erzeugten wir einige der angebotenen Berichte und konnten feststellen, dass diese sehr umfassend und informativ sind. Dabei sollte man sich nicht von der augenscheinlich geringen Anzahl von 13 Berichten täuschen lassen. Jeder Report für eine Rubrik beinhaltet auf mehreren Seiten diverse Tabellen und Grafiken, sodass die erwähnte Inhaltsverzeichnisstellung wirklich sinnvoll ist.

Support-Informationen gezielt teilen

Um beispielsweise für Supportzwecke einem Helpdesk oder einem anderen Spezialisten die notwendigen Informationen via Opvizor bereitzustellen, ist eine Sharing-Funktion implementiert. Voraussetzung ist, dass dieser Supporter ebenfalls einen Opvizor-Account besitzt. Ist dies noch nicht der Fall, kann ihm der Hilfesuchende via Opvizor eine E-Mail zukommen lassen mit der Aufforderung, sich zu registrieren.

Sobald dies geschehen ist, kann der Administrator das Dashboard für einen Supporter freigeben. Dieser kann sich nun die Umgebung ansehen. Sofern die Anonymisierung aktiviert ist, sind keine Bezeichnungen im Klartext sichtbar. Gefallen hat uns, dass beim Sharing anzugeben ist, wann dieses automatisch wieder aufgehoben wird. So ist es nicht notwendig, alle Freigaben manuell wieder rückgängig zu machen.

Sofern Systemhäuser Opvizor zur Überwachung von Kundenumgebungen nutzen wollen, gibt es hierfür eine spezielle Ansicht, auf die wir im Test einen Blick werfen konnten. In einer Partnerview für Managed Service Partner sieht ein System-Integrator alle Kundenumgebungen in einer Übersicht mit den wichtigsten Informationen und Bewertung in Ampelfarben. Durch einen Klick auf

einen Kunden gelangt er dann auf die freigegebene Ansicht und kann so bei Problemen weiter analysieren. Änderungen sind wie schon erwähnt auf diesem Wege nicht möglich.

Fazit

Der Test hat gezeigt, dass Icomasoft mit Opvizor eine äußerst informative Systemanalyse für Virtualisierungsumgebungen unter VMware vSphere sowie für NetApp-Filer anbietet. Mit der aktuellen Version 2.1 hat das Tool deutlich an Leistungsumfang zugelegt und beinhaltet mittlerweile über 700 Regeln zur Aufdeckung von Fehlkonfigurationen und potentiellen Problemen. Den größten Vorteil sehen wir darin, dass Opvizor proaktiv arbeitet und über die Regelprüfung auf Missstände hinweist, die sich oft aktuell noch gar nicht als richtiges Problem bemerkbar gemacht haben.

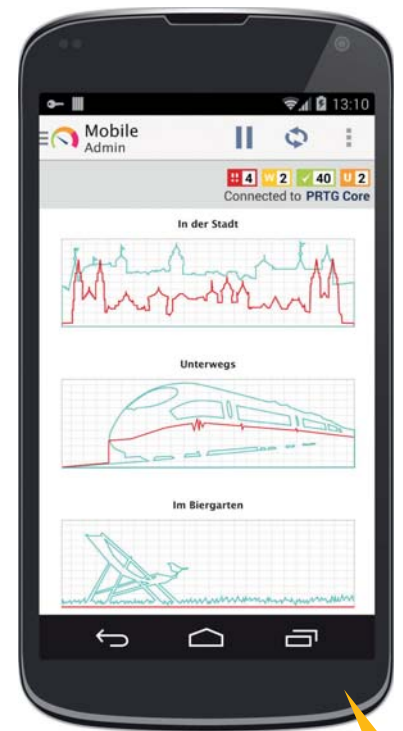
Durch das Konzept der SaaS-Dienstleistung ist der Einrichtungsaufwand auf Kundenseite minimal. Vielmehr erfolgt die Auswertung auf Servern in der Cloud, die die Informationen halten. Unter Sicherheitsaspekten sehr von Vorteil sehen wir die Arbeitsweise, dass Opvizor ausschließlich lesend zugreift und keine eigenständigen Änderungen durchführen kann. Darüber hinaus können die Daten vor der Übergabe an die Cloud anonymisiert werden, was einen gewissen zusätzlichen Schutz bietet. Sehr interessant sehen wir Opvizor als Hilfsmittel für Systemhäuser, die auf diesem Wege die Umgebungen ihrer Kunden überwachen wollen. Momentan noch auf vSphere 4/5 und NetApp-Filer beschränkt, soll Opvizor gegen Ende 2014 auch für Hyper-V verfügbar sein.

Bei den Lizenzen gibt es eine kostenlose Free Community Edition für zwei ESX-Hosts, allerdings mit einem deutlich eingeschränkten Funktionsumfang und ohne Anonymisierung. Einen sehr preisgünstigen Einstieg erlaubt die Starter-Edition für drei Hosts in einem vCenter und einem größeren Funktionsumfang. Unbegrenzte Hosts und vCenter mit vollem Funktionsumfang wie beschrieben bietet schließlich die Professional Edition. (jp)



PRTG Network Monitor Apps für alle!

Auch unterwegs Ihr
Netzwerk im Blick.



**HIER GEHT'S
ZU PRTG FOR
ANDROID –
KOSTENLOS!**



**LADEN SIE
KOSTENLOS
PRTG FOR iOS
HERUNTER!**



Testen Sie auch die
Vollversion von PRTG
30 Tage kostenlos!

www.paessler.de



Datensammelstelle

von Thomas Bär



Mit Splunk Enterprise 6 können Administratoren auch die Masse an unstrukturierten Maschinendaten überwachen, indizieren und visualisieren. Die Lösung macht es möglich, historisch gesammelte Informationen sowie Daten in Echtzeit, präzise und mit hoher Geschwindigkeit zu analysieren. Der Hersteller nennt diese Technik "Operational Intelligence", da die Datensammlung allein nicht das Wesen der Software beschreibt. Die Auswertung der End-to-End-Infrastruktur-Überwachung, das Erkennen von Beeinträchtigungen oder die Verhinderung von Dienstaussfällen ist letztendlich das Ziel, das der Administrator mit der Software erreichen soll. Die aktuelle Version 6 ist am deutschen Markt seit Herbst 2013 verfügbar.

Jedem Interessenten stellt Splunk einen kostenlosen Download der Software gegen Nennung einiger personenbezogener Informationen zur Verfügung. 60 Tage arbeitet die Software mit allen hier beschriebenen Enterprise-Funktionen und erlaubt ohne die Eingabe eines Lizenzschlüssels die Indizierung von maximal 500 MByte an Log-Informationen pro Tag. Nach den 60 Tagen reduziert sich der Leistungsumfang auf die "Free Edition" mit deutlichen Einschränkungen. Die Überwachung und Benachrichtigungsfunktionen sind in

Windows protokolliert alle relevanten System- und Anwendungsmeldungen mit der Ereignisanzeige. Proxy- und Web-Server schreiben ihre Protokolle im verbreiteten W3C-Format, Router und Switches senden Syslog-Meldungen. Kurzum: Es gibt eine sehr große Anzahl vollkommen verschiedener Protokollierungstechniken. Diese Datenmenge im Überblick zu behalten ist eine große Herausforderung, die das passende Werkzeug erfordert – beispielsweise Splunk Enterprise 6. Dieser Test beleuchtet, wie sich virtuelle und physische Infrastrukturen damit überwachen lassen.

der freien Variante deaktiviert, die Weitergabe an andere Management-Lösungen ist nicht mehr möglich, die Suchfunktion über verteilte Splunk-Instanzen entfällt und die gezielte Benutzersteuerung wird ebenfalls abgeschaltet. Bei der "Free"-Edition handelt es sich faktisch um eine lokale Einzelnutzersoftware, die dennoch ausreichend Potenzial bietet, sich als Administrator mit der Thematik der Logfile-Analyse genauer auseinanderzusetzen.

Wir installierten die Software, die es für die derzeit am Markt üblichen Betriebssysteme gibt, einmal auf einem Windows Server 2008 R2 x64 und in einer Umgebung unter Windows 7 x64. Die Installation des knapp 90 MByte großen MSI-

Pakets dauerte lediglich ein paar Minuten. Außer der Festlegung eines Zielverzeichnisses und der Eingabe eines Benutzerkontos für die Dienstzugriffe hat der Administrator nichts weiter zu tun als ein paar Augenblicke zu warten. Nach dem Setup bietet der Installer an, den Benutzer auf die Hauptseite im Browser zu leiten. Ohne aktiviertes Java-Script geht es jedoch erst einmal nicht weiter. Ansonsten arbeitete die Software sowohl unter dem Internet Explorer 11, Googles Chrome 31 und dem Firefox 26 ohne erkennbare Schwierigkeiten.

Freie Wahl der Datenquelle

Der Administrator wird von einer modernen Weboberfläche begrüßt und direkt

Bild 1: Die Einbindung von lokalen Datenquellen in Splunk ist in wenigen Minuten erledigt

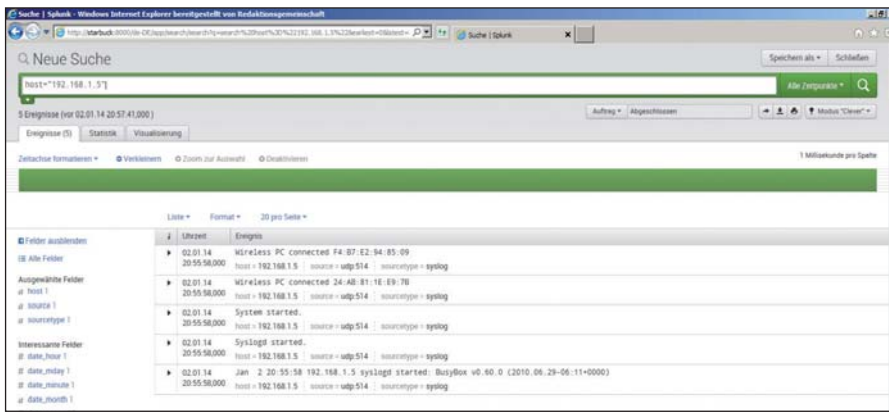


Bild 2: Die Suche nach Logmeldungen lässt sich per Textfeld durchführen

dazu ermuntert, das Standardpasswort durch ein eigenes zu ersetzen. Treffenderweise heißt das Vorab-Passwort auch "changeme". Im aktuellen Zustand verfügt die Software über noch keinerlei Kenntnis über die Umgebung und darüber, welche Daten es in der Anlage auszuwerten gibt. Dementsprechend folgten wir der Schaltfläche auf der rechten Seite mit der Aufschrift "Daten hinzufügen".

Wer zunächst nicht weiß, was er tun soll, kann jederzeit auf die vielen Hilfsquellen zurückgreifen. Splunk bietet eine große Anzahl von Hilfen wie etwa Video-Clips, Foren oder Dokumentationen. Sobald das Thema etwas spezieller wird, ist es mit der deutschen Sprachunterstützung allerdings vorbei und die Dokumentation wechselt, ohne vorherigen Hinweis, ins Englische. Da es sich um typisches IT-Englisch handelt, kann der versierte Administrator aber sehr gut mit den Anleitungen arbeiten.

Der Hersteller rühmt sich, faktisch jede Datenquelle als Grundlage für Suche, Auswertung oder Diagramme nutzen zu können. Entsprechend umfangreich ist die Auswahl von Datentypen und Datenquellen, nachdem der Benutzer auf die oben genannte Schaltfläche geklickt hat. Datentypen können Dateien oder Dateiverzeichnisse sein, Windows-Event-

logs, die Registry, Windows-Leistungsmetriken, Unix/Linux-Protokolle und Metriken oder Cisco-Geräteprotokolle. Weitere sind die Überwachungen der Dateiintegrität, OPSEC LEA von Checkpoint, IIS- oder Apache-Protokolle, WebSphere-Protokolle und Metriken sowie andere Dateitypen. Unter Datenquellen verstehen die Entwickler TCP- oder UDP-Ports, Verzeichnisse, Skripte, WMI, Registry-Wert-Erfassungen oder Windows-Ereignisanzeigen.

Einfach gelöst: Lokale Daten und Zugriffsrechte

Lokale Windows-Ereignisse oder Syslog-Aussendungen von aktiven Netzwerkkomponenten sind mithilfe des Assistenten in wenigen Augenblicken als Datenquelle integriert. Der Benutzer klickt im Auswahlmenü auf die gewünschten Datentypen oder Datenquellen, wählt den obersten Eintrag, beispielsweise "Windows-Ereignisprotokolle von diesem Splunk-Server erfassen", und klickt auf "Weiter". In Abhängigkeit zur vorherigen Auswahl erscheint ein weiteres Dialogfenster mit der Möglichkeit, die gewünschten Daten, beispielsweise Application, Security, Setup oder System der Ereignisprotokolle, auszuwählen.

Es empfiehlt sich, die verschiedenen eingerichteten Datenabfragen mit einem selbstsprechenden Namen zu versehen und im Zweifelsfall mehrere unterschiedliche Abfragen für mitunter identische Einsatzgebiete anzulegen – die Software kennt diesbezüglich keine Einschränkungen. Somit ist ein späteres Ein- und Ausschalten einer Datengewinnung im täglichen Umgang sehr einfach möglich.

Beispielsweise kann Splunk den Zugriff auf Registry-Werte als Event für ein Mitprotokollieren werten, aber auch das Festlegen, Erstellen, Löschen oder Umbenennen eines Registry-Eintrags.

Unter welchem Index Splunk die Daten künftig verarbeiten soll, wählt der Administrator ebenfalls per Mausklick aus. Standardmäßig legt die Software die Indizes "History", "Main", "Summary" und "Default" an. Je nach Umgebungsgröße kann es erforderlich sein, die Daten in verschiedene Index-Bereiche einzugliedern, was eine spätere Verarbeitung vereinfacht und für eine verbesserte Übersicht sorgt. Gleichzeitig kann der Administrator über die Indizes eine Zugriffskontrolle aufbauen, die in der Rollenverwaltung eine Zuordnung von Index und Zugriffsrechten, beispielsweise "Change Own Password", "Delete By Keyword" oder "Change Authentication", erlaubt. Für unsere Teststellung in den eher überschaubaren Umgebungen reichte uns der Eintrag "Default" aus.

Im Zweifelsfall ist Handarbeit gefragt

Um auf Daten zugreifen zu können, die sich außerhalb des lokalen Splunk-Servers befinden, muss der Administrator zunächst auf den betreffenden Maschinen den sogenannten "Splunk Universal Forwarder" installieren. Dieser wird, wie die Splunk-Software selbst, für eine große Anzahl unterschiedlicher Plattformen zum Download angeboten. Unter Windows sind dies beispielsweise Windows XP, 2003 und höher. Je nach Größe des zu verwaltenden Netzwerks kann der Administrator auch eine Deployment-Umgebung nutzen.

Die Einrichtung von Hand ist an sich ganz einfach: Die nur wenige MByte große Installationsdatei herunterladen und auf dem gewünschten Server starten. Wir wollten für den Test die Protokolle eines Microsoft Internet Information Servers (IIS) auf einem Windows Server 2003, der für das Intranet genutzt wird, einlesen. Während bei klassischen Abfragen, beispielsweise für Leistungsmetriken oder die Registry, der Installer seine Hilfe anbietet und die Daten automatisch abgreift, ist für das Auslesen der IIS-Daten ein wenig Handarbeit gefragt.

Die Software selbst arbeitet unter Microsoft Windows 2003 und höher (x86/x64), Linux ab Kernel 2.6, Solaris 10 für SPARC/x86/x64, Apple OS X 10.7 und höher, FreeBSD 6.x 32-Bit, AIX 6.1 und 7.1, HP-UNIX v11 v2/v3 für PA-RISC- und die Intel Itanium-Plattform.

Systemvoraussetzungen



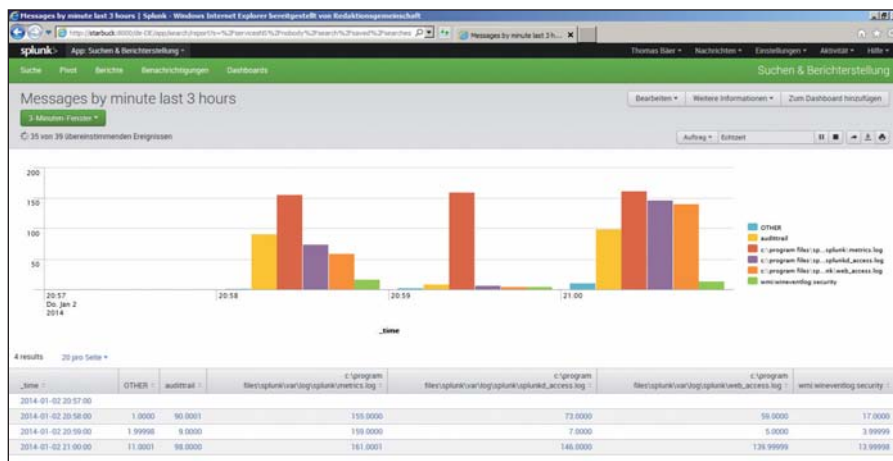


Bild 3: Das Datenmaterial stellt Splunk auch grafisch dar und erlaubt das Surfen durch die Daten

In der Ordnerstruktur des Forwarders entdeckten wir eine Datei mit der Bezeichnung *Inputs.conf*. In dieser mussten wir zwei Zeilen einfügen: einerseits das Zielverzeichnis des Logfile-Ordners und den “sourcetype=iis”. Bis zur vorherigen Version von Splunk mussten Administratoren noch einige Klimmzüge machen, um sich die sogenannten Multi-Line-Header-Protokolle zu erarbeiten, nun reicht der Sourcetype-Hinweis. Nach einem Neustart des Dienstes auf dem Webserver beginnt der Forwarder mit der Übermittlung der Daten auf den Splunk-Index-Server.

Virtuelle und physische Umgebungen im Blick

Es ist zwar zeitgemäß, kleine Programme als Apps zu bezeichnen. Im Fall von Splunk handelt es sich jedoch nicht um eigenständige Programme, die ein Benutzer ohne viel Aufwand auf ein Betriebssystem installiert, sondern um spezielle Auswertungs-Agenten für unterschiedliche Szenarien. Beispielsweise bietet der Hersteller allein 128 Apps im Segment für “Security and Compliance”, darunter für Cisco-Firewalls oder für Geräte von Palo Alto Networks. Aber auch weniger hochtechnische Bereiche wie Hadoop, Excel-Export, Sideview Web Analytics oder einen Datenbank-Connector bietet der Hersteller an. Ebenso Zusätze für das IT-Operations-Management unter Windows, Linux oder Unix.

Wir übergaben im Rahmen unseres Tests Informationen aus einer VMware vCenter-Umgebung an Splunk. Auf den ESX-Servern mussten wir hierzu eine kleine virtuelle Appliance im OVA-Format hoch-

laden. Auf dem vCenter-Server installierten wir den bereits erwähnten Forwarder-Client unter Windows sowie einige Dateien aus einem Zusatzpaket. Wer auch die vCenter-Daten selbst auswerten möchte, spielt einige weitere Dateien ein. Ist das vCenter in Form der virtuellen Appliance auf Linux-Basis aufgebaut, ist eine Auswertung mit Splunk nicht möglich. Die Installations- und Lösungsbeschreibung umfasst knapp 80 Seiten und erfordert eine größere Anzahl administrativer Schritte und ein vCenter ab Version 5.

Sind die Hürden der Einrichtung erst einmal überwunden, präsentiert sich die “VMware App” als eigenständiger Bereich, eine App in der Weboberfläche von Splunk, und erlaubt die Abfrage und Sammlung von VMware-bezogenen Daten. Was wahrlich beeindruckte, war die Geschwindigkeit, mit der die Software die spezifischen Daten anlieferte und dauerhaft speicherte – alles wirkte wie in Echtzeit.

Mächtige Analyse, Verdichtung und Visualisierung

Die verschiedenen Datenquellen lieferten nun die Informationen an den Splunk-Indexer und dieser erlaubte die weitere Verarbeitung und die Definition eigener Dashboards für verschiedene Unternehmensbereiche oder Systeme. Auf der rechten Seite zeigte ein Counter die Anzahl der bisher gesammelten Datenereignisse – in unserer Testumgebung mit VMware, Windows-Domäne, Windows-Server und Syslog-Meldungen von einem WLAN-Access-Point immerhin 2.840.318. Da die Informationen auch historischer Natur sind, reichte das früheste Ereignis drei Jahre zurück. Wer sich also um die Veränderung von Logging-Informationen in verschiedenen Zeiträumen interessiert, wird mit der Software seine wahre Freude haben. Aufgrund des engen Datenrasters blieb das “letzte Ereignis” in unserer Testumgebung stets auf “Jetzt”.

Die einfachste Form, mit der Software zu interagieren, ist die Eingabe eines Suchbegriffs in die obere Eingabeleiste im Browserfenster. Möchte der Administrator beispielsweise wissen, wann zuletzt eine Änderung in den Benutzerrechten vorgenommen wurde, so muss er einfach den gewünschten Benutzernamen eingeben. Wenige Augenblicke später erscheint eine Auflistung aller gefundenen Treffer der Volltextsuche über alle im Index gesammelten Logquellen. Die Information wird in dem generischen Format dargestellt, in dem sie von ihrem Quellsystem erzeugt wurde. Somit ist es wichtig, dass der Benutzer die Dar-

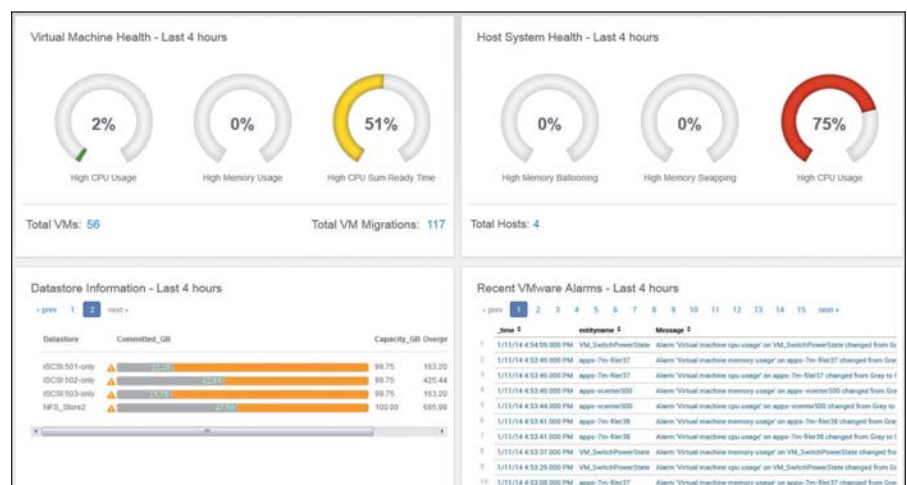


Bild 4: Die Zustandsdaten einer vCenter/ESX-Umgebung in Splunk sind grafisch übersichtlich aufbereitet

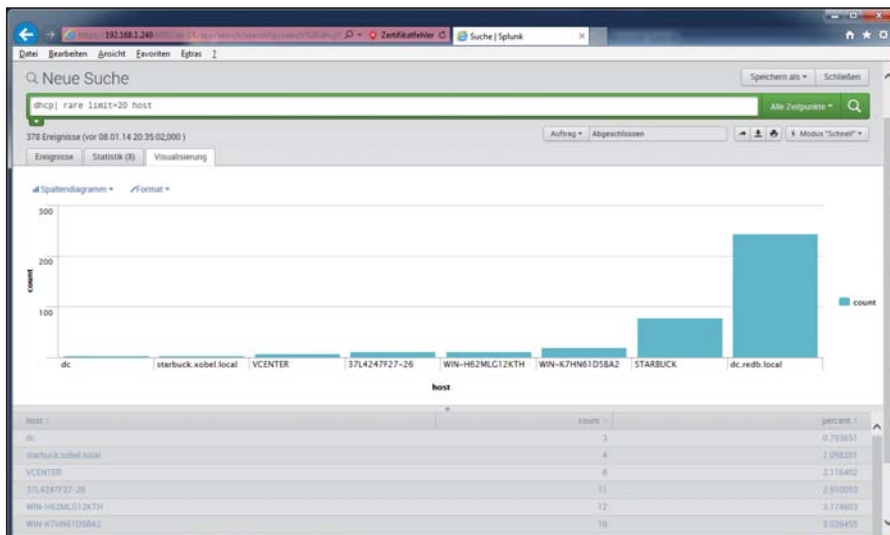


Bild 5: Die Auswertung der DHCP-Ereignisse vor einem bestimmten Datum

stellung auf die gewünschten Informationen begrenzen kann. Auf der linken Fensterseite zeigt die Software dazu einige interessante Felder – beispielsweise die Anzahl von Hosts, auf denen das Stichwort entdeckt wurde. Oberhalb der Ergebnisaufstellung entdeckt der Administrator wiederum eine Balkengrafik, die in Abhängigkeit zur Suche und deren Ergebnismenge eine Zeitachse einblendet. Führt der Benutzer mit dem Mauszeiger über die Balken, zeigt ein Tool-Tipp an, wie viele Ereignisse an dem Tag, in der Woche oder in dem Monat zu der Suche entdeckt wurden.

Die Eingrenzung des Zeitraums haben die Entwickler gut umgesetzt. Es gibt einerseits enge Zeitfenster, die sich dynamisch ändern, aber auch relative Zeiträume wie "Woche bis dato", Geschäftswochen, letztes Jahr oder letzte sieben Tage. Neben diesen in der Regel wichtigeren Zeiteingrenzungen existieren aber auch Datumsbereiche wie "Vor einem Datum" oder zwischen einem Anfangs- und Endzeitpunkt. Je nach Zeitraum kann es eine Weile dauern, bis Splunk die Daten zusammen hat – ob eine Auswertung bereits abgeschlossen ist oder noch verarbeitet wird, erkennt der Benutzer an der Statusanzeige neben den Befehlspiktogrammen. Sollte der Anwender einen dynamischen Zeitraum wählen, arbeitet die Abfrage so lange weiter, bis der Benutzer auf Pause klickt, da laufend weitere Daten eingehen und von Splunk visualisiert werden müssen.

Wie detailliert oder wie schnell die Software arbeitet, legt der Administrator über den "Modus" fest, den das Programm zu jedem Suchergebnis als Schaltfläche anzeigt. Zur Auswahl stehen neben "Ausführlich", bei dem die Software alle Informationen darstellt, auch die Modi "Schnell", bei dem Feldinterpretation unterbleibt, und "Clever". Letzterer versucht sich daran, die Daten schon im Vorfeld passend zu interpretieren. Alle Zusammenfassungen kann der Administrator als Dashboard oder Bericht speichern und grafisch mit Elementen aufwerten.

Die fertigen Auswertungen der "Apps" zeigen dem Benutzer, welches Potential in der Software und den Daten tatsächlich steckt. So liefert die VMware App unter "Performance and Capacity Planning" entsprechende Darstellungen, welche VMware-Hosts einen vom Anwender einzugebenden Prozentwert an CPU-Leistungen überschritten. Welche Maschine musste am meisten auslagern? Auf welchen Hosts war der Ballooning-Prozess zur Speicherrückgewinnung besonders aktiv? Das spannende an Splunk ist damit die Zusammenfassung aller Quellen an einer zentralen Stelle. Dank der Benachrichtigung kann die Software IT-Verantwortliche bei bestimmten Ereignissen per E-Mail kontaktieren.

Fazit

Es ist beeindruckend, was der Hersteller aus den verschiedensten Datenquellen für Informationen gewinnt, verdichtet und zentral bereitstellt. Dank der großen

Anzahl an zusätzlichen Apps scheint eine Erweiterung für die eigenen Bedürfnisse in fast allen Fällen problemlos möglich. Splunk ist weniger ein einziges Programm denn eine umfassende Infrastruktur für eine gezielte Datensammlung und Auswertung in zentralen und dezentralen Umgebungen. Die Bezeichnung "Operational Intelligence", die der Hersteller dafür selbst gewählt hat, ist somit absolut zutreffend. Alle technischen und organisatorischen Möglichkeiten der Plattform aufzulisten, wäre ein aussichtsloses Unterfangen. Dafür setzt die Plattform aber in vielen Fällen auch ein fundiertes Know-how über die eingesetzten Techniken voraus. (dr)

Produkt

Software zur zentralen Verarbeitung von Logdaten aus unterschiedlichsten Datenquellen und Plattformen.

Hersteller

Splunk
www.splunk.de

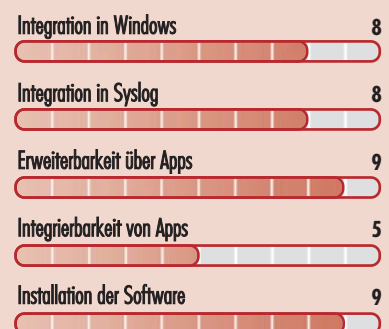
Preis

Die Lizenzkosten variieren je nach benötigtem Datenvolumen. Einschließlich VMware-App und 1 GByte Logdaten pro Tag kostet die Umgebung beispielsweise rund 15.000 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für Unternehmen, die über verschiedenste Plattformen und verteilte Standorte ein zentrales Logdaten-Management einführen möchten.

bedingt für Organisationen, die bereits eigene Techniken zur Zusammenführung der Logdaten im Einsatz haben.

nicht für kleine Firmen mit nur wenigen Servern.

Splunk Enterprise 6

Backup mit doppeltem Boden

von Jürgen Heyer



Schon seit einigen Jahren bieten zahlreiche Provider die Datensicherung im Internet als sogenanntes Online-Backup an. Viele Unternehmen wollen sich aber nicht allein auf ein Backup im Internet verlassen. Sie bevorzugen einen Stufenplan, indem sie Sicherungen zuerst auf einen großen Plattenspeicher im Haus durchführen, um diesen Datenbestand dann weiter an einen entfernten Ort zu replizieren. So lassen sich Aspekte wie Performance, Sicherheit und eine hohe Verfügbarkeit der Sicherungsdaten kombinieren.

Genau dies ermöglicht Veeam mit seiner Sicherungssoftware Backup&Replication v7 Cloud Edition. Dazu hat Veeam sein Werkzeug um die optionale Komponente Veeam Cloud Backup erweitert. Der prinzipielle Ablauf erweist sich als sehr übersichtlich: Der Administrator definiert innerhalb von B&R die notwendigen Speicherpools, erstellt die gewünschten Sicherungsjobs und legt die Daten in den Pools ab. Veeam Cloud Backup repliziert dann in eigenen Sicherungsjobs diese Pools auf einen Cloud-Storage und realisiert so die beschriebene Stufenlösung.

Bei der Datensicherung ist es überaus wichtig, das Backup entfernt vom Produktionssystem zu lagern, damit im Katastrophenfall nicht womöglich beides zerstört wird. In räumlich begrenzten Umgebungen ist dies aber schwierig. Als Alternative bietet sich die Nutzung von Cloud-Storage an.

Um diesen Speicher einfach anzubinden, hat Veeam sein Backup-Tool Backup&Replication v7 um eine optionale Cloud-Anbindung erweitert. Genau diese Komponente haben wir uns im Detail angesehen.

Unterschiedliche Lizenzmodelle

Bei der Recherche zum Test mussten wir feststellen, dass uns die Angaben auf der Veeam-Webseite zuerst etwas in die Irre führten, wie sich das normale Produkt B&R v7 sowie die Cloud Edition unterscheiden. Nach dem Herunterladen und Entpacken der rund 1,2 GByte großen ISO-Datei erkannten wir aber schnell, dass es sich um zwei eigenständige Produkte handelt, die zusammenarbeiten, sich vom Prinzip her aber auch eigenständig nutzen lassen. Das führt sogar soweit, dass Veeam für beide Versionen unterschiedliche Lizenzformen gewählt hat. Das herkömmliche B&R v7 ist nach wie vor anhand der Sockel der Hostsysteme, die die zu sichernden VMs beherbergen, einmalig zu erwerben (zuzüglich laufender Wartung). Als Cloud Edition dagegen ist die Software auf Mietbasis jährlich zu lizenzieren. Sie adressiert in erster Linie kleinere und mittlere Unternehmen.

Die Installation beider Produkte erwies sich im Test als problemlos und machte einen sehr ausgereiften Eindruck. Das Setup von B&R ist dabei deutlich umfangreicher. Angenehm ist, dass sämtliche benötigten Voraussetzungen wie Visual C++ 2010 und SQL Server 2008 R2 Express mitinstalliert werden. Auch prüft die Routine die Hardwarevoraussetzungen und weist beispielsweise darauf hin, dass mindestens zwei vCPUs bei der Installation in einer virtuellen Maschine empfohlen sind. Im Laufe der Einrichtung

werden Anmeldedaten abgefragt und zwei notwendige Verzeichnisse angelegt.

Das im Test verwendete Cloud Backup hatte die Version 3.5.2. Diese Installation dauerte nur wenige Sekunden und es war anzugeben, ob die Software für alle Benutzer oder nur den angemeldeten eingerichtet werden soll. Außerdem wurde der Installationspfad abgefragt.

Hilfreiche Assistenten

Beim ersten Aufruf von Cloud Backup startet ein Assistent in englischer Sprache, um entweder einen Sicherungsplan zu definieren oder ein Backup wiederherzustellen. Eine Umstellung der Oberfläche auf Deutsch ist möglich, dann wird Cloud Backup kurz geschlossen und startet entsprechend angepasst erneut. Als erste Aktion beim Anlegen eines Sicherungsplans fragt der Assistent den zu nutzenden Cloud-Storage ab. Dazu erscheint eine Liste von 25 Anbietern beziehungsweise Produkten. Darin enthalten sind auch die Optionen, auf ein eigenes Dateisystem oder via FTP sowie SFTP zu sichern. Dies hat uns insofern gefallen, da es so möglich ist, Cloud Backup optional in Verbindung

vSphere 5.x/4.x oder Infrastructure 3.5 (VI3.5) mit Hosts unter ESX(i) 3.x/4.x/5.x als Umgebung für zu sichernde virtuelle Maschinen.

Systemvoraussetzungen



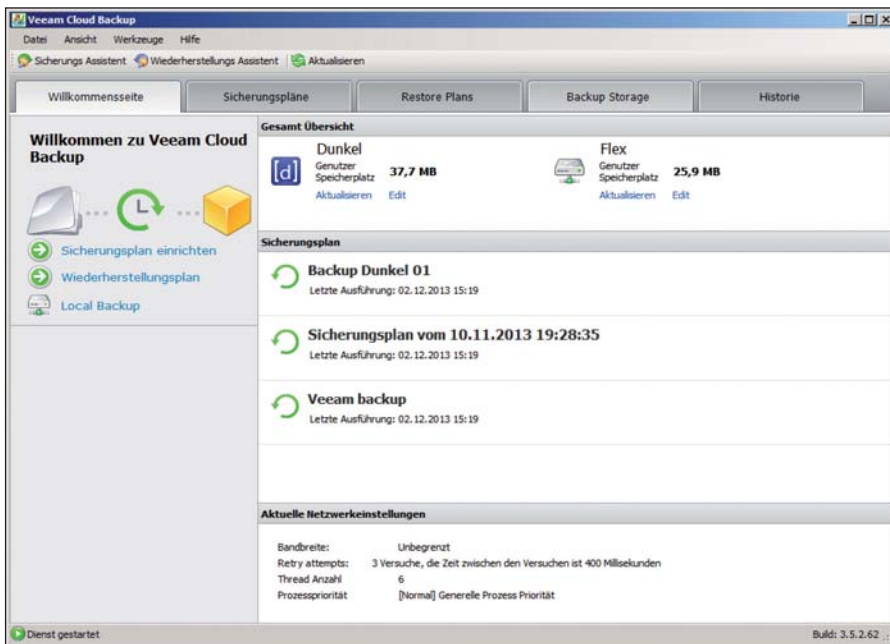


Bild 1: Cloud Backup listet in der Hauptansicht alle angelegten Sicherungspläne und verfügbaren Cloud-Storage-Zugänge auf

mit eigenen Sicherungszielen zu nutzen, statt zwingend auf einen externen Cloud-Storage zugreifen zu müssen.

Bei den unterstützten Anbietern ist alles dabei, was weltweit Rang und Namen hat: Amazon S3 und Glacier, Microsoft Azure, Openstack, Rackspace, Google Storage, HP Cloud, Clodo, Hylis, Scalify, Dunkel, Tiscali, Host Europe, DreamObjects, GreenCloud, Seeweb, Connectria, Walrus, Mezeo, Cloudian, Constant und Aruba Cloud. In der Praxis dürfte sich hierzulande der Fokus auf eine Handvoll an praktikablen Angeboten konzentrieren, da abgesehen von der diskussionsbehafteten Datenablage in den USA kaum ein deutsches Unternehmen Interesse haben dürfte, einen australischen oder russischen Provider zu wählen.

Erfreulich ist aber, dass auch bekannte deutsche Provider wie Dunkel und Host Europe dabei sind, die zusichern, dass die Daten in Deutschland verbleiben. Für unseren Test wandten wir uns an den Provider Dunkel GmbH aus Hattersheim bei Frankfurt, wo wir schnell und unbürokratisch einen Zugang erhielten. Dies eröffnete uns die Möglichkeit für einen möglichst praxisnahen Test. So wollten wir die gesicherten Daten etwa mit typischen Tools für den Cloud-Storage-Zugriff durchsuchen.

Was das Eintragen der Zugangsdaten für den Speicher in Cloud Backup anbetrifft, gestaltet sich dies bei den diversen Providern praktisch identisch. Das hängt unter anderem damit zusammen, dass der angebotene Cloud-Storage in der Regel kompatibel zu einem der verbreiteten, großen Angebote wie Amazon S3 oder Openstack ist. Komfortabel fanden wir es, dass in Cloud Backup die allgemeinen Parameter der Provider hinterlegt sind wie der Authentifizierungsdienst oder der Service Port. Auch sind entsprechende Links zu finden, um aus Cloud Backup heraus zu einem Provider zu springen, um dort einen Zugang zu beantragen. Weiterhin bietet es die Software an, den Zugang als virtuelles Laufwerk zu mounten, sofern der Provider dies unterstützt. Dazu wird der notwendige Treiber installiert.

Sofern Sicherungen von verschiedenen Computern im gleichen Bereich (Bucket) abgelegt werden, vereinfacht Cloud Backup das Wiederfinden dadurch, dass sich ein Backup-Präfix vorgeben lässt, weiterhin ist eine Absicherung der Verbindung per SSL möglich. Um die Kosten unter Kontrolle zu halten, lässt sich der GByte-Preis angeben und eine Obergrenze festlegen. Aus diesem Betrag kalkuliert das Programm dann sofort die maximale Kapazität. Es stellt übrigens kein Problem dar, auf verschiedene Speicherbereiche bei

unterschiedlichen Providern zu sichern, pro Sicherungsplan lässt sich ein anderes Ziel angeben.

Cloud Backup nur verschlüsselt sinnvoll

War der zu verwendende Cloud-Storage einmal festgelegt, folgten noch diverse Abfragen, die uns im Test zeigten, dass das Programm enorm viele Möglichkeiten und Optionen zur individuellen Anpassung beinhaltet. Dies beginnt mit einem Namen für den Sicherungsplan und der Möglichkeit, die Konfiguration mit auf dem Sicherungsspeicher abzulegen.

Dann unterscheidet Cloud Backup zwischen drei Sicherungsmodi, dem erweiterten, einfachen und Custom Modus, auf Wunsch in Verbindung mit VSS. Dabei kommt unseres Erachtens nur der erweiterte Modus für die Datenablage auf einem Cloud-Storage bei einem Provider in Frage, denn nur dieser unterstützt eine Verschlüsselung sowie eine Versionierung der Sicherungen. Eine Rücksicherung ist dann ausschließlich mit Cloud Backup möglich. Für eine Verschlüsselung beherrscht die Software 18 verschiedene Modi. Dies sind AES, DES, 3DES, RC2 mit unterschiedlichen Schlüssellängen zwischen 40 und 256 Bit. Standardmäßig wird nur der Dateiinhalt verschlüsselt, optional aber auch die Datei- und Ordernamen.

Die Verschlüsselung erfolgt auf Job-Basis, es lässt sich also jederzeit eine andere verwenden. Die Credentials können im Job mit gespeichert werden und sind an das

Veeam Backup&Replication beinhaltet im aktuellen Release deutlich mehr Funktionen als die, die wir bei unserem Test von Version 6 im April-Heft 2012 im Detail vorgestellt haben. So wurde unter anderem eine **WAN-Beschleunigung** integriert, um eine externe Speicherung zu beschleunigen. Dazu verwendet B&R Caching, Fingerprints für Datenblöcke variabler Länge und eine TCP/IP-Protokolloptimierung. Für diese Beschleunigung sind keine zusätzlichen Backup-Jobs, Kopierskripte oder eine speicherbasierte Replikierung erforderlich. Auch zusätzliche Agenten oder Änderungen am Netzwerk sind nicht nötig. Neu sind weiterhin **Hochleistungs-Backups von Storage-Snapshots** sowie eine **native Bandunterstützung**, während in der Vergangenheit nur Sicherungen auf Plattensystemen möglich waren.

Neuerungen in B&R v7



Profil des Backup-Servers gebunden. Das hat den Vorteil, dass sie bei späteren Wiederherstellungen und beim Durchsuchen des Backup-Speichers nicht jedes Mal erneut einzugeben sind. Besteht der Bedarf, das Profil des Servers auf ein anderes System zu exportieren, lassen sich die Credentials herausnehmen. Bei Amazon S3 ist es zudem möglich, alternativ über einen Request Header eine "Server Side Encryption" zu veranlassen. Zusätzlich komprimiert Cloud Backup die Daten optional.

Der einfache und der Custom Modus unterstützen keine Verschlüsselung und keine Versionierung. Sie unterscheiden sich darin, dass sich beim Custom Modus ein Ordner für die Datenablage vorgeben lässt und das Programm keine weiteren Verzeichnisse erzeugt. Beim einfachen Modus kümmert sich Cloud Backup um die notwendigen Verzeichnisse. Aufgrund der nicht vorhandenen Verschlüsselung ist es bei beiden Modi problemlos möglich, mit anderen Client-Tools wie etwa dem Cloudberry Explorer auf die Daten zugreifen. Letztendlich repliziert die Software die Quelle unverändert ins Ziel. Dies ergibt unserer Meinung nach nur dann Sinn, wenn ein Unternehmen keinen externen Cloud-Storage verwendet, sondern die Möglichkeit nutzt, die Daten zusätzlich auf eine eigene Netzfreigabe oder per FTP sowie SFTP zu kopieren und sie das Unternehmen dabei nicht verlassen.

Umfassendes Regelwerk

Bei der Auswahl der Sicherungsquelle listet Cloud Backup alle lokalen sowie gemappten Laufwerke auf, bei Bedarf lässt sich eine Netzwerkfreigabe hinzufügen. Auch steht ein Dateifilter zur Verfügung, um sich auf bestimmte Dateitypen zu beschränken oder welche auszuklammern. Weiterhin legt Cloud Backup optional leere Ordner mit an oder schließt Verzeichnisse aus. Dateien lassen sich anhand des Änderungsdatums sichern und auf eine maximale Größe eingrenzen. Auf Wunsch werden Systemdateien und versteckte Ordner ausgeklammert.

Retention leicht gemacht

Der erweiterte Modus erlaubt es, Löschoptionen für die Versionen vorzugeben,

also eine Retention-Regel festzulegen. Hierbei gibt es die Möglichkeit, allgemeingültige Regeln für die gesamte Anwendung zu nutzen oder Plan-spezifische Vorgaben zu machen. Gelöscht wird wahlweise aufgrund des Versionsalters oder anhand der Anzahl der vorliegenden Versionen, wobei Cloud Backup dies erfreulicherweise für jede Datei einzeln prüft. Für am Quellort gelöschte Dateien lässt sich schließlich vorgeben, nach wie vielen Tagen diese auch in der Sicherung entfernt werden.

Als sehr umfangreich erweisen sich die Zeitplanungsoptionen. Eine Sicherung kann manuell, einmalig oder wiederkehrend (täglich, wöchentlich, monatlich, Tag des Monats) um eine feste Zeit oder in Abständen erfolgen. Ein Administrator kann beispielsweise festlegen, dass in der Zeit zwischen 8 und 17 Uhr alle 15 Minuten gesichert wird. Darüber hinaus kennt das Programm ein Real-Time Backup, was einer CDP (Continuous Data Protection) entspricht: Sobald neue Dateien oder Ordner im Quellbereich erscheinen, werden diese ins Ziel kopiert. Weiterhin lässt sich ein Plan nach einer gewissen Laufzeit stoppen und ausgelassene Sicherungen werden auf Wunsch sofort nach Systemstart nachgeholt.

Start- und Stoppbefehle möglich

Falls es notwendig ist, in Verbindung mit einer Sicherung Start- und Stoppbefehle abzusetzen, ist dies bei Cloud Backup möglich. Benachrichtigungen über eine Sicherung kann das Programm per SMTP-Mail verschicken oder ins Windows Ereignis-Log schreiben. Letzteres ist vor allem dann sinnvoll, wenn im Unternehmen ein Monitoring-Werkzeug eingesetzt wird, das dieses Log überwacht und auswertet.

Unter dem Reiter "Sicherungspläne" sind alle angelegten aufgelistet. Der Administrator kann diese jederzeit editieren, löschen, sich die Historie anzeigen lassen oder einen Plan klonen, falls er einen ähnlichen erstellen möchte. So spart er sich die komplette Erfassung. In der Kopfzeile eines jeden Plans signalisiert eine farbige Unterlegung den aktuellen Status, außerdem ist die nächste geplante Ausführung angegeben, der Administrator kann einen Plan aber auch jederzeit starten.

Grundsätzlich arbeitet Cloud Backup im erweiterten Modus inkrementell. Bei der Feststellung der Unterschiede orientiert sich das Programm am Änderungsdatum. Insgesamt hat uns die Vielzahl der Möglichkeiten zur Definition eines Sicherungsplans beeindruckt.

