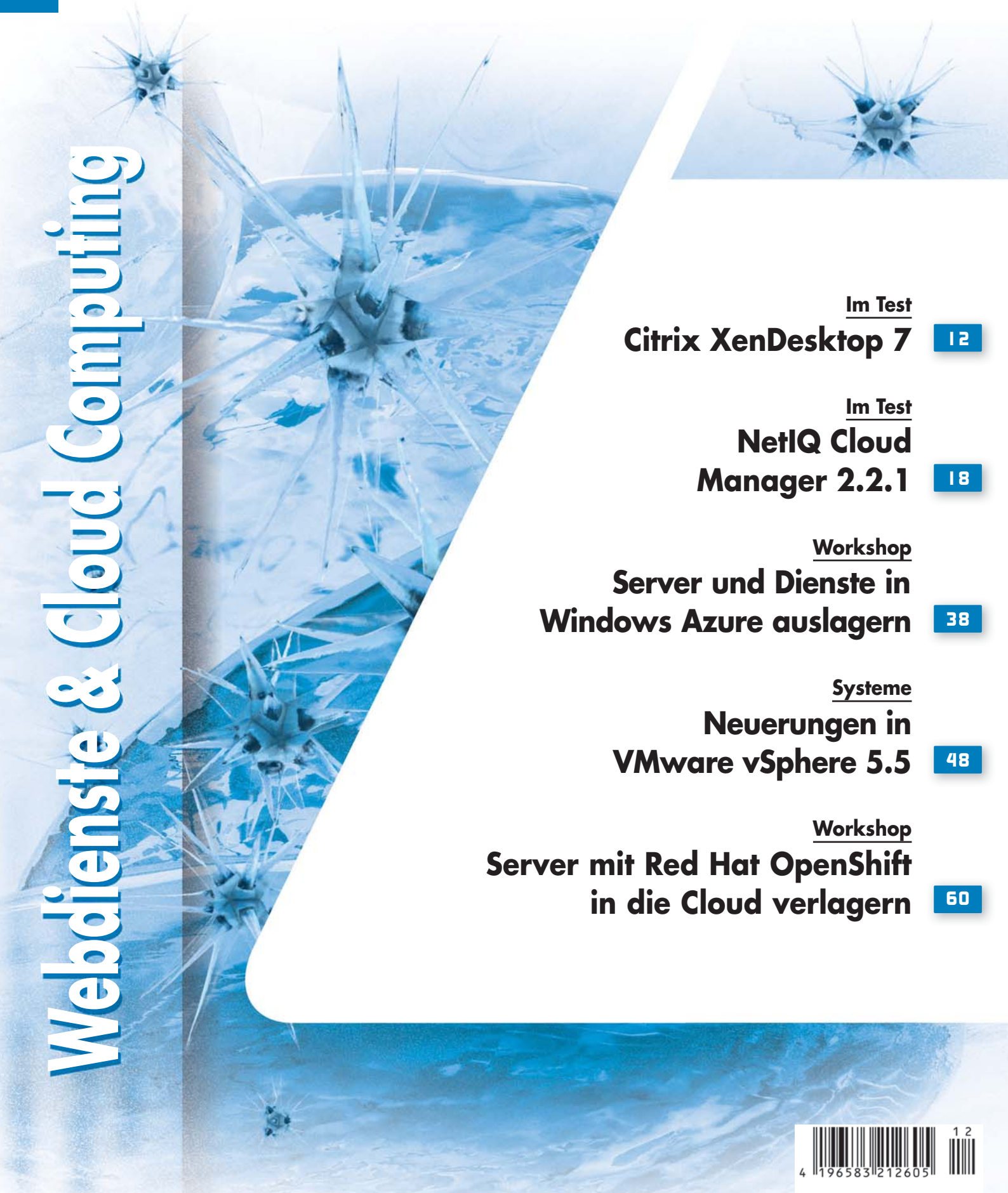
IT-ADMINISTRATOR.DE

12/2013

€ 12,60 ISSN 1614-2888

iadministrator

Das Magazin für professionelle System- und Netzwerkadministration



Webdienste & Cloud Computing

4 196583 212605 12

Flexibel. Einfach. Leistungsstark.

Das IBM NeXtScale System.

Durch zunehmende Datenvolumen steigt der Bedarf an intelligenter Analyse. Und damit die Nachfrage nach höherer Effizienz in der Cloud. All das führt dazu, dass Datenzentren heute Ihren Anforderungen nicht mehr gerecht werden können. Die Lösung: das IBM NeXtScale System. Eine einfache und kosteneffektive Plattform für Hyperscale-Computing mit maximaler Dichte, höchster Leistung und Effizienz bei niedrigen Betriebskosten. Durch seine einfache Handhabung und offene Bauweise kann es in Ihre bestehende Infrastruktur integriert werden. Außerdem reduziert es die Einarbeitungszeit Ihrer Mitarbeiter um 75% – dank optionalem IBM Intelligent Cluster.[1]

Angetrieben durch den neuen Intel® Xeon® Prozessor E5-2600 v2, enthält das IBM NeXtScale System dreimal mehr Rechenkerne.[2] So ergibt sich eine Leistungssteigerung[3] bis zu 37% gegenüber früheren Generationen von 1U-Servern und eine Erhöhung der Effizienz[4] bis zu 36% im Vergleich zu Systemen früherer Generationen. Dadurch schöpfen Sie eine maximale Aussagekraft aus Ihren Daten. Lassen Sie also die High-Performance-Computing-Erfahrung von IBM mit Höchstleistung für Sie arbeiten.

Erfahren Sie, was das IBM NeXtScale System für Sie tun kann, um Ihre Datenzentren mit rechenintensiven Workloads zu optimieren.

Laden Sie sich den Bericht von Clabby herunter. Auf ibm.com/systems/de/nextscale

---

[1] Basierend auf einem von IBM erstellten Vergleich von Konfiguration und Setup beim Kunden vor Ort, gegenüber der Ausführung mit dem Intelligent Cluster von IBM, welches optional erhältlich ist.
[2] 3 Rechenkerne in einem branchenüblichen 42U-Rack zum Vergleich von 42 1U-x3550-M4-Rackservern mit 2 Intel® Xeon® E5-2600 Prozessoren mit jeweils 8 Kernen = 672 Kernen gegenüber 84 NeXtScale System nx360 M4 Knoten mit 2 Intel® Xeon® E5-2600 v2 Prozessoren mit jeweils 12 Kernen für insgesamt 2.016 Kerne.
[3] SPECint_rate_base2006 - 669 auf IBM iDataPlex dx360 M4 (Intel® Xeon® E5-2690) gegenüber 918 auf IBM NeXtScale nx360 M4 (Intel® Xeon® E5-2697 v2.) www.spec.org. Ergebnisse mit Stand vom 20.9.13.
[4] SPECpower_ssj2008 - 5392 auf IBM iDataPlex dx360 M4 gegenüber 7347 auf IBM NeXtScale nx360 M4. www.spec.org. Ergebnisse mit Stand vom 20.9.13.

EDITORIAL

Gewusst wie

Liebe Leser,

es gibt heute eigentlich keine Netzwerkkomponente mehr, die sich nicht über ein Webinterface konfigurieren lässt. Kein Administrator käme noch auf die Idee, den Router, das NAS oder die Security-Appliance mit jeweils einer eigenen Software zu verwalten – ist diese doch erst zeitraubend auf einem PC zu installieren und dann vom IT-Verantwortlichen für alle Zeiten von ebendiesem Rechner zu bedienen. Mehr als unflexibel. Mit dem Siegeszug des Browsers wurde hingegen ein einheitliches Werkzeug geschaffen, um mit Hilfe von anpassungsfähigen Bedienoberflächen ganz ohne Kommandozeile bequem auf das Innenleben der zahlreichen Geräte zugreifen zu können.

Mit der Cloud stellt es sich eigentlich ganz ähnlich dar: Diverse Dienstleistungen werden über ein Web-Frontend angeboten, der Betrieb einer speziellen Software auf eigenen Rechnern ist (meist) nicht nötig. Auch hier profitiert der Nutzer im Regelfall von Flexibilität und spart Investitionen in eigene Hard- und Software. Voraussetzung hierfür ist zum einen eine schnelle Internetverbindung. Dies sollte das geringste Problem darstellen, plant doch die Politik eine flächendeckende Versorgung mit Anschlüssen von 50 MBit/s bis 2018. Als größte Hürde gilt – wie unter anderem unser Vor-Ort-Bericht ab Seite 10 von der Kongressmesse "Storage Networking World" in Frankfurt zeigt – die Sicherheitsproblematik und die oft unscharfe Definition von Cloud-Diensten durch die Anbieter.

Und auch wenn Sie als IT-Verantwortlicher den Gang in die Cloud favorisieren: Nicht für alle Anwendungsfälle ergibt ein Umzug in die Cloud Sinn. Unser Workshop ab Seite 38 erläutert, wie Sie IT-Bereiche mit stark schwankender Arbeitslast zu Windows Azure auslagern und welche Faktoren dabei zu beachten sind. Wer lieber an der eigenen Cloud bastelt, kann dabei auf Open Source-Tools zurückgreifen. Eines davon ist OpenNebula 4.2, das im aktuellen Release diverse Neuerungen vorzuweisen hat. Wie wir ab Seite 64 zeigen, hat sich gerade bei der VDI-Verzahnung einiges getan. Für unsere Test-Rubrik haben wir ab Seite 18 NetIQ Cloud Manager 2.2.1 unter die Lupe genommen und uns angesehen, welche Möglichkeiten das Portal beim Monitoring, bei der Paketerstellung oder der Provisionierung bietet.

Dass Cloud-Dienste einmal so leicht und sicher zu nutzen sein werden wie das Webinterface Ihres Routers, ist vorerst nicht zu erwarten. Eine klare Definition, was Sie überhaupt in der Wolke machen wollen und die Wahl der entsprechenden Mittel stellen aber den ersten Schritt in die Cloud dar.

Eine schöne Advents- und Weihnachtszeit wünscht

Lars Nitsch
Redakteur

Webdienste & Cloud Computing

Im Test: Bomgar Box 13.1.2

Der Fernzugriff ist eines der zentralen Hilfsmittel des Administrators. Bomgar hat mit der gleichnamigen Box eine Fernwartungslösung im Angebot, die mehr sein will als ein reines Bildschirmübertragungstool. Sie koordiniert Support-Anfragen selbständig und verschafft den Kontakt zum richtigen IT-Team. Wir haben die neue Version 13.1.2 der zugrundeliegenden Software Base zum Anlass genommen, uns das Gerät genauer anzuschauen.

Seite 24

Im Test: EgoSecure Endpoint 5.4

Datenverluste entstehen nicht nur durch vorsätzlichen Diebstahl – sei es nur, dass sensible Dateien unverschlüsselt in die Cloud wandern. Um Unternehmen vor den meist weitreichenden Folgen zu schützen, bietet EgoSecure mit Endpoint einen Endgeräte-Schutz an. Die neue Version 5.4 konnte im Test beweisen, wie sie Datenverlust vorbeugt.

Seite 30

AKTUELL

PRODUKTE

PRAXIS

WISSEN

RUBRIKEN

Desktop-Virtualisierung mit Microsoft System Center Virtual Machine Manager

Cloud-artige Desktop-Umgebungen, die hochautomatisiert bereitgestellt werden und im eigenen Rechenzentrum laufen, nennen sich Private Desktop Cloud oder auch Desktop-as-a-Service. Dieses Konzept gewinnt zunehmend Akzeptanz, da insbesondere im Desktop-Umfeld massenweise identische Systeme bereitgestellt werden müssen. Dieser Beitrag zeigt den Weg zu einer Desktop-Cloud mit dem Microsoft System Center Virtual Machine Manager.

Seite 44

Neuerungen in OpenNebula 4.2

Nach einer rund fünfjährigen Entwicklungszeit stellte das OpenNebula-Team im Mai dieses Jahres mit Release 4 sein neuestes Release vor, das gegenüber der Vorgängerversion in allen Subsystemen wichtige Verbesserungen erfahren hat. In diesem Workshop sehen wir uns die wichtigsten Neuerungen der Cloud-Umgebung an – gerade beim Benutzer-Interface und der VDI-Verzahnung hat sich einiges getan.

Seite 64

Link-Codes

Unsere Link-Codes ersparen Ihnen mühsame Tipparbeit bei langen URLs

Switch ohne Stromkabel

Von **Netgear** kommt mit dem Modell **ProSAFE GS516TP** ein 16 Port-GBit-PoE-Smart-Switch auf den Markt, der vom Hersteller als "PoE Powered Device" (PD) klassifiziert wird. Die Neuerscheinung **lässt sich über die zwei PD-Ports über einen anderen PoE-Switch mit Strom versorgen** und kann diesen dann – unter Nutzung der insgesamt acht PoE-Ports – an weitere Geräte ausgeben. Der Switch muss also nicht zwingend selbst über ein Netzkabel versorgt werden. Netgear spricht in diesem Zusammenhang auch von einer **Pass-Through-Funktionalität**. 100 Meter Distanz zum GS516TP-Switch und weitere 100 Meter zu den zu versorgenden Geräten sollen ohne Probleme möglich sein. Kommt ein Netzteil zum Einsatz, beträgt das zur Verfügung stehende PoE-Budget bis zu 76 Watt. Ist der Switch selbst über PoE angebunden, sind bis zu 22 Watt möglich. Neben den genannten Funktionen zum Strom-Management will der Hersteller den GS516TP auch mit umfassenden L2-Features ausgestattet haben. Dazu zählen zum Beispiel dynamische VLAN-Unterstützung und QoS. Zu den weiteren Merkmalen der Verteilstation gehören statisches Routen, IPv6-Unterstützung, MDP Snooping, Dynamic Assignement und Protected Ports. Der Smart-Switch ist ab sofort für rund 340 Euro erhältlich. *(ln)*

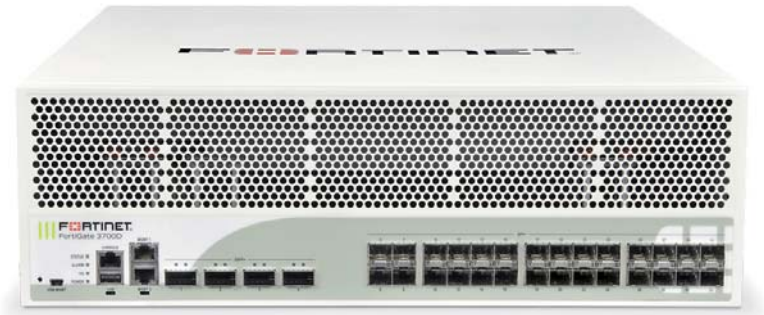
Netgear: www.netgear.com/smart-switches

Der ProSAFE GS516TP kann Access Points, VoIP-Telefone oder IP-Kameras mit Strom versorgen, aber auch selbst ohne Netzkabel arbeiten

Firewall unter Dampf

Fortinet erweitert sein Portfolio um eine leistungsstarke und kompakte **Netzwerk-Firewall-Appliance** für große Rechenzentren, Service-Provider, Cloud-Anbieter und Carrier. Die **FortiGate 3700D** verfügt über vier **40-GBit-Ethernet-(QSFP+)** und 28 **10-GBit-Ethernet (SFP+)-Ports** und verspricht einen **Firewall-Durchsatz von bis zu 160 GBit/s**. Die Latenz der drei Höheneinheiten großen Firewall soll zwei Mikrosekunden betragen bei bis zu 44 Millionen gleichzeitigen TCP-Sitzungen. Der **IPSec VPN-Durchsatz** soll bei **100 GBit/s** liegen und 64.000 Client-zu-Gateway-Tunnel unterstützen. Die Anzahl der gleichzeitigen Gateway-zu-Gateway-Tunnel liegt laut Hersteller bei 10.000. Mit **aktiviertem IPS** setzt die Appliance noch **16 GBit/s** durch. Die Appliance erlaubt ferner eine physische, hybride oder virtuelle **Netzwerksegmentierung** über virtuelle Domains (VDOM). Das zugrundeliegende FortiOS 5 bietet mehrere Formen der **Hochverfügbarkeit** wie Active-Active, Active-Passive oder Virtual Cluster. Abhängig von der Konfiguration befänden sich die Zeiten von Systemausfällen im Millisekunden-Bereich. Ab ungefähr 130.000 Euro ist die FortiGate 3700D zu erwerben. *(dr)*

Fortinet: www.fortinet.com



Die FortiGate 3700D soll durch ihre Performance und Portdichte glänzen

Kommandozentrale für APs

Auf den KMU-Markt zielt **Allied Telesis** mit dem neu vorgestellten WLAN-Controller **AT-UWC**. Das Management-Werkzeug ist entweder **als virtuelle oder als Hardware-Appliance erhältlich**. Die Software-Variante unterstützt die **Verwaltung von bis zu 210 Access Points**, während die Hardware-Version maximal 60 APs unter ihre Fittiche nimmt. Bei beiden Erscheinungsformen findet die Administration über ein Webinterface statt. Laut Hersteller arbeitet der **Discovery-Mechanismus** der Neuvorstellung **sowohl auf Layer 2- als auch auf Layer 3-Ebene** und soll so das Deployment des Geräts selbst sowie das Auffinden von APs beschleunigen. Das Weiterleiten der Daten an die Clients über die APs lässt sich auf zwei Arten regeln: Einmal zentralisiert, indem der **gesamte Traffic über den Controller** geleitet und es dem Administrator erlaubt wird, strenge Sicherheitsregeln und Filter durchzusetzen. Im **verteilten Szenario** hingegen entscheiden die einzelnen APs autonom, wie und wohin Daten geschickt werden. Damit obliegt den APs auch das Durchsetzen von Security-Richtlinien und das QoS-Management. Das QoS erfolgt dabei auf Ende-zu-Ende-Basis und weist einzelnen Anwendungen gemäß ihren Anforderungen die entsprechende Bandbreite zu. Hohe Latenzzeiten oder Jitter sollen so der Vergangenheit angehören. Zu den weiteren Merkmalen des AT-UWC gehört ein integriertes **Intrusion Prevention System** und die Möglichkeit, mit Hilfe eines VLANS Gastzugänge zu schaffen, die vom Unternehmensnetzwerk getrennt sind. Beim Einsatz mehrerer WLAN-Controller lassen sich diese auch als Cluster betreiben – Firmware-Updates müssen dann etwa nur einmal an die gesamte Gruppe verteilt werden. Die virtuelle Appliance ist ab sofort mit einem Lizenz-Paket von bis zu zehn APs zum Preis von rund 730 Euro erhältlich. Die Hardware-Variante soll im Januar 2014 verfügbar sein. *(ln)*

Allied Telesis: www.alliedtelesis.eu

Ungetrübter Blick

Axis Communications stellt die IP-Kamera **Q1614** für den **Innenbereich** sowie die für den **Außenbereich** geeignete **Q1614-E** vor. Die Neuzugänge können schnelle Bewegungen mit dem Doppelten der üblichen Bildrate erfassen. So zeichnen die Geräte ihre Videos in HDTV-720p-Qualität mit 50 oder 60 Bildern pro Sekunde auf. Sie kommen laut Hersteller auch mit komplexen, sehr kontrastreichen Szenen und schwacher Beleuchtung zurecht. Mithilfe der dynamischen Erfassung **Wide Dynamic Range** (WDR) könnten die Kameras **kontrastreiche, komplexe Szenen** verarbeiten, wenn etwa durch Sonneneinstrahlung sehr helle Bereiche und tiefe Schatten entstehen. Auch bei solchen Lichtverhältnissen böten die Kameras gleichmäßig ausgeleuchtete Bilder ohne zu dunkle oder helle Zonen. So seien Personen und Objekte selbst dann noch deutlich erkennbar, wenn sie sich in sehr hellen oder sehr dunklen Abschnitten des überwachten Bereichs befinden. Axis stellt mit den beiden Kameras auch neue Installationsfunktionen vor, die eine schnelle Installation und optimale Einrichtung der Kameras ermöglichen sollen. Zum Beispiel unterstützt der neue **Ausrichtungsassistent** den Monteur mit einem Summer und einer blinkenden LED dabei, die Kamera horizontal richtig auszurichten, insbesondere wenn nicht sicher ist, ob die Halterung wirklich gerade angebracht ist. Die Kameras sind die ersten mit einstellbarer **Stoßerkennung**. Mit dieser Funktion können sie automatisch einen Alarm senden, wenn eine Erschütterung detektiert wird. Zu haben sind die Kameras ab sofort für 923 Euro (Q1614) beziehungsweise 1.175 Euro (Q1614-E). *(dr)*

Axis Communications: www.axis.com

Die IP-Kameras Q1614 und Q1614-E sollen auch mit schwierigen Lichtverhältnissen klarkommen

Ausbaufähig

Infortrend lüftet den Vorhang für sein neues **Storage-System E75-2230** (E75) mit drei Höheneinheiten als Ergänzung der ESVA IP SAN-Produktfamilie. Mit **10 GBit-Ethernet iSCSI Host-Konnektivität, Unterstützung von bis zu 4.800 HDD-Laufwerken** und einem neuen Infortrend Hardware-Design verspricht das Modell den Anwendern die nötige Performance, Skalierbarkeit und Unterstützung für die Virtualisierung auch für anspruchsvolle Rechenzentrumsanwendungen. Dank der Scale-Out-Architektur können die IT-Verantwortlichen außerdem die Kapazität des Storage-Systems durch den Anschluss separater Gehäuse auf die bis zu 4.800 erwähnten Laufwerke erweitern und damit eine **Gesamtkapazität von 18 PByte** ermöglichen. Das Storage-System fasst 16 Festplatten. An Disks werden 2,5 und 3,5 Zoll-Modelle mit SAS-Anbindung unterstützt. Die Administration findet über die Java-basierte Software SANWatch statt. Für 15.000 Euro ist die E75 zu haben. *(dr)*

Infortrend: www.infortrend.com

Über externe Storage-Geräte unterstützt die E75 bis zu 4.800 Festplatten

+++TICKER+++TICKER+++TICKER+++

Fujitsu stellt den **Storage ETERNUS Snapshot Manager** (ESM) für seine Speichersysteme ETERNUS DX vor. Damit können Unternehmen Daten wiederherstellen und so Ausfallzeiten minimieren. Der ESM soll dabei einen vollständigen Überblick über sämtliche Snapshot-Daten ermöglichen, und zwar über gängige Anwendungen, Geräte und Betriebssysteme hinweg. Die Preise für die Entry-Systeme beginnen bei 3.624 Euro, für die Midrange-Systeme bei 10.228 Euro und für die Enterprise-Systeme bei 38.357 Euro. Alle ESM-Lizenzen sind uneingeschränkt pro System nutzbar. *(dr)*
www.fujitsu.com/de/

SolarWinds erweitert die Remote-Verwaltungslösung **DameWare Remote Support** um neue Mobilfunktionen für Android-Geräte. Zusätzlich unterstützt SolarWinds' Mobile Admin zur mobilen IT-Verwaltung auch Apples aktuelles Betriebssystem iOS 7. Mit DameWare Remote Support verwalten Administratoren Mac OS X-, Linux- und Windows-Computer per Fernzugriff. Die Benutzer können ohne Remote-Steuerung Windows-Dienste starten, anhalten und neu starten, Benutzer und Gruppen aus mehreren Active Directory-Domänen verwalten, AD-Objekte exportieren oder von entfernten Computern detaillierte Informationen erhalten. Mobile Admin liefert dabei auch Echtzeit-Benachrichtigungen und Statusaktualisierungen. DameWare Remote Support ist ab einem Preis von 285 Euro einschließlich Wartung im ersten Jahr erhältlich. *(dr)*
www.solarwinds.com

Avira stellt mit Version 2.0.1 ein neues Release von **Free Mac Security** zum kostenfreien Download bereit. Die Antivirus-Software ist kompatibel mit dem aktuellen Betriebssystem Mac OSX 10.9. Die neue Quick Scan-Funktion durchsucht schon während der Installation gezielt gefährdete Verzeichnisse und erkennt so bereits vorhandene Bedrohungen, die die Installation eines Schutzprogramms behindern könnten. Daneben ermöglicht Avira Free Mac Security Anwendern nun auch die Aktualisierung von Produkt- und Virensignaturen gleichzeitig mit einem Klick. One-Click Repair zur sofortigen Wiederherstellung des optimalen Sicherheitslevels, Echtzeit-Schutz und profiliertes Scanning gehören zu den weiteren Funktionen der Software. *(ln)*
www.avira.com/de/

WatchGuard rollt mit **XCS 10** die jüngste Version des Betriebssystems für seine XCS-Appliances aus. Der Hersteller will vor allem an der Hyper-V-Unterstützung, am IPv6-Support und an der Leistungsfähigkeit bei der Spamabwehr im ausgehenden Datenverkehr gearbeitet haben. Administratoren soll es mit dem überarbeiteten OS leichter fallen, unternehmensspezifische Vorgaben gezielt umzusetzen. Funktionalitäten wie Anti-Malware, Anti-Spam, Anti-Phishing, Data Loss Protection oder E-Mail-Verschlüsselung sichern nun auch den Datentransfer von virtualisierten Anwendungen ab. WatchGuard XCS 10 ist ab sofort für alle Nutzer, die eine physische oder virtuelle XCS-Appliance einsetzen und über ein LiveSecurity-Abonnement verfügen, kostenfrei erhältlich. *(ln)*
www.watchguard.com/products/xcs/

Verteilstation mit vielen Extras

ZyXEL baut sein Switch-Angebot um die Serie **XGS3700/GS3700** aus. Die Neuvorstellungen sind für den Einsatz unternehmenskritischer Anwendungen in kleinen und mittelständischen Unternehmen konzipiert, in denen hohe Bandbreiten und 24/7-Verfügbarkeit wichtig sind. Der Hersteller bewirbt die Geräte unter anderem mit seinem **platzsparenden Hardware-Design, PoE+ und GBit-Speed**. Insgesamt **acht Modelle stehen zur Auswahl**, in Konfigurationen mit 24 und 48 Ports, mit und ohne PoE sowie Uplink-Optionen mit 1 GbE (Serie GS3700) und 10 GbE (Serie XGS3700). Die Produktreihe ist mit erweiterten Funktionen ausgestattet wie beispielsweise statischem Routing, Policy-basiertem Routing (PBR) und Unterstützung für ECMP und VRRP. **Mit Equal Cost Multipath Routing können die Switches der neuen Serie den Traffic auf mehrere Links mit hoher Bandbreite verteilen**, was die Qualität der Anbindung erhöhen soll. Das Virtual Router Redundancy Protocol bietet einen dynamischen und automatischen Ansatz für virtuelle Router-Redundanz. Mehrere First-Hop virtuelle Router können sich damit eine IP-Adresse dynamisch teilen, wobei einer davon als Master und die anderen als Backup fungieren. Sollte der Master ausfallen, wird automatisch ein Backup zugewiesen und tritt an seine Stelle. Als Ergebnis soll eine bessere Belastbarkeit des Netzwerks und ein niedrigerer administrativer Aufwand stehen, etwa im Vergleich zur Verwendung dynamischen Routings. Die Hardware-Architektur bietet Redundanz und umfasst zwei interne Stromversorgungen sowie im laufenden Betrieb austauschbare Lüfter- und Netzmodule. Je nach Modell und Anzahl der Ethernet-Ports liegen die Preise der neuen Switche zwischen 1.050 und 2.020 Euro. *(ln)*

ZyXEL: www.zyxel.de

Die Modelle der XGS3700/GS3700-Serie bieten ein PoE-Budget bis zu 1.000 Watt bei zwei Stromversorgungen beziehungsweise 460 Watt bei einer Stromversorgung

Drucker mit Draht zur Cloud

Mit dem **Dell Document Hub** gibt Dell den Startschuss für einen neuen Dienst für den einheitlichen Zugang zu gängigen **Dokumenten-Management-Plattformen in der Cloud**. Die Verwaltung von Cloud-Dokumenten würde dadurch wesentlich vereinfacht. Zu den angebundenen Plattformen gehören Box, Dropbox, Google Drive, Microsoft SkyDrive und Microsoft SharePoint Online. Der Zugriff auf den Hub kann durch eine App auf Geräten mit den Betriebssystemen Windows 8, Windows 8.1 und Windows RT erfolgen. Außerdem lässt sich der Dienst direkt vom neuen **Multifunktions-Farbdrucker C2665dnf** aus nutzen. So lassen sich etwa gescannte Unterlagen via Cloud-OCR in editierbare Dateien umwandeln. Nutzern des neuen Druckers steht ein 4,3 Zoll großer Farb-Touchscreen zur Verfügung, mit dem sie das Gerät wie ein Smartphone bedienen können. Der C2665dnf ist außerdem NFC-fähig und unterstützt die Dell Mobile Print App für Android, AirPrint sowie Google Cloud Print Direct. Darüber hinaus kann direkt vom C2665dnf aus an unterschiedliche Ziele wie FTP, E-Mail, USB oder PCs gescannt werden. Der Drucker ist für 449 Euro verfügbar. *(dr)*

Dell: www.dell.de

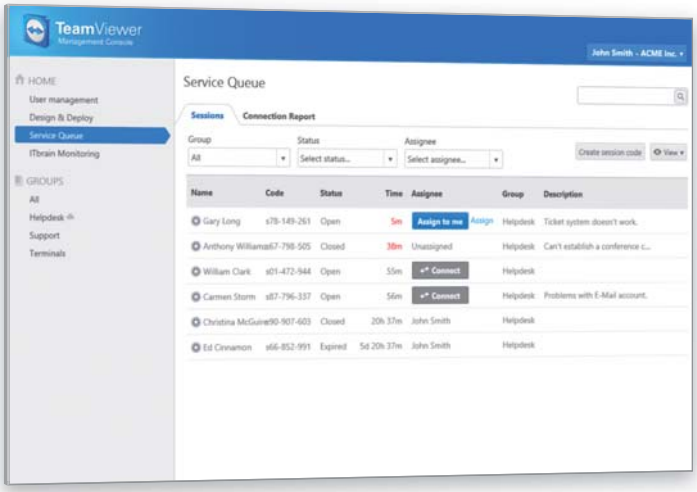
Kommunikationstalent

Metaways hat unter dem Codenamen **Collin** das nächste **Major Release** der **Open Source-Groupware Tine 2.0org** veröffentlicht. Die Software lässt sich jetzt unter anderem in **Active Directory-Strukturen** einbinden. Anwender können aus der Groupware heraus neue Benutzerkonten sowie -gruppen anlegen und verwalten. Daneben kann die Groupware nun als **Server für ownCloud-Clients** fungieren. Daten zwischen verschiedenen Rechnern und Smartphones lassen sich dadurch leichter synchronisieren. Auch unterstützt die neue Version den **CardDAV eM-Client**. Darüber hinaus lassen sich Aufgaben jetzt auch per **CalDAV** anlegen und verwalten. Neben diesen neuen Funktionen bietet das Major Release auch zahlreiche kleinere Verbesserungen, die die Nutzung der Software noch komfortabler und sicherer machen sollen. Die **Anmeldung an Tine 2.0org ist nun alternativ mit einem Zertifikat** möglich, so dass kein Benutzername oder Passwort mehr im Browser eingegeben werden muss. In der Sales-Anwendung lassen sich jetzt Kostenstellen definieren, die in allen anderen Anwendungen wiederverwendbar sind. Damit lassen sich alle Daten nun auch nach Kostenstellen filtern. Administratoren haben die Möglichkeit, den maximalen Zeitraum zu definieren, über den zurückliegende Termine mit Smartphones synchronisiert werden dürfen. Das zahlt sich vor allem bei großen Installationen aus, da hierdurch der CPU-Bedarf deutlich reduziert werden kann. Bei Tine 2.0org handelt es sich um die Community-Variante der Open Source-Groupware. In Zusammenarbeit mit der Gemeinschaft werden Verbesserungen an der aktuellen Version durchgeführt und dann auch in das nächste Release der Enterprise-Version übernommen. Die kommerzielle Variante der Groupware-Lösung wird von Metaways unter dem Namen Tine 2.0 angeboten. Das neue Major Release ist ab sofort verfügbar und kann kostenlos heruntergeladen werden. *(dr)*

Metaways: www.metaways.de

Fernwartung reloaded

Anfang Dezember ertönt der Startschuss für Version 9 der Fernwartungs-Software **TeamViewer**. Das jüngste Release ist unter anderem mit einer **Wake-on-LAN-Funktion** ausgestattet. Damit können Nutzer entfernte Computer vom aktuell verwendeten Gerät aus über das Internet einschalten. Des Weiteren verfügt Version 9 über eine **Service-Warteschlange**. Damit lassen sich laut Hersteller **Support-Anfragen innerhalb von Teams komfortabel und effizient verwalten, teilen und Mitarbeitern zuweisen**. Vereinfacht wurde auch die Teilnahme an Fernwartungssitzungen. Anstatt wie bisher mit ID und Kennwort ist diese jetzt optional mit einem einmalig generierten Sitzungscode möglich. Mit an Bord ist nun auch eine **Zwei-Faktor-Authentifizierung** – neben dem Passwort können Anwender mit Hilfe ihres mobilen Geräts und einer standardkonformen Authenticator-App optional zusätzlich einen Einmal-Sicherheitscode generieren. Nicht zuletzt haben die Entwickler am Fileshare gearbeitet. Dateien jeder Größe lassen sich nun auch austauschen, ohne dass dazu extra eine traditionelle Remote-Sitzung aufgebaut werden muss. Dies funktioniert auch zwischen unterschiedlichen Betriebssystemen. Nutzer haben außerdem die Möglichkeit, über die bekannte Copy & Paste-Tastenkombination Dateien von ihrem Gerät zu kopieren und direkt auf einem entfernten Desktop einzufügen. Schließlich soll die neue REST-API dafür sorgen, Reporting-Aufgaben durch Automatisierung schneller und einfacher zu erledigen. Eine Benutzerverwaltungs-API soll die Migration von TeamViewer-Nutzerkonten innerhalb von bestehenden IT-Infrastrukturen einfacher machen. Last but not least werden nun sämtliche TeamViewer-Systembenachrichtigungen in einem Popup-Fenster innerhalb der Computer & Kontakte-Liste aufgelistet. In der Business-Lizenz ist TeamViewer 9 für rund 500 Euro zu haben. *(ln)*



Zu den Neuerungen von TeamViewer 9 zählt eine Service-Warteschlange, mit der sich Nutzer-Anfragen sortieren und geeigneten Support-Mitarbeitern zuordnen lassen

TeamViewer: www.teamviewer.com/de/

Dünn und leistungsstark

MSI fügt dem Tablet-Markt mit dem **Primo81** ein weiteres Modell hinzu. Punkten will der Hersteller mit dem **besonders dünnen (8 Millimeter) und leichten (330 Gramm) Aluminium-Gehäuse** und überzeugenden Akku-Laufzeiten. Selbst beim Abspielen von HD-Videos soll der Akku mehr als sieben Stunden durchhalten. Der 7,85-Zoll-Begleiter ist mit einem **Quad Core-Prozessor ausgestattet** und soll auch mit herausfordernden Multimedia-Anwendungen und hochauflösenden Videos zurechtkommen. **16 GByte Speicher sind bereits integriert, eine Erweiterung ist mit einer microSSD-Karte möglich**. Als Betriebssystem kommt Android 4.2 zum Einsatz. Mit Hilfe des HDMI-Ausgangs lassen sich Bilder und Videos auf dem Fernseher anzeigen. Die Front-Kamera ermöglicht HD-Aufnahmen für die Video-Telefonie. Für hochauflösende Fotos und Full-HD-Videoaufnahmen steht die 2 Megapixel-Kamera auf der Rückseite bereit. Die Bedienung erfolgt per 10-Punkt-Multi-Touch-Steuerung. Verbindungsfreundlich zeigt sich der Primo81 mit dem USB On-The-Go (OTG)-Standard. Damit lässt sich das Tablet über den Mini-USB-Port sowohl mit Host-Rechnern wie PCs oder Notebooks verbinden, kann aber auch selbst als Host für eine externe Tastatur, USB-Sticks, Digitalkameras oder Smartphones agieren. Die notwendigen Adapterkabel sind im Lieferumfang enthalten. Der Primo81-216S ist in den Farbvarianten Weiß/Silber oder Schwarz/Blaugrau-Metallic erhältlich und kostet knapp 170 Euro. *(ln)*

MSI sieht sein Tablet Primo81 als Kommunikations- und Unterhaltungszentrale in schickem Alu-Look

MSI: http://de.msi.com

SNW Europe, 29. und 30. Oktober, Frankfurt/Main

Mehr Fokus, bitte

von John Pardey

Ende Oktober feierte der europäische Ableger der Storage Networking World – die SNW Europe – sein zehnjähriges Bestehen. Dabei hat die Kongressmesse seit einigen Jahren ihr angestammtes Feld erweitert und kümmert sich neben Storage-Fragen und -Produkten auch um die Themen IT-Infrastruktur und Virtualisierung. Den Teilnehmern boten sich also im Rahmen einer umfangreichen Fachausstellung und mehr als 150 Vorträgen zahlreiche Gelegenheiten, sich über Trends und Neuerungen im IT-Betrieb zu informieren. IT-Administrator war für Sie vor Ort.

Die inhaltliche Erweiterung der SNW fand ihr Echo sowohl in den Themen der Vortragsreihen als auch bei den Ausstellern, die mittlerweile eine weit über Storage hinausgehende Produktpalette präsentieren. Entsprechend bot der Veranstalter sechs parallele Vortragsreihen mit Themenschwerpunkten wie Datensicherheit, Big Data, Cloud oder Infrastrukturmanagement.

Ein Wermutstropfen mag dabei für manchen Teilnehmer gewesen sein, dass sich hinter so manchem unter einem sehr praxisnahen Titel angekündigten Vortrag lediglich die Produktpräsentation eines Ausstellers verbarg. Dagegen ist im Rahmen einer Kongressmesse auch grundsätzlich nichts einzuwenden, genauso wenig jedoch gegen ein wenig mehr Transparenz über die inhaltliche Ausrichtung der Sessions.

Dennoch konnte der Besucher natürlich jede Menge interessante Trends und Neuigkeiten aus den Vortragsreihen ziehen, von denen wir einige ausgewählte für Sie im Folgenden aufbereiten. Denn in der IT gibt es nach wie vor echte Mehrwerte zu gewinnen, abseits von überstrapazierten Buzzwords wie Cloud oder Big Data.

Eine Messe der kurzen Wege: Vom Vortragsbereich gelangte der SNW-Besucher mit nur wenigen Schritten in die Fachausstellung

Der Mittelstand will keine Cloud

Doch zunächst bleiben wir beim wohl wichtigsten Schlagwort der aktuellen IT: Cloud. Dass ein vom Marketing praktisch aller IT-Hersteller völlig überstrapazierter Begriff als Bumerang zurückkommen kann, zeigte Jochen Dedek vom SHD System-Haus-Dresden in seinem Vortrag "Cloud – und was der Mittelstand wirklich benötigt". Darin legte er dar, dass die Nicht-IT-Entscheider im Mittelstand – also die Geschäftsführung – sich zahlreichen Umfragen zufolge der Cloud völlig verweigern. Dedek bezeichnete den Begriff Cloud dabei als völlig überstrapaziert, da er mittlerweile für zahlreiche Angebote herhalten müsse, obwohl diese Dienste gar nicht der Definition eines Cloud Service entsprechen. Dies führe bei vielen Geschäftsführern letztendlich dazu, dass der potentielle Nutzen echter Cloud-Angebote in einem völlig unübersichtlichen Markt gar nicht erkannt werden kann.

Zudem fürchten viele Mittelständler Know-how-Verluste durch den Zugriff Unbefugter auf die in der Cloud gelagerten Unternehmensdaten. Mitten im NSA-Skandal liege der Fokus der Betrachtung von Cloud Computing beim Mittelstand daher bei der Sicherheit. Und hier fehle schlicht das Vertrauen. Und auf Herstellerseite wird die Lage insofern noch verschlimmert, als dass die Kosten vieler Cloud-Dienste völlig intransparent seien. Ein Zustand, der für nutzungsbasiert abgerechnete Leistungen untragbar ist.

Es sollte in diesem Dschungel aus fehlendem sichtbaren Nutzen, gefürchteter Unsicherheit und undurchsichtiger Abrechnung letztendlich niemanden überraschen, dass ein Großteil mittelständischer Firmen eine IT on premise nach wie vor für das Mittel der Wahl hält. Hier liegt der Ball jetzt bei den Herstellern. Wenn es Ihnen nicht gelingt, den Nutzen ihrer Leistungen zu vermitteln, werden sie den Mittelstand als Kunden abschreiben müssen.

Hidden Champion: Vertikal integrierte Systeme

Ein wichtiger Trend in der IT-Infrastruktur sind mittlerweile Vertikal integrierte Systeme (VIS), auch als Converged Infrastructure bekannt. Im Gegensatz zu "Cloud" oder "Big Data" fliegt dieser Trend derzeit wohl noch etwas unter dem Radar, was nicht zuletzt an der überschaubaren Zahl von Anbietern liegt. VIS kombiniert alle Elemente einer IT-Infrastruktur – CPU, Storage, Netz und Software – in einem Rack oder einer Box, die vorkonfiguriert und einsatzbereit an die Kunden ausgeliefert wird. Wer noch nie von VIS gehört hat, kann sich diese Systeme am besten als Zwischenstufe zwischen klassischen, offenen IT-Systemen und geschlossenen, für einen bestimmten Dienst vorgesehenen Appliances vorstellen.

Für Ingolf Wittmann von IBM Deutschland steht eine steigende Nachfrage nach derartigen Systemen außer Frage. Dies rühre daher, dass Unternehmen zunehmend die Vorteile neuartiger Technologien und deren gesteigerte Leistungsfähigkeit nutzen möchten. Technologien wie Virtualisierung oder Echtzeitanalyse von Unternehmensdaten bringen aber auch eine gesteigerte technische Komplexität in die IT. Und hier fehle es der bestehenden IT-Mannschaft dann oft an Know-how und es sei äußerst aufwendig, entsprechend geschultes Personal – wie etwa einen SAN-Fachmann – zu finden oder selbst auszubilden.

Dabei spielen die vertikal integrierten Systeme dann ihre Stärke aus: Sie kommen vollständig vorkonfiguriert ins Unternehmen und lassen sich als Applikationsplattform unmittelbar in Betrieb nehmen und über eine einheitliche Managementoberfläche einfach administrieren. Zudem leiste der Hersteller kompletten Support für so unterschiedliche VSI-Komponenten wie Netzwerk oder Storage.

Dennoch gelte es selbstverständlich, genau zu prüfen, ob so ein System der richtige Weg für die eigene IT sei. Denn die nicht gerade preiswerten Systeme, die aktuell von sieben Herstellern in unterschiedlichen Integrationstiefen verfügbar sind, müssen sich natürlich auch in die bestehende Landschaft integrieren. So ist beispielsweise eine zentrale Frage, inwieweit die bestehenden Storage-Systeme mit dem Storage der VIS harmonieren. Aber auch die Gefahr eines Vendor Lock-In stehe, so Wittmann, natürlich im Raum.

Flash macht ernst

Nicht ganz neu, aber auch noch nicht hundertprozentig im Markt angekommen ist Flash-Speicher. Doch die SNW 2013 führte dem interessierten Besucher vor Augen, dass der schnelle Speicher nunmehr Ernst macht. Zum einen ist es das Ziel der Hersteller, sich ein Stück vom 50-Milliarden-Dollar-Kuchen abzuschneiden, der weltweit pro Jahr mit spindelbasierten Festplatten erzielt wird. So beschäftigten sich denn auch im Rahmen der Konferenz gleich acht Vorträge mit dem Einsatz von Flash beziehungsweise SSDs im Unternehmen.