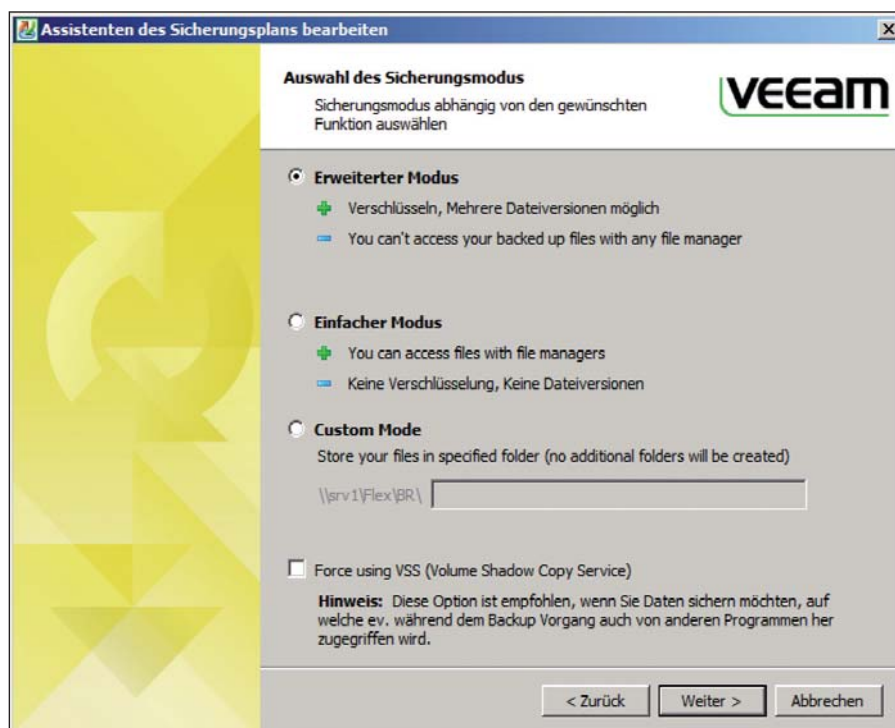


Bild 2: Dem Administrator stehen drei Modi zum Anlegen von Sicherungsplänen zur Verfügung. Die wichtigsten Vor- und Nachteile sind in der Maske aufgeführt.

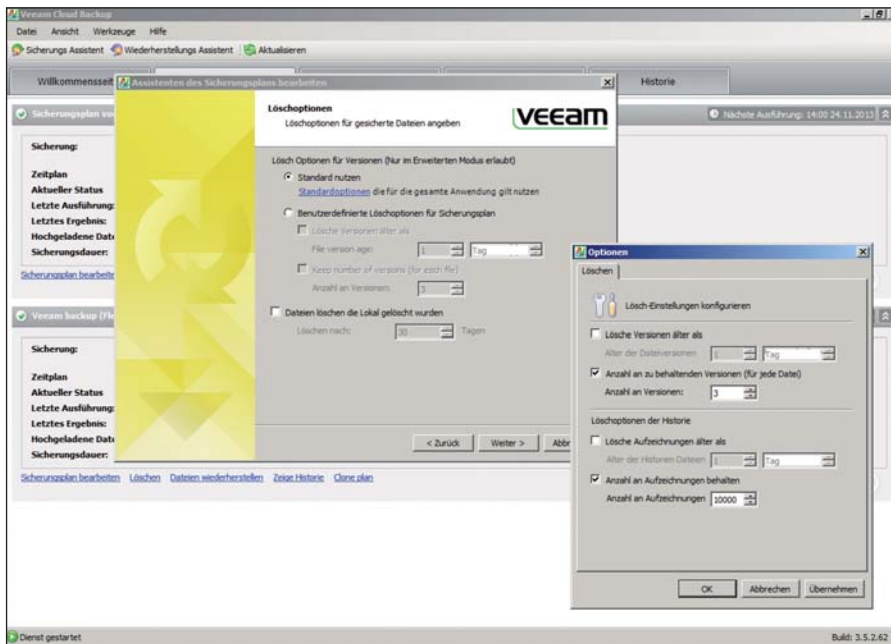


Bild 3: Die Aufbewahrungsregeln lassen sich in Cloud Backup sehr detailliert festlegen

Einfache Datenwiederherstellung

Ähnlich komfortabel wie die Erstellung eines Sicherungsplans präsentiert sich auch die Wiederherstellung. Dabei ist es möglich, eine einmalige Wiederherstellung durchzuführen oder die Angaben als Si-

cherungsplan abzuspeichern. Der Assistent fragt dann den Wiederherstellungstyp ab. Dies kann die letzte Version sein oder der Bestand zu einem bestimmten Zeitpunkt. Als dritte Möglichkeit lassen sich die Dateien einzeln auswählen. Dann möchte

die Software das Ziel wissen, denn sie sichert wahlweise an den ursprünglichen Ort zurück oder an ein anderes Ziel. Optional werden vorhandene Dateien überschrieben, ebenfalls optional nur neuere Dateien als zum Zeitpunkt der Sicherung.

Sofern es sich um verschlüsselte Dateien handelt, lässt sich das verwendete Passwort angeben, wobei dieses wie oben erwähnt nicht in jedem Fall erforderlich ist, da Cloud Backup die Credentials auch im Profil des Backup-Servers ablegt. Beim Zeitplan gibt es ähnliche Möglichkeiten wie bei der Sicherung, selbst wenn regelmäßige Wiederherstellungen normalerweise relativ selten der Fall sein dürften.

War es erforderlich, Daten auf einem anderen System wiederherzustellen, so klappte auch dies im Test reibungslos. Der Administrator muss nur dort einen Wiederherstellungsplan starten und den Account zum benötigten Cloud-Storage anlegen. Sofern er sich zum gleichen Bucket verbindet, erkennt dies Cloud Backup, weist darauf hin, dass dort bereits Sicherungsdaten liegen

Was guckst Du mich an!?
Frag Deinen IT-Dienstleister!



migRaven

für IT-Dienstleister

Saubere NTFS Berechtigungen
ohne Consulting-Exzesse

- zufriedene Kunden durch niedrige Kosten & schnelle Ergebnisse
- saubere und nachhaltige Ergebnisse nach Microsoft Best Practices
- für Fileserver-Migrationen aller Art, auch von Novell zu Microsoft

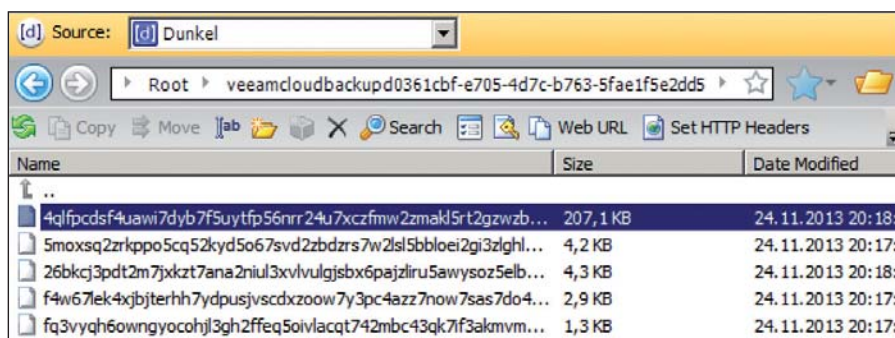


Bild 4: Beim Blick mit einem Explorer-Tool auf die verschlüsselten Daten auf dem Cloud-Storage sind außer dem Dateidatum keine Informationen herauslesbar, die Rückschlüsse erlauben

und fragt dann, ob etwas wiederherzustellen ist. Im Falle verschlüsselter Daten will die Routine das Passwort wissen. Anschließend startet die Wiederherstellung.

Ad-hoc Zugriff auf Backuppeicher

Neben den Sicherungs- und Wiederherstellungsplänen ist es möglich, direkt auf den Sicherungsspeicher zuzugreifen. Hierzu ist nur der entsprechende Cloud-Storage-Account auszuwählen, um dann innerhalb von Cloud Backup den Speicher wie im Explorer zu durchsuchen. Verschiedene Versionen der Dateien werden in einem eigenen Fenster aufgelistet, sodass hier Zugriff auf jede Version besteht und der Administrator sich schnell ein Bild über den Sicherungsstand machen kann. Das mittels rechter Maustaste aufrufbare Kontextmenü erlaubt es, Dateien oder ganze Ordner schnell wiederherzustellen, wobei jedes Mal der Wiederherstellungsassistent gestartet wird. Auch lassen sich hier die Cloud-Informationen aktualisieren, da es sein könnte, dass parallel etwas geändert wird und die Anzeige nicht mehr korrekt ist. Die Datei- und Ordneransicht ist beim Durchsuchen innerhalb von Cloud Backup lesbar, auch wenn die Inhalte verschlüsselt gesichert wurden. Nur bei einer Wiederherstellung will die Software das Passwort wissen.

Parallel zur Explorer-Funktion in Cloud Backup haben wir den Cloud-Storage auch mit einem eigenständigen Werkzeug, dem Cloudberry Explorer, durchsucht. Schnell konnten wir erkennen, dass die Verschlüsselung Wirkung zeigt, denn wir sahen nur eine unstrukturierte, flache Liste mit nicht lesbaren Bezeichnungen. Die Verwendung eines derartigen Tools ergibt also nur Sinn, wenn ohne Verschlüsselung gearbeitet wird.

Automatisierung per CLI

Neben der GUI liefert Veeam eine Kommandozeilenschnittstelle in Form einer EXE-Datei mit. Im Handbuch sind die Optionen und Schalter eingehend beschrieben. Die CLI kann bestehende Sicherungspläne nutzen. Sie lassen sich mit einem Befehl auflisten und anhand einer ID adressieren. Wenn es übrigens darum geht, einen individuellen Zeitplan zu erstellen, so stehen in der CLI nur beschränkte Möglichkeiten zur Verfügung. Veeam empfiehlt, in so einem Fall den Windows Scheduler zu verwenden. Ergänzend zur CLI hat Veeam damit begonnen, eine C#-API zur Verfügung zu stellen. Deren Funktionsumfang ist allerdings noch eingeschränkt, sie wird aber laut Hersteller kontinuierlich anhand von Kundenanforderungen erweitert.

Fazit

Mit der Backup&Replication v7 Cloud Edition verbindet Veeam die übliche Datensicherung innerhalb eines Unternehmens mit der bequemen Möglichkeit, diese Daten auf einen Cloud-Storage zu replizieren. Vor allem für kleinere und mittlere Unternehmen, die nicht selbst über mehrere Lokationen zur sicheren Aufbewahrung ihrer Daten verfügen, ist dieser Zusatz äußerst interessant. Bei ihnen kann der Cloud-Storage bei einem der renommierten Provider den zweiten Standort ersetzen. Sehr gut gefallen haben uns die vielen in Cloud Backup hinterlegten Provider, die eine Anbindung zu einem Kinderspiel machen. Dabei sind nur die Anmeldedaten zu hinterlegen, alles andere liefert Cloud Backup zu. Bezüglich der Datensicherheit ist positiv zu erwähnen, dass Cloud Backup diverse Verschlüsselungsarten mit einer Tiefe bis zu 256

Bit unterstützt, wenn auch AES als einzig zeitgemäßer Algorithmus Sinn ergibt. Indem die Daten bereits auf Unternehmensseite verschlüsselt und bei einem Restore auch nur dort wieder entschlüsselt werden, ist die bestmögliche Sicherheit gegeben. Es ist somit nicht notwendig, dem Provider Informationen zur Verschlüsselung zu geben. (In)

Produkt

Programm zur Datensicherung und Wiederherstellung in virtuellen Umgebungen samt Auslagerung auf einen Cloud-Storage.

Hersteller

Veeam
www.veeam.com

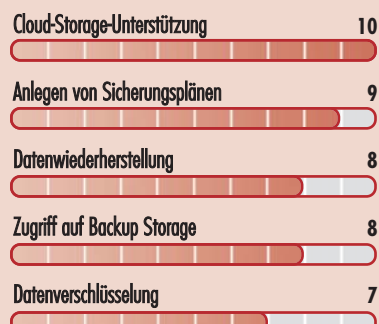
Preis

Die B&R v7 Cloud Edition ist pro CPU-Sockel auf jährlicher Abonnementbasis zu lizenzieren. Die Preise liegen je nach Version zwischen 395 und 1.010 Euro inklusive Wartung.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für kleinere und mittlere Unternehmen, die über keinen geeigneten zweiten Standort verfügen, ihre Sicherungsdaten aber räumlich getrennt lagern wollen.

bedingt für Unternehmen, die über einen geeigneten zweiten Standort verfügen und ihre Sicherungsdaten dort lagern möchten. Dann bietet sich die Freigabe- oder FTP-Funktion von Cloud Backup an, es gibt hier aber auch andere Möglichkeiten zur Replizierung.

nicht für Unternehmen, die ausreichend Möglichkeiten zur Datensicherung im eigenen Netz haben oder die ihre Daten aus Sicherheitsgründen ungeachtet jeder Verschlüsselung nicht in die Cloud auslagern dürfen.

**Veeam Backup & Replication v7
Cloud Edition**

Kompetentes Schnupperabo sucht neugierige Administratoren

Sie wissen, wie man Systeme
und Netzwerke am Laufen hält.
Und das Magazin IT-Administrator weiß,
wie es Sie dabei perfekt unterstützt:

mit praxisnahen Workshops, aktuellen
Produkttests und nützlichen Tipps und Tricks
für den beruflichen Alltag.

Damit Sie sich Zeit,
Nerven und Kosten sparen.

**Teamwork in Bestform.
Überzeugen Sie sich selbst!**



6

**Monate
lesen**

3

**Monate
bezahlen**

www.it-administrator.de



Heinemann Verlag
Im Dialog mit Spezialisten.

Verlag / Herausgeber

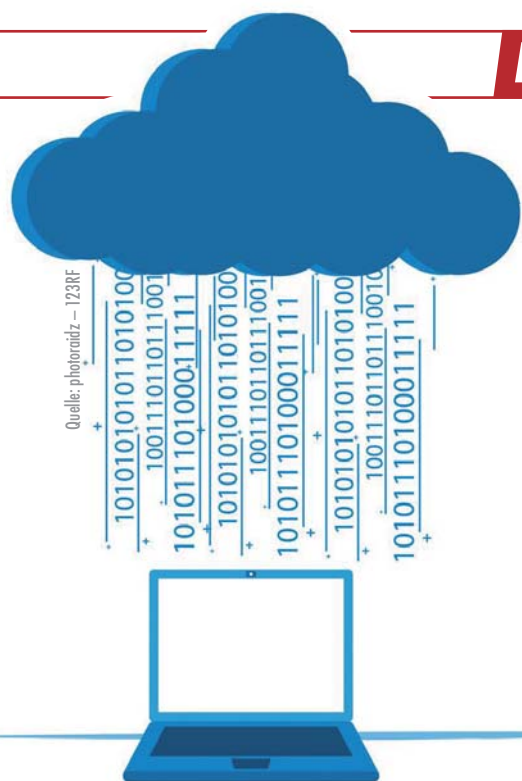
Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München

Tel: 0049-89-4445408-0
Fax: 0049-89-4445408-99
info@heinemann-verlag.de

Vertrieb, Abo- und Leserservice IT-Administrator

vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville

Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de



Im Test: Cloud Management mit Witsbits

Fern und doch ganz nah

von Sandro Lucifora

Die Virtualisierung hält unaufhaltsam Einzug in die IT. Während die virtuellen Umgebungen Flexibilität bieten, steigt auch der Verwaltungsaufwand. Witsbits geht dabei gegenüber etablierten Anbietern wie VMware und Microsoft einen anderen Weg und bietet das VM-Management als Software-as-a-Service an. Welche Vorteile dieses Konzept bietet und wie technisch ausgereift es ist, hat sich IT-Administrator im Test angeschaut.

Virtuelle Systeme bestehen immer aus mehreren Komponenten: dem Hypervisor, dem Server-Betriebssystem, auf dem die virtuellen Maschinen laufen, und einer Management-Konsole zur Administration des Systems. Regulär gibt es dazu fast immer eine Desktopanwendung zur Verwaltung. Andere Systeme, wie zum Beispiel Collax V-Cube, setzen auf ein lokales, webbasiertes Management, das auf dem Hostsystem läuft. Witsbits entwickelte eine webbasierte Management-Konsole, die als Software-as-a-Service im Internet läuft und standortunabhängig eine beliebige Anzahl von Hosts verwaltet. Diese basieren auf KVM (Kernel Based Virtual Machine) von Red Hat.

Standortunabhängiges Management

Um das Witsbits-System zu betreiben, genügte in unserem Test ein einfacher Desktop-Rechner mit Webbrowser. Zum Erstellen des Bootmediums für den Server benötigten wir zusätzlich einen CD-Brenner oder USB-Anschluss. Als Host-Server – dem physikalischen Computer, auf dem wir später die virtuellen Maschinen einrichteten – dienten uns ein Server in unseren Räumen sowie ein gemietetes Gerät, das in einem entfernten Rechenzentrum stand. Mit Witsbits

spielt es keine Rolle, wo die Server stehen. Sie müssen lediglich per Internet erreichbar sein. Als Mindestkonfiguration sind ein 64 Bit-Prozessor (Intel VT oder AMD-V), ein CD-Laufwerk oder USB-Port vorgegeben sowie mindestens 1 GByte RAM und 20 GByte Festplattenplatz auf einer lokalen Festplatte oder einem NFS-Speicher.

Die Installationsdatei für den Host erhielten wir über unseren zuvor angelegten Witsbits-Account. Zur Auswahl standen zwei Nutzermodelle: Kostenlos und Premium. Die kostenlose Version ist auf fünf physikalische CPUs begrenzt. Die Premium-Variante gibt es in Paketen von jeweils zehn physikalischen CPUs. Gut gefallen hat uns, dass Witsbits jederzeit ein Upgrade von der kostenlosen auf die Premium-Version ermöglicht, ohne das System neu installieren zu müssen. So wächst die Management-Umgebung bei Bedarf mit. Die Anzahl der installierbaren Host-Server ist dabei unlimitiert.

Nach dem Login luden wir die Installations-ISO-Datei herunter. Zuvor gaben wir an, ob der Host seine IP-Adresse später über einen DHCP-Server erhält oder die Netzwerkinformationen manuell, noch vor dem Download, eingetragen werden.

Der Vorteil der DHCP-Variante ist, dass wir mit einer Installationsdatei mehrere Host-Systeme installieren konnten. Bei der festen IP-Adressvergabe benötigten wir für jeden zu installierenden Server eine eigene Installationsdatei, da Witsbits diese schon vorab mit den Netzwerkangaben konfiguriert. Nach den Eingaben erhielten wir den Downloadlink für die 726 MByte große, mit dem Witsbits Cloud-Key angereicherte ISO-Datei.

Das Installationsmedium erstellten wir mit dem Programm "Image Writer for Windows" als bootfähigen USB-Stick. Alternativ ließ sich auch eine CD brennen oder die ISO-Datei in der Remote Access Card des Servers als virtuelle CD einbinden. Nach dem Booten startete der Installationsprozess automatisch und dauerte nur wenige Minuten. Ein Eingriff unsererseits war nicht notwendig, sodass sich der Host-Server auch ohne weitere KVM- und Linux-Kenntnisse installieren lässt. Anhand des Cloud-Keys verband sich der Host automatisch mit der Witsbits Management-Plattform, von der aus wir unsere private Cloud im eigenen Rechenzentrum über die zentrale und Web-basierte Oberfläche verwalteten. Der physikalische Server war nun vorbereitet, um virtuelle Maschinen zu starten.

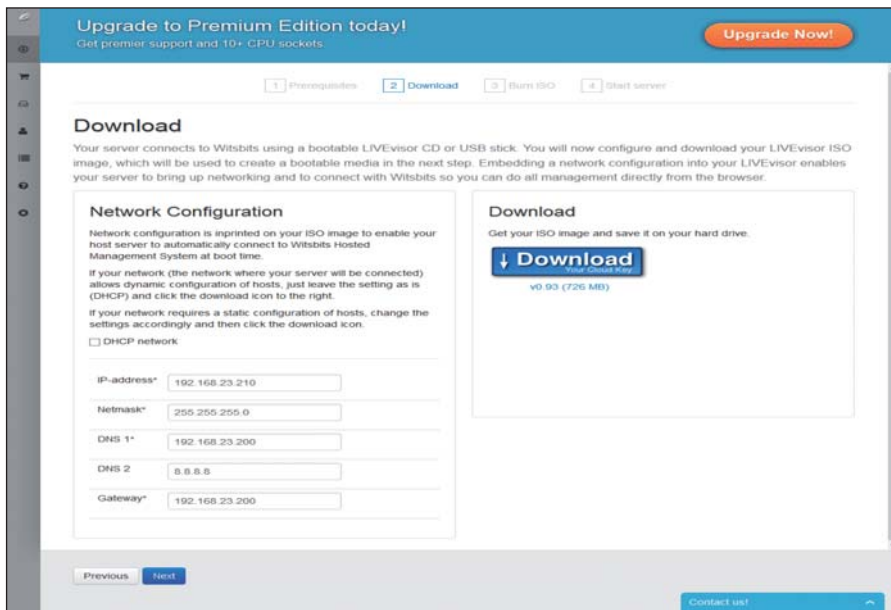


Bild 1: Für den Download der Installationsdatei legen wir die Netzwerkconfiguration fest

Vorbereitete Images aus dem Store

Über die Management-Konsole initialisierten wir als Erstes die physikalischen Festplatten als Speicherbereich für die virtuellen Maschinen. Neben den im Server eingebauten Speichermedien fügten wir zusätzlich einen iSCSI-Speicherort zu. Alternativ stand uns auch das Protokoll NFS für den Zugriff auf einen externen Storage zur Verfügung.

Die erste virtuelle Maschine installierten wir mittels Template aus dem Store. Dabei handelt es sich um eine Liste bereits installierter und frei verfügbarer virtueller Maschinen. Aus Lizenzgründen befand sich im Store jegliche Art vorinstallierter und betriebsbereiter Linux-Derivate als reine Server-Installationen oder bereits betriebsbereit als LAMP-Server. Die Windows-VMs stellt Witsbits als Testversionen und in verschiedenen Sprachen und Ausführungen als Server und Workstation bereit. Diese dienen lediglich dem schnellen Aufbau einer Testumgebung und nicht als Grundlage für ein Produktivsystem.

Der Host Server benötigt einen 64 Bit x86-Prozessor mit Intel VT oder AMD-V, CD/DVD-ROM-Laufwerk oder USB Anschluss, mindestens 1 GByte Hauptspeicher sowie 20 GByte Platz auf einer lokalen Festplatte oder einem NFS-Speicher.

Systemvoraussetzungen



Wir klickten auf den Start-Button hinter der zu installierenden VM, in unserem Fall nahmen wir einen Ubuntu 13 LAMP-Server, legten neben dem Namen und dem Root-Passwort auch die Eckdaten wie Arbeitsspeicher, Tastaturlayout und Festplattengröße fest und gaben an, auf welchem unserer physikalischen Server die Installation erfolgen sollte. Danach startete das System die Datenübertragung auf unseren Server. Nach der Fertigstellung, die je nach Bandbreite mal länger dauert oder schneller geht, stand uns der LAMP-Server zur Verfügung.

ISO-Datei nur per HTTP

Einen Windows-Server installierten wir von der regulären Microsoft-ISO-Datei. Dazu legten wir im privaten Teil des Stores ein neues Template an, vergaben einen aussagekräftigen Namen und stellten den Arbeitsspeicher, die CPUs und den Festplattenplatz ein. Auf die ISO-Datei griff Witsbits jedoch nur über HTTP zu. Von Vorteil ist dies, sofern die Installationsdatei – die neben einer ISO-Datei zum Beispiel auch eine VMDK-Datei sein kann – nur online zur Verfügung steht. In unserem Fall störte diese Einschränkung jedoch, da wir unsere ISO-Datei eigentlich über eine Netzwerkfreigabe erreichen mussten.

Es ergibt wenig Sinn, eine 4 GByte große Datei ins Internet zu übertragen, um sie dann zur Installation wieder herun-

terzuladen. Schließlich ist die DSL-Leitung der Flaschenhals und zögert den Prozess unnötig heraus. Daher benötigten wir in unserem lokalen Netz einen Webserver für die Bereitstellung der Installationsdateien. Wir bedienten uns des zuvor über den Store installierten Ubuntu LAMP-Servers, ergänzten die Installation um Samba, mappten das Netzwerklaufwerk, konfigurierten den Apache-Server um und griffen dann über HTTP auf die ISO-Datei zu. Ein umständlicher Zwischenschritt. Die URL zur ISO-Datei gaben wir dann im Template an.

Die Einrichtung starteten wir wieder durch den Start-Button neben unserem Template und wählten einen Host als Ziel für die Installation aus. Die Angaben zum Speicher, den CPUs und der Festplattengröße nahmen wir erneut vor, da der Wizard diese nicht aus unseren Voreinstellungen übernahm. Witsbits legte die VM auf dem Virtualisierungs-Server an und bootete die als virtuelle CD eingebundene Microsoft-ISO mit der Setup-Prozedur von Windows.

Im Gegensatz zu VMware, wo Easy Install die Installation von Windows komplett automatisiert, mussten wir nun die einzelnen Setup-Schritte wie bei einer regulären Installation durchklicken. Dazu benötigten wir einen virtuellen Bildschirm mit Zugriff auf die VM. Da Windows zu dem Zeitpunkt noch nicht installiert und somit RDP nicht verfügbar war, griffen wir über einen VNC-Client auf die VM zu. Die IP-Adressen und den Port entnahmen wir der Detailanzeige der VM in der Weboberfläche von Witsbits. Dass Witsbits VNC als Remote-Protokoll wählte, hat sicher etwas damit zu tun, dass KVM den VNC-Server kostenlos beinhaltet. Jedoch konterkariert dies den Ansatz, den Server aus dem Internet sicher erreichbar zu machen, da nach dem Sicherheitsaspekt die Nutzung von VNC ausschließlich in geschlossenen Netzwerken oder nur über ein VPN zu empfehlen ist. Deshalb hätten wir uns hier eine – gerne auch kostenpflichtige – Alternative für den Remote-Zugriff gewünscht, die ein sicheres Übertragungsprotokoll verwendet.

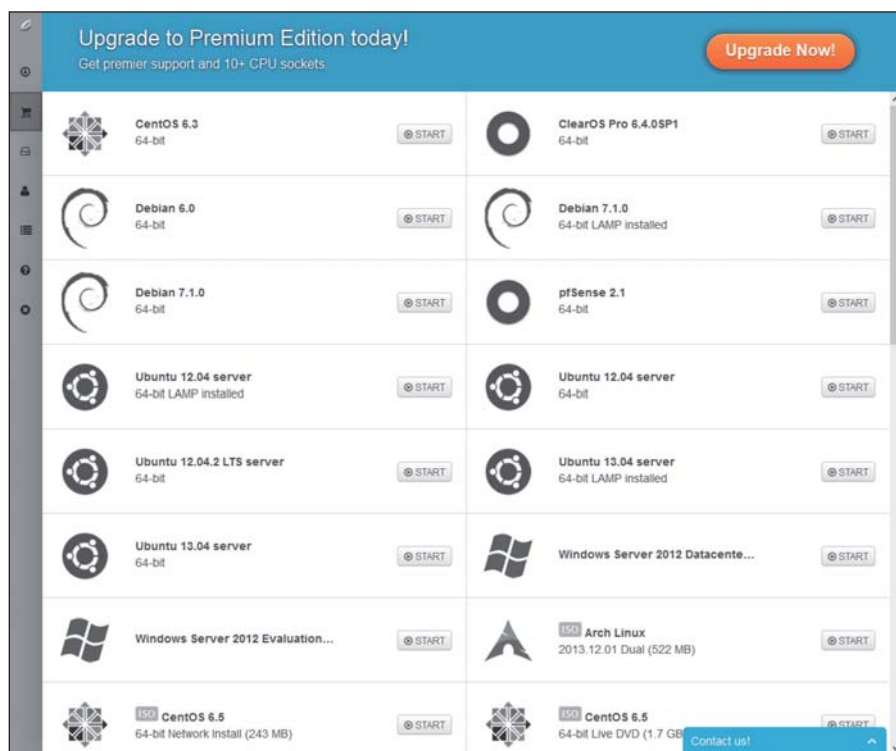


Bild 2: Der Store liefert eine Vielzahl fertig installierter virtueller Maschinen

Über die Remote-Konsole erhielten wir Zugang zur virtuellen Maschine und klickten uns durch das Windows-Setup. Dabei stellten wir fest, dass Windows Server 2012 R2 keine SCSI-Treiber für die virtuellen Festplatten von Witsbits beziehungsweise KVM bereitstellte. Um diese nachzuladen, wählten wir im Dialog der Festplattenauswahl, die bisher keine Festplatte anzeigte, den Link "Treiber laden" aus und navigierten in der Dateiauswahl auf das zusätzliche Witsbits-CD-Laufwerk, das alle notwendigen Windows-Treiber enthielt. Dabei hat uns gefallen, dass das System dieses von vornherein mountet und wir darauf immer Zugriff hatten. So wählten wir den mitgelieferten "RedHat VirtIO SCSI controller" aus, nach dessen Installation die virtuelle Festplatte zur Auswahl für die weitere Windows-Installation erschien. Nach der sonst unspektakulären Windows-Installation zeigte uns der Gerätemanager noch einen fehlenden Treiber für die Netzwerkkarte an. Diesen luden wir ebenfalls über die eingebundene Witsbits-Treiber-CD nach, wonach der Windows Server 2012 als virtuelle Maschine in Betrieb war.

Management-Konsole mit Verbesserungspotenzial

Nach der Installation der virtuellen Maschine verwalteten wir diese über die

Witsbits Management-Konsole. Neben den obligatorischen Funktionen wie Start, Stopp und Neustart erstellten wir auch Snapshots. Dabei führte die Konsole den Befehl, wie auch alle anderen, nicht direkt aus, sondern legte ihn in eine Warteschlange für den Server ab. Dieser holte sich seine Aufgaben im Zwei-Sekunden-Takt ab und führte sie lokal aus. Sobald der Server die Aufgabe begann, sahen wir dies anhand einer Fortschrittsanzeige auf der Konsole. Der so erzeugte Snapshot war lediglich eine Kopie der aktuellen Version der VM und entsprechend als zusätzliche virtuelle Maschine in der Liste zu sehen. Die Kopie benötigte daher genauso viel Speicherplatz wie das Original, was schnell den verfügbaren Plattenplatz sprengen kann.

Ganz ähnlich arbeitete die vorhandene Backup-Funktion: Sie legte eine Kopie der VM an, übertrug diese jedoch in das Witsbits-Rechenzentrum, aus dem wir sie jederzeit zurückspielen konnten. Was uns während des Backup-Prozesses fehlte, war zum einen eine Anzeige, wie groß die zu übertragende Datenmenge war, und eine Funktion, um das Backup abubrechen beziehungsweise zeitlich zu planen. Denn die Übertragung aus dem lokalen Netz auf einen Online-

Speicher dauert mitunter sehr lange und belastet die Bandbreite stark. Verlor etwa der Host die Internetverbindung während des Backupprozesses, hing die Anzeige in der Webkonsole und wir konnten keinerlei Eingaben für den Host und die VM tätigen. Nach der wieder vorhandenen Internet-Verbindung führte das System das Backup stur weiter. Besonders ärgerlich war die magere Upload-Geschwindigkeit, die sich bei gerade mal 250 bis 280 KBit/s einpendelte, obwohl die Bandbreite unseres Anschlusses volle 10 MBit/s zum Upload zur Verfügung stellte.

Weiterhin bot uns die Konsole die Option, die VM auf einen anderen Witsbits-Server zu migrieren oder sie auf unseren lokalen Computer herunterzuladen. Der Import einer bestehenden VM erfolgt auf Basis von VMDK-Dateien, die wir als Template im Store anlegten und auf dem Host einrichteten. Auch hier ließ Witsbits wieder nur HTTP als Übertragungsprotokoll zu.

Failover per NAS

Um das integrierte Failover zwischen zwei Host-Systemen zu nutzen, mussten beide Witsbits-Hosts Zugriff auf dasselbe NAS-System haben. So konfigurierten wir den NAS-Server als Speicherbereich für beide physikalischen Server. Dabei hat uns besonders gestört, dass das Einbinden des NAS nur über die Eingabe des Linux-nfs-Kommandos erfolgte. Somit mussten wir die komplette Linux-Befehlszeile eingeben, inklusive aller Parameter, um auf den Netzwerkspeicher zuzugreifen. Wir hätten uns hier einen anwenderfreundlichen Dialog gewünscht, über den sich diese Funktion konfigurieren lässt. Den Ausfall eines Hosts simulierten wir, indem wir die Netzwerkverbindung unterbrachen. In dem Moment schalteten wir über die Webkonsole auf den Fail-over-Server um, sodass dieser den Speicherbereich des ausgefallenen Servers übernahm und die sich darin befindlichen VMs ausführte.

Eingeschränkte Hardware-Konfiguration

Spartanisch zeigte sich die weitere Hardware-Konfiguration der VM. Neben den von den Templates bekannten Angaben

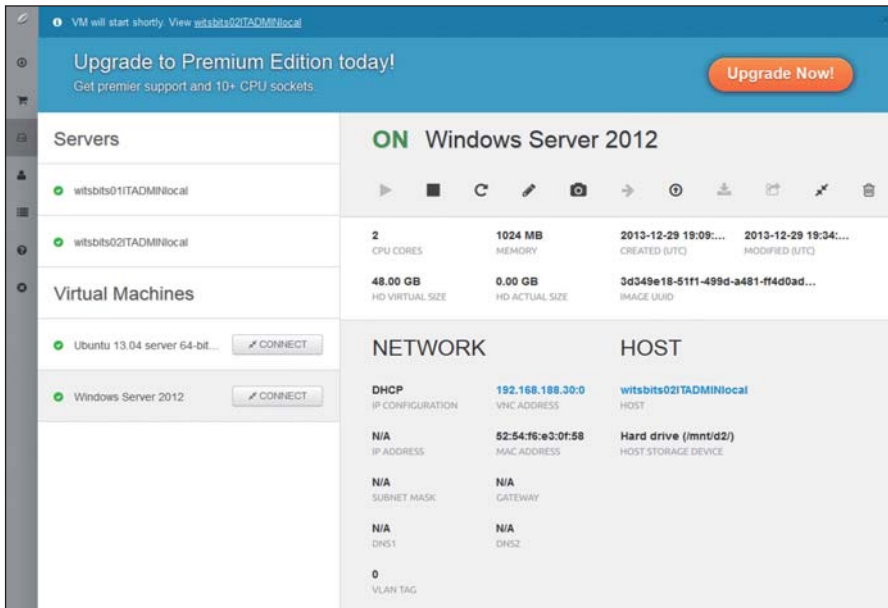


Bild 3: Die Verwaltungsoberfläche der virtuellen Maschine zeigt die wichtigsten Rahmendaten an

zum Hauptspeicher der CPU, der Festplatte und des VLAN ließen sich keine ergänzenden Einstellungen in Bezug auf die virtuelle Hardware vornehmen. Die Konfiguration für die Peripherie am physikalischen USB-Port oder eingesteckten Erweiterungskarten, das PCI-Passthrough, fehlten gänzlich.

Während des Tests verlor Witsbits einige Male die Verbindung zum Server beziehungsweise zeigte Statusmeldungen an, die nicht mit dem Zustand der Server korrespondierten. So war ein Server noch als aktiv gelistet, obwohl wir diesen schon längst über die Kommandozeile heruntergefahren hatten. Die Anzeige synchronisierte sich erst wieder, nachdem wir über die Konsole nochmal den Befehl gegeben hatten, den Server herunterzufahren. Dazu mussten wir den Server wieder starten, damit er den in der Warteschlange liegenden Befehl abarbeiten konnte.

Auch der Dialog vor dem Start einer VM war zeitweise durcheinander beziehungsweise verlor zuvor getätigte Einstellungen. So mussten wir immer wieder das Tastaturlayout auf Deutsch einstellen, bevor wir eine VM starteten, da diese Einstellung grundsätzlich auf Englisch stand. Verlor der Host die Verbindung zur Konsole, zeigte diese den Host und alle darauf befindlichen VMs zudem mit dem Status offline an, auch nachdem der Server wieder erreichbar war. Im Test hatten wir ein-

mal diesen Fall, wonach es unmöglich war, mit der Konsole eine Verbindung zum Server aufzubauen. Im Nachhinein stellte sich heraus, dass ein Prozess im Browser festhing und erst nach dem Neustart wieder alles richtig anzeigte. Hier haben die Entwickler noch viel Potenzial nach oben, um gerade bei außergewöhnlichen Ereignissen das Webmanagement fehlerfrei am Laufen zu halten.

Fazit

Beim Hypervisor setzt Witsbits auf bewährte Technologie und bedient sich des Red Hat KVM-Servers. Die Idee der webbasierten und von überall erreichbaren Management-Konsole ist vom Grundgedanken her gut, doch zeigte sich im Test, dass die Umsetzung noch viel Potenzial besitzt. Neben immer wieder auftretenden Anzeige-Problemen, die teilweise nichts mit den realen Status der Server zu tun hatten, fehlten uns vor allem weitergehende Konfigurationsmöglichkeiten der virtuellen Hardware. Handelt es sich bei den Gastsystemen um mehr als nur um einen Web- oder Fileserver, ist die Einstellung für CPU, Speicher und Festplatte schlicht zu wenig. Auch die Einschränkung, auf Installations-Medien nur über HTTP zuzugreifen, obwohl Witsbits beziehungsweise der Server auch mit NFS und iSCSI umgehen können, grenzt den sinnvollen Einsatzbereich der Host-Systeme auf Internetdienste ein.

Ebenfalls etwas unglücklich ist der Konso-lenzugriff auf die virtuellen Gäste über VNC, was wiederum im Internet für Sicherheitsprobleme sorgt. Eine Notfallkonsole für die Verwaltung bei einer fehlenden Internet-Verbindung stellt Witsbits derzeit nicht zur Verfügung. Aufgrund der zwingenden Internetverbindung zur Verwaltung der physikalischen Server und des schlechten Handlings, falls diese ungeplant ausfällt, sehen wir Witsbits noch nicht als Verwaltungskonsole für Inhouse-Systeme. Laut Hersteller ist zumindest geplant, in Zukunft ein Out-of-Band-Management zu implementieren. Für das Management virtueller Systeme mit Internet-Diensten auf Basis von zur Verfügung stehenden virtuellen Maschinen ist Witsbits in jedem Fall einen Blick wert. (dr)

Produkt

Cloud-basiertes Management für virtuelle Maschinen.

Hersteller

Witsbits Inc.
www.witsbits.com

Preis

Bei Verwaltung von bis zu fünf physikalischen CPUs kostenlos, danach je zehn physikalische CPUs 199 Euro im Monat.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Hardware-Konfiguration VM	3
Einbindung Storage für VM	6
Zuverlässigkeit der Webkonsole	4
Ausfallsicherheit	5
Installation des Hosts	6

Dieses Produkt eignet sich

optimal für die Verwaltung im Internet stehender Host-Systeme.

teilweise für die Virtualisierung von Windows-Systemen.

nicht für das Management umfangreicher Inhouse-Virtualisierungs-Strukturen mit hohen Sicherheitsanforderungen.

Witsbits



Im Test: Ocster Backup Business 8

Der Preis ist heiß

von Jürgen Heyer

Dass eine vor allem auf kleinere und mittelständische Unternehmen zugeschnittene Datensicherung für Desktops und Server nicht teuer sein muss, möchte die neue Business-Version 8 von Ocster Backup beweisen. Durch eine Reduzierung auf die wesentlichen Funktionen ist die Software leicht bedienbar. Zudem besteht die Möglichkeit zur schnellen Wiederherstellung im Katastrophenfall. Doch ganz ohne Abstriche ist die günstige Backup-Software nicht zu haben. IT-Administrator hat sich Stärken und Schwächen angesehen.

Eine auch auf Server zugeschnittene, leistungsfähige Backup-Software für 50 Euro pro Lizenz, gibt es das? Das war unsere erste Reaktion bei der Ankündigung der Version 8 von Ocster Backup und wir beschlossen, die mit den am meisten Funktionen ausgestattete Businessvariante eingehend zu prüfen. Und um es gleich vorweg zu nehmen: Ja, es lassen sich Server sichern, auf spezielle Agenten für Applikationen wie Exchange oder SQL-Datenbanken muss allerdings verzichtet werden. Auch bei der Sicherung dynamischer Datenträger gibt es Einschränkungen und der Administrator muss bei mehreren Servern jeden separat administrieren. Wenn das akzeptabel ist, dann lässt sich mit Ocster Backup gut und vor allem günstig arbeiten.

Schnelle Einrichtung

Die Installation von Ocster Backup Business gestaltet sich einfach. Das Setup prüft im Internet, ob eine neuere Version verfügbar ist, und lädt diese auf Wunsch für die Installation gleich herunter. Nach abschließender Eingabe des Freischaltcodes erscheint die Benutzeroberfläche, die im Wesentlichen aus sechs großen Schaltflächen besteht. Bezüglich sonstiger Einstellungen ist kaum etwas zu beachten. Neben dem Ändern der Sprache lässt sich das automatische Pausieren ein- und ausschalten. Ist die Funktion aktiviert, hält Ocster Backup die Sicherung an, wenn die Auslastung des Systems zu hoch ist,

und arbeitet dann weiter, wenn sie wieder gesunken ist. Welche Kriterien hierbei zur Anwendung kommen, ist allerdings nicht nachzulesen, außerdem lassen sich diese nicht verändern. Eine dritte im Programm noch enthaltene Funktion zur Nutzung von externem Speicher bei Ocster kann nicht mehr genutzt werden, da Ocster dieses Angebot mittlerweile eingestellt hat. Abgesehen davon lassen sich zu sichernde Daten auf lokalen Festplatten, USB-Sticks sowie auf Netzwerklaufwerken speichern.

Wahlweise Vollsicherung oder inkrementell

Durch die Reduzierung der GUI auf letztendlich sechs Schaltflächen gestaltet sich die Bedienung sehr übersichtlich. Um eine Sicherung durchzuführen, ist zuerst ein Backup-Plan zu erstellen, wozu ein Assistent startet. Dieser unterscheidet im ersten Schritt zwischen der Sicherung des ganzen Computers beziehungsweise der darauf befindlichen Partitionen sowie einer Auswahl von Ordnern und Dateien. Bei der ersten Variante erfolgt die Sicherung blockorientiert auf Imagebasis und es ist später möglich, aus dieser Sicherung komplette Partitionen oder auch ein vollständiges System von Grund auf wiederherzustellen, also einen Bare Metal Restore durchzuführen.

Der Assistent bietet nun an, einen Sicherungsplan neu zu erstellen oder einen be-

stehenden zu importieren, was bei der Einrichtung mehrerer Aufträge Zeit spart. Dabei ist eine Bezeichnung zu vergeben und der Backup-Ort festzulegen. Zur leichteren Auswahl schlägt Ocster Backup die lokalen sowie gemappten Laufwerke vor oder ermöglicht durch die Auswahl "Anderer Ort" eine individuelle Vorgabe. Weiterhin wird ein Ordner abgefragt. Es ist sinnvoll, unterschiedliche Systeme jeweils in eigene Ordner zu sichern, da jede Sicherung wiederum aus einer Ordnerstruktur mit mehreren Dateien besteht.

Sofern es sich bei dem Ziel um eine Netzwerkfreigabe handelt, fragt Ocster Backup entsprechende Anmeldeparameter ab, was sich auch gleich auf eine korrekte Eingabe prüfen lässt. Der Hintergrund ist, dass die Sicherung durchaus unter einem anderen Benutzer erfolgen kann als dem, der gerade angemeldet ist, und die Sicherung auch bei nicht angemeldetem Benutzer läuft. Gerade bei Servern ist hier auf eine genaue Organisation zu achten, damit Sie die Sicherungen auch wiederfinden. Sie müssen nämlich wissen, welchen Benutzer Sie für ein Backup verwendet haben, um die Berichte einsehen zu können. Vor allem soll-

Windows 8, 7, Vista, XP, Windows Server 2012, 2008/2003. Dazu 512 MByte RAM und rund 125 MByte freien Festplattenplatz.

Systemvoraussetzungen





Bild 1: Der Einstieg beginnt bei Ocster Backup über sechs große Schaltflächen zur Auswahl der gewünschten Aktion

ten Sie für die Sicherungen nicht unterschiedliche Benutzer verwenden, da sonst schnell die Gefahr besteht, den Überblick zu verlieren. Diesbezüglich orientiert sich Ocster Backup in erster Linie am Bedarf für Arbeitsplätze, wo durchaus mehrere Benutzer jeweils ihre eigenen Daten sichern können, was aber bei einem Server wenig sinnvoll ist.

Anschließend fragt die Software die zu sichernden Laufwerke ab. Sofern sich auf einer Festplatte interne oder versteckte Bootinformationen befinden, werden diese automatisch mitgesichert. Auf Wunsch komprimiert und/oder verschlüsselt die Software die Daten, wobei zu planen ist, wie später gegebenenfalls auf die Dateien zugegriffen werden soll. Ocster Backup nutzt das StandardVMDK-Format, was ein Öffnen der Sicherungsdateien mit anderen Werkzeugen erlaubt. Dann ist allerdings die Kompatibilität größer, wenn unkomprimiert gesichert wird. Beispielsweise lassen sich die VMDK-Dateien mit virtuellen Maschinen von VMware und Virtualdisk öffnen und auslesen. Nur das Booten als VM ist nicht möglich, auch nicht bei komplett gesicherten Bootpartitionen.

Eine weitere Rubrik ist die Vorgabe der Sicherungsart sowie die Aufbewahrung. Hierzu geben Sie an, wie viele Versionen Sie aufbewahren wollen. Weiterhin können Sie wahlweise endlos-inkrementell oder

wechselweise voll und inkrementell sichern. Im ersten Fall wird beim ersten Mal eine Vollsicherung durchgeführt, anschließend nur noch inkrementelle. Im zweiten Fall lässt sich vorgeben, nach wie vielen inkrementellen Sicherungen ein volles Backup erfolgen soll. Die Software sichert umgekehrt inkrementell (Reverse incremental), was bedeutet, dass immer aufgrund der zu sichernden Daten als letzte Sicherung eine synthetische Vollsicherung erzeugt wird und die älteren Sicherungen als Inkremente vorliegen. Der Vorteil besteht darin, dass die Wiederherstellung mit der letzten Sicherung am schnellsten geht und die älteren Backups problemlos gelöscht werden können.

Bei der zweiten Variante, der Datei- und Ordner-orientierten Sicherung, beherrscht Ocster Backup wiederum zwei Vorgehensweisen. Beim sogenannten Standard-Format speichert es die Daten in Archiven, was eine Versionierung sowie eine Komprimierung und Verschlüsselung erlaubt. Weiterhin werden die Zugriffsrechte sowie Hard-Links und Sym-Links mitgesichert. Die zweite Art besteht in einer einfachen Datei-Kopie in entsprechende Unterverzeichnisse ohne Zugriffsrechte, Verschlüsselung und Komprimierung. Während die erste Vorgehensweise die Daten deutlich besser organisiert ablegt, eine Wiederherstellung aber nur über das Backupprogramm möglich ist, reicht im

zweiten Fall für den Zugriff auch der Windows Explorer, da die Dateien letztendlich einfach kopiert wurden.

Flexible Zeitplanung

Die Zeitplanung erlaubt das manuelle Sichern täglich zu einer bestimmten Zeit oder wöchentlich. Falls diese Standardmöglichkeiten nicht reichen, lassen sich unter dem Punkt "Erweitert" auch mehrere Einträge für täglich, wöchentlich und monatlich individuell hinterlegen. Dabei erlaubt das Programm die Vorgabe von Sprüngen, um beispielsweise jeden dritten Tag oder jede zweite Woche zu sichern. Wir empfanden die Optionen insgesamt als geeignet, um auch außergewöhnliche Sicherungsfolgen zu hinterlegen. Bezüglich verpasster Sicherungen besteht die Möglichkeit, diese bei nächster Gelegenheit nachzuholen oder zu überspringen. Für permanent laufende Server sicher weniger sinnvoll ist die Option, den Computer nach der Sicherung herunterzufahren. Auch der Umgang mit dem Schlafmodus orientiert sich mehr an den Anforderungen an einen Arbeitsplatz.

Bei der Aufbewahrung der Sicherungsberichte schlägt die Software eine Zahl vor, die sich an der Menge der aufzubewahrenden Sicherungen orientiert. Das Programm verschickt die Berichte auf Wunsch per E-Mail. Dies kann über einen Mailserver von Ocster geschehen. Der Zugang erfolgt dabei über das Konto beim Hersteller, das jeder lizenzierte Anwender erhält. Mit der aktuellen Version kann auch der eigene SMTP-Server verwendet werden. Als umständlich empfanden wir, dass die Daten des SMTP-Servers bei jedem Job erneut einzutragen sind und nicht einmalig global im Programm hinterlegt werden können.

Sofern es erforderlich ist, vor oder nach einem Sicherungsjob Befehle abzusetzen, um Verbindungen aufzubauen, zu trennen oder Dienste zu stoppen und zu starten, können hierzu die entsprechenden Befehle als Skript hinterlegt werden. Dazu stehen diverse Umgebungsvariablen zur Verfügung, die die Programmierung erleichtern. Gerade bei der Sicherung von Servern sehen wir diese Befehle als recht wichtig an, da die Software zwar offene Dateien sichert, dies aber nicht für die

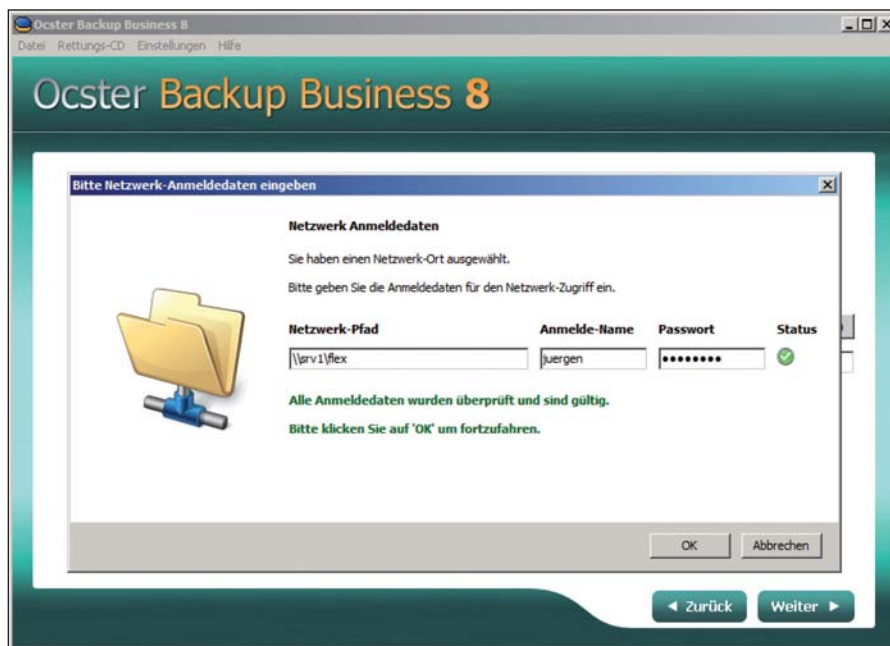


Bild 2: Für eine Sicherung auf eine Freigabe fragt Ocster Backup entsprechende Anmeldedaten ab, um den Zugriff unabhängig vom Benutzer zu machen, der für den lokalen Zugriff verwendet wird

konsistente Sicherung beispielsweise einer Datenbank ausreicht und hierfür auch keine Agenten zur Verfügung stehen. Das passende Skript setzt eine Datenbank offline und erzeugt vorher einen Dump, um so konsistente Daten zu gewährleisten.

Sind alle Informationen für den Sicherungsauftrag eingegeben, zeigt Ocster Backup diese in einer Übersicht an und fragt abschließend, ob zusätzlich sofort gesichert werden soll oder gemäß des hinterlegten Zeitplans. Hinsichtlich der Anzahl der Sicherungspläne gibt es keine Beschränkungen, hier lassen sich problemlos mehrere anlegen. Natürlich sollten hinsichtlich der Sicherungszeiten Überlappungen vermieden werden.

Sicherungsumfang mit Licht und Schatten

Wie bereits erwähnt, gibt es keine Agenten beispielsweise für die Sicherung von Exchange oder Datenbanken. Offene Dateien sichert das Programm aber mit, ebenso die Kontakte von Outlook und Lesezeichen der Browser Internet Explorer, Google Chrome und Mozilla Firefox. Speziell im Serverumfeld ist zu beachten, dass die Software keine dynamischen Datenträger als vollständige Laufwerke blockorientiert sichert. Hier erhält der Anwender sofort einen Hinweis, wenn er solch einen Datenträger auswählt. Das sehen wir als gewich-

tige Einschränkung, da dynamische Datenträger im Serverumfeld eine große Rolle spielen – gerade wenn es um das Spannen über mehrere Partitionen oder das Spiegeln geht. Erfreulicherweise ist ein Workaround möglich, indem statt der blockorientierten Vollsicherung des Laufwerks die Funktion zum Sichern von Ordnern und Dateien genutzt wird. Da es hierbei möglich ist, beim Sicherungsumfang ab dem Root eines Laufwerks zu beginnen, ist auf diese Weise auch relativ einfach eine Komplettsicherung möglich. Nur werden nicht die Laufwerksinformationen selbst mitgespeichert. Auf Nachfrage bei Ocster erfuhren wir, dass eine umfassendere Unterstützung dynamischer Datenträger geplant ist und in einem der nächsten kostenlosen Updates enthalten sein soll.

Im Test haben wir verschiedene Sicherungsjobs einige Male laufen lassen und uns anschließend die Sicherungsverzeichnisse angesehen. Ocster Backup legt hier eine individuelle Verzeichnisstruktur an, wobei bei der Sicherung ganzer Festplatten im Verzeichnisnamen der genaue Zeitpunkt mit enthalten ist. So lassen sich die einzelnen Sicherungen jederzeit leicht identifizieren.

Schnelle Rettung mit Ubuntu

Bei der Wiederherstellung von Daten erlaubt Ocster Backup zwei prinzipielle Vorgehensweisen: die Rücksicherung auf

Ordner- und Dateibasis sowie die Wiederherstellung ganzer Laufwerke. Im letzten Fall wird ein komplettes Laufwerk auf den ausgewählten Sicherungsstand zurückgesetzt. Beim Restore einzelner Ordner und Dateien arbeitet die Software mit einer Mount-Funktion, indem sie einen Sicherungsstand als virtuelles Laufwerk zur Verfügung stellt. Die benötigten Daten können dann von diesem virtuellen Laufwerk per Drag and Drop wieder auf die aktiven Laufwerke zurückkopiert werden. Änderungen am Inhalt eines virtuellen Laufwerks sind verständlicherweise nicht möglich, Dateien lassen sich jedoch öffnen. Gut gefallen hat uns im Test, dass wir auch mehrere Sicherungen parallel jeweils als virtuelle Laufwerke mounten konnten. Das erlaubt eine schnellere Suche und einen Vergleich, wenn der Administrator beispielsweise nicht mehr genau weiß, zu welchem Zeitpunkt eine wiederherzustellende Datei noch vorhanden war.

Eine weitere Stärke von Ocster Backup ist die Möglichkeit, die Laufwerke inklusive der Bootpartition mit einfachen Mitteln auf ein nagelneues System aufzuspielen, also einen Bare Metal Restore durchzuführen. Dazu bedient sich das Programm einer Boot-CD, die auf Ubuntu basiert. Nach dem Booten eines Systems mit dieser CD beziehungsweise der ISO-Datei startet ein vorbereitetes Ubuntu mit einem darauf eingerichteten Ocster Rescue System, um sich zu einer Netzwerkfreigabe zu verbinden oder auf einen USB-Stick zuzugreifen. Dann kann sich der Administrator mit der von Ocster Backup erstellten Verzeichnisstruktur verbinden, worauf das Tool die verfügbaren Sicherungen als Auswahl anbietet.

Es lassen sich wahlweise das komplette System oder einzelne Laufwerke wiederherstellen, indem der Backupinhalt auf die angezeigten Laufwerke gezogen wird. Eventuell dort vorhandene alte Daten werden hierbei überschrieben. Ist die Rücksicherung abgeschlossen, wird das System wieder ohne CD gebootet und es sollte von der wiederhergestellten Installation starten. Im Test funktionierte dies problemlos und zügig, so dass wir unseren Server in wenigen Minuten wieder in Betrieb hatten.

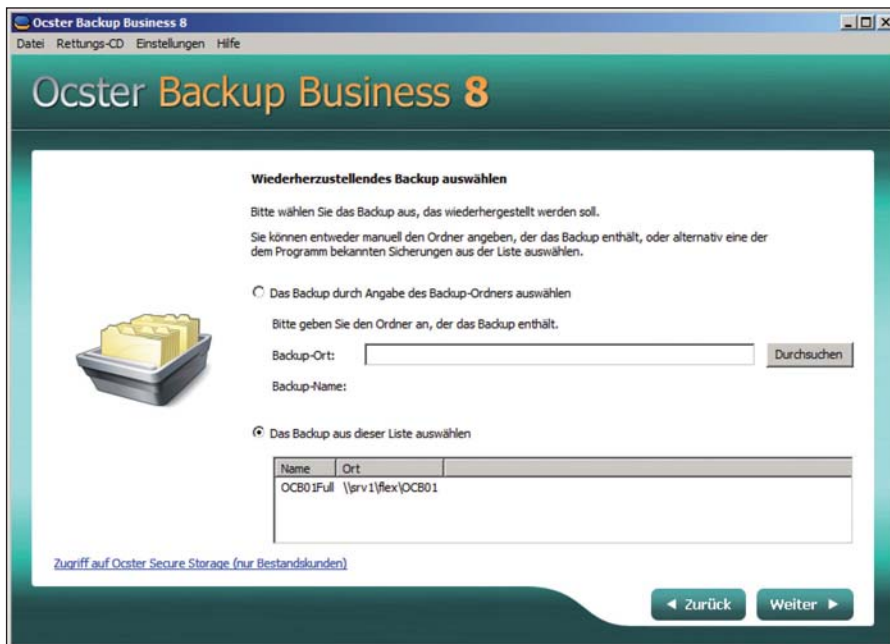


Bild 3: Für die Wiederherstellung können Sie entweder den Backup-Ordner angeben oder einen Job aus der Liste der erstellten Sicherungen auswählen

Zentrale Überwachung ja, Fernsteuerung nein

In der von uns getesteten Business-Variante ist eine Möglichkeit zur zentralen Überwachung integriert. Um diese zu nutzen, muss der Nutzer in jeder Installation die Fernüberwachung aktivieren beziehungsweise erlauben. Ocster Backup ermöglicht mit dieser Funktion eine zentrale Überwachung in der Form, dass an einer zentralen Stelle die Backup-Berichte auf den entfernten Systemen zur Verfügung stehen. Auch hier ist ähnlich wie bei der Einrichtung der Sicherungsjobs eine sinnvolle Benutzerverwendung zu planen. So gilt es, die Fernüberwachung durch den Benutzer zu aktivieren, der auch die Sicherung durchführt. Weiterhin ist ein lokaler Benutzer auf dem System einzutragen, der für eine Fernaufschaltung zum Einsatz kommen soll. Bei mehreren Sicherungen unter verschiedenen Benutzern muss jeder für die Fernüberwachung aktiviert sein. Auch die Verwendung von Domänenbenutzern bei einer Einbindung in ein Active Directory ist möglich. Um auf der Überwachungsseite ein System hinzuzufügen, sind wiederum der Benutzer anzugeben, dessen Berichte eingesehen werden sollen, sowie der lokale Benutzer, der bei der Aktivierung der Fernüberwachung eingetragen wurde. Alle überwachten Computer oder richtigerweise Benutzer-Computerkombinationen führt die

Software dann in einer Liste zur Auswahl auf. Umständlich ist, dass bei einem Eingabefehler der Eintrag nicht korrigiert werden kann. Vielmehr müssen Sie den Eintrag wieder aus der Liste löschen und neu hinzufügen. Auch empfanden wir hier die gesamte Vorgehensweise als unübersichtlich und damit fehleranfällig.

Die Berichte selbst liefern recht gute statistische Informationen zum Sicherungsumfang und zur Änderungsrate. Die Konfiguration des Backupjobs lässt sich allerdings nicht einsehen. Sofern Ocster zukünftig auf eine größere Verbreitung in kleineren Unternehmen setzt, sehen wir hier ein deutliches Optimierungspotenzial, indem die Ocster-Backup-Entwickler die Benutzerabhängigkeiten der Jobs reduzieren und die Fernüberwachung zu einer richtigen Fernadministration erweitern.

Fazit

Ocster Backup Business überzeugt durch diverse Stärken, besitzt aber genauso einige Schwächen, deren sich ein Administrator bewusst sein sollte. Klare Stärken sind der absolut günstige Preis, die einfache Bedienbarkeit und die Möglichkeit für einen Bare Metal Restore. Erfreulich ist ferner, dass es zumindest die Möglichkeit zur zentralen Überwachung mehrerer Server gibt und sich Meldungen und Berichte per E-Mail verschicken lassen.

Schwächen sind die aktuell noch fehlende Unterstützung von dynamischen Datenträgern (soll jedoch per Update kommen), die recht einfach gestaltete Fernüberwachung sowie nicht vorhandene Agenten zur Sicherung spezieller Daten wie Exchange oder Datenbanken. Letzteres erfordert, dass derartige Daten als Export oder Dump geschrieben werden oder die jeweilige Applikation für die Sicherung beendet wird. Auch empfanden wird das Einrichten der Fernüberwachung als etwas umständlich. Es zeigt sich damit, dass Ocster Backup von den Funktionen her mehr die Sicherung von Arbeitsplätzen adressiert. (dr)

Produkt

Programm zur Datensicherung und -wiederherstellung auf Server-Systemen mit zentraler Steuerung.

Hersteller

Ocster
www.ocster.com

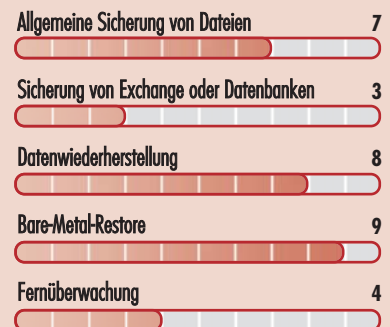
Preis

Ocster Backup Business 8 kostet zeitlich unlimitiert 50 Euro, eine Klein-Unternehmens-Lizenz für drei Rechner kostet 80 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für die preiswerte Datensicherung einer überschaubaren Anzahl von Servern in kleinen und mittleren Unternehmen.

bedingt, wenn es um die Sicherung von Exchange- und Datenbanksystemen geht, da keine Agenten verfügbar sind. Hier ist offline zu sichern oder unter Zuhilfenahme von vorherigen Exports.

nicht für die Sicherung vieler Server in größeren Umgebungen. Hierfür sind Funktionsumfang und möglicher Automatisierungsgrad zu gering.

Ocster Backup Business 8

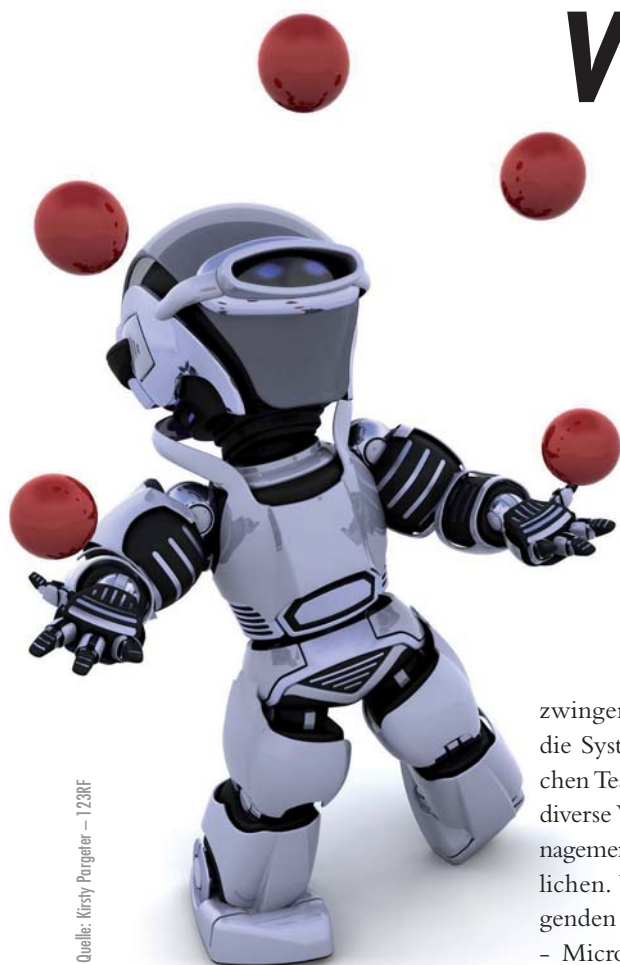


Systeme: Verwalten von Multi-Hypervisor-Infrastrukturen

Virtuelles Jonglieren

von Jörn Meyer und Daniel Neumann

Die Auswahl des passenden Hypervisors hat massiven Einfluss auf die Gesamtarchitektur der bereitzustellenden IT-Infrastruktur und die damit verbundenen Kosten. Allerdings gibt es nur selten ein "One Size Fits All"-Modell. Immer mehr Unternehmen erscheint es deshalb aus strategischer und wirtschaftlicher Sicht sinnvoll, unterschiedliche Hypervisoren einzusetzen. Der Artikel beschreibt die Erfordernisse einer solchen Konstruktion und nennt Werkzeuge, die beim Management mehrerer Hypervisoren nützlich sind.



Quelle: Kirsty Pargeter – 123RF

Noch vor wenigen Jahren stellte der Hypervisor vSphere ESX(i) von VMware den De-facto-Standard zur Virtualisierung von Server-Systemen im Rechenzentrum dar. Aufgrund überlegener Technik und herausragender wirtschaftlicher Vorteile, aber auch mangelnder Konkurrenz, veränderte vSphere ESX(i) den IT-Betrieb nachhaltig. Mit dem anhaltenden Erfolg der Server-Virtualisierung drängten Mitbewerber in den Markt, allen voran Citrix und Microsoft – mit kostenpflichtigen Lösungen für Enterprise-Kunden sowie KVM und Open Source-Xen im Open Source-Umfeld.

Ein Werkzeug für alle

Historisch betrachtet stellte das Management mehrerer Hypervisoren eines der größten Probleme für die IT-Administration dar. Jeder Hypervisor brachte seine eigenen Verwaltungswerkzeuge und Schnittstellen mit. Ein einheitliches Management war kaum möglich und Spezialwissen für die Verwaltung der Systeme

zwingend erforderlich. Zudem wurden die Systeme zumeist von unterschiedlichen Teams betreut. Heute gibt es jedoch diverse Werkzeuge, die das effektive Management mehrerer Hypervisoren ermöglichen. Unser Artikel fokussiert die folgenden Lösungen:

- Microsoft System Center Virtual Machine Manager (SCVMM)
- Citrix CloudPlatform (in Verbindung mit dem Apache Cloudstack)

Um die Leistungsfähigkeit der genannten Produkte besser bewerten zu können, betrachten wir zwei unterschiedliche Aufgabengebiete, in denen sich die Werkzeuge beweisen müssen:

- Operations Management: In diesem Fall bildet der Hypervisor quasi die Infrastruktur für die darauf laufenden virtualisierten Ressourcen. Er stellt die Schnittstelle zur physikalischen Infrastruktur dar. Aus Sicht des Services oder der Applikation ist der Hypervisor die unterste Ebene, präsentiert er dem Betriebssystem doch die zur Verfügung stehenden Ressourcen. Das Operations-Management fokussiert sich also auf die Verwaltung der virtuellen Ressourcen oberhalb des Hypervisors.
- Configuration Management: In diesem Fall arbeitet der Hypervisor wie eine Applikation, die mit den darunterliegenden physikalischen Ressourcen interagiert.

System Center 2012 R2 Virtual Machine Manager

Microsoft unterstützt schon seit den früheren Produktversionen des Virtual Machine Manager das Multi-Hypervisor Management. In den Versionen 2008 und 2008 R2 beschränkte sich dies auf Microsoft Hyper-V und VMware ESX. Mit Version SCVMM 2012 kam der Citrix XenServer hinzu. Das Unternehmen aus Redmond beschränkt sich bei SCVMM seit der Ver-

Hyper-V

- Windows Server 2008 R2 SP1 – Standard, Enterprise und Datacenter Edition
- Windows Server 2012/2012 R2 – Standard und Datacenter Edition
- Hyper-V Server 2008 R2 SP1, 2012 & 2012 R2

Citrix

- XenServer 6.0, 6.1 & 6.2

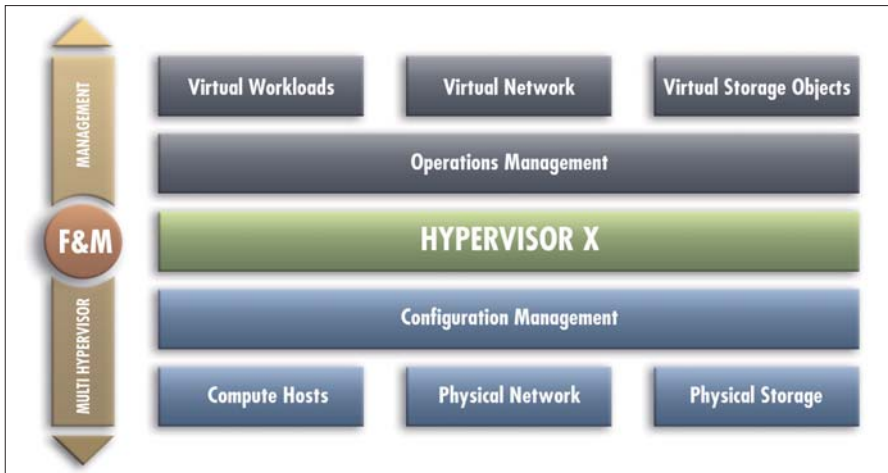
VMware

- vCenter Server & ESXi 4.1, 5.0, 5.1 & 5.5

VMware bildet hierbei eine Besonderheit. Es erfolgt kein natives Management der Komponenten wie bei Microsoft Hyper-V oder Citrix XenServer, sondern es wird als Zwischeninstanz ein VMware vCenter Server benötigt, der dann die ESX/ESXi Hosts aktiv verwaltet. Weiterhin ist zu beachten, dass vCenter Server & ESXi 5.5 und Citrix XenServer 6.2 derzeit laut TechNet offiziell nicht unterstützt werden. Beide Versionen lassen sich aber ohne Probleme in das Management von SCVMM aufnehmen.

Von SCVMM 2012 R2 unterstützte Hypervisoren





Die Multi-Hypervisor-Verwaltung lässt sich in die Teilbereiche Operations Management und Configuration Management aufteilen

sion 2012 nicht mehr nur auf das Operations Management, sondern hat auch das Configuration Management gestärkt, das unter anderem ein Bare-Metal-Provisioning von Hyper-V-Hosts umfasst.

So dient SCVMM nicht mehr nur zum Verwalten der virtuellen Maschinen und der Virtualisierungs-Hosts, sondern ist mit der aktuellen Version 2012 R2 in der Lage, das komplette Fabric Management zu übernehmen. Dazu zählen Fibre Channel Zoning, Patch-Management, Top-of-Rack-Switch-Integration, IPAM-Integration und das Management der Netzwerkvirtualisierung mit Hyper-V.

Im Operations Management unterstützt Microsoft für seinen hauseigenen Hypervisor Hyper-V alle Funktionalitäten. Die einzige Ausnahme bildet das Feature Hyper-V Replica. Hier bedarf es zusätzlich des unter Windows Azure betriebenen Hyper-V Recovery Managers inklusive Agenten, um die Hyper-V Replica mittels der Konsole von SCVMM konfigurieren zu können. Besonders interessant ist für uns jedoch, welche Funktionalitäten von VMware und Citrix sich über SCVMM nutzen lassen.

VMware-Verwaltung

Befinden sich der vCenter-Server und die ESXi-Hosts im Management von SCVMM, so lassen sich diese nicht nur über die grafische Oberfläche verwalten, sondern auch über die SCVMM PowerShell-Cmdlets. Dies hat den Vorteil, dass der Administrator nicht mehrere PowerShell-Skripte für die unterschiedlichen Hy-

pervisoren entwickeln muss. Voll unterstützt wird das Bereitstellen von virtuellen Maschinen und den sogenannten SCVMM Services. Diese stellen eine Sammlung von virtuellen Maschinen dar und basieren auf Vorlagen, die sich in der Bibliothek von SCVMM befinden. Die VMware-eigenen Services, vApp genannt, können nicht über SCVMM bereitgestellt werden. Eine Koexistenz von SCVMM Services und vApp ist aber möglich und verwaltbar.

Um bei der Bereitstellung den optimalen Virtualisierungs-Host für die virtuellen Maschinen zu ermitteln, wird für das Erstellen und Bereitstellen sowie die Migration von VMware VMs das Host Rating vollständig unterstützt. Dies gilt ebenso bei gleichzeitigen Bereitstellungen während der Provisionierung eines Services. Dieses Host Rating findet auch in einer Private Cloud Verwendung, die sich mittels VMware ESXi Hosts, VMware Resource Pools oder über verschiedene Hypervisoren durch SCVMM bereitstellen lässt.

VMware-VMs, VMDK-Dateien und VMware-Vorlagen können in der SCVMM-Bibliothek abgelegt werden. Dort besteht die Möglichkeit, weitere Anpassungen an diesen Objekten für die spätere Bereitstellung vorzunehmen oder in der Bibliothek gespeicherte VMware-VMs nach Hyper-V zu konvertieren.

In einem ESXi-Cluster lassen sich über SCVMM verschiedene VM-Migrationsverfahren wie vMotion oder Storage vMotion initiieren. Genauso wird das Set-

zen des Wartungsmodus für ESXi-Hosts unterstützt. Die unter System Center 2012 Virtual Machine Manager eingeführten Features "Dynamic Optimization" zum Lastenausgleich und "Power Optimization" zum Stromsparen stehen für ESXi-Hosts ebenfalls zur Verfügung. Letztgenannte Funktion lässt sich entweder durch die SCVMM Dynamic Optimization oder durch den VMware Dynamic Resource Scheduler steuern. Die Integration in die vom System Center Operations Manager bereitgestellten Performance & Resource Optimization Tipps ist ebenfalls möglich.

Im Bereich Virtual Network erkennt SCVMM die Standard- oder Distributed-Switches sowie die Portgruppen der ESXi-Hosts. Die Konfiguration muss allerdings über das VMware vCenter erfolgen. Ebenso verhält es sich mit den SCVMM-Netzwerkfunktionalitäten wie dem Zuweisen von logischen Netzwerken, statischen IP-Adressen und MAC-Adressen zu Windows-basierten virtuellen Maschinen. All dies wird von den ESXi-Hosts unterstützt, die Konfiguration muss

Einer oder viele? Geht es um die Entscheidung für den passenden Hypervisor, spielen folgende Aspekte bei der Entscheidungsfindung eine wichtige Rolle:

Service Level Agreements

Durch die Definition und Klassifizierung von Applikationen oder Diensten wird die IT-Infrastruktur fragmentiert. Es entstehen unterschiedliche Anforderungen pro Service. Durch die Nutzung des jeweils optimal zu den Anforderungen passenden Hypervisors können die Infrastrukturkosten erheblich gesenkt werden. So stellen die Bereitstellung zentraler Netzwerkdienste oder betriebskritischer Anwendungen andere Anforderungen an Verfügbarkeit und Leistung als die Themen Software-Entwicklung/Software-Test oder auch Schulungsmaßnahmen.

Lizenzkosten

Spezielle Lizenzmodelle für die Kernanwendungen großer Hersteller von Unternehmens-Software (Microsoft, Oracle, RedHat, Citrix) differenzieren bei den Lizenzkosten nach dem eingesetzten Hypervisor. Oftmals muss der Einsatz der Applikationen auf einem "fremden" Hypervisor sogar mit einem Aufpreis bezahlt werden.

Schutzbedarf

Der Schutzbedarf eines Systems oder einer Applikation kann ebenfalls ausschlaggebend für den Einsatz mehrerer Hypervisoren sein. Besonders schützenswerte Daten sind auf einem speziell gehärteten Hypervisor besser abgesichert.

Wahl des richtigen Hypervisors





aber im vCenter stattfinden, damit diese Einstellungen in den Portgruppen wirksam werden.

Was Virtual Storage-Objekte betrifft, kann SCVMM mit den VMware Paravirtual SCSI-Storageadaptern umgehen, unterstützt dafür aber keine VMware VMs mit IDE-Adaptern. Das Hinzufügen und Entfernen von virtuellen Festplatten im laufenden Betrieb einer VMware-VM läuft genauso ab wie bei einer Hyper-V-VM. Die Storage Automatisierung, die SCVMM für Hyper-V Hosts bereitstellt, funktioniert allerdings nicht mit den ESXi Hosts. Hier muss der Administrator wieder auf das vCenter und dessen Möglichkeiten zurückgreifen.

Citrix-Unterstützung

SCVMM unterstützt für Citrix XenServer oder XenServer-Pools die Virtual Workloads SCVMM PowerShell-Cmdlets, das Host Rating, die SCVMM-Services, die Private Cloud Erstellung sowie die Dynamic Optimization und Power Optimization vollständig. Das gilt ebenso für den Wartungsmodus, die VM-Vorlagen sowie die Performance und Resource Optimization-Tipps. Einige Besonderheiten gibt es aber auch hier zu beachten.

Citrix XenServer oder XenServer-Pools lassen sich nativ mit SCVMM verwalten, ohne dass dieser eine Zwischeninstanz benötigt. Allerdings müssen die XenServer oder XenServer-Pools vorher über das XenCenter konfiguriert worden sein. Einen Cluster aus mehreren XenServern über SCVMM zu erstellen, ist nicht möglich. Bei den VM-Vorlagen müssen Administratoren beachten, dass die XenServer-Tools nach der Bereitstellung der virtuellen Maschine manuell zu installieren sind. Da XenServer auch VHD-Dateien als virtuelle Festplatten verwendet, kann die SCVMM-Bibliothek ohne Probleme XenServer VMs und VHDs speichern. Leider werden die XenServer-Vorlagen nicht unterstützt, sodass diese nicht mit SCVMM arbeiten. Hier müsste der IT-Verantwortliche dann wieder auf das XenCenter zurückgreifen oder die XenServer-Templates als SCVMM-Templates nachbauen. Bei der Migration von virtuellen Maschinen im laufenden Betrieb wird die XenMotion Technologie genutzt.

Citrix XenServer bietet zwei Arten von virtuellen Maschinen: Paravirtual (PV) und Hardware-assisted Virtualization (HVM). Beides unterstützt SCVMM. Windows-basierte VMs sind nur als HVM möglich. Neue durch SCVMM erstellte virtuelle Maschinen sind per Default ebenfalls vom Typ HVM. Um eine VM vom Typ PV bereitzustellen, muss der Administrator eine bestehende virtuelle Maschine klonen, so dass sich diese weiter bearbeiten lässt.

Im Bereich Virtual Network erkennt SCVMM die bereits bestehenden externen virtuellen Netzwerke der XenServer. Die Konfiguration dieser muss allerdings über das XenCenter erfolgen. Die SCVMM-Netzwerkfunktionen wie das Zuweisen von logischen Netzwerken, statischen IP-Adressen und MAC-Adressen zu Windows-basierten virtuellen Maschinen werden dabei entsprechend unterstützt. Bezüglich Virtual Storage-Objekten unterstützt SCVMM sämtliche Storage Repositories des XenServers. Die Storage-Automatisierung, die SCVMM für Hyper-V-Hosts bereitstellt, funktioniert allerdings nicht mit Citrix XenServer. Hier muss der Administrator wieder auf das XenCenter und dessen Funktionen zurückgreifen.

Citrix CloudPlatform 4.21

Citrix CloudPlatform (CCP) ist ein sogenanntes Cloud-Orchestrierungs-Werkzeug, also eine Plattform, die ähnlich wie die Amazon Web Services verschiedenste physikalische Ressourcen (Computing-Einheiten mit oder ohne Hypervisor, Netzwerk-Komponenten und Storage-Systeme) dynamisch verwaltet. Massive Skalierbarkeit, Multi-Mandanten-Fähigkeit und Mandanten-Self-Service, ein intuitives grafisches Benutzer-Interface, Hochverfügbarkeit der Management-Komponenten sowie einfache Erweiterbarkeit und Automatisierung durch APIs oder Command-Line-Interfaces sind neben der Multi-Hypervisor-Unterstützung die Stärken dieser Lösung.

Eine Besonderheit von CCP ist die Unterstützung von Bare-Metal-Provisioning. In diesem Fall wird kein Hypervisor installiert, sondern direkt ein RPM-basiertes Linux-Betriebssystem. Die Installation des Betriebssystems kann mittels "Kickstart" automatisiert erfolgen. Hierbei gibt es üb-

rigens eine interessante Integration mit Cisco UCS, die es ermöglicht, UCS-Blades über eine Schnittstelle des UCS-Managers direkt aus CloudPlatform heraus als Bare-Metal-Host zur Verfügung zu stellen.

Citrix CloudPlatform kann nativ jeden Standard-NFS- oder iSCSI-Storage als sogenannten Primary Storage verwalten, das von den Hypervisor-Hosts unterstützt wird. Auf dem Primary Storage befinden sich später die Disks der laufenden VMs. Natürlich findet auch ein lokaler Storage der Hosts volle Unterstützung. Andere Storages, zum Beispiel FibreChannel-basierte Systeme, müssen zunächst über die Hypervisor-Verwaltungstools konfiguriert werden, stehen dann aber ebenfalls innerhalb von CCP zur Verfügung.

Mit der Version 4.2 hat Citrix ein Plug-In-Framework zur Verfügung gestellt, das es Drittherstellern ermöglicht, ihre Storage-Systeme ebenfalls nativ aus CCP heraus verwalten zu lassen. Aktuell gibt es bereits eine sehr interessante Integration des Herstellers Solidfire, weitere befinden sich in der Entwicklung.

Zusätzlich zum Primary Storage benötigt CloudPlatform noch einen Secondary Storage, der zwingend auf NFS basiert. Auf diesem werden statische Daten wie Templates, ISOs oder Snapshots gespeichert.

Des Weiteren gibt es seit der Version 4.2 die Möglichkeit eines Object Storage, der in Kombination mit dem Secondary Storage

Citrix

XenServer 5.6 SP2 - 6.2

VMware

vSphere / vCenter 4.1 - 5.1

KVM

KVM 5.5, 5.6, 5.7, 6.1, 6.3

Microsoft

Hyper-V Release in Q1/2014 geplant

Citrix XenServer wird dabei nativ unterstützt, für VMware ist ein vCenter Voraussetzung, über das die vSphere-Hosts im Betrieb angesprochen werden. Kommt KVM zum Einsatz, ist auf jedem KVM-Host ein zusätzlicher Agent zu installieren, über den dann die Kommunikation mit CloudPlatform erfolgt.

**Von Citrix CloudPlatform 4.21
unterstützte Hypervisoren**



die statischen Daten in der gesamten Cloud zur Verfügung stellt. Object Storage lässt sich über ein Object Storage-Plug-In ansprechen. CCP liefert Admins standardmäßig ein Plug-In für Amazon Simple Storage (S3) oder Openstack Swift mit, wobei das S3-Plug-In mit jedem S3-kompatiblen Object Storage funktioniert.

Neben der Storage-Konfiguration legt CloudPlatform besonderen Wert auf Flexibilität im Netzwerk-Umfeld. So kann auf Basis von KVM oder XenServer ein Netzwerkmodell analog Amazon AWS (Basic Networking) implementiert werden. Alternativ stehen in der sogenannten Advanced Networking Konfiguration erweiterte Netzwerk-Funktionen wie vLAN, Firewall, Load-Balancing, NAT und VPN zur Verfügung, die vor allem von Enterprise-Kunden nachgefragt werden. Advanced Networking funktioniert mit jedem der unterstützten Hypervisoren und wird standardmäßig durch einen virtuellen Router auf Linux-Basis implementiert. Des Weiteren ist es möglich, bestimmte Netzwerk-Funktionen vom virtuellen Router auf sogenannte externe Netzwerk-Provider zu verlagern. So können Firewall-Funktionen, zum Beispiel von Juniper SRX oder einer Cisco ASA 1000v, übernommen werden oder Load-Balancing von Citrix Netscaler beziehungsweise F5 Big-IP.

CloudPlatform unterstützt darüber hinaus virtuelle Switches wie VMware vSphere Distributed vSwitch (VDS), Cisco Nexus 1000v oder Open vSwitch und darauf basierende moderne Netzwerktechnologien.

Fazit

Die in diesem Artikel beschriebenen Werkzeuge sind grundsätzlich nicht ohne weiteres miteinander vergleichbar. Microsoft SCVMM eröffnet der IT-Administration vor allem bei klassischen Enterprise-Kunden die Möglichkeit, mehrere Hypervisoren im täglichen Betrieb aus einer Anwendung heraus zu verwalten und damit das Management der vorhandenen IT-Infrastruktur zu optimieren. Citrix CloudPlatform greift an dieser Stelle deutlich weiter, indem es wie beschrieben zusätzliche Themen adressiert. Multi-Mandanten-Fähigkeit bis auf Netzwerk-Ebene und weitreichende Self-Service-Funktionen seien an dieser Stelle nur noch einmal exemplarisch erwähnt.

Die Kernanforderung, nämlich unterschiedliche Hypervisoren zu administrieren und damit die beschriebenen Vorteile für Unternehmen zu realisieren, erfüllen beide. Trotzdem decken die genannten Werkzeuge nicht alle Funktionen und Aktionen ab, die notwendig sind, um mehrere Hypervisoren vollumfänglich verwalten zu können. Für bestimmte Maßnahmen werden auch weiterhin die nativen Management-Tools notwendig sein, zum Beispiel zur Fehleranalyse und -behebung. Nichtsdestotrotz bieten die Produkte bei richtiger Nutzung einen erheblichen Mehrwert für Unternehmen und helfen dabei, die Hürde des Managements unterschiedlicher Hypervisoren zu überwinden. (ln) 

Jörn Meyer arbeitet als Solution Engineer Cloud Architekturen bei FRITZ & MACZIOL. Daniel Neumann ist als Consultant Microsoft Virtualisierung & Cloud für FRITZ & MACZIOL tätig.

BUSINESS CLASS WLAN

MADE IN GERMANY

NEU! Mit integrierter kostenloser WLAN-Controller Lizenz zur Steuerung von bis zu 6 Access Points



bintec W-Serie



- ▶ Gleichzeitiger Betrieb auf dem 2,4-GHz und 5-GHz-Band
- ▶ Bruttoübertragungsraten bis zu 2x 450 Mbit/s (802.11n MIMO 3x3)
- ▶ Stand-Alone Betrieb oder Betrieb mit **bintec** WLAN Controller
- ▶ 2-Port Gigabit Ethernetanschluss mit PoE (Power over Ethernet)
- ▶ Elegantes, unauffälliges Gehäusedesign für Wand- und Deckenmontage
- ▶ Integrierte MIMO-Antennen für 2,4- und 5-GHz



bintec elmeg GmbH
Südwestpark 94
D-90449 Nürnberg
Telefon: +49-911-96 73-0
www.bintec-elmeg.com/wlanpower





Systeme: Optimierung von Virtual Desktop-Infrastrukturen

Mehr Lagerfläche

von Bertram Wöhrmann

Die Virtualisierungsrate steigt und steigt. Auch Desktops wandern vermehrt ins Rechenzentrum. Die IT-Planer aber stehen beim Thema VDI vor gänzlich neuen Herausforderungen, etwa Flaschenhälsen besonders zu Stoßzeiten. Am Beispiel virtueller Client-Sitzungen wollen wir in diesem Beitrag zeigen, welches Optimierungspotential gerade beim Thema Storage schlummert und wie Atlantis ILIO, eine Software zur Optimierung von VDI-Landschaften, den Administrator unterstützen kann.

Das Thema VDI (Virtual Desktop Infrastructure) ist in aller Munde. Trotzdem werden viele Projekte aus Kostengründen nicht umgesetzt, ist doch die benötigte Hardware recht teuer. Auch die üppigen Lizenzkosten bringen das Budget weiter an die Grenzen. Nicht zuletzt scheuen viele IT-Verantwortliche die Reaktionen der Anwender, gilt doch eine positive Nutzererfahrung als wichtigster Punkt bei einer VDI-Einführung. Vor Technik und Akzeptanz durch die Anwender steht immer das Design einer VDI-Umgebung. Zu Beginn sollte daher stets eine Ist-Analyse stehen.

Abschied vom Fat Client

Bestehende Clientlandschaften bauen auf standardisierte Hardware. Diese Komponenten werden automatisiert mit dem Betriebssystem, den passenden Treibern und den Systemtools bereitgestellt. Eine Versorgung mit Applikationen erfolgt dann über entsprechende Werkzeuge und Wege. Am Ende steht ein Fat Client, den der Anwender für seine Arbeit nutzt. Im optimalen Fall haben die Anwender keine weitergehenden Rechte auf ihrem System, was die Installation von Treibern und Software angeht. Oftmals wird die Ablage

von eigenen Dokumenten auf dem lokalen System erlaubt, mit dem Hinweis, dass die Daten nicht gesichert werden.

Bei unternehmensrelevanten Daten sieht das natürlich anders aus. Diese Daten sollten immer zentral im Netzwerk liegen und mit einer Datensicherung auch geschützt werden, damit bei Ausfällen kein Schaden durch Datenverlust entstehen kann. Im Netzwerk gibt es Gruppenlaufwerke, Ablagen für Projekte und andere Dateisysteme, in denen der Anwender Daten speichern kann. Ein weiterer wichtiger Punkt ist die Behandlung der Nutzerprofile. Auch diese sollten im Netzwerk liegen. So ist gewährleistet, dass ein Anwender sich an unterschiedlichen Stationen anmelden kann und ihm immer sein Profil zur Verfügung steht.

Sind alle diese Voraussetzungen erfüllt, ist der Schritt zum VDI-Desktop gar nicht mehr so groß. Einige der bestehenden Prozesse können übernommen werden, andere bedürfen einer Anpassung. Das betrifft im Besonderen das Thema Storage. Durch die zentrale Abbildung des Platzes besteht der Bedarf, eine hohe I/O-Last vor allem zu Stoßzeiten (Start der Systeme, Anmeldung, Benutzerprofilbereitstellung) abbilden zu können, deren Anforderung mit einem Anwachsen der Userzahlen steigt.

Optimieren die am Markt vorhandenen Virtualisierungstechnologien die Ressourcen von CPU und Arbeitsspeicher noch recht gut, sieht es bei der Festplatte schon anders aus. Das betrifft zum einen den Platz selbst und zum anderen den Durchsatz. Die einfachste Rechnung wäre die zentrale Bereitstellung einer Festplatte pro Anwender. Das macht bei 1.000 Anwendern auch 1.000 Festplatten – eine sehr unwirtschaftliche Zahl.

Lizenzen und Storage sind teuer

Eine genaue Betrachtung der im Kasten "Kostenpunkte bei VDI" aufgelisteten Punkte zeigt, dass die größten Kostentreiber die Microsoft-Zugriffslizenzen, die VDI-Lizenzen und die Ausgaben für den Storage sind. Das Potential bei den Endgeräten hingegen

Die Kostenbetrachtung erfolgt hier vom Client hin zum Rechenzentrum, ohne dabei die Infrastrukturkomponenten einzubeziehen, die für jede Client-Umgebung benötigt werden, wie etwa den Netzwerk-Port oder das Active Directory. Typische Kostenpunkte sind:

- Endgerät
- Microsoft-Zugriffslizenz
- Rechenleistung für VDI-Sitzung
- Lizenzen für VDI (Hypervisor, VDI Broker, eventuell Applikationsvirtualisierung)
- Storage

Kostenpunkte bei VDI



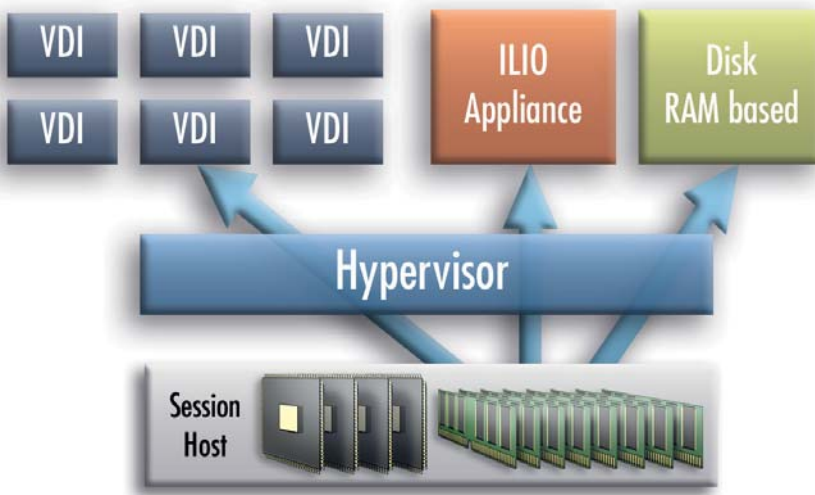


Bild 1: Mögliche Struktur einer Atlantis ILIO-Implementierung auf einem Host

ist nicht sonderlich hoch, es sein denn, dass an dieser Stelle ein vollständiger Erneuerungsbedarf ansteht. Der Preisunterschied zwischen PCs und Thin Clients beziehungsweise Zero Clients ist zwar nicht so groß, dafür gibt es aber große Unterschiede, was den Stromverbrauch angeht.