Doch nicht nur die reine Datenspeicherung treibt die Entwicklung voran. Vielmehr versuchen aktuelle Applikationen zunehmend Daten im RAM zu halten, um so Geschwindigkeitsvorteile zu erzielen. Hier stehen den IT-Verantwortlichen nun diverse Ausprägungen von Flash-Caches zur Verfügung, die das Potential haben, Anwendungen wie Datenbanken um die Größenordnung 20 bis 40 zu beschleunigen oder die Anzahl von VMs pro Host zu verdoppeln. So wird Flash zu einer ernsthaften Alternative, wenn es um VDI, ERP, Datenbanken oder Business Intelligence geht.

Fazit

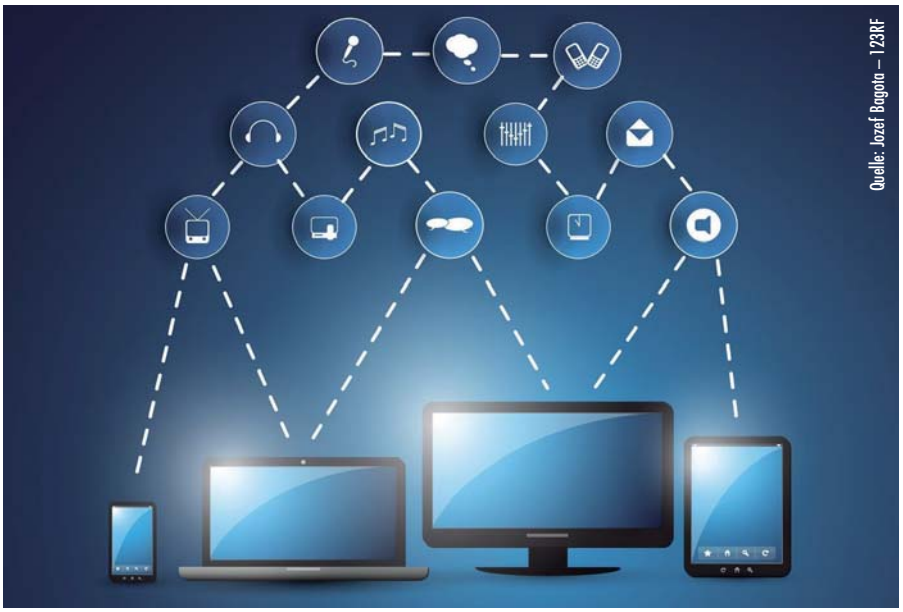
Storage bleibt – angesichts der zunehmenden Mobilität parktisch aller IT-Dienste und -Komponenten – die tragende Säule von IT-Infrastrukturen und braucht deshalb eine Veranstaltung wie die SNW. Mit seiner fokussierten Fachausstellung und den begleitenden Vorträgen hat sich die SNW daher nicht ohne Grund als Nummer eins in Europa etabliert. Doch leider verschwimmt diese Fokussierung mit der Integration von weiteren Infrastrukturthemen, die nicht mehr in derselben Tiefe abgehandelt werden können und daher oft in einer Buzzword-Schlacht enden. Ob Teilnehmer und Aussteller ähnlich denken, wird über den Erfolg der SNW in den nächsten Jahren entscheiden.

Im Test: Citrix XenDesktop 7

Desktop(r)evolution

von Christian Knermann

Mit XenDesktop 7 hat Citrix sein neues Flaggschiff für die Bereitstellung von Applikationen und Desktops veröffentlicht. Das neue Paket führt die bisherigen Produktlinien XenApp und XenDesktop zusammen. In unserem Test zeigte sich dabei, dass sich insbesondere XenApp-Administratoren auf eine umfangreiche Umgewöhnung einstellen müssen. Gleichzeitig wurde deutlich, dass die Zusammenführung der Produkte in einer deutlich übersichtlicheren Administrationsumgebung sinnvoll ist.



Die Entwicklung hatte sich bereits 2012 unter dem Projektnamen "Avalon" angekündigt. Im Rahmen dieses zweistufigen Projekts hatte Citrix es sich zum Ziel gesetzt, die hauseigene Anwendungsbereitstellung fit für die Zukunft zu machen, insbesondere für den Einsatz in der Cloud. Die erste Stufe, Codename "Excalibur", fokussierte darauf, Installation und Administration deutlich zu vereinfachen sowie die Unterstützung mobiler Clients weiter zu verbessern. Ergebnis dieser Phase ist XenDesktop 7.

Neue Editionen und Lizenzen

XenDesktop 7 tritt die Nachfolge der bisherigen Pakete XenDesktop 5.6 und XenApp 6.5 an. XenApp als reine Terminalserver-Lösung verschwindet damit vom Markt und geht in XenDesktop auf. Damit stellt sich insbesondere für Bestandskunden, die bisher nur auf Terminalserver gesetzt haben, die Frage, wie das neue Release zu lizenzieren ist.

XenDesktop 7 ist in vier verschiedenen Editionen verfügbar [1]. Den Einstieg bildet die "VDI Edition", mit der sich ausschließlich virtualisierte Desktop-Betriebssysteme betreiben lassen. Neu ist die sogenannte "App Edition", die die Nachfolge von XenApp antritt und nur den Betrieb von Terminalservern beinhaltet. Die "Enterprise Edition" umfasst sowohl Desktops als auch Terminalserver, kann physische Maschinen einbinden und bringt die Optimierung grafikintensiver Anwendungen mittels "Citrix HDX 3D Pro" mit. Die "Platinum Edition" schließlich erweitert den Funktionsumfang noch, unter anderem um die AppDNA genannte automatisierte Analyse der Kompatibilität von Anwendungen oder auch die Langzeitstatistik von Performance-Daten im Rahmen von Citrix EdgeSight. Die Platinum Edition kann diese Daten bis zu ein Jahr rückwirkend speichern, während die Enterprise Edition diese nur für sieben Tage aufbewahrt.

XenDesktop 7 integriert sämtliche Bereitstellungsarten für virtuelle Desktops und Applikationen, die bislang auf zwei separate Produkte und damit auch getrennte Management-Werkzeuge verteilt waren:

- Ein "Hosted Shared Desktop" bezeichnet eine Sitzung auf einem klassischen Terminalserver. Neben Windows Server 2008 R2 unterstützt XenDesktop 7 auch Windows 2012 als Plattform.
- Der Begriff "Hosted VDI" umfasst virtuelle Instanzen von Windows 7 und 8, die als dedizierte Desktops einzelnen Benutzern fest zugeordnet sein können oder zur Laufzeit dynamisch Anwendern zugewiesen werden.
- Mit der "Remote PC" genannten Option lassen sich auch physische PCs in eine XenDesktop 7-Umgebung einbinden. Das ist nützlich, um in einem ersten Schritt Mitarbeitern von zu Hause Zugriff auf ihren Büro-Rechner zu erlauben, ohne ihnen diesen gleich komplett wegzunehmen und ins Rechenzentrum zu verlagern. Auch lassen sich auf diesem Wege exotische Systeme in eine zentralisierte Umgebung einbinden, die sich nicht ohne Weiteres virtualisieren lassen, etwa weil besondere Erweiterungskarten im PC stecken.

Bisherige Komplexität

Um zu erschließen, wie XenDesktop 7 unter der Haube funktioniert, bietet sich ein Blick zurück an. Bislang basierte die Administration der XenApp-Server innerhalb einer Farm auf dem Protokoll Independent Management Architecture (IMA), einer auf der Microsoft MMC fußenden Management Console und einer Datenbank für den Citrix Datastore mit der kompletten Konfiguration der Farm. Mit XenApp 6.5 kam dann die Aufteilung in die Rollen der Controller und Worker hinzu. Erstere bilden den Kopf der Farm

und erlauben deren Administration. Die Worker verfügen nur über einen reduzierten IMA-Stack und dienen der Abwicklung der Benutzersitzungen.

Mit dieser Arbeitsteilung wurde es vereinfacht, die Worker mittels Citrix Provisioning Services (PVS) aus einem gemeinsamen Basis-Image zu starten. Kehrseite der Medaille war, dass die PVS neben weiteren Servern ebenfalls eine eigene Datenbank nebst separater Konsole sowie einen Agenten erforderten. Sofern Monitoring und statistische Erfassung der Farm gewünscht waren, kam zusätzlich Citrix EdgeSight hinzu, wiederum mit eigenen Agenten auf den Zielsystemen, einer zusätzlichen Datenbank und webbasierter Konsole.

Sollten dann einer solchen Umgebung virtuelle Desktops unter XenDesktop 5.6 hinzugefügt werden, musste neben der XenApp-Farm eine eigenständige XenDesktop Site gepflegt werden. Bei XenDesktop hatte Citrix das IMA-Protokoll bereits durch die Flexcast Management Architecture (FMA) ersetzt, da IMA zwar auf mehrere Hundert Terminalserver skalierbar war, nicht aber auf Tausende oder gar Zehntausende von Desktops. XenDesktop brachte natürlich auch die Anforderung für eine zusätzliche Datenbank sowie eigene Management-Werkzeuge mit sich, nämlich das Desktop Studio für die grundlegende Konfiguration der Site und den Desktop Director als webbasiertes Frontend für Helpdesk-Aufgaben.

Zwar ließ sich die Komplexität vor dem Endanwender verstecken, indem die Ressourcen beider Welten in einem gemeinsamen Webinterface, genannt StoreFront, zusammengefasst wurden. StoreFront erforderte aber eine weitere Datenbank-Instanz. Wer als Administrator mit XenApp 6.5 und XenDesktop 5.6 das komplette Portfolio nutzen wollte, sah sich somit einer kaum überschaubaren Vielzahl von Konsolen und Datenbanken gegenüber.

Neue Einfachheit

Um diesen Gordischen Knoten zu lösen, hat Citrix die Produkte grundlegend renoviert. XenDesktop 7 führt die Entwicklungszweige konsequent zusammen, was für XenApp die größten Umwälzungen bedeutet. Auch die Terminalserver kommunizieren nun intern über FMA. Nunmehr sind ein und dieselben Controller für beide Welten zuständig und es ist nur noch ein Paket des Virtual Desktop Agent (VDA) für die Installation auf den Workern erforderlich – unabhängig davon, ob es sich beispielsweise um einen Windows 8-Desktop oder einen Windows Server 2008 R2-Terminalserver handelt.

Die Setup-Routine des VDA integriert weitere Komponenten, die bisher separat zu pflegen waren. So sind nun der EdgeSight-Agent und auch das Citrix Profile Management enthalten. Welche Funktionen nutzbar sind, entscheidet sich anhand der lizenzierten Edition. Entsprechend ist für eine solche Umgebung nur noch eine Datenbank erforderlich, die wahlweise auf

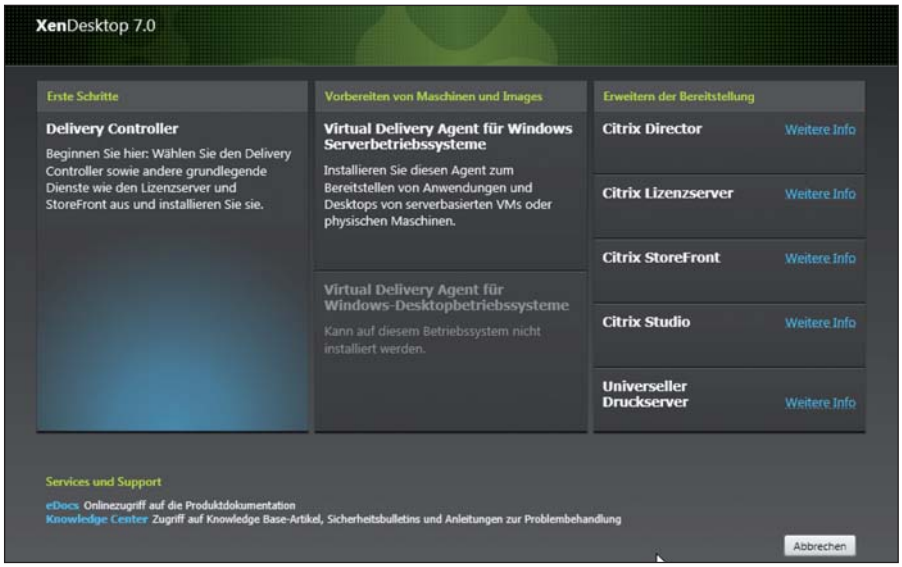


Bild 1: XenDesktop 7 deckt mit einer Setup-Routine alle Anwendungsfälle ab

Bild 2: Der Citrix Receiver vereinfacht die Bedienung von Windows-Anwendungen auf Tablets

einem SQL Server 2008 R2 oder einem SQL Server 2012 laufen darf [2]. Im einfachsten Fall installiert das Controller-Setup die Express Variante des SQL Server 2012.

Für Installationen mit mehr als einem Controller empfiehlt es sich, die Datenbank auf einen eigenständigen Datenbankserver auszulagern. Da die FMA erwartet, dass die Datenbank dauerhaft online ist, sollte dieser Server hochverfügbar auslegt sein, wobei XenDesktop sämtliche von Microsoft gebotenen HA-Techniken unterstützt. Mit XenDesktop werden die "StoreFront"-Dienste auf Version 2 aktualisiert. Diese benötigt nun keine SQL Datenbank mehr, sondern speichert die Favoriten der User in XML-Dateien. Sollen mehrere StoreFront-Server zum Einsatz kommen, werden diese Dateien automatisch synchronisiert.

Ein früheres Feature, das Citrix Anwendungsstreaming, ist nicht mehr dabei. Hierbei handelte es sich um eine Technik, bei der Anwendungen nicht fest installiert, sondern stattdessen paketiert und zur Laufzeit hinzugeladen werden. Citrix hat diese Entwicklung zugunsten des artverwandten Produkts Microsoft App-V aufgegeben. Bestandskunden entsteht aus dieser Entscheidung insoweit kein Nachteil, als die ohnehin erforderlichen Microsoft-Lizenzen für die Remotedesktopdienste (RDS-CAL) beziehungsweise den Virtual Desktop Access (VDA) die Anwendungsvirtualisierung mittels App-V bereits beinhalten. Wer bisher auf das Streaming von Citrix gesetzt hat, muss nun allerdings seine Anwendung mit App-V neu paketieren.

Neben den Kernkomponenten bringt XenDesktop 7 auch für die Infrastruktur die jeweils neuesten Versionen mit. Der Hypervisor XenServer ist in der Version 6.2 enthalten. Allerdings besteht kein Zwang, sofort alle Virtualisierungshosts zu aktualisieren. XenDesktop ist abwärtskompatibel bis zum XenServer 6.0.2. Die Provisioning Services (PVS) als Komponente zur Bereitstellung vieler Desktops und Terminalserver aus jeweils einem Master-Image sind in der Version 7 an Bord. Auch hier besteht keine Verpflichtung, diese einzusetzen, da die Machine Creation Services (MCS) als Alternative nun sowohl mit Desktops als auch Terminalservern umgehen können.

10 Minuten bis zur fertigen Installation

Die gute Nachricht für Neueinsteiger ist, dass für XenDeskop 7 eine Evaluierungsversion heruntergeladen werden kann, die 90 Tage lang läuft. Alternativ zum Test auf eigene Faust bietet der Hersteller auch eine durch einen Citrix-Techniker geführte Demo an. Da wir für unseren Test auf bereits bestehende Lizenzen zurückgreifen konnten, entschieden wir uns stattdessen für den Download der Platinum Edition. Diese umfasst ein 1,8 GByte großes ZIP-Archiv mit den Kernkomponenten von XenDesktop, darunter der Controller, der VDA und auch StoreFront. Bei den "Additional Components" finden sich unter anderem die PVS und der XenServer.

Die Installation des XenServers bietet in der Version 6.2 gegenüber früheren Ausgaben keine Überraschungen. Der XenServer bleibt seinem Slogan "10 to Xen", also zehn Minuten bis zur fertigen Installation, treu. Die weitere Konfiguration inklusive der Hochverfügbarkeit mehrerer Hosts und Anbindung von Shared Storage kann je nach Umgebung natürlich komplexer werden und mehr Zeit beanspruchen. Insgesamt hat Citrix hier aber nur Modellpflege betrieben, sodass sich Admins früherer Versionen ebenso wie Neulinge schnell zurechtfinden werden. Wir widmeten uns daher direkt der eigentlichen Desktop-Infrastruktur.

Controller ermöglicht variable Desktop-Verwaltung

Hierzu installierten wir zunächst einen Windows Server 2008 R2 als Basis für den Controller sowie eine erste Windows 7-VM als Desktop. Zunächst fügten wir auf dem Server das .NET Framework 3.5.1 als Feature manuell hinzu und starteten dann die XenDesktop 7-Setup-Routine. Hier steht zur Wahl, ob die typische Installation eines Controllers gewünscht ist oder ob das System mittels VDA-Installation zu einem Worker werden soll. Weiterhin können zur Erweiterung einer Infrastruktur Komponenten wie der Lizenzserver oder StoreFront separat installiert werden. Wir entschieden uns für die erste Option.

Im nächsten Schritt wählten wir die Kernkomponenten aus. Wir ließen den Lizenzserver aus, da wir auf bestehende Lizenzen zurückgreifen konnten. Den entsprechenden Dienst hatten wir zuvor auf die in XenDesktop 7 enthaltene Version 11.11 aktualisiert. Im folgenden Dialogschritt wurden zusätzliche Komponenten angeboten, darunter der SQL Server 2012 Express, die wir ebenfalls installierten. Das Setup bot daraufhin die automatische Anpassung der Windows-Firewall

an. Auch um weitere Abhängigkeiten wie den Webserver IIS kümmerte es sich selbsttätig. Damit konnten wir die Installation starten, die nach wenigen Minuten erledigt war und keinen Neustart erforderte. Anschließend öffnete sich automatisch das Citrix Studio und wir begannen mit der Konfiguration.

Zur Wahl steht, entweder eine Site zu erstellen, die mittels MCS Ressourcen bereitstellt, oder mit einer leeren Site zu starten und Anwendungen sowie Desktops später hinzuzufügen. Wir entschieden uns für Letzteres. Im nächsten Schritt konnten wir eine Datenbank anlegen. Dann war die Art der Lizenzierung zu konfigurieren. Wir gaben den Namen unseres vorhandenen Lizenzservers ein und konnten daraufhin unsere bestehenden XenDesktop Platinum-Lizenzen einbinden. Wir installierten noch den Virtual Desktop Agent (VDA) auf unserer Windows 7-Maschine. Damit war die Basis-Konfiguration erledigt und wir erstellten einen ersten Katalog. Dabei stehen drei verschiedene Typen von Maschinen zur Wahl:

- Desktopbetriebssysteme umfassen gleichartige Desktops, unabhängig davon ob diese per MCS, PVS oder anderweitig erzeugt und verwaltet werden.
- Serverbetriebssysteme fassen Terminalserver-Hosts zusammen, deren Management ebenfalls über MCS, PVS oder eine andere nicht von Citrix bereitgestellte Technologie erfolgen kann.
- Der Remote-PC-Zugriff dient dem Zugriff auf physische, nicht zentral verwaltete Maschinen.

Im Rahmen unseres Tests veröffentlichten wir unsere Maschine zunächst als Remote-PC. Das entsprechende Computerkonto konnten wir im nächsten Dialogschritt auswählen. An dieser Stelle ist es auch möglich, mehrere Maschinen hinzuzufügen. Das ergibt aber nur dann Sinn, wenn alle Maschinen gleichartig sind. Denn bei einer späteren Veröffentlichung wird eine Remote-PC-Maschine dem ersten Benutzer, der sich anmeldet, exklusiv zugeordnet und steht damit auch nach Abmeldung dieses Benutzers niemand anderem mehr zur Verfügung. Mit der Auswahl der Maschine ist der Katalog fertig. Allerdings werden Kataloge nicht automatisch für Endanwender freigegeben. Dies erfolgt erst im nächsten Schritt über eine sogenannte Bereitstellungsgruppe, die wir ebenfalls über das Studio erzeugen konnten.

Dazu wählten wir den gewünschten Maschinenkatalog und legten einen Benutzer fest, der darauf zugreifen darf. Anschließend konnten wir über die StoreFront unter *http://controller/Citrix/StoreWeb* darauf zugreifen. Nach Anmeldung unseres Test-Benutzers konnten wir von einem Client mit installiertem Citrix Receiver über die entsprechende Webseite eine Verbindung zum gehosteten Desktop aufbauen. Um die verfügbaren Anwendungen und Desktops in das Startmenü zu integrieren, muss der Client-lokale Receiver passend konfiguriert werden und den Webservice unter *http://controller/Citrix/Store* konsumieren. Dies wollte aber zunächst nicht gelingen, da der Client zwingend eine SSL-gesicherte Verbindung erwartet.

Zu Testzwecken erzeugten wir daher über den IIS-Manager ein selbstsigniertes Zertifikat und aktivierten SSL für die Standardwebseite. Daraufhin mussten wir lediglich noch im Citrix Studio über den Knoten "Citrix StoreFront \ Servergruppe" die bisherige Basis-URL auf das Präfix "HTTPS" ändern. Nachdem wir das selbstsignierte Zertifikat auf dem Client in den Speicher der vertrauenswürdigen Stammzertifizierungsstellen importiert hatten, gelang auch die Konfiguration des Receivers.

Ähnlich einfach konnten wir den Receiver für iOS auf einem iPad verwenden. Im Test haben wir dazu mit dem integrierten Cisco-Client eine IPsec-gesicherte VPN-Verbindung ins interne Netz mit der XenDesktop Infrastruktur aufgebaut. Für eine produktive Implementierung ist natürlich eine SSL-gesicherte Verbindung zu bevorzugen. Diese setzt allerdings einen Reverse Proxy, wie beispielsweise Citrix NetScaler, voraus, dessen Einrichtung aber den Umfang dieses Tests sprengen würde.

Den Citrix Receiver hatten wir zuvor kostenlos über den App Store bezogen und konnten über den Browser Safari zunächst auf das Webinterface der StoreFront

zugreifen. Nach der Anmeldung unseres Test-Benutzers konnten wir unseren Desktop direkt aus der Webseite heraus starten oder die Aktion "Aktivieren…" aus dem Dropdown-Menü des Benutzernamens ausführen. Diese lädt eine Konfigurationsdatei mit der Endung "CR", die den Receiver automatisch so konfiguriert, dass zukünftig der Start von Anwendung und Desktops ohne Umweg über den Browser direkt aus der App heraus möglich ist.

Beim Start eines Desktops fällt auf, dass Citrix weitere Funktionen integriert hat, um die Windows-Oberfläche vom Touchscreen des Tablets einfacher bedienen zu können. So tauscht XenDesktop den bekannten Windows-Desktop gegen eine eigene touch-optimierte Variante aus, bei der das Startmenü mit größeren Symbolen aufwartet. Spätestens innerhalb nativer Windows-Anwendungen stößt dieses Hilfsmittel naturgemäß an seine Grenzen, da die Oberflächen der Anwendungen weiterhin auf die Bedienung mit Tastatur und Maus ausgelegt sind. Hier helfen weitere Werkzeuge, wie eine um typische Windows-Tastenkombinationen erweiterte Bildschirm-Tastatur, ein frei positionierbarer Cursorblock oder eine virtuelle Bildschirm-Maus. So lassen sich klassische Windows-Anwendungen auch am Tablet bedienen.

Desktops schnell veröffentlicht

Nachdem wir die RemotePC-Verbindung erfolgreich getestet hatten, untersuchten wir im nächsten Schritt die Veröffentlichung mehrerer gleichartiger Maschinen per Machine Creation Services (MCS). Diese Technik war bereits in früheren Versionen von XenDesktop enthalten. Neu ist nun, dass die MCS ebenso zur Bereitstellung von Terminalservern genutzt werden können. Gegenüber den Provisioning Services sind die MCS weniger komplex und schneller in Betrieb zu nehmen, da sie direkt auf Storage-Ebene des XenServers ansetzen und keiner weiteren Infrastruktur wie TFTP- oder PXE-Server bedürfen.

Das Ganze funktioniert so, dass eine VM mit installiertem VDA als Vorlage benötigt wird. Die MCS legen von dieser VM einen Snapshot an, der im nächsten Schritt als Ausgangspunkt für beliebig viele weitere Desktop-VMs dient. Alle Desktops verwenden somit dieselbe schreibgeschützte Grundlage. Der große Vorteil der MCS besteht darin, dass sie mit geringem Konfigurationsaufwand benutzbar sind. Wenn eine große Anzahl an Zielsystemen zu verwalten ist, empfiehlt es sich aber, alternativ über den Einsatz der Provisioning Services (PVS) nachzudenken, da diese weniger Last auf den Storage-Systemen erzeugen.

Images komfortabel pflegen

Mit ihrer Streaming-Technologie können die Provisioning Services virtuelle und physische Maschinen gleichermaßen verwalten. Allerdings stellen die PVS auch in der Version 7.0 einen eigenständigen Verwaltungsbereich dar, der sich nicht über das Citrix Studio verwalten lässt, sondern eine separate Konsole, eine eigene Datenbank sowie einen oder mehrere zusätzliche Server erfordert.

Da die Targets in der Regel über keine eigene Festplatte mehr verfügen, sondern über das Netzwerk starten, sind zusätzlich DHCP-, TFTP- und PXE-Boot-Dienste erforderlich. Die Dienste lassen sich mit den PVS installieren oder von separaten Servern bereitstellen. Targets werden beim Start via DHCP mit einer IP-Adresse versorgt und laden per TFTP ein initiales Boot-Image, das das Target wiederum in die Lage versetzt, die PVS zu kontaktieren. Die Zuordnung von vDisks zu Target Devices erfolgt basierend auf deren MAC-Adressen. Das Target bootet von der gewünschten vDisk über das Netzwerk. Dies ermöglicht ein Windows-Festplatten-Treiber, der über ein UDP-basierendes Protokoll mit den PVS kommuniziert und dem Target die vDisk als lokalen Datenträger anbietet. Dieses Protokoll arbeitet weitestgehend tolerant gegenüber Störungen im Netzwerk. Verliert ein Target die Verbindung zu den PVS, so stürzt es nicht ab, sondern bleibt lediglich stehen, bis die Konnektivität wiederhergestellt ist.

Mit der Installation und Konfiguration der PVS haben wir uns bereits in einem früheren Workshop beschäftigt [3]. Insbesondere haben wir den äußerst flexiblen Update-Prozess erläutert, der es erlaubt, verschiedene aufeinander aufbauende Versionsstände zu verwalten, zu neuen Images zusammenzuführen oder bei Bedarf auch zu früheren Ständen zurückzukehren. Nachteilig ist zwar die höhere Komplexität, doch trotzdem geht unsere Empfehlung in Richtung der PVS. Denn diese sind ein mächtiges Werkzeug, wenn es darum geht, verschiedene Entwicklungsstände eines Images zu verwalten. Auch sind Bereitstellung, Test und Inbetriebnahme von Image-Updates – ebenso im Notfall die Rückkehr zu einem älteren Stand – wesentlich schneller zu bewerkstelligen, als dies mit den MCS möglich wäre. Und wer die PVS bereits aus früheren Versionen kennt, kann sein vorhandenes Wissen auch unter XenDesktop 7 nahtlos weiterverwenden.

XenApp macht vieles neu und einfacher

Die größte Umstellung haben Administratoren zu schultern, die bislang nur XenApp kennen. Auch Terminalserver werden nun als Bereitstellungsgruppe verwaltet. Der Unterschied besteht lediglich darin, dass Desktop-Betriebssysteme typischerweise nur eine vollständige Desktop-Umgebung veröffentlichen, während Terminalserver sowohl Desktops als auch Applikationen bereitstellen. Damit bietet XenDesktop einen Vorteil gegenüber den reinen Microsoft Remotedesktopdiensten ohne Citrix-Aufsatz, die pro Server von Haus aus entweder nur Desktops oder RemoteApps, jedoch nicht beides gleichzeitig veröffentlichen können.

Welche Applikationen veröffentlicht werden, lässt sich per Rechtsklick auf die Bereitstellungsgruppe festlegen. Der Assistent zeigt sämtliche auf dem Server verfügbaren Anwendungen an und erlaubt es, viele Anwendungen in einem Zug zu veröf-

[1] XenDesktop 7 Features and Entitlements
DAT51

[2] System Requirements for XenDesktop 7
DAT52

[3] Desktops griffbereit
IT-Administrator 05/2012, Seite 46

[4] Lifecycle Announcement for Citrix XenApp
DAT53

Link-Codes

fentlichen. Dies bedeutet allerdings auch, dass Anwendungen pauschal für alle Benutzer der Bereitstellungsgruppe verfügbar sind. Wer den Nutzerkreis einschränken möchte, kann dies nachträglich über die Eigenschaften der einzelnen Anwendung tun. Dort lässt sich die Sichtbarkeit der Anwendung im Receiver auf Benutzer oder Gruppen beschränken.

Ansonsten fällt auf, dass gegenüber XenApp 6.x außer der Zuordnung von Dateitypen zu zentral bereitgestellten Anwendungen keine Konfigurationsoptionen mehr übrig geblieben sind. Der Freigabe-Prozess wurde somit signifikant vereinfacht. Sämtliche Optionen wie Farbtiefe und Bildschirmauflösung werden nun über die Citrix-Richtlinien einheitlich geregelt und müssen nicht mehr pro Anwendung gepflegt werden.

Produkt
Infrastrukturlösung zur Virtualisierung von Desktops und Anwendungen.

Hersteller
Citrix Systems
www.citrix.de

Preis
Die Preise richten sich nach der jeweiligen Edition und der Lizenzierung als "Named User/Device" oder "Concurrent User". So ergibt sich für die vier Editionen jeweils folgender Preis: VDI-Edition: 95/195 US-Dollar; App-Edition 200/450 US-Dollar; Enterprise-Edition 225/500 US-Dollar; Platinum-Edition 350/700 US-Dollar.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator *(max. 10 Punkte)*

Installation und Inbetriebnahme	7
Funktionsumfang	8
Grafik-Performance	8
Tablet-Unterstützung	9
Migration von XenApp	3

Dieses Produkt eignet sich

optimal für Umgebungen, in denen Windows-Anwendungen und -Desktops zentral bereitgestellt werden sollen.

bedingt für mittlere und größere Unternehmen, insbesondere auch zur Anbindung von Außenstellen und mobilen Mitarbeitern.

nicht für Unternehmen, die alternative Betriebssysteme wie Linux zentral bereitstellen wollen.

Citrix XenDesktop 7

Fazit

Citrix XenDesktop 7 räumt die bislang unterschiedlichen Strukturen von XenApp und XenDesktop auf und vollzieht damit einen dringend notwendigen Schritt, da die Vielzahl der Konsolen kaum mehr beherrschbar war. Nunmehr reichen zwei Frontends, um den Überblick zu behalten. Beim Einsatz von PVS kommt maximal eine dritte Konsole hinzu. Die Schritte, die zum Aufbau einer Desktop-Infrastruktur notwendig sind, wurden somit deutlich vereinfacht und Administratoren bisheriger XenDesktop 5.x-Umgebungen finden sich schnell zurecht.

Langgediente XenApp-Administratoren müssen sich aber neu orientieren und sind noch dazu damit konfrontiert, dass noch nicht alle Funktionen von XenApp 6.5 im neuen Produkt implementiert sind. So fehlt beispielsweise das Management von CPU- und Hauptspeicher-Auslastung. Hinzu kommt, dass aufgrund der Änderungen in der Architektur wiederum kein Upgradepfad existiert und die Terminalserver unter XenDesktop 7 entsprechend neu aufgebaut werden müssen. Noch besteht aber kein Grund zu Aktionismus, denn mit dem Feature Pack 2 hat auch XenApp 6.5 noch eine Aktualisierung erfahren, die die Verbesserungen bei der Grafikdarstellung aus XenDesktop 7 enthält. Wer Terminalserver unter Windows Server 2008 R2 mit XenApp 6.5 betreibt, bekommt dafür noch bis Februar 2016 Support [4]. Für die Vorgänger XenApp 5.0 und 6.0 ist zwar bereits früher Schluss, die Zeit sollte aber reichen, um sich mit dem neuen Produkt vertraut zu machen.

Wer allerdings plant, seine IT-Landschaft in Richtung Windows 8 und Windows Server 2012 weiterzuentwickeln, kommt an XenDesktop 7 nicht vorbei. Diese Betriebssysteme werden von den älteren Versionen nicht unterstützt – Grund genug also, sich mit den Neuerungen aus dem Hause Citrix zu beschäftigen. *(jp)*

Im Test: NetIQ Cloud Manager 2.2.1
Selbstbedienung 4.0

von Jürgen Heyer

Ein komfortables Cloud-Portal ist eine wichtige Voraussetzung für eine schnelle, zuverlässige und automatische Bereitstellung dynamischer Ressourcen. Neben den großen Hypervisor-Herstellern, die für ihre virtuellen Infrastrukturen entsprechende Zusätze anbieten, gibt es auch eigenständige Lösungen wie den NetIQ Cloud Manager, der sich nach Belieben kombinieren lässt. IT-Administrator hat sich das Portal genauer hinsichtlich Monitoring, Paketerstellung, Provisionierung und Abrechnung angesehen.


Quelle: Kittisak Taramas – 123RF

Neben den Suiten der großen Hypervisor-Anbieter wie Citrix, Microsoft und VMware, die teilweise selbst Portale für den eigenen Hypervisor zum Aufbau einer Cloud-Umgebung anbieten, gibt es eine überschaubare Anzahl an unabhängigen Produkten wie den NetIQ Cloud Manager, der dafür konzipiert ist, mit allen gängigen Virtualisierern wie VMware vSphere, Citrix XenServer, Microsoft Hyper-V, SUSE Xen und KVM zusammenzuarbeiten. Ein großer Vorteil der Unabhängigkeit ist, dass ein Unternehmen ein Portal nutzen kann und dennoch nicht an einen bestimmten Hypervisor gebunden ist, sondern sogar mehrere parallel betreiben und integrieren kann.

Der NetIQ Cloud Manager (NCM) beschleunigt die auftragsbezogene Auslieferung von Diensten inklusive deren Provisionierung, sodass ein Anwender komfortabel über ein Portal innerhalb einer virtuellen Infrastruktur die benötigten Dienste aus einem Servicekatalog beauftragen und anschließend auch administrieren kann. In der Regel handelt es sich bei den Diensten im Kern um virtuelle Maschinen mit Betriebssystem und darauf vorinstallierten Applikationen wie etwa MS SQL Server 2012, SUSE Apache Web Server oder Adobe Media Server. Selbstverständlich kümmert sich das Portal auch um die Abrechnung.

NCM ist dabei in vollem Umfang mehrmandantenfähig, sodass er sich sowohl zur internen Nutzung als auch zur Bereitstellung an externe Kunden nutzen lässt. Weiterhin lässt sich die Optik durch die Einbindung von Logos sowie einer individuellen Farbgebung kundenorientiert anpassen. Einige große Provider wie Vodacom Afrika, Triple 4, Nixu, EOH und der deutsche Hoster Itenos nutzen NCM und stellen darauf teilweise mehrere tausend virtuelle Maschinen bereit.

Komplette Demo-Umgebung im Internet erreichbar

Der NetIQ Cloud Manager besteht aus mehreren Komponenten, die einzeln einzurichten sind. In der Regel geschieht die Installation in Verbindung mit Spezialisten von NetIQ oder einem Vertriebspartner, wobei in einem ersten Schritt entsprechend der benötigten Umgebungsgröße ein passendes Design zu entwerfen ist. Für interessierte Administratoren, die einen Blick auf eine fertige Umgebung werfen wollen, stellt NetIQ im Internet eine komplett bestückte Demoumgebung bereit.

Hier können Sie sich mit unterschiedlichen Rollen anmelden, um die Möglichkeiten aus Sicht eines Administrators, aber auch eines Anwenders zu betrachten, darüber hinaus Aufträge abzusetzen, den notwendigen Workflow durchzuspielen und zu beobachten, wie der Cloud Manager reagiert und arbeitet.

Eigeninstallation nur mit umfassenden Linux-Kenntnissen

Wer den NetIQ Cloud Manager selbst installieren will, benötigt umfassende Linux-Kenntnisse, denn die gesamte Plattform läuft unter SUSE Linux Enterprise Manager 11 SP2 (SLES 11). Zum Herunterladen der Ressourcen erhielten wir einen entsprechenden Link auf die Download-Seiten.

Im Wesentlichen besteht NCM aus zwei Komponenten, die eng zusammenarbeiten. Dies sind der "Cloud Manager Application Server" und der "Orchestration Server" mit jeweils eigenen Konsolen. Den Application Server gibt es in einer Cloud-Umgebung nur einmal, der Orchestration Server wird je nach Größe und Design der Plattform mehrfach benötigt. So unterteilt sich eine Cloud Manager-Umgebung in Zonen und Ressourcengruppen. Eine Ressourcengruppe besteht aus einem oder mehreren Servern mit gleichem Hypervisor. Optional kann es sich auch um einen vSphere-Ressourcenpool handeln, der als Ressourcengruppe abgebildet wird. Alle Ressourcen in einer Gruppe sollten sich auf gleichem Leistungsniveau bewegen, damit ein Dienst stets mit identischer Performance läuft und es letztendlich keine Rolle spielt, wohin ihn das System legt. Eine Ressourcengruppe kann sich nicht über mehrere Zonen erstrecken und nicht den Plattenspeicherbereich mit einer anderen Gruppe teilen. Über getrennte Ressourcengruppen in einer Zone können Sie beispielsweise einen Bereich mit besonders leistungsstarken vSphere-Hosts für geschäftskritische Anwendungen definieren und eine Laborumgebung mit Standardhosts auf Xen-Basis.

Das Management und die Aufgabenverteilung in einer Zone übernimmt der Orchestration Server. Ist dieser mit der Abarbeitung aller Aufträge überfordert, sind weitere Server zu installieren, die jeweils wieder eigene Zonen mit darunter liegenden Ressourcengruppen bilden. So ergibt sich eine übersichtliche und gut skalierbare Baumstruktur.

Die Kommunikation zwischen einem Orchestration Server und den zugewiesenen Hypervisor-Hosts erfolgt über einen Agenten, der auf diesen zu installieren ist. Bei einem VMware vCenter kann der Agent auf dem vCenter Server oder einer anderen VM, deren Betriebssystem unterstützt wird, mitinstalliert werden.

Für die initiale Administration der Orchestration Server in einer Cloud dient die Cloud Manager Orchestration Console, die Application Console ist schließlich das Portal, über das die Benutzer und Administratoren die Plattform nutzen.

Anfangs zwei, später nur eine Konsole erforderlich

Nur in der Einrichtungsphase werden beide Konsolen im Wechsel benötigt, bei der tatsächlichen Nutzung des Cloud Managers konzentrieren sich die Tätigkeiten ausschließlich auf die als WebGUI realisierte Application Console. Mit dieser beginnt auch der Einstieg, indem eine Struktur wie beschrieben bestehend aus Zonen und Ressourcengruppen angelegt wird. Beim Anlegen einer Zone sind der zugehörige Orchestration Server und dessen Anmeldeinformationen anzugeben. Optional können Sie für die Kommunikation SSL aktivieren.

Weiterhin muss der Administrator mindestens eine Organisation anlegen. Dabei handelt es sich um die Bereiche oder auch Mandanten beziehungsweise Kunden, die die Cloud-Dienste nutzen. Einer Organisation weist der IT-Verantwortliche nun die Ressourcengruppen mit den Hosts, Servicelevels (SLAs) und Netzwerken zu, ebenso die erstellten Templates, die im Servicekatalog sichtbar sein sollen. Die Konsolenansicht lässt sich für jeden Mandanten individuell anpassen und beispielsweise das jeweilige Firmenlogo einbinden. Innerhalb einer Organisation können wiederum Geschäftsbereiche (Business Groups) definiert werden. Die Bereiche können wahlweise Ressourcen gemeinsam nutzen oder auch nur einzelne für sich.

Der Zugang zu NCM erfordert eine Benutzeranmeldung, wobei sich in den Konsolen manuell Benutzer und Gruppen anlegen oder diese von einer LDAP-Quelle importieren lassen. Über die Gruppen hinaus gibt es noch Rollen, die innerhalb von NCM die Berechtigungen festlegen wie Business Group Viewer, Business Group Owner, Organization Manager oder Zone Administrator. Entsprechend der Rolle sieht der Benutzer oder Manager in der Kopfzeile der Konsole nur einen Teil der Schaltflächen.

Vom Aufbau her ist die Application Console recht übersichtlich gestaltet und unter anderem in Deutsch verfügbar, auch wenn einige vom Administrator genutzte Bereiche nicht übersetzt wurden. Wie bereits erwähnt sieht ein Benutzer nur einen Teil der Icons entsprechend seiner Rolle, die volle Ansicht genießt nur der Cloud Administrator. Dieser findet unter der Home-Ansicht namens "Getting Started" diverse Assistenten, um die beschriebenen Zonen, Ressourcengruppen, Organisationen, Geschäftsbereiche sowie Benutzer und Gruppen anzulegen. Weiterhin definiert er hier die Service-Levels und die sogenannten Workload Templates, auf die wir später noch genauer eingehen. Wichtig für den Cloud Administrator ist auch die Capacity-Ansicht, die einen schnellen Überblick über den Zustand der gesamten Cloud liefert. Grafisch dargestellt sind die Belegung von Arbeits- und Festplattenspeicher, vCPU sowie Pooled MHz für die komplette Cloud, die Nutzung durch einen einzelnen Mandanten sowie die Auslastung der Zonen und der Ressourcengruppen. Farbige Häkchen zeigen, ob alles in Ordnung ist oder nicht.