Die Zugriffslizenzen sind ein feststehender Faktor, der stark davon beeinflusst wird, mit welchen Endgeräten zugegriffen wird, ob Anwender mehrere Endgeräte nutzen und wem die Endgeräte gehören. Des Weiteren spielt es bei der Zugriffslizensierung eine Rolle, von wo aus auf die Umgebung zugegriffen wird. Zu diesem Thema gibt es ein interessantes Whitepaper von Login Consultants [1], das Sie kostenfrei herunterladen können.

Die Größe der Hardware-Umgebung und die Anzahl der benötigten Server errechnen sich aus der Anzahl der abzubildenden Sitzungen und der Ausstattung derer. Hier

gibt es kaum Spielraum für eine Kostenoptimierung. Ähnlich stellt sich das bei den VDI-Lizenzen dar. Einzig ein Kosten/Nutzen-Vergleich der unterschiedlichen Hersteller kann die Rechnung hier positiv oder negativ beeinflussen.

Der letzte große Kostenblock ist der Storage. Wer diesen Teil der Infrastruktur nur aus Sicht des benötigten Plattenplatzes betrachtet, könnte dem Trugschluss erliegen, dass die Kosten an dieser Stelle gar nicht so groß werden können. Das ist aber nur die halbe Wahrheit. Letztendlich lässt sich zwar die Summe des Plattenplatzes auf das Nötigste reduzieren, dann aber reicht der Durchsatz oft nicht mehr aus.

Ein einfaches Beispiel soll das verdeutlichen: Eine Firma möchte eine VDI-Umgebung aufbauen. Das Design für den Client hat ergeben, dass pro VDI-Sitzung eine Festplattengröße von 50 GByte ausreicht. Rein rechnerisch könnten nun 20

Anwender auf einer 1 TByte großen Festplatte arbeiten und für die angesprochenen 1.000 Anwender würden "nur" 50 1 TByte-Platten benötigt. Eine gute klassische Desktop-Festplatte hat einen Durchsatz von rund 75 bis 100 IOPS. Eine schnelle Platte in einem zentralen Storage kommt auf rund 180 IOPS. Das würde in unserem Fall bedeuten, dass pro Anwendersitzung nur 9 IOPS zur Verfügung stehen.

Anhand dieses Beispiels ist deutlich zu sehen, dass im Bereich des Storage weniger der Platz, als vielmehr der Durchsatz eine Rolle spielt. Daraus ist zu folgern, dass zentral mehr Festplatten bereitgestellt werden müssen, und zwar nicht wegen des Festplattenplatzes, sondern wegen der Leistung, die sich mit jeder hinzugefügten Festplatte erhöht und somit den Anwendern direkt zugute kommt.

Portfolio der Hersteller

Es gibt mittlerweile Lösungen, die den Bedarf an Plattenplatz stark reduzieren. Die Ansätze sind dabei vielfältig. Der Hersteller Fusion-io etwa verkauft Beschleunigerkarten für Server mit verbautem Flash-Speicher. Der Speicher wird genutzt, um die Zugriffe auf den Storage um ein Vielfaches zu beschleunigen. Vorteil bei dieser Technologie ist neben der Zugriffsbeschleunigung die Flexibilität bei der Weiternutzung von Hardware. Fusion-io unterstützt auch Bladesysteme, hier stehen Cisco und HP auf der Supportmatrix. Virident arbeitet mit ähnlichen Technologien und nutzt ebenso Beschleunigerkarten.

Einige Unternehmen bieten auch optimierte Storage-Systeme an. Dabei kommen immer Technologien wie Deduplizierung und



isits AG International School of IT Security

Berufsbegleitend zum IT-Sicherheitsexperten

- » Masterstudiengang „Applied IT Security“ in Fernlehre, akkreditiert an der Ruhr-Universität Bochum.
- » Studieren Sie ortsungebunden bei freier Zeiteinteilung, mit Start zum Sommer- oder Wintersemester.
- » Fachmodule sind einzeln buchbar und schließen mit einem hochwertigen Universitäts-Zertifikat ab.
- » Entscheiden Sie sich für einen internationalen Studiengang - Jetzt informieren und kostenlos testen.

Unser Studienkonzept – Der Weg zu Ihrer erfolgreichen Weiterbildung!

TIPP: Besuchen Sie auch unsere bundesweiten Informationsveranstaltungen.

isits
International School
of IT Security AG



www.is-its.org

Komprimierung zum Einsatz. Pure Storage etwa setzt auf Flash-basierten Storage. Das Unternehmen Tegile baut hybride Storage-Systeme und nutzt als Zugriffsbeschleunigung DRAM und SSD-Platten. Die Ablage der Daten erfolgt dabei auf herkömmlichen Platten. Einen ähnlichen Ansatz verfolgt die Firma Tintri. Auch hier wird mit Standardplatten im Backend und SSD-Platten im Frontend eine hybride Umgebung bereitgestellt. Weitere Ansätze liefern die Firmen Nimble und Nutanix. Nimble nutzt ebenfalls SSD-Platten als Beschleunigung und herkömmlichen Festplattenspeicher für die Ablage der Daten. Die Anbindung der Serversysteme erfolgt dabei blockbasiert per iSCSI über das Netzwerk.

Nutanix geht einen anderen Weg. Hier werden Computer- und Storagekapazität zusammen in einer Box verkauft. Eine Appliance nimmt bis zu vier Knoten auf. Zur Dezentralisierung der I/O-Last werden die lokalen Platten der einzelnen Knoten allen Systemen per NFS zur Verfügung gestellt, auch hier kommen schnelle SSDs als Cache zum Einsatz und herkömmliche Platten als Datenablage. Um die Verfügbarkeit durch einen Single Point of Failure nicht zu schwächen, werden über Replikationsmechanismen die Daten auf dem Nutanix-Storage entsprechend verteilt.

Nicht zuletzt bieten auch die traditionellen Storage-Hersteller Erweiterungen an, die mehr Storage-Leistung zum Server bringen. Dabei wird der Zugriff über große Cachespeicher in den Storage-Boxen optimiert, wie dies etwa NetApp mit der PAM-Karte tut; oder es werden Kombinationen aus Cache-Speichern und SSD-Platten gebaut.

VDI-Optimierung mit Atlantis ILIO

Atlantis Computing geht mit dem Produkt ILIO einen neuen Weg. Hierbei handelt es sich um eine reine Softwarelösung. Sie optimiert den Datenstrom und bildet den Storage auf dem Virtualisierungshost in einer RAM-Disk ab, die per NFS als Datastore bereitgestellt wird. Dieses Produkt schauen wir uns im Folgenden genauer an.

Tempo durch eigene Storage-Appliance

VDI erlaubt den Einsatz zweier Arten von Desktops, dem persistenten Desktop und

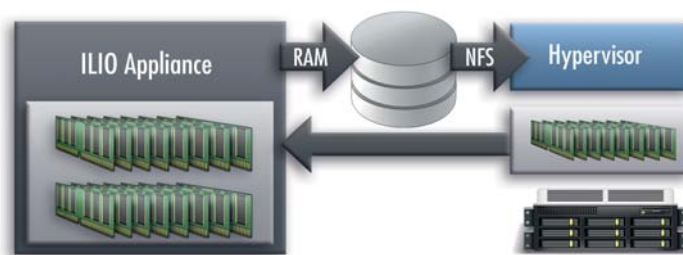


Bild 2: Aus Host-RAM erzeugt Atlantis ILIO einen Datastore

dem nichtpersistenten Desktop. Bei der ersten Variante bekommt der Nutzer immer wieder denselben Desktop, quasi seinen persönlichen virtuellen Desktop; eigene Einstellungen werden gespeichert. Beim nichtpersistenten Desktop wird der Anwender aus einem Pool bedient und erhält bei der Anmeldung die nächste freie verfügbare Sitzung. Der Arbeitsplatz ist nach jedem Start taufrisch, persönliche Änderungen werden nicht gespeichert. Aus technischer Sicht lassen sich beide Varianten auch parallel fahren.

Wie ist nun das Funktionsprinzip von Atlantis ILIO im Allgemeinen und wo liegt das Einsparpotential? Ein nichtpersistenter Desktop kann eigentlich gelöscht werden, wenn der Anwender sich abgemeldet hat, und er wird neu erstellt, wenn eine erneute Anmeldung erfolgt beziehungsweise bekommt der Anwender eine wartende Sitzung, die über einen Pool zuvor bereitgestellt worden ist. Das ist möglich, weil der Nutzer keine Daten in der Sitzung selbst speichert, die länger aufbewahrt werden sollen als der Lebenszyklus der Sitzung selbst. Alle firmenrelevanten Daten werden für diese Konfiguration im Netzwerk gespeichert, dazu dienen dann die Ablageorte auf den Fileservern, egal ob als Software- oder Hardwarelösung. Letztendlich kann so jede Nacht eine Neuprovisionierung der VDI-Sitzungen erfolgen, ohne Nachteile für den Anwender.

Bei ILIO werden die Sitzungen aber gar nicht erst auf einem Storage im klassischen Sinne abgelegt. Atlantis stellt eine Appliance bereit, die auf jedem VDI-Host installiert wird, im Idealfall und wenn vorhanden, auf den lokalen Platten des Hosts. Diese Appliances werden in ein ILIO Center Management Tool eingebunden und dieses wiederum verbindet sich mit dem vCenter Server in VMware Horizon View-

Umgebungen. Bei der Einrichtung der ILIO-Appliances wird dem System ein Teil des Arbeitsspeichers und eine vCPU des vSphere Hosts zur Verfügung gestellt. Aus einem Teil des Host-Arbeitsspeichers wird eine RAM-Disk erstellt. Diese wiederum wird dem Host, auf dem die Appliance installiert worden ist, über das NFS-Protokoll als Storage bereitgestellt. Dieses ist nun der Datenbereich, in den die virtuellen Desktops installiert werden.

Speicherbedarf minimieren

Bedenken über die Größe des Arbeitsspeicherbedarfs für den "Memory-Storage" müssen Sie nicht haben, denn Atlantis optimiert das Handling und den Datenfluss. Die Formel für die Berechnung der Größe des benötigten Speichers für die RAM-Disk ist recht einfach gehalten. Wichtig zu wissen ist, dass die Appliance nicht nur Storage bereitstellt, sie übernimmt auch noch weitere Aufgaben, die alle nur eines im Fokus haben: das Sparen von Ressourcen. So etwa wird der Datenverkehr für eine Inline-Deduplizierung ständig analysiert. Insgesamt eröffnet sich mit der integrierten Kompression ein enormes Optimierungspotential bei den zu speichernden Datenmengen und den zu übermittelnden Datenmengen. So etwa ergibt sich bei aktiver Komprimierung, 512 GByte Arbeitsspeicher im Host und 3 GByte Arbeitsspeicher in der VDI-Sitzung, eine Packungsdichte von 140 Sitzungen pro Host. Daraus resultierend ist mit einem NFS-Bedarf von 84 GByte zu kalkulieren.

Alle VDI-Sitzungen auf einem Host liegen nun in der per NFS bereitgestellten RAM-Disk. Je nach physischer Bestückung des Hosts lassen sich hier 18.000 IOPS und mehr auf die laufenden Desktops verteilen. Je nach Alter und Ausstattung der Hardware sind auch wesentlich höhere Werte erreichbar. Bei rund 100

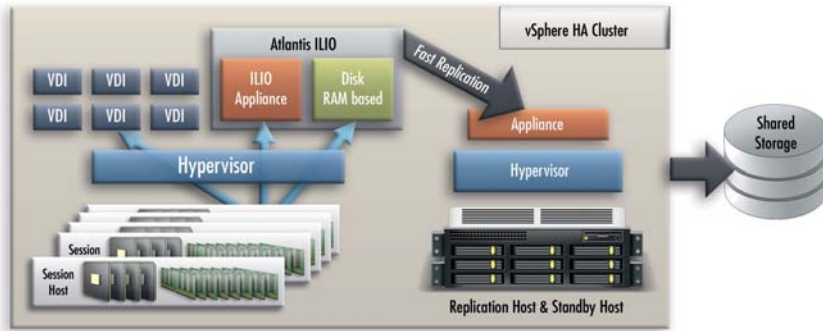


Bild 3: Der Aufbau von Atlantis ILIO sieht bei der Nutzung von persistenten Desktops etwas komplizierter aus

abbildbaren Sitzungen pro Host liegt die Festplattenperformance dann höher als bei einem klassischen FAT-Client.

Sitzungen schnell wiederherstellen

Jede Appliance versorgt immer nur den Host mit Storage, auf dem sie installiert worden ist. Es ergibt also keinen Sinn, sie zu verschieben. Was passiert aber, wenn der Host beziehungsweise die Appliance im Betrieb einen Fehler verursacht? Für das nichtpersistente Modell spielt das eigentlich keine Rolle. Der Nutzer meldet sich neu an und bekommt einen neuen Desktop bereitgestellt und kann wieder arbeiten.

Voraussetzung dafür ist natürlich, dass noch ausreichend Rechenleistung bereitsteht, um die neuen Desktops zu starten.

Für den Fall, dass Sitzungen nicht einfach wieder gelöscht werden dürfen, weil sie etwa einen definierten längeren Lebenszyklus von beispielsweise einer Woche haben sollen, ist eine andere Vorgehensweise zu wählen. Für diesen Fall wird an die Appliance eine virtuelle Festplatte angehängt, die auf einem externen Storage liegt. Auf diesen Plattenplatz wird dann ein Online-Snapshot des ILIO-Storages erstellt. Im Falle eines Reboots der Appliance wird dieser Snap-

shot erkannt und zurück in die Appliance gespielt. Damit können alle betroffenen virtuellen Sitzungen wieder genutzt werden mit dem Status des letzten Snapshots.

Es zeigt sich aber, dass dieses Design genau durchdacht werden sollte, damit der Betrieb der VDI-Umgebung nicht zu komplex wird. Jede Abweichung vom Grunddesign resultiert in zusätzlichen Prozessen und unter Umständen komplizierteren Betriebsprozessen. Die Größe des benötigten externen Plattenplatzes muss doppelt so groß sein wie der von der ILIO-Appliance zur Verfügung gestellte Plattenplatz. Der Storage wird aber nur zum Teil belegt und sollte zwingend thin provisioned bereitgestellt werden, damit sich auch hier der genutzte Plattenplatz auf ein notwendiges Minimum reduzieren lässt.

Mehr Host, weniger Storage

Bisher haben wir keine Betrachtung der Datenkommunikation vorgenommen. Sie ist aber nicht weiter kompliziert. Jede Atlantis-Komponente benötigt eine Verbindung in das Management-Netzwerk, über

Unsere Bücher machen Sie zum Experten!

Als Admin können Sie sich auf unsere Bücher verlassen: Unsere Autoren liefern Ihnen zuverlässiges Know-how zu VMware, Linux, Microsoft und Apple. Kompetent und praxisnah.

Unser gesamtes Admin-Programm:

www.GalileoComputing.de



1.155 Seiten, gebunden, 39,90 €
ISBN 978-3-8362-2405-5

659 Seiten, gebunden, 59,90 €
ISBN 978-3-8362-1787-3



Jetzt
reinschauen!



das auch die Hosts angebunden werden. Somit stehen keine Firewalls der Kommunikation der Komponenten untereinander im Weg. Die ILIO-Appliance benötigt aber zusätzlich noch eine weitere Anbindung zu einem dedizierten virtuellen Switch ohne Uplink mit nicht gerouteter IP-Adresse. Zusätzlich benötigt der Host, auf dem die Appliance residiert, einen vmkernel-Port, der sich mit diesem virtuellen Switch verbindet. Über diesen Weg erfolgt die Bereitstellung des NFS-Datstores zum Host und über dieses Protokoll wird der Host dann auch mit dem Datastore verbunden.

Die Beschleunigung des Storage wird somit erkauft zu Lasten einiger Ressourcen des Virtualisierungshosts. Die Komponenten für die Hosts sind allerdings wesentlich preiswerter als diejenigen, die in zentralen Storage-Systemen verbaut werden, beziehungsweise die Storage-Systeme selbst. Selbst bei Nutzung der SnapClone Funktionalität – hier wird wie bereits beschrieben ein nachgelagerter Storage zur Sicherung des ILIO-Storages benötigt – ergibt sich eine Platzersparnis an Storage von bis zu 80 Prozent. Für eine objektive Kostenrechnung muss aber das Mehr an Ressourcen am Host gegengerechnet werden. In unserem Beispiel stehen 672 GByte zusätzlicher Arbeitsspeicher und ein wegen der Reduzierung der Packungsdichte zusätzlich nötiger Host den Ausgaben für ein Storage-System gegenüber, das den benötigten Durchsatz und die passende Plattenplatzmenge direkt bereitstellt.

Sonderfall persistenter Desktop

Soweit die Betrachtung einer Landschaft mit nichtpersistenten Desktops. Das Design sieht aber anders aus, wenn mit persistenten Desktops gearbeitet wird. In dieser Kon-

figuration könnten im schlimmsten Fall Daten verloren gehen, wenn die Appliance ihren Dienst quittiert. Für dieses Szenario hat Atlantis vorgesorgt. Zusätzlich zu den schon aufgeführten Appliances wird eine weitere Appliance benötigt, die für das Handling der Daten verantwortlich ist, die den persistenten Desktop ausmachen. Alle ILIO-Appliances, auf denen die VDI-Sitzungen abgelegt sind, replizieren ihre Daten optimiert an den Replication Host. Dieser wiederum hält die Daten nicht selber vor, sondern leitet sie bandbreiten- und platzoptimiert an einen angeschlossenen nachgelagerten Storage weiter. Für die Abbildung von Ausfallsicherheit sollte der Storage nicht lokal auf dem Replication Host liegen, sondern im Netzwerk. Für den Datentransport zwischen der ILIO-Appliance und dem Replication Host wird eine ausreichende Storage-Netzwerk-Bandbreite benötigt. Zu Zeiten von bezahlbaren 10 GBit-Anbindungen sollte das aber kein echtes Problem darstellen.

Was verbirgt sich nun hinter diesem Replication Host? Es ist eine zusätzliche Appliance auf einem weiteren Virtualisierungshost. Bis hier ist es möglich, den Ausfall einer ILIO Appliance abzufangen. Der einzige Single Point of Failure ist jetzt der Replication Host selbst. Aber auch hier gibt es eine Lösung: den Standby Host. Atlantis nutzt an dieser Stelle die Mechanismen von VMware High Availability. Fällt der ILIO Replication Host aus, so wird die Appliance durch VMware HA auf dem Standby Host wieder gestartet. Bei einer korrekten Konfiguration des Storage-Netzwerks kann das System dann nach kurzer Zeit die Arbeit der Original-Maschine übernehmen. Eine solche Konfiguration vereinfacht Wartungsarbeiten

in der Umgebung. Zusätzlich kann der Standby Host auch den Ausfall anderer Systeme abfangen.

Eine Besonderheit gibt es bei einer persistenten Konfiguration noch: Der Storage der VDI-Sitzungen lässt sich entweder in Memory oder on Disk abbilden. Entsprechend sind die passenden Parameter beim Sizing der Umgebung auszuwählen. Zudem sollten Sie für eine optimale Deduplizierung bei der Bereitstellung von virtuellen Desktops nicht mit Linked Clones arbeiten. Dabei handelt es sich um eine Funktion, die VMware inView-Umgebungen bereitstellt, um den Plattenplatz zu optimieren. Diese Komponente wird beim Einsatz von Atlantis nicht benötigt.

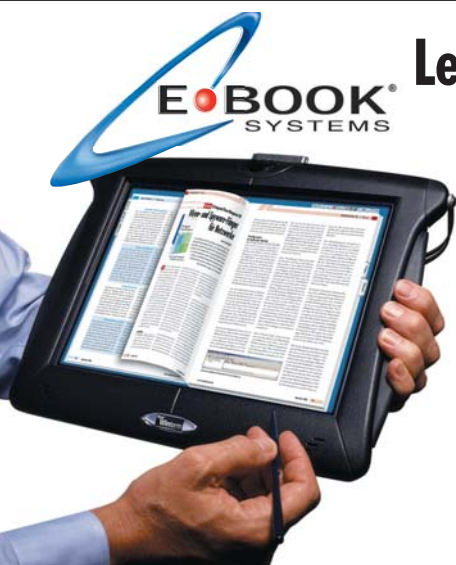
Fazit

Atlantis Computing hat mit seiner Lösung in die Zukunft investiert. Eine große Installationsbasis zeigt, dass die Software eine gute Alternative gegenüber klassischen Storage-Systemen darstellt. Dabei wird derzeit nicht nur VMware Horizon View unterstützt, auch XenDesktop und XenApp von Citrix profitieren von dieser Technologie. Nutzer dieser Appliance reduzieren aber nicht nur den Bedarf an Storage, sondern entlasten zudem das Storage-Netzwerk. Die stark reduzierten Datenströme schonen die Netzwerkkomponenten und geben anderen Systemen mehr Freiraum in Spitzenzeiten. Hier können sich also ebenfalls signifikante Einsparungen ergeben. (In)



[1] Whitepaper "Demystify complex Microsoft VDI licensing"
E3P21

Link-Codes



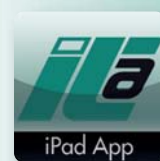
Lesen Sie den IT-Administrator als E-Paper

Testen Sie **kostenlos** und unverbindlich die elektronische IT-Administrator Leseprobe auf www.it-administrator.de.

Wann immer Sie möchten und wo immer Sie sich gerade befinden – Volltextsuche, Zoomfunktion und alle Verlinkungen inklusive. Klicken Sie sich ab heute mit dem IT-Administrator einfach von Seite zu Seite, von Rubrik zu Rubrik!

Infos zu E-Abos, E-Einzelheften und Kombiangeboten finden Sie auf:

www.it-administrator.de/magazin/epaper



NEU! Jetzt auch mit App fürs iPad!



Workshopserie: Datensicherung, Wiederherstellung und Livemigration mit Hyper-V 2012 R2 (1)

Festplatte auf Reisen

von Thomas Joos



Mit der Virtualisierung ist jede Art von Server praktisch nur noch eine virtuelle Festplatte. Mit ihr sichert der Administrator alle relevanten Daten des Servers, kann sie gleichzeitig aber zum einfachen Verschieben eines Servers auf einen anderen Host nutzen. Doch in beiden Fällen muss der IT-Verantwortliche die speziellen Eigenschaften virtueller Systeme kennen und seine Herangehensweise anpassen. Unsere Workshopserie zeigt im ersten Teil die Sicherung von virtuellen Maschinen unter Hyper-V und wendet sich im zweiten Teil dem Verschieben von virtuellen Maschinen mit Livemigration unter Windows Server 2012 R2 zu.

Mittlerweile bieten viele Backup-Softwarehersteller Unterstützung für Hyper-V, VMware oder Citrix an. Diese Produkte sichern die Server und den Host auf Ebene des Hypervisors. Beispiele sind der Data Protection Manager 2012 von Microsoft oder Symantec Backup Exec. Ersterer beherrscht auch die Online-Sicherung von Hyper-V-Hosts und den laufenden virtuellen Servern. Backup-Programme, die Hyper-V unterstützen, nutzen die Schnittstellen von Hyper-V zur Datensicherung. In diesem Zusammenhang kann die Software Snapshots der virtuellen Server zur Sicherung verwenden sowie den Schattenkopiedienst. Das ist wesentlich effizienter, schneller und auch stabiler als herkömmliche Sicherungen. Die Anwendung erstellt Snapshots im laufenden Betrieb automatisch und die virtuellen Server stehen den Anwendern weiterhin zur Verfügung. Solche Online-Sicherungen belasten die Hardware des Hosts nicht und ermöglichen auch Sicherungen während der Arbeitszeit.

Müssen Sie mehrere virtuelle Server auf einem Host sichern, kann eine kompatible Lösung auch gemeinsame Dateien erken-

nen und muss diese nicht doppelt sichern. Laufen auf einem Hyper-V-Host zum Beispiel zehn Windows-Server, erkennt das die Software und sichert die Daten nicht doppelt, sondern ignoriert identische Systemdateien und sichert nur unterschiedliche Dateien.

Bei der Sicherung von Hyper-V spielt der Schattenkopiedienst eine wichtige Rolle, da die Sicherung auf Snapshots des Servers und der virtuellen Server aufbaut. Mit aktiviertem Schattenkopiedienst lassen sich Hyper-V-Server inklusive der laufenden virtuellen Server sichern.

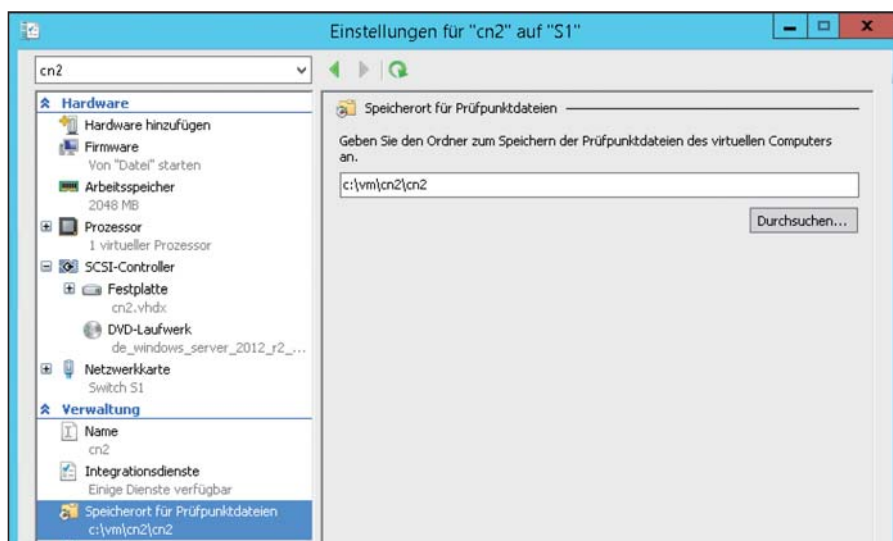
Arbeiten mit Snapshots unter Hyper-V

Snapshots helfen dabei, den Zustand von virtuellen Servern vor Konfigurationsänderungen oder zur Sicherung festzuhalten. Das heißt, Sie können bei Problemen in wenigen Sekunden den virtuellen Server auf den ursprünglichen Zustand zurücksetzen. Snapshots sind aber auch bei der Sicherung von Servern nützlich, zumindest wenn ein optimales Datensicherungsprogramm für Hyper-V im Einsatz ist. In

Windows Server 2012 R2 hat Microsoft Snapshots in Prüfpunkte umbenannt, in Windows Server 2012 war die Bezeichnung noch "Momentaufnahmen". Die Technik beschreibt die gleiche Funktion wie Snapshots.

Erstellen Sie einen Snapshot, sperrt Hyper-V die VHD(X)-Datei des virtuellen Servers vor Änderungen und speichert alle zukünftigen Daten in eine neue differenzierende Festplatte (AVDX). Erstellen Sie auf Basis dieses Snapshots einen weiteren Snapshot, verwendet auch dieser eine neue AVDX-Datei, die wiederum auf die vorangegangene AVDX-Datei verweist. Je mehr Snapshots Sie erstellen, desto mehr solcher Dateien werden angelegt, was die Leistung des Servers beeinträchtigt.

Nach der Erstellung eines Snapshots finden Sie im Snapshot-Ordner mehrere Dateien, darunter eine XML-Datei für jeden Snapshot. Standardmäßig besteht ein virtueller Server aus einer VHD(X)-Datei (seiner Festplatte), einer XML-Datei, die die Einstellungen des Servers enthält, sowie den Statusdateien mit den Endungen



Administratoren legen für jeden virtuellen Server den Speicherort der Snapshotdateien fest

BIN und VSV. Erstellen Sie einen Snapshot, legt der Server zunächst eine neue virtuelle Platte (eine AVHD(X)-Datei) an, die als Basis die VHD(X)-Datei nutzt. Der Snapshot schreibt zukünftige Änderungen des Servers in die AVHD(X)-Datei. Ab jetzt verweist die XML-Datei des virtuellen Servers auf die AVHD(X)-Datei, die die Änderungen seit dem Snapshot enthält.

Setzen Sie den Server zum Stand eines Snapshots zurück, verwendet Hyper-V nicht mehr die AVHD(X)-Datei, sondern wieder die originale VHD(X)-Datei. Sie sehen den Verweis zu der AVHD(X)-Datei auch in der XML-Konfigurationsdatei des Servers. Ein Snapshot eines virtuellen Servers besteht aus der BIN- und VSV-Datei mit der Konfiguration des Servers zum Zeitpunkt des Snapshots. Auf diese Dateien verweist die XML-Datei des Snapshots. Das heißt, ein Snapshot eines virtuellen Servers enthält folgende Dateien:

- Eine XML-Datei, die auf die Statusdateien (VSV und BIN) verweist.
- Eine neue VSV-Datei und eine neue BIN-Datei.
- Eine neue differenzierende Festplatte (AVHD(X)), die die produktive Festplatte des Servers (VHD(X)) als Quelle nutzt.

Erstellen Sie einen weiteren Snapshot, der auf dem Stand des ersten Snapshots aufbaut, verwendet dieser ebenfalls eine neue differenzierende Festplatte (AVHD(X)). Diese erhält als Quelle aber nicht die pro-

duktive virtuelle Festplatte des Servers (VHD(X)), sondern die AVHD(X)-Datei des vorherigen Snapshots. Dies liegt daran, dass der neue Snapshot auf dem alten Snapshot beruht. Daher muss hier ein stufenweiser Aufbau erfolgen. Da heißt, je mehr Snapshots eines Servers Sie erstellen, umso mehr differenzierende Festplatten setzen Sie ein, die aufeinander aufbauen. Durch diesen Aufbau kann die Leistung eines Servers stark einbrechen.

Bewahren Sie Snapshots also nur so lange auf, wie es unbedingt notwendig ist. Löschen Sie einen Snapshot, entfernt Hyper-V auch die erstellten XML-, VSV- und BIN-Dateien. Die differenzierenden Festplatten schreibt Hyper-V in Windows Server 2012 R2 aber erst dann in die produktive virtuelle VHD(X)-Festplatte, wenn Sie den Server einmal ausschalten, nachdem Sie den Snapshot gelöscht haben. In Windows Server 2012 R2 findet dieser Vorgang online statt, der Server muss dazu nicht neu gestartet werden (Onlinemerge).

Snapshots von virtuellen Servern erstellen

Hyper-V ermöglicht die Erstellung von Snapshots, auch ohne dass Sie Zusatzanwendungen installieren. Den entsprechenden Befehl finden Sie im Kontextmenü der virtuellen Computer im Hyper-V-Manager. In Windows Server 2012 R2 hat Microsoft die Snapshots verbessert. So besteht jetzt die Möglichkeit, Snapshots zusammenzuführen, ohne dass die virtuellen Server heruntergefahren werden müssen.

Diese Onlinemerges sollen die Ausfallzeiten von virtuellen Servern reduzieren. Verwenden Sie Hyper-V-Replikation in Windows Server 2012 R2, überträgt der Assistent die Daten auf Basis von Snapshots und erstellt für bereits übertragene virtuelle Server auf dem Zielserver erneut Snapshots.

Während der Erstellung des Snapshots bleibt der Computer online und steht weiterhin den Anwendern zur Verfügung. Die erstellten Snapshots zeigt der Hyper-V-Manager im mittleren Bereich der Konsole an. Hyper-V speichert die Snapshots in dem Ordner, den Sie in den Einstellungen des virtuellen Computers im Bereich "Speicherort für Prüfpunktdateien" angeben. Sobald ein Snapshot erstellt ist, können Sie den Ordner nicht mehr ändern.



Mehr Praxisnahes und Bedarfsgerechtes zur Verwaltung der Version R2 von Windows Server 2012 sowie Windows 8.1 finden Sie auf **180 Seiten im neuen IT-Administrator Sonderheft "Windows Server 2012 R2 & Windows 8.1"**.

Dabei fokussiert das Sonderheft insbesondere die zahlreichen Neuerungen und Verbesserungen, die Windows Server 2012 R2 mit sich bringt. Besonders im Bereich Virtualisierung haben Administratoren zahlreiche neue Optionen zur Verwaltung ihrer IT-Landschaft. In einer eigenen Sonderheft-Rubrik zeigt Ihnen Autor Thomas Joos daher die **praktische Nutzung des neuen Servers als Virtualisierungsplattform**. Darüber hinaus finden Sie im neuen Sonderheft selbstverständlich auch alle neuen Features der allgemeinen Administration und für den **Einsatz als Applikationsplattform**. Hier lassen sich beispielsweise mit Workplace Join mobile Clients anbinden und mit dem Web Application Proxy stellt Microsoft Bordmittel als Nachfolge von TMG und UAG bereit. Eine breite Plattform finden im Sonderheft auch die **Windows Server Essentials**, die den schmerzlich vermissten Small Business Server ablösen. Und wie all dies im Zusammenspiel mit Windows 8.1 funktioniert, zeigt unser Sonderheft ebenso.

Sie können das Sonderheft, das Ende März erscheint, ab sofort unter www.it-administrator.de/kiosk/sonderhefte vorbestellen. Als Abonnent erhalten Sie das Sonderheft zum vergünstigten Preis von 24,90 Euro (regulär 29,90 Euro – alle Preise inklusive Mehrwertsteuer und Versand).

Sonderheft "Windows Server 2012 R2 & Windows 8.1"





Rufen Sie den Befehl "Zurücksetzen" im Kontextmenü des virtuellen Computers auf, wendet Hyper-V den letzten erstellten Snapshot an und setzt den Computer auf diesen Stand zurück. Snapshots ersetzen allerdings keine Datensicherung, sondern bieten nur eine Rückversicherung vor einer Konfigurationsänderung auf dem Server.

Snapshots selbst erstellen Sie über den Befehl "Prüfpunkt" im Kontextmenü. Durch diesen Vorgang erstellt der Server eine neue differenzierende Festplatte der aktuellen Systemfestplatte. Beim Zurücksetzen gehen aber keine Änderungen verloren, sondern werden wiederum in einem anderen Snapshot erfasst.

Wenn Sie einen Server zurücksetzen oder einen älteren Snapshot anwenden beziehungsweise Snapshots löschen und die differenzierende Festplatte des Snapshots in die übergeordnete VHDX-Datei überführen, vergrößert sich unter Umständen diese Datei. In diesem Fall sollten Sie diese im Hyper-V-Manager bearbeiten und verkleinern lassen. Sie finden dazu im Aktionen-Bereich den Eintrag "Datenträger bearbeiten". Auch für die einzelnen Snapshots steht ein Kontextmenü zur Verfügung, über das Sie diese steuern. Setzen Sie eine Hyper-V-kompatible Datensicherung ein, kann diese ebenfalls automatisiert einen solchen Snapshot erstellen und dessen Daten sichern.

Verwalten der Snapshots

Snapshots verwalten Sie ebenfalls im Hyper-V-Manager über das Kontextmenü der einzelnen Prüfpunkte. Ihnen stehen hierzu verschiedene Möglichkeiten zur Verfügung. Über "Einstellungen" rufen Sie die Einstellungen des virtuellen Computers auf, zu dem dieser Snapshot gehört. Es handelt sich dabei um die Einstellungen, die zum Zeitpunkt des Erstellens gültig waren. Haben Sie Einstellungen nach dem Erstellen des Snapshots geändert, sind diese an dieser Stelle nicht zu sehen. Auf diese Weise schützen Sie auch die Konfiguration von virtuellen Servern. Wählen Sie "Anwenden" aus, setzt der Assistent den virtuellen Computer wieder auf den Stand zurück, an dem Sie diesen Snapshot erstellt haben. Vorher erscheint aber ein Abfragefenster, das Sie auf die Folgen hinweist. Außerdem können Sie vorher noch mal einen Snapshot er-

stellen, der dann den aktuellen Zustand sichert. Im Gegensatz zum Zurücksetzen über das Kontextmenü der VM können Sie hier nicht nur den letzten Snapshot verwenden, sondern beliebige Snapshots.

Beim "Exportieren" von virtuellen Servern in Windows Server 2012 R2 können Sie auch Snapshots berücksichtigen. Über das Kontextmenü eines Prüfpunktes können Sie daher einen virtuellen Server mit dem Stand des Snapshots exportieren und auf anderen Servern wieder importieren. Neu ist die Möglichkeit, dass Sie diese Vorgänge im laufenden Betrieb des virtuellen Servers durchführen können.

Durch "Umbenennen" weisen Sie dem Snapshot einen anderen Namen zu. Hyper-V verwendet als Namen normalerweise das Datum und die Uhrzeit. Über diesen Menübefehl können Sie zum Beispiel noch Informationen hinzufügen, warum Sie den Snapshot erstellt haben. Mit "Prüfpunkt löschen" löschen Sie den Snapshot und die dazugehörigen Daten vom Server und überführen die notwendigen Daten in die produktive Festplatte. Beim Löschen eines Snapshots gehen daher keine Daten verloren, sondern Änderungen, die Sie seit dem Erstellen des Snapshots durchgeführt haben, werden in die virtuelle Festplatte des Servers geschrieben und anschließend wird der Snapshot und seine differenzierende Festplatte gelöscht (AVDX). Server 2012 R2 beherrscht diesen Vorgang online; der virtuelle Server kann weiter in Betrieb sein.

Die Option "Prüfpunkt-Unterstruktur löschen" entfernt den aktuellen Snapshot sowie alle Sicherungen, die Sie nach dem Snapshot erstellt haben und auf diesen aufbauen. Der Vorgang ist ähnlich zu Prüfpunkt löschen, führt aber alle zusammengehörigen Snapshots zusammen.

Datensicherung und Snapshots bei Hyper-V im Cluster

Setzen Sie Hyper-V im Cluster ein, um beispielsweise die Livemigration zu nutzen, müssen Sie bei der Datensicherung und der Erstellung von Snapshots einige wichtige Punkte beachten. Sie sollten es möglichst vermeiden, Snapshots von laufenden virtuellen Maschinen (VM) in Clustern zu erstellen. Setzen Sie nämlich einen solchen

Snapshot zurück, setzt dieser nicht nur den Inhalt der virtuellen Festplatte zurück, sondern auch den des Arbeitsspeichers der VM. Dieser Umstand bereitet vor allem im Zusammenhang mit der Livemigration Probleme. Wenn Sie also Snapshots von VMs in einem Cluster durchführen wollen, fahren Sie die VM herunter. Gleiches gilt, wenn Sie einen Snapshot auf eine VM anwenden.

Bei Domänencontrollern (DC) sichern Snapshots auch die Active Directory-Datenbank. Setzen Sie auf einem Domänencontroller mit Windows Server 2008 R2 einen Snapshot zurück, kann es zu Inkonsistenzen der Active Directory-Datenbank kommen, die auch die anderen Domänencontroller beeinflussen. Das liegt daran, dass in Active Directory alle Objekte eine bestimmte Nummer besitzen, die Update Sequence Number (USN). Jeder DC hat eine eigene Liste dieser USNs und befindet sich auch selbst in dieser Liste. Setzen Sie einen Snapshot zurück, ändern sich die USNs zahlreicher Objekte, was mit hoher Wahrscheinlichkeit zu Inkonsistenzen führt. In jedem Fall aber trennen die anderen Domänencontroller den wiederhergestellten DC vom Netzwerk, um Fehler zu beheben.

Zwar hat Microsoft das Problem in Windows Server 2012 R2 mit der "Generation-ID" besser im Griff, aber generell ist das Sichern von Servern, die eine Datenbank bereitstellen, nicht über Snapshots empfohlen. Das Gleiche gilt übrigens für alle Server, die eine Datenbank nutzen, auch Exchange und SQL. Sie sollten solche Datenbanken niemals über Snapshots zurücksetzen.

In Hyper-V haben Sie die Möglichkeit, einem Gastsystem eine differenzierende virtuelle Festplatte zuzuweisen. Dazu bauen die Festplatten auf eine übergeordnete Festplatte mit einer Windows-Installation auf und speichern die Daten auf einer eigenen Festplatte. Für Domänencontroller ist das nicht empfohlen, da sich solche Festplatten zu leicht wieder in den Ursprungszustand zurückversetzen lassen. Hier gibt es das gleiche Problem wie mit den Snapshots.

Im zweiten Teil unserer Workshopserie lesen Sie, wie Sie virtuelle Server im laufenden Betrieb mittels Livemigration zwischen Hyper-V-Hosts verschieben. (jp)

Systeme: Server mit Red Hat CloudForms in die Cloud verlagern

All-inclusive Management

von Thorsten Scherf



Quelle: alphaspirit – 123RF

Das Management von virtuellen Systemlandschaften stellt eine immer größere Herausforderung in modernen Rechenzentren dar. Der Linux-Distributor Red Hat stellt mit CloudForms ein einheitliches Management-Framework für unterschiedliche Hypervisoren zur Verfügung, um diese Aufgabe zu bewerkstelligen. Basierend auf vier Modulen verbindet CloudForms öffentliche und private Clouds und stellt dabei unter anderem Sicherheits- und Softwareverteilungsfunktionen bereit.

Fast keine Firma kann es sich mehr leisten, auf den Einsatz von privaten oder öffentlichen Clouds zu verzichten. Ein Problem von Cloud-Infrastrukturen ist jedoch die Verwaltbarkeit einer solchen Umgebung und der darin befindlichen Systeme. Kaum eine IT-Organisation setzt in der eigenen System-Landschaft nur Produkte eines einzelnen Herstellers ein. Die Wahrscheinlichkeit, dass unterschiedliche Lösungen zum Virtualisieren von Systemen vorhanden sind, ist also recht groß. Beim Thema Cloud-Computing wird es noch etwas komplexer: Hier sind Systeme vorhanden, die teilweise zum unternehmens-eigenen Netzwerk gehören, teilweise aber auch bei entfernten Cloud-Anbietern gehostet werden. Wir sprechen in einem solchen Fall von Systemen in privaten und öffentlichen Clouds.

Management für hybride Cloud-Umgebungen gefragt

Hier sind Management-Systeme gefragt, die solche hybriden Cloud-Lösungen leicht wartbar machen. Niemand möchte mit einer Vielzahl von Tools hantieren müssen, um solche Landschaften zu verwalten. Dies wäre nicht nur fehleranfällig und zeitaufwändig, sondern würde auch gerade für neue Mitarbeiter eine sehr steile Lernkurve bedeuten. Schließlich geht es nicht nur um das Bereitstellen von neuen

Systemen. Die Systeme sind natürlich auch mit Software-Updates zu versorgen, Ressourcen müssen dynamisch hinzugefügt und auch wieder entfernt werden, Abrechnungen und Reports über die Nutzung von Ressourcen sind zu erzeugen, Compliance-Anforderungen sind auf den Systemen umzusetzen. Und das sind nur einige der typischen Anforderungen, die ein Management-Framework für Cloud-Infrastrukturen umsetzen muss.

Eine weitere Anforderung macht das ganze Szenario noch um einiges komplexer, denn typischerweise wollen Anwender ihre Systeme heutzutage selbst zusammenstellen können. Bleiben wir beim zuvor genannten Beispiel von Entwicklern, die ihre Entwicklungssysteme zum Testen von Applikationen selbst bereitstellen. Um hier einen möglichst einfachen Ablauf zu gewährleisten, sind Service-Kataloge mit entsprechenden System-Templates bereitzustellen. Aus dem Katalog kann ein Anwender dann das für ihn richtige Template auswählen, zusätzliche Parameter wie beispielsweise Speicher, Festplattengröße und notwendige Netzwerke bestimmen und dann die Bereitstellung eines neuen Systems beantragen. Hier hört der Prozess aber leider noch nicht auf: Ein Management-Framework muss Regelwerke dahingehend auswerten können, ob die

Bereitstellung eines solchen Systems automatisch stattfinden soll, und wenn ja für welchen Personenkreis, oder ob eine solche Anfrage die manuelle Bestätigung beispielsweise eines Vorgesetzten benötigt.

Wir erkennen, es existiert eine Vielzahl von unterschiedlichen Anforderungen, die an ein umfassendes Cloud-Management gestellt werden. Zusammengefasst lässt sich sagen, dass ein Cloud-Management-Framework zumindest die folgenden Anforderungen erfüllen sollte:

- Unterstützung für ein Self-Service Portal und/oder einen Service-Katalog, sodass Benutzer selbstständig ihre virtuellen Systeme installieren können. Idealerweise ist dieses mit einem Regelwerk verknüpft, um vollautomatisierte Installationen zu gewährleisten.
- Automatische Umsetzung von vordefinierten Compliance-Regeln. Das Management-Tool sollte auf gewisse Rahmenparameter reagieren können. Beispielsweise eine Regel, die verhindert, dass ein System überhaupt startet, solange noch ein temporäres Installationsnetzwerk mit dem System verbunden ist.
- Das Framework sollte vorhandene Ressourcen optimal ausnutzen und dafür sorgen, dass Systeme die Anforderungen der darauf laufenden Services erfüllen. Nur so kann sichergestellt werden, dass

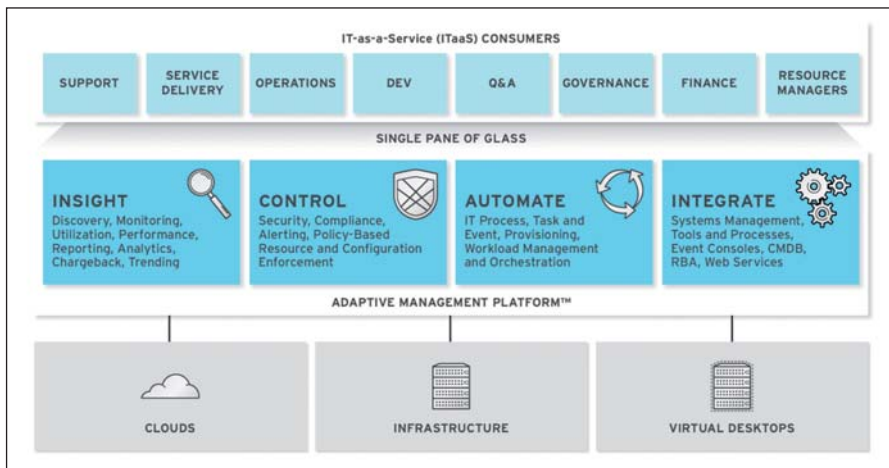


Bild 1: Die vier CloudForms-Kernmodule stellen alle wesentlichen Verwaltungsoptionen bereit

Dienste unterbrechungsfrei auf einem System arbeiten.

- Trending-Funktionen sollten aufzeigen, wenn Ressourcen für den Betrieb von Systemen knapp werden. Dies hilft dabei, SLAs für die Dienste einzuhalten.
- Gerade in hybriden Cloud-Infrastrukturen muss es möglich sein, eine Übersicht sämtlicher zur Verfügung stehenden Ressourcen und Systeme ("Devices") zu bekommen. Hierzu gehört ebenfalls ein sauberer Mechanismus zum Dekommissionieren von Ressourcen und Systemen. Anhand der gesammelten Daten muss es möglich sein, entsprechende Reports und auch Abrechnungen für die Nutzung der einzelnen Ressourcen generieren zu können.
- Es müssen Schnittstellen existieren, die das Anbinden von Drittanbieter-Software ermöglichen. Beispielsweise ist es sinnvoll, dass bei der Provisionierung von Systemen eine Interaktion mit einem IP-Address-Management-System (IPAM) stattfindet, sodass neu zu installierende Systeme automatisch eine IP-Adresse zugewiesen bekommen und diese mit dem dazugehörigen Namen im DNS registriert wird.

Eigenentwicklung vs. Zukauf

Nur wenn zumindest diese Anforderungen erfüllt sind, ist eine optimale Orchestrierung der vorhandenen IT-Ressourcen möglich. Auf dem Markt tummeln sich eine Vielzahl unterschiedlicher Hersteller und buhlen um die Gunst der Benutzer. Auf der anderen Seite ist es aber auch so, dass heutzutage immer noch viele Unternehmen versuchen, eigene Lösungen auf

Basis von selbstentwickelten Anwendungen zu entwerfen. Nach und nach rücken diese selbstentwickelten Lösungen jedoch immer weiter in den Hintergrund, da diese zwar oftmals schneller die Bedürfnisse der Anwender abdecken, langfristig gesehen aber nicht sämtliche Anforderungen erfüllen können.

Bei der strategischen Entscheidung, welche Art und welche Form von Cloud-Lösung tatsächlich umzusetzen ist, greifen immer mehr Unternehmen auf hybride Modelle zurück. Das heißt, es werden interne (private) mit externen (öffentlichen) Cloud-Lösungen verbunden und damit wird zwangsläufig auch ein Mix der eingesetzten Virtualisierungs-Technologien eingeführt. Der hybride Ansatz hat den Vorteil, dass es sich hier tatsächlich um eine ganzheitliche Lösung handelt und keine Silos entstehen, da auch bereits vorhandene Infrastrukturen mit in das hybride Lösungsmodell eingebunden werden können. Kein Unternehmen kann es sich leisten, komplett auf der grünen Wiese zu planen. In den allermeisten Fällen sind bereits Infrastrukturen vorhanden, die mit in das neue Konzept eingearbeitet werden müssen. Der hybride Cloud-Ansatz macht genau dies möglich.

Architektur von CloudForms

Ende 2013 veröffentlichte Red Hat CloudForms in Version 3.0. Der Termin wurde unter anderem deshalb gewählt, da das Framework nun auch OpenStack als Virtualisierungslösung supported. Daneben unterstützt CloudForms auch noch die Red Hat Enterprise Virtualization (RHEV),

VMware vSphere, Microsoft Hyper-V und Amazon EC2. Diese Art der Unterstützung von unterschiedlichen Hypervisoren ist ein Alleinstellungsmerkmal von CloudForms. Kein anderes Produkt auf dem Markt kann diese Bandbreite anbieten. Mit CloudForms 3.0 steht nun ein umfassendes Management-Framework zur Verfügung, mit dem sich private und öffentliche Cloud auf Basis unterschiedlicher Technologien verwalten lassen. Dieser Open-Hybrid-Cloud-Ansatz erlaubt es, Infrastructure-as-a-Service (IaaS)-Software von unterschiedlichsten Herstellern mit nur einem einzelnen Management-Interface zu verwalten.

CloudForms besteht im Kern aus einer Komponente, die sich "CloudForms Management Engine" (CFME) nennt. Diese wird als Appliance im OVF-Format ausgeliefert und steht somit als virtuelles System innerhalb einer VMware- oder Red Hat-Virtualisierungsumgebung zur Verfügung. Die Appliance enthält einen Server, der mit den anderen CloudForms-Komponenten kommuniziert. Der Server unterstützt dabei das sichere SSL-Protokoll. Die "Virtual Management Database" (VMDB) enthält sämtliche Informationen über die hybride Cloud-Infrastruktur. Die VMDB kann dabei auch auf einem externen System installiert werden.

Gleiches gilt für den SmartProxy, der ebenfalls auf der Appliance selbst oder auf einem Hypervisor-System installiert wird. Der SmartProxy sammelt Meta-Informationen der virtuellen Systeme ein. Dazu zählen beispielsweise vorhandene Benutzer-Accounts, installierte Anwendungen, Software-Patches und andere relevante Informationen eines virtuellen Systems. Der ganze Vorgang wird in CloudForms dann als Smart-State-Analyse bezeichnet und ist ein extrem mächtiges Werkzeug. Hiermit lassen sich Compliance-Anforderungen umsetzen, die beispielsweise testen, ob ein bestimmter Security-Patch auf einem System installiert ist. Sollte dies nicht der Fall sein, so lässt sich eine entsprechende Warnmeldung generieren oder sogar das ganze System runterfahren.

Schließlich enthält die Appliance auch noch eine Web-Konsole, mit der Clients



eine Verbindung zu der Appliance und dem darauf laufenden CloudForms-Server herstellen können, um die gesamte Umgebung zu administrieren. Über die Konsole lassen sich sämtliche Management-Aufgaben für die hybride Cloud-Landschaft durchführen. Die Authentifizierung von Benutzern an der Konsole kann dabei über einen bereits vorhandenen Verzeichnisdienst laufen, beispielsweise das Active Directory.

CloudForms stellt zusätzlich ein Rollen-Model zur Verfügung, mit dem die AD-Benutzer bestimmte Rechte erhalten. Somit ist eine fein granulierte Unterscheidung möglich, welche Benutzer welche Aktionen in dem CloudForms-Management-Framework ausführen dürfen. Für sehr große Installationen bietet CloudForms ein Regionen/Zonen-Modell an. Hiermit ist es möglich, mehrere Regionen – beispielsweise auf Basis der geografischen Installation der CloudForms-Appliances – zu erzeugen und diese dann mittels Zonen weiter zu unterteilen. In einem solchen Setup würde jede Region eine eigene VMDB bekommen. Eine Top-Level-Datenbank sammelt die Daten der einzelnen VMDBs dann ein und stellt diese über die Konsole zur Verfügung.

Module von CloudForms

CloudForms gliedert sich in insgesamt vier Kernbereiche [1] mit unterschiedlichen Funktionen.

Ressourcen verwalten

Das Insight-Modul stellt grundlegende Informationen über die vorhandene Cloud-Infrastruktur zur Verfügung. Mittels sogenannter Provider stellt die Appliance eine Verbindung zu sämtlichen Hosts her, auf denen virtuelle Systeme laufen und an denen andere Ressourcen wie beispielsweise Speicher und Netzwerke angebunden sind. Diese Informationen sammelt das Framework über ein Discovery der Umgebung ein, nachdem sämtliche Provider konfiguriert sind. Hiermit ist es bereits möglich, ein umfassendes Bild der eigenen Cloud-Landschaft zu erhalten, Utilization- und Performance-Reports zu erstellen und Abrechnungen über die Nutzung von einzelnen Ressourcen zu erzeugen.

Die vom Insight-Modul erkannten Ressourcen lassen sich mit Tags versehen. Dies ist ebenfalls ein enorm mächtiges Feature von CloudForms, da sich mit Hilfe dieser Tags Aktionen auf sämtliche Ressourcen eines bestimmten Tags anwenden lassen. Beispielsweise ließe sich ein Tag auf Provider für bestimmte Virtualisierungslösungen setzen. Somit ist es ohne große Probleme möglich, zu erkennen, welche und wie viele Ressourcen ein bestimmter Provider (beispielsweise für Red Hat Enterprise Virtualization oder VMware) tatsächlich zur Verfügung stellt. Das Insight-Modul ist dabei auch in der Lage, Ressourcen eines bestimmten Typs in Clustern zu organisieren.

Compliance wahren

Im Control-Modul werden Compliance- und Control-Policies festgelegt, mit denen sich die virtuelle Umgebung verwalten lässt. Diese Regelwerke setzen sich aus “Events”, “Conditions” und “Actions” zusammen. Die Regeln können sich dabei entweder auf Compliance- oder auch auf Control-Anforderungen beziehen. Sollte ein Host oder eine virtuelle Maschine den Anforderungen einer Compliance-Regel nicht entsprechen, so markiert CloudForms dieses System automatisch als nicht compliant und stellt es auf der Übersichtsseite in einer eigenen Statistik dar. Somit erhält der Administrator recht leicht einen Überblick darüber, welche Systeme den eigenen Compliance-Regeln entsprechen und welche nicht.

Ein Beispiel für eine einfache Regel könnte sein, dass CloudForms beim Hochfahren einer Maschine testet, ob die Maschine ein bestimmtes Software-Paket installiert hat. Ist dies nicht der Fall, so könnte eine mögliche Aktion lauten, dass die Maschine wieder gestoppt und ein Alert versendet wird. Eine andere Regel könnte testen, ob eine virtuelle Produktionsmaschine auch in der richtigen Umgebung abläuft und nicht versehentlich auf einem Host gestartet wurde, der Teil der Entwicklungsumgebung ist. CloudForms kann im Control-Modul auch die Auslastung von Ressourcen überprüfen und auf Basis der Ergebnisse entsprechende Aktionen einleiten. Sollte beispielsweise die Last auf einem Host-System zu hoch werden, so sorgt eine entsprechende Control-Regel dafür, dass beim Erreichen einer gewissen Lastgrenze virtuelle Systeme auf andere Hosts umgezogen werden.

Lifecycle-Management

Der Bereich “Automate” stellt die Lifecycle-Funktionen zur Verfügung. Hierzu zählt die Installation von neuen Systemen über einen der vorhandenen Provider, aber auch die Dekommissionierung von alten Systemen. Die Funktionen werden über sogenannte “State-Machines” bereitgestellt. Die Installation von virtuellen Maschinen erfolgt dabei entweder auf Basis von Templates oder durch das Klonen bereits bestehender Systeme. Templates lassen sich um entsprechende virtuelle Ressourcen, wie beispielsweise die Anzahl der CPUs, Speicher, Block-Geräte und Netzwerke,

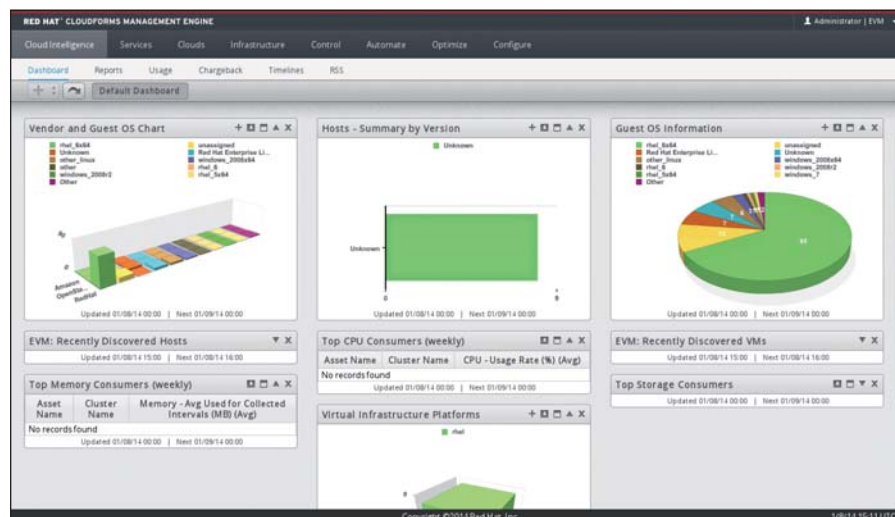


Bild 2: CloudForms stellt eine Übersichtsseite zur Verfügung, die sich individuell anpassen lässt, sodass alle relevanten Informationen auf einer Seite ersichtlich sind.

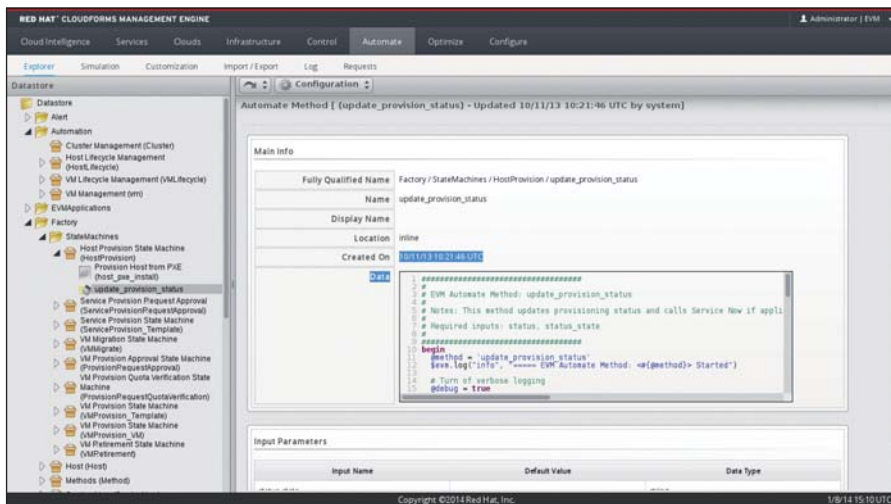


Bild 3: CloudForms stellt eine Vielzahl von vordefinierten Methoden zur Installation neuer Systeme bereit

erweitern. Die Installation eines Systems erfolgt dann beispielsweise über einen Red Hat Network Satellite-Server oder aus einer anderen Installationsquelle heraus.

Ein solcher Installationsprozess durchläuft dabei immer mehrere Phasen. Zuerst ist das Template entsprechend den Anforderungen des Benutzers anzupassen. Dann ist die Anfrage entweder automatisch oder manuell zu verifizieren. Erst danach wird in der letzten Phase der eigentliche Installationsvorgang eingeleitet. In dieser Phase finden auch noch sogenannte Pre-Install und Post-Install Aktionen statt. Hierbei kann der IT-Verantwortliche beispielsweise über eine Pre-Install-Aktion eine Anfrage an ein IP-Address-Management-System (IPAM) stellen, um dem neuen System automatisch eine IP-Adresse zuzuweisen. Eine typische Post-Install-Aktion ist beispielsweise das Versenden einer E-Mail an den Benutzer, der die Installation des neuen Systems initiiert hat, um

diesen über den Abschluss des Prozesses zu benachrichtigen.

CloudForms ist in der Lage, sehr komplexe Service-Dialoge zur Provisionierung von neuen Systemen anzubieten. Diese Dialoge lassen sich selbst zusammenstellen und als Teil eines Service-Katalogs veröffentlichen. So ist ein Benutzer in der Lage, Systeme aus einem Katalog heraus zu installieren. Ein klassischer Use Case stellt beispielsweise virtuelle Systeme mit einer bestimmten Softwareauswahl zur Verfügung. Somit lassen sich leicht Multi-Tier-Systeme erzeugen.

Das Automate-Modul ist sehr vielschichtig und lässt sich individuell anpassen. CloudForms stellt hierfür verschiedene Namespaces zur Verfügung. Diese können Klassen oder wieder andere Namespaces enthalten. Klassen werden durch Schemas definiert und enthalten Attribute, Methoden und Beziehungen zu anderen Klassen-Instanzen.

Anwendungsintegration

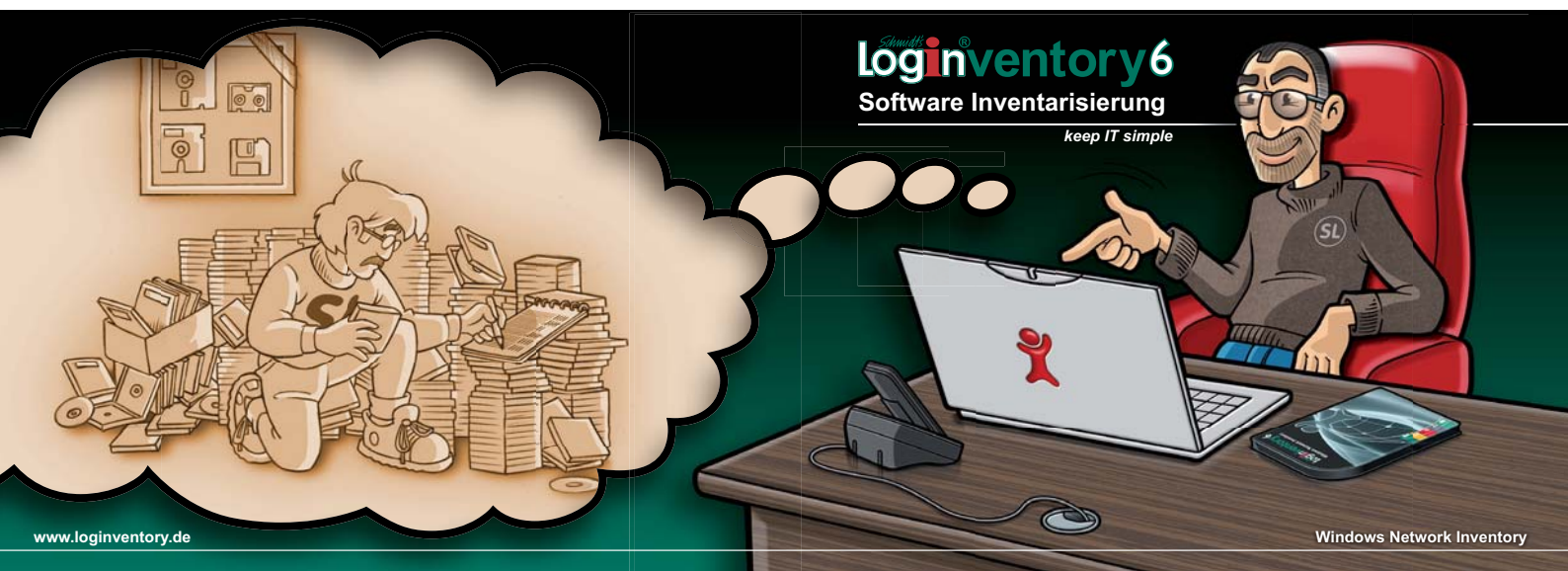
Mit dem Integrate-Modul lässt sich die Integration mit bestehenden Anwendungen erleichtern, indem die CloudForms Management Engine als SOAP Web Service Provider eingesetzt wird. Dies ist beispielsweise sehr hilfreich, wenn eine Inventarisierung der Cloud-Umgebung über ein eigenes Tool stattfinden soll oder wenn die Installation von neuen Systemen mittels eines bereits vorhandenen Provisionierungsframeworks abläuft. Solange die Anwendungen mittels SOAP auf die entsprechenden CloudForms Web-Services zugreifen können, ist eine Integration möglich.

Fazit

CloudForms ist eine umfassende Management-Lösung für hybride Cloud-Umgebungen. Wie kaum ein anderes Produkt vereint es eine Vielzahl von unterschiedlichen Funktionen und unterstützt dabei alle führenden Virtualisierungslösungen. Als OVF-Template für RHEV oder VMware vSphere ist die einfache Installation sichergestellt. Dank des äußerst flexiblen Automatisierungsmodells lassen sich auch komplexe Anforderungen in umfangreichen Cloud-Umgebungen umsetzen. Mit der Integration von OpenStack dürfte das Cloud-Management Framework weiter an Bedeutung gewinnen, da gerade diese Open Source-Lösung immer populärer wird. (jp)

[1] CloudForms-Dokumentation
E3P71

Link-Codes





Workshopserie: Mobile Geräte mit Workplace Join und Web Application Proxy in Windows Server 2012 R2 anbinden (2)

Neue Arbeitsplätze

von Florian Frommherz



Im zweiten Teil des Workshops zu Workplace Join und dem Web Application Proxy binden wir ein Apple iPad ein. Ohne Anwendungen macht das Beitreten des Arbeitsplatzes aber keinen Spaß, weshalb wir sowohl eine Beispielwebseite installieren als auch veröffentlichen.

öffentlichen DNS ein. Dieser zeigt aber nicht auf unseren internen ADFS-Server, sondern auf den Web Application Proxy. Er wird später im Internet veröffentlicht und nimmt Anfragen an den DRS entgegen.

Mit der erfolgreichen Installation von ADFS sind auch alle notwendigen Komponenten für den Device Registration Service installiert. Es bleibt die Aktivierung der Komponente mit der PowerShell. Zuerst erteilen Sie dem Dienstkonto von ADFS Berechtigungen im Active Directory, danach wird der Dienst registriert, um Anfragen von Geräten entgegennehmen zu können. Über das Cmdlet "Initialize-AD-DeviceRegistration" leiten Sie die Vorbereitungen ein. Das Kommando erkundigt sich nach dem Dienstkonto von ADFS, das Sie in der Form "Domäne\Konto\$" angeben, etwa "fabrikam\adfs-2012r2\$" wie zuvor angelegt, mit einem abschließenden \$-Zeichen. Die Konfiguration schließen Sie mit `Enable-AdfsDeviceRegistration` ab. Das System quittiert den Befehl mit einer Erfolgsmeldung, die besagt, dass der Device Registration Service gestartet wurde.

Authentifizierung konfigurieren

Um Geräte authentifizieren zu können und Zugriff anhand von Geräteattributen zu erlauben, ist eine letzte Konfiguration notwendig. Die Authentifizierung der Ge-

räte muss konfiguriert werden. Dazu öffnen Sie die ADFS-Administrationskonsole im Server Manager via "Tools" und wählen "Authentication Policies". Per Klick auf "Edit Global Primary Authentication Policy" in der rechten Spalte der Konsole öffnen Sie ein weiteres Dialogfeld, dessen Checkbox "Enable Device Authentication" Sie aktivieren und mit "OK" bestätigen.

DNS aktualisieren

Alle Clients auf der Suche nach dem Device Registration Service werden nach "enterpriseregistration.fabrikam.com" suchen. Für Geräte innerhalb unseres Netzwerkes muss eine DNS-Zuordnung für "enterpriseregistration" erfolgen, die auf die IP-Adresse unseres ADFS-Servers zeigt. Im DNS der Beispielkonfiguration wird ein neuer CNAME in DNS erstellt, dessen Name "enterpriseregistration" auf den ADFS-Server "adfs-2012r2-1.fabrikam.com" zeigt.

Clients außerhalb unseres Netzwerkes werden später ebenfalls "enterpriseregistration.fabrikam.com" auflösen wollen – hierzu richten Sie einen weiteren CNAME im

Einen Client hinzufügen

Der Dienst ist bereit und alle Komponenten sind an ihrem Platz, um internen Clients den Workplace Join zu ermöglichen. Für einen Funktionstest ziehen wir einen Windows 8.1-Client heran, der nicht zur Domäne hinzugefügt wurde. Der Client muss jedoch in der Lage sein, die interne Domäne "fabrikam.com" auflösen zu können.

Zusätzlich wird dem Client das Root-Zertifikat der Enterprise-CA als "Vertraute Stammzertifikatsstelle" konfiguriert. Hierzu lässt sich der öffentliche Teil des Zertifikats auf ein Netzlaufwerk kopieren, das vom Testclient aus erreichbar ist. Das Zertifikat wird in die Liste der "Vertrauten Stammzertifikatsstellen" aufgenommen.

In der Modern UI-Oberfläche navigieren Sie über das Charms-Menü am rechten Bildschirmrand zu "Settings" und weiter zu "Change PC Settings". Dies wird entweder mit dem Mauszeiger durch Fahren in die rechte untere Ecke erzielt oder auf Touch-Geräten durch Wischen mit dem

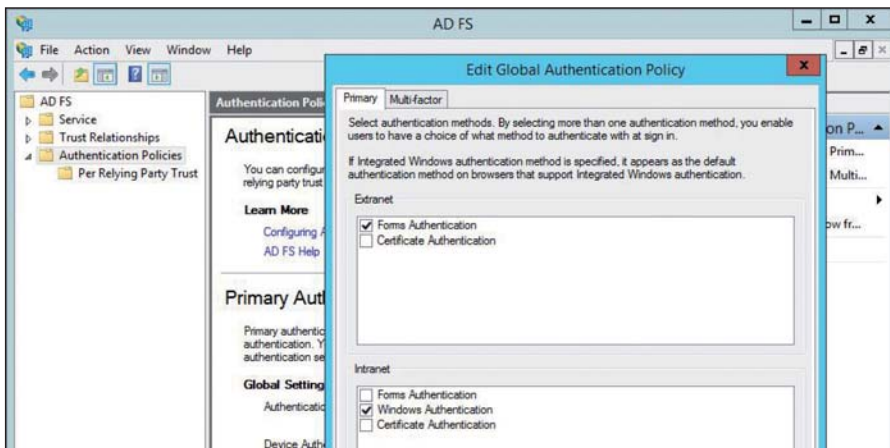


Bild 1: Die Geräteauthentifizierung wird in diesem Teil des Workshops sehr gute Dienste leisten. In ADFS wird sie aktiviert.

Finger vom rechten Bildschirmrand aus zur Mitte. In der Einstellungskonfiguration kann links im Menü "Network" gewählt werden, worauf im Folgemenu der Eintrag "Workplace" den richtigen Konfigurationsort beherbergt. Die Maske verlangt das Eingeben der Firmen-E-Mailadresse und einen Klick auf "Join". Durch die eingetragene E-Mailadresse ist der Client in der Lage, die richtige Domäne für Workplace Join zu finden. Für einen Test geben wir also die E-Mailadresse "dave@fabrikam.com" ein und bestätigen mit "Join". Aus der eingegebenen E-Mailadresse wird lediglich der Domänenteil für die Suche nach ADFS verwendet, es werden keine E-Mails oder Bestätigungen generiert – auch eine Mailbox zu dieser Adresse muss nicht existieren.

Wurde ADFS kontaktiert, öffnet der Client eine Anmeldemaske, mit der sich Benutzer am Active Directory und am Device Registration Service anmelden müssen. Auf dieser Seite werden AD-Anmeldeinformationen verlangt, mit denen der Benutzer später Zugriff auf Ressourcen erhalten will. Die E-Mailadresse des vorherigen Dialogs ist bereits als Voreingabe hinterlegt. Per Klick auf "OK" vollzieht der Nutzer den Workplace Join. Nach wenigen Sekunden sollte der Dialog die Erfolgsmeldung anzeigen, dass das Gerät erfolgreich zur IT-Infrastruktur hinzugefügt wurde.

Fehlersuche am Client

Für eine Fehleranalyse existiert auf Windows-Clients ein spezielles Eventlog, das bei Problemen zu Rate gezogen werden kann. Dort navigieren Sie über "Application

and Service Logs" und "Microsoft" zur Windows-Baumstruktur. Nahezu am Ende der Liste der Logs befindet sich das Workplace Join-Log. Fehler und weitere Informationen, wenn das Hinzufügen eines Geräts nicht funktioniert hat, finden Sie dort. Schlägt Workplace Join für ein Gerät fehl, sind alle wichtigen Informationen dort zu finden – meist ist der Dienst nicht via DNS auflösbar oder das Zertifikat ist im Fall von nicht öffentlich vertrauten Zertifikaten für das Zielgerät unbekannt.

Eine weitere Fehlerquelle gerade bei Enterprise-CAs ist häufig, dass der Client den Revocation-Server nicht erreichen und das Zertifikat überprüfen kann. Workplace Join besteht zwingend darauf, das Zertifikat prüfen zu können. Für Produktionsumgebungen nicht praktikabel, für ein Testlab zur Funktionsüberprüfung aber durchaus akzeptabel ist die Deaktivierung der Revokationslisten-Überprüfung in den Einstellungen des Internet Explorers. Im Tab "Advanced" befinden sich unter "Security" die Einstellungen "Check for publisher's certificate revocation" und "Check for server certificate revocation". Beide Einstel-

lungen werden deaktiviert und nach einem Neustart des Computers wirksam.

Bei erfolgreicher Verbindung des Gerätes zur IT-Infrastruktur kann auch das Active Directory-Objekt für das Gerät überprüft werden. Hierzu öffnen Sie die Active Directory-Benutzer und -Computer-Konsole. Hier stellen Sie sicher, dass die "Advanced Features" unter "View" aktiviert werden. Anschließend ist unter dem Domänenobjekt ein Container namens "Registered Devices" zu erkennen. Unterhalb dieses Containers werden alle registrierten Geräte aufgelistet – als Objekte mit einer eindeutigen Kennung. Beim Aufrufen eines der Objekte und der genaueren Betrachtung der Attribute erkennen Sie die folgenden Informationen: Der Gerätenamen ist unter "displayName" zu finden, der Benutzer, der das Gerät hinzugefügt hat, ist unter "msDS-RegisteredUsers" aufgeführt. Das Betriebssystem des Gerätes ist in "msDS-DeviceOSType" gespeichert, dessen Version in "msDS-DeviceOSVersion".

Mit iOS-Geräten beitreten

Für iOS-Geräte existiert für einen Unternehmensbeitritt keine Standardfunktion im Betriebssystem, sodass ein Beitrittsprofil über den Webbrowser installiert wird. Mit Hilfe von Safari wird die Profilverwaltungsseite auf ADFS geöffnet (<https://adfs-2012r2.fabrikam.com/enrollmentserver/ota-profile>). ADFS öffnet eine Eingabemaske, in die Benutzername und Passwort des im AD hinterlegten Nutzers in der Form "dave@fabrikam.com" eingegeben werden. Ist der Benutzer authentifiziert, leitet ADFS an die Registrierungsseite weiter, die die Installation eines Zertifikatsprofils auf dem iPad lanciert. Automatisch öffnet sich das iPad-Kontrollzentrum, das um die Erlaubnis für die Zertifikatsinstallation fragt. Mit ei-

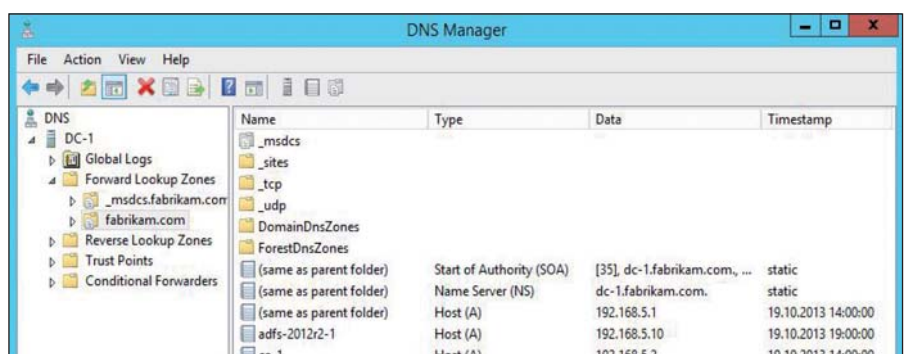


Bild 2: Es kann losgehen: Die DNS-Einträge für den Device Registration Service zeigen auf den ADFS-Server

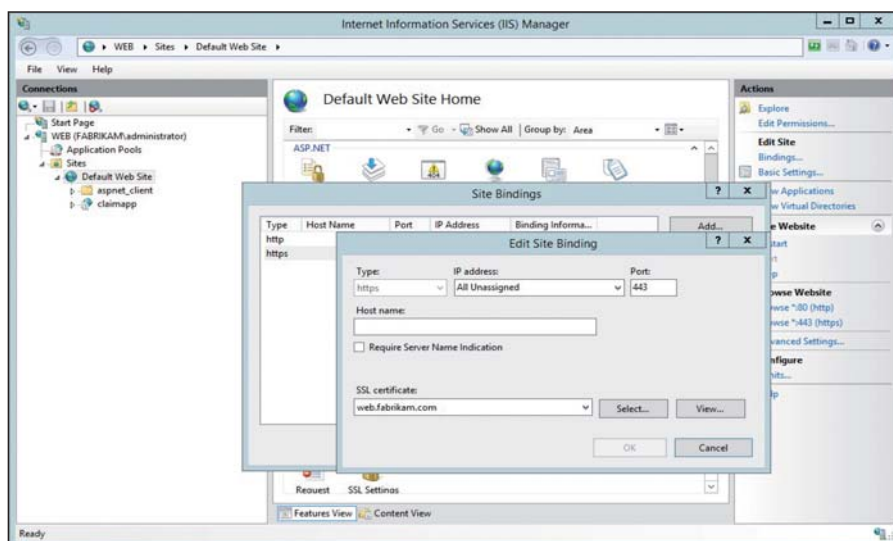


Bild 3: Der Webserver erhält sein eigenes SSL-Zertifikat, das für die Standardwebseite konfiguriert wird

nem Fingertipp auf "Install" und anschließend auf "Install Now" wird das Zertifikat auf dem iPad aufgebracht. Das Gerät ist nun zum Workplace hinzugefügt worden – inklusive Referenzobjekt im "Registered Devices" Container im Active Directory.

Eine Webseite aufsetzen

Nachdem mobile Geräte dem Arbeitsplatz beitreten können, wird es Zeit, den Mehrwert des Beitritts aufzuzeigen. Um Zugriffsszenarien zu konfigurieren, wird eine Webanwendung im Backend benötigt. Entgegen der üblichen "Hello World"-Beispielanwendungen stellen wir an dieser Stelle eine claimsbasierte Anwendung bereit. Die Anwendung ist simpel und stellt alle Claims eines Benutzers tabellarisch dar. Nicht spektakulär, im Vergleich zu "Hello World" allerdings in zweierlei Hinsicht sinnvoll: Einerseits lassen sich damit die korrekte Konfiguration von ADFS und die erfolgreiche Federierung mit Webseiten kontrollieren, andererseits bietet die Seite einen Überblick zu allen verfügbaren Claims des gerade angemeldeten Benutzers in Verbindung mit seinem Gerät.

Der Server, der die Claims-Anplikation hosten soll, wird über den Servermanager mit der Webserver (IIS)-Rolle bestückt. In der Auswahl der zusätzlichen Features des Server Managers wählen Sie dazu im Wizard "Windows Identity Foundation 3.5" aus. Für die Installation der Claims-Anwendung sollten Sie sicherstellen, dass unter "Application Development" die Komponente "ASP.NET 4.5" installiert

ist sowie unter "Security" die "Windows Authentication" als IIS-Komponenten zur Verfügung stehen.

Auch der Webserver wird für gesicherte Kommunikation konfiguriert, indem die Enterprise-CA ein SSL-Zertifikat mit dem Namen des Webserver ("web.fabrikam.com") anfordert. In der IIS-Verwaltungskonsolle wird das Zertifikat dann für die "Default Web Site" konfiguriert.

Die Claims-Anwendung selbst ist Teil des Windows Identity Foundation SDKs [1], das Microsoft frei zum Download anbietet. Es existiert in zwei Versionen, wobei wir die aktuelle Version 4.0 für die Beispieleinrichtung nutzen. Das SDK kann auch auf einem anderen Rechner als dem Webserver installiert werden, da nur die Quelldaten der Claims-Anwendung benötigt werden. Nach Abschluss der Installation des SDKs liegen diese im Verzeichnis "C:\Program Files (x86)\Windows Identity Foundation SDK\v4.0\Samples\Quick Start\Web Application\PassiveRedirectBasedClaimsAwareWebApp". Das komplette Verzeichnis kopieren Sie auf den Webserver nach "C:\inetpub" und benennen es anschließend um, sodass unter "C:\inetpub\wwwroot\claimapp" die Anwendungsdaten zu finden sind. Per Rechtsklick auf "claimapp" in der IIS-Administrationskonsole lässt sich eine Webanwendung daraus erstellen.

Für die Test-Einsatzzwecke wird die Applikation weiter konfiguriert, indem Sie

im Verzeichnis der Anwendung die Datei *Default.aspx.cs* mit Notepad öffnen. Sie enthält Teile des Programmcodes der Webanwendung. Um die relevanten Daten anzeigen zu können, bedarf die Datei einer Modifikation. Die Zeile "WriteClaim (claim, table);" ist von einer Abfrage und zwei geschweiften Klammern umschlossen. Die Zeile der "if"-Abfrage sowie die Zeilen der geschweiften Klammern werden mit zwei Slashes auskommentiert – jede dieser drei Zeilen startet dann mit "//".

Die Datei *web.config* im gleichen Verzeichnis modifizieren wir ebenfalls. Hier entfernen Sie die Sektion "IdentityModel", die mit "<microsoft.identityModel>" beginnt und mit "</microsoft.identityModel>" endet. In der Datei *TrustedIssuer-NameRegistry.cs*, die sich im Unterverzeichnis "App_Code" befindet, kommentieren Sie die Zeile "using Microsoft.IdentityModel.Tokens;" aus – ebenfalls mit zwei Slashes vor "using", also "//using Microsoft.IdentityModel.Tokens;".

Als letzten Schritt passen wir den Application Pool des IIS an, sodass die Federierung funktionieren kann. In der IIS-Verwaltungskonsolle wählen Sie im Knoten "Application Pool" den Punkt "Default-AppPool" aus. Per Rechtsklick und "Advanced Settings" öffnen Sie die erweiterten Einstellungen des Pools, wo Sie in der Kategorie "Process Model" die Einstellung "Load User Profile" auf "True" setzen. Der Wert steht per Vorgabe auf "False".

Fazit

Die Basiskonfiguration von Workplace Join und der Gerätereistration haben wir mittlerweile vollzogen und verifiziert. Mit dieser Konfiguration lassen sich weitere, komplexere Webanwendungen des Unternehmens flexibel veröffentlichen. Wie dies funktioniert und wie Sie die Single Sign-On-Funktionen nutzen, die WAP und ADFS in Windows Server 2012 R2 bietet, zeigt der abschließende Workshopteil. (jp)

[1] Windows Identity Foundation SDK
E3P91

Link-Codes



IT-Administrator Sonderhefte

Je **180 Seiten**
geballtes Wissen zu:



Abonnenten erhalten
Sonderhefte zum Vorzugspreis!

www.it-administrator.de/kiosk/sonderhefte/



Workshop: Mit TeamDrive eine Private Cloud betreiben

Auf Wolke sieben

von Thomas Joos



Quelle: Jorge Alcaraz Fernández – 123RF

Wenn Sie mobilen Anwendern die Möglichkeit geben wollen, Daten untereinander auszutauschen, ist nicht unbedingt eine große Lösung wie SharePoint vonnöten. So etwa stellt TeamDrive [1] eine gute Alternative zu kommerziellen Produkten dar.

Wir haben TeamDrive für diesen Workshop mit Windows 8.1 und Server 2012 R2 eingesetzt, Sie können die Software also in Netzwerken mit den neuesten Microsoft-Betriebssystemen nutzen. Dabei ist es möglich, TeamDrive Personal Server auf Computern mit Windows 7/8 zu installieren sowie auf virtuellen Servern mit Windows Server, Linux und auch auf MacOS. Hier haben Sie also fast freie Auswahl, was die Flexibilität deutlich erhöht.

Datenaustausch auf allen Wegen

Sie können TeamDrive auf zwei verschiedenen Arten nutzen. Zunächst besteht die Möglichkeit, dass die Anwender einen speziellen Client herunterladen und installieren. Nach einer Registrierung können die Nutzer dann untereinander Daten austauschen. Deren Ablage erfolgt aller-

dings in der Public Cloud, also direkt beim Anbieter. Es stehen bis zu 2 GByte kostenloser Speicher zur Verfügung sowie Clients für alle relevanten Betriebssysteme (Windows, Linux und MacOS) und mobilen Geräte (iOS und Android) außer Windows Phone. Die Informationen werden beim Hochladen auf den Server mit einer AES 256-Verschlüsselung gesichert. So sollte selbst in der Public Cloud niemand außer dem Nutzer selbst die Daten lesen können.

Die zweite Möglichkeit ist der Betrieb eines eigenen Servers. Hier stellen die Entwickler den Personal Server zur Verfügung. Diesen können Sie im Netzwerk als Server betreiben und als Systemdienst starten. Der Personal Server ist bis zu einem Datenvolumen von 10 GByte kostenlos und lässt sich kostenpflichtig weiter ausbauen. Außerdem besteht die Möglichkeit, beide Modelle parallel einzusetzen. Das heißt, Anwender können mit dem Server in ihrem Unternehmen arbeiten, aber auch mit dem Cloud-Speicher im Internet. Die Anbindung erfolgt über das gleiche Client-Programm und stellt sich identisch dar. Wir zeigen Ihnen im Rahmen dieses Workshops beide Möglichkeiten.

Der Austausch von Daten zwischen Anwendern ist in Unternehmen heute gang und gäbe und sollte unabhängig vom Standort der Nutzer funktionieren. Hierzu bieten sich Cloud-Dienste wie OneDrive, Dropbox oder Google Drive an. Allerdings haben all diese Dienste das Problem, dass sich die Informationen nicht mehr in der Hoheit des Unternehmens befinden. Um ungewollten Datenzugriffen einen Riegel vorzuschieben, bietet sich mit TeamDrive ein kostenloses Werkzeug an. Wir stellen Ihnen in diesem Workshop die wichtigsten Funktionen vor und erklären, wie Sie die nötige Client/Server-Konstruktion aufsetzen und betreiben.

Auf den Personal Servern – die Anbindung mehrerer Personal Server ist möglich – legen Sie virtuelle Ordner, Spaces genannt, an. Zusätzlich können Sie unterhalb dieser Spaces noch Unterordner anlegen. Für alle Verzeichnisse lassen sich umfassende Rechte festlegen, sodass jeder Nutzer nur die Rechte erhält, die er auch wirklich benötigt. Wir zeigen Ihnen nachfolgend, wie Sie Client und Server einrichten und miteinander verbinden.

TeamDrive-Server installieren

Um TeamDrive als Private Cloud zu verwenden, benötigen Sie zunächst einen Server, auf dem Sie den Server-Part [2] installieren. Wir gehen nachfolgend auf die Installation auf einer Maschine mit Windows Server 2012 ein. Sie können den Server aber auch auf PCs ab Windows XP aufspielen. Ferner stehen Installationsdateien für Linux und MacOS zur Verfügung. Wollen Sie mehr als 10 GByte auf dem Server speichern, müssen Sie durch die Eingabe einer Lizenznummer kostenpflichtig mehr Speicherplatz freischalten. Für unbegrenzten Speicherplatz müssen Sie mit rund 100 Euro pro Jahr rechnen. Verwenden Sie nur den Cloud-Speicher direkt beim Anbieter, können Sie auch hier mehr Volumen als die kostenlosen 2 GByte dazubuchen.

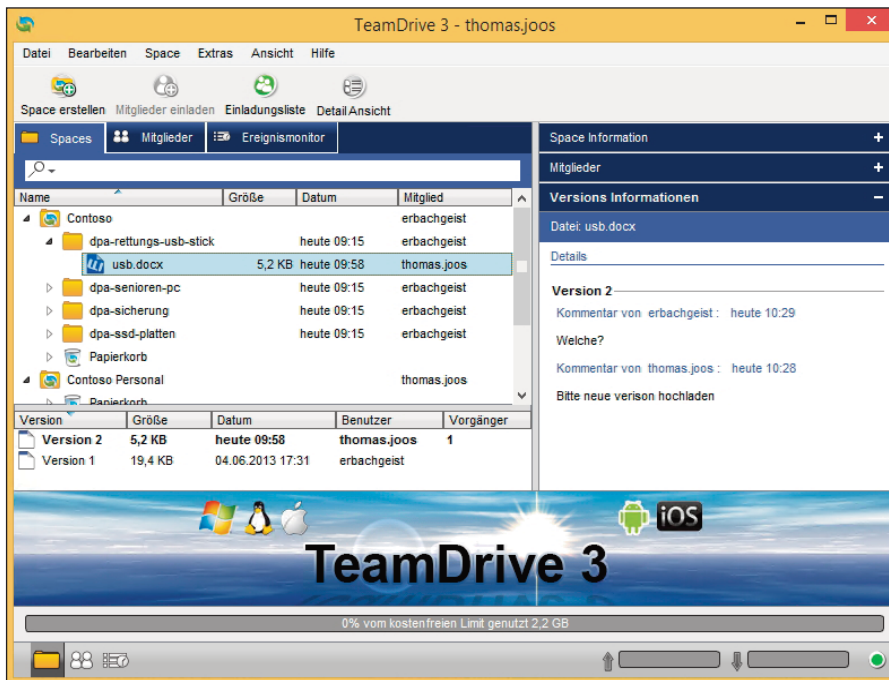


Bild 1: Mit dem TeamDrive-Client können Anwender auf mehrere Server zugreifen, auch auf öffentliche und private gleichzeitig

Die Installation des Servers ist in wenigen Schritten abgeschlossen. Die eigentliche Einrichtung nehmen Sie erst danach vor. Starten Sie dazu das Verwaltungsfenster. Im ersten Schritt klicken Sie auf die Schaltfläche "Konfigurationsdatei" unten im Fenster. Hier nehmen Sie maßgebliche Einstellungen für die Verbindung zum Server vor. Im Grunde genommen reicht es aus, wenn Sie den Hostnamen oder die IP-Adresse für den Server sowie das Kennwort für die Verbindung festlegen. Geben Sie den Namen oder das Präfix "http" ein, es genügt der FQDN oder die IP-Adresse. Achten Sie darauf, dass der Port für den Zugriff auf den Personal Server in der Firewall des Servers freigeschaltet sein muss. Damit auch Clients aus dem Internet auf den Server zugreifen können, müssen Sie in der externen Firewall des Unternehmens eine Weiterleitung zum entsprechenden TeamDrive-Server einrichten – hierzu später noch mehr.