Die in Java geschriebene Orchestration Console dient nur dazu, die grundlegenden Einstellungen für die Orchestration Server in einer NCM-Umgebung vorzugeben. So ist es für die Aufnahme des Betriebs zuerst erforderlich, mindestens einen Host über den zu installierenden Agenten

Systemvoraussetzungen

Orchestration und Application Server

SUSE Linux Enterprise Server 11 Service Pack 2 (SLES 11 SP2 64 Bit), Intel CPU Dual-Core 2,5 GHz, 64 Bit, 4 GByte RAM, 40 GByte Plattenkapazität, Datenbank PostgreSQL (in SLES enthalten)

Cloud Manager Application Console

Web-basierend, Internet Explorer 9.0 oder höher, Mozilla Firefox 7.x oder höher, Safari 5 oder höher

Unterstützte Hypervisoren

VMware vSphere 4, vSphere 5 ESXi; Citrix XenServer 5.6, XenServer 6 Free Edition; Microsoft Hyper-V auf Windows Server 2008 R2; SUSE Xen 4.0 auf SLES 11; KVM auf SLES 11 SP1/SP2

Unterstützte Gastbetriebssysteme (nicht auf jedem Hypervisor)

SLES 10/11, RHEL 5/6, Windows Server 2003 R2/2008 R2 (jeweils aktuellste Service-Packs)

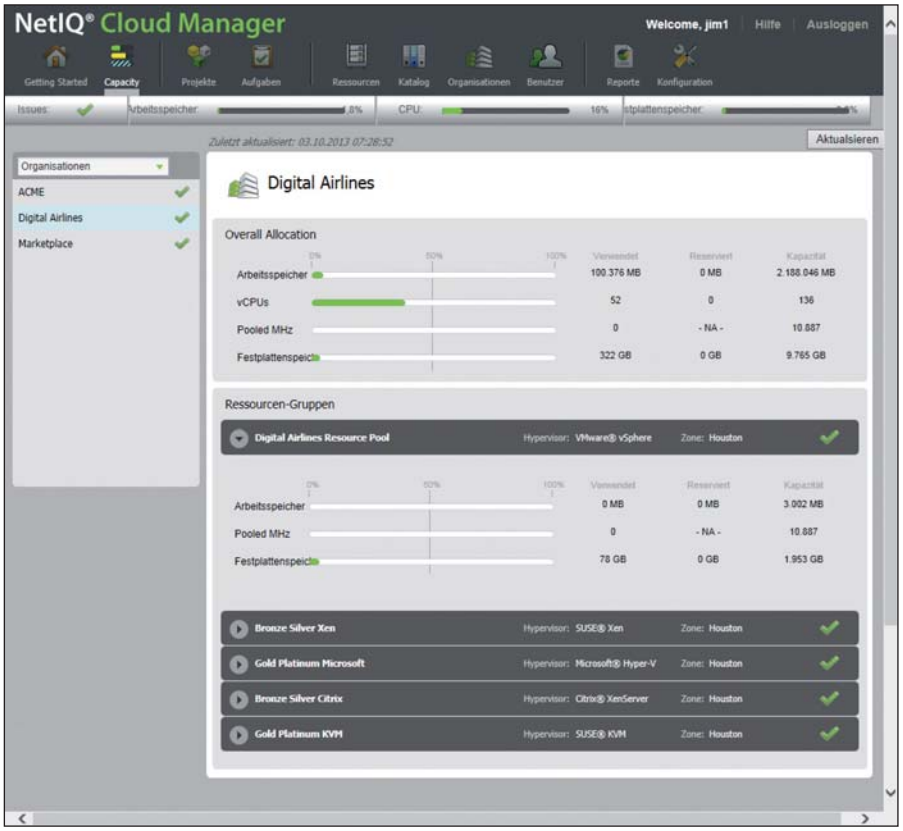


Bild 1: Der Cloud Administrator kann die Verteilung der Ressourcen auf die unterschiedlichen Kunden sowie die Auslastung sehr übersichtlich einsehen

anzubinden, damit der Orchestration Server eine Ressource besitzt, die er für eine Provisionierung nutzen kann. Ist dies geschehen, laufen automatisch die ersten Discovery Jobs, die von diesem Host relevante Informationen wie Betriebssystem, CPU-Typ und -Takt, den Arbeitsspeicher und so weiter einlesen. Weiterhin loggt die Console alle Aktivitäten mit und dient bei Problemen zum Debugging.

Die Aufgabe des Orchestration Servers in Verbindung mit den Agenten ist es auch, die VMs auf den Hosts zu steuern. Während der Agent bei Xen und Hyper-V direkt auf dem Host installiert wird, geschieht dies bei vSphere über den vCenter Server beziehungsweise den vSphere Client. Zur Provisionierung virtueller Maschinen verwendet der Orchestration Server Hypervisor-spezifische Provisionierungsadapter, die für VMware vSphere, Citrix Xen Server, MS Hyper-V, SUSE Xen und KVM verfügbar sind. Das Handbuch beschreibt im Detail, welcher Adapter welche Aktion (unter anderem Provisionieren, Klonen, Herunterfahren, Löschen) auf welchem Gastbetriebssystem unterstützt.

Fertige Pakete bequem schnüren

Damit Anwender über das Portal Aufträge einstellen können, muss der Servicekatalog gefüllt werden, beim Cloud Manager mit sogenannten Workload Templates. Dies sind letztendlich virtuelle Maschinen mit einem Betriebssystem und optional zusätzlich installierter Applikation. In der Demo-Umgebung war hierzu bereits eine Vielzahl an Beispielen angelegt. Der Servicekatalog wird ergänzt durch Add-ons wie beispielsweise zusätzliche Applikationen oder auch einen Dienst wie Backup oder Load Balancing. Hinterlegt sind weiterhin relevante Nutzungsbedingungen und Paketpreise. Gut gefallen hat uns die informative Übersicht der Workload Templates, die neben einer Bezeichnung und Beschreibung die Zone, den genutzten Hypervisor und das als Basis genutzte VM Template auflistet.

Der Administrator kann sehr einfach weitere Pakete schnüren, indem er ein VM Template (Vorlage) auswählt, Namen und Beschreibung vergibt, bei Bedarf die Ressourcengrenzen anpasst und die Einrichtungskosten hinterlegt. Diese Ressourcengrenzen geben für die CPUs, den Arbeitsspeicher, die Anzahl der Netzwerkkarten sowie die Plattenkapazität Werte für Minimum, Standard und Maximum vor. Daneben lassen sich weitere Festplatten hinzufügen, Betriebssystemeinstellungen (Hostname, Domäne, Run Once-Befehl), bei Windows der Produktschlüssel und Registrierungsinformationen ergänzen, verfügbare Add-ons, Preispakete und hinterlegte Nutzungsbedingungen eintragen sowie Verknüpfungen zu bestimmten Organisationen vorgeben. Letzteres dient dazu, eine Vorlage nur einer bestimmten Organisation oder Abteilung zur Verfügung zu stellen.

Ein Benutzer, der eine Vorlage auswählt, kann nun wiederum selbst die Ressourcen in dem vorgegebenen Bereich variieren und muss die noch fehlenden Informationen vervollständigen. Im Test haben wir problemlos einige neue Templates angelegt. Wenn nun ein Benutzer einen neuen Service anfordern will, muss er dazu ein Projekt eröffnen. Dieses bekommt einen Namen sowie optional ein Laufzeitende und wird einer Abteilung zugewiesen.

Ein Projekt kann wiederum aus mehreren Aufträgen (Workloads) bestehen. Beim Hinzufügen eines Auftrags kann der Nutzer wie oben beschrieben weitere Angaben ergänzen und die Ressourcen in den vorgegebenen Grenzen verändern. Auch muss er ein Service Level auswählen und für einen Fernzugriff per VNC ein Passwort angeben. Sofern er eine virtuelle Maschine mehrfach benötigt, kann er diese einmal festlegen und dann mehrfach kopieren. So ist sichergestellt, dass alle VMs die gleichen Einstellungen haben. Beim Anlegen eigener Projekte im Test wunderten wir uns gelegentlich, dass sich das Anlegen eines Auftrags nicht abschließen ließ. Dies war aber regelmäßig darin begründet, dass noch eine zwingend geforderte Eingabe offen war. Die Konsole springt dann zwar auf das Registerblatt, wo die Angabe fehlt, das betroffene Feld ist aber nur durch ein kleines rotes Kreuz markiert, das nicht direkt ins Auge sticht. Gefallen hat uns, dass die anfallenden Kosten bei allen Änderungen angepasst werden und auch überall zu den Positionen die einzelnen Kosten angegeben

Einfach verlässlich scannen

Die wegweisende Technik zum Scannen von Dokumenten – damit Ihre Geschäftsprozesse durchlaufen.

you can

ScanFront 330 | P-208 | P-215 | DR-C125/W | DR-C120 DR-C130 | DR-M140 | DR-M160 | DR-6010C | DR-6030C | DR-G1100 DR-G1130 | DR-X10C

Strom und Platz sparen dank CMOS Contact Image Sensor

Die Canon Dokumentenscanner verfügen über einen CMOS Contact Image Sensor. Dank mehrerer Linsen, die auf dem Sensor untergebracht sind, werden scharfe, saubere Scans erzielt. Zudem werden die Lesbarkeit von Texten und das OCR verbessert. Da das reflektierte Licht direkt vom Dokument zum Sensor gelangt, ist die Bauweise des Scanners sehr leicht und kompakt. Durch den extrem kurzen Lichtweg und den Einsatz von LEDs als Lichtquelle wird der Stromverbrauch gesenkt* und der Scanner ist ohne Aufwärmzeit sofort einsatzbereit. Über zwei Scanleisten werden Vorder- und Rückseite gleichzeitig eingelesen.

Variabler, zuverlässiger Dokumenteneinzug

Höchst vielseitig: Die Canon Scanner verarbeiten mühelos unterschiedlichste Vorlagen vom Stapel – von schwerem Papier über Durchschläge bis hin zu Scheckkarten. Der Papiereinzug ist unkompliziert und zuverlässig und umfasst bei den meisten Systemen auch eine Ultraschall-Doppelzufuhrerkennung.

Benutzerfreundliche Software für verschiedene Anwendungen

Die Canon Software ist auf die Anforderungen des Nutzers zugeschnitten und bietet ein einfaches, intuitives Bedienfeld.

Überragende Bildqualität mit hochentwickelter Bildverarbeitung

Eine große Zahl von Bildbearbeitungsfunktionen (z.B. die Entfernung von Moiré-Effekten, schwarzen Rändern und Lochungen) sorgt für makellose Scans. Und die Funktionen zur automatischen Textverbesserung und Kontrastschärfung erleichtern die Weiterverarbeitung und Archivierung (und nicht zuletzt das Wiederfinden).

Mehr Infos in Internet unter
www.canon.de/dr-scanner

oder per Mail an
dr-scanner@canon.de

Canon Electronics Inc.
www.canon-elec.co.jp

Canon

* Der Stromverbrauch für den CIS Sensor und die LEDs zusammen ist in etwa nur 1/16 dessen, was konventionelle CCD Sensoren und Fluoreszenzlampen benötigen

sind. Kostentreiber sind so für den Auftraggeber einfach erkennbar. Auch kann dieser sich auf einer Detailseite alle Projektdetails rund um die Laufzeit und die Kosten auflisten lassen.

Sofern es bei der Anlage eines Projekts eine Frage gibt, die sich nicht sofort klären lässt, kann der Benutzer den Auftrag speichern, ohne ihn zu verschicken. So wird vermieden, dass ein Auftrag aus solch einem Grund verworfen und später nochmals von Anfang an erfasst werden muss. Ist der Auftrag komplett, verschickt ihn der Anwender, wodurch er in den Genehmigungsworkflow gelangt. Ist ein Auftrag im Workflow, kann der Benutzer ihn jederzeit einsehen und auch zurückziehen, aber nicht mehr verändern. Das Zurückziehen eines Auftrags bedeutet nicht, dass dieser gelöscht wird, sondern er erhält wieder den Status wie beim anfänglichen Speichern und kann nun bei Bedarf verändert werden. Anschließend muss er allerdings den gesamten Genehmigungsweg erneut durchlaufen. Um bei vielen Projekten ein einzelnes leichter zu finden, lässt sich die Ansicht mit wenigen Mausklicks filtern.

Vertragskonforme Bereitstellung

Je nach Vertragsverhältnis zwischen Cloud-Provider und Kunden lässt sich der im NCM hinterlegte Genehmigungsworkflow unterschiedlich gestalten, wozu es neben der Administratorenrolle auch eine Sponsorenrolle gibt: Benötigt ein Anwender eine Ressource in der Cloud, so erstellt er wie beschrieben einen Auftrag. Dieser muss nun womöglich von einem Administrator im eigenen Unternehmen genehmigt werden. Ist dies geschehen, landet die Anfrage beim Cloud-Provider als Sponsor, der ebenfalls zustimmen muss, dass er den Auftrag auch annimmt. Erst dann wird der Auftrag realisiert. Hat dagegen ein Kunde bereits einen festen Ressourcenpool gemietet, ist die Zustimmung eines Sponsors nicht erforderlich, solange sich der Kunde im Rahmen seiner Ressourcen bewegt.

Letztendlich handelt es sich bei NCM um ein Werkzeug, mit dem nicht nur Aufträge realisiert werden, sondern auch Verträge zwischen zwei Unternehmen mit den entsprechend verbindlichen Abläufen abgeschlossen werden. Damit dies gesetzeskonform geschehen kann, lassen sich in NCM diverse Szenarien realisieren. Dies gilt übrigens auch für die Laufzeit. So ist es möglich, Mindestlaufzeiten festzulegen und für längere Laufzeiten oder Leistungspakete Rabatte einzuräumen. So kann ein Mandant jederzeit weitere Ressourcen beantragen, um letztendlich den Umsatz zwischen Provider und Kunde zu erhöhen. Eine Rückgabe ist dann aber vor Ablauf der vereinbarten Laufzeit nicht möglich.

Auch wenn der Fokus des Cloud Managers auf der Bereitstellung von Ressourcen liegt, kann er zusätzlich noch weitere Dienstleistungen anbieten, was die anschließende Betreuung anbetrifft. In der Regel übernimmt ein Kunde nach der Bereitstellung einer VM dessen Pflege, es lässt sich aber auch ein "Managed Server"-Add-On einrichten, mit dessen Ergänzung ein Kunde weitere Dienstleistungen kauft. Dies kann eine Applikationsaktualisierung sein, was beispielsweise dann interessant ist, wenn es sich beim Cloud-Angebot darum handelt, dass ein Unternehmen die Nutzung seiner eigenen Applikationen vermarktet und dafür dann den Updatedienst übernimmt. In so einem Fall müssen natürlich auch Wartungsfenster vereinbart werden, in denen die Updates stattfinden dürfen. Neben dem Applikationsupdate kann weiterhin ein Patchmanagement für das Betriebssystem mit enthalten sein. Weiterhin kann der Provider die Last einer VM kontinuierlich überwachen und dem Kunden bei einer längeren oder dauerhaften Überschreitung von vorgegebenen Lastgrenzen eine Erweiterung vorschlagen.

Remote-Zugriff komfortabel, Reporting eher nicht

In NCM integriert ist der administrative Zugriff auf die gemieteten Ressourcen. Aus dem Portal heraus kann ein Anwender eine VM starten, anhalten und abschalten sowie das Ereignislog einsehen. Der Konsolenzugriff erfolgt per VNC und erfordert die Angabe des bei der Einrichtung festgelegten Passworts. Der Prozess ist so gestaltet, dass dieses Passwort nicht zwischengespeichert werden kann und eine Konsole sich nach dem Schließen nicht ohne erneute Passworteingabe wieder öffnen lässt.

Neben dem Zugriff über das Portal wird auch der Zugang über mobile Medien unterstützt. In einem Webcast demonstrierte uns NetIQ eine Aufschaltung auf das Portal und eine virtuelle Maschine per iPad.

Berichte lassen sich wahlweise in den Formaten PDF, CSV und XLS abrufen. Um einen Report zu erstellen, ist ein Assistent

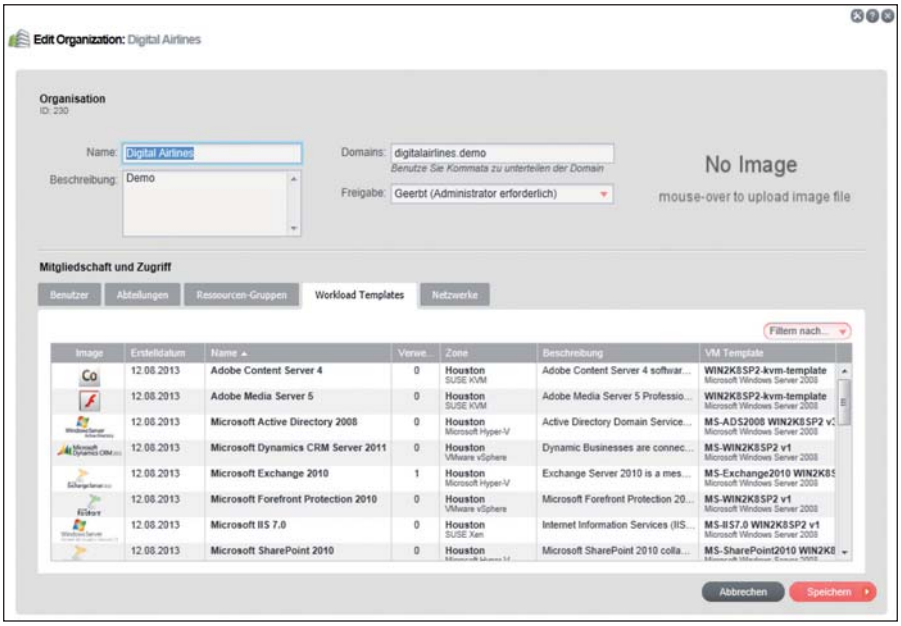


Bild 2: Der Anwender kann bei der Bestellung von Diensten aus den vorbereiteten Images wählen, für die er oder seine Organisation berechtigt ist

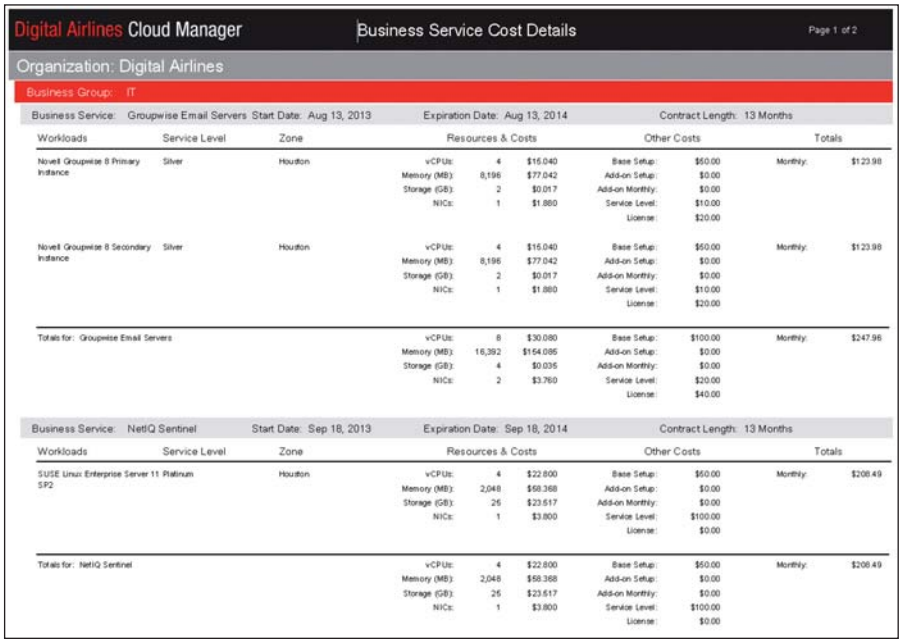


Bild 3: Der Cloud Manager bietet eine übersichtliche Anzahl an Berichten an, die sich unter anderem auch als PDF-Datei generieren lassen

in NCM integriert. Dieser bietet neun Vorlagen zur Auswahl an und fragt dann noch den einen oder anderen Filter ab (Zone, Organisation und ähnliches). Anschließend wird der Report erstellt. Insgesamt ist die Anzahl der zur Verfügung stehenden Berichte überschaubar. Allerdings müssen wir hier dem Cloud Manager zugutehalten, dass die einzelnen Ansichten zu den gebuchten Ressourcen schon sehr informativ sind.

Optionen für mehr Komfort und Sicherheit

Neben den eingangs beschriebenen Basiskomponenten lassen sich einige spezielle Funktionen beziehungsweise Tools ergänzen, um die IP-Adressvergabe zu vereinfachen, das Logging zu erleichtern und die Anmeldesicherheit zu erhöhen.

So lässt sich NCM mit dem NetIQ Cloud Security Service (NCSS) und dem Novell Access Manager (NAM) kombinieren. So sorgt der NCSS Connector dafür, dass sich NCM besser in verschiedene LDAP-Infrastrukturen integrieren lässt und LDAP-Benutzer Rechte in NCM entsprechend ihrer Firmenzugehörigkeit bekommen.

Novell Sentinel wiederum ist eine Lösung, um Sicherheitshinweise und Ereignisse von NCM zu sammeln und auszuwerten, um so Hinweise zu Bedrohungen zu geben und den Administrator beim Treffen von sicherheitsrelevanten Entscheidungen zu unterstützen.

Um eine automatische IP-Adressvergabe zu ermöglichen, lässt sich NCM mit der "Nixu Cloud IP Suite" kombinieren, einem leistungsfähigen IP Address Management (IPAM). NetIQ und Nixu haben hierzu eine Kooperation vereinbart.

Fazit

Der NetIQ Cloud Manager erwies sich im Test als leistungsstarkes Portal, um Cloud-Dienste automatisch und effizient bereitzustellen. Durch seine Mehrmandantenfähigkeit eignet sich das Werkzeug nicht nur für eine Nutzung in einer Private Cloud, sondern auch als öffentliches Portal für große Provider. Von Vorteil ist, dass sich bei Bedarf neben der Bereitstellung auch weitere Leistungen wie das Einspielen von Updates oder eine Lastanalyse mit Vorschlägen für eine Erweiterung der Ressourcen hinzufügen lassen.

Gut gefallen hat uns, dass sich mit der Bereitstellung verschiedene SLAs verknüpfen und bepreisen lassen und das Portal die kompletten Abrechnungsdaten ermittelt. Aus Kundensicht vorteilhaft ist, dass alle Kosten für eine zu buchende Ressource bereits im Vorfeld detailliert aufgelistet werden, inklusive der Teilbeträge, sodass sich die Kostentreiber leicht identifizieren lassen.

Ein weiterer Vorteil ist die gleichzeitige Unterstützung aller namhaften Hypervisor-Typen, was einen flexiblen Einsatz erlaubt. Nicht ganz trivial ist allerdings die Einrichtung des Cloud Managers. Hier empfiehlt es sich, bei der Konzeption und Implementierung die Dienste von NetIQ oder eines Partners in Anspruch zu nehmen. Und auch beim Reporting besteht noch Verbesserungspotenzial. *(jp)*

Produkt

Lösung zum Aufbau eines mehrmandantenfähigen Cloud-Portals zur Bereitstellung von Diensten.

Hersteller

NetIQ
www.netiq.de

Preis

Der Cloud Manager wird unter anderem in einem Pay-as-you-go Modell angeboten, das pro Workload monatlich 8,50 Euro kostet.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

***So urteilt IT-Administrator** (max. 10 Punkte)*

Mehrmandantenfähigkeit	9
Hypervisor-Unterstützung	9
Paketerstellung	8
Gestaltung des Portals	8
Reporting	5

Dieses Produkt eignet sich

optimal für Unternehmen, die sich in ihrer Cloud-Umgebung nicht auf einen Hypervisor festlegen, sondern verschiedene parallel nutzen wollen. Der Cloud Manager unterstützt hier die namhaften Produkte.

bedingt für Unternehmen, die beim Aufbau einer Cloud nur auf den Hypervisor eines Herstellers setzen. Hier sollte im Detail geprüft werden, ob sich nicht das Cloud-Produkt des gleichen Herstellers noch besser integrieren lässt.

nicht für Firmen, die keinen Bedarf haben, eine Cloud zur Bereitstellung von Diensten aufzubauen.

NetIQ Cloud Manager 2.2.1

Im Test: Bomgar Box 13.1.2

Fernwartung aus der Kiste

von Sandro Lucifora

Der Fernzugriff ist eines der zentralen Hilfsmittel des Administrators. Dabei spielt natürlich die Sicherheit eine entscheidende Rolle. Bomgar hat mit der gleichnamigen Box eine Fernwartungslösung im Angebot, die mehr sein will als ein reines Bildschirmübertragungstool. Sie koordiniert Support-Anfragen selbstständig und verschafft den Kontakt zum richtigen IT-Team. Wir haben die neue Version 13.1.2 der zugrundeliegenden Software Base zum Anlass genommen, uns die umfangreiche Bomgar Box genauer anzuschauen.

Wer unter Fernwartung bisher die direkte Verbindung zwischen zwei Computern und das Übertragen von Bild, Ton und der Signale der Eingabegeräte verstand, der muss mit der Bomgar Box umdenken. Denn hierbei handelt es sich um eine physikalische oder virtuelle Appliance, die als Knotenpunkt den Fernwartungs-Datenverkehr steuert. Herkömmliche Lösungen wie etwa Microsoft Remote Desktop bauen hingegen reine Peer-to-Peer-Verbindungen von Rechner zu Rechner auf, was aus vielerlei Hinsicht Sicherheitsrisiken birgt. Je nach eingesetzter Lösung sind daher Einstellungen an der Firewall notwendig, um wie bei RCP und VNC über die Kombination von IP-Adresse und Port auf einen bestimmten Rechner zu gelangen. Diese Ports sind somit auch für ungewollte Gäste geöffnet. Diverse Systeme am Markt stellen die Verbindung zwar über den Web-Port 80 her und gelangen somit durch die Firewall. Doch laufen die Sitzungsdaten auch über den Server des Herstellers.

Der Fokus von Bomgar liegt vor allem auf der Sicherheit der Datenverbindungen. Daher routet und protokolliert die Bomgar Box den gesamten Sitzungsdatenverkehr zentral. Jede Remotesitzung läuft über die orangene Appliance. Da sie im eigenen Unternehmen steht, bleiben sensible Daten hinter der Firewall und sämtliche Remote-Zugriffe lassen sich zentral verwalten. Daher ist die Lösung auch im Bereich von Banken, dem Militär und Regierungen wiederzufinden. Aber auch die Handhabung selbst ändert sich durch den Einsatz der Appliance. Support-Teams und hilfesuchende Anwender finden über die webbasierte Supportseite in Echtzeit zueinander.

Neben der Fernwartung von Windows-PCs unterstützt der Hersteller auch Mac- und Linux-Systeme und greift auf die möglichen Remote-Support-Werkzeuge von Android, iOS, BlackBerry und Windows Mobile zu. Die Clients aller unterstützten Plattformen sind im Produktpaket enthalten, wodurch sich die verschiedenen Geräte über ein und denselben Weg bedienen lassen.

Installation mit SSL-Zertifikat

Die Hardware ist in den drei Varianten B200, B300 und B400 lieferbar, die mit unterschiedlichen Prozessoren, Hauptspeichergrößen und RAID-Systemen ausgestattet sind. Neben der Hardware-Appliance hat der Hersteller auch eine virtuelle Variante der Bomgar Box im Programm. Der Funktionsumfang ist bei beiden Varianten derselbe, lediglich die Plattform ist eine andere. Die VM läuft auf einem VMware-Host wie vSphere, ESX-Server oder Workstation.

Die Installation einer Bomgar-Appliance besteht aus mehreren Schritten. Um die VM in Betrieb zu nehmen, mussten wir diese dem VMware-Host hinzufügen, die zusätzliche Festplatte für die Sitzungsdaten einrichten und starten. Ab hier bestand kein Unterschied mehr in der weiteren Konfiguration zwischen der virtu- ellen und der Hardware-Version. Nach dem Start war die Appliance noch nicht einsatzbereit. Für den reibungslosen Betrieb richteten wir einen öffentlichen Domainnamen im DNS ein und ließen ihn auf die IP-Adresse der Appliance zeigen. In der Testumgebung lief die VM hinter einem Router, auf dem wir ein Port-Forwarding für Port 443 einrichteten. Danach installierten wir ein öffentliches SSL-Zertifikat. Dies ist wichtig, da bei selbst signierten Zertifikaten die Zusammenarbeit mit mobilen Endgeräten nicht reibungslos abläuft. Wir stellten uns

Systemvoraussetzungen

Virtuelle Appliance

VMware vSphere, ESX-Server oder Workstation. Neben 12 GByte Platz für die VM benötigt die Appliance rund 200 bis 300 GByte freien Speicherplatz, um Daten auszulagern.

Ausstattung der Hardware-Appliance

B200: Intel Xeon Quad Core-Prozessor mit 3,1 GHz, eine 3,5 Zoll 500 GByte SAS-Festplatte, 4 GByte RAM, zwei 1 GBit-Ethernet-Ports, 1 HE.

B300: Dual Intel Xeon Quad Core-Prozessor mit 2,53 GHz, vier 3,5 Zoll 300 GByte SAS-Platten mit 15.000 Umdrehungen und RAID 6, 12 GByte DDR2-RAM, Zwei 1 GBit-Ethernet-Ports, 1 HE.

B400: Zwei Intel Xeon 2,93 GHz Quad Core-Prozessoren, zwei 2,5 Zoll 64 GByte SSDs (RAID 1) und sechs 3,5 Zoll 600 GByte SAS-Disks (RAID 6), Gesamtkapazität 2,1 TByte, zwei 1 GBit-Ethernet-Ports, 2 HE.

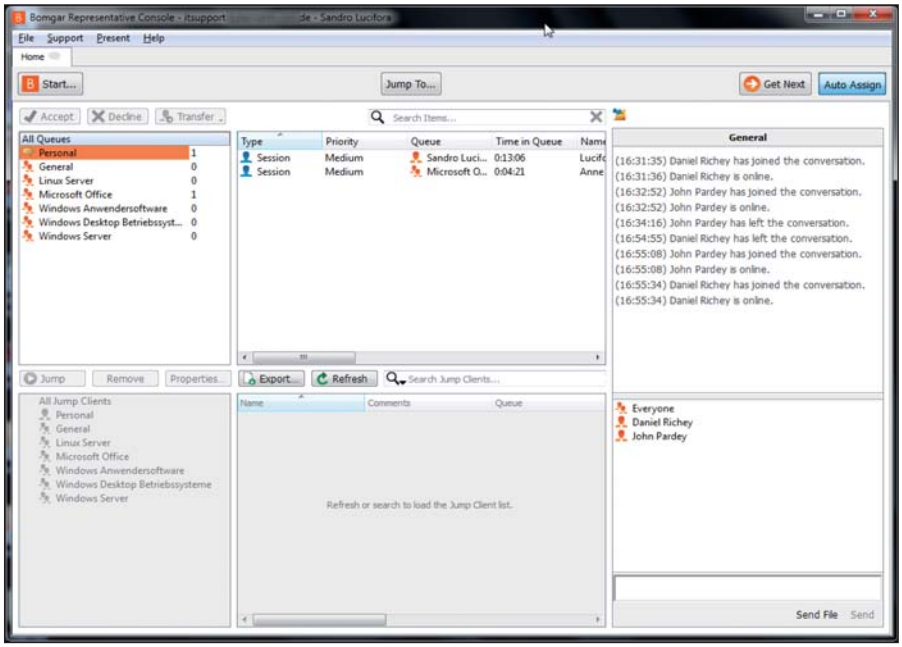


Bild 1: Über die Mitarbeiter-Konsole stellt der Techniker die Verbindung zum Computer des Anwenders her

ein kostenloses Zertifikat über die Zertifizierungsstelle StartSSL [1] aus. Wie Sie sich dieses kostenlose Zertifikat bestellen, lesen Sie in unserem Workshop "Vertrauen ist gut…" [2] in Ausgabe 11/2013.

Danach übermittelten wir den privaten Schlüssel des Zertifikates an Bomgar. Der Hersteller erzeugte daraufhin eine individualisierte und auf den DNS-Namen und das SSL-Zertifikat ausgestellte Version der sogenannten Base-Software. Hierbei handelt es sich um ein Paket, das als Mandant auf der Appliance läuft. Dadurch ließe sich auch Support betreiben über unterschiedliche Domainnamen hinweg und für verschiedene Unternehmen getrennt, aber über dieselbe Bomgar Box. Dazu passt die Möglichkeit, die Oberfläche optisch anzupassen. Nachdem Bomgar die Base-Software erstellt hatte, erhielten wir eine E-Mail und loggten uns über das Webinterface der Box ein. Wir navigierten zum Menüpunkt "Updates" unter dem Reiter "Support", führten eine Prüfung auf Updates durch und installierten die uns angezeigte, nun verfügbare Version. Danach wechselten wir zum Punkt "Security" und "Certificates" und schlossen mit der Einrichtung des SSL-Zertifikates die Installation ab.

Im Rahmen der Konfiguration nahmen wir noch einige Sicherheitseinstellungen vor und bestimmten, über welche IP-Adressen beziehungsweise Netze das Administrationsinterface erreichbar war, richteten einen SMTP Relay-Server ein, um Nachrichten von der Box zu verschicken, und legten die Administrator-E-Mailadressen fest.

Flexible und gruppenbasierte Rechteverwaltung

Jegliche Administration und Einstellungen erfolgen ausschließlich über das Web-basierte Interface. Dazu gibt es drei Zugriffsbereiche: Die Appliance-Administration, in der wir unsere Einstellungen bisher vornahmen, im User-Login, über den wir Benutzer konfigurierten und die personenbezogenen Einstellungen vornahmen, und das Support-Portal. Die gesamte Oberfläche und Texte für Kunden sind nur in Englisch, was daran liegt, dass wir die neueste noch nicht für Deutschland lokalisierte Version testeten. Laut Hersteller soll Bomgar Base 13.1.2 bis zum Erscheinen dieses Artikels komplett in Deutsch verfügbar sein.

Jetzt wechselten wir von der Appliance-Administration in den User-Login und meldeten uns mit dem Administrator-Konto an. Über diese Oberfläche legten wir die "Representatives", also die "Mitarbeiter" beziehungsweise "Supporter", an. Einem so angelegten Benutzer wiesen wir sehr detailliert Rechte zu. Diese fingen an bei reinen Support-Tätigkeiten und reichten bis hin zur Funktion, als Administrator tätig zu sein. Um nicht jedem Mitarbeiter aufs Neue granulare Rechte zuweisen zu müssen, legten wir Benutzergruppen an, in denen wir die Rechte definierten. So unterschieden wir zwischen 1st- und 2nd-Level Support, Team-Leiter und Administratoren und vergaben die für die Aufgaben jeweils notwendigen Rechte. Einem neu angelegten Benutzer wiesen wir dann nur noch die Gruppenrechte zu. Auch nachträgliche Änderungen der Rechte übernahm das System direkt bei jedem einzelnen Anwender.

Fähigkeiten der Supporter abgefragt

Um eine Sitzung zu starten, müssen sich Mitarbeiter und Hilfesuchende über das Appliance-eigene Support-Portal treffen, das sich im Layout an den Unternehmensauftritt anpassen lässt. Benötigt ein Mitarbeiter Remote-Support, so navigiert er mit seinem Browser auf diese Seite und trägt sein Anliegen in ein Formular ein. Dazu beschreibt der Anwender sein Problem, indem er aus einer Liste ein vorgegebenes Problem auswählt. Dahinter steckt ein ausgeklügelter Zuweisungsmechanismus, um die Anfrage an die richtigen Supportmitarbeiter zu leiten.

Um diesen Mechanismus zu testen, legten wir im Administrationsbereich eine Liste persönlicher Fähigkeiten an, die wir Mitarbeitern zuordneten. Wir definierten zum Beispiel die Gruppe Apache mit den Fähigkeiten Installation, Virtual Hosts, PHP und Konfiguration. Ebenso die Gruppe Word mit den Fähigkeiten Serienbrief und Vorlage erstellen. Je nach dem persönlichen Wissensstand gaben wir einem Mitarbeiter den Skill-Level gut, weniger gut oder gar nicht. Nun legten wir die Supportthemen an, zum Beispiel "Microsoft Word, Serienbrief". Diesem Thema wiesen wir den benötigten Skill zu. Gleichzeitig legten wir auch Support-Teams an, im Kontext zu unserem Beispiel das Team "Microsoft Office". Dann wiesen wir diesem Team alle Mitarbeiter zu, die zu dem Thema Hilfe leisten können.

Support-Konsole für Desktop und Mobile

So vorbereitet meldeten wir uns als Mitarbeiter an und erhielten eine entsprechend unseren Rechten zusammengestellte Oberfläche. Um eine Supporttätigkeit durchzu-

führen, luden wir uns einmalig die "Bomgar Representative Console" herunter. Hierbei handelt es sich um eine Desktop-GUI, über die wir jeglichen Support- beziehungsweise Fernwartungs-Auftrag abwickelten. Diese Konsole steht für Windows, Mac OS X und Linux zum Download bereit und ist mit der jeweiligen Appliance beziehungsweise Instanz hart verbunden. Sie ist vorkonfiguriert mit der Support-URL sowie dem SSL-Zertifikat und beinhaltet alle restlichen Konfigurationen, die für den Zugriff auf die Bomgar Box notwendig sind.

Betreibt ein Unternehmen mehrere Instanzen beziehungsweise Mandanten auf einer Appliance, muss der Mitarbeiter für jeden Mandanten eine eigene Konsole herunterladen und lokal installieren. Was den Eindruck einer komplizierten Vorgehensweise erweckt, ist jedoch dem hohen Sicherheitsstandard der Box geschuldet. Nur so ist sichergestellt, dass das manuelle Verändern von Konfigurationsdateien unmöglich ist, und so der unerlaubte Zugriff auf die Remote-Box verhindert. Weiterhin steht für Windows ein Bomgar Display Driver zur Verfügung, der Probleme beim Teilen des Bildschirms lösen soll. Da in unserem Test keine derartigen Schwierigkeiten auftraten, installierten wir den Treiber nicht.

Auch für Android und iOS ließen sich mobile Konsolen-Apps über die jeweiligen Stores herunterladen. Für Samsung-Geräte war eine spezielle Version verfügbar. Wir trugen die Zugriffsadresse und unsere Login-Daten manuell ein. Leider fanden wir keine Option in der App, die Zugangsdaten für verschiedene Mandanten einzutragen. Hier sollte der Hersteller noch nachbessern.

Verschiedene Wege zum Techniker

Um die erste Fernwartungssitzung zu beginnen, starteten wir die Mitarbeiter-Konsole und loggten uns ein. Der Support erfolgt ausschließlich über diese Konsole. Die Oberfläche ist mehrgeteilt und liefert übersichtlich Informationen über die Warteschlange und die eigenen aktiven Sessions.

Im Test standen uns zwei Wege zur Verfügung, einem Anwender Remote-Support zu leisten: Entweder fordert der Anwender diesen direkt über die Portal-Webseite an oder ein Supportmitarbeiter startet die Session aufgrund eines Telefonanrufes. Für die Anforderung öffnet der Anwender die Internetseite der Appliance. Auf dieser Seite fanden sich drei Bereiche. Im oberen Teil waren die in der Mitarbeiter-Konsole angemeldeten Support-Mitarbeiter aufgelistet. In der Appliance-Administration ließ sich konfigurieren, ob diese Liste sichtbar sein sollte. Und in den Mitarbeiter-Einstellungen legten wir auch fest, ob einzelne Mitarbeiter auf dieser Liste sichtbar waren. Klickte der Anwender auf den Mitarbeiternamen, bot die Bomgar Box einen temporären Client zum Download an. Diesen starteten wir, woraufhin sich ein Chatfenster öffnete. In der Mitarbeiter-Konsole erhielten wir die Mitteilung, dass eine Person in der persönlichen Warteschlange wartet.

Bei der durch den Mitarbeiter initiierten Sitzung erhielt der Anwender den Client zum Download, nachdem wir auf der Bomgar-Support-Seite eine zuvor erstellte Session-ID eingetragen hatten. Um diese zu erhalten, generierten wir als Supporter über die Konsole einen Session-Key. Diesen Schlüssel teilt ein Mitarbeiter dem User dann entweder per E-Mail oder telefonisch mit. Nach dem Start des Clients landete die Anfrage ebenso in der persönlichen Warteschlange des Mitarbeiters.

Hat der Kunde noch keinen Ansprechpartner, an den er sich mit seinem Problem wenden kann, nutzt er die dritte Variante: Das Erstellen eines Support-Falls. Und hier kommen auch die von uns zuvor in einer Liste definierten Probleme, die Mitarbeiter-Fähigkeiten und die Support-Teams zum Tragen. Im Test wählten wir als Problem "Word" aus, hinterlegten unseren Namen und forderten Hilfe an. Nun bot uns die Bomgar Box den Kunden-Client zum Download an. Nachdem wir diesen auf der Arbeitsstation gestartet hatten, erhielten alle Support-Mitarbeiter, die wir zuvor dem Team für das Problem "Word" zugeordnet hatten, auf ihrer Konsole einen Hinweis, dass jemand für das Problem "Word" Hilfe anforderte. Die jeweiligen Mitarbeiter bekamen die Option, die Anfrage direkt anzunehmen oder den Kunden in die Warteschleife zu stellen.

Eine weitere Alternative, Support zu erhalten, ist der Bomgar-Button. Hierbei handelt es sich um einen direkten Supportzugang über eine fest eingestellte EXE-Datei. Der Hilfesuchende braucht in dem Fall nur einen Doppelklick auf das Icon durchzuführen, um direkt in der von uns in der Konfiguration festgelegten Warteschlange zu erscheinen. Auch die Gültigkeit des Bomgar Buttons legten wir fest. So wäre es möglich, einen von vornherein befristeten Support zum Beispiel im Rahmen eines Services Level Agreements zu realisieren.

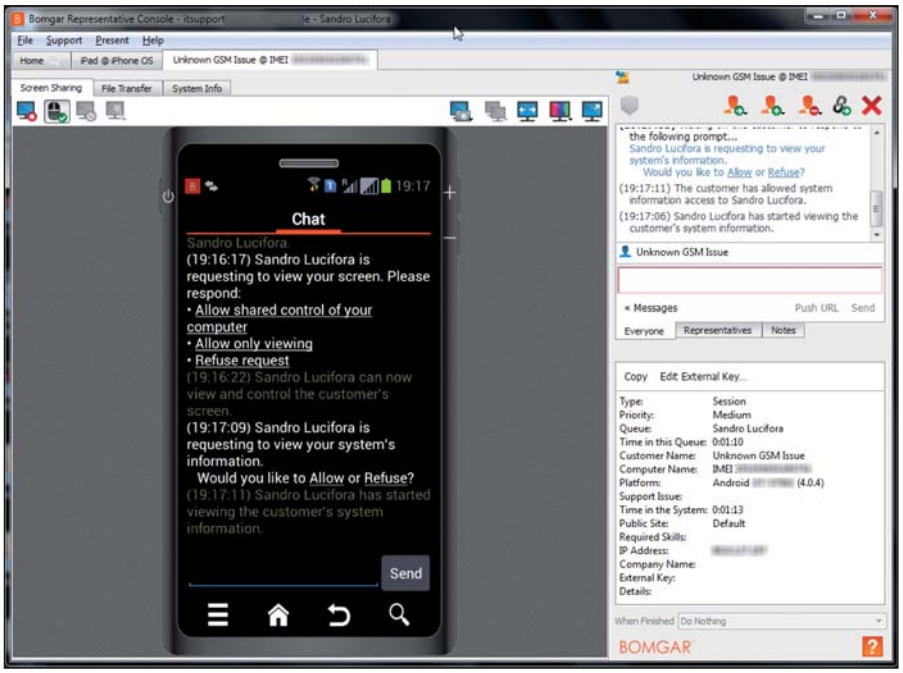


Bild 2: Ob sich mobile Geräte aus der Ferne bedienen lassen, ist vom Betriebssystem abhängig

NACHFOLGE IN GEFAHR?

WWW.DUB.DE

Mit einem Inserat auf DUB.de erreichen Sie bis zu 1,2 Mio. Interessenten – einfach, sicher und schnell.

Service für „IT-Administrator“-Leser

Schalten Sie Ihr Verkaufsangebot auf DUB.de für nur 59 Euro pro Monat. Es fallen keine weiteren Kosten an. Bei einer Buchung profitieren Sie von unserem 3-für-2-Angebot. Hierbei erstatten wir Ihnen den dritten Monat.

„IT-Administrator“-Leser schreiben einfach eine E-Mail mit dem Betreff „IT-Administrator“ an: aktion@dub.de oder rufen an unter 040/46 88 32-660. Wir richten dann Ihren Zugang für Sie ein und senden Ihnen umgehend Ihre Benutzerdaten zu.