Das Kennwort für den Zugriff auf den Server speichert der Assistent verschlüsselt als MD5-Hash in der Konfigurationsdatei. Die Daten lassen sich daher nicht ohne Weiteres auslesen. Die weiteren Einstellungen sind bereits ausreichend, lassen sich aber jederzeit anpassen. Die kleinste Größe für ein Repository (Space) sind 10 MByte. Diese lässt sich in den Konfigurationsein-

stellungen aber anpassen. Achten Sie jedoch darauf, nicht das lizenzierte Volumen zu überschreiten.

Sie legen im Verwaltungsfenster auch die maximale Anzahl an Verbindungen fest, die der Server zulässt. "Poll-Intervall" steuert, wie oft Clients nach Aktualisierungen auf dem Server suchen. "Connection Timeout" legt fest, wann der Server eine Verbindung zum Client schließt, wenn keine Anfragen des Clients mehr auf dem Server eingehen. Mit "Put-Verify-Timeout" bestimmen Sie, wie lange der MD5-Check dauern darf, den der Server beim Hochladen von Dateien durchführt.

Haben Sie die Einstellungen festgelegt, klicken Sie nun auf

"Speichern". Immer wenn Sie an dieser Stelle eine Änderung vornehmen, müssen Sie den Systemdienst für den Server neu starten. Haben Sie alle Einstellungen vorgenommen, können Sie den Personal Server nutzen. Durch die Option "Als Dienst ausführen" legen Sie fest, dass der Assistent einen Systemdienst erstellt, über den der Server auch startet. Zudem können Sie im Fenster zur Steuerung des Servers den Dienst jederzeit beenden.

Der Systemdienst des Personal Server trägt die Bezeichnung "TeamDrive Personal Server". In der Befehlszeile beenden Sie ihn mit `net stop teamdrive_ps` und starten ihn mit `net start teamdrive_ps`. Wenn Sie den Server auf einem Linux-Rechner installieren, sollten Sie vor der Aktivierung des Servers einen neuen Benutzer für TeamDrive anlegen. Der Server darf nicht mit dem Benutzer "root" verbunden sein.

Betreiben Sie den TeamDrive-Server auf einem Windows-Rechner, müssen Sie eine neue Firewall-Regel erstellen, damit

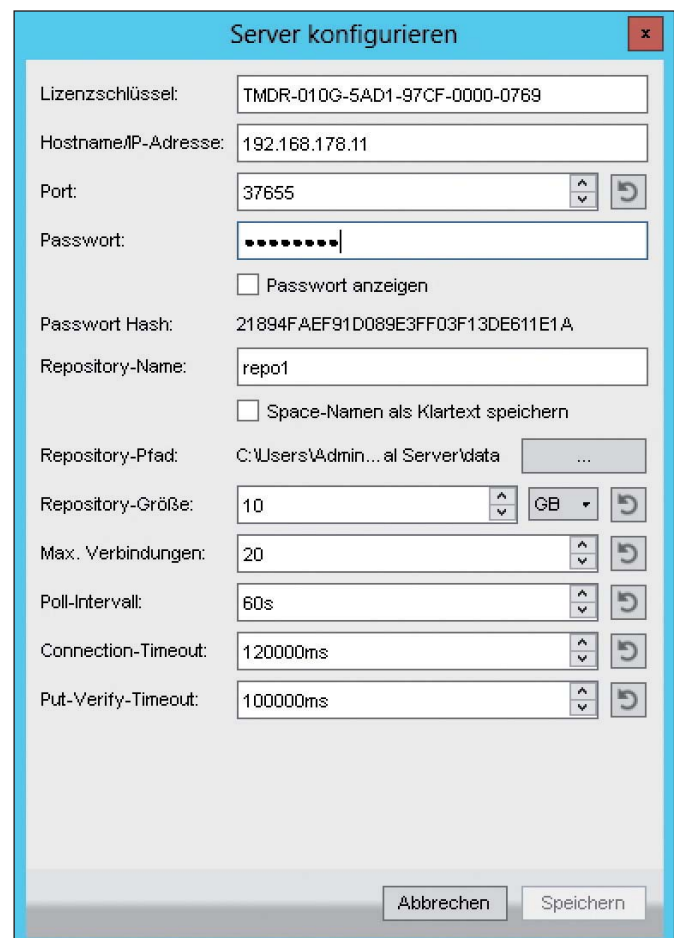


Bild 2: Vor der Verwendung von TeamDrive Personal Server passen Sie den Server an Ihre Bedürfnisse an



sich die Clients verbinden können. Starten Sie dazu die erweiterte Verwaltung der Windows-Firewall mit *wf.msc*. Erstellen Sie eine neue Regel für eingehenden Datenverkehr und verwenden Sie "Port" als Option. Tragen Sie hier den entsprechenden Port ein, lassen Sie den Zugriff zu und geben Sie der Regel einen passenden Namen.

Konfiguration speichern und wieder einspielen

Die Protokolldatei mit den Systemänderungen des Servers öffnen Sie ebenfalls über die Verwaltungsoberfläche von TeamDrive. Die Einstellungen des Servers sind in der Datei *tdps.config* gespeichert. Diese können Sie direkt in der Verwaltungsoberfläche öffnen. Es ist zu empfehlen, dass Sie die Datei bei Änderungen sichern. Müssen Sie den Server neu installieren, können Sie Ihre Einstellungen einspielen, indem Sie die Steuerungsdatei auf den Server kopieren. Standardmäßig befindet sich die Datei in folgenden Verzeichnissen, abhängig vom Betriebssystem, auf dem Sie den Personal Server installieren:

- Windows XP: C:\Dokumente und Einstellungen \ Benutzernamen \ Anwendungsdaten \ TeamDrive Personal Server
- Windows Vista/7/8: C:\Users \ Benutzernamen \ AppData \ Roaming \ TeamDrive Personal Server
- Mac OS X: /Users / Benutzernamen / TeamDrive PersonalServer
- Linux: Hauptverzeichnis des TeamDrive Personal-Servers

Im Verzeichnis "data" der Personal Server-Installation befinden sich die Spaces aller Benutzer, die mit dem Server synchronisiert sind. Daher sollten Sie auch dieses Verzeichnis sichern. Um die Daten wiederherzustellen, können Sie das Verzeichnis dann einfach überschreiben. Der Speicherort der Daten ist in der Konfigurationsdatei *tdps.config* festgelegt. Bearbeiten Sie die Datei nie mit einem Texteditor, sondern nur in der Verwaltungsoberfläche des Servers. Generell sollten Sie darauf achten, das Repository, also die Spaces-Daten auf dem Server, auf einer lokalen Festplatte zu speichern. Verwenden Sie kein Netzlaufwerk, da ansonsten die Stabilität des Servers und die Leistung beeinträchtigt werden kann.

Clients an den Personal Server anbinden

Haben Sie bisher alle Einstellungen wie beschrieben vorgenommen, ist der Server bereit für eine Verbindung mit den Clients. Dazu müssen natürlich die Anwender zunächst die Client-Software auf dem PC oder dem mobilen Gerät installieren und einrichten:

1. Starten Sie die Client-Software und klicken Sie auf "Extras / Einstellungen".
2. Wechseln Sie zu "Hostserver" und wählen unten im Fenster "Personal Server hinzufügen".
3. Geben Sie einen Namen für den Server und bei "TDPS-Passwort" das Kennwort des Servers ein, das Sie bei dessen Einrichtung festgelegt haben. Ändern Sie das Kennwort auf dem Server, haben Anwender erst dann wieder Zugriff, wenn sie das neue Kennwort im Client eintippen.
4. Tragen Sie bei "TDPS-URL" die Adresse des Servers in der Form *http://Servername oder IP-Adresse* ein. Verwenden Sie hier die gleiche Adresse oder den Namen, den Sie auch in der Konfiguration des Servers eingegeben haben.
5. Überprüfen Sie, ob der Port, der im Client eingetragen ist, dem Port auf dem Server entspricht. Auf dem Server muss in der lokalen Firewall der Port erlaubt sein. Bei der Anbindung über

das Internet müssen Sie die Anfragen von der externen Firewall zum TeamDrive-Server weiterleiten.

Um die Anbindung zu überprüfen, klicken Sie auf der Registerkarte "Spaces" des Servers auf den Space, der den Personal Server darstellt. Wenn Sie hier keine Verbindung herstellen können, erhalten Sie eine entsprechende Meldung und das Icon zeigt einen Fehler an. Überprüfen Sie in diesem Fall die Settings der Firewall auf dem Server. Auf dem Client müssen Sie normalerweise keine Einstellungen in der Firewall ändern, außer Sie haben eine besonders sichere Firewall im Einsatz.

TeamDrive für Anwender

Wenn Sie Clients an den Server angebunden haben, können diese bereits Daten untereinander austauschen. Der Austausch zwischen Client und Personal Server findet über eine 256 Bit AES Ende-zu-Ende-Verschlüsselung statt. Nachdem die Client-Software installiert, aktiviert und gestartet ist, können Nutzer im bereits vorhandenen Space Daten hochladen oder selbst Spaces auf dem Server anlegen. Spaces erstellen Sie in der Verwaltungsoberfläche über die Schaltfläche "Spaces erstellen". Im neuen Fenster geben Sie den Namen des Space

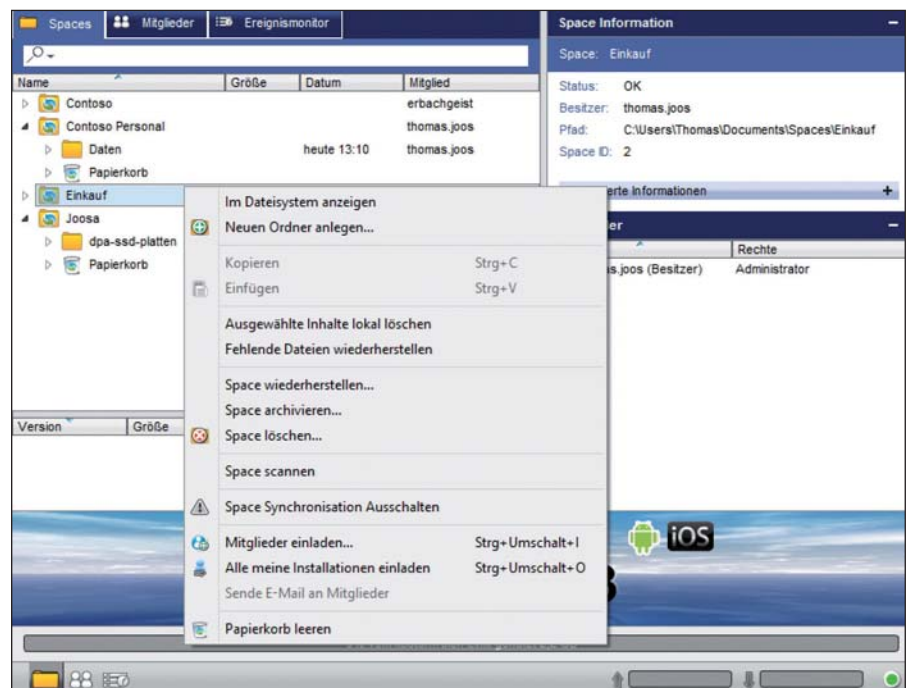


Bild 3: Über Spaces tauschen Anwender untereinander Daten aus. Für den Zugriff lassen sich andere Anwender einladen, um gemeinsam an Dokumenten zu arbeiten.

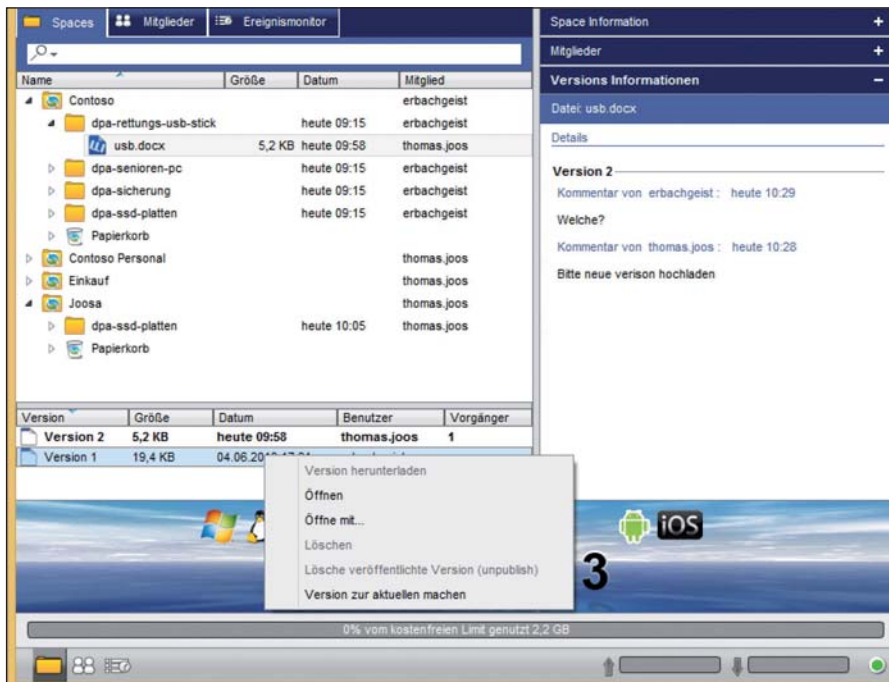


Bild 4: TeamDrive unterstützt mehrere Versionen für Dokumente und erlaubt Anwendern auch das Schreiben von Kommentaren für Dokumente

an, wo dessen Daten abgelegt sein sollen und wie viele Versionen von gespeicherten Dateien Sie zulassen wollen. Sie haben ferner die Möglichkeit, vorhandene Ordner zu Spaces zu deklarieren.

Daten kopieren Sie entweder über den Explorer oder den TeamDrive-Client auf den Space. Unterhalb eines Space können Sie Unterordner anlegen. Daten, die sich auf dem Server und dem Client befinden, werden automatisch synchronisiert. Über das Menü "Extras" können Sie die Synchronisierung beenden. Spaces verwalten Sie über das Kontextmenü der Registerkarte "Spaces". Hier binden Sie oder auch die Anwender selbst über die Option "Mitglieder einladen" andere Nutzer mit installierten TeamDrive-Clients an den Space an. Es spielt keine Rolle, wo der Space gespeichert ist, der Zugriff erfolgt immer über den TeamDrive-Client. Vorgänge auf dem Client können Sie auf der Registerkarte "Ereignismonitor" verfolgen. Hier sind alle Systemvorgänge der Clients zu sehen.

Beim Hinzufügen neuer berechtigter Anwender können Sie entweder die E-Mail-Adresse oder den TeamDrive-Mitgliedernamen für bereits registrierte Benutzer auswählen. Klicken Sie auf "Hinzufügen", um den Anwender in die Liste aufzuneh-

men. Sie können über diesen Weg auch mehrere Benutzer aufnehmen. Für jeden Anwender legen Sie fest, welche Rechte er für den Space hat. Sie können Anwendern das Recht zum Schreiben, Lesen und Administrator-Rechte zuweisen.

Tritt ein Anwender einem Space bei oder trifft eine Einladung ein, erscheint eine Nachricht im TeamDrive-Client. Es besteht jederzeit die Möglichkeit, Einladungen für einen Space zurückzunehmen und Rechte zu ändern. Dazu klicken Sie auf dem Client auf den entsprechenden Space und mit der rechten Maustaste auf das Mitglied. Laden Sie andere TeamDrive-Benutzer zu Spaces ein, können Sie bereits bei der Einladung festlegen, welche Rechte die Anwender erhalten sollen. Auch nach der Einladung können Sie in der Oberfläche jederzeit die Einstellungen anpassen. Über "Extras / Einstellungen" finden Sie auf der Registerkarte "Rechteverwaltung" die einzelnen Rollen, die Sie Anwendern zuweisen können.

Versionierung und Kommentarfunktion

TeamDrive speichert verschiedene Versionen von Dokumenten, ähnlich wie SharePoint. Wenn Anwender ein Dokument bearbeiten und ändern, legt TeamDrive automatisch eine neue Version an.

Wie viele, hängt von den Einstellungen des Spaces ab. Klicken Nutzer auf ein Dokument, sind im TeamDrive-Explorer die verschiedenen Versionen zu sehen. Über das Kontextmenü lassen sich die Dokumente ganz löschen oder ein älterer Stand zur aktuellen Version machen, wenn bestimmte Änderungen nicht gewünscht sind. Bei den Versionen ist stets zu sehen, welcher Benutzer die Änderung in der Version durchgeführt hat. Modifikationen können natürlich nur Anwender vornehmen, die entsprechende Rechte besitzen.

Über das Kontextmenü von Dokumenten können Anwender Kommentare schreiben. Diese erscheinen im rechten Bereich des Fensters, wenn ein Dokument angeklickt wird. Außerdem erhalten die Anwender des Spaces eine Benachrichtigung über den Kommentar. Über diesen Weg können Anwender miteinander kommunizieren und Informationen zu Versionen und den Dokumenten austauschen. Die Bedienung des Clients und das Erstellen von Versionen und Kommentaren erfolgt weitgehend intuitiv. Außerdem informiert der Client die Anwender über alle Arten von Änderungen und wer diese durchgeführt hat.

Fazit

Mit TeamDrive Personal Server bauen sich Unternehmen einen einfachen und effizienten eigenen Cloud-Speicher auf. Der leichte und sichere Datenaustausch steht dabei im Fokus. Auch zur Datensicherung wichtiger Daten von mobilen Clients ist die Anwendung geeignet. Im Gegensatz zu Lösungen wie OwnCloud bietet TeamDrive jedoch keine gemeinsamen Kontakte oder Kalender. Organisationen, die auf der Suche nach einem stabilen und sicheren Private Cloud-Speicher sind, sollten sich TeamDrive ansehen. Ein Test kostet nichts und der Nutzen ist gerade im Hinblick an die mögliche Anbindung diverser Endgeräte enorm. (ln)

[1] Homepage TeamDrive
E2P61

[2] Download TeamDrive Personal Server
E2P62

Link-Codes





Workshopserie: Dateiverwaltung mit dem Ressourcen-Manager für Dateiserver in Windows Server 2012 R2 (2)

Daten an der kurzen Leine

von Thomas Joos

Quelle: anyka – 123RF



Mit einem installierten Ressourcenmanager für Dateiserver unter Windows Server 2012 R2 haben wir im ersten Teil dieser Workshopserie zunächst Daten-Kontingente für die Anwender eingerichtet. Der zweite Teil zeigt nun auf, wie FSRM dabei hilft, für Sicherheit im Unternehmen zu sorgen, indem wir die Verwendung und Speicherung bestimmter Dateitypen unter unsere Kontrolle bringen.

Sie können mit dem Ressourcen-Manager Berichte erstellen, die die Nutzung der Freigaben und Ordner anzeigen. Dazu nutzen Sie den Eintrag "Speicherberichteverwaltung" in der Konsolenstruktur von FSRM. Wenn Sie diesen mit der rechten Maustaste anklicken, stehen Ihnen verschiedene Optionen zum Erstellen der Berichte zur Verfügung. Sie können einen Zeitplan definieren, nach dem ein Bericht regelmäßig erstellt werden soll oder Sie fertigen einen manuellen Bericht an. Dazu stehen Ihnen verschiedene Berichtsdaten und Formate zur Verfügung.

Speicherberichte verwalten

Ein Bericht kann zum Beispiel alle doppelt vorhandenen Dateien auf einem Laufwerk oder auf einem Server identifizieren. So lässt sich Speicherplatz schnell freigeben, ohne dass Daten verloren gehen. Sie können einen Bericht für Dateien nach Dateigruppen ausführen, um zu identifizieren, wie Speicherressourcen zwischen verschiedenen Dateigruppen aufgeteilt sind. Oder Sie erstellen einen Bericht für Dateien nach Besitzer, um zu analysieren, wie einzelne Benutzer die gemeinsamen Speicherressourcen verwenden.

Jeder Bericht kann ein eigenes Format besitzen. Sie können zum Beispiel regelmäßige HTML-Berichte und Abteilungsberichte erstellen, die den Abteilungsleitern einen Überblick über den aktuellen Speicherbedarf verschaffen. Durch die Speicherberichte können Sie sich ferner per E-Mail regelmäßig einen Überblick über den aktuellen Stand der Dateiserver verschaffen. Um einen Speicherbericht zu erstellen, klicken Sie mit der rechten Maustaste auf "Speicherberichteverwaltung" und dann auf "Neue Berichtsaufgabe planen". Klicken Sie im Dialogfeld auf der Registerkarte "Bereich" auf die Schaltfläche "Hinzufügen" und wählen Sie die Volumes und/oder Ordner aus, für die Berichte generiert werden sollen. Selektieren Sie im Bereich "Berichtsdaten" auf der Registerkarte "Einstellungen" per Klick auf das entsprechende Kontrollkästchen die Berichte, die Sie generieren möchten. Um die Einstellungen eines Berichts anzupassen, markieren Sie diesen und klicken Sie auf die Schaltfläche "Parameter bearbeiten".

Dateitypen kontrollieren

Bislang haben wir uns mit der Frage nach dem Speicherbedarf beschäftigt und Nutzer darin pauschal eingeschränkt. Ein weiterführender Ansatz ist das Erlauben oder

Verbieten bestimmter Dateitypen. Über den Eintrag "Dateiprüfungsverwaltung" erstellen Sie Dateiprüfungen für Ordner. Mit diesen steuern Sie, welche Dateitypen von Benutzern gespeichert werden können. Allerdings ist die Prüfung nicht sehr effizient, da sie nur die Dateieindung zur Prüfung nutzt. Ändern Anwender die Dateieindung, erkennt die Dateiprüfungsverwaltung dies nicht.

So stellen Sie mit der Dateiprüfung einerseits sicher, dass keine Musikdateien, Bilder oder Videos in persönlichen Ordnern auf einem Server gespeichert werden, können jedoch die Speicherung bestimmter Arten von Mediendateien zulassen, die die Rechteverwaltung unterstützen oder den Unternehmensrichtlinien entsprechen. Speziellen Anwendern im Unternehmen lassen sich dagegen besondere Privilegien zum Speichern beliebiger Dateien in ihrem persönlichen Ordner gewähren. Mit diesem Feature von FSRM untersagen Sie also Ihren Anwendern das Speichern bestimmter Dateitypen wie MP3, MPEG oder WMV. Versucht ein Anwender eine solche Datei zu speichern, können Sie Benachrichtigungen konfigurieren, die automatisch verschickt werden. Eine weitere Einsatzmöglichkeit ist die Prüfung auf bestimmte Dateitypen, die Sie im Unternehmen ein-



setzen. So können Sie zum Beispiel untersagen, dass Anwender Excel-Tabellen, die unter Umständen geheime Informationen enthalten, in öffentlichen Laufwerken speichern.

Klicken Sie in FSRM den Eintrag "Dateiprüfungen" mit der rechten Maustaste an, können Sie eine neue Dateiprüfung erstellen. Ähnlich wie bei den Kontingenten legen Sie einen Pfad fest, auf dem die Dateiprüfung aktiviert ist. Sie können die Prüfung anhand einer Vorlage anlegen oder eine benutzerdefinierte Prüfung einrichten. In beiden Fällen können Sie konfigurieren, dass die Anwender daran gehindert werden, die Dateien zu speichern (aktive Prüfung). Sie können den Nutzern allerdings auch das Speichern erlauben, aber dennoch eine Aktion zur Überwachung konfigurieren (passive Prüfung). Wenn im geprüften Pfad einer Dateiprüfung bereits Dateien gespeichert sind, die blockiert werden sollen, hindert die Dateiprüfung Anwender jedoch nicht am Zugriff. Erst das Speichern nach der aktivierten Dateiprüfung wird verhindert und überwacht.

Wie bei den Kontingenten können Sie auch für die Dateiprüfungen eigene Vorlagen erstellen oder die bereits erstellten Vorlagen bearbeiten und verwenden. So lassen sich die Einstellungen einer bereits erstellten Vorlage in eine neue kopieren und die Einstellungen einer Vorlage für andere verwenden. Wenn Sie eine Vorlage bearbeiten und speichern, werden Sie (wie

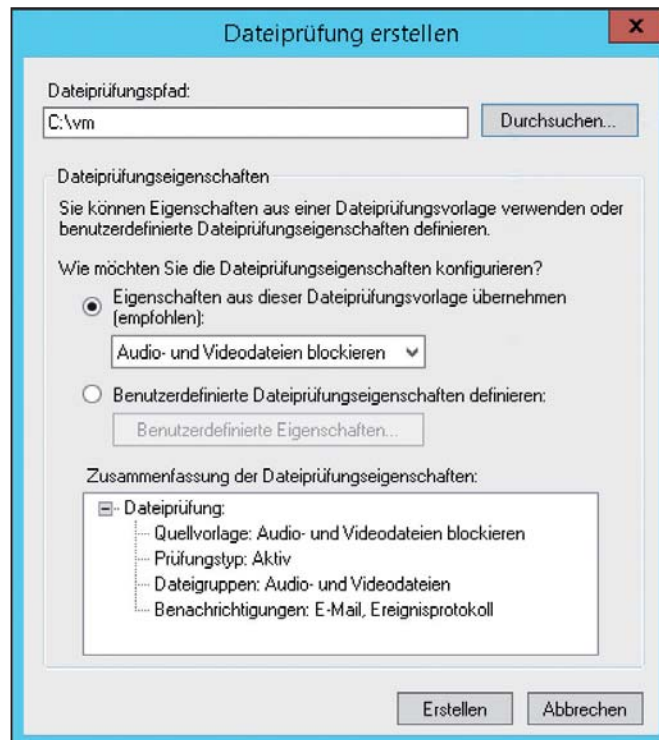


Bild 1: Mit einer Dateiprüfung können Sie Anwendern das Speichern bestimmter Dateitypen in einzelnen Verzeichnissen untersagen

bei den Vorlagen für Kontingente) gefragt, ob die Änderungen an die Dateiprüfungen übergeben werden sollen, die mit Hilfe dieser Vorlage erstellt wurden.

Wählen Sie bei "Wie möchten Sie die Dateiprüfungseigenschaften konfigurieren?" die Option "Benutzerdefinierte Dateiprüfungseigenschaften definieren" aus und klicken Sie dann auf die Schaltfläche "Benutzerdefinierte Eigenschaften". Möchten Sie Eigenschaften aus einer vorhandenen Vorlage kopieren, wählen Sie die zu verwendende Vorlage aus und klicken Sie auf "Kopieren". Geben Sie nun unter "Prüfungstyp" den Typ aus, der angewendet werden soll:

- Aktives Prüfen: Verhindert, dass Benutzer Dateien speichern, die zu blockierten Dateigruppen gehören, und generiert Benachrichtigungen, wenn Benutzer versuchen, blockierte Dateien zu speichern. Versucht ein Benutzer, eine verbotene Datei zu speichern, erhält er eine entsprechende Fehlermeldung.
- Passives Prüfen: Sendet Benachrichtigungen, hindert Benutzer jedoch nicht daran, blockierte Dateien zu speichern.

Wählen Sie unter "Dateigruppen" die Dateien aus, die einbezogen werden sollen. Um E-Mailbenachrichtigungen für die Dateiprüfung zu konfigurieren, legen Sie auf der Registerkarte "E-Mail-Nachricht" die Optionen fest, analog zur Erstellung von Kontingenten. Klicken Sie auf "Erstellen", um die Dateiprüfung zu speichern. Sie werden gefragt, ob Sie eine Dateiprüfungsvorlage auf der Grundlage der Dateiprüfungseigenschaften speichern möchten, die Sie gerade definiert haben. Wenn Sie die aktuellen Einstellungen in anderen Dateiprüfungen verwenden möchten, sollten Sie eine Vorlage speichern. Die Vorlage wird auf die neue Dateiprüfung angewendet.

Dateiprüfungsausnahmen

Um Dateien zuzulassen, die von Dateiprüfungen eigentlich blockiert werden sollen, erstellen Sie eine Dateiprüfungsausnahme. Eine Dateiprüfungsausnahme ist eine besondere Art der Dateiprüfung, die Datei-

IT clever managen!



CeBIT

Besuchen Sie uns!
Halle 3 Stand E06/1

f c s FAIR
COMPUTER
SYSTEMS
GMBH

www.fair-computer.de



prüfungen in einem bestimmten Ausnahmepfad außer Kraft setzt. Sie können aber keine Dateiprüfungsausnahme für einen Ordner erstellen, für den bereits eine Dateiprüfung besteht. Sie müssen die Ausnahme einem Unterordner zuweisen oder Änderungen an der vorhandenen Dateiprüfung vornehmen.

Klicken Sie mit der rechten Maustaste auf "Dateiprüfungen" und rufen Sie im zugehörigen Kontextmenü den Befehl "Dateiprüfungsausnahme erstellen" auf. Wählen Sie unter "Ausnahmepfad" den Pfad aus, für den die Ausnahme gelten soll. Die Ausnahme wird auf den Ordner und alle Unterordner angewendet. Um festzulegen, welche Dateien von der Dateiprüfung ausgenommen werden sollen, wählen Sie unter "Dateigruppen" jede Dateigruppe aus, die in der Dateiprüfungsausnahme enthalten sein soll.

Dateigruppen verwenden Sie, um einen Namensraum für eine Dateiprüfung, eine Dateiprüfungsausnahme oder einen Speicherbericht zu definieren. Sie werden in "Einzuschließende Dateien" (Dateien, die zur Gruppe gehören) und "Auszuschließende Dateien" (Dateien, die nicht zur Gruppe gehören) unterschieden. Standardmäßig sind bereits einige Dateigruppen angelegt, die Sie bearbeiten können. Um eine neue Dateigruppe zu erstellen, klicken Sie in der Konsolenstruktur von FSRM mit der rechten Maustaste auf "Dateigruppen" und wählen im zugehörigen Kontextmenü den Eintrag "Dateigruppe erstellen" aus. Bei Eingabe von "*.exe" werden zum Beispiel alle ausführbaren Dateien ausgewählt.

Praktischer Einsatz der Dateiklassifizierungsdienste

Die Dateiklassifizierungsdienste (File Classification Infrastructure, FCI) im Ressourcen-Manager für Dateiserver stellen eine interessante Funktion dar, um zum Beispiel Daten zu SharePoint zu migrieren. Mit den Dateiklassifizierungsdiensten lassen sich Metadaten zu Dokumenten zuweisen. Dazu können Sie Dokumenten zusätzliche Ei-

Bild 2: Klassifizierungsregeln passen die Metadaten von Dateien auf Servern an

enschaften zuweisen, wie auch in SharePoint. Die Eigenschaften liegen direkt im Dokument, nicht im NTFS-Dateisystem. Die Dateiklassifizierungsdienste gehören zum Rollendienst "Ressourcen-Manager für Dateiserver". Sie verwalten diese Funktion daher über die Verwaltungskonsolle des Ressourcen-Managers für Dateiserver.

Über den Menüpunkt "Klassifizierungsverwaltung" administrieren Sie die Dateiklassifizierung. Klicken Sie mit der rechten Maustaste auf "Klassifizierungseigenschaften", legen Sie mit "Nur für" fest, welche neuen Kriterien Dateien zugeordnet werden sollen. So bestimmen Sie beispielsweise, ob ein Dokument zu einem Projekt gehört, private Daten enthält, nur für den internen Gebrauch oder für bestimmte Personen nutzbar sein soll. Im neuen Fenster geben Sie zunächst den Namen der neuen Eigenschaft an, zum Beispiel "Nur für internen Gebrauch". Geben Sie anschließend eine Beschreibung der Eigenschaft an, falls diese nicht aus dem Namen ersichtlich ist.

Über "Eigenschaftentyp" stehen Ihnen verschiedene Möglichkeiten zur Verfügung, die Eigenschaft festzulegen. Neben "Ja" oder "Nein" können Sie eine Multiple Choice-Liste erstellen, eine Nummer angeben oder eine Uhrzeit hinterlegen. Im unteren Bereich bearbeiten Sie schließlich die Eingaben genauer, die als Klassifizierung zur Auswahl

stehen. Sie können mehrere Eigenschaften festlegen und diese auch nachträglich ändern. Die Eigenschaften werden in FSRM unter "Klassifizierungsverwaltung / Klassifizierungseigenschaften" angezeigt.

Das Anlegen und Bearbeiten von Klassifizierungseigenschaften ändert aber noch keine Dokumente ab, sondern bietet nur die Verwendung der jeweiligen Eigenschaften an. Damit diese auch mit Dokumenten verknüpft werden, müssen Sie Klassifizierungsregeln anlegen. Erstellen Sie eine neue Regel, legen Sie zunächst den Namen der Regel fest und bestimmen auf der Registerkarte "Bereich", welche Ordner im Dateisystem die Re-

gel steuern soll. Auf der Registerkarte "Klassifizierung" legen Sie zudem fest, dass Sie Dateien mit der Ordnerklassifizierung ändern wollen und wählen die erstellte Klassifizierungseigenschaft und den Wert aus, den der Server den Dateien zuordnen soll. Anschließend stempelt die Regel alle Dateien in den entsprechenden Ordnern automatisch mit den hinterlegten Klassifizierungseigenschaften.

Über den Befehl "Klassifizierungszeitplan konfigurieren" im Kontextmenü der Klassifizierungsregeln bestimmen Sie, wann Klassifizierungsregeln starten sollen, ob Sie einen Bericht erhalten wollen und wenn ja, in welchem Format. Klassifizierungsregeln werden durch Klassifizierungszeitpläne gesteuert.

Speichern Anwender neue Dokumente in den überwachten Ordnern, stempelt der Server automatisch die Dateien mit den festgelegten Metadaten. Die Klassifizierungsregeln verwenden wiederum die Klassifizierungseigenschaften. Sie können die Regeln an dieser Stelle auch sofort ausführen lassen. Auf der Registerkarte "Klassifizie-

[1] Klassifizierung über das .NET Framework DS174

Link-Codes





lung" in den Eigenschaften einer Regel legen Sie bei "Klassifizierungsmethode" fest, ob Sie die Klassifizierung auf Basis des Ordners, in dem das Dokument gespeichert ist, durchführen wollen oder auf Basis des Inhalts. Bei "Eigenschaft" wählen Sie die Klassifizierungseigenschaft aus, die Sie für die Regel und den hinterlegten Bereich untersucht und festgelegt haben wollen.

Auf der Registerkarte "Klassifizierung" legen Sie bei Bedarf erweiterte Eigenschaften fest, die auf dem .NET Framework basieren. Welche Möglichkeiten Sie hier haben, erfahren Sie am schnellsten über die Microsoft-Webseite [1]. Der Einsatz ist nur sinnvoll, wenn Sie sich mit den Hintergründen von .NET Framework, insbesondere den .NET Regular Expressions, auskennen. An dieser Stelle können Sie den Inhalt des Dokumentes entsprechend nach bestimmten Inhalten und Textstellen durchsuchen. Sie können mehrere Regeln erstellen und komplexere Regeln anwenden. Auch das Zuteilen von einzelnen Eigenschaften zu Dateien ist möglich. Haben Sie den Suchlauf gestartet, sehen

Sie in den Eigenschaften der Dateien auf der Registerkarte "Klassifizierung" die zugeordneten Eigenschaften.

Klassifizierte Dateien verwalten

Nachdem Sie Klassifizierungsregeln erstellt haben, die zum festgelegten Zeitpunkt die Dateiklassifizierungseigenschaften auf bestimmte Dateien anwenden, können Sie über Dateiverwaltungsaufgaben festlegen, was der Server mit den gefundenen Dateien machen soll. Über das Kontextmenü von Dateiklassifizierungsaufgaben legen Sie eine neue Aufgabe an. Auf verschiedenen Registerkarten steuern Sie den Ablauf:

- Auf der Registerkarte "Allgemein" legen Sie den Namen sowie den Bereich fest, auf den die Aufgabe angewendet werden soll.
- Auf der Registerkarte "Bereich" legen Sie den Ordner oder das Laufwerk fest, das Sie verwalten wollen.
- Unter "Aktion" bestimmen Sie, was die Aufgabe durchführen soll. Sie können zum Beispiel abgelaufene Dateien, also Dateien die schon lange nicht mehr im Einsatz sind, archivieren oder löschen.

Oder Sie hinterlegen benutzerdefinierte Skripte, die bestimmte Rechte setzen oder Dateien verschieben.

- Unter "Bedingung" geben Sie an, auf welche Dateien die Aktion angewendet werden soll. Zusätzlich legen Sie die Tage fest, nach deren Grenzwerte die Aktion auf der Registerkarte "Aktion" durchgeführt werden soll, etwa um die Archivierung nach der Aktion "Dateiablauf" festzulegen.
- In "Zeitplan" tragen Sie ein, wann die Aufgabe starten soll. Über das Kontextmenü können Sie eine Aufgabe auch sofort starten.

Fazit

Ohne eine zentrale Kontrolle ufer die Datenflut im Unternehmen schnell aus. Mit dem Ressourcen-Manager für Dateiserver bietet Microsoft zumindest eine rudimentäre Möglichkeit in Windows Server, um die Dateien der Anwender in den Griff zu bekommen. Richtig interessant wird es in Zusammenhang mit dem .NET Framework, mit dessen Hilfe Sie auch die Inhalte von Dateien klassifizieren können. (dr) 

Bestellen Sie jetzt das IT-Administrator Sonderheft I/2014!

180 Seiten Praxis-Know-how rund um das Thema

Windows Server 2012 R2 und Windows 8.1

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

* IT-Administrator Abonnenten erhalten das Sonderheft I/2014 für € 24,90. Nichtabonnenten zahlen € 29,90. IT-Administrator All-Inclusive Abonnenten "zahlen" für Sonderhefte nur € 19,90 - diese sind im Abonnement dann automatisch enthalten. Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.



Liefertermin:
März 2014

Mehr Infos und Bestellung unter
www.it-administrator.de/kiosk/sonderhefte/





Tipps & Tricks ohne Gewähr

In jeder Ausgabe präsentiert Ihnen IT-Administrator Tipps, Tricks und Tools zu den aktuellen Betriebssystemen und Produkten, die in vielen Unternehmen im Einsatz sind. Wenn Sie einen tollen Tipp auf Lager haben, zögern Sie nicht und schicken Sie ihn per E-Mail an tipps@it-administrator.de.



Auf meinem **Desktop**, der unter **Windows 8.1** läuft, habe ich neulich festgestellt, dass in den Einstellungen **diverse WLAN-Profil**e auftauchen, mit denen ich zumindest mit diesem PC nie verbunden war. Da mein Windows-Tablet unter dem gleichen **Microsoft-Konto** läuft, tippe ich einmal darauf, dass hier eine Synchronisierung stattgefunden hat. Kann ich diesen **Abgleich irgendwie deaktivieren**?

Wie Sie richtig vermuten, speichert Microsoft die WLAN-Zugriffsdaten von Nutzern mit Microsoft-Konto in der Cloud ab. Eine Praxis, die etwa bei Android-Geräten schon länger Usus ist, aus Datenschutzgründen aber zu Recht für Kritik sorgt. Wenn Sie "das Backup" von Netzwerkeinstellungen in die Cloud verhindern wollen, bleibt Ihnen nur, die Set-

tings von SkyDrive zu modifizieren. Öffnen Sie dazu über die rechte Charms-Leiste "Einstellungen", klicken/tippen Sie auf "PC-Einstellungen ändern", im folgenden Menü auf "SkyDrive" und dann auf "Synchronisierungseinstellungen". Unter dem Oberpunkt "Weitere Einstellungen" deaktivieren Sie nun den Schalter "Kennwörter", was auch die Zugangsdaten zu Netzwerken betrifft. Wollen Sie nicht mehr benötigte WLAN-Verbindungen löschen, funktioniert dies unter Windows 8.1 nur noch über die Kommandozeile – unter Windows 8 war dies noch mit der rechten Maustaste möglich. Wechseln Sie zunächst auf den Desktop und starten Sie über "WIN+X" die Eingabeaufforderung. Hier geben Sie dann den Befehl

netsh wlan show profiles

ein und bringen so eine Liste aller auf dem Rechner hinterlegten WLAN-Netzwerke auf den Schirm. Zum Löschen eines WLAN-Profiles tippen Sie

**netsh wlan delete profile
name=Name des Profils**

ein. Abschließend können Sie mit dem ersten Befehl prüfen, ob das Löschen der alten Profile auch wirklich funktioniert hat. (In)

Die **PowerShell** ist ja wirklich ein feines Werkzeug. Gerade um Einstellungen auch remote zu ändern, ist mir das Tool oft eine große Hilfe. Für etwas ganz simples habe ich jedoch die Befehlskette vergessen: Das **Ändern eines User-Passworts im Active Directory**. Können Sie mir hier auf die Sprünge helfen?

Voraussetzung für die Passwort-Änderung eines Nutzers ist zunächst, dass Sie die PowerShell in Version 3.0 nutzen oder das Active Directory-Modul importiert haben. Ist Letzteres nicht der Fall, laden Sie sich am besten die Remote Server Administration Tools (RSAT) herunter. Außerdem müssen natürlich Sie selbst mit einem Account angemeldet sein, der zum Ändern von Passwörtern berechtigt ist. Ist dies der Fall, lautet der Befehl zum Setzen eines neuen Passworts:

Set-ADAccountPassword Nutzer

-NewPassword \$newpwd -Reset

Wollen Sie erzwingen, dass der Anwender beim nächsten Einloggen ein neues Passwort vergibt, so greifen Sie auf dieses Kommando zurück:

Set-ADAccountPassword Nutzer

-NewPassword \$newpwd -Reset

-PassThru | Set-ADuser

-ChangePasswordAtLogon \$True

Weiterführende Informationen zu allen Schaltern des Cmdlets erhalten Sie auf ei-

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. Alle Rechte vorbehalten.
C:\WINDOWS\system32>netsh wlan show profiles
Profile auf Schnittstelle Wi-Fi:
Gruppenrichtlinienprofile <schreibgeschützt>
<Kein>
Benutzerprofile
Profil für alle Benutzer : HU
Profil für alle Benutzer : Ex
Profil für alle Benutzer : Ne
Profil für alle Benutzer : Co
Profil für alle Benutzer : BS
Profil für alle Benutzer : Na
Profil für alle Benutzer : HU
Profil für alle Benutzer : XP
C:\WINDOWS\system32>
```

Wer unter Windows 8.1 WLAN-Profil löschen will, kann dies nur noch über die Kommandozeile tun

ner äußerst umfangreichen TechNet-Seite [Link-Code E3PE6]. (ln)

Bereits in Windows Server 2008 R2 und Windows 7 hatte Microsoft mit **DISM** ja zahlreiche Möglichkeiten geschaffen, das Betriebssystem an die eigenen Bedürfnisse anzupassen und Installationsmedien zu ändern. Mit **Windows 8 und Windows Server 2012** erweitert Microsoft diese Fähigkeiten. Können Sie kurz darauf eingehen, **was sich mit DISM nun alles machen lässt** und wie die wichtigsten Befehle aussehen?

DISM ist Bestandteil des kostenlosen Windows Assessment and Deployment Kit (ADK). Das ADK unterstützt die Bereitstellung von Windows Server 2012, Windows Server 2008/2008 R2 und Windows 7. Um ein Image zu erstellen, verwenden Sie zum Beispiel den folgenden Befehl:

```
dism /Capture-Image /CaptureDir:D:\
/ImageFile: E:\ThinImage.wim
/Name:"Contoso"
```

Um später ein Image auf einem Computer bereitzustellen, geben Sie die folgende Anweisung ein:

```
dism /Apply-Image /ImageFile:Datei
/Index:1 /ApplyDir:Laufwerk:\
```

Eine interessante Neuigkeit in Windows 8 und Windows Server 2012 ist die Möglichkeit, mit DISM auch virtuelle Festplatten (VHD und VHDX) zu mounten. Die Syntax dazu lautet:

```
dism /Mount-Image
/ImageFile:"C:\win.vhd" /Index:1
/MountDir:2C:\temp\Mount"
```

Ebenfalls neu ist die Option "/List-Image". Diese zeigt den Inhalt eines Image an, also die enthaltenen Dateien und Ordner. Der Befehl

```
dism /Image:Name /Get-Packages
```

zeigt die installierten Pakete an, und mit

```
dism /Image:Name /Remove-Package
/PackageName: Paket
```

entfernen Sie Pakete. (Thomas Joos/ln)



Um in unserem Unternehmen **Exchange 2010** und die E-Mails zu schützen, bildet ein **Edge-Transport-Server** die Schnittstelle zum Internet. Dieser muss ja nicht Mitglied einer Windows-Domäne sein. Diese Rolle haben wir auf einem Server mit dem **Threat Management Gateway** installiert und betreiben sie zusammen mit **Forefront Protection 2010**. Können Sie kurz beschreiben, was wir für ein **reibungsloses Zusammenspiel** beachten müssen?

Haben Sie die Edge-Transport-Rolle auf einem Server mit dem Forefront Threat Management Gateway installiert, müssen Sie in der TMG-Konsole vor der Einrichtung des Edge-Transports den Datenverkehr für Edge-Transporte freischalten: Rufen Sie die TMG-Verwaltungskonsole auf und klicken Sie auf "E-Mail-Richtlinie". Während der Erstellung einer neuen E-Mail-Richtlinie wählen Sie die Option "Konnektivität für EdgeSync-Datenverkehr aktivieren" aus. Haben Sie bereits eine Richtlinie erstellt, können Sie diese Einstellung auch nachträglich setzen. Damit der E-Mailfluss zwischen Internet, Edge-Transport-Server, Hub-Transport-Server und Mailboxservern funktioniert, müssen Sie nach der Installation den Edge-Transport-Server mit der Exchange-Organisation verbinden. Der Server tauscht dazu mit den Hub-Transport-Servern und den Domänencontrollern Daten aus. Die Synchronisation findet ausschließlich vom Hub-Transport-Server zum Edge-Transport-Server statt. Durch das Abonnement eines Edge-Transport-Servers erstellt der Dienst folgende Konnektoren auf dem Edge-Transport-Server: Einen Sendekonnektor von den Hub-Transport-Servern der Gesamtstruktur zum Edge-Transport-Server. Zudem einen Sendekonnektor vom Edge-Transport-Server zu den Hub-Transport-Servern. Zuletzt noch einen Sendekonnektor vom Edge-Transport-Server zum Internet. Falls

der Edge-Transport-Server in der DMZ positioniert ist, sollten Sie sicherstellen, dass die Firewall die notwendigen Ports durchlässt. Für die Kommunikation zwischen Hub-Transport-Server und Edge-Transport-Server wird die Kommunikation per LDAP über den Port TCP 50389 benötigt. Verwenden Sie Secure LDAP, bedarf es des Ports TCP 50636. Leiten Sie die DNS-Abfrage vom Edge-Transport-Server zu den internen DNS-Servern weiter, muss zusätzlich der Port TCP 53 geöffnet sein. Bevor Sie das Abonnement einrichten, sollten Sie auf den Hub-Transport-Servern die akzeptierten Domänen, das gewünschte Relaying sowie alle anderen Einstellungen und Konnektoren eingerichtet haben.

(Thomas Joos/ln)

In unserer Organisation nutzen immer mehr Anwender **Android-Handys**. Die **Anbindung an Exchange-Server über die ActiveSync-Technologie** ist hier ja genauso möglich wie bei iPhones. Seit Android 2.2 unterstützen die Smartphones ja sogar **ActiveSync-Postfachrichtlinien**. Können Sie kurz schildern, **welche Schritte nun notwendig** sind, um eine sichere Anbindung an Exchange durchzuführen?



Die Anbindung eines Android-Smartphones an Exchange stellt zumindest mit den aktuellen Versionen des Betriebssystems kein Problem dar

Viele weitere Tipps & Tricks sowie konkrete Hilfe bei akuten Problemen bekommen Sie auch im Internet bei unserem exklusiven Foren-Partner administrator.de. Über 70.000 registrierte Benutzer tauschen dort in über 100 Kategorien ihre Erfahrungen aus und leisten Hilfestellung. So wie der IT-Administrator das praxisnahe Fachmagazin für Administratoren ist administrator.de die Internetplattform für alle System- und Netzwerkadministratoren.
www.administrator.de



Öffnen Sie die App "E-Mail" und beginnen Sie dort das Einrichten eines neuen Kontos. Alternativ gehen Sie über "Einstellungen / Konten / Konto hinzufügen". Auch hier können Sie neue E-Mailkonten erstellen. Wählen Sie "Microsoft Exchange (ActiveSync)". Geben Sie die E-Mailadresse ein und das Kennwort für das Konto und klicken Sie auf "Weiter". Erfolgt hier eine Rückfrage nach dem Kontotyp, wählen Sie auch hier noch einmal "Exchange". Auf der nächsten Seite geben Sie den Benutzernamen ein. Diesen müssen Sie in der Syntax "Domäne\Benutzername" eintragen. An dieser Stelle tippen Sie zudem den Namen der Windows-Domäne ein, an der Sie sich authentifizieren wollen. Im Feld "Server" tragen Sie den Namen des Servers ein, mit dem Ihr Exchange-Server an das Internet angebunden ist. Meistens handelt es sich hier um den gleichen Namen, den Sie auch in OWA verwenden. Klicken Sie jetzt auf "Fertig". Aktivieren Sie noch die beiden Optionen "Sichere Verbindung (SSL) verwenden" und "Alle SSL-Zertifikate akzeptieren" und klicken Sie im Anschluss auf "Weiter". Danach versucht das Gerät, eine Verbindung herzustellen und blendet Hinweise ein, dass bestimmte Sicherheitseinstellungen auf dem Smartphone geändert werden müssen. Abschließend geben Sie dem Konto noch einen Namen. Haben Sie auf dem Server Richtlinien gesetzt, müssen Sie auf dem Smartphone in den meisten Fällen noch Einstellungen vornehmen, zum Beispiel eine PIN festlegen, mit der Sie das Gerät entsperren können. Nun stehen die Nachrichten aus dem Exchange-Postfach über das Anwendungsfenster im Bereich "E-Mails" zur Verfügung. (Thomas Joos/ln)



Auf der Homepage des IT-Administrator-Magazins stellen wir jede Woche für Sie ein praktisches Tool zum Download bereit. Neben einer Kurzbeschreibung finden Sie Systemvoraussetzungen und alle weiteren wichtigen Informationen auf einen Blick. Und können so gezielt Werkzeuge für Ihren täglichen Administrationsbedarf herunterladen.

www.it-administrator.de/downloads/software/

Download der Woche



Linux

Zur Installation meiner Systeme setze ich Kickstart-Profil ein. Somit laufen meine Installationen vollautomatisch ab. Zur Authentifizierung der Benutzer möchte ich nun eine möglichst sichere Variante konfigurieren. Welchen Parameter kann ich hierfür in meinen Kickstart-Profilen verwenden?

Der Parameter "auth" kann in einer Kickstart-Datei zum Einsatz kommen, um die Art der Benutzerauthentifizierung festzulegen. Für lokale Benutzer sieht ein möglicher Aufruf beispielsweise folgendermaßen aus:

```
autconfig --enablesdow
--passalgo=sha512
```

Um das Passwort für den Benutzer root direkt als verschlüsselten SHA512-Hash in der Kickstartdatei abzulegen, generieren Sie mittels