DUB
DEUTSCHE UNTERNEHMERBÖRSE
DAS BUSINESS-PORTAL FÜR MITTELSTÄNDLER UND MANAGER

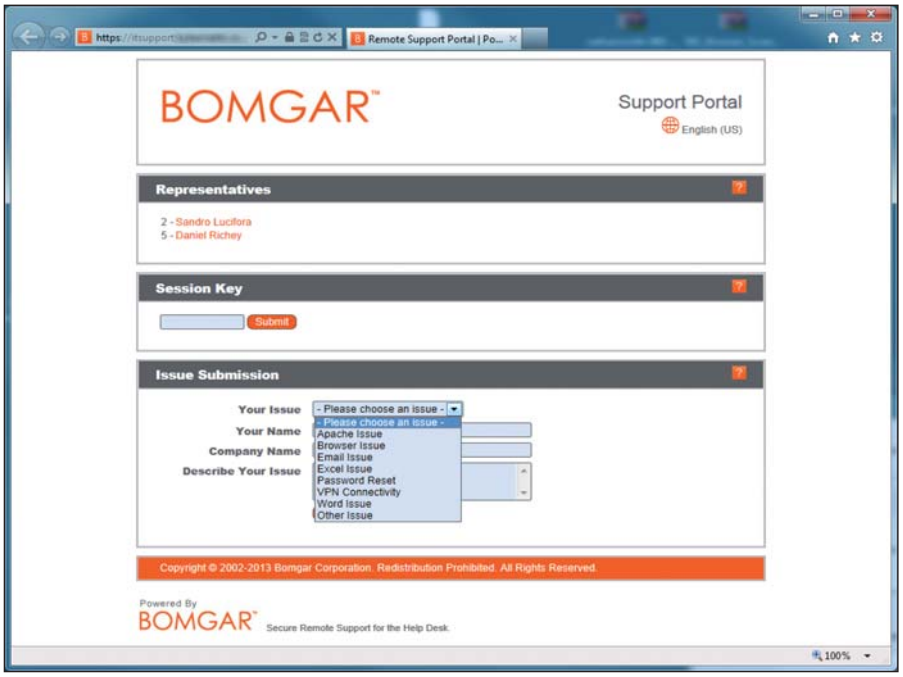


Bild 3: Über das Bomgar Support-Portal fordert der Kunde Hilfe an

Teamwork auf dem Endgerät

Wurde eine Supportsitzung gestartet, sah der Anwender einen Chatdialog mit Informationen über den Status. Wollte der Supporter nun auf den Desktop zugreifen, stellte er über den Client eine Anfrage, über die der Anwender den Zugriff erlaubte und gleichzeitig bestimmte, ob nur die Ansicht oder auch die Bedienung des Computers erlaubt ist. Dies galt auch für den Dateitransfer: Wollte der Supporter auf den Kundencomputer Dateien übertragen, musste der Anwender dieses erst erlauben.

Reichte für den Supportfall die User-Berechtigung nicht aus und der Mitarbeiter benötigte administrative Rechte, konnte dieser die Rechte wahlweise durch die Eingabe eines Benutzernamens und Kennwortes selbst heraufstufen oder der Anwender erhielt eine Dialogbox, in der er die Benutzernamen-Kennwort-Kombination eintrug. So bekam der Techniker keinen Zugriff auf die Zugangsdaten.

Nun kann es sein, dass während der Sitzung ein IT-Kollege assistieren muss. In diesem Fall konnten wir einen weiteren Techniker zu unserer Sitzung bitten – wahlweise einen konkreten Kollegen, einen aus einem bestimmten Team oder jemanden mit konkreten Fähigkeiten. Dies ist notwendig, wenn der Anwender einen Support-Fall zum Beispiel mit dem Bezug auf Word öffnet, sich jedoch herausstellt, dass die Ursache im Betriebssystem zu suchen ist. So konnten wir im Test die Support-Session auch in eine andere Warteschlange verschieben, aus der der nächste Mitarbeiter den Fall übernahm. Benötigten wir für eine Support-Leistung tiefergehende Informationen, wie die laufenden Prozesse, die letzten Events oder Auskunft über die Speichersituation, lieferte uns die in der Konsole integriere System-Info diese Angaben.

Fernwartung von iOS und Android

Neben Windows testeten wir die Mitarbeiter-Konsole sowie den Kunden-Client auf Android- und iOS-Geräten. Bis auf den versteckten Zugriff auf die Kommando-Konsole hatten wir auf den mobilen Geräten dieselbe, aber teilweise nicht so umfangreiche Funktionalität.

Da der Kunden-Client für iOS und Android als App aus dem Store kam und nicht wie unter den Desktop-Systemen bereits alle Zugriffsdaten implementiert hatte, erfolgte die Fernwartung dieser Geräte nicht auf Anforderung durch den Kunden über die Support-Seite, sondern nur mittels individuell generiertem Session Key. Dazu erstellten wir über die Mitarbeiter-Konsole den Schlüssel, den wir zusammen mit der URL der Bomgar Box im Client eintrugen. Nach dem Verbindungsaufbau standen uns die Ansicht, aber nicht die Bedienung des iOS-Gerätes als auch der FileTransfer und die System-Info zur Verfügung. Diese eingeschränkten Funktionen liegen an den Vorgaben von Apple.

Unter Android testeten wir ein Samsung-Smartphone und installierten die speziell für Samsung angebotene Client-App. Auch hier trugen wir die URL und die zuvor erstellte Session-ID ein, bevor wir nicht nur den Bildschirm des Gerätes sahen, sondern auch die Kontrolle übernahmen. Wie

Produkt

Appliance zur Koordinierung und Durchführung von Fernwartung auf PCs und mobilen Endgeräten.

Hersteller

Bomgar Cooperation
www.bomgar.com/de

Preis

Das Einstiegmodel bei Bomgar besteht aus einer B200 Hardware-Einheit und zwei Standard Concurrent-Lizenzen und liegt inklusive Support bei 3.995 Euro. Eine virtuelle Appliance mit zwei Enterprise-Lizenzen kostet inklusive Support 5.950 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator *(max. 10 Punkte)*

Inbetriebnahme	5
Unterstützte Clients	7
Teamarbeit	7
Sicherheitskonzept	8
Protokollierung und Berichte	6

Dieses Produkt eignet sich

optimal für Unternehmen mit hohem Support- und Fernwartungsaufwand für verschiedene Endgeräte an unterschiedlichen Standorten und mit hohen Sicherheitsanforderungen.

teilweise für Unternehmen mit einem mittleren Supportaufkommen, das auch an einem Standort bedient werden kann, jedoch mit erhöhten Sicherheitsanforderungen.

nicht für kleinere Unternehmen mit wenigen Arbeitsplätzen, in denen der Techniker vor Ort ist.

Bomgar Box 13.1.2

von der Arbeit auf dem Desktop-Rechner bekannt, musste der Anwender jeglicher Zugriffsaktion zustimmen. Neben dem Screen-Sharing standen uns unter Android auch der Datei-Transfer auf das Gerät und dessen Systeminformationen zur Verfügung. Grundsätzlich hängen die möglichen Funktionalitäten in einer Sitzung vom administrierten Gerät ab.

Zugriff auf unbeaufsichtigte Rechner

Das Einsatzgebiet der Bomgar Box ist nicht nur auf persönliche Supportleistung gegenüber Anwendern beschränkt, sondern lässt sich auch mittels Jump-Technologie auf unbeaufsichtigten Geräten ausführen. Dazu standen die Jumpoints und die Jump-Clients zur Verfügung. Der Jumpoint stellt eine Art Eingangstüre für das Remote-Netzwerk dar. Wir installierten den Jumpoint-Agent an einem beliebigen Punkt im Netzwerk und erhielten darüber später unbeaufsichtigten Zugriff auf jeden PC in diesem Netzwerk, auf dem wir einen Jumpoint-Client installiert hatten. In den Einstellungen legten wir auch fest, ob der Zugriff auf den Jumpoint über die Shell und SSH erfolgte. Bei den Clients hinterlegten wir, welcher Support-Mitarbeiter sich mit diesen verbinden durfte. Die Installation und Einrichtung war gegenüber den gängigen Fernwartungslösungen aufwändiger, stellte so jedoch ein hohes Maß an Sicherheit dar.

Fazit

Die Bomgar Box ist durch das zentrale Management und die individuelle Standortwahl eine sehr sichere Lösung, um Anwendern Hilfestellung aus der Ferne zu bieten sowie auf unbeaufsichtigte Rechner zuzugreifen. Das Konzept richtet sich an große Unternehmen mit einem hohen Fernwartungsaufkommen und verschiedenen Support-Mitarbeitern sowie Anbieter von Supportleistungen für verschiedene Kunden. Für kleinere und mittelständische Unternehmen sehen wir die Box als zu umfangreich an.

Funktional hat uns der Sicherheitsaspekt überzeugt. Das gilt auch für die Arbeit in Teams und die Möglichkeit, dass mehrere Supporter und Techniker zeitgleich zusammen an ein und demselben Client arbeiten. Der Einsatz der Mitarbeiter-Konsolen ermöglicht es zudem, Wissen aus dem gesamten Unternehmen über ein und dasselbe System für einen Supportfall zu bündeln. Für den Anwender ist es irrelevant, für welches Endgerät er Hilfestellung benötigt, der Weg zum Techniker-Team ist immer derselbe. Lediglich die Tatsache, dass es nur einen Chat zur Verständigung zwischen Anwender und Mitarbeiter gibt und wir keine Gespräche über das System führen konnten, sehen wir als Punkt zur kurzfristigen Nachbesserung und auch die Installation mit SSL-Zertifikaten erweist sich in kleineren Umgebungen als eher komplex. Ansonsten haben uns das Konzept, die Umsetzung und die Möglichkeiten überzeugt. *(dr)*

[1] StartSSL
D9P51

[2] Workshop "Vertrauen ist gut…"
in IT-Administrator 11/2013, ab Seite 46

Link-Codes

Im Test: EgoSecure Endpoint 5.4

Rundumschutz

von Sandro Lucifora

Datenverluste entstehen nicht nur durch vorsätzlichen Diebstahl. Oft ist der fahrlässige Umgang mit Daten durch Anwender Schuld: Laptops bleiben im Taxi liegen, USB-Sticks rutschen aus der Tasche, virenverseuchte Datenträger gelangen ins Unternehmen oder sensible Dateien wandern unverschlüsselt in die Cloud. Um Unternehmen vor den meist weitreichenden Folgen zu schützen, bietet EgoSecure mit Endpoint einen Endgeräte-Schutz an. Die von uns getestete Version 5.4 musste beweisen, wie sie Datenverlust vorbeugt.

Mit Endpoint hat EgoSecure eine Kombination von vier Modulen im Programm, die über ihre Bereiche hinweg die Daten schützen sollen. Dabei steht beim sogenannten "C.A.F.E.-Management Prinzip" je ein Buchstabe für einen Bereich. Das "C" für Control definiert, welcher Benutzer welche Datenwege benutzen darf. Damit haben nur die Mitarbeiter Zugriff auf sensible Daten, die diese auch für ihre Arbeit benötigen.

Mit dem "A" für Audit protokolliert Endpoint Verstöße gegen die Vorgaben und Bestimmungen. Dadurch sollen Mitarbeiter bewusster mit den Daten umgehen und nur innerhalb der Vorgaben arbeiten. Mit dem "F" für Filter separiert EgoSecure kritische von unkritischen Datentypen. Das heißt Dateien, die im Unternehmen nichts verloren haben, blockiert die Software und verhindert damit das ungewollte und unerlaubte Speichern. Der letzte Buchstabe "E" steht für Encrypt und verschlüsselt die Daten auf externen Datenspeichern, inklusive der Cloud.

Für kleine Umgebungen ohne Server möglich

Was sich in der Theorie einfach anhört, muss technisch so umgesetzt sein, dass es den Arbeitsfluss nicht stört. So besteht EgoSecure Endpoint aus lediglich zwei Programmodulen und benötigt keinen Windows-Server – besonders für kleinere Umgebungen ist dies interessant. Die EgoSecure Agents laufen unabhängig auf den Clients und der Administrator nimmt die Rechteverwaltung über die Managementkonsole vor. Die vorgenommenen Änderungen sendet das System an die Agenten, sodass die Rechteanpassungen sofort greifen. Dabei gefiel uns im Test sehr gut, dass dazu weder eine Aktion des Users noch ein Rechnerneustart notwendig war.

Der "EgoSecure Endpoint Server" läuft auf einem beliebigen Rechner im Netzwerk, egal ob physikalisch oder virtuell, und besteht aus der Management-Konsole, dem Verteildienst und einer Datenbank. In Letzterer speichert die Lösung die vorhandene Verzeichnisdienst-Struktur sowie alle Einstellungen ab. Dazu zieht das System die Informationen aus Domänen oder Workgroups, unterstützt das eDirectory von Novell und das LDAP-Protokoll. Alle Datensätze speichert die Software in einer SQL-Datenbank und unterstützt dabei MSDE, MS SQL Server Express und MS SQL Server ab 2000 bis 2012. Zudem arbeitet die Software über einen ODBC-Treiber mit MySQL ab Version 5 zusammen.

Der Endpoint-Server muss für die Agenten nur erreichbar sein, sofern ein Update der Rechte ansteht. Ansonsten arbeiten sie unabhängig und benötigen weder Zugriff zum lokalen Netzwerk noch zum Endpoint-Server. In unserem Test installierten wir die Serverkomponente auf Windows 2008 R2 in einer Active Directory-Domäne. Bei einem Einsatz von bis zu fünf Clients ist auch die Installation auf einem Arbeitsplatzrechner möglich. Ohne vorhandenen Verzeichnisdienst

Server physikalisch oder virtuell

- Betriebssysteme (32 oder 64 Bit): Windows Server 2003, 2008, 2012 (R2); Windows XP, Vista, 7, 8
- LDAP-Verzeichnisse: Active Directory; Novell eDirectory 4.91 SP2 und höher; LDAP / open LDAP (oLDAP); eigenes Directory / Microsoft Workgroup
- Datenbankserver: SQL Server 2000 SP3a, 2005, 2008, 2012; SQL Server 2005/2008/2012 Express Edition; MSDE
- Arbeitsspeicher: 512 MByte
- Verfügbarer Festplattenspeicher: 100 MByte

Systemvoraussetzungen für Clients

- Betriebssysteme (32 oder 64 Bit): Windows XP (SP2, SP3); Windows Vista (SP1); Windows 7 und 8; Citrix XenApp ab Version 6; Citrix XenDesktop ab Version 5
- Arbeitsspeicher: 512 MByte
- Verfügbarer Festplattenspeicher: 50 MByte

Systemvoraussetzungen

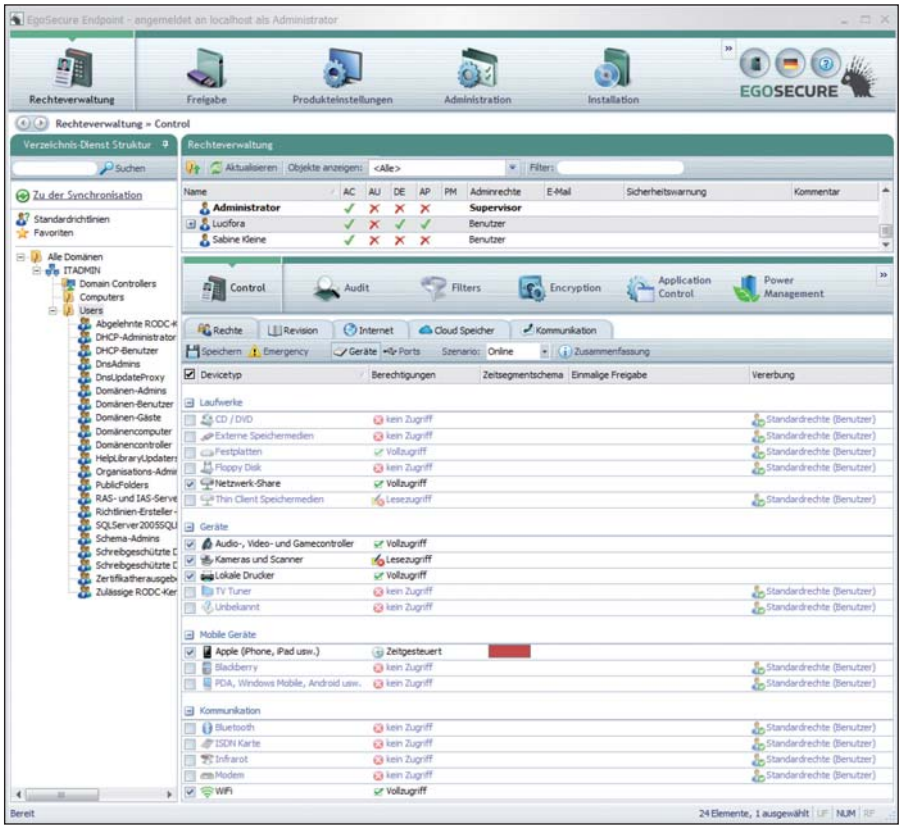


Bild 1: Über eine klar strukturierte GUI lassen sich die Rechte vergeben – sowohl für Nutzer als auch für Geräte

greift EgoSecure auf die eigene, integrierte Benutzerverwaltung zurück.

Für die Installation benötigten wir lediglich einen Benutzer mit Leserechten auf das AD als auch einen User mit Berechtigung zum Erstellen von Datenbanken. Da auf unserem System kein SQL Server lief, installierten wir vor der Endpoint-Software einen MS SQL-Server Express 2012. Dabei benötigten wir die Edition mit Advanced Services, da EgoSecure diese Dienste voraussetzt. Wir fuhren mit der Installation von Endpoint 5.4 fort, indem wir während des Setups die Ports für die Verbindung zwischen Server und Client festlegten und unseren Verzeichnisdienst bestimmten. Weiter gaben wir die Anmeldedaten für das AD sowie den SQL-Server ein. Nach einer kurzen Installationsphase stand uns die Management-Konsole für eine erste Konfiguration zur Verfügung.

Unterscheidung zwischen Benutzer- und Geräterechten

Bevor wir die Agenten auf den Clients installierten, legten wir die Standardrechte für alle User und Rechner fest. Denn diese Rechte erhalten die neu eingelesenen Geräte und Benutzer, sofern für sie keine spezielle Rechtevergabe erfolgt. Wir verboten den Geräten und Nutzern so die Zugriffe auf externe Medien wie CDs, DVDs und USB-Sticks sowie die Verbindung zu mobilen Geräten via Bluetooth, Infrarot, Modem und WiFi. Damit stellten wir zunächst sicher, dass keine Daten unkontrolliert das Unternehmen verlassen. Ebenso riegelten wir alle Datenwege für unbekannte Benutzer ab. Dabei handelt es sich um Anwender, die sich auf den Arbeitsplätzen anmelden und nicht im AD vorhanden sind. Das sind in unserem Fall die am Rechner eingerichteten lokalen Anwender.

Vor dem ersten Import konfigurierten wir die AD-Synchronisation und legten fest, wie sich die Software beim Import neuer Objekte verhalten sollte. Wir bestimmten, dass der Import nur aktive Benutzer berücksichtigte, nicht mehr vorhandene Objekte löschte und gaben an, welche Module für neue User aktiviert waren. Ebenso trugen wir bei Bedarf von der Synchronisation auszunehmende Objekte ein. Dabei konnte es sich um eine gesamte Organisation oder auch Gruppen handeln. Die Synchronisierung arbeitet im reinen Pull-Verfahren, sodass EgoSecure keine Daten in das Active Directory schreibt. Der Datenabgleich mit dem Verzeichnisdienst erfolgt dazu entweder manuell oder automatisch per Scheduler. Gut ist, dass die Software bei Bedarf auch Daten mehrerer Domänen importiert.

Granulare Gruppenrechte

Darauf aufbauend erstellten wir Gruppen mit modifizierten Rechten. Wir machten uns dazu die Vererbung der Rechte bei EgoSecure Endpoint zunutze. Nach dem Import der Gruppeneinstellungen und Userzuordnungen im AD legten wir die Rechte für Gruppen und einzelne Benutzer fest. Ist auf einem Client bereits ein Agent installiert, verteilt die Serverkomponente die vorgenommenen Änderungen direkt an die Agenten, sodass die neuen Rechte quasi in Echtzeit auf den Arbeitsplätzen zur Verfügung stehen. Die möglichen Rechteeinstellungen unterteilten wir grob in die Gruppen "Laufwerke", "Geräte", "Mobile Geräte" und "Kommunikation" und deckten zusätzlich alle Schnittstellen ab, die es an den Geräten gab, inklusive LPT, COM und virtueller Medien. Als Rechte wählten wir je nach Gerät, ob Anwender darauf Vollzugriff, Lesezugriff, keinen Zugriff oder zeitgesteuert eingeschränkten Zugriff erhielten. Wir konnten Geräte auch komplett aus der Rechteverwaltung ausnehmen.

Im Test stellten wir ferner sicher, dass an keinem Rechner externe Medien wie USB-Sticks oder SD-Karten lesbar waren. Eine Gruppe von Anwendern musste jedoch weiterhin von ausgewählten Medien Daten einlesen dürfen, sodass wir der ausgewählten Gruppe lediglich Leserechte für CDs zuwiesen. Dann machten wir uns die gezielte Hardwarefreigabe und den Contentfilter zunutze. Wir gaben nur die USB-Sticks und SD-Karten von bestimmten Herstellen und Modellen frei.

Zusätzlich erlaubten wir von diesen Medien nur das Kopieren von Bilddaten in das lokale Netzwerk. Dabei prüft EgoSecure nicht nur die Endung der Datei, sondern analysiert auch die Binärdaten. Damit ist es nicht möglich, in JPG umbenannte EXE-Dateien ins Netzwerk einzuschleusen. Zusätzlich kontrollierten wir auch die Datenwege ins Internet und verboten das

Das ist neu in Version 5.4

Mit dem Release der Version 5.4 hat EgoSecure vor allem die Unterstützung von Cloudspeichern erweitert. So hat der Hersteller die Kontrolle der Cloudspeicher um weitere Anbieter ergänzt und erlaubt, auch die Contentheader-Filterung auf Cloudspeicher anzuwenden. Das Logging berücksichtigt nun auch Cloudzugriffe. Bei der Verschlüsselung schützt Endpoint 5.4 jetzt auch Dateien, die der Anwender auf ein Internet-Laufwerk speichert, verschlüsselt ganze Ordner und unterstützt auch die dateibasierte Verschlüsselung für Android.

Herunterladen von Dateien über den Internet Explorer und Firefox. Da diese Einstellung auf Prozessebene abläuft und nicht als Plug-In, sind die fortwährenden Browser-Updates kein Problem. Leider griff die Beschränkung nicht bei Google Chrome.

Grundsätzlich spielte es keine Rolle, an welchem Endgerät sich der Benutzer später anmeldete, da die Agenten die Rechte auf Benutzerebene überwachen. Daher konnten wir zwar an jedem Gerät zum Beispiel den Zugriff auf die externen Medien untersagen, doch mit der Anmeldung eines berechtigten Benutzers diese Einschränkung durch die Userrechte explizit aufheben beziehungsweise anpassen. Sehr gut gefallen hat uns, dass der Agent eine Funktion zum Ummelden von Usern bereitstellt. Das ist gerade für Administratoren sehr hilfreich, die im Rahmen einer Supportleistung zum Beispiel auf einen USB-Stick zugreifen müssen und sich dazu nur im Agent ummelden und nicht den Windows-Benutzer wechseln müssen.

Cloud-Sicherheit mit Verbesserungspotenzial

Wenn das Herausschleusen von Daten über externe Medien nicht mehr funktioniert, greifen Mitarbeiter gerne auf Storage im Internet zurück. Hier hat Endpoint 5.4 aufgerüstet und unterbindet den Zugriff auf die Cloud-Speicher zumindest rudimentär. Dabei berücksichtigt der Hersteller jedoch nur die in den USA verbreiteten Systeme wie Box Sync, Dropbox, Google Drive, SkyDrive und andere. Im Test hatten wir keine Möglichkeit, eigene Cloud-Speicher wie HiDrive oder Amazon hinzuzufügen. Auf Nachfrage bestätigte der Hersteller jedoch, dass er die Liste der Cloud-Speicher auf Kundenanfrage erweitert. Dadurch, dass diese aber so lückenhaft ist, bietet diese Funktionen derzeit nur einen eingeschränkten Schutz.

Zusätzlich hatten wir die Möglichkeit, den Datentransfer über Skype zu unterbinden. Weitere Funktionen sollen in diesem Bereich hinzukommen. Gänzlich vermisst haben wir die Möglichkeit, den Datenupload via FTP zu kontrollieren. Zwar ist dies über eine Firewall-Regel machbar, die Port 25 blockiert, doch ist die Rechtekontrolle dazu bei Endpoint deutlich besser aufgehoben.

Einfache Erweiterung der Rechte

Nachdem wir im System die grundlegenden Rechte eingestellt hatten, verteilten wir die Agenten. Dies erfolgt entweder über die Management-Konsole, manuell über eine Setup-Datei oder via Softwareverteilung auf Basis des mitgelieferten MSI-Paketes. Wir testeten die Installationswege sowohl auf einer Windows 7- als auch Windows 8-Workstation. Anschließend meldeten sich die Agenten automatisch am Server an, holten sich die Rechte ab und setzen diese lokal um. Wir sahen danach in der Taskleiste das Symbol des Agenten und ließen uns über das Kontextmenü die definierten Rechte anzeigen. So erhalten Anwender einen Überblick über ihre Möglichkeiten.

Sobald wir eine unerlaubte Aktion ausführen wollten, erhielten wir einen entsprechenden Hinweis durch den Agenten. Daraufhin dürfte es nicht selten vorkommen, dass Benutzer Rechteanpassungen wünschen. In diesem Fall bestünde der Workflow darin, dass sich der User beim Administrator telefonisch oder per E-Mail meldet und um Erweiterung der Rechte bittet. Um diesen Prozess zu verkürzen, gibt es im Agenten die Funktion "Zugriffsrechte beantragen". Der Benutzer füllt dazu ein Formular aus, in dem er das Gerät, den gewünschten Zugriff sowie eine kurze Begründung hinterlegt und diese Anfrage absendet. Der Administrator erhält diesen Request, kann ihn bearbeiten und die Rechte vergeben.

Praktische Rechtevergabe unterwegs

Anwender, die keine Anbindung zum EgoSecure-Server haben, erstellen auf demselben Wege eine Anfrage, übermitteln diese dem Administrator, der daraufhin wiederum eine Freigabe erstellt. Doch fehlt dem Gerät nun zum Empfangen der Änderungen die Verbindung zum Server. Daher stellt die Management-Konsole einen analogen Freischaltcode bereit. Diesen trägt der Anwender dann im Agenten ein. Die damit erteilten Rechte sind grundsätzlich zeitlich oder bis zum nächsten Login limitiert und ein Vollzugriff lässt sich so nicht gewähren.

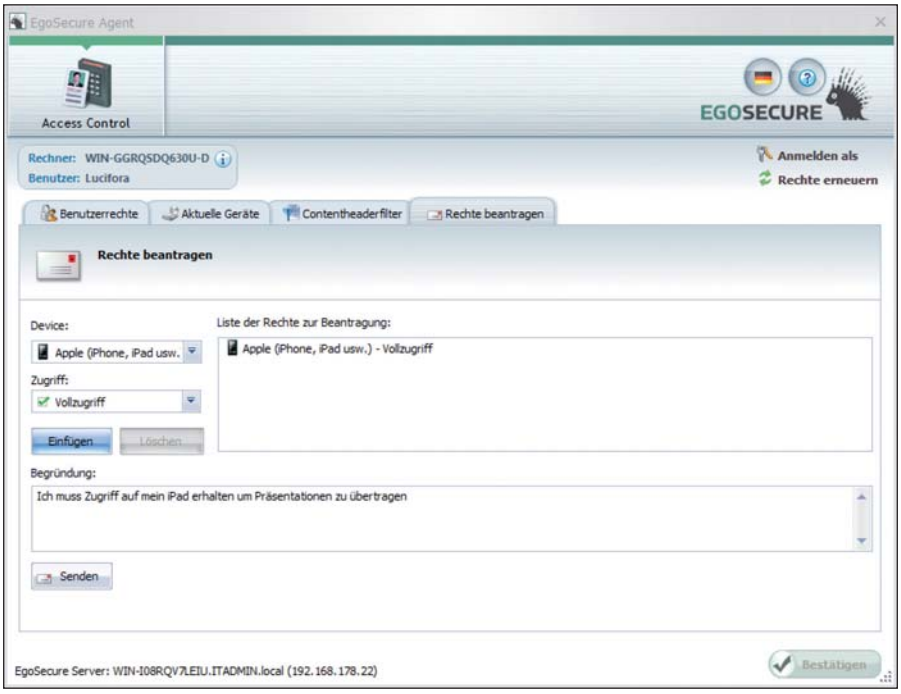


Bild 2: Über das integrierte Workflow-System beantragt der User Rechteänderungen beim Administrator

Da die Rechte bei der Arbeit im lokalen Netzwerk meist andere sind als die für Geräte, die sich außer Haus befinden, unterscheidet die Software zudem zwischen Online- und Offline-Rechten. Damit ist es zum Beispiel möglich, die Netzwerkanbindung über LAN und WLAN zu reglementieren, sollte sich das Gerät außerhalb des Firmennetzwerkes befinden.

Schließlich setzten wir bei der Gruppe der Administratoren eine Kombination aus Zugriffs- und Contentfilter ein, um diesem Personenkreis zum Beispiel den Zugriff auf vertrauliche Dateien zu verweigern. Denn hin und wieder reichen auch Administratoren interne Daten weiter. Damit ein IT-Verantwortlicher sich nicht selbst diese Rechte einräumt, legten wir fest, dass ein Administrator seine Rechte nur im Vier-Augen-Prinzip verwalten durfte.

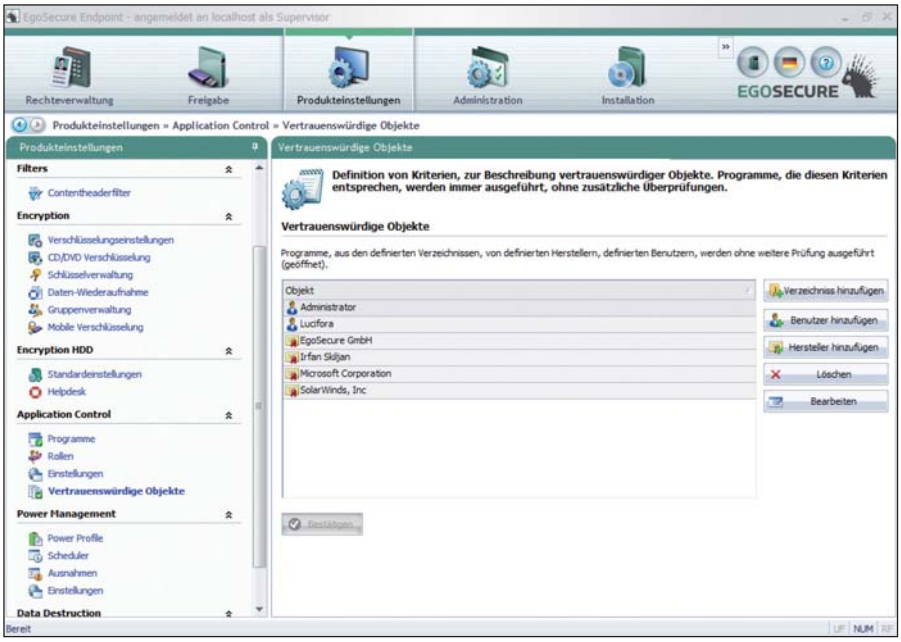


Bild 3: In der Whitelist der Applikationskontrolle definierten wir die vertrauenswürdigen Objekte

Programmsperre per White- und Blacklist

Nicht selten installieren Mitarbeiter eigene Software auf ihren Computern oder führen Programme aus, die keine Installation benötigen. Hat ein Benutzer, absichtlich oder ungewollt, eine ausführbare Programmdatei ins Unternehmen eingeschleust, verhindert "Application Control" den Start. Die Anwendungszugriffssteuerung erfolgt dazu nach dem Black- oder Whitelist-Verfahren. Dazu erstellt Application Control vorab für das Programm einen Hashwert und prüft diesen vor der Ausführung auf dem Client. Somit erhält der Benutzer immer dieselben Programmzugriffsrechte an sämtlichen Rechnern. Aufgrund des Hashwertes ist zudem der Dateiname irrelevant, weshalb Anwender

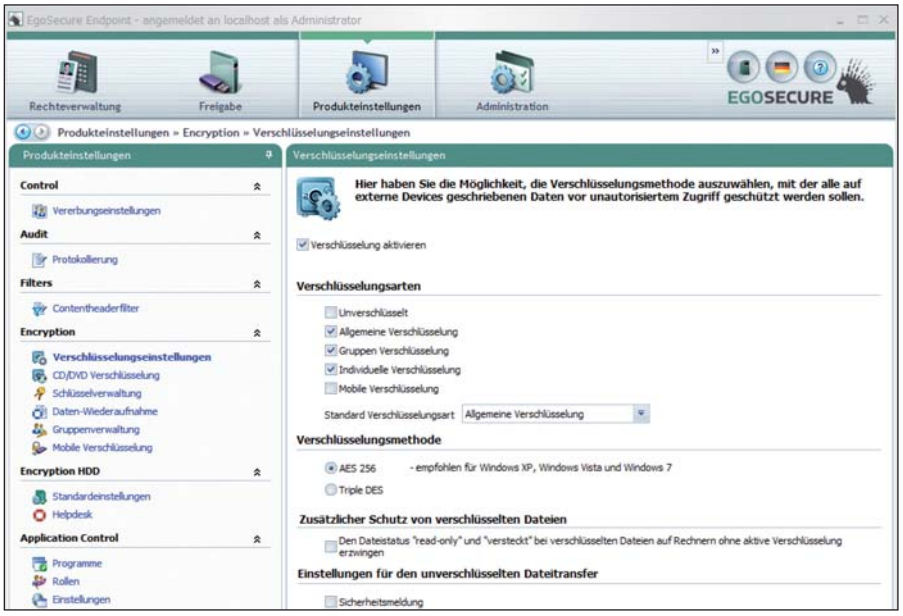


Bild 4: Für die Verschlüsselung von Dateien stehen AES und Triple-DES zur Verfügung

auch nicht durch Umbenennen Zugriff auf nicht erlaubte Programme erhalten.

Wir legten in den Produkteinstellungen sogenannte vertrauenswürdige Objekte und Hersteller an. Im Test durften die Benutzer unter anderem jede Software von Microsoft starten. Zudem erlaubten wir grundsätzlich den Start von Software, die der Administrator installierte. Als Drittes vertrauten wir jeder Software, die der Anwender über den lokalen Programmordner ("ProgramFiles") startete. Da dieses Vorgehen nur eine Basis darstellt, erleichtert der Lernmodus weitere Freigaben. Dabei führt der Benutzer auf dem Client seine Programme wie gewohnt aus. Anschließend erhält der Administrator eine Liste und gibt einzelne Applikationen frei.

Flexible Datenverschlüsselung

Mit dem Modul zur Verschlüsselung lassen sich Dateien auf externen Speichermedien vor unberechtigten Zugriffen schützen. Dabei war es im Test egal, ob wir Daten auf einen USB-Stick, eine SD-Karte oder eine externe Festplatte kopierten. Bei eingeschalteter Encryption-Funktion verschlüsselte Endpoint die Daten dateibasiert. Die Entschlüsselung erfolgte wiederum nur über einen Rechner mit dem EgoSecure-Agenten des Unternehmens. Für Daten, die der Anwender auf einem anderen Computer ohne Agenten entpacken will, bietet EgoSecure die "ToGo-Version" an. Dabei speichert das System eine EXE-Datei mit auf den Datenträger, über die der Nutzer die verschlüsselten Dateien nach Eingabe eines Kennwortes auf anderen Windows-Rechnern entschlüsseln kann. Neu in der Version 5.4 ist dabei, dass die Verschlüsselung auch auf Cloud-basierten Speichern funktioniert. Damit haben wir Daten zum Beispiel in Dropbox abgelegt, die nur über unseren EgoSecure-Agenten oder die ToGo-Variante zu entschlüsseln waren.

Welche Art der Verschlüsselung möglich ist und ob Benutzer auch eine ToGo-Version verwenden dürfen, steuerten wir über die Management-Konsole. Hier legten wir zudem fest, ob die Verschlüsselung nur dateibasiert arbeiten oder auch ganze Ordner oder das gesamte Speichermedium verschlüsseln sollte. Sobald wir mehrere Optionen zuließen, stand dem Anwender diese Auswahl zur Verfügung.

Mobile Device Management nur mit Einschränkungen

Jedoch gehören nicht nur Desktop- und Laptop-Computer zum IT-Inventar – auch Smartphones und Tablets sind längst zur Standard-Ausstattung geworden. Um auch hier die Hoheit über die Unternehmensdaten zu behalten, installierten wir das Mobile Device Management als Zusatzmodul zu EgoSecure Endpoint. Nach der Installation sahen wir einen zusätzlichen Menüpunkt, über den wir den EgoSecure MDM-Server einrichteten. Während der Installation hinterlegten wir einen Port, den wir über die Unternehmes-Firewall beziehungsweise den Router auf unseren Server weiterleiteten. Das ist notwendig, damit die Geräte über das Internet eine Verbindung zu EgeSecure Endpoint aufbauen können.

Wir inventarisierten zunächst ein Android-Smartphone und ein iPad. Für Android bietet EgoSecure eine App an, über die die Anmeldung erfolgt. Mit dem iPad griffen wir dagegen auf eine SSL-verschlüsselte Internetseite unseres MDM zu, loggten uns mit unseren Benutzerdaten ein, wonach Endpoint auch das Apple-Gerät auflistete. Die Fernkonfiguration der iOS-Geräte erfolgt über die Apple-Komponente – also

Produkt
Software zur Absicherung von Endpoint-Rechnern und -Geräten.

Hersteller
EgoSecure GmbH
www.egosecure.de

Preis
EgoSecure Endpoint ist bis fünf Lizenzen kostenfrei, danach fallen zehn Euro pro Lizenz und Modul an. So kostet der Basisschutz zehn Euro pro Lizenz, der Standardschutz 36 Euro pro Lizenz und der erweiterte Schutz 64 Euro je Lizenz.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator *(max. 10 Punkte)*

Rechtevergabe	7
Handhabung des Agenten	6
Verwaltung mobiler Geräte	5
Verschlüsselung von Daten	7
Protokollierung	7

Dieses Produkt eignet sich

optimal für Umgebungen mit einem AD- oder LDAP-Server sowie Windows-Arbeitsplätzen.

teilweise für Umgebungen ohne zentrale Benutzerverwaltung wie AD oder LDAP.

nicht für Einzelplätze und Stand-Alone-Geräte.

EgoSecure Endpoint 5.4

über die Funktionen, die Apple über die eigenen Dienste zur Verfügung stellt. Für die Kommunikation zwischen Endpoint-Server, Apple und dem Gerät ist regulär ein eigenes Zertifikat notwendig. Da die Beantragung und Installation sehr aufwändig ist, stellt EgoSecure deren eigenes Zertifikat zur Verfügung. Das erspart viel Zeit und Mühe bei der Installation.

Auf dem Android-Gerät richteten wir die Datenverschlüsselung der microSD-Karte ein und starteten dazu die App. Wir wechselten in den Dateimanager und wählten eine der zur Verfügung stehenden Optionen aus. Dabei glich sich die App mit den auf dem Server liegenden Schlüsseln ab, sodass wir die verschlüsselten Daten später auch auf einem beliebigen Rechner mit EgoSecure-Agent in unserem Netzwerk weiterverarbeiteten. Die Kontrollmöglichkeiten bei iOS-Geräten sind hingegen begrenzt, da sich Apple sehr restriktiv bei der Remote-Steuerung seiner Geräte zeigt. BlackBerry unterstützt EgoSecure gar nicht. Die Verwaltung von Windows Phone soll Ende 2013 verfügbar sein.

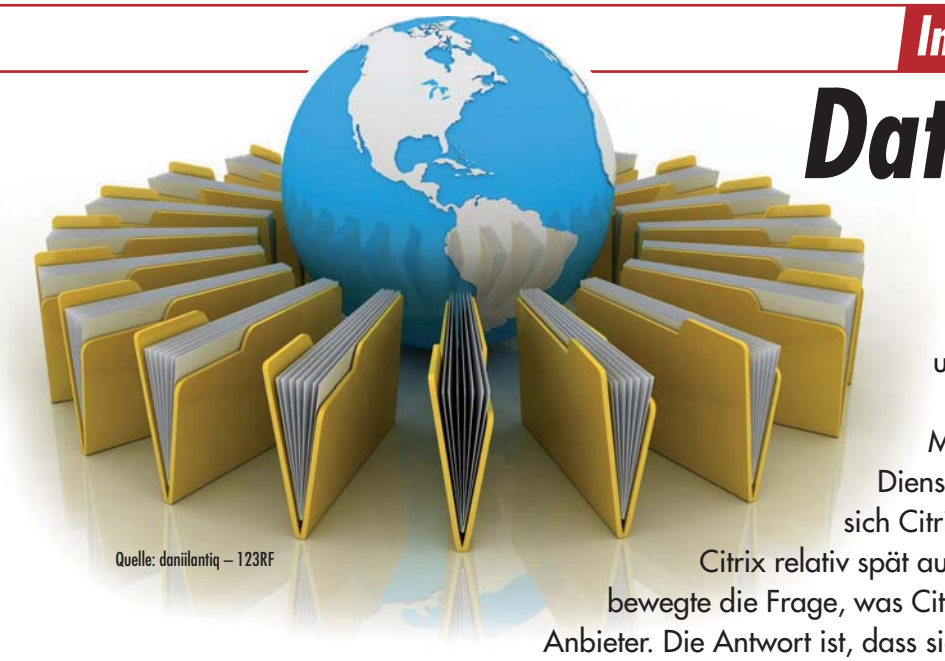
Protokollierung mit Vier-Augen-Prinzip

Sollten doch einmal Daten verlorengehen, ist es wichtig nachzuvollziehen, wer dafür verantwortlich ist. Dazu gibt es das Modul "Audit", das die Protokollierung jeglicher Aktionen inklusive Netzwerkzugriffe durchführt. Das Ziel ist, die Benutzer für das verlustfreie Arbeiten mit den Daten zu sensibilisieren. Die Protokollierung erfolgt datenschutzkonform in Bezug auf den Betriebsrat und das Bundesdatenschutzgesetz und hält sich an die Richtlinien des BSI: Die Protokolle sind grundsätzlich nur anonymisiert einzusehen. Stellt der Administrator einen Verstoß fest, kann er nur mit Zustimmung des Betriebsrats weitere Details anzeigen lassen. Dabei gilt das Vier-Augen-Prinzip über die Abfrage mehrerer Passwörter.

Über die Protokolle sahen wir im Test unter anderem, wann Zugriffe auf welche Medien durch welchen Benutzer erfolgten und erkannten zum Beispiel, wer welche Datei über Outlook versendete. Im Supportfall half uns die Übersicht nachzuvollziehen, warum etwa ein Netzwerkzugriff nicht möglich war. Wir sahen, ob in dem Fall das Betriebssystem oder doch der Contentfilter den Zugriff verweigerte. Bei kritischen, unerlaubten Zugriffen ließen wir uns außerdem per E-Mail informieren. So erfahren Administratoren oder die Geschäftsleitung direkt, wenn unerlaubt versucht werden sollte, Unternehmensdaten herauszusenden oder auf andere Medien zu kopieren.