```
python -c 'import crypt; print
crypt.crypt("Passwort")'
```

einen entsprechenden Kennwort-Hash und geben diesen als Argument zu dem Parameter "rootpw --iscrypted" in der Kickstartdatei an.

(Thorsten Scherf/ln)



Wir nutzen bei uns im Unternehmen Citrix XenMobile, und zwar noch in der Version 8.5. Die Apple-User unter unseren Mitarbeitern haben seit dem Update auf iOS 7 mitunter Schwierigkeiten, ihre Geräte ordnungsgemäß am System anzumelden. Stattdessen erhalten sie die Fehlermeldung "Server Error - Could Not Connect 500". Wie lässt sich dieses Problem beheben?

Zur aktuellen Version des iOS-Betriebssystems hat Citrix ein Patch für XenMobile 8.5 bereitgestellt, mit dem die Kompatibilität zu iOS 7 Geräten hergestellt wird. Um die Aktualisierung auf dem XenMobile Device Manager 8.5 Server zu installieren, gehen Sie wie folgt vor: Laden Sie zunächst unter [Link-Code E3PE5] den XenMobile Device Manager Server Patch 8.5.0 Build 9995 auf den Server herunter. Kopieren Sie dann die JAR-Datei in das Verzeichnis "C:\Program Files (x86) \ Citrix \ XenMobile

Device Manager \ tomcat \ webapps \ Name der Instanz \ WEB-INF \ lib". Wiederholen Sie diesen Schritt für alle Cluster-Knoten beziehungsweise in jeder XDM-Config. Starten Sie anschließend den XenMobile Device Manager neu. Die Geräte mit iOS 7 lassen sich nun ohne Probleme nutzen. (Citrix/ln)



Tools

Die stetig umfangreicher werdenden Erkenntnisse über die Machenschaften sogenannter Sicherheitsinstitutionen in Sachen Kommunikations-Überwachung dürften so manchen IT-Verantwortlichen dazu gebracht haben, über die Integrität und Vertraulichkeit der Unternehmensdaten nachzudenken. Zur Einleitung geeigneter Gegenmaßnahmen hat der IT-Verantwortliche mittlerweile eine umfangreiche Auswahl an Tools, wenn es um die Verschlüsselung von E-Mails geht. Doch die Geheimhaltung telefonischer Kommunikation ist ein weit weniger besetzter Marktplatz. Ein kostenloses Angebot, um Telefonie abhörsicher zu gestalten, bietet der Verschlüsselungsexperte SecurStar nun mit PhoneCrypt Desktop. PhoneCrypt

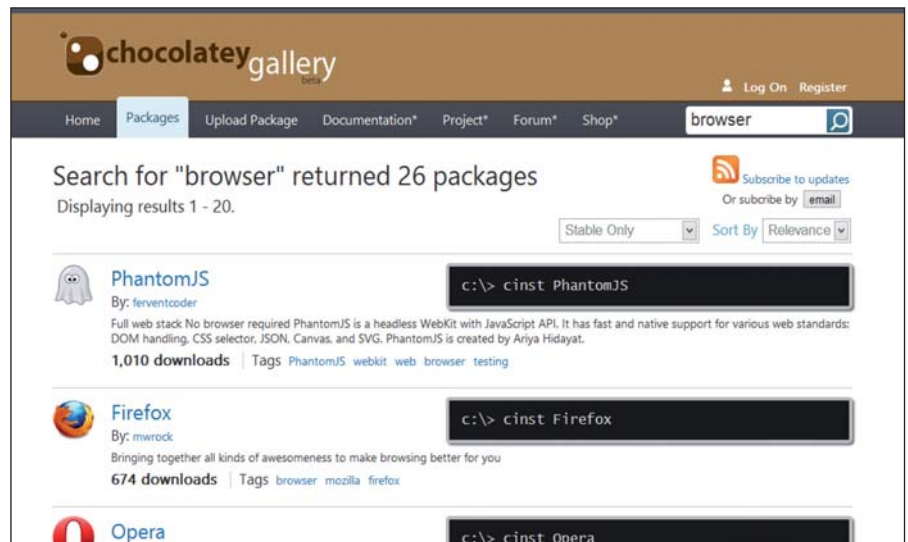


PhoneCrypt Desktop verschlüsselt Telefonate
Peer-to-Peer mit 256 Bit AES

verschlüsselt Telefongespräche über das Festnetz und Mobiltelefon im In- und Ausland gemäß militärischen Sicherheitsstandards. Die Desktop-Version funktioniert ähnlich wie Skype, aber abhörsicher. Die Software wird auf dem PC oder mobilen Endgerät installiert und schützt sowohl die Chat- als auch Voice-Kommunikation. Das Produkt arbeitet mit einer **starken Verschlüsselung (DH 2048 Bit)** und erzeugt dabei einen **geheimen 256 Bit AES-Schlüssel**. Die PhoneCrypt-Kommunikation ist Point-to-Point verschlüsselt und bei jedem Verbindungsaufbau wird automatisch ein Code generiert, der sich regelmäßig erneuert. Auf diese Weise wird **jeder Abhörversuch durch einen nicht zu knackenden Zifferncode unterbunden** und es sind keine Backdoors vorhanden. Die Desktop-Variante ist zudem kompatibel mit PhoneCrypt Mobile, das für iPhones, Android, Symbian und Windows Mobile Telefone entwickelt wurde. Im Gegensatz zu den kostenpflichtigen Angeboten des Herstellers muss PhoneCrypt Desktop bei beiden am Gespräch Beteiligten installiert sein, um die Vertraulichkeit zu gewährleisten. Laut Hersteller ist die Verbindung dann sicher verschlüsselt und die Software soll sogar Man-in-the-Middle-Angriffe erkennen. (jp)

Link-Code: E3PE1

Wenn es ein Feature in Linux gibt, auf das Windows-Admins wirklich neidisch sind, dann dürfte es die Funktionalität der **Packagemanager** sein, die sich in jeder Linux-Distribution finden. Egal ob RPM, APT, YUM oder dpkg – alle ermöglichen es mittels kurzem Konsolenbefehl oder grafischer Oberfläche mit minimalem Aufwand **Anwendungen herunterzuladen, zu installieren, updaten und deinstallieren**. Unter Windows hingegen bleibt dem Administrator nur eine Suche bei Google und Konsorten, gefolgt von händischem Download und Installation. Und die laufende Pflege besteht nicht selten aus einer manuellen Suche nach Updates für jede einzelne Anwendung. Ein ganz neues Administrationsfeeling bringt daher **Chocolatey** in die Windows-Stube. Mit der Freeware Chocolatey **installieren IT-Verantwortliche Tools wie unter Linux über die**



Ein Paketmanager für Windows: Chocolatey zeigt auf der Website die über die Kommandozeile installierbaren Anwendungen – hier Browser

Kommandozeile. Passenderweise wird Chocolatey auch über einen Konsolenbefehl installiert. Über die Eingabeaufforderung und einen PowerShell-Befehl lädt sich das Tool selbst aus dem Internet herunter und installiert sich mit erweiterten Rechten. Anschließend lassen sich über die Kommandozeile zahlreiche Funktionen nutzen – unter anderem ein sehr hilfreicher Befehl, der alle auf diesem Weg installierbaren Programme auflistet. Die installierbaren Programm-Pakete lassen sich auch auf der Herstellerseite nachlesen. Einige Programme benötigen jedoch Administratorrechte, um ohne weitere Programmabfrage installiert werden zu können. Dazu muss die Eingabeaufforderung als Administrator ausgeführt werden. Und wer so gar nicht mit der Kommandozeile warm wird, dem **bietet Chocolatey auch ein grafisches Interface**. Damit installieren Sie die Programme auch ohne Konsole. Um in den Genuss von Chocolatey zu kommen, ist lediglich das Microsoft .NET-Framework 4 Voraussetzung. (jp)

Link-Code: E3PE4

Microsoft stellt seit geraumer Zeit mit **Click-to-Run** (auf deutschen Microsoft-Seiten etwas holprig mit "Klick-und-Los" übersetzt) eine Streaming- und Virtualisierungstechnologie bereit, die nicht nur den **Installationsvorgang für Office beschleunigen**, sondern auch die **Ausführung mehrerer Versionen von Office auf dem gleichen Computer** ermöglichen soll. Dank der

Streamingtechnologie können IT-Verantwortliche ein Office-Produkt herunterladen und zum Einsatz bringen, bevor das gesamte Produkt auf dem Computer installiert wurde. Die Virtualisierungstechnologie bietet eine isolierte Umgebung für die Ausführung von Office auf dem Computer und ermöglicht so die Nutzung der neuesten Version von Office parallel zu einer älteren Version. Doch eine Sache, die so schön klingt, muss natürlich einen Haken haben und dieser ist nicht ohne: Bisher fehlte es an Anpassungsmöglichkeiten für Administratoren, um spezielle Unternehmensanforderungen zu konfigurieren.

Diese liefert Microsoft nun mit dem kostenlosen **Office Deployment Tool for Click-to-Run** nach. Das Kommandozeilenprogramm bietet eine Reihe von Optionen für Administratoren wie beispielsweise die **Verlagerung der Installationsquellen vom Internet auf interne File-Server** oder das Deaktivieren von automatischen Updates. Darüber hinaus ist es mit dem Office Deployment Tool for Click-to-Run nun möglich, **die zu installierenden Sprachen zu konfigurieren**. Auch erlaubt der kleine Helfer die Erstellung von App-V-Paketen. Und auch das im Unternehmensumfeld wichtige Entfernen der Installationen findet sich in dem Tool wieder. Eine Einführung in die Nutzung des Tools findet sich in einem Microsoft-Blog, wenn Sie den Link-Code E3PE2 auf unserer Webpage eingeben und der URL folgen. (jp)

Link-Code: E3PE3



Reportage: Modernisierte IT-Infrastruktur bei Julius Kleemann

Virtuelle Flexibilität

von Michal Vitkovsky

Als mittelständisches Fertigungsunternehmen für Metallverpackungen ist Julius Kleemann auf eine stabile und zuverlässige IT angewiesen. Doch war diese den stetig gestiegenen Anforderungen des Unternehmens nicht mehr gewachsen. Der IT-Dienstleister Controlware konzipierte und realisierte deshalb für Julius Kleemann eine neue, virtualisierte IT-Infrastruktur und überführte die vorhandenen Daten und Anwendungen in die neu aufgesetzte Umgebung. Diese ermöglicht es nun, flexibler auf die Bedürfnisse der Kunden einzugehen.



Zur Palette von Julius Kleemann gehören im Wesentlichen die Segmente chemisch-technische Verpackungen, Konserven sowie Lebensmittelverpackungen

tont Josef da Costa. "Wir waren uns daher sicher, dass das Team über die Kompetenz und Erfahrung verfügt, um unser Projekt im vorgegebenen Rahmen umzusetzen." Controlware übernahm als Projektleiter die gesamte Planung und Implementierung der neuen Infrastruktur sowie die Migration der bestehenden Daten und Applikationen.

Definition von SLAs und Worst-Case-Szenarien

Um einen reibungslosen Projektverlauf sicherzustellen, legten Julius Kleemann und Controlware zunächst im Rahmen eines Workshops die Projektziele fest und definierten klar terminierte Teilprojektschritte. Das IT-Team von Julius Kleemann lieferte dafür im Vorfeld des Workshops eine verbindlich klassifizierte und priorisierte Aufstellung der zu implementierenden Anwendungen und benannte unverzichtbare Grundfunktionen. Wichtige Teilaspekte waren hierbei die Definition klarer SLAs sowie die Ausarbeitung denkbarer Worst-Case-Szenarien mit den zugehörigen Handlungsanweisungen. Als international tätiger Fertiger ist Julius Kleemann im Alltag nämlich auf eine Reihe kritischer Anwendungen angewiesen, die ausnahmslos im hauseigenen Data Center gehostet und betrieben werden. Hierzu gehören:

- Klassische IT-Services wie E-Mailzugriff, Collaboration-Werkzeuge und Remote Desktop für eine effiziente Anwendungsbereitstellung
- Eine solide Security-Architektur mit Firewall, Web- und VPN-Gateway sowie Push-E-Mail, die das Unternehmen vor Angriffen schützt

Die Abläufe im Backoffice und in der Produktionsumgebung sind bei Julius Kleemann eng verzahnt und weitgehend automatisiert: "Eingehende Bestellungen werden bei uns im CRM-System Navision erfasst und dann automatisch für die Generierung von Stücklisten im ERP-System herangezogen. Das ist zwar effizient, bedeutet aber auch, dass sich jeder Ausfall der IT unmittelbar auf die Produktionszahlen auswirken würde", erklärt Josef da Costa, Betriebsleiter und Prokurist bei Julius Kleemann. "Als Ende 2011 für eine Reihe unserer Server-Systeme der Hersteller-Support auslief und auch nicht mehr verlängert werden konnte, entschieden wir

uns, unsere Infrastruktur neu aufzusetzen. Das Ziel war es, die Server weitgehend zu virtualisieren und so die Weichen für mehr Effizienz, einfachere Skalierbarkeit und höhere Verfügbarkeit zu stellen."

Julius Kleemann setzte bei dem umfangreichen Modernisierungsprojekt auf die Unterstützung von Controlware. Der Systemintegrator ist seit über fünf Jahren für das Unternehmen tätig und daher mit dessen Infrastruktur und Anforderungen gut vertraut. "Wir kennen Controlware seit Jahren als zuverlässigen und kundenorientierten Partner, der uns bei allen Herausforderungen flexibel und engagiert unterstützt", be-

- Front- und Backoffice-Anwendungen für die Verwaltung – von der Textverarbeitung im Marketing über die Tabellenkalkulation in der Buchhaltung bis hin zum CRM-System der Kunden-Hotline
- Software für die Steuerung der Produktion, der Anlagen und der Prozesse sowie für die Verwaltung des Materiallagers und die Rückverfolgung von Produkten
- Dedizierte Systeme für die Abwicklung von Druckdiensten sowie für die Verwaltung des Wareneingangs und des Wareneingangs

Um die effiziente und durchgängige Bereitstellung dieser Anwendungen sicherzustellen, wurde die gesamte Netzwerktechnik inklusive Router und Switches neu aufgesetzt und die Server-Landschaft anschließend auf neue Hardware migriert und virtualisiert. Die Virtualisierung schaffte die Voraussetzungen für einen redundanten und hochverfügbaren 24/7-Betrieb, der reibungslose Abläufe in der Produktion sicherstellt und teure IT-Ausfälle vermeidet.

Auch wirtschaftlich bietet der Wechsel auf eine virtuelle Infrastruktur Julius Kleemann Vorteile, etwa im Hinblick auf eine effizientere Ausnutzung der vorhandenen Ressourcen oder wenn es um die Optimierung der laufenden Kosten und Wartungsaufwendungen geht. So lässt sich die virtualisierte Umgebung gut skalieren und bei Bedarf erweitern. Julius Kleemann profitiert durch die Modernisierung von einer zukunftssicheren, serviceorientierten Architektur, die sich auch mittel- und langfristig an aktuelle und neue Anforderungen anpassen wird.

Mix marktführender Hersteller

Produktseitig entschied sich das Projektteam für einen Mix marktführender Lösungen: Das Fundament des neuen Netzwerkes bilden Switches und Router von Alcatel. Die Server-, Storage- und Backup-Systeme laufen auf Hardware von Dell und bieten ein gutes Preis-Leistungs-Verhältnis. Um sicherzustellen, dass alle kritischen Anwendungen stabil und schnell bereitgestellt werden, wurde die gesamte Server-Landschaft mit VMware virtualisiert. Terminalserver von Microsoft sorgen für eine reibungslose Application Delivery auf den 60 Clients. Auch Softwareseitig verlässt sich Julius Kleemann weitgehend auf Lösungen aus dem Hause Microsoft – vom Server-Betriebssystem über die Collaboration- und Application Delivery-Lösungen bis hin zum Threat Management Gateway.

Stabiler Betrieb

Die Implementierung der neuen Infrastruktur wurde über den Jahreswechsel 2011/2012 während der Betriebsruhe in Angriff genommen und nach rund vier Monaten abgeschlossen. Seit der Inbetriebnahme hat die Lösung die Erwartungen erfüllt: Der Betrieb läuft stabil und zuverlässig, bislang gab es keine außerplanmäßigen Ausfälle. Die Performance der Anwendungen stimmt, und auch die Verzahnung zwischen dem Backoffice und der Produktionsumgebung funktioniert einwandfrei. (dr) 

Michal Vitkovsky ist Redakteur bei der
H zwo B Kommunikations GmbH.

„Mein neues Cisco IP Phone beherrsche ich
perfekt – dank ExpertTeach UC-trainer!“



- Multimediale Lernsoftware
- Für alle Cisco IP Phones
- Jabber, WebEx und weitere Applikationen
- In elf Sprachen verfügbar
- CI/CD-Anpassung nach Wunsch
- In Ihr Intranet integrierbar

Hier finden Sie eine Demo: www.experteach.de/uctrainer



Sprechen Sie uns bitte an,
gerne erstellen wir Ihnen
ein Angebot für Ihr
UC-Projekt!

ExpertTeach GmbH
ITK Training & Consulting
Waldstraße 94
63128 Dietzenbach

info@experteach.de
Telefon 06074 4868-0
www.experteach.de

**Know-how: Compliance in virtuellen Infrastrukturen**

Willkommen im Lizenz-Labyrinth

von Torsten Boch



Gehen Unternehmen dazu über, Anwendungen oder ganze Desktops zu virtualisieren, um die Betriebs- und Verwaltungskosten ihrer IT zu optimieren, hat dies Auswirkungen auf die Lizenzierung der eingesetzten Software. Eine zentrale Fragestellung ergibt sich daraus, ob die Hersteller der eingesetzten Produkte diese Benutzer- oder Hardware-zentrisch lizenzieren. Daran anknüpfend muss sich der IT-Verantwortliche seinen mit Lizenz-Fußangeln gepflasterten Weg zur gewünschten Infrastruktur bahnen. Dieser Artikel gibt Hinweise, wie die IT die Kontrolle über die Compliance behält.

Arbeitsplatz-Virtualisierung hat ein signifikantes Momentum in Unternehmen erreicht, denn die Virtualisierungstechnologien sind inzwischen ausgereift und unterstützen nahezu jede Art von Endgerät. Die korrekte Lizenzierung der virtualisierten Software ist allerdings nach wie vor eine große Herausforderung, die bei der Umsetzung eines Virtualisierungs-Projekts nicht außer Acht gelassen werden darf. Wie groß die Komplexität der Lizenzierung ist, hängt davon ab, welche Technologien zum Einsatz kommen und welche Regeln die Hersteller der jeweils bereitgestellten Software definiert haben. Fundiertes Know-how, funktionierende Prozesse und leistungsfähige Werkzeuge sind unerlässlich, um den rechtlichen Anforderungen der Hersteller gerecht zu werden.

Viele Softwarehersteller zögern noch immer, ihre Lizenzmetriken auf Benutzer anstatt auf Hardware auszurichten. Windows und die meisten Anwendungen von Microsoft werden beispielsweise weiterhin nach physischen Geräten lizenziert und damit die Charakteristik einer auf Benutzer ausgerichteten Virtualisierung ignoriert. Da die standortunabhängige Nutzung einer Anwendung auf mehreren

Geräten aber ein wesentlicher Vorteil einer Arbeitsplatz-Virtualisierung ist, liegt es auf der Hand, dass die Lizenzierungsfrage hier zum Spielverderber werden kann.

Empfehlungen zu Virtualisierung und Compliance

Bereits im Jahr 2011 hat Gartner eine Forschungsarbeit über die Virtualisierung von Arbeitsplätzen aus lizenzrechtlicher Perspektive durchgeführt und kommt darin zu interessanten Schlüsselerkenntnissen:

- Kundenerwartungen reichen von weniger bis mehr Lizenzkosten.
- Ohne ein strammes Lizenzmanagement besteht für Kunden die Gefahr hoher Nachzahlungen bei Lizenzaudits der Hersteller.
- Lösungsansätze, die den Lizenzbedarf allein über die Inventarisierung der Software ermitteln, werden fehlschlagen.
- Die virtuelle Bereitstellung von Software wird Lizenzkosten und Risiken in den meisten Fällen ansteigen lassen.

Daraus leiten sich laut Gartner folgende Empfehlungen ab:

- Hersteller, Lieferanten oder Systemintegratoren sollten in die Verantwortung genommen werden, korrekte Lizenz-

bedingungen für genau definierte Konfigurationen festzulegen.

- Es muss sichergestellt sein, dass der verantwortliche Lizenzmanager in alle Maßnahmen zur Einführung von Virtualisierungstechnologien sowie bei nachgelagerten Änderungen der Konfiguration eingebunden ist.
- Es empfehlen sich regelmäßige Validierungskontrollen, um zu gewährleisten, dass die genehmigten Konfigurationen beibehalten werden.
- Die Compliance sollte über den gesamten Software-Lebenszyklus hinweg dokumentiert werden.

Um diesen Empfehlungen Folge leisten zu können, sollte das Lizenzmanagement nach Best Practices prozessorientiert ausgerichtet und mit entsprechenden Befugnissen ausgestattet sein sowie nachhaltig betrieben werden.

Vielfältige Szenarien mit vielfältigen Konsequenzen

Die Virtualisierung von Anwendungen und Arbeitsplätzen gibt es in verschiedenen Ausprägungen und abhängig davon ergeben sich unterschiedliche Lizenzierungsfragen wie etwa:



- Remote Desktop: Windows-Desktop mit Server-Betriebssystem über Fernzugriff (Terminalserver)
- Lokale virtuelle Maschine: Verschiedene Betriebssysteme, die in virtuellen Maschinen auf derselben Client-Hardware betrieben werden (etwa Citrix Xen-Client oder VMware Horizon View).
- Virtuelle Anwendung: Anwendungen, die isoliert vom Betriebssystem auf einem Server oder dem Client ausgeführt werden (beispielsweise Citrix XenApp, Microsoft Remote App, Microsoft App-V, VMware ThinApp).
- Hosted Virtual Desktop: Windows-Desktop mit Client-Betriebssystem über Fernzugriff (Virtual Desktop Infrastructure; VDI).
- Neben diesen Szenarien gibt es weitere Virtualisierungsansätze, beispielsweise Microsoft Enterprise Desktop Virtualisierung (MED-V) oder Microsoft Windows Thin PC (WinTPC).

All diese Technologien können genutzt werden, um Softwareanwendungen virtualisiert bereitzustellen. Allerdings sind ihre Auswirkungen auf die Lizenzierung mitunter sehr unterschiedlich. Denn weil es keinen Standard gibt, hat jeder Hersteller die Freiheit, eigene Regeln und Bedingungen zu definieren und zwischen Technologien zu unterscheiden.

Dies hat zur Folge, dass sich Voraussetzungen und Machbarkeit einer Virtualisierungs-Lösung nicht aus rein technischer Perspektive validieren lassen. Vielmehr ist für jeden relevanten Softwarehersteller zu klären, welche lizenzrechtlichen Auswirkungen das vom Unternehmen präferierte Szenario hat; ein erheblicher Aufwand, wenn wir berücksichtigen, dass ein normaler Computerarbeitsplatz 30 verschiedene Anwendungen oder mehr aufweist.

Lizenzierung der Virtualisierungs-Technologie

Zunächst einmal muss die Technologie selbst richtig lizenziert werden. Während Microsoft Remote Desktop Services und Hyper-V mit Windows Server, MED-V mit Microsoft Desktop Optimization Pack (MDOP) und WinTPC mit Windows Software Assurance bündelt, bieten andere Hersteller wie Citrix und VMware be-

sondere Produktlizenzen an. Dabei ist zu beachten, dass Sie unter Umständen verschiedene Lizenzen für eine Implementierung benötigen, beispielsweise für die zentrale Lizenzierungstechnologie selbst, sowie zuzüglich Lizenzen für den Zugriff nutzender Anwender oder Geräte.

Im Einzelfall kann es technisch sinnvoll sein, verschiedene Virtualisierungs-Methoden zu kombinieren. So ist es durchaus denkbar, einen Hypervisor von VMware zu verwenden, um virtuelle Maschinen von VMware zu betreiben und diese den Anwendern über Citrix XenDesktop zur Verfügung zu stellen.

Lizenzierung eines Server-Betriebssystems

Ein Server-Betriebssystem kann als Träger der Virtualisierungstechnologie eine Rolle spielen, wobei es entweder unmittelbar selbst dem Endnutzer zur Verfügung steht (etwa als Remote Desktop Service) oder lediglich virtuelle Maschinen hostet, auf die zugegriffen wird. Letzteres ist genauer zu betrachten, weil es in einer lizenzrechtlichen Beurteilung einen Unterschied macht, ob das Betriebssystem ausschließlich Virtualisierungsdienste bereitstellt oder ob weitere Anwendungen das System benutzen. Als "weitere Anwendung" gilt beispielsweise jede andere Software, die dort gestartet wird – auch wenn es sich lediglich um einen Virenschanner handelt.

Bei der Bereitstellung von Remote Desktop Diensten (Terminalserver), über die Benutzer Anwendungen per Fernzugriff nutzen, erweitert sich die Lizenzpflicht auch auf die sogenannten "Client Access Licenses" (CAL), die je zugreifendem Gerät oder Benutzer anfallen.

Lizenzierung eines virtuellen Client-Betriebssystems

Im Mittelpunkt aller Diskussionen über die korrekte Lizenzierung virtueller Arbeitsplätze liegt das Client-Betriebssystem Microsoft Windows. Das ist kein Wunder, erklärt doch Microsoft in zahlreichen Dokumenten, wie die lizenzrechtliche Gestaltung in solchen Fällen aussieht, und erzeugt damit eine Komplexität, wie sie bislang nur von Serversoftware im Rechenzentrum bekannt war. Die darin lie-

gende Komplexität erschließt sich alleine aus den Fragen, die sich der IT-Verantwortliche dabei stellen muss:

- Welcher Datenträger wird verwendet, um das virtualisierte OS aufzusetzen?
- Auf welchem Host wird die virtuelle Maschine betrieben?
- Wird die virtuelle Maschine vorübergehend auf anderen Hosts ausgeführt?
- Wann wurde die virtuelle Maschine dauerhaft auf einen anderen Host verlagert?
- Werden auf dem gleichen Host andere virtualisierte Client-Betriebssysteme ausgeführt?
- Ist ein zugreifendes Gerät das primäre Arbeitsgerät eines Benutzers oder nicht?
- Gehört das zugreifende Gerät der Organisation oder dem Benutzer?
- Erfolgt der Zugriff von innerhalb des lokalen Netzwerks oder von außerhalb?
- Erfolgt der Zugriff sporadisch oder regelmäßig?
- Nutzen mehrere Personen ein virtualisiertes Client-Betriebssystem gemeinschaftlich?
- Nutzt ein Benutzer immer denselben virtuellen Desktop oder verschiedene?
- Auf wie viele virtuelle Client-Desktops greift ein Benutzer "gleichzeitig" zu?
- Welche Prozessorplattform hat das zugreifende Gerät (ARM/Intel/AMD)?
- Welches Betriebssystem wird auf dem zugreifenden Gerät genau ausgeführt?
- Wie ist das lokale Betriebssystem des zugreifenden Geräts lizenziert?

Microsoft legt ausdrücklich fest, dass die Visualisierung der Benutzeroberfläche eines Client-Betriebssystems auf einem anderen, über ein Netzwerk zugreifendem Gerät mit einer gewöhnlichen Windows-Lizenz nicht erlaubt ist. Dies gilt auch dann, wenn das entsprechende zugreifende Gerät bereits mit einer gültigen Windowslizenz für die lokale Kopie ausgestattet ist.

Stattdessen sieht Microsoft vor, dass der Zugriff auf einen virtuellen Client-Desktop über eine sogenannte "Virtual Desktop Access" (VDA)-Lizenz zu berechtigen ist. Dieses Recht ist jedoch auch in der von Microsoft angebotenen Software Assurance enthalten. Sollte sich das zugreifende Gerät jedoch im persönlichen Eigentum des Mitarbeiters befinden und der Zugriff innerhalb des lokalen Netzwerks



Stichtag	Identifiziertes Endgerät	Softwareprodukt	Identifiziertes Endgerät	Identifizierte Person	Programmname	Anwendungshost
25.10.2013 13:59:42	23.01.2014	Microsoft, Office Enterprise 2007	MA2-HB-086	Valentine, Vincent	WINWORD.EXE	MA2SRV
25.10.2013 13:59:42	23.01.2014	Microsoft, Office Enterprise 2007	MA2-HB-086	Valentine, Vincent	POWERPNT.EXE	MA2SRV
25.10.2013 13:47:42	23.01.2014	Microsoft, Office Enterprise 2007	MA2-HB-086	Valentine, Vincent	WINWORD.EXE	MA2SRV
25.10.2013 13:47:42	23.01.2014	Microsoft, Office Enterprise 2007	MA2-HB-086	Valentine, Vincent	POWERPNT.EXE	MA2SRV
25.10.2013 13:59:42	23.01.2014	Microsoft, Office Enterprise 2007	MA2-HB-086	Valentine, Vincent	EXCEL.EXE	MA2SRV

Ein Werkzeug zur Lizenzverwaltung liefert wie in diesem Beispiel Nutzungsdaten einzelner Anwendungen, muss aber dazu tief in die IT-Prozesse integriert sein

erfolgen, muss dieser ausnahmsweise über eine "Companion Device Subscription License" (CDL/CSL) lizenziert werden.

Es ist offensichtlich, dass die Lizenzierung von virtuellen Desktops mit Client-Betriebssystem eine weitaus höhere Komplexität aufweist, als bei gerätelokalen Windowsinstanzen oder klassischen Terminal Service-Szenarien. Nun sind sogar der Nutzungsort und die Eigentümerschaft des Geräts von Bedeutung. Deshalb ist nicht nur eine umfassende Ermittlung der tatsächlichen Konfiguration und der faktischen Nutzung virtueller Desktops erforderlich, sondern auch eine Berücksichtigung von Implikationen für ein IT-Asset-Management, das unter Umständen relevante Geräte umfasst, die zwar Eigentum der Mitarbeiter sind, aber beruflich genutzt werden.

Lizenzierung virtualisierter Anwendungen

Softwareanwendungen, die entweder über einen virtuellen Desktop bereitgestellt oder auf andere Weise virtuell zugänglich gemacht werden, unterliegen grundsätzlich denselben Lizenzbedingungen wie die konventionelle, lokale Bereitstellung auf physischen Geräten. Als Grundregel bei der Ermittlung des Lizenzbedarfs kann davon ausgegangen werden, dass in vielen Fällen pro Installation/Gerät oder pro Benutzer abgerechnet wird. Da die Hersteller Virtualisierungsszenarien zumeist sehr verschieden beurteilen und regeln, gibt es allerdings keine allgemeingültige Sicht darauf. Während Microsoft auf die Metrik aus den Produktnutzungsrechten pocht, gewährt

Adobe bei virtualisierten Anwendungen eine Pro-Benutzer-Metrik, die in der Regel um einiges einfacher gehandhabt werden kann.

Die Beibehaltung der Gerätemetrik kann bei virtualisierten Anwendungen eine gewisse Lizenzfalle darstellen. Keine Frage, dass hier nicht die physischen Hosts, sondern die zugreifenden Geräte gemeint sind. Diese Systematik legt den Paradigmenkonflikt offen, der zwischen benutzerspezifischer Bereitstellung virtueller Anwendungen (Zugriffsrechte werden primär über Benutzerkonten gesteuert) und der althergebrachten Lizenzierung nach Geräten entsteht.

Durch die Gewährung von Zugriffsrechten für ein Benutzerkonto wird letztlich nicht automatisch valide definiert, wie viele Lizenzen erforderlich sind. Die Berechtigung einer definierten Anzahl von Benutzern lässt in diesem Fall kaum Rückschlüsse zu, wie viele Lizenzen tatsächlich benötigt werden. Nutzen beispielsweise zehn berechnete Anwender eine virtualisierte Anwendung mit jeweils drei Endgeräten werden insgesamt 30 Lizenzen fällig! Folglich kommt der IT-Verantwortliche nicht darum herum, die tatsächliche Nutzung unter Berücksichtigung der Geräteidentität zu messen und valide auszuwerten.

Letztlich – und nicht nur, weil der eine oder andere Softwarehersteller es vielleicht sogar verbietet, seine Software überhaupt zu virtualisieren – empfiehlt es sich von vornherein, die Lizenzbedingungen mit

jedem einzelnen relevanten Hersteller verbindlich abzuklären.

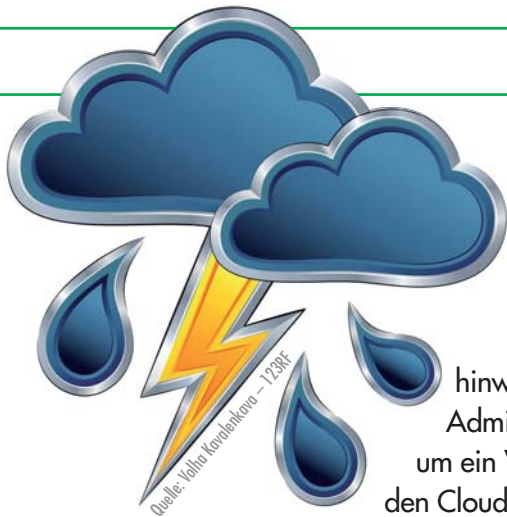
Implikation für das moderne Lizenzmanagement

Lizenzmanagement setzt in jedem Fall valide Prozesse in allen relevanten Bereichen des Softwarelebenszyklus voraus, wenn Risiken und Kosten damit erfolgreich adressiert werden sollen. Sobald Arbeitsplätze von Anwendern ganz oder teilweise virtualisiert werden, kommt diesem Grundsatz noch größere Bedeutung zu. Dies ist dem Umstand geschuldet, dass die Hersteller zum Teil sehr komplizierte Lizenzbedingungen geschaffen haben, die es bereits im Rahmen der Softwareverteilung, des Configuration Managements sowie des Change Managements zu beachten gilt.

Darüber hinaus benötigen Sie für ein wirkungsvolles Lizenzmanagement auch ein geeignetes Werkzeug, das in der Lage ist, diese Komplexitäten abzubilden, und dabei immer größtmögliche Transparenz und Nachvollziehbarkeit sicherstellt. Nur dann können sich Unternehmen sicher sein, dass sie auch hinsichtlich der virtuellen Infrastrukturen korrekt lizenziert sind. Unabhängig davon versetzen derartige Lösungen Lizenzverwalter außerdem in die Lage, bei Nachkäufen, Vertragsabschlüssen sowie Audits besser zu argumentieren und beispielsweise sogar die Lizenzkosten reduzieren zu können.

Bestens aufgestellt sind an dieser Stelle vor allem Lösungen, die das Management von Lizenzen als Teil eines ganzheitlichen Managements moderner Arbeitsumgebungen betrachten. Das Spektrum reicht inzwischen nahtlos vom klassischen Computer über das mobile Gerät bis hin zu virtualisierter Softwarebereitstellung. Gerade Letzteres, aber auch generell erfordert erfolgreiches Lizenzmanagement daher eine prozessual vernetzte IT, die ohne Medienbrüche alle relevanten Schritte abbilden, steuern, auswerten und valide nachvollziehen kann. Anders formuliert: Lizenzmanagement ist kein eigener Prozess, sondern eine Querschnittsfunktion, die in vielen IT Prozessen erfüllt werden muss. (jp)

Torsten Boch ist Senior Product Manager bei der Matrix42 AG in Neu-Isenburg.



Know-how: Sicherer IT-Betrieb in der Cloud Blitzschlag vermeiden

von Henning von Kielpinski

Bei vielen Unternehmen verteilen sich die IT-Systeme über mehrere Standorte hinweg und werden als Cloud-Dienste über das Internet bezogen. Das birgt für den Administrator zweierlei Herausforderungen: Erstens ist die potenzielle Angriffsfläche um ein Vielfaches größer geworden. Zweitens entzieht sich ein Teil der Infrastruktur bei den Cloud-Modellen schlicht und einfach der direkten Kontrolle. Wir beschreiben, welche Risiken es genau gibt und wie sie sich beheben oder zumindest eingrenzen lassen.

Der IT-Betrieb hat sich in den letzten Jahren rasant geändert: Früher ging es darum, die IT-Systeme eines Unternehmens in den eigenen Rechenzentren zu administrieren und zu sichern. Das ließ sich relativ leicht durch eine physische und logische Verkapselung nach dem Zwiebelprinzip realisieren: Das entsprechende Netz wurde im Idealfall über einen (einzigen) Zugangspunkt mit einer restriktiven Firewall abgesichert. Systeme, die von außen erreichbar sein mussten, zum Beispiel durch Partner und Lieferanten, wurden und werden in einer DMZ betrieben und wiederum über eine oder mehrere Firewalls gesichert.

Dieses Zwiebelprinzip der Absicherung gegen äußere Angriffe hat sich bis heute bewährt und ist relativ gut kontrollierbar. Jede externe Anbindung an das zentrale Netzwerk, zum Beispiel für externe Standorte oder mobile Mitarbeiter, wird in einem solchen Kontext über ein VPN realisiert, das unter der Verwendung von IPSec oder SSL die Punkt-zu-Punkt-Verschlüsselung sicherstellt. Die Kontrolle über die gesamte Infrastruktur obliegt dabei dem Administrator. Dies funktioniert bei der Nutzung von Cloud-Diensten leider nicht so einfach, was wir am Beispiel der Amazon-Cloud verdeutlichen wollen.

Cloud-Dienste durch VPN absichern

Die gängigen und preislich interessanten IaaS-Angebote (Infrastructure-as-a-Service) aus der Amazon-Cloud erlauben jeglichen Traffic aus dem Internet zur entsprechenden

IaaS-Instanz beziehungsweise zum virtuellen Server. Die Absicherung erfolgt erst auf der durch den Benutzer zu konfigurierenden Firewall des Betriebssystems in der Cloud. Das bedeutet: Ein potentieller Angreifer kann per se schon einmal bis auf die Betriebssystemebene gelangen, da keine dedizierten Sicherheitsappliances wie Firewalls vorgeschaltet sind. Darin verbirgt sich ein hohes Sicherheitsrisiko.

Wie also vorgehen? Gerade bei der Nutzung von Cloud-Diensten sollte eine VPN-Verbindung den Zugang schützen. Anstelle eines Endpunktes an einer dedizierten Firewall ist es besser, die entsprechenden VPN-Server direkt auf dem Gastbetriebssystem in der Cloud zu installieren und zu konfigurieren. Ein minimalistischer Weg, dies bei Amazons EC2 zu realisieren, ist die Verwendung eines PPTP-Servers. Dieser sorgt zwar für maximale Kompatibilität, bietet aber dennoch einige Sicherheitslücken. Alternativ ist OpenSSL die sicherere Variante.

Als Einstiegsinstanz in den virtuellen Rechenpark kann eine kostengünstige Micro-Instanz dienen. Das Problem der wechselnden IP-Adressen des Endpunktes umgeht der IT-Verantwortliche dann zum Beispiel mit DynDNS. Optimalerweise stellt er dann auch sicher, dass nicht nur der Transportweg gesichert ist, sondern eine echte End-To-End-Sicherheit gewährleistet ist. Eine solche lässt sich zum Beispiel durch die Verwendung von Mechanismen aus dem XML Security Framework von W3C zur Verschlüsselung der Payload erreichen.

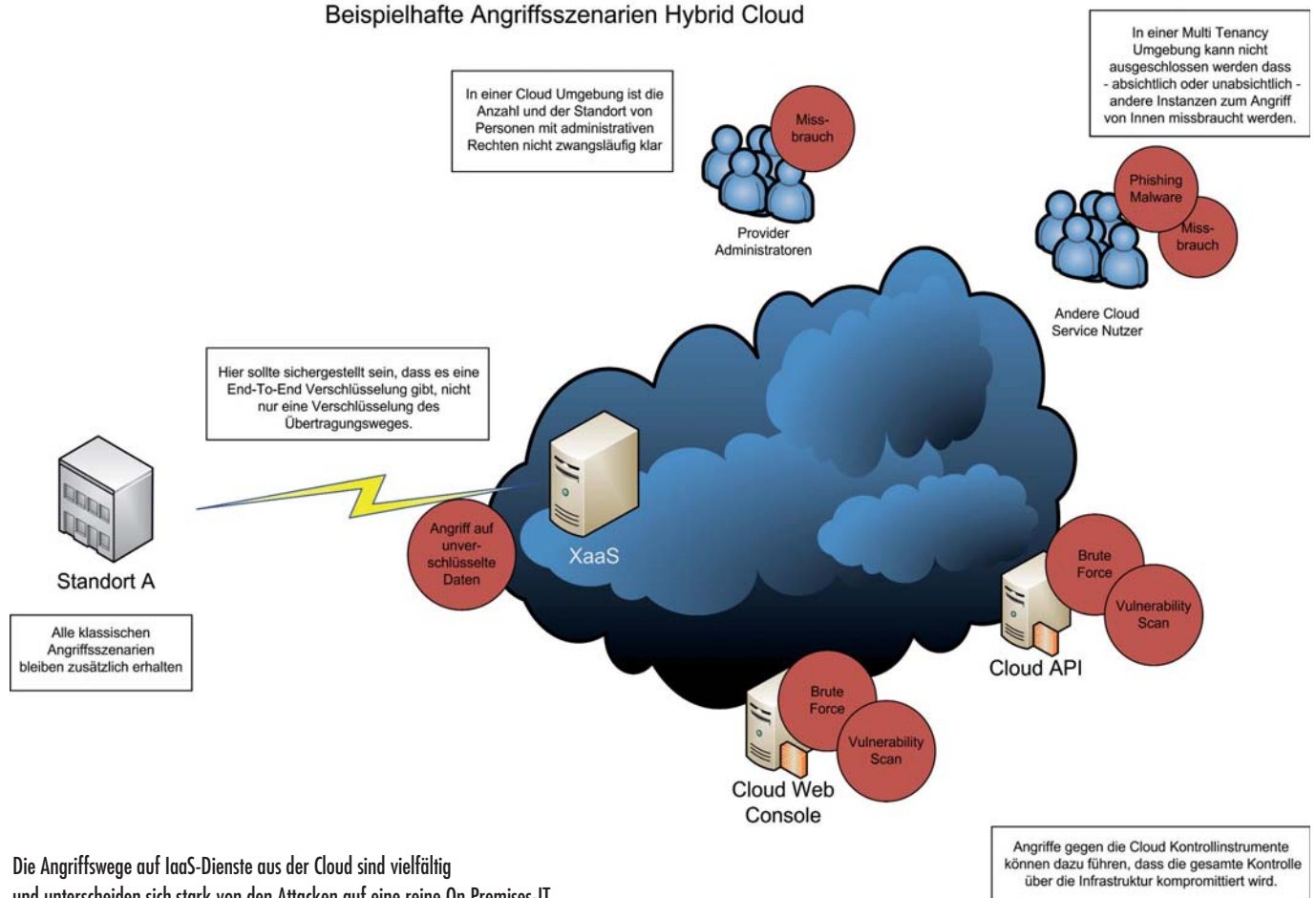
Angriffe aus dem Web

Trotz aller Sicherheitsvorkehrungen öffnen Unternehmen bei Cloud Computing eine im Vergleich zu einer "herkömmlichen" Security Appliance oder Firewall relativ breite Front möglicher Sicherheitslücken auf Ebene des Betriebssystems in Richtung des Internets. Dass diese Tatsache den Angreifern bekannt ist und nicht nur eine theoretische Überlegung, belegen die Ergebnisse einer Analyse von Alert Logic 2013. Das Angriffsverhalten auf Systeme von Cloud-Providern unterscheidet sich messbar von Angriffen auf die klassischen Datacenter.

Letztere werden neben der Brute Force Methode, also dem einfachen Knacken von Passwörtern mittels Ausprobieren, aufgrund der gehärteten Endpunkte inzwischen stark über eingeschleuste Malware angegriffen. Die Cloud-Provider hingegen sehen sich derzeit deutlich mehr Attacken aus dem Web gegenüber. Ziele der Angreifer sind hier häufig die Logik und Datenbankebenen der verwendeten Applikationen. Das Beispiel einer gehackten Bank aus Indien, die versehentlich die JMX-Konsole ihrer Applikation im Internet stehen hatte, ist ein mahnendes Beispiel für die Risiken von offenen Ports – trotz vermeintlicher Passwortsicherheit. Alternativen gibt es natürlich auch hier, zum Beispiel das Virtual Privat Cloud-Angebot, das einen Hardware-VPN-Endpunkt beinhaltet. Dieses kann jedoch relativ schnell den eigentlichen Kostenvorteil der Cloud vollständig eliminieren. Denn neben der erhöhten Preise einer Virtual Privat Cloud berechnet Amazon jede



Beispielhafte Angriffsszenarien Hybrid Cloud



Die Angriffswege auf IaaS-Dienste aus der Cloud sind vielfältig und unterscheiden sich stark von den Attacken auf eine reine On Premises-IT

Stunde der Verwendung eines Hardware-VPN-Endpunktes extra.

Nicht zuletzt gibt es zusätzliche Angriffsvektoren durch die administrativen Tools der Cloud selbst. Webtools und APIs zur Steuerung der Cloud-Funktionalität können im schlimmsten Fall einem Angreifer nicht nur die Kontrolle über einzelne Rechner, sondern über gesamte Abschnitte der Cloud-Infrastruktur ermöglichen.

Risiko geteilte Verantwortung

Doch selbst wenn die Anbindung einer fremdgehosteten Lösung durch die Verwendung der beschriebenen Sicherheitsvorkehrungen und eines dedizierten Zugriffssrechners ausreichend sichergestellt ist, bewegen sich IT-Verantwortliche in einen zweiten Themenkomplex hinein: den der geteilten Verantwortung.

Während Unternehmen mit einem eigenen Rechenzentrum die Aktualität der Sicherheitsvorkehrungen und deren Funktionieren messbar überprüfen können, müssen sie in der Cloud darauf vertrauen, dass der

Cloud-Provider seinen Verpflichtungen auf die Einhaltung von Best Practices nachkommt. Eine tatsächliche Überprüfung oder ein Monitoring ist an dieser Stelle selten möglich. Es herrscht also der Grundsatz des Vertrauens in den Provider.

Keiner will es gewesen sein

Tritt der Fall eines Datenmissbrauchs zu Tage, steht zuallererst der Nachweis an, wie die Daten kompromittiert wurden und ob dies ein Versäumnis des Cloud-Providers möglich gemacht hatte. Oftmals kommt dann heraus, dass interne Mitarbeiter ihren kaum eingeschränkten Zugang zu den Daten genutzt haben. Die Möglichkeit des Zugriffs eines Administrators oder IT-Mitarbeiters auf Daten innerhalb der Unternehmens-Infrastruktur ist eine extrem sensible Thematik. Konsequenterweise beschränken Sicherheitsverantwortliche den Zugriff auf sensible Daten auf einen kleinen, vertrauensvollen Benutzerkreis, um eventuelle Risiken zu minimieren.

Ist es aber doch einmal der Cloud-Provider, dessen Versäumnis für einen Datenmiss-

brauch oder einen Stillstand der IT gesorgt hat, begleicht der Provider dies normalerweise durch die Rückerstattung von bezahlten oder zukünftigen Infrastrukturkosten an das Unternehmen. Was ein solcher Vorfall jedoch in Form von rechtlichen Problemen, dem Verlust von Kundenvertrauen oder auch die Einbuße von Intellectual Property für das Unternehmen bedeutet, findet dabei keine Berücksichtigung. Dieses Risiko und seine Folgen trägt das Unternehmen allein.

Die durch Standardisierungsgremien wie PCI, aber auch durch Cloud-Provider wie Amazon propagierte "SharedResponsibility" enthält also zusätzliche Risiken, die ohne weiteres nicht klar abgegrenzt sind. SharedResponsibility entlässt ein Unternehmen in keiner Weise aus seiner Verantwortung für den letztendlichen Verbleib oder den Missbrauch von Kunden- oder Unternehmensdaten. Stattdessen kommt erschwerend hinzu, dass sich das Unternehmen die Verantwortung für die tatsächliche Sicherheit dieser Daten mit einem Cloud-Provider teilen muss.



Verschlüsseln in der Cloud

Eine zumindest weitergehende Sicherheit bietet die von den meisten Cloud-Providern angebotene Verschlüsselung der virtuellen Maschinen innerhalb der Cloud-Infrastruktur. Dies würde zumindest eine Steigerung der gefühlten Sicherheit bedeuten. Eine solche Verschlüsselung schützt zwar die Daten nicht auf ihrem Übertragungsweg. Aber falls jemand in den Besitz der VM käme, könnte er sie nicht ohne weiteres auslesen.

Allerdings gibt es hier zu bedenken: Fast alle Cloud-Provider nutzen einen Master Key für die verschlüsselten Daten und machen von ihm auch Gebrauch. Einige Beispiele hierzu: Häufig werden automatisierte Scans auf Copyright-Verletzungen oder Anfragen von Regierungsorganisationen genannt. In diesen Fällen händigen Cloud-Provider die Daten unverschlüsselt aus. Gerade im Hinblick auf die Verquickung von Tätigkeiten der Geheimdienste oder um sich vor Wirtschaftsspionage zu schützen, sollten Unternehmen ihre schützenswerten Daten zusätzlich sichern.

Des Weiteren müssen sich IT-Verantwortliche – ob sie möchten oder nicht – des grundsätzlich gegebenen Risikos bewusst sein, dass auch Administratoren des Cloud-Providers durch den Master Key Zugang zu den Daten haben und diese, je nach wirtschaftlicher Lage, theoretisch auch missbrauchen könnten. Entgegenwirken lässt sich dem beispielsweise durch die unternehmensseitige Verschlüsselung der in der Cloud abgelegten Daten mit eigenen Schlüsseln. Dazu können die IT-Verantwortlichen entweder auf Filesystem-Ebene verschlüsseln, wie zum Beispiel mit Loop-AES, TrueCrypt oder Crypto-FS, oder die Verschlüsselung der Daten innerhalb der Applikation sicherstellen. MySQL und Oracle zum Beispiel bieten beide AES-Verschlüsselung der Datensätze innerhalb der Datenbank an.

Zugegebenermaßen sind Bedrohungsszenarien dieser Art durch Insider nicht Cloud-spezifisch. Der Unterschied aber ist der Multiplikatoreffekt, den ein Cloud-Provider durch seine eigenen Administratoren und eventuell zusätzlich involvierte

dritte Parteien darstellt. Eine Kontrolle ist durch einen sicherheitsbewussten Kunden kaum möglich. Insgesamt gesehen reduziert sich die Shared Responsibility also auf ein reines Vertrauensverhältnis.

Prozesse müssen definiert sein

Wie schon skizziert, ist die Sicherheit in einer verteilten Infrastruktur herausfordernd und komplex und basiert zu großen Teilen auf dem Vertrauen in den jeweiligen Partner. Hierbei kommt nun eine weitere Komponente ins Spiel: die Prozesse, die Kommunikation und Austausch mit den Partnern regeln. Die IT Infrastructure Library (ITIL) hat sich in vielen Unternehmen zumindest als Richtlinie für den Betrieb der Infrastruktur etabliert. Sie sieht sich nun vor die Herausforderungen der Cloud und anderer schnell wechselnder Technologien gestellt. Umfragen zum Status Quo zeigen jedoch, dass für Cloud-Services sehr selten Prozesse auf Basis von ITIL verwendet werden, obwohl doch die ITIL-Prozesse in der Theorie unabhängig von der verwendeten Technologie betrachtet werden.

Ein Punkt, warum ITIL-Prozesse in Cloud-Umgebungen oft nicht stringent umgesetzt werden, ist sicher die heimliche Verwendung von Cloud-Services innerhalb des Unternehmens, ohne dass die IT-Abteilung davon überhaupt etwas mitbekommt. Häufig genanntes Beispiel ist hier die Verwendung von DropBox und Skype. Diese Schatten-IT wird oftmals von den jeweiligen Fachabteilungen aus Bequemlichkeit und unter Ignoranz aller gebotenen Datensicherheitsregeln genutzt. Denn sie ist oftmals schnell verfügbar und einfach in der Abrechnung – zwei in der Tat starke Argumente für Cloud Services.

Ein zweiter Punkt für eine mangelnde ITIL-Umsetzung ist, dass bei der Verwendung von Cloud-Diensten Unternehmensgrenzen überschritten und Technologien eingesetzt werden, die deutlich von den bestehenden Unternehmenssystemen abweichen. Problematisch ist hierbei, dass sich in der Regel keine oder wenige brauchbare ITIL-kompatible Schnittstellen finden, über die sich Changes und Incidents übermitteln lassen.

Häufig sind die Informationen, die dann vom Provider zurückfließen, zu spärlich. Zum anderen sind viele Changes in der Cloud durch automatisierte Deployments im Self-Service-Verfahren möglich – das ist ja gerade einer der wesentlichen Vorteile der Cloud. Die Prozess-Definitionen aus dem ITIL tun sich jedoch schwer, solche Szenarien 1-zu-1 abzubilden. Nicht umsonst geben in einer Umfrage von 451 Research im Jahr 2013 68 Prozent der Unternehmen an, dass die Migration zur Cloud nicht wegen IT-Problemen stockt, sondern aus sonstigen Unternehmensgründen. Fehlende Prozesse sind hier sicher ein großer Faktor.

Fazit

Die Cloud hat inzwischen das Tal der Desillusionierung erreicht. Und dies vor allem aus Sicherheitsaspekten. Das ist nicht zwangsläufig schlecht, befreit es doch den Cloud-Begriff von durch Hype getriebenen Erwartungen und falschem Aktionismus. Trotzdem hat die Cloud noch einen weiten Weg vor sich, um tatsächlich auch im Unternehmensumfeld Mainstream zu werden. Auch vor der NSA-Affäre war Sicherheit der primäre Schmerzfaktor, sowohl bei der Auswahl des Providers als auch bei der Cloud-Thematik. Trotzdem gibt es kaum Bestrebungen, die Cloud-Sicherheit als eigenen Punkt auf die IT-Security-Agenda zu setzen.

Letztlich wird Cloud-Sicherheit oft nur als ein Bestandteil der IT-Security-Strategie eines Unternehmens angesehen. Und dies kann fatale Folgen haben. Denn Cloud-Sicherheit umfasst deutlich mehr und vor allem andere Szenarien. Sie ist deshalb auch gesondert zu betrachten. Beziehen IT-Verantwortliche den Overhead für einen verantwortungsvollen Umgang mit Daten in die Kosten-Kalkulation eines Cloud-Projektes mit ein, stellen sie schnell fest, dass billig nicht unbedingt günstig für das Unternehmen ist. Oder dass eine sichere Cloud-Lösung eben doch nicht unbedingt billig ist. Die Kosten-Nutzen-Risiko-Aspekte sind also immer von Fall zu Fall gegeneinander abzuwägen. (In)

Henning von Kielpinski ist Cloud-Experte bei der Consol Consulting & Solutions Software GmbH.

Windows Server 2012 R2



Vier Auflagen und kein bisschen schlanker: Der neue Boddenberg zum aktuellen Microsoft-Server-Betriebssystem wartet mit einem Betriebshandbuch zum Server

2012 R2 auf und setzt dabei nicht zwingend Vorkenntnisse im Bereich der Windows-Server-Administration voraus. Damit dürfte das Buch Admin-Einsteigern als deutschsprachige Referenz dienen, denn der Autor nähert sich mit einem Rückblick der bisherigen Microsoft-Server-Versionen der aktuellen Version und findet auch genügend Freiraum, Lizenzierung, Dimensionierung von Hardware sowie die Protokolle vorzustellen. Damit

nicht genug, denn auch ein Blick in die .NET-Philosophie wird gewährt, bevor der Leser detailliert über Active Directory-Domänendienste, Netzwerkdienste, LDS, RMS und Zertifikatdienste informiert wird. Die Federation Services (interessant für Office 365) finden ebenfalls eine kurze Beschreibung.

Löblich sind WSUS, Firewall und NAP beschrieben, wenngleich das VPN nicht vergessen wird. Für einen noch tiefergehenden Einblick in diese Dienste bietet sich dann Spezial-Literatur an. Der Fokus der Beschreibungen inklusive Grafiken ist deutlich auf den Praxiseinsatz ausgerichtet. EFS, iSCSI und RMDs sind in den Dateisystemdiensten ebenso beschrieben wie klassische Dateidienste. Bei den Server-Diensten finden sich Abschnitte zu Druckserver, Webserver (IIS), Terminaldienste, SharePoint (kurz angerissen), Hochverfügbarkeit und eine gelungene Beschreibung von Hyper-V.

Den Abschluss bilden die Grundlagen zum Scripting und Automatisierung mit der PowerShell.

Fazit

Die Fachkenntnisse des Autors stehen außer Frage, doch wäre es wünschenswert, dass Galileo die Inhalte auf zwei Bände verteilt, da die für erfahrene Admins nicht relevanten einleitenden Kapitel dazu beitragen, dass das Buch auf mittlerweile fast 1.400 Seiten angewachsen ist. Vermisst haben wir einen detaillierten Abschnitt zum IP-Adress-Management, das seit der 2012-Version im Server-Betriebssystem verfügbar ist.

Frank Große

Autor	Ulrich B. Boddenberg
Verlag	Galileo Computing
Preis	59,00 Euro
ISBN	978-3836220132

Bewertung (max. 10 Punkte)

9

Praxisbuch IT-Dokumentation



Bereits 2008 erschien das Buch unter demselben Titel und vom gleichen Autoren-Paar im Addison-Wesley-Verlag. Dort haben zuletzt Kürzungen stattgefunden, weswegen

der Titel nun deutlich überarbeitet im Hanser Verlag erschienen ist. Dabei haben sich die Autoren die Mühe gemacht, die kritischen Stimmen zur Erstauflage zu hören und vor allem die Entwicklungen der IT-Branche berücksichtigt. Im Detail bedeutet dies, dass die Besonderheiten neuer Techniken wie Virtualisierung oder verteilte Systeme Einzug in die Dokumentationsfelder und Dokumentationsanforderungen gefunden haben. Die Autoren wenden sich vom traditionellen Betriebshandbuch ab und konzentrieren sich in ihrer Strategie auf die praktischen Felder Support und Serviceorientierung.

Daraus ergibt sich, dass die IT-Dokumentation keineswegs nur verwaltende Aspekte erfüllen soll, sondern den prozessorientierten Faktoren Rechnung trägt, um IT-Organisationen die nötige Flexibilität bei der Service-Leistung zu ermöglichen.

Dem zugrunde liegen die branchenübergreifenden Anforderungen an die IT-Dokumentation, die den Einstieg und rechtlichen Rahmen der Materie liefern. In jedem Fall lesenswert ist der Folgeabschnitt, der sich mit der Strukturierung einer ganzheitlichen IT-Dokumentation befasst und Fallstricke vermeiden lässt, die eine wachsende IT-Dokumentation mit sich bringen kann. Die Inhalte sind zwar etwas trocken zu lesen, aber sowohl für interne als auch externe Audits ist das Verständnis entscheidend, um der geplanten IT-Dokumentation mehr Bedeutung als nur archiviertes Papier zu verleihen. Hierauf folgen praktische Abschnitte, die sich neben der Dokumentation von IT-Projekten und dem Notfallhandbuch insbesondere der IT-Betriebsdokumentation widmen, die in fünf Stufen eingeteilt und mit Beispielen belegt ist. Den Abschluss bildet die Präsentation der verschiedenen Dokumentations-Tools, die gewöhnlich am Markt zu finden sind.

Fazit

Eine funktionierende IT-Dokumentation kann alles andere als nebenbei geleistet werden. Auf knapp 450 informativ-gefüllten und klar strukturierten Seiten bieten die Autoren einen deutlichen Nutzwert. Davon können sowohl Administratoren, interne IT-Organisationen oder auch externe Dienstleister profitieren.

Die Struktur der methodischen Ansätze zeugt von einem durchdachten Konzept. Die Umsetzung im Buch erfolgt in erster Linie praxisorientiert anhand eines potentiellen Dokumentationsprojekts, was weitestgehend auch gelingt. Ein Werk in erster Linie für Praktiker, die bei entsprechender Umsetzung wahrscheinlich eine zusätzliche Arbeitskraft hinzuziehen müssen, da der Administrator dies alles nicht im Vorbeigehen erledigen kann.

Frank Große

Autor	Manuela Reiss, Georg Reiss
Verlag	Hanser
Preis	44,99 Euro
ISBN	978-3446437807

Bewertung (max. 10 Punkte)

9

Besser informiert: Mehr Fachartikel auf www.it-administrator.de

Unser Internetauftritt versorgt Sie jede Woche mit neuen interessanten Fachartikeln. Als Heftleser können Sie über die Eingabe des Link-Codes schon jetzt exklusiv auf alle Online-Beiträge zugreifen.



Nutzerberechtigungen konsistent verwalten

Berechtigungen für Netzwerke, Daten und Anwendungen finden sich an vielen Stellen und nur das Active Directory allein eignet sich kaum, um diese konsistent und nachvollziehbar zu verwalten. Mit Hilfe eines einheitlichen Identity- & Access-Managements lässt sich eine zentrale Stelle zur Steuerung der Benutzerrechte schaffen, die alle Teilbereiche der IT-Infrastruktur einbezieht und zudem die Erstellung von Reporten auf Knopfdruck erlaubt. Dabei sind sehr umfassende Einsatzmöglichkeiten denkbar. Unser Fachartikel im Web nennt diese.

Link-Code: E3W51

Software-Klone in Trainingsumgebungen

Ein Software-Rollout ist kein einfaches Unterfangen und mit hohen Kosten verbunden. Schlecht geschulte Anwender sind einer der wesentlichen Gründe, weshalb eine Softwareinvestition noch kostenaufwendiger wird. Virtuelle Trainingsumgebungen, sogenannte Software-Klone, können hier Abhilfe schaffen. Sie generieren ein objektorientiertes Abbild des zu implementierenden Systems, das aber mit exakt denselben Funktionen ausgestattet ist wie die Live-Anwendung. Der Online-Beitrag erläutert, welche Vorteile es bringt, Mitarbeiter mit einem solchen Software-Klon zu schulen.

Link-Code: E3W52

Anwenderbericht: Standardisierte Arbeitsplätze in der Tourismusbranche

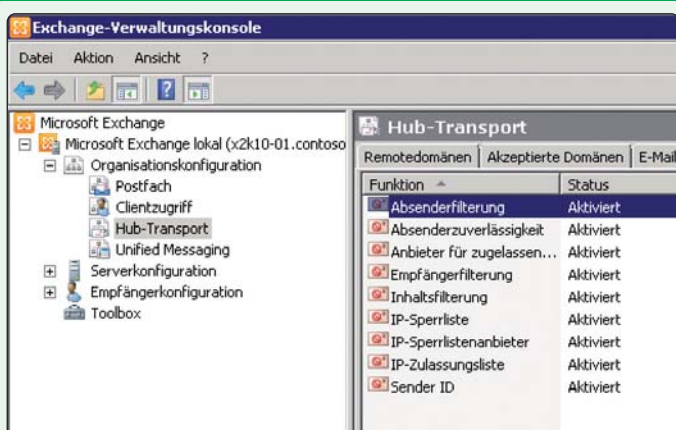
Die Auftragsvolumina von Veranstaltern und Reisebüros unterliegen starken zyklischen Schwankungen. Die zur Hochsaison anfallenden Datenmengen benötigen enorme Ressourcen und bringen die Technik oft an ihre Grenzen. Für optimale Arbeitsprozesse bedarf es leistungsfähiger Hardware und standardisierter Buchungsprozesse. Diese Optimierung strebte auch TUI Suisse an und entschied sich, die Hard- und Software der Filialen zu erneuern und standardisierte Arbeitsplätze auf Basis von Citrix Published Desktop zu installieren. Wir schildern, wie diese Umstellung ablief.

Link-Code: E3W53

Automatisierte PDF-Generierung zur Unterstützung von Systemprozessen

Ob Kundenkorrespondenz per E-Mail, Geschäftsdokumente oder via Online-Eingabemaske generierte Daten – in der digitalen Welt laufen tagtäglich Unmengen von Daten auf, die es so systematisch wie möglich zu bewältigen gilt. Systemspezifische Prozessabläufe wie eine strukturierte E-Mail-Ablage von Geschäftsbriefen, die den gesetzlichen Aufbewahrungsanforderungen entsprechen, helfen dabei, den Arbeitsablauf zu optimieren. Unser Online-Fachartikel erklärt, wie eine automatisierte PDF-Generierung die Datenaufbereitung und Dokumentenverwaltung unterstützt.

Link-Code: E3W54



In der Exchange-Verwaltungskonsolle kann der Administrator die Transport-Filter für den Spamschutz einzeln konfigurieren

Exchange bietet seit der Versionen 2003 Bordmittel, mit denen sich eine Exchange-Organisation vollkommen kostenlos vor Spam schützen lässt. Zwar arbeitet Exchange 2010 in diesem Bereich mit dem Forefront Threat Management Gateway 2010 und Forefront Protection für Exchange Server 2010 zusammen, doch die Bordmittel sind weiterhin nutzbar. Und zusammen mit der verbesserten automatischen Spam-Filterung von Outlook 2007/2010 lässt sich der Mailverkehr auch ohne Zusatzprodukte absichern. Die Einstellungen für den Spamschutz sind auf Edge-Transport-Servern automatisch installiert und aktiviert. Diese Server sind unter Exchange 2010 für das Senden von E-Mails vom und ins Internet in der DMZ verantwortlich und müssen nicht Bestandteil einer Windows-Domäne sein. Diese Rolle müssen Sie explizit getrennt installieren. Unser Online-Workshop zeigt die dafür notwendigen Konfigurationen in Exchange und Outlook, das in den jüngsten Versionen unter anderem über einen aktiven Phishing-Schutz verfügt.

Link-Code: E3W55

Spamschutz und E-Mail-Sicherheit mit Exchange und Outlook 2010

IT-Administrator Trainings 2014

Best Practices Hyper-V

5. Juni 2014: Nürnberg (10 bis 17 Uhr)

New Elements,
Thurn-und-Taxis-Straße 10, 90411 Nürnberg

24. Juni: Essen (10 bis 17 Uhr)

PC-College,
Kruppstraße 96, 45145 Essen

15. Juli: München (10 bis 17 Uhr)

ExperTeach Training Center München,
Wredestr. 11, 80335 München

vSphere-Tuning und -Monitoring

8. April 2014: München

ExperTeach Training Center München,
Wredestr. 11, 80335 München

14. April: Berlin

Fast Lane Institute for Knowledge Transfer GmbH,
Oranienburger Straße 66, 10117 Berlin

22. April: Hamburg

ExperTeach Training Center Hamburg,
Esplanade 6, 20354 Hamburg

6. Mai: Frankfurt/M.

ExperTeach Training Center Frankfurt am Main,
Waldstraße 1, 60594 Frankfurt am Main

Weitere Informationen und Anmeldung

www.it-administrator.de/workshops

International PHP Conference 2014

Termin & Ort

1. bis 4. Juni

Maritim proArte, Friedrichstraße 151, 10117 Berlin

Inhalt

Pragmatisches Know-how im PHP- und Webumfeld.

Teilnahmegebühr

Ab 399 Euro für einen Tag und 899 Euro für alle drei Tage der Veranstaltung. Bis 3. April gelten reduzierte Frühbucherpreise.

Weitere Informationen und Anmeldung

Link-Code: D5W45

Linux Tag 2014

Termin & Ort

8. bis 10. Mai

STATION, Luckenwalder Straße 4-6, 10963 Berlin

Inhalt

Linux-Administration und -Entwicklung.

Teilnahmegebühr

Ab etwa 30 Euro.

Weitere Informationen und Anmeldung

Link-Code: E3W42

IPv6-Kongress 2014

Termin & Ort

22. und 23. Mai

CineStar METROPOLIS Frankfurt,
Eschenheimer Anlage 40, 60318 Frankfurt am Main

Inhalt

Planung und Management von IPv6-Netzen.

Teilnahmegebühr

Etwa 600 Euro.

Weitere Informationen und Anmeldung

Link-Code: D5W44

WorldHostingDays 2014

Termin & Ort

1. bis 3. April

Europa Park, Europa-Park-Straße 2, 77977 Rust

Inhalt

Kongressmesse rund um Cloud- und Hosting-Technologien.

Teilnahmegebühr

349 Euro. Kostenlose Teilnahme unter Verwendung des Anmelde-Codes ME712NW.

Weitere Informationen und Anmeldung

Link-Code: E3W46

WORLD of CLOUD

Termin & Ort

7. und 8. April

Sheraton Frankfurt Airport,
Hugo-Eckener-Ring 15, 60549 Frankfurt am Main

Inhalt

Kongressmesse zu Cloud- und Virtualisierungsthemen.

Teilnahmegebühr

Ab 995 Euro.

Weitere Informationen und Anmeldung

Link-Code: E3W41

»Ressourcenplanung ist in virtuellen Umgebungen eine Herausforderung«

Jascha Petersen ist in einem Team von mehreren IT-Administratoren für zwei Hamburger Firmen tätig. innobis ist ein SAP-Beratungshaus für Banken- und Finanzdienstleister. Circle Unlimited bietet SAP-integrierte Software-Lösungen für mittelständische und große Unternehmen. Das Thema Virtualisierung ist für den Admin in den letzten Jahren immer interessanter geworden, bringt aber auch so manche Herausforderung mit sich.

Warum sind Sie IT-Administrator geworden?

Das kristallisierte sich bereits in jungen Jahren heraus, da ich schon damals den Rechner nicht nur nutzen, sondern auch sein Innenleben verstehen wollte. Als ich dann später im Schulcomputerraum immer häufiger auch von den Lehrern um Rat gefragt wurde und ihnen bei den Problemen helfen konnte, war mein Berufswunsch schnell klar.

Warum würden Sie einem jungen Menschen raten, Administrator zu werden?

Es ist ein sehr spannender Beruf, der abwechslungsreicher kaum sein kann. Es ist aber von Vorteil, sich immer zu fragen, warum dieses oder jenes so funktioniert, wie es funktioniert und gerne über den Tellerrand zu schauen.

Welche Aspekte Ihres Berufs machen Ihnen am meisten Spaß und welche weniger?

Gerade die extreme Vielfältigkeit und morgens nicht zu wissen, was der Tag bringt, sich immer wieder neuen Problemen zu stellen und dafür Lösungen auszuarbeiten und die Chance, mit den neuesten Technologien zu arbeiten, ist hoch spannend. Weniger erfreulich ist es, wenn wir eine Lösung für ein Problem gefunden haben, diese aber einfach nicht funktionieren will. Das passiert aber zum Glück eher selten.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Wir wollen unseren Mailserver auf eine neue Version migrieren. Das wird ein sehr spannendes Thema. Ansonsten war unser Firmenumzug mit Implementierung eines Blade-Servers mit neuer Virtualisierungstechnik ein aufregendes Projekt.

Mit welcher aktuellen IT-Technologie würden Sie gern einmal arbeiten?

Ich wollte schon seit langer Zeit mit Blade-Servern arbeiten. Der Wunsch wurde

letztes Jahr erfüllt. Ansonsten reizt mich das Mobile-Thema mit all seinen Facetten – wenn Tablets und Co. die IT auf den Kopf stellen. Hinz kommt das Systemmanagement, das unseren Job vereinfachen soll.

Welches IT-Problem oder Produkt ließ Sie in letzter Zeit verzweifeln und warum?

Der IT-Umzug in die neuen Büroräume hat mich schon einige graue Haare gekostet, da die gesamte Planung parallel zum normalen Tagesgeschäft lief. Am Ende hat aber alles super funktioniert.

Wie sieht Ihre virtuelle Server-Umgebung aus?

Wir setzen sowohl für unsere Windows- als auch Linux-Server unterschiedliche Virtualisierungsmethoden ein. Für uns ist das Thema Virtualisierung in den letzten Jahren immer interessanter geworden, da wir dadurch flexibler auf Anforderungen aus dem eigenen Haus reagieren können.

Worin sehen Sie die größten Herausforderungen bei der Verwaltung virtueller Server?

Den Überblick zu behalten, gerade was die Ressourcenplanung angeht, da bestimmte Ressourcen wie Speicherplatz oder Arbeitsspeicher schnell nicht mehr vorhanden sein können. Eine weitere Herausforderung ist die Ausfallsicherheit.

Spielt der Storage eine tragende Rolle in Ihrer virtuellen Umgebung?

Wir haben für unsere virtuelle Umgebung den Storage aufgestockt, da der Speicherbedarf von neuen Servern immer größer wird und sich dort schnell ein Flaschenhals auftut. Der Storage selbst muss aber auch wieder redundant ausgelegt sein, da sich sonst daraus ein Single-Point-of-Failure ergibt.

Welche Vorteile hat die Server-Virtualisierung gebracht?

Es ist jetzt möglich, mehr Server auf weniger Hardware laufen zu lassen. Dadurch schrumpfen der Serverraumplatz sowie die



Geburstag: 1979
Admin seit: 11 Jahren
Hobbys: Filme, Musik, IT, Games

Jascha Petersen, IT-Administrator

Ausbildung und Tätigkeit

- Ausbildung zum Informatikkaufmann.
- Heute in der Systemadministration.
- Betreuung des Service Desk bis hin zur Server-Landschaft, physikalisch wie auch virtuell.

Betreute Umgebung

- Windows- und Linux-Server mit Diensten wie Active Directory, SAP, E-Mail, Firewall, Backup, oder Systemmanagement.
- Die gesamte Client-Infrastruktur.

Stromkosten. Am Ende ergibt sich daraus eine Kostenersparnis. Wir sind mit der Virtualisierung außerdem sehr viel flexibler als mit physikalischen Servern.

Welches ist der lustigste Anwenderfehler, der Ihnen untergekommen ist?

Während einer Inventur ist bei einem Steuergerät für die USV der 9 Volt-Stromanschluss abgefallen. Dies hatte zur Folge, dass die USV sich ausschaltete und damit auch gleich den kompletten Serverraum. Im ersten Moment war die Aufregung groß, da die Auswirkungen auf die Server nicht klar waren. Am Ende haben alle Server diese Aktion gut überlebt und wir konnten über dieses 9 Volt-Kabel lachen.

Das Interview führte Petra Adamik.

Möchten Sie auch einmal das letzte Wort im IT-Administrator haben? Dann melden Sie sich einfach unter redaktion@it-administrator.de (Betreff: "Das letzte Wort"). Wir freuen uns auf Sie!

Was haben Sie zu sagen?

Die Ausgabe 04/14 erscheint am 28. März 2014

Schwerpunktthema

Infrastruktur & Netzwerke

Das lesen Sie in den nächsten Ausgaben des IT-Administrator:

Im **Mai** dreht sich im IT-Administrator alles um den Schwerpunkt **Messaging & Collaboration**. In den Tests werfen wir einen Blick auf UCS als Groupware-Server und Good Collaboration for Mobile. Im Praxisbereich zeigen wir Ihnen, wie das Backup und Recovery bei SharePoint 2013 abläuft und was Sie bei der Migration von Small Business Server 2011 auf Windows Server 2012 R2 Essentials beachten müssen. Außerdem beleuchten wir wichtige Sicherheitsüberlegungen für VoIP- und Unified Communications-Projekte.

Die **Juni-Ausgabe** befasst sich dann mit dem Schwerpunkt **Monitoring & Dokumentation**.

Im Test: Dell PowerEdge VRTX

Workshop: Netzwerkkonzepte in Systems Center Virtual Machine Manager 2012 R2

Workshop: Data Center-Infrastrukturmanagement mit OpenDCIM

Systeme: Nutzen und Auswirkungen von Software Defined Networking

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

Redaktion

John Pardey (ip), *Chefredakteur*
verantwortlich für den redaktionellen Inhalt
john.pardey@it-administrator.de

Daniel Richey (dr), *Stellv. Chefredakteur und Cvd*
daniel.richey@it-administrator.de

Lars Nitsch (ln), *Redakteur*
lars.nitsch@it-administrator.de

Markus Heinemann, *Schlussredakteur*
markus.heinemann@email.de

Autoren dieser Ausgabe

Petra Adamik, Thomas Bär, Torsten Boch,
Florian Frömmerth, Frank Große, Jürgen Heyer,
Thomas Joos, Sandra Lucifora, Jörn Meyer, Daniel
Neumann, Thorsten Scherf, Michal Vitkovsky,
Henning von Kelpirsk, Bertram Währmann

Anzeigen

Anne Kathrin Heinemann, *Anzeigenleitung*
verantwortlich für den Anzeigenteil
kathrin@it-administrator.de
Tel.: 089/4445408-20

Es gilt die Anzeigenpreisliste
Nr. 10 vom 01.01.2013

LAC/2011



Produktion / Anzeigendisposition

Lighttrays: Andreas Skrzypnik, Gero Wortmann
dispo@it-administrator.de
Tel.: 089/4445408-88
Fax: 089/4445408-99

Druck

Konrad Triltsch
Print und digitale Medien GmbH
Johannes-Gutenberg-Straße 1-3
97199 Ochsenfurt-Hohesfeld

Vertrieb

Anne Kathrin Heinemann
Vertriebsleitung
kathrin@it-administrator.de
Tel.: 089/4445408-20

Abo- und Leserservice

Vertriebsunion Meynen GmbH & Co. KG
Stephan Orgel
Große Hub 10
65344 Eltville
leserservice@it-administrator.de
Tel.: 06123/9238-251
Fax: 06123/9238-252

Vertriebsbetreuung

DPV Deutscher Pressevertrieb GmbH
www.dpv.de

Erscheinungsweise

monatlich

Bezugspreise

Einzelheftpreis: € 12,60
Jahresabonnement Inland: € 135,-
Studentenabonnement Inland: € 67,50
Jahresabonnement Ausland: € 150,-
Studentenabonnement Ausland: € 75,-

Jahresabonnement Inland mit Jahres-CD: € 144,84
Studentenabonnement Inland mit Jahres-CD: € 77,34
Jahresabonnement Ausland mit Jahres-CD: € 159,84
Studentenabonnement Ausland mit Jahres-CD: € 84,84
All-Inclusive Jahresabo
(incl. E-Paper Monatsausgaben, 2 Sonderheften
und Jahres-CD) Inland: € 184,64
All-Inclusive Studentenabo Inland: € 117,14
All-Inclusive Jahresabo Ausland: € 199,64
All-Inclusive Studentenabo Ausland: € 124,64
E-Paper-Einzelheftpreis: € 8,99
E-Paper-Jahresabonnement: € 99,-
E-Paper-Studentenabonnement: € 49,50
Jahresabonnement-Kombi mit E-Paper: € 168,-
(Studentenabonnements nur gegen Vorlage
einer gültigen Immatrikulationsbescheinigung)

Alle Preise verstehen sich inklusive der
gesetzlichen Mehrwertsteuer sowie
inklusive Versandkosten.

Verlag / Herausgeber

Heinemann Verlag GmbH
Leopoldstraße 87
80802 München
Tel.: 089/4445408-0
Fax: 089/4445408-99

(zugleich Anschrift aller Verantwortlichen)

Web: www.heinemann-verlag.de
E-Mail: info@heinemann-verlag.de

Eingetragen im Handelsregister des
Amtsgerichts München unter
HRB 151585.

Geschäftsführung / Anteilsverhältnisse

Geschäftsführende Gesellschafter zu gleichen Teilen
sind Anne Kathrin und Matthias Heinemann.

ISSN

1614-2888

Urheberrecht

Alle in IT-Administrator erschienenen Beiträge sind
urheberrechtlich geschützt. Alle Rechte, einschließlich
Übersetzung, Zweitverwertung, Lizenzierung vorbe-
halten. Reproduktionen und Verbreitung, gleich wel-
cher Art, ob auf digitalen oder analogen Medien, nur
mit schriftlicher Genehmigung des Verlags. Aus der
Veröffentlichung kann nicht geschlossen werden, dass
die beschriebenen Lösungen oder verwendeten Be-
zeichnungen frei von gewerblichen Schutzrechten sind.

Haftung

Für den Fall, dass in IT-Administrator unzutreffende
Informationen oder in veröffentlichten Programmen,
Zeichnungen, Plänen oder Diagrammen Fehler en-
thalten sein sollten, kommt eine Haftung nur bei
grober Fahrlässigkeit des Verlags oder seiner Mit-
arbeiter in Betracht. Für unverlangt eingesandte
Manuskripte, Produkte oder sonstige Waren über-
nimmt der Verlag keine Haftung.

Manuskripteinsendungen

Die Redaktion nimmt gerne Manuskripte an. Diese
müssen frei von Rechten Dritter sein. Mit der Ein-
sendung gibt der Verfasser die Zustimmung zur Ver-
wertung durch die Heinemann Verlag GmbH. Sollten
die Manuskripte Dritten ebenfalls zur Verwertung
angeboten worden sein, so ist dies anzugeben.
Die Redaktion behält sich vor, die Manuskripte
nach eigenem Ermessen zu bearbeiten. Honorare
nach Vereinbarung.

So erreichen Sie den Leserservice

Leserservice IT-Administrator
Stephan Orgel
65341 Eltville
Tel.: 06123/9238-251
Fax: 06123/9238-252
E-Mail: leserservice@it-administrator.de

Bankverbindung für Abonnenten

Kontoinhaber: Vertriebsunion Meynen
Postbank Dortmund
IBAN: DE96440100460174966462
BIC: PBNKDEFFXXX

So erreichen Sie die Redaktion

Redaktion IT-Administrator
Heinemann Verlag GmbH
Leopoldstr. 87
80802 München
Tel.: 089/4445408-10
Fax: 089/4445408-99
E-Mail: redaktion@it-administrator.de

So erreichen Sie die Anzeigenabteilung

Anzeigenverkauf IT-Administrator
Anne Kathrin Heinemann
Heinemann Verlag GmbH
Leopoldstr. 87
80802 München
Tel.: 089/4445408-20
Fax: 089/4445408-99
E-Mail: kathrin@it-administrator.de

Tundl
aikux
baramundi
bintec elmeg

S. 11 EXPERTeach
S. 27 FCS
S. 5, S. 15 Galileo
S. 41 IBM

S. 71 isits
S. 63 Schmidts Login
S. 45 World Hosting Days
S. 84

S. 43
S. 53
S. 13

INSERTENVERZEICHNIS

Bleiben Sie in Verbindung!



Folgen Sie uns auf Twitter

twitter.com/ita_blog



Kreisen Sie mit uns auf Google+

<http://it-a.eu/googlep>



Werden Sie ein Fan auf Facebook

www.facebook.de/itanet



Treten Sie unserer Xing-Gruppe bei

www.xing.com/net/itanet



Lesen Sie unseren RSS-Feed

www.it-administrator.de/rss.xml

Werden Sie Teil unserer Community. Wir freuen uns auf Sie.

Virtualisierung und Cloud-Computing leicht gemacht. IBM System x Server und Lösungen.



Der erste Schritt in Richtung virtualisierte oder private Cloud-Umgebung ist oft eine Herausforderung. Das hat sich jetzt geändert. Denn IBM System x® M4 Express® Server mit integrierten Virtualisierungs- und Cloud-Lösungen von IBM vereinfachen und beschleunigen die Implementierung. Dank der neuesten Intel® Xeon® Prozessoren bieten IBM System x Server optimale Performance-, Skalierbarkeits- und Speichermerkmale für virtualisierte Workloads. IBM hat kürzlich durch das erste x86-virtualisierte TPC-C-Benchmark-Ergebnis mit den niedrigsten Kosten pro Transaktion¹ bewiesen, wie effizient und wirtschaftlich diese Lösungen sind. Ab sofort profitieren Sie also nicht nur von den Vorteilen einer Cloud oder einer virtualisierten Umgebung, sondern auch von einer neuen Einfachheit und geringeren Kosten. Und Sie können sich jederzeit auf die Unterstützung von erfahrenen IBM Geschäftspartnern verlassen, um Ihr System zu konfigurieren und auf Ihre geschäftlichen Anforderungen abzustimmen.

IBM System x3650 M4 Express

2.212,21 € (inkl. MwSt.)*

monatl. IBM Leasingrate bei
36 Monaten Vertragslaufzeit: 48,65 €**

Best.-Nr.: 7915E7G

Intel® Xeon® Prozessor E5-2620 v2 (6-Core, 2,1 GHz)

1x 8-GB-RDIMM-Hauptspeicher

O/B 2,5" HS SAS/SATA, RAID Controller M5110 (ohne Batterie)

Multiburner, 1x 550 Watt HS Power Supply

1 Jahr Gewährleistung, 3 Jahre freiwilliger Herstellerservice



IBM System x3550 M4 Express

2.226,49 € (inkl. MwSt.)*

monatl. IBM Leasingrate bei
36 Monaten Vertragslaufzeit: 48,96 €**

Best.-Nr.: 7914E7G

Intel® Xeon® Prozessor E5-2620 v2 (6-Core mit 2,1 GHz)

1x 8-GB-RDIMM-Hauptspeicher

O/B 2,5" HS SAS/SATA, RAID Controller M5110
(512 MB Cache, ohne Batterie)

Multiburner, 1x 550 Watt HS Power Supply

1 Jahr Gewährleistung, 3 Jahre freiwilliger Herstellerservice



IBM Storwize® V3700

8.423,- € (inkl. MwSt.)*

monatl. IBM Leasingrate bei
36 Monaten Vertragslaufzeit: 206,48 €**

Best.-Nr.: 2072S2C, 00Y2501, 39Y7917

(Plus: 8x 300 GB 2,5"-SAS-Festplatten, 2x 2,8 m Kabel)

1-Gbps-iSCSI- und 6-Gbps-SAS-Schnittstellen,
optional 8-Gbps-FC, 10-Gbps-iSCSI/FCoE

Dual Controller fasst bis zu 24 Festplatten

kostenfrei integriert: interne Virtualisierung

Datenmigrationsfunktion, Thin Provisioning, Flash Copy,
intuitive IBM Storwize Benutzeroberfläche

1 Jahr Gewährleistung, 3 Jahre freiwilliger Herstellerservice



Lesen Sie das Technology Business Research-Whitepaper

Erfahren Sie, wie IBM mit seiner Virtual Desktop Infrastruktur für mehr Einfachheit sorgt.

Weitere Informationen: ibm.com/systems/de/express1



¹Siehe <http://www.tpc.org/1791> vom 07.05.2013.

*Alle Preise sind Einzelhandelsverkaufspreise von IBM, gültig vom 31.10.2013, und beinhalten möglicherweise weder Speicher, Festplatte, Betriebssystem noch andere Leistungsmerkmale.

**Monatliche IBM Leasingrate zzgl. MwSt. bei 36 Monaten Laufzeit und einem Mindestvertragsvolumen von 4.000,- EUR. Die Finanzierungsangebote sind freibleibend, gelten vorbehaltlich einer positiven Bonitätsprüfung durch IBM und richten sich ausschließlich an Geschäftskunden. IBM behält sich das Recht vor, dieses Angebot ohne Vorankündigung zurückzuziehen oder zu modifizieren.

IBM Hardwareprodukte werden fabriktreu hergestellt. Unabhängig davon gelten in jedem Fall die IBM Gewährleistungsbedingungen.

Die aktuellen Bedingungen finden Sie auf http://www.ibm.com/servers/support/machine_warranties. IBM übernimmt keinerlei Verantwortung oder Garantie für Produkte und Leistungen anderer Hersteller. IBM, das IBM Logo, System x und Express sind Marken der International Business Machines Corporation in den Vereinigten Staaten und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie unter www.ibm.com/legal/copytrade.shtml. Intel, das Intel Logo, Xeon und Xeon Inside sind Marken oder eingetragene Marken der Intel Corporation in den USA und/oder anderen Ländern. Preise von IBM Geschäftspartnern können von den hier angezeigten Preisen abweichen. Die Produkte sind je nach Verfügbarkeit lieferbar. IBM bietet die hierin beschriebenen Produkte, Dienstleistungen oder Leistungsmerkmale möglicherweise nicht in allen Ländern an. Aktuelle Preisinformationen erhalten Sie von Ihrem IBM Vertriebsbeauftragten oder IBM Geschäftspartner. © 2013 IBM Corporation.