Fazit

Insgesamt hat uns die Anwendung und Bedienung der Managementkonsole sehr gut gefallen. Nur bei der Absicherung des Cloud-Traffics darf sich EgoSecure noch flexibler zeigen. Die Möglichkeiten zur Rechteverwaltung lassen fast keine Wünsche offen. Das Ändern der Rechte erfolgte ohne Neustart der Clients und sogar ein Workflow zur Anforderung weiterer Rechte im Agenten ist integriert. Dies lässt die Akzeptanz der Software sowohl bei Administratoren als auch Anwendern steigen. Die Datenschutz-konforme Protokollierung rundet das Gesamtpaket ab. *(dr)*



Quelle: daniilantiq – 123RF

Im Kurztest: Citrix ShareFile

Daten weltweit

von Sandro Lucifora

Mitarbeiter wollen zunehmend mit unterschiedlichen Geräten von verschiedenen Orten auf Unternehmensdaten zugreifen. Meist bleibt hier nur die Wahl, einen Cloud-Dienst zu mieten oder selbst zu betreiben – oder sich Citrix ShareFile anzuschauen. Mit ShareFile ist Citrix relativ spät auf den europäischen Markt gekommen. Uns bewegte die Frage, was Citrix anders macht als die etablierten Cloud-Anbieter. Die Antwort ist, dass sich Citrix voll und ganz auf den Einsatz der Lösung im Unternehmensumfeld konzentriert. Ob die Funktionen diesem Anspruch gerecht werden, zeigt unser Kurztest.

Citrix beschreibt ShareFile als einen Cloud-basierten Dateifreigabedienst, mit dem Benutzer einfach und sicher Dateien austauschen können. Das ist grundsätzlich keine besondere Aussage, wenn der Fokus nicht auf dem Begriff "sicher" liegt. Denn der Unterschied zu allen anderen Angeboten liegt darin, dass ShareFile Speicherplatz wahlweise auf den europäischen Servern von Citrix oder lokal im eigenen Unternehmen nutzt. Dabei speichert der Dienst die Daten physikalisch auf den eigenen, privaten Festplattenspeichern ab, was Citrix "ShareFile StorageZones" nennt. Durch den Einsatz einer StorageZone behält der Kunde die Daten immer unter eigener Kontrolle und genießt gleichzeitig die Vorteile eines öffentlich gehosteten Cloud-Dienstes.

Einfache Inbetriebnahme

Zu ShareFile bietet der Hersteller vier Lizenz-Pakete von Basic bis Enterprise, die sich in der Anzahl der Mitarbeiter-Accounts, der Größe des Datenspeichers und des Datentransfers unterscheiden. Doch lediglich das Paket "Enterprise" beinhaltet auch StorageZones und die Benutzerverwaltung über das Active Directory des eigenen Unternehmens.

Nach der Anmeldung erhielten wir die notwendigen Zugangsdaten und eine eigene URL für den zukünftigen Webzugriff in Form von *http://alias.sharefile.eu*, wobei wir den Alias im Administrations-Menü nachträglich frei änderten. Nach dem Login über den Webbrowser zeigte sich uns eine übliche Ordner- und Datei-Navigation, unterteilt in die Bereiche "My Files & Folders", "Shared Folders", "Favorite Folders" und "Connectors". Zunächst legten wir unseren persönlichen Repository Ordner an und übertrugen Dateien. Weitere Möglichkeiten erlaubten es uns auch, Notizen und Internetadressen abzulegen, Ordner zu verschieben und zu kopieren.

Benutzer über das eigene AD authentifizieren

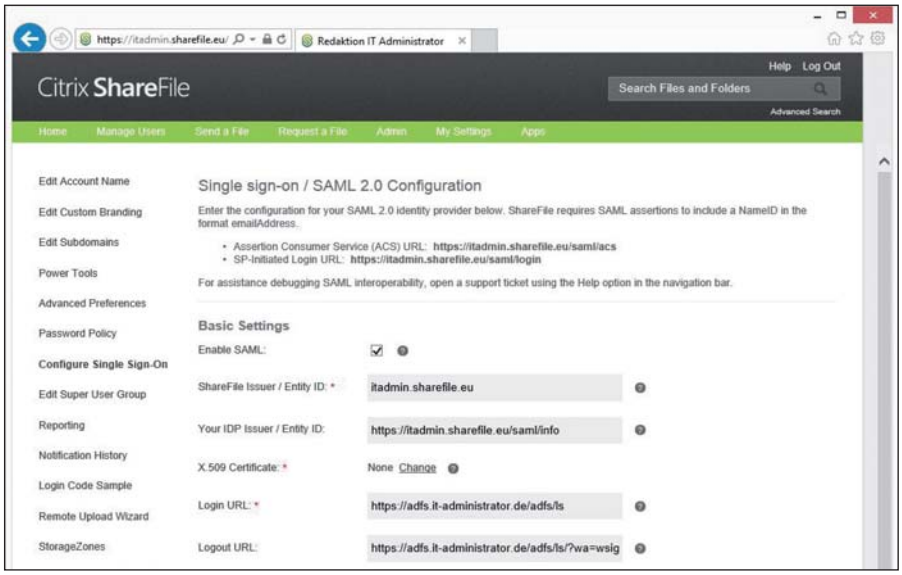
Interessant für Unternehmenskunden ist die Benutzerverwaltung. ShareFile kennt unterschiedliche Nutzer und unterscheidet zusätzlich zwischen den Zugängen für Mitarbeiter und Kunden. Mitarbeitern teilten wir granular Rechte im System zu und Kunden durften lediglich auf Dateien und Verzeichnisse zugreifen, die wir explizit freigaben.

Die meisten Unternehmen setzen für die Benutzerverwaltung schon ein Active Directory ein. Um die Daten nicht mehrfach pflegen zu müssen, bietet ShareFile auch die Anbindung ans AD. Die Integration nahmen wir im Test auf Basis eines Windows Server 2012 vor, den wir mit der AD FS-Rolle installierten. Mit diesem Dienst richteten wir eine Vertrauensstellung zwischen unserem Windows-Server und ShareFile ein. Nach der Windows-Konfiguration trugen wir die notwendigen Daten über die Admin-Konsole im ShareFile ein. Über ein X.509-Zertifikat verschlüsselten beide Systeme ihren Datenaustausch.

Nun legten wir fest, wie zukünftig die Login-Maske erscheinen sollte – entweder nur mit der SAML-Authentifizierung über das AD oder parallel weiterhin mit der Anmeldung über die ShareFile-Benutzerliste. Im Test entschieden wir uns für einen Mix zwischen ShareFile-Usern, wie zum Beispiel Kunden, und unseren AD-Anwendern.

Datenspeicher im eigenen Hause

Neben dem Zugriff auf die AD-Benutzerdaten speichert ShareFile auch Daten auf Geräten, die das Unternehmen unter eigener Kontrolle hat. Denn alle bisher vorgestellten Datei-Aktionen fanden auf dem physikalischen Speicherplatz des Herstellers statt. Bei einer ShareFile StorageZone handelt es sich um die Kopplung zwischen ShareFile und zusätzlichen Speicherorten. In unserem Fall stellten wir eine Verbindung zu einem SAN in unserem lokalen Netzwerk her.



Über SAML erfolgt die Verbindung zum eigenen Active Directory

Dazu installierten wir auf einem Windows 2008 das StorageCenter, das über den IIS 7 eine virtuelle Seite einrichtet und darüber die Zugriffe steuert. Leider arbeitete das StorageCenter 2.1 im Test nur auf einem englischen Betriebssystem, wodurch wir gezwungen waren, einen eigenen Server dafür aufzusetzen. Laut Hersteller ist die Version 2.2 noch für 2013 geplant, die dann auch auf einer deutschen Installation lauffähig ist. Nach der Installation unter Windows wechselten wir in die ShareFile-Oberfläche und legten die neue StorageZone fest. Dazu trugen wir eine Benutzernamen-Passwort-Kombination und die öffentliche URL zu unserem StorageCenter-Server, den wir zuvor eingerichtet hatten, ein. Leider bietet Citrix keinen Connector für Linux-Geräte an, die prädestiniert für diese Aufgabe wären.

Nachdem wir die StorageZone erstellt und über das Webinterface einen neuen Ordner angelegt hatten, erhielten wir nun die Auswahl, ob wir in der ShareFile-Cloud oder in unserer neuen StorageZone arbeiten möchten. Per Standard ist die ShareFile-Cloud als Speicher festgelegt. Anwender, die nicht darauf achten, speichern daher weiterhin Daten bei Citrix ab. Über den Hersteller-Support ließen wir den Default-Wert auf unsere Zone umstellen. Leider war es nicht möglich, generell festzulegen, auf welchen Speicher der Anwender überhaupt zugreifen durfte. So liegt es immer in der Verantwortung der Mitarbeiter, die Daten im richtigen Ort abzulegen.

Einsatz auf mobilen Geräten

Um ShareFile mobil und flexibel einzusetzen, bietet Citrix einige Zusatzprogramme an. Natürlich dürfen da die Apps für Android und iOS nicht fehlen. Zusätzlich unterstützt das System auch Windows Phone und Blackberry-Geräte. Durch diese erhielten wir auch über ein Tablet und Smartphone Zugang zu den Daten. Unter Windows 8 installierten wir die Sharefile-App, die uns ebenfalls den Datenzugriff ermöglichte. Auch per FTP griffen wir auf die Dateien zu. Lediglich die Einrichtung von WebDAV blieb erfolglos. Auch wenn die neue Weboberfläche schon alle benötigten Verbindungsdaten preisgab, war die offizielle Aussage, dass dieses Feature noch nicht verfügbar ist.

Sehr praktisch war für uns das Outlook Plug-In. Regulär haben viele Mailserver eine Begrenzung der Postfachgröße. Aber auch generell belastet das Versenden großer Dateien, womöglich noch an mehrere Empfänger, den Datenverkehr unnötig. Nach der Installation des Plug-Ins fügten wir zum Versenden von Dateien diese nicht mehr als Anhang an, sondern nutzten die neu integrierte ShareFile-Option "Send File". Wir wählten im erscheinenden Auswahldialog eine oder mehrere Dateien aus, die das Tool automatisch auf den ShareFile-Server lud und uns einen Downloadlink bereitstellte. Wollten wir von einem Dritten Daten empfangen, stellten wir über das Plug-In in einer E-Mail einen Upload-Link bereit, über den der E-Mailempfänger uns Daten auf unseren ShareFile-Speicher spielte.

Fazit

Im Großen und Ganzen ist ShareFile ein Cloud-Speicher, wie er vielfach zu buchen ist. Einige Features wie das Outlook-Plug-In heben sich von anderen Angeboten ab. Lediglich der Enterprise-Account macht das Produkt für Unternehmen interessant, da sie die Kontrolle über Benutzerdaten, Kennwörter und Dateien behalten, sofern sie ein Active Directory nutzen und lokal eine oder mehrere StorageZones anlegen. In diesem Fall fungiert ShareFile lediglich als sichere Eingangstüre mit Einlasskontrolle. In der jetzigen Form ist ShareFile zu teuer. Die rein englische Oberfläche, das StorageCenter, das im Test nur auf einem englischen Windows-Server lief, und einige Konfigurationen, die nur über das Support-Center des Herstellers umsetzbar waren, zeigten im Test, dass ShareFile noch recht jung ist. *(jp)*

Produkt
Cloud-basierte Software zum Datenaustausch.

Hersteller
Citrix
www.citrix.de/products/sharefile/overview.html

Preis
Die Enterprise-Lizenz kostet im jährlichen Abonnement 83 US-Dollar pro User. Eine unbefristete Lizenz kostet 150 US-Dollar pro User und Jahr zuzüglich 33 US-Dollar Servicevertrag pro User und Jahr in den ersten zwei Jahren. Danach nur noch 33 US-Dollar pro User und Jahr.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator *(max. 10 Punkte)*

Funktionsumfang	5
Unterstützung mobiler Geräte	7
Anbindung ans Unternehmensnetz	8
Sicherheit der Daten	7
Zugriffszeit	6

Citrix ShareFile

Server und Dienste in Windows Azure auslagern

Rechenpower auf Knopfdruck

von Thomas Joos

Quelle: gradt – Fotolia.com

Mit Windows Azure bietet Microsoft mittlerweile zahlreiche Möglichkeiten an, um einzelne Dienste oder ganze Server in die Cloud auszulagern. Dabei werden in den wenigsten Fällen Unternehmen alles auslagern, aber für einzelne IT-Bereiche ergibt der Betrieb in der Cloud durchaus Sinn – besonders, wenn deren Arbeitslast stark schwankt. Auf welchem Weg Sie Ihre Dienste in die Microsoft-Cloud auslagern, lesen Sie in diesem Workshop.

Neben der Option, Dienste wie Datenbanken oder Webseiten über Windows Azure zur Verfügung zu stellen (Platform as a Service, PaaS), unterstützt der Cloud-Dienst nun auch virtuelle Server und virtuelle Netzwerke. Sie können dabei mit Servern in der Cloud arbeiten und diese mit Ihrem lokalen Netzwerk verbinden. Auch Speicherkonten lassen sich in Windows Azure erstellen und an lokale Netzwerke anbinden. Somit können Unternehmen auch Infrastructure as a Service (IaaS) nutzen und komplette virtuelle Server in Windows Azure erstellen. Die Verwaltung der Server erfolgt zum Beispiel mittels RDP. Auf den Servern lassen sich Serverdienste installieren, genau wie auf Servern im lokalen Netzwerk.

Für das Aufsetzen von Servern bietet Microsoft Vorlagen an, mit denen Windows Server 2012 oder 2012 R2 in wenigen Sekunden zur Verfügung steht. Außerdem ist es möglich, Linux- und Windows-Server parallel in der Cloud zu betreiben und über das Web zu verwalten. Als Vorlagen dienen aber nicht nur Betriebssysteme, sondern auch komplette Serverdienste wie BizTalk oder SQL Server. Sogar neue Serverversionen mit SQL Server 2014 samt Windows Server 2012 R2 lassen sich mit wenigen Klicks selbst erstellen und auf diesem Weg testen, ohne im internen Netzwerk eine Software installieren zu müssen. Auf Basis dieser Server können Sie weitere Serverdienste einrichten und über das Internet mit Ihrem Netzwerk verbinden.

Die Server-Umgebung in Azure eignet sich vor allem für hybride Clouds, da sich die Dienste auf den virtuellen Servern mit lokalen Servern gemeinsam betreiben lassen. Neben den bereits vorgefertigten Vorlagen können Sie natürlich eigene erstellen und hochladen. Auch komplette Server lassen sich in die Cloud migrieren. Darauf gehen wir nachfolgend ein.

Möchten Sie neue Server in Windows Azure erstellen, wählen Sie eine Vorlage aus. Neben den Betriebssystemen lassen sich auf den Servern auch Programme auf Basis von Entwickler-Bibliotheken für .NET, Java, PHP und Node.js bereitstellen. Im Rahmen der Migration von lokalen Servern in die Cloud können Sie virtuelle Festplatten zwischen lokalen Servern und Cloud-Servern hin- und herschieben. Am besten nutzen Sie dazu das System Center, genauer gesagt System Center Virtual Machine Manager 2012 R2. Für Entwickler und Administratoren stellt Microsoft auch ein Trainings Kit zur Verfügung [1]. Mit diesem können Sie im Vorfeld die Umgebung testen und sich einarbeiten.

IaaS und PaaS im Angebot

Windows Azure bietet für Unternehmen also die Möglichkeit, nicht nur Dienste auf Basis von PaaS zu verwenden, sondern auch vollwertige Server zur Verfügung zu stellen. Sie können auf virtuellen Servern Dienste installieren und diese wie lokale Server verwalten und überwachen (IaaS). Parallel dazu ist es auch weiterhin möglich, in Windows Azure PaaS-Dienste zu nutzen. Dabei verwenden Sie Dienste in der Cloud wie SQL Azure oder Windows Azure Active Directory. In diesem Fall betreiben Sie keine eigenen Server, sondern verwalten nur den Serverdienst. Das erspart einiges an Aufwand, erfordert aber teilweise Anpassungen an Ihren Anwendungen.

Die darunterliegenden Server werden wiederum von Microsoft verwaltet und in Microsoft-Rechenzentren zur Verfügung gestellt. Sie können daher nur den entsprechenden Dienst ansprechen, nicht die zugrundeliegende Infrastruktur oder das Basis-Betriebssystem. Windows Azure bietet auch die Möglichkeit, PaaS und Iaas zu mischen. So können Sie mit Windows Azure Virtual Machines zum Beispiel Server erstellen, auf denen Dienste bereits installiert und konfiguriert sind. Beispiele dafür sind SQL, SharePoint, aber auch Exchange, BizTalk oder Active Directory. Ferner können Sie auch Dienste von

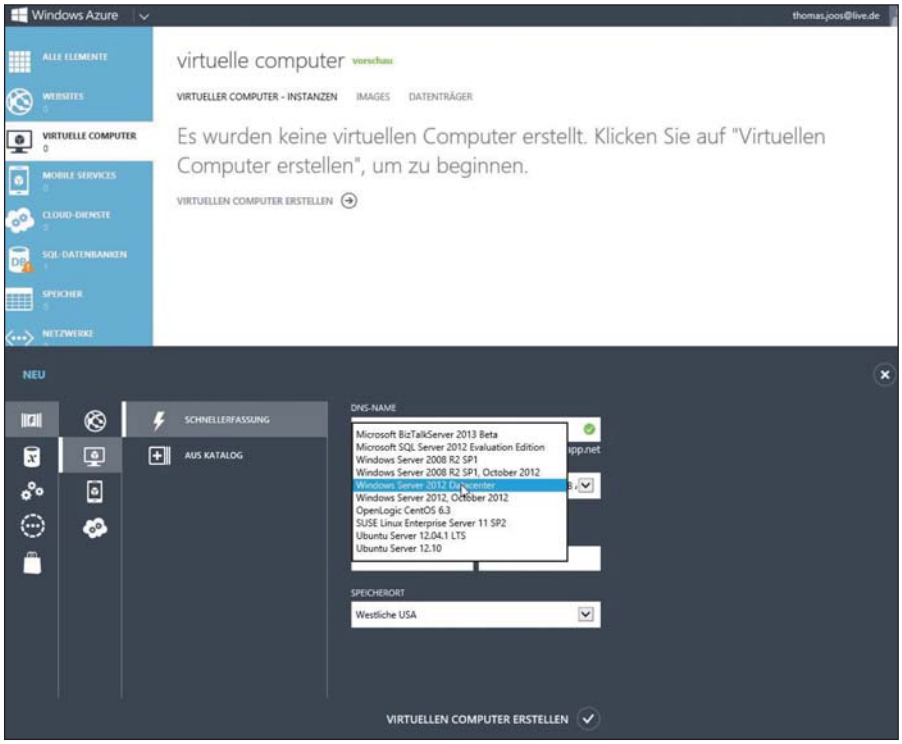


Bild 1: In Windows Azure erstellen Sie mit wenigen Klicks komplette virtuelle Server, die Sie produktiv in das Netzwerk einbinden können

Drittherstellern wie Hadoop oder MySQL über virtuelle Server zur Verfügung stellen. Diese Server erzeugen Sie entweder über die bereits vorhandenen oder neue Vorlagen.

Auf der anderen Seite lassen sich PaaS-Dienste in Windows Azure, zum Beispiel SQL Azure, fast so verwalten und ansprechen wie herkömmliche SQL Server-Instanzen, die Sie im internen Netzwerk betreiben. Der IaaS-Ansatz spielt daher seine Vorteile aus, wenn Sie das Betriebssystem oder Einstellungen auf dem Server für die Anwendung besonders anpassen müssen. Im Gegensatz zu PaaS-Diensten wie SQL Azure oder Azure Active Directory können Sie auf virtuellen Servern die gleichen Einstellungen vornehmen wie auf lokalen Servern. Das gilt auch für die Verwaltung, Sicherung und Fehlerbehebung.

IaaS-Cloud mit lokalem Netzwerk verbinden

Damit sich Cloud-Dienste, welcher Art auch immer, mit dem lokalen Netzwerk verbinden lassen, müssen Sie zunächst eine physische Verbindung schaffen. Es ist selbsterklärend, dass Sie für den Betrieb eine schnelle und stabile Internetleitung benötigen, inklusive einer gewissen Ausfallsicherheit. Die Firewall im Netzwerk muss in der Lage sein, Serverdienste über die Cloud schnell und sicher im internen Netzwerk zur Verfügung zu stellen, und für Anwender muss die Anbindung vollkommen transparent erfolgen.

Der einfachste Weg, einen lokalen Dienst in die Cloud auszulagern, ist sicherlich der IaaS-Ansatz. Sie erstellen einen neuen virtuellen Server mit dem passenden Betriebssystem in Azure, installieren auf diesem Ihren Serverdienst und passen den Server und die notwendigen Dienste an. Danach verbinden Sie den Server mit einem virtuellen Netzwerk in Azure, das wiederum über das Internet mit Ihrem internen Netzwerk über Ihre Firewall kommuniziert. Virtuelle Server in Azure sind daher zunächst mit einem virtuellen Netzwerk dort verbunden. Dieses Netzwerk verbinden Sie über das Internet mittels VPN-Gateway mit Ihrem internen Netzwerk und bei Bedarf auch mit der Active Directory-Domäne. Ab hier läuft der Zugriff auf das virtuelle Netzwerk für Anwender und Administratoren transparent. Auch Serverdienste, die mit dem ausgelagerten Dienst zusammenarbeiten müssen, funktionieren nach der Auslagerung wie zuvor.

Durch die VPN-Verbindung zwischen Azure und Ihrem lokalen Netzwerk können Sie im virtuellen Netzwerk auch mit den IP-Adressen aus Ihrem LAN arbeiten. Achten Sie aber darauf, dass die Leistung durchaus etwas einbrechen kann, da die wenigsten Internetleitungen mit den Geschwindigkeiten lokaler Netze mithalten können. Alle Serverdienste lassen sich über diesen Weg daher nicht auslagern. Hier sollten Sie vor einer Auslagerung gründlich testen.

Verwaltung und Überwachung von Cloud-Servern

Betreiben Sie im Netzwerk und in der Cloud mehrere virtuelle Server, müssen Sie auch die Verwaltung und Überwachung dieser Server berücksichtigen. Hier bietet sich vor allem das neue System Center 2012 R2 an. Die neue Version lässt sich als Preview testen [2]. System Center arbeitet sehr eng mit den Cloud-Diensten in Windows Azure zusammen. Sie können in den einzelnen Werkzeugen virtuelle Computer auf Basis von Windows Azure Virtual Machines verwalten, also zum Beispiel in System Center Virtual Machine Manager 2012 R2 erstellen und an das interne Netzwerk anbinden. Über diesen Weg können Sie auch andere Cloud-Dienste wie Windows Azure Active Directory und Windows Azure Online Backup an Windows Server 2012 und Windows Server 2012 R2 anbinden und zentral verwalten.

Arbeiten Sie mit virtuellen Servern in Windows Azure, ergibt der Einsatz des System Center Virtual Machine Manager 2012 R2 besonders Sinn. Die neue Version erlaubt die Verwaltung der verschiedenen Virtualisierungssysteme im Netzwerk. Der Windows Azure Hyper-V-Wiederherstellungsmanager kann wiederum Server, die Unternehmen in System Center 2012 R2 erstellen und betreiben, an einen zweiten Speicherort sichern und replizieren. Haben Sie erst einmal virtuelle Server angebunden, verwalten Sie diese also zentral in System Center oder mit jedem anderen Tool, das Sie im Netzwerk einsetzen. Auch RDP-Sitzungen sind problemlos möglich. Sie können für virtuelle Server auch automatisches Routing in verschiedenen Rechenzentren einrichten. Damit erhö-

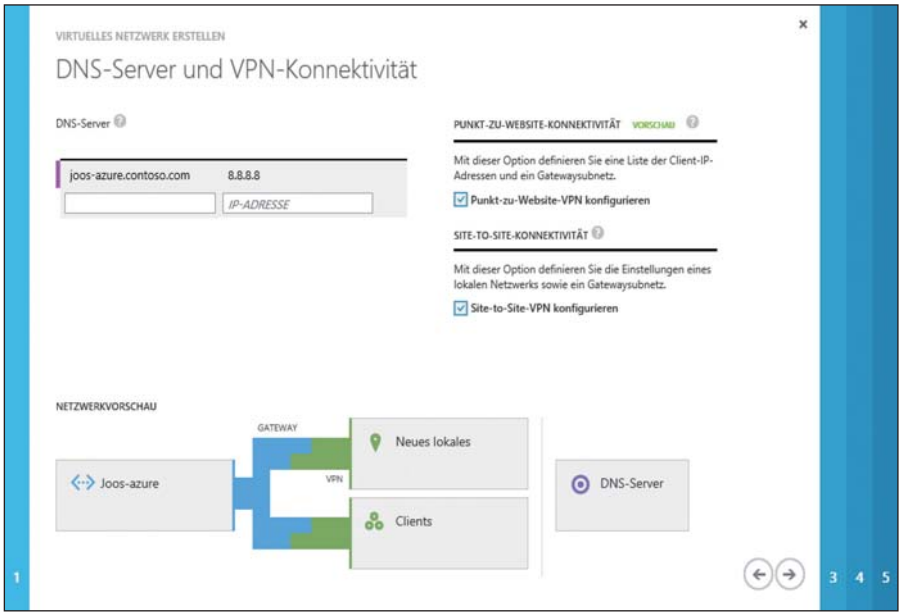


Bild 2: In Windows Azure erstellen Sie ein virtuelles Netzwerk für Ihre virtuellen Server. Das virtuelle Netzwerk verbinden Sie per VPN mit Ihrem lokalen Netzwerk.

hen Sie die Verfügbarkeit und verbessern die Antwortzeiten für Benutzer. Mit diesen Möglichkeiten verbinden Sie lokale Server mit Servern in der Cloud, synchronisieren Daten und können sogar mehrere Rechenzentren nutzen.

Erst testen, dann migrieren

Microsoft stellt eine nahezu uneingeschränkte Testmöglichkeit von 90 Tagen für Windows Azure zur Verfügung. Innerhalb dieses Zeitraums können Sie alle Szenarien durchspielen und Ihr Azure-Netzwerk an das interne Netzwerk anbinden, virtuelle Server erstellen und die einzelnen Serverdienste installieren. Möchten Sie den entsprechenden Server produktiv übernehmen, können Sie entweder einen weiteren Azure-Vertrag abschließen und die Testversion auslaufen lassen oder Sie verwenden die aktuelle Testumgebung weiter als Produktivumgebung. Um virtuelle Server in der Cloud zu betreiben, müssen Sie nicht unbedingt auf aktuelle Betriebssysteme wie Windows Server 2012 oder Windows Server 2012 R2 setzen. Sie können aus den Vorlagen auch Server mit Windows Server 2008 R2 SP1 auswählen. Ältere Versionen stehen jedoch nicht zur Verfügung.

Der nächste Schritt, nach dem Verwenden von IaaS, zum Auslagern von Serverdiensten in die Cloud wäre der PaaS-Ansatz. Hier betreiben Sie keine eigenen Server mehr, sondern nur noch die Anwendung selbst. Den Betrieb und die Verwaltung der Server übernimmt Microsoft. Allerdings müssen Sie hier, wie schon erwähnt, in vielen Fällen die Anwendungen an den Cloud-Betrieb anpassen. Haben Sie keinen Zugriff auf den Quellcode, kann eine Auslagerung problematisch sein. In diesem Fall können Sie aber immer noch mit dem IaaS-Ansatz den kompletten Server auslagern. Betreiben Sie zum Beispiel Webanwendungen im Unternehmen, müssen Sie nicht unbedingt einen kompletten Server in Windows Azure erstellen und verwalten, sondern können auch einfach eine Website erstellen und über PaaS-Ansätze die Anwendung in die Cloud übernehmen. Allerdings müssen hier Anpassungen bezüglich der Authentifizierung und anderer Funktionen erfolgen. Auch dieser Bereich spielt für das Auslagern von Serverdiensten in die Cloud eine wichtige Rolle. Die Sicherheit und der Datenschutz müssen gewahrt bleiben, auch wenn sich die Dienste nicht mehr im internen Unternehmen befinden.

Die Migration planen

Microsoft bietet das kostenlose "Cloud Security Readiness Tool" an, mit dem Sie über einen Fragebogen Informationen und Hilfen zum sicheren Betrieb oder Nutzen von Cloud-Diensten erhalten. Sie starten das Tool über die Internetseite [3]. Der anschließende Bericht bietet eine Grundlage für den Cloud-Einsatz im Unternehmen. Das Cloud Security Readiness Tool befasst sich allerdings ausschließlich mit dem Thema Sicherheit. Microsoft arbeitet hier mit der Cloud Security Alliance (CSA) zusammen. Natürlich sind die Berichte darauf ausgelegt, dass Unternehmen auf Microsoft-Produkte in der Cloud setzen – zum Beispiel Office 365 oder die verschiedenen Azure-Dienste wie virtuelle Computer. Sie müssen bei der Eingabe der Daten keine vertraulichen Informationen eingeben. Sobald Sie die Daten eingetragen haben, wird der Bericht erstellt und Sie können ihn als PDF-Datei herunterladen.

Virtuelle Netzwerke im Detail

Basis der Verbindung von virtuellen Servern mit lokalen Netzwerken in Unternehmen sind die virtuellen Netzwerke. Diese bauen über VPN-Verbindungen eine Kommunikation mit lokalen Netzwerken auf. Verwenden Sie virtuelle Server in Azure, sind virtuelle Netzwerke also der zentrale Bereich, um Ihre Azure-Server mit dem lokalen Netzwerk zu verbinden. Erstellen Sie die virtuellen Netzwerke und lokalen Netzwerke über den Bereich "Netzwerke" und legen Sie für die einzelnen Netzwerke eine "Affinitätsgruppe" fest. Dabei handelt es sich um eine Gruppierung von Diensten und Netzwerken.

Erstellen Sie dann neue virtuelle Server in Azure und wählen Sie aus, in welcher Affinitätsgruppe der entsprechende Server platziert werden soll. Alle Azure-Dienste und Netzwerke, die Sie der gleichen Affinitätsgruppe zuordnen, befinden sich auch im gleichen Rechenzentrum. Wie Sie virtuelle Netzwerke erstellen, zeigt Microsoft in der Azure-Dokumentation unter [4]. Natürlich haben Sie auch die Möglichkeit, mehrere Netzwerke zu erstellen und verschiedenen Affinitätsgruppen zuzuordnen.

Um Serverdienste in der Cloud zu testen, sind aber weder Netzwerke noch Affinitätsgruppen notwendig. Sie können in den ersten Schritten den Serverdienst in der Cloud testen und im Anschluss an die produktive Umgebung anbinden. Erst danach müssen Sie Netzwerke erstellen. Vorher müssen Sie dazu Ihre Internetleitung entsprechend prüfen.

Virtuelle Server für die Migration vorbereiten

Möchten Sie virtuelle Server von Ihrem lokalen Netzwerk in Windows Azure auslagern, können Sie einzelne virtuelle Festplatten in Windows Azure hochladen und die darauf befindlichen Systeme in Windows Azure als virtuelle Server einbinden. Wie Sie lokale Server in die Cloud transferieren, zeigt Microsoft in einem TechNet-Beitrag [5]. Auf diesem Weg erstellen Sie schnell eine Testumgebung auf Basis Ihrer produktiven Umgebung. Sie sollten in diesem Fall auch das Windows Azure SDK herunterladen und installieren. Die aktuelle Version finden Sie im Downloadbereich des Azure-Verwaltungsportals, nachdem Sie sich angemeldet haben.

Ein wichtiges Werkzeug, um virtuelle Server von lokalen Netzwerken in die Cloud hochzuladen, ist *csupload.exe*. Bevor Sie aber virtuelle Server in die Cloud laden, müssen Sie diese lokal vorbereiten. Dazu sollten Sie zunächst die virtuellen Festplatten bereinigen und verkleinern. Auch die Defragmentierung der Platten ergibt Sinn. Verwenden Sie möglichst keine dynamischen Arbeitsspeicher, sondern weisen Sie den Arbeitsspeicher fest zu. Die Festplatte sollte ebenfalls eine feste Größe haben. Diese Aufgaben nehmen Sie in Ihrer Virtualisierungslösung vor.

Haben Sie virtuelle Festplatten vorbereitet, laden Sie die Dateien mit *csupload.exe* in Azure, genauer gesagt in den Speicher von Windows Azure. Sie finden die Datei nach der Installation des Windows Azure SDK unter "C:\Program Files\Microsoft SDKs\Windows Azure\.NET SDK\Version des SDK\bin\". Die Aufgabe von *csupload.exe* besteht vor allem im Hochladen der virtuellen Festplatten Ihrer lokalen virtuellen Server in den Speicher Ihres Windows Azure-Kontos. Auf diesen Speicher greifen die virtuellen Server in Windows Azure zu. Erstellen Sie neue Server, verwenden Sie die hochgeladenen Festplatten für die neuen Server.

CSUpload benötigt für die Verbindung zu Azure ein Zertifikat. Sie können der Einfachheit halber auch ein selbst signiertes Zertifikat verwenden. Dieses erstellen Sie für Testzwecke zum Beispiel mit dem SDK für Windows 7 [6]. Arbeiten Sie mit Windows 8, laden Sie sich die Version des Windows SDK [7] für Windows 8. Um mit dem SDK ein Zertifikat für CSUpload zu erstellen, verwenden Sie den Befehl:

```
makecert -r -pe -n "CN=Meine Azure-
  Umgebung" -a sha1 -ss My -len 2048
  -sy 24 -b 01/01/2013 -e 01/01/2019
```

Den Namen in Anführungszeichen können Sie anpassen, das gilt auch für die Dauer der Gültigkeit des Zertifikats. Im Anschluss exportieren Sie das Zertifikat vom Rechner und binden es in Windows Azure ein:

1. Starten Sie mit *certmgr.msc* die Zertifikateverwaltung und klicken Sie doppelt auf das Zertifikat.
2. Wechseln Sie auf die Registerkarte "Details" und wählen dort die Option "In Datei kopieren".
3. Wählen Sie im Assistenten die Option "Nein, privaten Schlüssel nicht exportieren".
4. Belassen Sie auf der nächsten Seite die Option "DER-codiert-binär X.509 (.CER)".
5. Rufen Sie die Verwaltungswebseite von Windows Azure auf [8].
6. Klicken Sie auf "Einstellungen" und dann auf "Verwaltungszertifikate".
7. Klicken Sie unten auf "Hochladen" und laden Sie das exportierte Zertifikat in Windows Azure hoch.
8. Nach einigen Sekunden sollte das Zertifikat erscheinen.

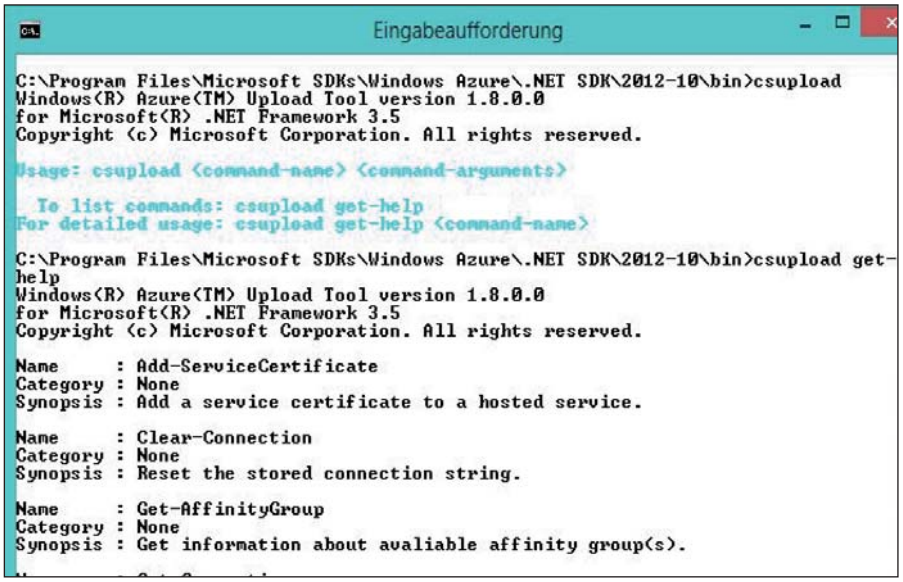


Bild 3: Mit CSUpload laden Sie virtuelle Server in die Cloud. Dazu sollten Sie vorher die Festplatten der Server entsprechend vorbereiten.

Nach der Integration des Zertifikats verbinden Sie *csupload.exe* mit Windows Azure. Dazu verwenden Sie Ihre Abonnenten-ID und den Fingerabdruck des erstellten Zertifikats. Die ID sehen Sie im Verwaltungsportal. Dazu klicken Sie auf "Speicher" und dann auf den Speicher Ihres Azure-Kontos. Den Fingerabdruck des Zertifikats finden Sie über "Einstellungen / Verwaltungszertifikate". Danach verwenden Sie den Befehl:

```
Csupload set-connection
  "SubscriptionID=ID;
  Certifi-cateThumbprint=Fingerab-
  druck; ServiceManagement End-
  point=https://management.core.
  windows.net"
```

Haben Sie die Verbindung erstellt, laden Sie mit CSUpload virtuelle Festplatten in Azure. Mit *csupload get-location* testen Sie die Verbindung. Mit *csupload get-persistentvmimage* zeigen Sie die verfügbaren Vorlagen für virtuelle Server in Windows Azure an. Eine Hilfe zu CSUpload finden Sie auf der Seite [9]. Ein Beispiel sieht folgendermaßen aus:

```
csupload.exe Add-PersistentVMImage
  -Destination Pfad zur VHD-Datei im
  Azure-Speicher -Label "Windows
  Server 2012" -OS Windows
  -LiteralPath "d:\Hyper-V\Virtual
  Hard Disks\disk.vhd" -Name
  basew2k12.vhd
```

Azure mit PowerShell und Tools administrieren

Die allgemeine Verwaltung von Windows Azure findet über ein Webinterface oder über die Werkzeuge in System Center ab Version 2012 R2 statt. Ebenfalls wichtig ist die Windows Azure PowerShell [10] zur Administration von Azure in einer lokalen PowerShell-Sitzung. Eine umfassende Anleitung bietet Microsoft im Blog-Beitrag [11].

Der häufigste Einsatz der Windows Azure-PowerShell liegt im Erstellen von neuen virtuellen Servern. Dazu verwenden Sie das Cmdlet "New-AzureQuickVM". Interessant wird die PowerShell-Erweiterung für Azure, wenn Sie die Erstellung virtueller Server oder Dienste automatisieren möchten. Sie können die Befehle zu komplexen Skripten zusammenbauen.

Auf diesem Weg lassen sich zum Beispiel virtuelle Server auf Basis von Windows Azure erstellen und mit Active Directory, SQL Server 2012 oder SharePoint Server 2013 bereitstellen. Sie benötigen für diese Vorgänge vorbereitete Skripte, die Sie mit eigenen Erweiterungen ergänzen. Sie finden diese auf der Seite [12].

Im Azure-Speicher liegen auch Daten von virtuellen Servern, die Sie online erstellen oder mit *csupload.exe* hochgeladen haben. Möchten Sie einen Überblick über die Daten im Storage erhalten, müssen Sie nicht immer das Verwaltungsportal nutzen, sondern können auch mit dem Open Source-Tool "Azure Storage Explorer" [13] arbeiten. Damit zeigen Sie den Inhalt des Speicherkontos an und laden Dateien aus dem Speicher herunter sowie in den Speicher hoch. Das ist bei Migrationen von virtuellen Servern besonders hilfreich, da Sie auch über diesen Weg die virtuellen Festplatten in die Cloud laden können.

Mit dem kostenlosen Tool CloudXplorer [14] verwalten Sie ebenfalls den Speicher

[1] System Center Virtual Machine Manager 2012 R2 Trainings Kit
DBP31

[2] System Center 2012 R2 als Preview testen
DBP32

[3] Cloud Readiness Tool
DBP33

[4] Windows Azure-Dokumentation
DBP34

[5] TechNet-Beitrag zur Übernahme lokaler Server in die Cloud
DBP35

[6] SDK für Windows 7
DBP36

[7] SDK für Windows 8
DBP37

[8] Verwaltungswebseite von Windows Azure
DBP38

[9] CSUpload
DBP39

[10] Windows Azure PowerShell
DBP30

[11] PowerShell-Anleitung in Blog-Beitrag
DBP3A

[12] Vorbereitete Skripte
DBP3B

[13] Azure Storage Explorer
DBP3C

[14] CloudXplorer
DBP3D

[15] Azure Explorer
DBP3E

[16] Free Azure Performance Monitor
DBP3F

[17] SQL Azure Migration Wizard
CAP46

Link-Codes

in Azure. Nach der Installation erstellen Sie zunächst über "Accounts" ein neues Konto. Das Werkzeug bietet vielfältige Möglichkeiten. Mit der Schaltfläche "Upload" laden Sie Dateien schnell und einfach in Ihre Container. Im Gegenzug laden Sie Dateien mit "Download" wieder herunter.

Sie können sich mit "Report" Berichte über die Nutzung des Kontos anzeigen lassen. Natürlich können Sie auch parallel mit CloudXplorer und Windows Azure Storage Explorer arbeiten.Eine ähnliche Software in diesem Bereich ist Azure Explorer [15]. Auch dieses Tool steht kostenlos zur Verfügung. Mit der Freeware Free Azure Performance Monitor [16] überwachen Sie daneben den Zustand Ihrer Windows Azure Dienste. Das Tool zeigt die Auslastung und die Leistung der Dienste an.

Datenbanken in die Cloud migrieren

Neben der Möglichkeit, virtuelle Server und im Bedarfsfall auch eigene SQL-Server in Windows Azure zu betreiben, können Sie auch reine Datenbanken in Azure einbinden. In diesem Fall nutzen Sie den PaaS-Ansatz und müssen sich nicht um die Server und das Betriebssystem an sich kümmern. Sie haben somit die Möglichkeit, Datenbanken von lokalen SQL-Servern zu SQL Azure oder auch von SQL Azure zu SQL 2012 zu übernehmen. Microsoft bietet hierfür den SQL Azure Migration Wizard [17] an. Diesen nutzen Sie, um Datenbanken von lokalen SQL Servern zu Windows Azure zu migrieren und umgekehrt. In der aktuellen Version unterstützt das Tool auch SQL Server 2012.

Sie haben auch die Möglichkeit, Datenbanken aus Azure im SQL Server Management Studio zu verwalten. Daneben können Sie mit *sqlcmd* von einem lokalen Server auf SQL Azure zugreifen. Das heißt, Sie greifen mit lokalen Werkzeugen auf Dienste in der Cloud zu. Um sich anzumelden, starten Sie sqlcmd mit folgender Syntax:

```
sqlcmd -U Benutzername@Servername
  ohne Domäne -P "Kennwort," -S
  Vollständiger DNS-Name
```

Zum Beispiel:

```
sqlcmd -U thomas@cn52c2k2do -P
  "ttt9790av" -S cn52c2k2do.
  database.windows.net
```

Überprüfen Sie nach der Migration alle Datenbanken. Deren Inhalt sehen Sie in der Windows Azure-Verwaltungsoberfläche, wenn Sie die Verwaltung der Datenbank starten. Sie können auch Daten zwischen Azure und SQL Server 2012 synchronisieren. Hierfür benötigen Sie Synchronisierungsgruppen. Diese legen Sie in der Webverwaltungs-Oberfläche von Azure an.

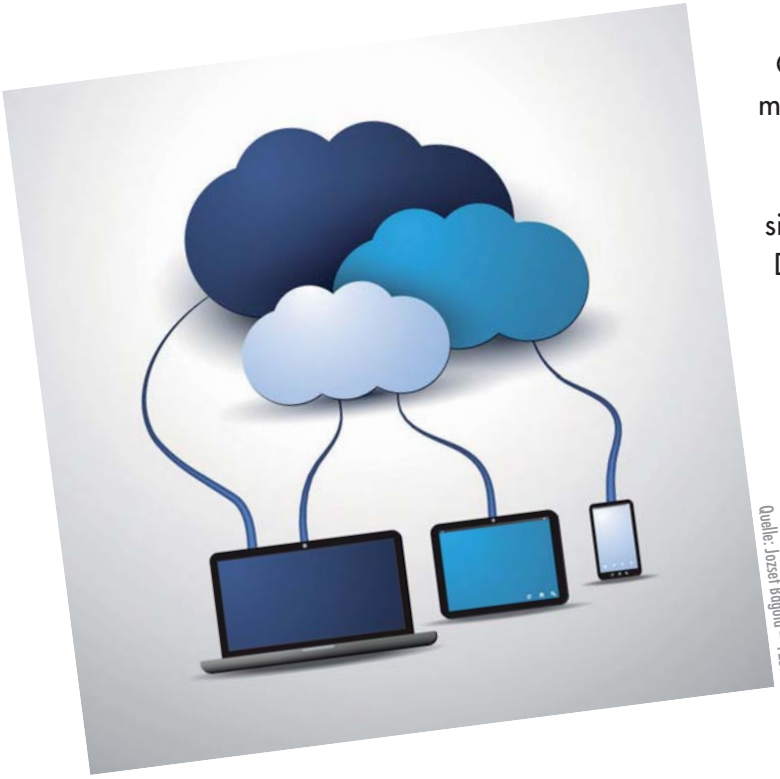
Fazit

Mit Windows Azure stehen Unternehmen verschiedene Ansätze zur Verfügung, um Server und Dienste in die Cloud auszulagern. Auch für Testumgebungen ist Azure interessant. Natürlich hängt viel von der Geschwindigkeit der Internetleitung ab. Setzt man sich etwas mit Windows Azure auseinander, sieht man schnell, dass sich viel bei dem Dienst getan hat und er zahlreiche Möglichkeiten für den produktiven Einsatz bietet. *(dr)*

Desktop-Virtualisierung mit Microsoft System Center Virtual Machine Manager

Der Himmel voller Desktops

von Matthias Wessner



Quelle: Jozsef Bagota – 123RF

Cloud-Computing stellt abstrahierte IT-Infrastrukturen mit Rechenkapazität, Datenspeicher, Netzwerkkapazität und entsprechender Software dynamisch bereit – häufig von einem externen Dienstleister. Handelt es sich jedoch bei der Infrastrukturkomponente um einen Desktop, so wird dieser in der Regel nicht extern eingekauft, sondern im eigenen Rechenzentrum gehostet. Entsprechende Cloud-artige Desktop-Umgebungen, die hochautomatisiert bereitgestellt werden und im eigenen Rechenzentrum laufen, nennen sich "Private Desktop Cloud" oder auch Desktop-as-a-Service. Dieses Konzept gewinnt zunehmend Akzeptanz, da insbesondere im Desktop-Umfeld massenweise identische Systeme bereitgestellt werden müssen. Dieser Beitrag zeigt den Weg zu einer Desktop-Cloud mit dem Microsoft System Center Virtual Machine Manager.

Das Thema Cloud ist in aller Munde – wenn auch Marketing-seitig von den Anbietern recht strapaziert. Neben zahlreichen technischen Assoziationen liegt bei der "Private Desktop Cloud" der Gedanke nicht fern, dass die IT Vergleichbares schon seit Ewigkeiten mit den Terminal-Diensten bereitstellt. Auch dabei gibt es einen zentralen Service, der automatisiert aufgesetzt wurde und der für verschiedene Endbenutzer sozusagen auf Abruf bereitsteht.

Doch so ganz Cloud-mäßig ist diese Bereitstellung dann doch nicht. Denn es müssen Hardware-Ressourcen zugewiesen, entsprechende Eingaben an verschiedenen Stellen getätigt werden, das Deployment-System muss vorbereitet werden, Rechnernamen sind zu erzeugen und so weiter. Sprich, für die wirkliche Installation eines Servers ist eine Menge Vorarbeit zu leisten. Im Cloud-Gedanken sieht das dann doch ein wenig anders aus. Hier gibt es eine Plattform, die immer gleichartig aufgebaut ist und Rechenkapazitäten für entsprechende Dienste bereitstellt. Auf dieser Plattform werden dann vollautomatisch Dienste bereitgestellt beziehungsweise erweitert.

Bereitstellung physikalischer Ressourcen

Microsoft hat den Begriff Cloud in den System Center Virtual Machine Manager (SCVMM) eingebaut. Hier ist die Cloud eine Zusammenfassung von Ressourcen – seien es Hostsysteme, Netzwerke, Netzwerk-Loadbalancer oder IP-Adressen; letztendlich alle Basis-Ressourcen, die notwendig sind, um Dienste zur Verfügung zu stellen. Über die SCVMM-Cloud ist also definiert, welche physikalischen und virtuellen Ressourcen neuen virtuellen Maschinen zur Verfügung stehen. Die Definition der Cloud ist demnach eine der ersten Aufgaben, denen sich der IT-Verantwortliche widmen muss. Eine Cloud muss genügend Ressourcen besitzen, um die neuen Aufgaben zu bewältigen. Sind die Ressourcen einer Cloud aufgebraucht, so können Sie diese im Nachhinein erweitern, indem sie zusätzliche physikalische Ressourcen zuweisen.

Ist die Cloud definiert, erstellen Sie als Nächstes ein Template. Ein Template beinhaltet entsprechende virtuelle Hardware-Ressourcen und auch eine virtuelle Festplatte, die zum Beispiel schon ein Grund-Image enthalten kann. Dieses sollte ein Standard-Betriebssystem sein, das ein Sysprep durchlaufen hat. In dem Template lassen sich auch verschiedene Konfigurationsdateien zuweisen. Diese Konfigurationsdateien sind die gleichen, die Sie für die normale Verteilung einer Sysprep-Datei nutzen. Eine gängige XML-Datei weist zum Beispiel das Keyboard-Layout zu (siehe Kasten "XML-Datei zur Zuweisung des Keyboard-Layouts").

Wenden Sie diese XML-Datei auf das Template an, so lässt sich keine direkte Veränderung erkennen, da das Keyboard-Layout nicht in der GUI erscheint. Es wird aber dennoch aktiv und neue Server verwenden das deutsche Tastaturlayout. Dies ist insbesondere von Vorteil, wenn Kennwörter spezielle Zeichen nutzen, die auf anderen Tastaturlayouts an anderer Stelle zu finden sind.

Sauberes Image nutzen

Das Image kann natürlich auch schon verschiedenste Rollen und Software-Produkte enthalten. Das spart zwar Zeit beim Deployment und der IT-Verantwortliche muss nicht wissen, wie er gewisse Schritte automatisiert, doch Best Practice ist es, das Image neutral zu halten und alle Veränderungen erst im Nachhinein zu skripten. Damit reduziert sich die Anzahl der Images und auch spätere Veränderungen lassen sich wesentlich schneller implementieren.

Ein Beispiel ist das aktuelle Windows Server 2012 R2-Release: Bauen Sie alle Rollen und Komponenten schon in das Image ein, so müssen Sie bei jedem Deployment alles neu aufsetzen. Haben Sie jedoch ein generisches Image genutzt, müssen Sie nur einmal das Template anpassen und alle weiteren Schritte bleiben identisch. Weitere Nacharbeiten können unterbleiben, da zum Beispiel PowerShell-Befehle in der Regel abwärtskompatibel sind.

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:
   unattend">
   <settings pass="oobeSystem">
      <component name="Microsoft-Windows-
      International-Core" processorArchitecture
      ="amd64" publicKeyToken=
      "31bf3856ad364e35" language="neutral"
      versionScope="nonSxS"
      xmlns:wcm="http://schemas.microsoft.com/
         WMIConfig/2002/State"
      xmlns:xsi="http://www.w3.org/2001/
         XMLSchema-instance">
         <InputLocale>De-de</InputLocale>
         <SystemLocale>de-de</SystemLocale>
         <UILanguage>de-de</UILanguage>
         <UILanguageFallback>de-de</UILanguage-
         Fallback>
         <UserLocale>de-de</UserLocale>
      </component>
   </settings>
   <cpi:offlineImage cpi:source="wim:c:/install.
   wim#Windows Server 2012 SERVERSTANDARD"
   xmlns:cpi="urn:schemas-microsoft-com:cpi" />
</unattend>
```

XML-Datei zur Zuweisung des Keyboard-Layouts

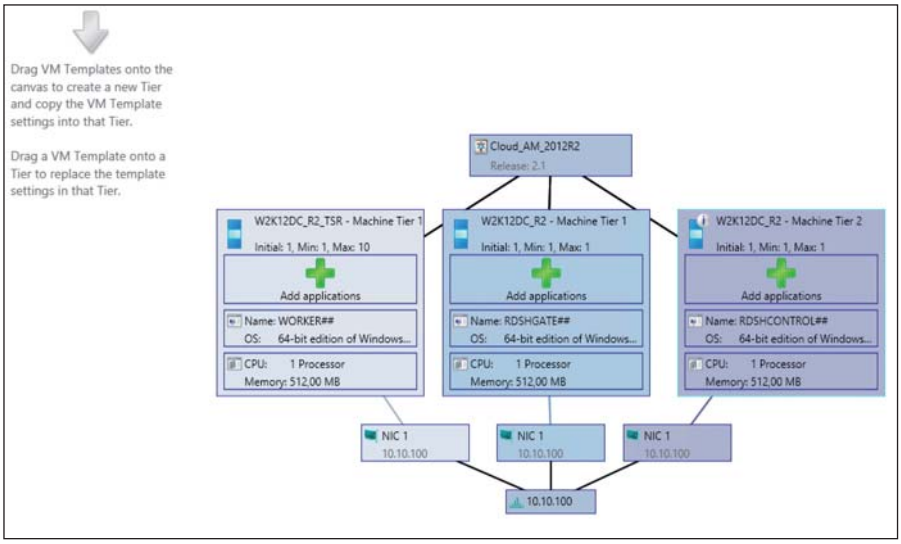


Bild 1: Im SCVMM benötigt die Desktop-Cloud ein Service Template mit drei Tiers

Backend-Dienste in Betrieb nehmen

Haben Sie das Template erstellt, ist der erste wichtige Schritt in Richtung private Desktop-Cloud gemacht. Als Nächstes erstellen sie ein sogenanntes Service Template. Service Templates sind verschiedene Arten von Servern, die zusammen einen gesamten Dienst ergeben. Als Beispiel wird hier gerne ein Service mit Webservern und SQL-Server genommen. Wenn wir uns den Service "Private Desktop Cloud" anschauen, benötigen wir auch verschiedene Serverrollen. Dies sind der Webserver, das Gateway, der Broker und die Remote Desktop Session Hosts. Der Desktop, der hier beschrieben wird, kommt also von einem Remote Desktop Session Host oder Terminalserver, wie er früher genannt wurde.

Wir nehmen einmal an, dass Sie den Web Service und das Gateway auf einem Server unterbringen wollen. Dann benötigen Sie drei weitere, unterschiedliche Rollen. Sie erstellen also ein Service Template mit insgesamt drei Tiers. Sie können mit einem Tier anfangen und die zwei weiteren einfach hinzufügen. Dabei müssen Sie beachten, dass eine Remote Desktop Session Host-Farm nur dann erstellt werden kann, wenn alle notwendigen Rollen vorhanden sind (die Webrolle, der Broker und der Remote Desktop Session Host). Sie müssen also dafür sorgen, dass das Farm-Erstellungsskript erst dann ausgeführt wird, wenn diese drei Rollen vorhanden sind. Dies funktioniert über das Service Template sehr einfach. Hier lässt sich definieren, in welcher Reihenfolge die einzelnen Tiers installiert werden. Definieren Sie, dass zuerst die Web-Rolle und die Broker-Rolle installiert werden, so können Sie die Installation der Farm im Rahmen der Installation des Remote Desktop Session Hosts veranlassen, der sozusagen in zweiter Reihe aufgespielt wird. Wird ein Gateway benötigt, so lässt sich dieses in einem vierten Tier nachträglich hinzufügen oder schon gleich mit der Web-Rolle auf den gleichen Server installieren und nachträglich einrichten.

Um die entsprechenden Rollen zu installieren, können Sie die Templates entsprechend der Rollen bearbeiten und die Features per grafischer Oberfläche hinzufügen. Damit macht SCVMM den Job für Sie. Die einzige Herausforderung, die Sie haben ist, dass Sie die Reboots selbst planen müssen. Sie müssen also wissen, wie viele Reboots eine Rollen-Installation benötigt. Das können beliebig viele Reboots sein. Die Rolle Remote Desktop Session Host mit der Desktop Experience erfordert zum Beispiel vier Neustarts.

Wird ein neuer virtueller Computer erstellt, so benötigt er einen Computernamen. Diesen können Sie pro Tier definieren. Ein Beispiel ist "RDSHGATE##". Damit vergibt SCVMM den Namen automatisch und zählt zweistellig hoch. Der erste Server dieser Rolle bekäme den Computernamen "RDSHGATE01". Führen Sie diesen Schritt für alle Rollen aus, indem Sie die Templates entsprechend konfigurieren.

Reboots per Skript steuern

Welches Skript sollten Sie nun zuerst starten? Es bietet sich zunächst an, die PowerShell Execution Policy zu deaktivieren. Dieser als Sicherheitsfeature implementierte Mechanismus ist unserer Meinung nach eher hinderlich, da das Skript natürlich entsprechende Ausführungsberechtigungen benötigt. Startet zum Beispiel ein normaler Anwender ein Skript, das Windows-Features installieren soll, scheitert es, da die Berechtigungen nicht ausreichen. Doch auch wenn ein Administrator das Skript startet, schlägt es wegen der Execution Policy fehl. Letztendlich ist es ein Registry-Eintrag, den Sie mit dem folgenden PowerShell-Befehl setzen können:

```
PowerShell.exe -command
  'Set-Executionpolicy bypass'
```

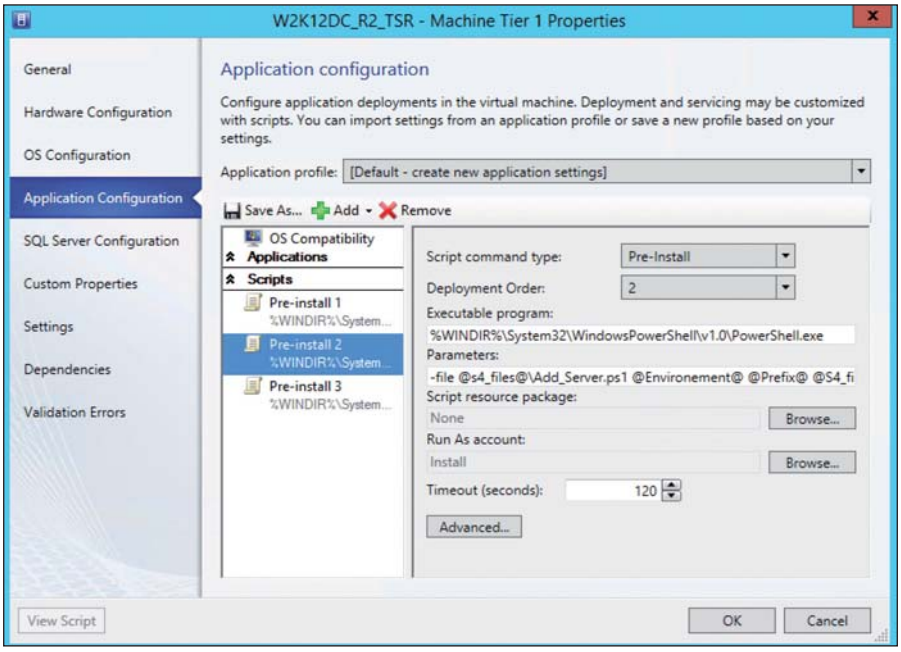


Bild 2: Die Steuerung der Applikationskonfiguration erfolgt über hinterlegte PowerShell-Skripte

Ist jedoch eine Gruppenrichtlinie gesetzt, die eine andere Execution Policy definiert, schlägt die Anweisung fehl. Als Lösung führen Sie PowerShell-Skripte mit dem folgenden Befehl aus und umgehen damit eine entsprechende Gruppenrichtlinie:

```
PowerShell.exe -executionpolicy
  bypass -file Script.ps1
```

Dazu muss das Konto, das zur Ausführung der Skripte definiert wurde, natürlich entsprechende Rechte haben.

Als Nächstes bauen Sie entsprechend viele Reboots ein, zum Beispiel mit dem Befehl

```
PowerShell.exe -command
  restart-computer
```

Für diesen Befehl benötigen Sie die Execution Policy noch nicht. Diese ist lediglich dazu notwendig, um PowerShell-Skripte zu starten.

Würden Sie jetzt dieses Service Template verteilen, bekämen Sie drei Server, die aber noch nicht in einer Farm arbeiten, sondern lediglich die notwendigen Rollen besitzen. Der letzte Server muss also noch ein Skript starten, das die Farm erstellt. Die Kommandozeile zum Erstellen einer Farm lautet:

```
New-RDSessionDeployment -Connection-
  Broker $Broker -WebAccessServer
  $Web -SessionHost $SessionHost
```

Danach erstellen Sie über folgenden Befehl einen Workspace:

```
Set-RDWorkspace -Name "Workspace01"
  -ConnectionBroker $Broker
```

Und letztendlich erstellen Sie dann noch eine Collection:

```
New-RDSessionCollection -Collection-
  Name $collection -SessionHost
  $SessionHost
-ConnectionBroker $Broker
  -CollectionDescription
  "Beschreibung der Collection"
```

Wir benötigen also den Namen des Brokers und des Webservers beziehungsweise Gateways. Doch während der letzte Server erstellt wird, weiß dieser nicht, wie diese Server heißen, da SCVMM diese ja gerade erst aufgebaut hat. Eine Möglichkeit wäre zum Beispiel, ein Check-File auf einem File Share abzulegen. Darin schaut dann der Server nach, wie die beiden anderen Rollen heißen – zum Beispiel: Ihr SCVMM-Server heißt "SCVMM01". Auf diesem legen sie ein Share an, worauf das Service-Konto Schreibberechtigungen erhält. Im Service Template für den SCVMM-Server definieren Sie den Zugriff auf das Share:

```
"Broker=$env:Computername" |
  out-file \\scvmm01\Share\
  @ENVIRONMENT@.log -append
```

Und für die Webrolle:

```
"Web=$env:computername" | out-file
  \\scvmm01\Share\@ENVIRONMENT@.log
  -append
```

Durch die beiden "@"-Zeichen definieren Sie eine Service Template-Variable. Diese können Sie beim Deployment der Templates angeben beziehungsweise kann die Variable auch als verbindlich definiert werden, sodass sich ein Deployment nicht starten lässt, bevor ein Wert für die Variable vergeben wurde. Sie geben dann zum Beispiel beim Deployment "Kunde1" ein. Damit wird ein Logfile angelegt mit den Werten der beiden Server. Bei der Erstellung der Farm wird dieses Logfile dann ausgelesen:

```
$Deployment_Servers =  get-content
  \\scvmm01\Share\@ENVIRONMENT@.log
Foreach ($value in $Deployment_Ser-
  vers){
New-variable -name $Deployment_Ser-
  vers.Split("=")[0] -value $Deploy-
  ment_Servers.Split("=")[1]
}
```

Damit verfügen Sie über die zwei Variablen "Broker" und "Web", die die Namen der

entsprechenden Server enthalten. Mit diesen Werten führen Sie nun die Erstellung der Farm durch. So lässt sich das Service Template modular halten und immer wieder nutzen. Damit ist der Grundstein einer gesamten Automatisierung der Bereitstellung einer Remote Desktop Session Host-Farm gelegt.

Zuweisung von Anwendungen

Natürlich müssten dann noch für eine Vervollständigung auch entsprechende Anwendungspakete installiert werden. Entweder erledigen Sie das über eine geskriptete Installation oder zum Beispiel über App-V-Anwendungen. Wählen Sie eine Skript-Methode, müssen Sie dafür sorgen, dass das Skript nicht selbst den Reboot ausführt, sondern einen Return Code liefert und SCVMM den Reboot durchführt. Ansonsten verliert SCVMM die Kontrolle und bricht mit einem Fehler ab. Nutzen Sie ein entsprechendes Skript, so lässt sich dieses immer wieder nach einem Reboot durch SCVMM neu starten.

Gibt es verteilte Maschinen zu einem Service Template, so lässt sich das Template nicht mehr modifizieren. Sie müssen in diesem Fall eine Kopie erstellen, die weiterverarbeitet werden kann. Komplexe Skripte sollten Sie auf ein entsprechendes File Share auslagern, sodass nicht immer das Service Template angepasst werden muss, sondern nur die externen Skripte.

In den erweiterten Skript-Einstellungen definieren Sie, wie SCVMM mit dem Skript umgeht. Hier kann SCVMM sogar das Skript erneut nach einem Reboot ausführen. Wichtig ist auch hier, dass das Skript nicht selbst den Reboot ausführt, da SCVMM sonst die Kontrolle verliert und in einen Fehler läuft. SCVMM kann aber selbst einen Reboot ausführen, wenn es einen entsprechenden Exitcode vom Skript zurückbekommt:

```
function ExitWithCode {
param ( $exitcode )
$host.SetShouldExit($exitcode)
exit
}
```

Die Funktion rufen Sie mit *ExitWithCode -Exitcode 1641* auf und SCVMM startet die Maschine und bei Bedarf auch das Skript neu.

Wollen sie dann noch das Ganze ein wenig mehr in Richtung Self Service treiben, können sie zusätzlich noch den App-Controller installieren. Dieser ermöglicht den Zugriff auf den Service über ein Webportal, sodass die Service Templates bequem aus dem Web verwaltet werden können.

Fazit

In Kombination der vorgestellten Technologien und mit diesem Workshop sollten Sie in der Lage sein, sich Ihre eigene Desktop-Cloud zu bauen. Voraussetzung ist natürlich, dass sie entsprechende Rechenressourcen zu einer Cloud-Infrastruktur zusammengefasst haben. *(jp)*

Neuerungen in VMware vSphere 5.5

Der Platzhirsch schlägt zurück

von Bertram Wöhrmann

Mit dem Release der Version 5.5 hat VMware seinem Flaggschiff vSphere weit mehr als nur ein kosmetisches Update verpasst. Neben den deutlich angehobenen Maximalwerten für Host-RAM oder der VMFS-Dateigröße finden sich signifikante Verbesserungen bei der Storage- und Netzwerkanbindung des Hosts. Dazu kommt eine neue Hardwareversion und auch das Single Sign-On funktioniert endlich. Dieser Artikel stellt die Neuerungen vor.

Ende September stellte VMware mit leichter Verzögerung die Version 5.5 von vSphere vor und überraschte alle, die annahmen, dass nach den umfangreichen Änderungen in der Version 5.1 die neuen Features diesmal nur kosmetischen Charakter haben würden.

Zunächst aber ein Blick auf die maximal konfigurierbaren Werte in vSphere. Die Tabelle "Neue Maximalwerte in vSphere 5.5" greift die wichtigsten Änderungen zentraler Parameter auf. Und auch bei der vCenter-Appliance gibt es entsprechende Anpassungen, sodass dem Einsatz in größeren produktiven Umgebungen nichts mehr im Wege steht. So lassen sich mit einer internen DB nunmehr 100 Hosts und 3.000 VMs managen, mit einer externen Datenablage sogar 1.000 Hosts und bis zu 10.000 VMs.

Arbeitserleichterungen im Management

Lassen wir die nackten Zahlen im Rückspiegel und widmen uns den Neuerungen im Bereich des Managements, denn wie gewohnt wird der vCenter-Server zuerst installiert. Neben der Erhöhung der Maximalwerte haben sich noch weitere Änderungen ergeben. Die interne Datenbank liefert in der Appliance-Variante eine vPostgress-Instanz. Als externe DB wird nur noch Oracle unterstützt. Beim klassischen vCenter-Server arbeitet intern nach wie vor eine MS SQL Express-DB. Auch hier hat sich beim Support der externen Datenbanken eine Änderung ergeben, dieser beschränkt sich auf Microsoft- und Oracle-DBs. Die DB-Produkte von IBM stehen nicht mehr in der Liste der unterstützten Hersteller.

Der Zugriff auf das Management ist weiterhin über den C#-vSphere-Client und über den Web-Client möglich. Nach wie vor integriert VMware alle neuen Funktionen nur noch in den Web Client. Für den direkten Zugriff auf einen Host wird der C#-Client aber weiterhin benötigt. Plattformunterstützung bei den Clients gibt es nun offiziell für alle Betriebssysteme, von Windows über Linux bis Mac OS X. Die Liste der unterstützten Browser erstreckt sich vom Microsoft Internet Explorer über Mozilla Firefox bis hin zu Google Chrome.

Der Web-Client hat drei zusätzliche erwähnenswerte Funktionen, die das Handling vereinfachen sollen. Mit der Unterstützung für Massenaktionen können nun mehrere Objekte gleichzeitig aus dem mittleren Bereich des Web-Clients in andere Bereiche verschoben werden, um so Aktionen an Objekten auszuführen. Ein Anwendungsbeispiel ist das gleichzeitige Verschieben von virtuellen Maschinen auf einen anderen Host mit der vMotion-Funktion. Aber auch andere Massenak-

Neue Maximalwerte in vSphere 5.5

	Bisheriger Maximalwert	Maximalwert in vSphere 5.5
Host RAM	2 TByte	4 TByte
Logische CPUs pro Host	160	320
NUMA Nodes pro Host	8	16
vCPUs pro Host	2.048	4.096
vCPUs pro Core	25	32
VMs pro Host	512	512
Filegröße auf vmfs	2 TByte	64 TByte

tionen sind unterstützt – beispielsweise die Konfiguration von Netzwerken.

Eine sehr mächtige Funktion sind die neu hinzugekommenen Filter. Diese sollen helfen, in großen Umgebungen auf einfachem Wege Objekte schneller in die Ansicht zu bekommen, die für die aktuelle administrative Aufgabe benötigt wird. Über die De- beziehungsweise Aktivierung von Auswahlkriterien lässt sich die Ansicht anpassen und der Administrator findet so wesentlich schneller die gesuchte Gruppe etwa von virtuellen Maschinen.

Eine weitere Neuerung, die eine Erleichterung der Arbeit bringen soll, sind die "Recent Items". Hierbei wird im Web-Client eine Liste angelegt, in der ein direkter Zugriff auf die Objekte möglich ist, mit denen in letzter Zeit gearbeitet wurde. Denn erfahrungsgemäß beschränkt sich die Administration häufig auf wenige Komponenten und somit erfolgt der Zugriff schneller.

Mächtige neue Netzwerk-Features

Der Host erfährt vor allem Erweiterungen für Netzwerk und Storage. Mit dem "Mellanox ConnextX-3 VPI-Adapter" im Ethernet-Modus wird der erste Netzwerkadapter unterstützt, der einen Durchsatz von 40 GBit anbietet, weitere werden folgen. Den IPv6-Support hat VMware ebenfalls ausgebaut, aber es gibt noch zwei Komponenten, die noch nicht "IPv6 Ready" sind: der Syslog-Server und die Auto Deploy-Funktion. Hier muss VMware noch nachbessern, denn diese Erweiterungen benötigen zwingend eine IPv4-Adresse.

Eine Unterstützung für das Link Aggregation Control Protocol (LACP) besteht seit der letzten Version, ist aber in 5.5 stark erweitert worden. So sind weitere 22 Hashing-Algorithmen für das Load Balancing an dieser Stelle integriert worden. Ansatzpunkt für die neuen Load Balancing-Berechnungen sind die Quell- und Ziel-IP-Adresse beziehungsweise die VLAN-ID. Insgesamt ist es möglich, bis zu 64 Link Aggregation Groups (LAG) pro Host und Virtual Distributed Switch (VDS) zu erstellen. Die Konfiguration der LAGs pro Host macht die Arbeit zeitintensiv und

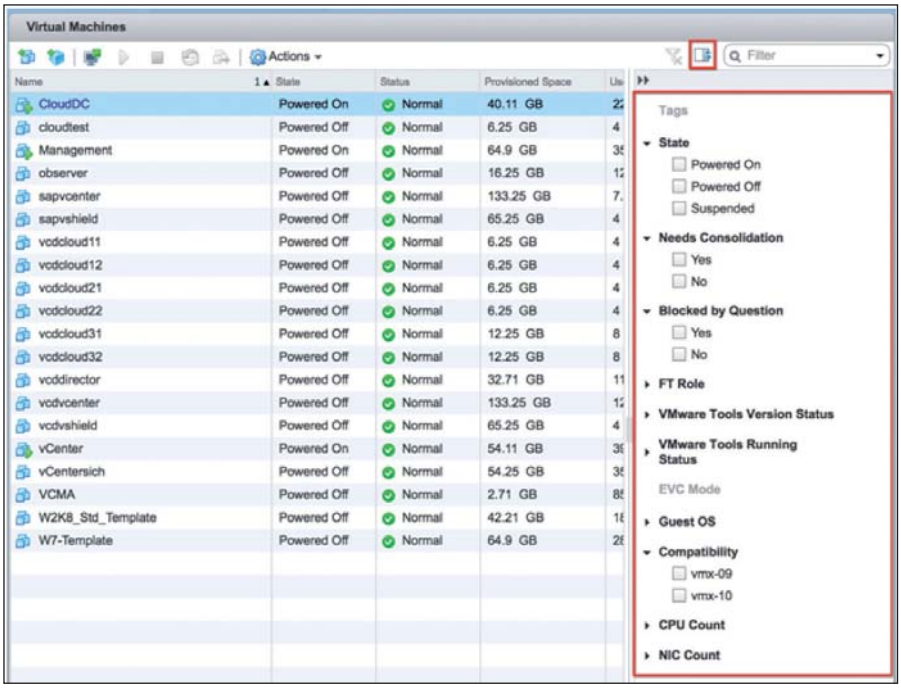


Bild 1: Durch die Filter im Web-Client lässt sich sehr viel schneller auf Objekte in vSphere zugreifen

fehleranfällig. Hier gibt VMware dem Administrator ein Hilfsmittel mit auf den Weg: Über einen Workflow kann der IT-Verantwortliche Templates erstellen, die es wiederum ermöglichen, mehreren Hosts identische LAG-Konfigurationen mitzugeben. Damit die LAGs in der virtuellen Maschine genutzt werden können, muss eine Konfiguration an drei Stellen hinterlegt werden. Am Anfang steht der Uplink am Host mit dem dazugehörigen physikalischen Switch. Der folgende Konfigurationspunkt ist die Portgruppe am VDS. Die abschließende Konfiguration wird dann an der virtuellen Maschine vorgenommen. So ist ein Durchreichen der LAG bis in die unterste Ebene gewährleistet.

Filtering ist im klassischen Netzwerkumfeld schon lange Standard. Diese Option steht Administratoren nunmehr auch auf dem VDS zur Verfügung. Das Filtering erfolgt direkt an der Portgruppe und die Nutzung von Access Control Lists (ACL) erhöht die Sicherheit auf Portebene. Der Netzwerkverkehr lässt sich auf Basis von drei unterschiedlichen Parametern klassifizieren. Zuerst sind hier die MAC-Adressen zu nennen, gefolgt von den IP-Adressen mit den zugehörigen IP-Ports. Selbstverständlich kann in beiden Fällen mit den Quell- und/oder Zieladressen gearbeitet werden. Letztes Klassifizierungsmerkmal ist der System-Datenverkehr. Dieser wird vom System erkannt und lässt sich ebenfalls absichern. System-Datenverkehr beschreibt alle netzwerkbasierten Datenpakete, die für die Funktion des Hosts beziehungsweise die Funktion seiner Erweiterungen genutzt werden wie Management, vMotion, Fault Tolerance et cetera. Die Flussrichtung schränkt an dieser Stelle nicht ein, weil ein- beziehungsweise ausgehender Datenverkehr verwaltet werden kann. Auch sind beide Flussrichtungen gleichzeitig einschränkbar.

Auch Quality of Service (QoS) hat Einzug im VDS gehalten. Das QoS setzt dabei auf den Ebenen 2 und 3 des OSI-Schichtenmodells an. Definiert werden die Technologien im Standard 802.1p. Im Datenpaket finden sich drei Bit im VLAN-Abschnitt, die dessen Priorität steuern. Die Werte null bis sieben definieren dabei unterschiedliche Anforderungen des Datenpakets hinsichtlich der Priorisierung. Je höher der Wert, desto höher ist auch die Priorität des Datenpakets. Eine ähnliche Funktion gibt es auch im Layer 3: Hier nutzt VMware sechs Bit, um dem Netzwerkpaket beim Verlassen des Systems eine Priorisierung mitzugeben. Der Code unterteilt sich in zwei 3 Bit-Blöcke. Der erste Block gibt an, wie hoch die Wahrscheinlichkeit eines Paketverlustes ist, und der zweite trifft eine Aussage über die Paketpriorität. Logischerweise erfolgt die Konfiguration an der Portgruppe.

Mit der Single-Root I/O Virtualization (SR-IOV) können physikalische Netzwerkkarten direkt in eine virtuelle Maschine gemappt werden. Das bringt vor allem dann Vorteile, wenn eine Applikation eine hohe Netzwerklast erzeugt. So lässt sich verhindern, dass eine virtuelle Maschine keinen Freiraum mehr für andere VMs im Netzwerk lässt. SR-IOV unterstützt Karten mit Chipsätzen von Emulex und Intel. Pro Host kann aber nur eine Karte weitergereicht werden, sie muss dabei dem PCIe-Standard entsprechen. Die Konfiguration erfolgt an einer Portgruppe mit allen gewünschten Einstellungen und diese werden dann an die VM weitergeleitet, wenn sie für diese Art der Kommunikation freigeschaltet wird.

Mittlerweile hat VMware schon einige Funktionen bereitgestellt, die ein Troubleshooting im Netzwerkbereich unterstützen sollen: Netzflusskontrolle und Portspiegelung, die im Laufe der Zeit durch den Switched Port Analyzer (SPAN), den Remote Switched Port Analyzer (RSPAN) und den Encapsulated Remote Switched Port Analyzer (ERSPAN) ergänzt worden sind. Mit vSphere 5.5 hat das erweiterte Netzwerkanalyse-Tool Einzug gehalten, das auf Host-Ebene ansetzt. VMware hat sich bei der Entwicklung des Tools am tcpdump-Befehl von Linux orientiert. Die Analyse kann dabei an drei Punkten erfolgen: am Uplink, am Switchport und am vNIC der virtuellen Maschine. Es ist dabei nicht von Interesse, ob die Landschaft mit VDS- oder VSS-Switchen konfiguriert wurde, beide Varianten werden unterstützt. Verlorene Pakete können ebenso gesammelt werden wie übermittelte Pakete. Zeitstempel helfen zudem, den Zusammenhang beim Laufweg genau abzubilden.

Reduzierter Speicherbedarf für VMs

VMware hat in den Vorversionen eine Funktion programmiert, die es ermöglicht, dass mit einer großen Menge von offenen Files gearbeitet werden kann. Mit der steigenden Anzahl an virtuellen Maschinen erhöhte sich auch die Anzahl offener Files und somit stieg auch der Speicherbedarf des Hypervisors für deren Verwaltung. Mit der Unterstützung der neuen Speichergrößen musste der Mechanismus geändert werden, damit das System moderater mit dem Arbeitsspeicher umgeht. Die Neuausrichtung hat dazu geführt, dass der Speicherbedarf für die Verwaltung offener Dateien von 640 MByte auf 256 MByte pro Datastore reduziert werden konnte. Mit dem Erfolg, dass 64 TByte offene Dateien erfolgreich vom System verwaltet werden können.

Weitere Unterstützung kommt durch optimierte Erkennungsprozesse, ob Datastores Probleme haben oder nicht ordnungsgemäß entkoppelt worden sind. Hier schafft das System schnell Klarheit und sorgt dafür, dass I/O-Datenströme nicht in einen Kanal laufen, der nicht mehr existent oder defekt ist. Die Funktion trägt den Namen Permanent Device Loss Auto-Remove (PDL AutoRemove). Eine Optimierung hat auch die VAAI-Komponente erfahren. Hier traten bislang zeitweise Unstimmigkeiten im Zusammenhang mit dem Thin Provisioning auf. Mit dem Befehl *# esxcli storage vmfs unmap* ist es möglich, Festplattenplatz zur weiteren Verwendung an den Host zurückzugeben. Letztendlich versucht das System, eine temporäre Datei mit den vakanten Blöcken anzulegen. Ist das möglich, werden die Blöcke an den Host freigegeben. Früher gab es hier aber zahlentechnische Differenzen. Nicht selten hat der Host andere Freistände angezeigt als der Storage. Dieser Missstand ist in der aktuellen Version behoben. Wurde der Schwellenwert früher in Prozent angegeben, so erwartet das System nun eine Blockgröße.

Für diejenigen, die Microsoft Cluster-Dienste auf einem VMware-Hypervisor einsetzen, gibt es auch positive Nachrichten. Nicht nur, dass es Support für MSCS unter Windows 2012 gibt, es werden auch iSCSI- und FCoE-Anbindungen für den Shared-Storage unterstützt. FibreChannel steht selbstverständlich auch noch in der HCL für diese Funktion. Das Load Balancing mit dem Round Robin-Verfahren hat eine Optimierung erfahren. War es früher notwendig, dass die SCSI-Reservierungen immer über den ersten Pfad an den Shared-Storage weitergeleitet werden, so ist der genutzte Pfad nun nicht mehr relevant.

Neue Hardwareversion bringt erweiterte SATA-Unterstützung

Änderungen haben sich auch an den virtuellen Maschinen ergeben und zwar weit mehr als die zuvor aufgelistete größere Parametrierbarkeit. Mit vSphere 5.5 geht auch eine neue virtuelle Hardwareversion an den Start. Alle VMs seit der Hardwareversion 4 können nach wie vor auf vSphere 5.5 betrieben werden. Somit ist garantiert, dass die Aktualisierung einer Landschaft von der Version 3.x nach 5.5 ohne vorherige Anpassung der Hardwareversion möglich ist. Jedoch existiert beim Host kein direkter Weg von 3.x nach 5.5 – hier muss der Administrator bei einer Aktualisierung ein Zwischenweg gehen. Eine Neuinstallation ist aber bei weitem nicht so zeitintensiv wie die schrittweise Aktualisierung.

Mit der HW-Version 10 finden neue CPU-Architekturen sowie aktuelle AHCI-Funktionen Unterstützung. Neu ist auch der LSI SAS-Support für Oracle Solaris 11. In den Eigenschaften der VM findet sich auch ein neuer Controller für SATA-Geräte, von denen sich nun bis zu 30 pro Controller anschließen lassen. Bei einer Maximalausstattung von vier Controllern ergibt sich eine theoretische Menge von 120 SATA-Geräten in einer VM. Bei den Grafikfunktionen hat VMware besonders an der 3D-Fähigkeit gearbeitet. Die Liste der unterstützten GPUs hat sich um die Chiphersteller Intel und AMD erweitert. Ein Rendering ist direkt auf der Hardware der Grafikkarte oder als Softwareemulation möglich.

Trotz der hart ins System eingreifenden Funktion können die virtuellen Maschinen mit vMotion über die Hosts verschoben werden. Nicht alle Betriebssysteme unterstützen derzeit diese Funktion. Einwandfrei können Windows 7 und Windows 8 mit der Funktion umgehen sowie die Linux-Dialekte Fedora 17 und höher, RHEL 7 und Ubuntu 12.04 und neuer. Es ist davon auszugehen, dass sich die Liste mit der nächsten Version verlängern wird.

Fehler in der Replikation beseitigt

Viele Teilkomponenten von vSphere haben ebenfalls signifikante Änderungen

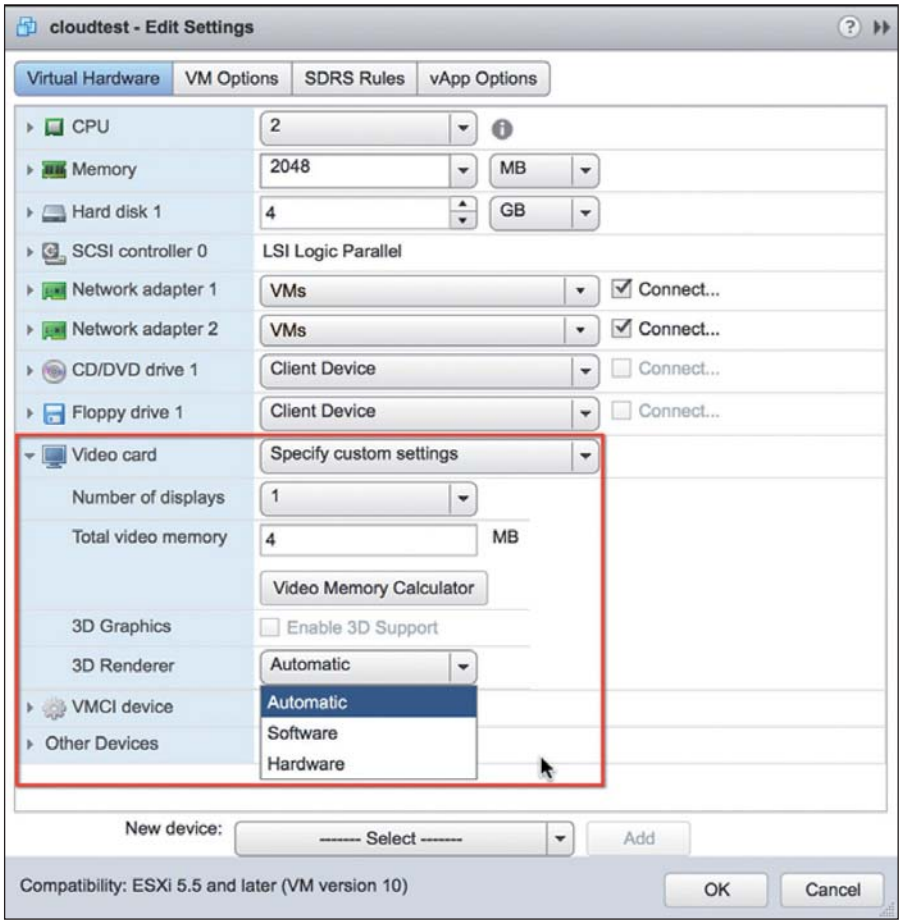


Bild 2: Die neuen Grafikeinstellungen einer VM in vSphere 5.5 zielen insbesondere auf optimierte 3d-Funktionalität

erfahren. Als Erstes sei vSphere Replication erwähnt. Früher gab es Situationen, in denen eine Neuerstellung des Replikats erfolgte, obwohl es aus Anwendersicht eigentlich nicht notwendig war. Mit vSphere 5.5 hat der Hersteller diese Ausreißer eliminiert. Ursache war das Verschieben der primären VM mit Storage vMotion auf einen anderen Data-store. Funktionierte das beim Verschieben einer einzelnen Disk noch gut, so wurde beim Verschieben der gesamten VM letztendlich deren Home-Verzeichnis sowie das Reporting-File für die Replikation gelöscht. Dies war die Ursache für die komplette Neureplikation. Nun sind auch Storage DRS und Storage vMotion kein Problem mehr, weder auf der primären noch auf der sekundären Seite. Das Replikationsziel hatte mit Storage DRS kein Problem, weil dort nur virtuelle Disks liegen und keine VMX-Files. Die VMDK-Dateien sind für das DRS keine VMs und werden somit keiner näheren Betrachtung für eine Verlagerung unterzogen.

Der Replikationsprozess als solches ist wesentlich verbessert worden. Wurden früher bei Replikationen die redo-Logdateien nach erfolgtem Schreiben sofort gelöscht, so werden sie nun länger behalten. Löschbasis für die Dateien ist die Retention Policy. Erst wenn diese greift, wird die betroffene Logdatei gelöscht. Ein einfaches Beispiel soll das verdeutlichen: Sollen 24 Snapshots behalten werden und liegt eine Recovering Point Objective (RPO) von 60 Minuten vor, so werden 24 Replikas neben den 24 Snapshots aufbewahrt. Ist die RPO kürzer, bleiben dem System entsprechend mehr Replikate erhalten. Die Anzahl der Snapshots ändert sich in dem Fall nicht.

Evolution des Backup

Die Datensicherungslösung von VMware hat sich ebenfalls leichten Änderungen unterziehen müssen. Die kosmetischen Korrekturen betreffen die Installation. Es gibt nur noch eine Appliance für alle Datensicherungsmengen. Erst bei der Konfiguration wird der benötigte Plattenplatz zugewiesen, das sind weiterhin 0,5, 1 oder 2 TByte. Größere Datenmengen können nur mit der kostenpflichtigen Version von VMware gesichert werden, dem vSphere Data Protection Advanced. Die Lizenzierung erfolgt auf Basis der Anzahl der CPUs.

Außer komplette VMs kann das System nun auch einzelne Disks sichern. Rücksicherungsziel kann jetzt auch direkt ein Host sein. Es lassen sich dedizierte Startzeiten für die Jobs hinterlegen. Also hat dieses Mal nicht schon wieder eine andere Version Einzug gehalten, sondern die bestehende wurde erweitert und verbessert.

Neue Funktionen in vSphere 5.5

Eine vollständig neue Funktion stellt "AppHA" dar, die das Virtual Machine Monitoring signifikant erweitert. Die Erweiterung besteht aus der AppHA-Appliance, der vFabric Hyperic-Appliance und dem AppHA-Agenten. Der Agent wird in die zu überwachende virtuelle Maschine installiert und kommuniziert mit dem Framework. In einer Policy hinterlegt der IT-Verantwortliche, wie das System im Falle eines auftretenden Dienstefehlers reagieren soll. Neben dem Neustart des Dienstes besteht auch die Option, die VM neu zu booten. Dabei wird dem System noch mitgeteilt, welche Aktion wie oft wiederholt werden soll. Informationen zu erfolgten Aktionen lassen sich direkt in die vCenter-Alarme integrieren oder es wird automatisch eine Benachrichtigungs-E-Mail versendet. Die DRS-Regeln werden hier nicht ausgehebelt, sie sind voll unterstützt. Dabei spielt es auch keine Rolle, ob es sich um "affinity"- oder "antiaffinity"-Regeln handelt.

Zur Optimierung der Laufstabilität des Hypervisors erfolgte die Integration der Reliable Memory-Funktion. Ein vSphere-Hypervisor läuft komplett im Arbeitsspeicher und nicht auf der Festplatte. Dadurch ist das System empfindlich für Speicherfehler. Reliable Memory sorgt nun dafür, dass Speicherbereiche identifiziert werden, die besonders stabil sind. In diesen Bereich werden zur Erhöhung der allgemeinen Stabilität die Laufzeitdaten des Hypervisors gelegt.

Immer mehr Funktionen zielen auf große Umgebungen und große virtuelle Maschinen ab. So auch die Big Data Extensions (BDE), die sich an Umgebungen wenden, die ein ähnliches Funktionsprinzip haben wie etwa Facebook, Google, AOL oder HTW Chur. Mit BDE lassen sich sogenannte Hadoop-Cluster auf vSphere-Basis installieren.

Die Funktion, die es erlaubte, lokale SSD-Platten als Ziel für die Swap-Dateien zu verwenden, löst VMware durch den Flash-Read-Cache ab. Beim diesem werden lokale SSD-Platten als I/O-Cache in den Datenstrom der virtuellen Festplatte integriert, um so die Operationen puffern und damit beschleunigen zu können. Die virtuelle Maschine sieht diesen Cache nicht, er wird voll transparent in den Datenpfad eingehängt. Der Cache kann dabei aus einer oder mehreren SSD-Platten bestehen. Im letzteren Fall werden die Disks zu einem Pool zusammengefasst. Die Einrichtung in der VM erfolgt pro virtueller Festplatte.

Eine der größten Änderungen hat die Single Sign-On-Funktion erfahren. Hier hat VMware massiv neu programmiert, damit die Funktion sich besser integrieren lässt und eine gute Skalierbarkeit gegeben ist. In der Knowledge Base von VMware finden sich so viele Artikel zu Problemen mit SSO, das mit der Version vSphere 5.1 vorgestellt wurde, dass ein Redesign unumgänglich war. Nicht funktionierende Aktualisierungen inklusive händischen Eingriffen an der Installation beziehungsweise der Datenbank gehören so hoffentlich der Vergangenheit an. Voraussetzung dafür ist selbstverständlich eine reibungslose Migration zur neuen Version. Eine eingebaute Replikationsfunktion erleichtert nun auch die Verteilung der Daten zwischen SSO-Systemen an unterschiedlichen Standorten.

Lizenzen und Preise unverändert

Bei so vielen neuen Funktionen stellt sich natürlich die bange Frage, was mit den Lizenzen und den damit verbundenen Kosten passiert. Denken wir zurück an die Veröffentlichung der Version vSphere 5.0, werden diesbezüglich nicht gerade positive Erinnerungen wach. Doch dieses Mal hat VMware die Füße still gehalten und die Grundzusammensetzung der Produktpakete ebenso wenig geändert wie den Preis.

Weiterhin gibt es die Standardpakete VMware vSphere Standard, Enterprise und Enterprise Plus. Die Limitierungen hinsichtlich der Größe der VMs beziehungsweise der Anzahl der nutzbaren Cores sind aufgehoben. Die neuen Funktionen Reliable Memory und Big Data Extensions finden sich auch in der Enterprise Version. AppHA und Flash-Read-Cache sind der Enterprise Plus-Version vorbehalten.

Die Essential Kits haben sich nicht verändert – auch die Einschränkung auf maximal drei Server mit nicht mehr als zwei CPUs ist geblieben. Hinzu gekommen ist nun noch eine Version mit der Storage Appliance von VMware. Bei dem Management Produkt von VMware, dem vCenter Server, gibt es weiterhin zwei unterschiedliche Versionen, die Foundation und die Standard Version.

Wie schon erwähnt, hat sich das Pricing nicht geändert, aber es gibt neue Produktzusammenfassungen, die der Optimierung der angestrebten Anwendung dienen sollen. Hier sei VMware vSphere mit Operation Management genannt. Diese Version gibt es als Standard, Enterprise und Enterprise Plus. Zur Optimierung des Einstiegs bietet VMware hier noch sogenannte Acceleration Kits an. Diese beinhalten sechs CPU-Lizenzen der entsprechenden Version und eine Lizenz für den vCenter Server Standard.

Weiterhin stellt VMware eine freie Version der Software zum Download bereit. Das Produkt nennt sich VMware vSphere Hypervisor und kommt mit funktionalen Einschränkungen daher. Pro virtueller Maschine lassen sich nur acht vCPUs nutzen. Die Limitierung auf eine maximale Anzahl von Cores beziehungsweise CPUs ist ebenso aufgehoben worden wie die Begrenzung auf maximal 32 GByte Arbeitsspeicher. Ein zentrales Management wird bei dieser Version aber nicht unterstützt.

Fazit

Die Liste der neuen Funktionen ist mit vSphere 5.5 länger als bei der letzten Version und dort waren die Neuerungen schon sehr zahlreich. Auch wenn nicht jede Funktion für jeden Anwender von Nutzen sein wird, so ist eine Aktualisierung doch sehr zu empfehlen. Das schließt die Nutzer genauso ein, die noch mit wesentlich älteren Versionen arbeiten, wie diejenigen, die sich schon die ein oder andere blutige Nase beim SSO oder anderswo eingefangen haben. Es ist gut investierte Zeit und wird die Stabilität der Landschaft erhöhen. Einen guten Rat möchten wir Ihnen aber zum Abschluss noch geben: Bitte behalten Sie stets die HCL im Auge. *(jp)*

IT-Administrator Sonderhefte

Jetzt im Online-Kiosk kaufen oder per Vorbestellung sichern!

Je 180 Seiten geballtes Wissen zu:

Abonnenten erhalten Sonderhefte zum Vorzugspreis!

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

Migration von Exchange 2007/2010 auf Exchange 2013 (3)

Öffentliche Ordner im Galopp

von Christian Schulenburg


Quelle: vasilkovv – 123RF

In den ersten beiden Teilen der Workshopserie haben wir die Umgebung eingerichtet und die Postfächer auf den neuen Exchange 2013-Server verschoben. Im letzten Teil der Serie befassen wir uns intensiv mit der Migration der Öffentlichen Ordner, die sich im Gegensatz zu vorangegangenen Migrationen vollständig verändert hat. Abschließend gehen wir auf die Deinstallation des alten Exchange-Servers ein.

Zum Start der Migration liegen bereits alle Benutzer-Postfächer auf dem Exchange 2013-Server, über den auch der gesamte E-Mailverkehr läuft. Der Zugriff auf die Öffentlichen Ordner erfolgt zum Zeitpunkt der Koexistenz von Exchange 2013 auf Exchange 2007/2010. Öffentliche Ordner bestehen auf dem neuen Server bisher nicht. Vorneweg sei darauf hingewiesen, dass es für die Migration der Öffentlichen Ordner keinerlei grafische Oberfläche gibt und dieser Teil des Workshops sehr PowerShell-lastig ist. Bevor es aber losgeht, noch kurz zu den Änderungen in den Öffentlichen Ordnern unter Exchange 2013. Mit diesem Hintergrundwissen können Sie den Aufbau der neuen Strukturen besser planen.

Aufbau der Öffentlichen Order

Eigentlich sollte es die Öffentlichen Ordner bereits mit Exchange 2010 nicht mehr geben. Der Protest war aber zu groß, sodass sie in Exchange 2010 wieder integriert wurden und mit Exchange 2013 eine komplette Überarbeitung erhalten haben. In Exchange 2013 wurde die neue Postfach-Kategorie "Öffentliche Ordner-Postfächer" eingeführt – auf Öffentliche Ordner-Datenbanken wird komplett verzichtet. Die Postfächer liegen nun ebenfalls in den Postfachdatenbanken und die Hochverfügbarkeit wird über die Database Availability Groups (DAG) gewährleistet. Die Replikation von Öffentlichen Ordnern über verschiedene Datenbanken findet somit nicht mehr statt.

Damit ist aber auch klar, dass es kein Multimaster-Modell mehr gibt und nur noch ein beschreibbarer Öffentlicher Ordner existiert. Hier beginnt nun die Schwierigkeit bei Organisationen mit verschiedenen Standorten: Ließen sich Öffentliche Ordner bei Exchange 2007/2010 einfach replizieren und möglichst dicht zum User bringen, kann es unter Exchange 2013 vorkommen, dass der Zugriff über Standorte hinweg erfolgt. Um diesem Verhalten entgegenzuwirken, ist es enorm wichtig, die Struktur der Öffentlichen Ordner genau zu kennen und die Ordner so auf die Öffentlichen Ordner-Postfächer aufzuteilen, dass die primär genutzten Ordner in einer Datenbank am lokalen Standort liegen.

Exchange 2013 unterscheidet zwischen Hierarchiepostfächern, die eine beschreibbare Kopie der Öffentlichen Ordner-Struktur halten, und den Inhaltspostfächern, die den Inhalt führen und eine Lesekopie der Struktur enthalten. Änderungen an der Struktur, etwa das Anlegen neuer Ordner, werden immer an das Hierarchiepostfach weitergeleitet und zu allen Öffentliche Ordner-Postfächern repliziert. Sollte sich ein Ordner nicht in dem aktuellen Postfach befinden, erfolgt eine Weiterleitung an das Postfach mit dem Ordner.

Aus den Neuerungen leiten sich folgende Empfehlungen ab:

1. Sie sollten die Öffentlichen Ordner weiterhin in einer eigenen Datenbank ablegen, um einen dedizierten Speicherbereich, zentrale Limits oder einen eigenen Server nutzen zu können.
2. Sie sollten zwischen dem Hierarchie-Postfach und den Inhaltspostfächern unterscheiden, auch wenn Sie das Hierarchie-Postfach ebenfalls als Inhaltspostfach nutzen können.
3. Für die Öffentliche Ordner-Postfächer werden im Active Directory deaktivierte User angelegt. Die erstellten Objekte sollten Sie in einer eigenen Organisationseinheit anlegen, damit Sie nicht versehentlich einer Löschaktion zum Opfer fallen.

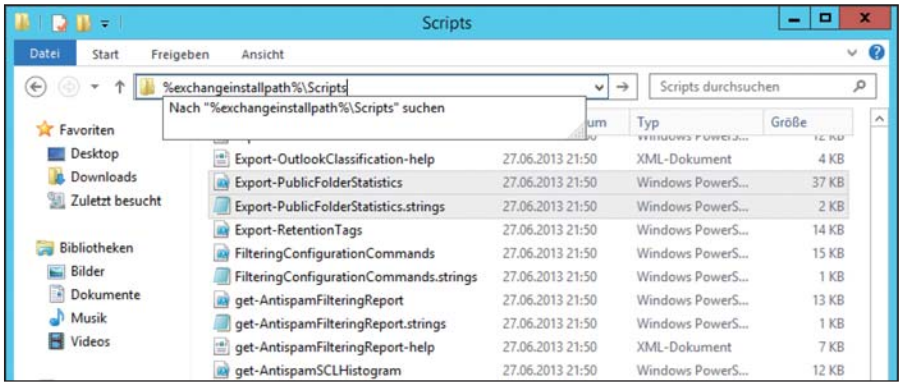


Bild 1: Für die Migration der Öffentlichen Ordner erforderliche Skripte finden Sie im Exchange-Skript-Verzeichnis auf dem neuen Exchange-Server

Details zur Arbeit mit Öffentlichen Ordnern können Sie im IT-Administrator unter anderem hier [1] nachlesen.

Bestandsaufnahme als erster Schritt

Um am Ende der Migration die Konfiguration und die Umsetzung zu verifizieren, sollten Sie am Anfang eine Bestandsaufnahme der Öffentlichen Ordner am Exchange 2007/2010-Server erstellen. Mit den folgenden Befehlen dokumentieren Sie sowohl statistische Informationen als auch die Berechtigungen auf die einzelnen Ordner in verschiedenen CSV-Dateien:

```
Get-PublicFolder -Recurse | Export-
  CSV D:\PF\2010_PFStruktur.csv
  -NoTypeInformation
Get-PublicFolder -Recurse |
  Get-PublicFolderStatistics |
  Export-CSV D:\PF\2010_PFStatis-
  tics.csv -NoTypeInformation
Get-PublicFolder -GetChildren | Get-
  PublicFolderClientPermission |
  Select Identity, User -Expand-
  Property AccessRights | Export-CSV
  D:\PF\2010_PFPerms.csv -NoType-
  Information
```

Die Befehle erstellen die Dateien im Ordner "D:\PF". Die Erweiterung "NoTypeInformation" führt dazu, dass die erste Zeile in der CSV-Datei mit den Spalteninformationen und nicht mit allgemeinen Informationen gefüllt wird. Das erleichtert die Weiternutzung in anderen Anwendungen. Sollten Sie mehr als 1.000 Öffentliche Ordner verwalten, müssen Sie die Befehle noch um die Erweiterung "-ResultSize Unlimited" ergänzen.

Achten Sie darauf, dass sich im Namen eines Öffentlichen Ordners kein Backslash befindet. In diesem Fall würde ein Ordner während der Migration an der falschen Stelle erstellt werden. Identifizieren Sie die Ordner mit Backslash über

```
Get-PublicFolderStatistics -Result-
  Size Unlimited | Where {$_.Name
  -like "*\*"} | fl Name, Identity
```

und benennen Sie diese um. Bevor die Migration startet, stellen Sie sicher, dass keine Rückstände einer vorangegangenen Öffentlichen Ordner-Migration vorhanden sind. Das Kommando dazu können Sie sowohl auf dem alten als auch auf dem neuen Exchange-Server ausführen:

```
Get-OrganizationConfig | fl
  PublicFoldersLockedforMigration,
  PublicFolderMigrationComplete
```

Sollten Sie ein "True" als Ergebnis erhalten, müssen Sie den Status mit *Set-OrganizationConfig* auf "False" zurücksetzen.

Bisher sind in unserem Workshop auf dem Exchange 2013-Server noch keine Öffentlichen Ordner vorhanden. Möchten Sie den neuen Server aber zur Sicherheit trotzdem noch einmal auf das Vorhandensein eines Öffentliche Ordnerpostfaches prüfen, nutzen Sie folgende Eingabe – in keinem Fall sollten Sie dazu eine Rückmeldung auf dem Exchange 2013-Server erhalten:

```
Get-Mailbox -PublicFolder
Get-PublicFolder
```

Bekommen Sie an dieser Stelle Öffentliche Ordner oder ein entsprechendes Postfach zurück, müssen Sie diese vor dem weiteren Vorgehen löschen. Eine aktuelle Migrationsanforderung sollte ebenfalls nicht vorliegen. Ist wider Erwarten ein Request vorhanden, löschen Sie diesen mit dem folgenden Befehl:

```
Get-PublicFolderMigrationRequest |
  Remove-PublicFolderMigrationRe-
  quest -Confirm:$false
```

Damit ist in der Organisation alles für die Migration bereit.

Brückenschlag mit Skripten vorbereiten

Die bisherigen CSV-Dateien haben wir zu Dokumentationszwecken angelegt. Im nächsten Schritt schaffen wir mit dem PowerShell-Skript *Export-PublicFolderStatistics.ps1* eine weitere Datei, die als Mapping-Grundlage zwischen der alten und neuen Struktur dient. Die Datei fungiert als Basis, um Öffentlichen Ordnern später in einer weiteren CSV-Datei Öffentliche Ordner-Postfächer zuzuweisen und in die neue Umgebung zu integrieren.

Das Skript liegt im Exchange-Skript-Verzeichnis des Exchange 2013-Servers. Am schnellsten finden Sie den Ordner über die Exchange-Variable. Geben Sie einfach im Explorer oder im Ausführen-Fenster wie in Bild 1 gezeigt die Variable *%ExchangeInstallPath%Scripts* ein. Kopieren Sie die beiden Dateien *Export-PublicFolderStatistics.ps1* und *Export-PublicFolderStatistics.strings.psd1* zum Exchange 2007/2010-Server und führen Sie die PS1-Datei dort aus. Definieren Sie während der Eingabe den Pfad, in dem Sie die CSV-Datei ablegen wollen, und geben Sie den FQDN des Servers an:

```
Export-PublicFolderStatistics.ps1
  D:\PF\PFmap.csv Ex2010.schulen-
  burg.lab
```

Eine kurze Zusammenfassung der gefundenen Ordner sehen Sie in der PowerShell. Die Datei selbst enthält die einzelnen Ordnernamen mit den entsprechenden Größen.

Als Nächstes weisen Sie jedem Ordner ein Öffentliche Ordner-Postfach zu. Hier-

bei geben Sie die maximale Größe eines Postfachs an und teilen die vorhandenen Ordner auf entsprechend viele Postfächer auf. In folgendem Beispiel soll ein Postfach eine maximale Größe von 300 MByte haben, wodurch die Ordner auf zwei Postfächer aufgeteilt werden.

Bevor Sie den Befehl *PublicFolderToMailboxMapGenerator.ps1* aus dem Skriptverzeichnis starten, kopieren Sie zunächst die zuvor erstellte CSV-Datei auf den Exchange 2013-Server. Geben Sie beim Ausführen die maximale Größe in Mbyte oder GByte sowie die entsprechende Quell- beziehungsweise Zieldatei an:

```
PublicFolderToMailboxMapGenerator.ps1
  300MB E:\PF\PFmap.csv
  E:\PF\PFmap2Mailbox.csv
```

Diese Mapping-Datei können Sie auch selbstständig erstellen und auf diesem Weg die Ordner gezielt Postfächern zuordnen. Organisationen mit verteilten Standorten müssen hier aktiv werden, um die Öffentlichen Ordner möglichst dicht am Benutzer abzulegen und die Bandbreiten zwischen Standorten nicht unnötig zu belasten. Gerade in verteilten Szenarien kommt diesem Schritt eine wichtige Rolle zu. Sie können die Datei selbst generieren und die Root-Ordner direkt mit Inhaltspostfächern verbinden. Ein ausführliches Beispiel finden Sie in einem Migrations-Guide für Öffentliche Ordner [2].

Anlegen der Postfächer

Im weiteren Vorgehen erstellen Sie nun die Öffentliche Ordner-Postfächer. Dabei müssen Sie darauf achten, dass das erste Postfach mit der Erweiterung "HoldForMigration" erstellt wird. Dadurch wird die Öffentliche Ordner-Hierarchie auf dem neuen Server gesperrt, sodass Clients keine Ordner erstellen können und weiterhin auf der alten Infrastruktur arbeiten.

Da das erste Postfach als Hierarchiepostfach eine besondere Funktion hat und sich dieses nicht verschieben lässt, sollten Sie das erste Postfach mit einem entsprechenden Namen anlegen. Hierfür nutzen Sie den folgenden Befehl:

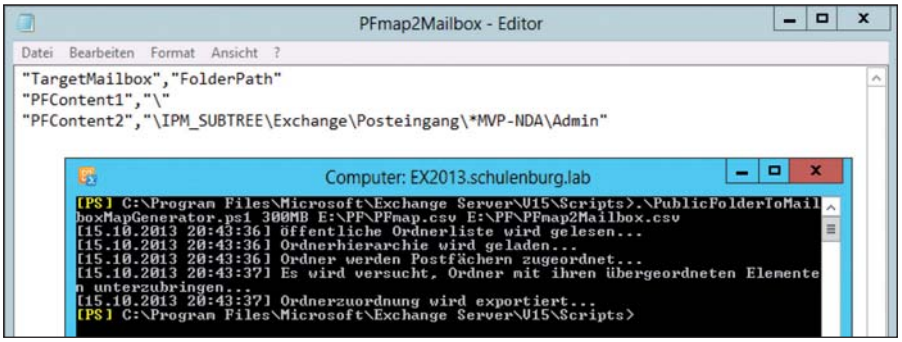


Bild 2: Mit dem Skript PublicFolderToMailboxGenerator weisen Sie die Ordner in der CSV-Datei einem Öffentlichen Ordner in der neuen Struktur zu

```
New-Mailbox -PublicFolder PFMaster-
  Hierarchy -HoldForMigration:$true
```

Legen Sie die Inhaltspostfächer der Öffentlichen Ordner losgelöst vom Hierarchiepostfach an. Das Hierarchiepostfach kann zwar auch den Inhalt aufnehmen, für die zukünftige Entwicklung sollten Sie die Funktionen aber separieren. Erstellen Sie die Inhaltspostfächer nach einer definierten Namenssyntax oder entsprechend der in der CSV-Datei definierten TargetMailbox. Weichen Ihre gewählten Name von der CSV-Datei ab, müssen Sie diese in der Spalte "TargetMailbox" anpassen.

Die zusätzlichen Postfächer legen Sie über *New-Mailbox -PublicFolder PFContent1* an. Das aktuelle Hierarchiepostfach können Sie sich jederzeit über

```
(Get-OrganizationConfig).Root-
  PublicFolderMailbox|fl
```

anzeigen lassen. Die GUID, die Sie über den Befehl erhalten, können Sie über

```
Get-Mailbox -PublicFolder |
  fl Name, ExchangeGuid
```

einem Postfach zuordnen. Beachten Sie, dass auch für die Öffentliche Ordner-Postfächer der Standardgrenzwert der Datenbank von 2 GByte gilt. Dies sollten Sie in der EAC in den Eigenschaften der Datenbank oder direkt am Postfach anpassen, da das Limit in den meisten Fällen etwas gering ist. Unter Exchange 2013 können einzelne Postfächer eine Größe von 100 GByte erreichen.

Start der Migration

Migrieren Sie von Exchange 2007, müssen Sie zunächst den BadItemCount über den folgenden Befehl anpassen:

```
$PublicFolderDatabasesInOrg=
  @(Get-PublicFolderDatabase)
  $BadItemLimitCount= 5 +
  ($PublicFolderDatabasesInOrg.Count-1)
```

Dieser Schritt ist nötig, da einige Systemordner sonst nicht erkannt und als ungültige Elemente behandelt werden. Als Nächstes starten Sie die Migrationsanforderung. Geben Sie dafür den alten Exchange 2007/2010-Server und die CSV-Datei mit den Zuordnungsdateien an:

```
New-PublicFolderMigrationRequest
  -SourceDatabase (Get-PublicFolder-
  Database -Server Ex2013) -CSVData
  (Get-Content E:\PF\PFmap2Mailbox.csv
  -Encoding Byte)
```

Ergänzen Sie bei Exchange 2007 noch das BadItemLimit mit *-BadItemLimit $BadItemLimitCount*. Die Migration wird im Anschluss in die Warteschlange eingereiht und Exchange erstellt im Hintergrund die nötigen Ordner und kopiert die Elemente.

Den aktuellen Status und weitere Details können Sie jederzeit über

```
Get-PublicFolderMigrationRequest |
  Get-PublicFolderMigrationRequest-
  Statistics
```

abfragen. Der Status wechselt von "Queued" über "InProgress" in den Status "AutoSuspended". Bis zum Erreichen des letzten Status kann je nach Größe etwas Zeit vergehen. Microsoft rechnet mit einem Fortschritt von zwei bis drei GByte je Stunde. Detailliertere Informationen zum Status erhalten Sie mit der Option

"IncludeReport" als Erweiterung von *Get-PublicFolderMigrationRequestStatistics*.

Kein Zugriff während des Umzugs

Die Ordner befinden sich nun auf dem neuen Exchange 2013-Server. Im letzten Schritt werden die Ordner auf dem alten Server gesperrt, ein letztes Mal synchronisiert und den Usern wieder zur Verfügung gestellt. Während des Vorgangs ist kein Zugriff auf die Öffentlichen Ordner möglich. Vom Erreichen des Status "AutoSuspended" bis zum Starten des letzten Migrationsschrittes kann auch wieder etwas Zeit vergehen. Dabei wird in der alten Öffentliche Ordner-Struktur weiter gearbeitet, wodurch sich der Inhalt zwischen alter und neuer Struktur über die Zeit immer stärker unterscheidet. Je größer der Unterschied, je länger dauert der letzte Migrationsschritt, da ein letzter Abgleich stattfindet. Um die Zeit dieses Schrittes weiter zu minimieren, ist es ratsam, die Strukturen vorab ein weiteres Mal über

```
Resume-PublicFolderMigrationRequest
  \PublicFolderMigration
```

zu synchronisieren. Nun werden die User von den Öffentlichen Ordnern abgemeldet und somit wird das Bearbeiten von Öffentlichen Ordnern gesperrt. Führen Sie den folgenden Befehl auf dem Exchange 2007/2010 Server aus:

```
Set-OrganizationConfig -Public-
  FoldersLockedForMigration:$true
```

Es beginnt die Downtime der Öffentlichen Ordner und es ist zu diesem Zeitpunkt kein Zugriff mehr möglich. Sollten sich im Netzwerk mehrere Öffentliche Ordner-Datenbanken befinden, müssen sich diese nun replizieren, damit alle über den gleichen Inhalt verfügen und die Datenbanken das Flag zur Sperrung übernehmen. Den letzten Punkt können Sie durch das Neustarten der Informationsspeicher auf den alten Servern beschleunigen. Auf die User hat dies keinen Einfluss, da sie sich bereits auf dem neuen Exchange-Server befinden.

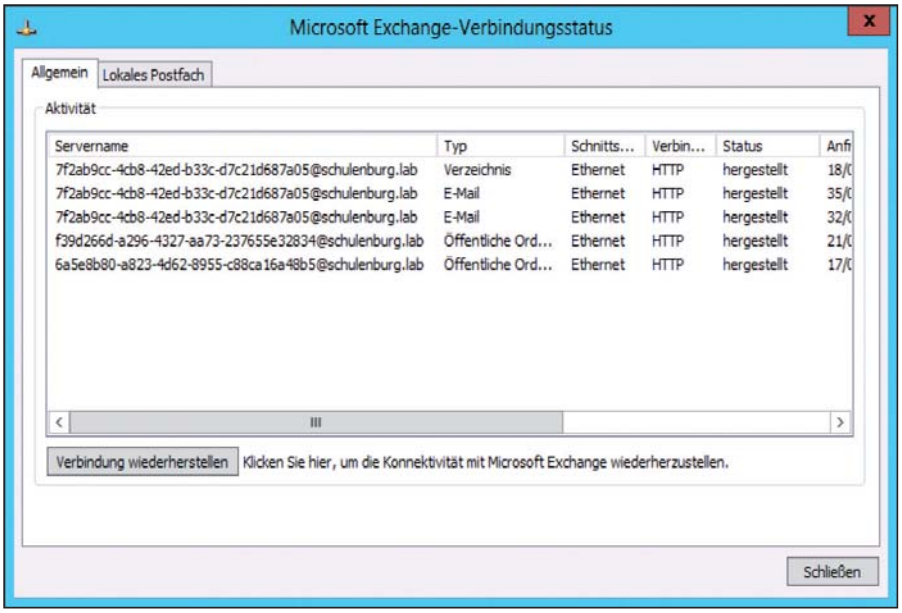


Bild 3: Im Outlook-Verbindungsstatus können Sie nach der Umstellung die GUID der Öffentliche Ordner-Postfächer beim Servernamen finden. Hier werden, wie auch im Outlookprofil, die GUIDs der Postfächer statt des Servers angezeigt.

Im nächsten Schritt heben Sie die Eigenschaft "PreventCompletion" der Migrationsanforderung auf und setzen die Migrationsanforderung fort. Führen Sie diese Schritte auf dem Exchange 2013-Server aus:

```
Set-PublicFolderMigrationRequest
  -Identity \PublicFolderMigration
  -PreventCompletion:$false
Resume-PublicFolderMigrationRequest
  -Identity \PublicFolderMigration
```

Ganz abschließen können Sie den Migrations-Request an dieser Stelle noch nicht, da wir die Hierarchie noch gesperrt haben. Abfragen können Sie den Status erneut über

```
Get-PublicFolderMigrationRequest |
  Get-PublicFolderMigrationRequest-
  Statistics.
```

Test auf der neuen Umgebung

Als Nächstes weisen Sie einem Benutzer-Postfach ein Standardpostfach für Öffentliche Ordner zu:

```
Set-Mailbox -Identity Administrator
  -DefaultPublicFolderMailbox
  PFContent1
```

Über Outlook oder OWA können Sie nun den Zugriff auf die Öffentlichen Ordner testen. Im Outlook sehen Sie im Verbindungsstatus, dass nun die neue Struktur genutzt wird (Bild 3). Sollte es an diesem Punkt Probleme geben, können Sie hier die Reißleine ziehen und die Struktur auf dem Exchange 2010-Server wieder verfügbar machen. Dadurch können Sie die Migration von vorne beginnen. Mehr dazu noch später im Verlauf des Artikels. Wenn alles fehlerfrei läuft, entsperren Sie die Öffentlichen Ordner auf Exchange 2013:

```
Get-Mailbox -PublicFolder |
  Set-Mailbox -Public Folder -IsEx-
  cludedFromServingHierarchy $false
```

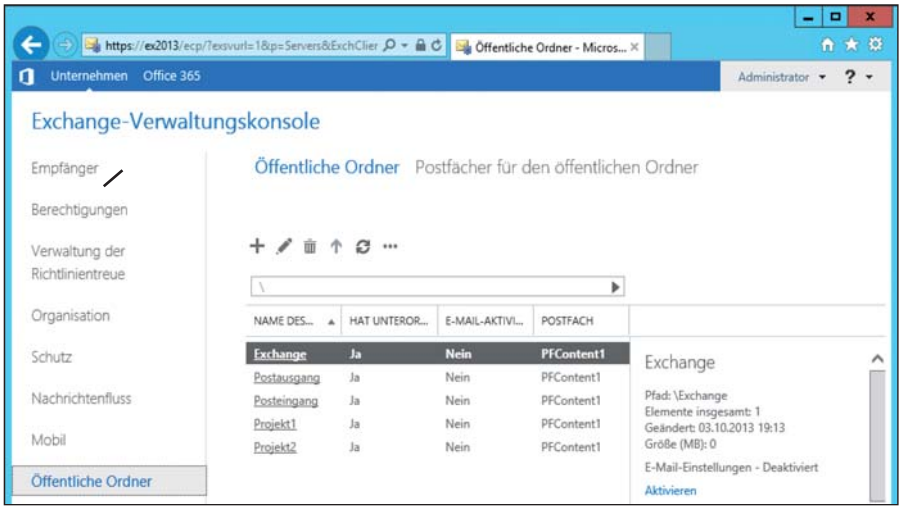


Bild 4: Nach dem Entsperren der Öffentlichen Ordner können Sie diese auch in EAC sehen und verwalten

Auf dem Exchange 2007/2010-Server setzen Sie die Migration im Anschluss auf den Status "Complete":

```
Set-OrganizationConfig -Public-
  FolderMigrationComplete:$true
```

Beim Prüfen des Migrations-Requests werden Sie feststellen, dass die Migration finalisiert und fertiggestellt wurde. Auch in der EAC sind die Öffentlichen Ordner nun zu finden. Ab jetzt können auch die User wieder uneingeschränkt auf die Öffentlichen Ordner zugreifen. Um die Öffentlichen Ordner auch inhaltlich zu prüfen, erstellen Sie erneut eine Momentaufnahme – dieses Mal aber von der neuen Struktur:

```
Get-PublicFolder -Recurse | Export-
  CSV D:\PF\2013_PFStruktur.csv
  -NoTypeInformation
Get-PublicFolder -Recurse | Get-Pu-
  blicFolderStatistics | Export-CSV
  D:\PF\2013_PFStatistics.csv
  -NoTypeInformation
Get-PublicFolder -GetChildren |
  Get-PublicFolderClientPermission |
  Select Identity, User -Expand-
  Property AccessRights | Export-CSV
  D:\PF\2013_PFPerms.csv
  -NoTypeInformation
```

Vergleichen Sie die verschiedenen CSV-Versionen, um Abweichungen festzustellen. Sind die Öffentliche Ordner-Strukturen etwas umfangreicher, leitet Sie ein Blog-Artikel [3] des Microsoft Exchange-Teams mit Access als Abgleich-Tool durch den Datenbestand.

Rolle rückwärts

Sollte es während der Migration Probleme geben, können Sie die Struktur auf dem Exchange 2007/2010-Server wieder aktivieren. Heben Sie hierfür die Sperre auf und setzen Sie den Migrationsstatus auf "$false" zurück:

```
Set-OrganizationConfig -Public-
  FoldersLockedforMigration $False
  -PublicFolderMigrationComplete
  $False
```

Löschen Sie zusätzlich die Öffentlichen Ordner-Postfächer und beginnen Sie die Migration von vorne – nach den folgenden Schritten haben Sie wieder den Ausgangszustand erreicht:

```
Get-Mailbox -PublicFolder |
  Where{$_.IsRootPublicFolderMailbox
  -eq $false} | Remove-Mailbox
  -PublicFolder -Force
  -Confirm:$false
Get-Mailbox -PublicFolder | Remove-
  Mailbox -PublicFolder -Force
  -Confirm:$false
Get-PublicFolderMigrationRequest |
  Remove-PublicFolderMigration-
  Request -Confirm:$false
```

Exchange deinstallieren

Als letzter Schritt der Exchange-Migration steht nun an, den alten Server aus der Organisation zu entfernen. Sicherheitshalber können Sie Exchange 2007/2010 noch etwas mitlaufen lassen oder nur herunterfahren, um das Verhalten weiter zu beobachten.

Haben Sie sich für das endgültige Entfernen des alten Servers entschieden, sollten Sie den Server richtig deinstallieren und nicht einfach nur ausschalten und aus dem Rack herausnehmen. Exchange speichert seine Konfiguration im Active Directory, und nur über die Deinstallation

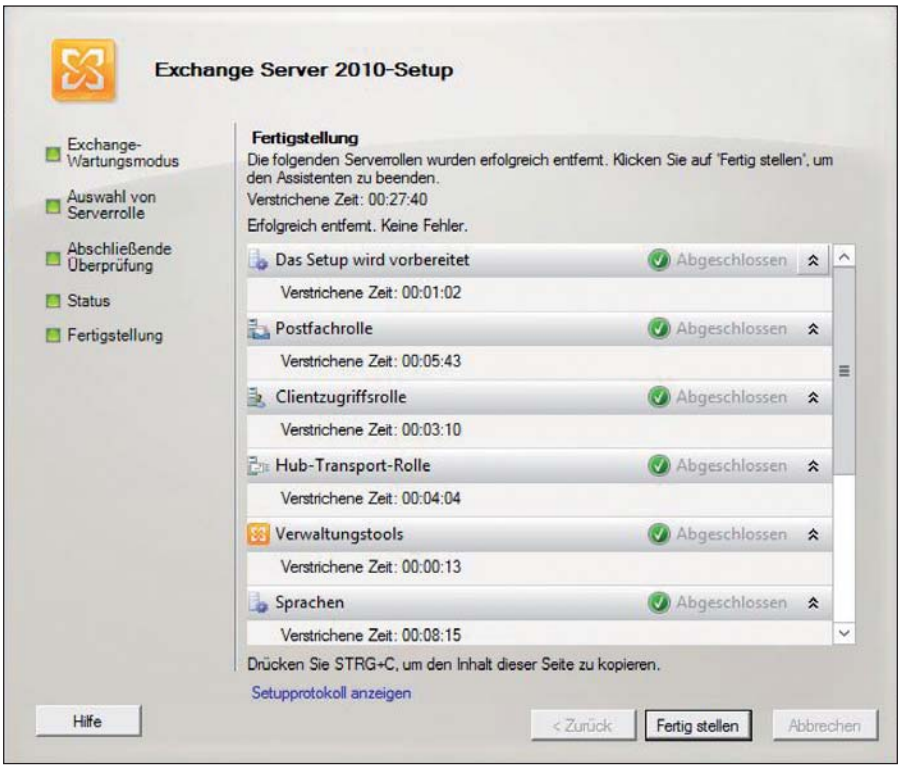


Bild 5: Die Deinstallation des Exchange 2007/2010-Servers sollte am Ende einer erfolgreichen Migration stehen

PowerShell-Befehle für die Migration Öffentlicher Ordner	
Umgebung prüfen und Vorbereitungen	
Offene Migrations-anforderungen ausschließen	Get-OrganizationConfig| fl PublicFoldersLockedforMigration, PublicFolderMigrationComplete Get-PublicFolderMigrationRequest | Remove-PublicFolderMigrationRequest -Confirm:$false
Vorhandensein von Öffentlichen Ordnern auf dem Exchange 2013 ausschließen	Get-Mailbox -PublicFolder Get-PublicFolder
Übersicht der Öffentlichen Ordner erstellen	Export-PublicFolderStatistics.ps1 D:\PF\PFmap.csv Ex2010.schulenburg.lab
Mapping-Datei erstellen	PublicFolderToMailboxMapGenerator.ps1 300MB E:\PF\PFmap.csv E:\PF\PFmap2Mailbox.csv
Neue Öffentliche Ordner erstellen	New-Mailbox -PublicFolder PFMasterHierarchy -HoldForMigration:$true New-Mailbox -PublicFolder PFContent1
Migration starten	
BadItemLimit bei Exchange 2007 setzen	$PublicFolderDatabasesInOrg= @(Get-PublicFolderDatabase) $BadItemLimitCount= 5 + ($PublicFolderDatabasesInOrg.Count-1)
Start der Migration auf dem Exchange 2013 (optional BadItemLimit bei Exchange 2007)	New-PublicFolderMigrationRequest -SourceDatabase (Get-PublicFolderDatabase -Server Ex2013) -CSVData (Get-Content E:\PF\PFmap2Mailbox.csv -Encoding Byte) -BadItemLimit $BadItemLimitCount
Status der Migration prüfen	Get-PublicFolderMigrationRequest | Get-PublicFolderMigrationRequestStatistics
Migration abschließen	
Zugriff auf den Exchange 2007/2010 stoppen	Set-OrganizationConfig-PublicFoldersLockedForMigration:$true
Migration auf den Exchange 2013 finalisieren	Set-PublicFolderMigrationRequest-Identity \PublicFolderMigration-PreventCompletion:$false Resume-PublicFolderMigrationRequest-Identity \PublicFolderMigration
Zugriff testen	Set-Mailbox -Identity Administrator -DefaultPublicFolderMailbox PFContent1
Öffentliche Ordner für User freigeben	Get-Mailbox -PublicFolder| Set-Mailbox -PublicFolder -IsExcludedFromServingHierarchy $false Set-OrganizationConfig -PublicFolderMigrationComplete:$true

löschen Sie diese Hinterlassenschaften auch richtig. Bevor Sie die Deinstallation starten, entfernen Sie zunächst die Datenbanken auf dem alten Server über die Exchange Management Console. Dadurch stellen Sie sicher, dass keine Postfächer mehr auf dem Server liegen – gerade die Systemmailboxen sind häufig noch aktiv und müssen vorab verschoben werden, damit es später keine Probleme beim AuditLogging oder dem eDiscovery gibt. Am schnellsten verschieben Sie die Postfächer über den folgenden Befehl am Exchange 2013-Server:

```
Get-Mailbox -Database MailboxDatabase2007-2010 -Arbitration | New-MoveRequest -Targetdatabase MailboxDatabase2013
```

Im Anschluss sollte die Löschung der Datenbanken funktionieren. Als letzte Aufgabe steht an, den alten Server noch von den Offline-Adressbüchern (OAB) zu befreien. Ein Verschieben des Standard-Offline-Adressbuchs ist nicht möglich, weshalb Sie das alte Adressbuch löschen müssen:

```
Remove-OfflineAddressBook -Identity "Standard-Offlineadressbuch"
```

Über *Get-OfflineAddressBook* sollte Ihnen nur noch das Exchange 2013-Adressbuch angezeigt werden. Sollten Sie über die Standard-Adressbücher hinaus weitere Adressbücher angelegt haben, müssen Sie diese auch löschen und auf dem Exchange 2013-Server neu erstellen. Eine Konfiguration ist dabei in der EAC nicht vorgesehen und sämtliche Aufgaben sind über die EMS durchzuführen.

Rufen Sie im nächsten Schritt die Deinstallation des Exchange Servers über die Systemsteuerung unter "Programme und Funktionen" auf und folgen Sie den Hinweisen des Assistenten. Wählen Sie alle Rollen und die Verwaltungstools ab. Nachdem die Deinstallation abgeschlossen wurde, entfernen Sie den Server noch aus der Active Directory-Domäne, damit auch das Computerkonto gelöscht wird.

Fazit

Die Migration auf Exchange 2013 gleicht an vielen Stellen vorangegangenen Exchange-Migrationen. Der Teufel steckt jedoch im Detail, denn es sind viele kleine Schrauben zu drehen, damit hinterher alles wie gewünscht funktioniert. In Abhängigkeit von der Größe der alten Datenbanken ist die Migration eine zeitliche Herausforderung, die sich über Wochen hinziehen kann. Auch die Neuerungen im Bereich der Öffentlichen Ordner bieten einige Stolpersteine, die Sie mit dieser Workshopserie aber leichtfüßig überspringen können. *(ln)*

[1] Workshop "Öffentliche Ordner in Exchange Server 2013"
IT-Administrator Ausgabe 05/2013, Seite 61

[2] Migrating Public Folders to Exchange 2013
DCP62

[3] Comparing Public Folder Item Counts
DCP63

Link-Codes

Server mit Red Hat OpenShift in die Cloud verlagern

Webapps auf Reisen

von Thorsten Scherf

OpenShift ist der hauseigene Platform-as-a-Service von Red Hat. Wer seine eigenen Applikationen ins Netz stellen möchte, der kann zwischen verschiedenen Anwendungsmodellen wählen. Damit lassen sich beispielsweise Lastspitzen bei Webanwendungen abfedern, ohne in eigene Infrastruktur investieren zu müssen. Dieser Workshop zeigt die Konfiguration des kostenfreien Webdienstes.

Cloud-basierte PaaS-Lösungen kommen in der Regel zum Einsatz, wenn schnell und ohne großen administrativen Aufwand neue Laufzeitumgebungen für Anwendungen benötigt werden. Dies kann beispielsweise dann notwendig sein, wenn es darum geht, zu bestimmten Zeiten Lastspitzen für den Zugriff auf eine Anwendung abzufangen. Viele Webshops sehen sich beispielsweise zum Weihnachtsgeschäft einer erhöhten Kundennachfrage ausgesetzt und sind froh, schnell und dynamisch Rechenressourcen nachschieben zu können. Aber auch im Bereich der Software-Entwicklung sind PaaS-Services sehr beliebt, können sich die Entwickler hier doch auf ihre eigene Arbeit – das Entwickeln von Software – konzentrieren, anstatt sich mit dem Setup und der Konfiguration der Laufzeitumgebung herumplagen zu müssen.

Mit OpenShift bietet Red Hat eine PaaS-Lösung auf Basis des hauseigenen Red Hat Enterprise Linux an. Das Framework unterstützt dabei eine Vielzahl von bekannten und beliebten Programmiersprachen zur Entwicklung der eigenen Webanwendung. Das gilt etwa für die Sprachen Perl, Python, Java, Ruby, PHP und Node.js. Für eine dauerhafte Datenvorhaltung sorgen fertige Datenbank-Dienste auf Basis von MySQL, PostgreSQL oder der No-SQL basierten MongoDB-Datenbank. Mit dem JBoss-Applikationsserver steht zudem eine fertige Laufzeitumgebung für Java-Anwendungen bereit. All diese Services werden in der OpenShift-Sprache als Cartridges bezeichnet. Für den Betrieb einer neuen Anwendung ist zumindest ein Cartridge für die gewünschte Programmiersprache notwendig. Weitere Cartridges lassen sich bei Bedarf hinzufügen. Eine komplette Liste aller zur Verfügung stehenden Cartridges findet man unter [1].

Drei Nutzungsvarianten

Red Hat bietet OpenShift in drei Varianten an. Bei der Variante "Online" läuft die Software auf einer von Red Hat gehosteten Umgebung. Es steht eine kostenlose Basis-Variante zur Verfügung. Benötigen Sie für Ihre Anwendungen mehr Ressourcen, können Sie diese gegen eine entsprechende Gebühr als Premium-Account [2] hinzubuchen, wobei hier neben den zusätzlichen Ressourcen auch der Zugriff auf den Support möglich ist. Red Hat bindet die Ressourcen an sogenannte Gears – Container, in denen die Anwendung läuft. Eine Auto-Scaling-Funktion verteilt die Anwendung über mehrere dieser Container. In der kostenfreien Variante stehen Ihnen drei Gears mit jeweils 512 MByte RAM und 1 GByte Speicherplatz zur Verfügung.

In der "Enterprise"-Variante hosten Sie Ihre Anwendung in der eigenen System-Landschaft. Hierfür ist jedoch die komplette OpenShift-Architektur entsprechend im eigenen Datencenter aufzubauen. Wer seine Daten nicht aus der Hand geben möchte, für den bietet sich diese Variante sicherlich an. Red Hat stellt auf Wunsch Evaluierungs-Subskriptionen zur Verfügung, mit denen sich die kostenpflichtige Software im Vorfeld testen lässt. Bei Erwerb der Software offeriert Red Hat einen entsprechenden Produkt-Support.

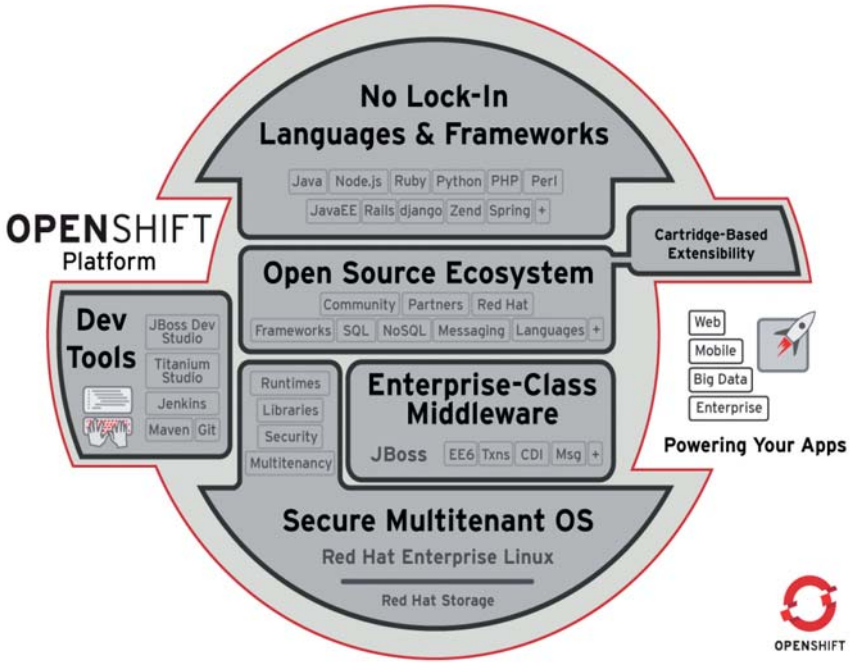


Bild 1: OpenShift besteht aus mehreren Komponenten und bietet eine Auswahl an bekannten OpenSource-Lösungen an

Die Upstream-Entwicklung von OpenShift findet in der dritten Variante, dem "Origin"-Projekt, statt. Hierüber steht der komplette Code des PaaS-Frameworks über ein Git-Repository [3] zur Verfügung. Wer sich die neuesten Entwicklungen im OpenShift-Umfeld ansehen möchte, für den lohnt sich ein Blick auf das Projekt. Für dieses OpenShift-Variante ist kein Support verfügbar. Jedoch existiert eine aktive Community, die gerne bereit ist, Fragen zu beantworten.

Setup per Kommando oder grafischer Oberfläche

Dieser Workshop basiert auf der OpenShift-Variante Online und zeigt, wie Sie eine Anwendung auf dem PaaS-Framework zur Verfügung stellen. Um Zugriff auf die Online-Plattform zu erhalten, legen Sie zuerst einen Account unter [4] an. Dieser wird mit einem SSH-Schlüssel verknüpft, sodass Sie später neuen Code auf die OpenShift-Plattform kopieren können, ohne hierfür jedes Mal Ihr Passwort eingeben zu müssen.

Für das Code-Management kommt üblicherweise das Kommandozeilen-Tool rhc zum Einsatz. Die grafische Webmanagement-Oberfläche bietet sich dafür an, den eigenen Account zu verwalten und neue Applikationen anzulegen und auch zu überwachen. Die Client-Anwendung rhc steht für Windows, Mac OS X und natürlich Linux zur Verfügung. Unter Fedora gehört das Tool zum Software-Repository. Die Installation gelingt wie immer mit Hilfe des Paketmanagers der Fedora-Distribution:

```
# sudo yum install rubygem-rhc
```

Aktuelle Versionen der Client-Anwendung lassen sich auch direkt als Ruby-Gem-Paket installieren. Diese Variante ist auf jeder Linux-Plattform verfügbar. Zur Installation ist zwingend Ruby ab der Version 1.8.7 notwendig:

```
# sudo gem update rhc
```

Die Installation auf anderen Plattformen beschreibt Red Hat in der Client-Dokumentation unter [5]. Nachdem Sie also Ihren Account erzeugt und das Client-Tool installiert haben, gilt es, die eigene Umgebung zu konfigurieren. Hierfür rufen Sie das Client-Tool auf:

```
# rhc setup
```

Daraufhin startet ein Wizard, der den eigenen Namespace für die eigenen Applikationen abfragt und den persönlichen SSH-Schlüssel mit dem Account verknüpft (siehe Bild 2). Hiermit ist der Zugriff auf das OpenShift Git-Repository einfacher. Im Git-Repository speichert OpenShift den Code der eigenen Benutzer-Anwendungen. Dieser steht dann zum Check-out zur Verfügung, lokale Änderungen lassen sich nach Belieben wieder einchecken und sind damit automatisch auf der OpenShift-Plattform sichtbar. Der Zugriff auf die Anwendung erfolgt über eine URL, die an den eigenen Namespace gebunden ist. Diese folgt stets dem Schema Anwendung-Namespace.rhcloud.com. Heißt die Anwendung also beispielsweise "spacetool" und haben Sie den eigenen Namespace als "tuxgeeks" definiert, rufen Sie die URL *http://spacetool-tuxgeeks.rhcloud.com* auf, um Zugriff auf die Webanwendung zu erhalten. Der ausgewählte Namespace lässt sich übrigens zu einem beliebigen Zeitpunkt ändern, sollte dies einmal notwendig sein. Hat das Setup ordnungsgemäß funktioniert, so sollte

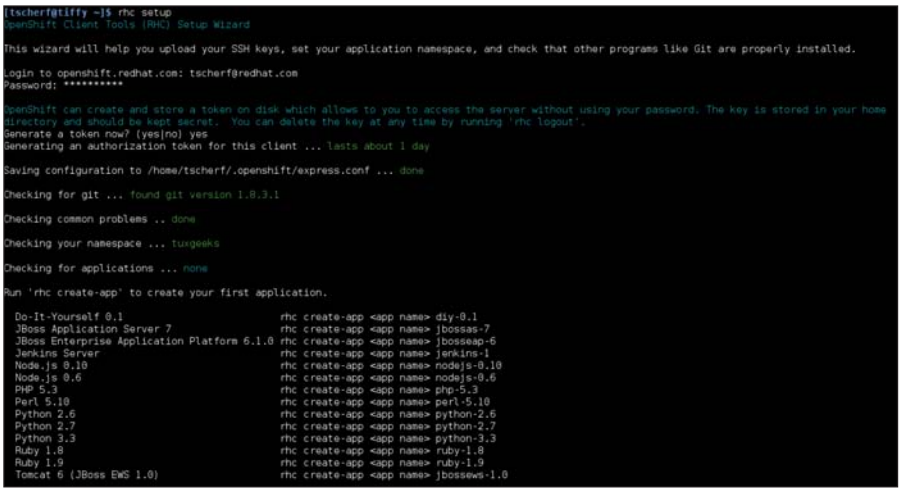


Bild 2: Mit dem OpenShift-Client Tool richten Sie die eigene Umgebung ein und können erste Applikationen für den Betrieb auf der Plattform konfigurieren

der Aufruf von *rhc account* entsprechende Informationen zurückliefern:

```
# rhc account
Server: openshift.redhat.com
Login: tscherf@redhat.com
Plan: Free
Gears Used: 1
Gears Allowed: 3
Allowed Gear Sizes: small
SSL Certificates Supported: no
```

Die erste Anwendung vorbereiten

Möchten Sie nun die erste Anwendung auf die OpenShift-Plattform übertragen, bereiten Sie zuerst ein entsprechendes Gear auf der Plattform vor. Hierbei wählen Sie zumindest ein Cartridge für die gewünschte Programmiersprache aus. Alternativ besteht die Möglichkeit, weitere Cartridges für Add-Ons, beispielsweise eine Datenbank oder ein Webframework, auszuwählen. Dies ist jedoch auch zu einem späteren Zeitpunkt noch möglich. Eine Liste der zur Verfügung stehenden Cartridges liefert der Befehl *rhc cartridge-list*.

In diesem Workshop laden wir zuerst eine einfache Perl-Anwendung auf die OpenShift-Plattform. Der Aufruf hierzu lautet:

```
# rhc app create spacetool perl-5.10
```

Das Ergebnis sollte aussehen wie in Bild 3. Im aktuellen Arbeitsverzeichnis sollte außerdem ein Ordner mit dem Namen der Anwendung, hier also "spacetool", vorhanden sein. Dieser enthält die Dateien des Git-Repositories und ist nun entsprechend mit dem Programmcode der eigenen Anwendung zu erweitern.

Im folgenden einfachen Beispiel wird lediglich eine neue *index.pl* dem Ordner hinzugefügt und dann in das Git-Repository übertragen:

```
# cd spacetool/perl
# echo 'print "Content-type:
  text/html\r\n\r\n";' > index.pl
# echo 'print "Hello World...\n\n";'
  > index.pl
# git add index.pl
# git commit -m "Initial Upload
  first OpenShift App"
# git push
```

```
[tscherf@tiffy git]$ rhc app create spacetool perl-5.10
Application Options
-------------------
  Namespace:  tuxgeeks
  Cartridges: perl-5.10
  Gear Size:  default
  Scaling:    no

Creating application 'spacetool' ... done


Waiting for your DNS name to be available ... done

Cloning into 'spacetool'...
Warning: Permanently added the RSA host key for IP address '54.234.174.227' to the list of known hosts.

Your application 'spacetool' is now available.

  URL:        http://spacetool-tuxgeeks.rhcloud.com/
  SSH to:     524983c2e0b8cdcc900000c7@spacetool-tuxgeeks.rhcloud.com
  Git remote: ssh://524983c2e0b8cdcc900000c7@spacetool-tuxgeeks.rhcloud.com/~/git/spacetool.git/
  Cloned to:  /home/tscherf/git/spacetool

Run 'rhc show-app spacetool' for more details about your app.
[tscherf@tiffy git]$
```

Bild 3: Mit Hilfe des Client-Tools lässt sich die OpenShift-Plattform für die erste Anwendung vorbereiten

Rufen Sie im Anschluss die URL *http://spacetool-tuxgeeks.rhcloud.com* im Webbrowser auf, sollte ein einfaches "Hello World" zu sehen sein. Natürlich lassen sich nun weitere Cartridges der Anwendung hinzufügen, also beispielsweise Datenbanken oder Webframeworks für die ausgewählte Sprache. Der Workflow zum Aktualisieren der Anwendung entspricht jetzt einem regulären Entwicklungsprozess: Der Code im lokalen Repository wird angepasst und mittels *git commit* dem lokalen Repository hinzugefügt. Ein *git push* übertragt dann die lokalen Änderungen in das OpenShift-Repository und die Änderungen an der Anwendung sind damit live und online einsehbar.

Vorhandenes Repository übertragen

Oft ist es so, dass Sie bereits ein bestehendes Git-Repository zur Verfügung haben, in dem der eigene Code vorliegt. GitHub [6] ist beispielsweise ein bekannter Hoster für solche Code-Repositories. Nun möchten Sie vielleicht den Code aus dem GitHub-Repository auf die OpenShift-Plattform übertragen und im dortigen Code-Repository vorhalten, um Änderungen direkt auf der neuen Plattform testen zu können. Dies ist mit Hilfe einiger weniger Git-Kommandos ohne großen Aufwand möglich. Als Erstes muss natürlich eine lokale Kopie des Upstream Git-Repositories verfügbar sein.

Aus diesem Verzeichnis heraus lässt sich dann mittels einer "git pull"-Abfrage der Code aus dem OpenShift-Repository in das lokale Arbeitsverzeichnis kopieren.

Die Git-URL des OpenShift-Repositories erhalten Sie mittels *rhc app show app-name*. Die Struktur des lokalen Arbeitsverzeichnisses passen Sie dann an das OpenShift-Repository an. So ist es beispielsweise notwendig, dass der Perl-Programmcode in einem eigenen Unterordner liegt. Sind alle Änderungen durchgeführt, können Sie diese mit *git commit* und *git push* in das Repository übertragen. Das Beispiel im Kasten "Repository übertragen" zeigt die hierfür notwendigen Befehle für die Beispielapplikation spacetool.

Danach steht die Applikation aus dem Upstream-Repository nun auch auf der OpenShift-Plattform zur Verfügung und kann dort über die zuvor angegebene URL aufgerufen werden.

Repository übertragen

```
# cd Upstream Code-Repository Ordner
# rhc app show spacetool
spacetool @ http://spacetool-tuxgeeks.rhcloud.com/ (uuid:
   524983c2e0b8cdcc900000c7)
------------------------------------------

  Domain:  tuxgeeks
  Created: Sep 30  3:59 PM
  Gears:   1 (defaults to small)
  Git URL: ssh://524983c2e0b8cdcc900000c7@spacetool-tux-
   geeks.rhcloud.com/~/git/spacetool.git/
  SSH: 524983c2e0b8cdcc900000c7@spacetool-
   tuxgeeks.rhcloud.com

  perl-5.10 (Perl 5.10)
  ---------------------

    Gears: 1 small

# git pull ssh://524983c2e0b8cdcc900000c7@spacetool-tux-
   geeks.rhcloud.com/~/git/spacetool.git/
# git commit -a -m "OpenShift merge"
# git push ssh://524983c2e0b8cdcc900000c7@spacetool-tux-
   geeks.rhcloud.com/~/git/spacetool.git/ master
```

Für Eilige: Quickstarts

Das OpenShift-Ecosystem verfügt mittlerweile über eine große Auswahl an Applikationen, die speziell für den Betrieb auf OpenShift vorgesehen sind. Diese Applikationen bringen bereits alle notwendigen Cartridges mit und auch die Struktur des Code-Repositories ist angepasst. Solche Anwendungen werden in der OpenShift-Sprache als "Quickstarts" bezeichnet und stehen über das OpenShift-Repository [3] zum Download bereit.

Noch einfacher geht es über die webbasierte Management-Konsole. Nach einem Login mit dem zuvor erzeugten OpenShift-Account klicken Sie auf "Create Application" und suchen in der Liste die zur Verfügung stehenden Anwendungen, um diese dann auf den eigenen Gears zu installieren. Das Einzige, was hierfür notwendig ist, ist ein neuer Name für die Anwendung. Nach einem Klick auf den Button "Create Application" steht diese dann unter der persönlichen OpenShift-URL zur Verfügung. Das Beispiel in Bild 4 zeigt den Ablauf für die Installation der Blog-Software Wordpress auf OpenShift. Das Code-Archiv enthält bereits alle notwendigen Anpassungen. Wird es installiert, steht die Setup-Seite für das Blog nach wenigen Momenten unter der eigenen URL zur Verfügung.

Natürlich funktioniert dieser Vorgang auch über die Kommandozeile, wie das folgende Beispiel zeigt. Hier wird die neue Anwendung mit den notwendigen Cartridges manuell erzeugt, um im Anschluss das leere Code-Repository mit dem Upstream-Repository der gewünschten Anwendung zu verknüpfen. Ein finales *git push* sorgt dafür, dass der Code aus dem lokalen Arbeitsverzeichnis zurück auf die persönliche OpenShift-Plattform gelangt:

```
# rhc app create -a blog -t php-5.3
# rhc cartridge add mysql-5.1 -a
  blog
# cd blog
# git remote add upstream -m master
  git://github.com/openshift/word-
  press-example.git
# git pull -s recursive -X theirs
  upstream master
# git push
```

Ein abschließender Test bestätigt, dass die Anwendung mit den notwendigen Cartridges erzeugt wurde und nun über die persönliche URL zum Abruf zur Verfügung steht. In der URL der Anwendung erkennen Sie, dass als Name für die Software "blog" gewählt wurde und diese zum Namespace "tuxgeeks" gehört:

```
# app show blog
blog @ http://blog-
  tuxgeeks.rhcloud.com/ (uuid:
  5249a02d4382ecfdfe000642)
------------------------------------

  Domain: tuxgeeks
  Created: Sep 30  6:00 PM
  Gears: 1 (defaults to small)
  Git URL:
  ssh://5249a02d42821cfdee000642@blog-
  tuxgeeks.rhcloud.com/~/git/blog.git/
  SSH:
  5249a02d4382ecfdee100642@blog-tux-
  geeks.rhcloud.com

  php-5.3 (PHP 5.3)
------------------------------------

  Gears: Located with mysql-5.1

  mysql-5.1 (MySQL Database 5.1)
------------------------------------

    Gears: Located with php-5.3
    Connection URL: mysql://$OPEN-
  SHIFT_MYSQL_DB_HOST:$OPENSHIFT_
  MYSQL_DB_PORT/
    Database Name: blog
    Password: xxx
    Username: xxx
```

Auch in diesem Fall steht nach wenigen Momenten der Konfigurations-Wizard der Blog-Software zur Verfügung.

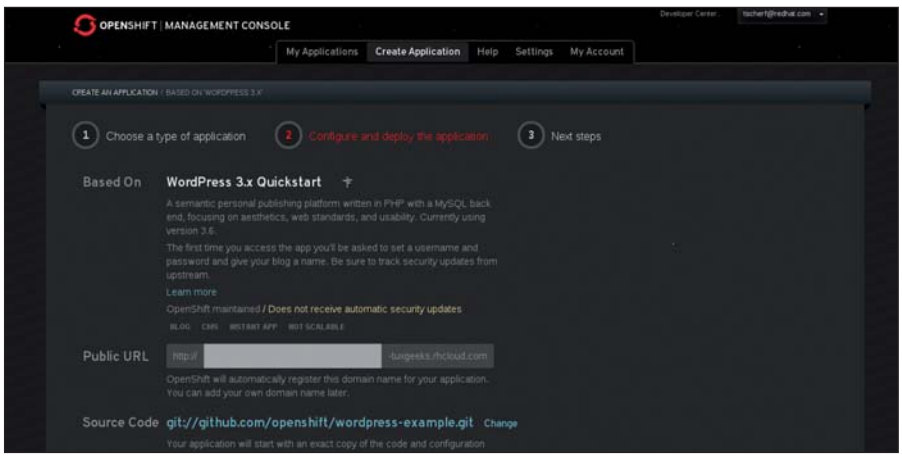


Bild 4: Über die webbasierte Management-Konsole fügen Sie vorhandene Anwendungen zur OpenShift-Plattform hinzu

Fazit

Mit OpenShift steht eine sehr mächtige und dennoch einfach zu bedienende PaaS-Lösung zur Verfügung. Dank der verschiedenen Anwendungs-Modelle kommt sie auch für Kunden in Frage, die ihre Daten im eigenen Rechenzentrum hosten wollen. Der Workshop konnte natürlich nur einen kleinen Einblick in die Welt von OpenShift liefern. Neben den gezeigten Beispielen gibt es noch vieles mehr zu entdecken. Wer auf den Geschmack gekommen ist, dem ist ein Blick auf das OpenShift-Videoarchiv [7] zu empfehlen. Viele interessante Anwendungsfälle sind hier audiovisuell dokumentiert. Das Projekt verfügt zudem über eine ausführliche Knowledgebase [8], die zahlreiche offenen Fragen beantwortet. *(dr)*

Link-Codes

[1] Liste der OpenShift-Cartridges
DBP41

[2] OpenShift-Preistabelle
DBP42

[3] OpenShift-Upstream Repository
DBP43

[4] OpenShift-Projektseite
DBP44

[5] OpenShift Client-Tools
DBP45

[6] GitHub
DBP46

[7] OpenShift-Videos
DBP47

[8] OpenShift-Knowledgebase
DBP48


Quelle: Burak çakmak – 123RF

Neuerungen in OpenNebula 4.2

Baukasten für die Cloud

von Dr. Holger Reibold

Nach einer rund fünfjährigen Entwicklungszeit stellte das OpenNebula-Team im Mai dieses Jahres mit Release 4 sein neuestes Release vor, das gegenüber der Vorgängerversion in allen Subsystemen wichtige Verbesserungen erfahren hat. In diesem Workshop sehen wir uns die wichtigsten Neuerungen der Cloud-Umgebung an – gerade beim Benutzer-Interface und der VDI-Verzahnung hat sich einiges getan.

Cloud-Umgebungen sind aktuell hoch im Kurs, da sich mit ihnen die Verfügbarkeit von Daten unternehmensweit erhöhen lässt – gerade bei verteilten Unternehmen, die viel mit mobilen Mitarbeitern und Dritten kommunizieren. OpenNebula ist in diesem Marktsegment schon lange eine feste Größe. Bei genauerer Betrachtung erweist sich OpenNebula, dessen Quellcode unter der Apache-Lizenz zum Download zur Verfügung steht, als eine Open Source-Werkzeugsammlung für das Cloud Computing, die für das Management heterogener Infrastrukturen konzipiert wurde. OpenNebula ist auch als IaaS (Infrastructure as a Service) einsetzbar, um private, öffentliche oder hybride Clouds zu erstellen.

Zentrale Neuerungen im Überblick

Nach der Installation von OpenNebula 4.2 fällt bei der ersten Verwendung der Web-Schnittstelle "Sunstone" das komplett überarbeitete Interface auf. Die neue Oberfläche ist für einzelne Nutzer oder Gruppen individuell anpassbar. Ab Version 4 haben Administratoren die Möglichkeit, System-Schnappschüsse der eingesetzten virtuellen Maschinen zu erstellen. Diese Funktionalität ist allerdings nur für KVM und VMware gegeben.

Sie können diese Funktion beispielsweise dazu nutzen, um eine VM nach einem definierbaren Zeitplan vom Netz zu nehmen und anschließend wieder verfügbar zu machen. Sie können mit der aktuellen Version von OpenNebula sogar die mit einer VM assoziierten Ressourcen modifizieren, konkret beispielsweise die Anzahl der CPU-Kerne und den verfügbaren Arbeitsspeicher. Damit einher geht ein deutlicher Gewinn an Flexibilität.

Zu den weiteren Neuerungen von OpenNebula 4.x gehört außerdem die Unterstützung für IPv6 und NIC-Hotplugging, um im laufenden Betrieb einfach Netzwerkgeräte hinzuzufügen. Da insbesondere Administratoren aus dem Linux-Umfeld die Konsole bevorzugen, kommen auch diese in den Genuss eines leicht verbesserten Command-Line-Interfaces. Einen sehr detaillierten Überblick über die Änderungen finden Sie auf der Website des OpenNebula-Teams unter [1].

Leistungsfähiges Benutzermanagement

Wie es sich für ein Werkzeug gehört, das auch professionellen Ansprüchen genügen soll, verfügt die Cloud-Umgebung über ein vollständiges Benutzer- und Gruppensystem. OpenNebula-Benutzer sind standardmäßig in vier Typen klassifiziert:

- Administratoren: Sie gehören standardmäßig der oneadmin-Gruppe an und können jede Aktion ausführen.
- Reguläre Benutzer: Sie haben Zugriff auf die meisten OpenNebula-Funktionen.
- Öffentliche Benutzer: Die Grundfunktionen stehen auch öffentlichen Benutzern zur Verfügung.
- Service-Benutzer: Hierbei handelt es sich um einen speziellen Account, der von OpenNebula-Services verwendet wird.

Für das Erstellen und Verwalten von Benutzern und Gruppen können Sie die verfügbaren Schnittstellen verwenden, beispielsweise das Web-Interface, aber auch die Konsole. Für die Benutzerverwaltung ist der Standard-Administrator oneadmin zuständig, der mit den Kommandos *oneuser create* und *oneuser delete* neue Benutzer anlegt beziehungsweise löscht. Um weitere Administratoren anzulegen, führen Sie den Befehl im Kasten "Anlegen eines Administrator-Accounts" aus. Der Beispielausgabe können Sie auch entnehmen, wie Sie in der überarbeiteten CLI die Benutzerliste ausgeben: Verwenden Sie den Befehl *oneuser list*.

```
$ oneuser create weiterer_admin password
  ID: 2

$ oneuser chgrp weiterer_admin oneadmin

$ oneuser list
  ID GROUP    NAME            AUTH       PASSWORD
   0 oneadmin oneadmin        core       5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
   1 oneadmin serveradmin     server_c   1224ff12545a2e5dfeda4eddacdc682d719c26d5
   2 oneadmin otheradmin      core       5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8

$ oneuser show otheradmin

USER 2 INFORMATION
ID              : 2
NAME            : otheradmin
GROUP           : 0
PASSWORD        : 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
AUTH_DRIVER     : core
ENABLED         : Yes

USER TEMPLATE
```

Listing: Anlegen eines Administrator-Accounts

Runderneuerte Web-GUI

Die Web-Schnittstelle Sunstone wird auch als OpenNebula Cloud Operations Center bezeichnet und ist für die Steuerung der verschiedenen OpenNebula-Komponenten zuständig. Die zentrale Aufgabe der GUI ist die Vereinfachung typischer Standardaufgaben beim Management der Umgebung. Die Schnittstelle lässt sich dabei an verschiedene Benutzerrollen adaptieren. Sie können beispielsweise dafür Sorge tragen, dass einer bestimmten Rolle auch nur die Ressource angezeigt wird, auf die diese Rolle Zugriff hat. Das Verhalten von Sunstone lässt sich über die sogenannten Ansichten (Views) anpassen und erweitern.

Die Konfiguration von Sunstone erfolgt über die Konfigurationsdatei *sunstone-server.conf*, die Sie standardmäßig unter */etc/one/sunstone-server.conf* finden. Die Konfigurationsdatei verwendet YAML-Syntax. Näheres zu den möglichen Settings entnehmen Sie der Tabelle "Konfigurationsoptionen für Sunstone 4.x". Soll der Sunstone-Server auch von anderen Rechnern als localhost genutzt werden können, müssen Sie zunächst die IP-Adresse mit der ":host"-Option konfigurieren, denn andernfalls ist der Server nicht für andere Systeme erreichbar. Um Sunstone nach der Installation zu starten, führen Sie folgenden Befehl aus:

```
$ sunstone-server start
```

Die Logfiles des Servers finden Sie in der Datei */var/log/one/sunstone.log*, Fehlermeldungen landen standardmäßig in der Datei */var/log/one/sunstone.error*. Sollten Sie Änderungen an der Sunstone-Konfiguration vornehmen und ein Anhalten/Neustart des Sunstone-Servers erforderlich sein, erledigen Sie dies mit *$ sunstone-server stop*.

Die perfekte Ansicht

Mit Hilfe der Sunstone Views steht Ihnen ein sehr leistungsfähiges und flexibles System zur Verfügung, um die Funktionalität der GUI in diese oder jene Richtung zu verändern. In der Regel empfiehlt sich ein Reduzieren der standardmäßig bereitgestellten Funktionalität auf die Features, die auch tatsächlich von der jeweiligen Gruppe benötigt werden.

Jeder Gruppe ihre GUI

In der Praxis können Sie beispielsweise mehrere Cloud-Ansichten für unterschiedliche Benutzergruppen anlegen. Jede Ansicht definiert dabei einen Satz UI-Komponenten. OpenNebula implementiert zwei Standardansichten: User- und Admin-Views, wobei die Admin-Ansicht nur für Mitglieder der oneadmin-Gruppe verfügbar ist. Neue Benutzer landen standardmäßig auf der User-Ansicht.

Nach dem Einloggen mit einer bestimmten Benutzerkennung lädt automatisch die Ansicht, die im Verzeichnis "/etc/one/sunstone-view" für die spezifische Gruppe beziehungsweise den betreffenden Benutzer definiert ist. Für jede Ansicht wird eine eigene Konfigurationsdatei mit der Endung .YAML angelegt. Die Ansichtsbezeichnung in der GUI entspricht dann der Bezeichnung der YAML-Dateien ohne die Dateierweiterung.

Prinzipiell können auch mehrere Ansichten für eine Gruppe angelegt werden. Ist das der Fall, kann jeder Benutzer individuell zwischen den verschiedenen Views hin-

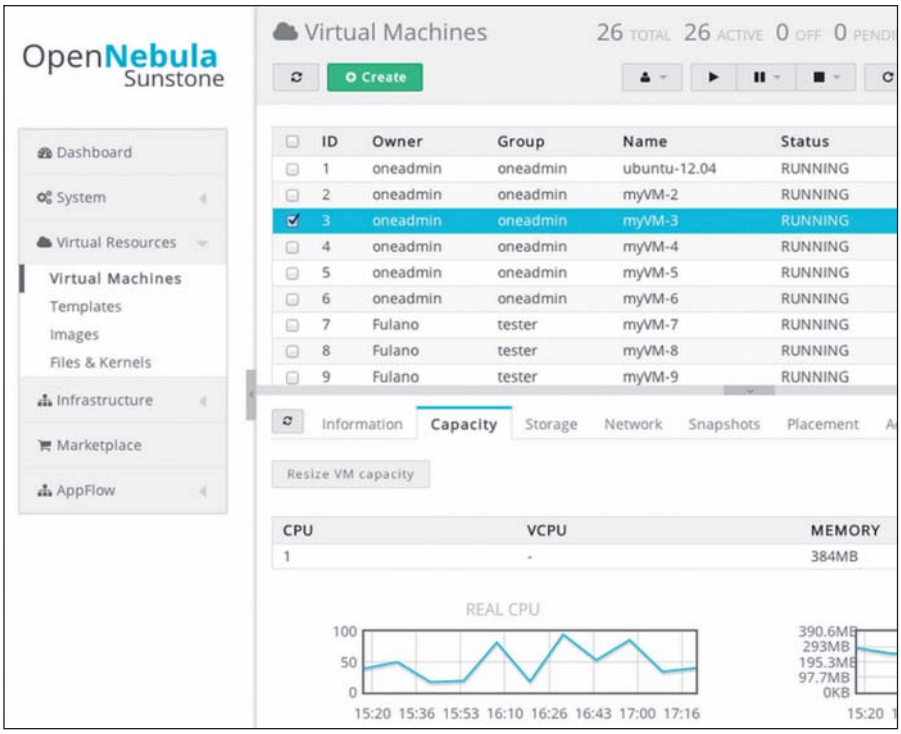


Bild 1: Springt direkt ins Auge: Das komplett runderneuerte Web-Interface von OpenNebula 4.x vereinfacht die Systemadministration

und herschalten. Für Anpassungen der Ansichten stehen Ihnen drei Bereiche zur Verfügung. Sie können für jede Ansicht festlegen, welche UI-Komponenten darin enthalten sind, bestimmen, welche Views für welche Benutzer/Gruppen gedacht sind und Sie können das Sunstone-Portal an Ihre Anforderungen anpassen und beispielsweise das Design oder das Logo ändern.

Der Inhalt der View-Datei spezifiziert auch die Registerkarten, die im linksseitigen Menü aktiviert sind. Dabei lässt sich jedes Tab ein- und ausschalten. Zuständig hierfür ist das Attribut "enabled_tabs". Um eine Karte auszublenden, setzen Sie das betreffende Attribut von "true" auf "false". In nachstehender Beispielkonfiguration ist das Clusters-Tab deaktiviert:

```
enabled_tabs:
    dashboard-tab: true
    system-tab: true
    users-tab: true
    groups-tab: true
    acls-tab: true
    vresources-tab: true
    vms-tab: true
    templates-tab: true
    images-tab: true
    files-tab: true
    infra-tab: true
    clusters-tab: false
    hosts-tab: true
    datastores-tab: true
    vnets-tab: true
    marketplace-tab: true
    oneflow-dashboard: true
    oneflow-services: true
    oneflow-templates: true
```

Sie können außerdem jede Registerkarte feintunen. Hierfür stehen Ihnen verschiedene Anpassungsmöglichkeiten zur Verfügung. Über das Attribut "panel_tabs" schalten Sie beispielsweise die Unterregister ein und aus, die eingeblendet werden, wenn Sie ein Objekt auswählen. Mit dem Attribut "table_columns" definieren Sie die Spalten in der Informationstabelle und mit "actions" legen Sie fest, welche Schaltflächen in einer Ansicht verfügbar sind.

Individuelle View nach Standort

Nachdem Sie die Ansichten für die verschiedenen Rollen definiert und konfiguriert haben, müssen Sie als Nächstes definieren, welche Benutzergruppe und welche Benutzer Zugriff auf welche Views haben. Diese Konfiguration erfolgt in der Datei */etc/one/sunstone-views.yaml*.

Sie können die Ansichten für einzelne Benutzer definieren. Hierfür weisen Sie jedem User die gewünschten Views zu. Entsprechendes funktioniert auch bei Gruppen. Außerdem kennt OpenNebula eine Standardansicht, die auf alle Anwender angewendet wird, die nicht in der Benutzer- oder Gruppenansicht notiert sind.

Beim Einsatz im Unternehmen oder als Service-Dienstleistung bietet es sich außerdem an, das Sunstone-Portal mit spezifischen Informationen wie einem Logo zu kennzeichnen. Um das Standard-OpenNebula-Logo des Login-Dialogs durch Ihr eigenes zu ersetzen, editieren Sie die Datei */etc/one/sunstone-views.yaml*. Das Logo ist für jede Ansicht in der View-Datei definiert.

OpenNebula für virtuelle Desktops

Erfahrungsgemäß ist für Betreiber einer OpenNebula-Umgebung eine der am häufigsten nachgefragten Funktionen das Deployment von virtuellen Desktops – und zwar sowohl für die Konvertierung von bestehenden Desktop-Umgebungen nach OpenNebula als auch für das Erzeugen von benutzerdefinierten Umgebungen, wie sie beispielsweise für Schulungen benötigt werden. Für derlei Anforderungen bieten Cloud-Umgebungen beträchtliche Vorteile im Bereich Management, aber auch auf der Kostenseite.

In der Praxis hat sich gezeigt, dass die Kombination von OpenNebula und KVM hierfür bestens geeignet ist. Muss der Start von einer bestehenden Desktop-Umgebung erfolgen, verwenden Sie hierfür einen entsprechenden Adapter wie den VMware Converter. Da die Performance der konvertierten Maschinen mangels eines fehlenden abgestimmten I/O- und Netzwerk-Treibers nicht gerade optimal ist, muss die Windows-Client-Umgebung zur Installation der entsprechenden Treiber bewegt werden.

Hierfür greifen Sie am besten zu Virtio. Unter [2] finden Sie das entsprechende ISO-Image, das Sie in OpenNebula laden und als CD-ROM-Image registrieren. Dann erzeugen Sie ein neues Template für das Windows-System, verlinken es mit der konvertierten Windows-Installation, einem kleinen VD-Image und dem Virtio-ISO-Image. Setzen Sie die Netzwerkschnittstelle auf "virtio" und führen Sie einen Neustart durch. Nach dem Neustart des Windows-Systems öffnen Sie dessen

Konfigurationsoptionen für Sunstone 4.x

Option	Beschreibung
:one_xmlrpc	Mit dieser Option bestimmen Sie den OpenNebula Daemon-Host und -Port.
:host	Hier geben Sie die IP-Adresse des Sunstone-Servers an. Die Standardkonfiguration lautet 127.0.0.1.
:sessions	Diese Konfiguration bestimmt, wie Session-Informationen gespeichert werden. Mögliche Werte sind "memory" und "memcache".
:memcache_host :memcache_port	Mit diesen beiden Optionen legen Sie den memcache-Host und dessen Port fest.
:debug_level	Diese Einstellung dient der Konfiguration des Debug-Levels. Der kann die Werte 0, 1, 2 und 3 besitzen, wobei 0 nur Fehlermeldungen ausgibt.
:auth	Diese Option bestimmt den Authentifikationstreiber für eingehende Requests. Mögliche Werte sind "sunstone", "opennebular" und "x509".
:lang	Bestimmt die Standardsprachvariante des Sunstone-Interfaces. Diese Variante wird verwendet, solange der Benutzer in seinem Template keine andere Konfiguration nutzt.
:vnc_proxy_port	Diese Option bestimmt den Basis-Port für den VNC Proxy-Server. Der Standardwert lautet 29876.
:routes	Hier hinterlegen Sie eine Liste mit Dateien, die benutzerdefinierte Routen laden.

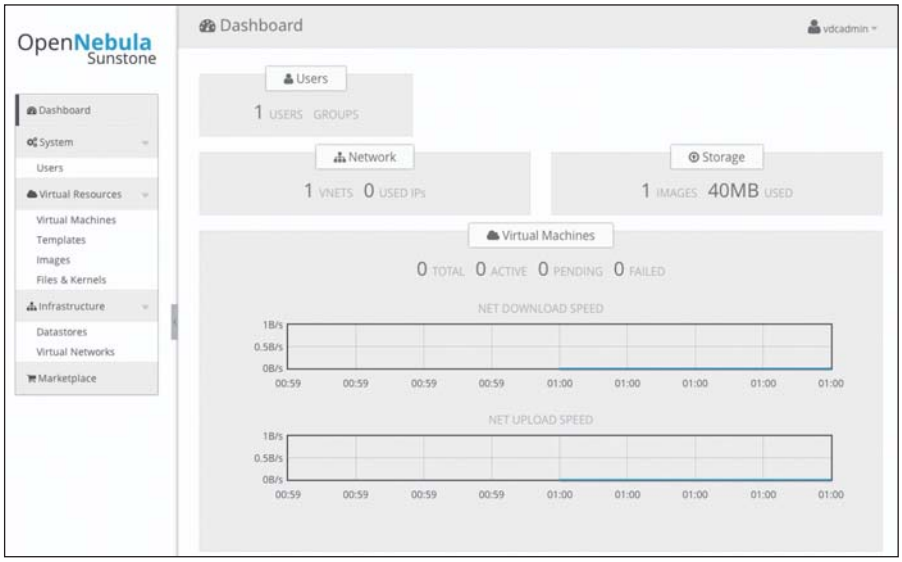


Bild 2: Die VDC-Ansicht stellt alle Ressourcen, die zu einem Virtual Data Center gehören, übersichtlich in der Web-Schnittstelle dar

Systemeinstellungen und dort den Hardware-Manager. Dort finden Sie verschiedene unbekannte Geräte. Führen Sie mit einem Rechtsklick jeweils eine neue Treiberinstallation durch und verwenden Sie hierfür die Virtio-CD-ROM als Installationsquelle. Anschließend sollte die Performance der virtuellen Umgebung optimiert sein.

Der einfachste Weg, ein VM-Image von jedem Desktop in OpenNebula zu integrieren, ist die Zuweisung einer statischen IP-Adresse zu jeder VM und die Verwendung von RDP – ähnlich, wie man es von Thin Clients kennt. Das bringt im Praxiseinsatz verschiedene Vorteile. So ist es beispielsweise mit Hilfe von RDP einfach, lokale Laufwerke und USB-Ports zu exportieren. Gerade auch durch die Verbesserungen der RDP-Implementierung in Windows 7 und 8 wird so eine schnellere Datenverarbeitung möglich.

Sicher mit Zertifikaten

OpenNebula kommt mit drei Servern daher: Sunstone, EC2 und OCCI. EC2 ist ein Web-Service, der Ihnen die Verwaltung und das Starten von virtuellen Maschinen über das Amazon EC2 Query Interface erlaubt. Der OCCI-Server (Open Cloud Computing Interface) stellt die notwendigen Dienste für die Integration von OGF OCCI-Implementierungen zur Verfügung. Interagiert ein Benutzer mit einer dieser Server-Komponenten, erfolgt zunächst eine Authentifizierung des Requests und die Anfrage wird nach erfolgreicher Prüfung von dem OpenNebula-Daemon verarbeitet. Der weitergeleitete Request zwischen den Servern und dem Code-Daemon beinhaltet auch den Benutzernamen und wird mit Informationen des Servers signiert, damit eine eindeutige Zuweisung gewährleistet ist.

Die drei OpenNebula-Server Sunstone, EC2 und OCCI kommunizieren mit dem Kern-Daemon über den "Server-User". Bei der Systeminstallation wird der Account serveradmin mit dem Authentifizierungstreiber *server_cipher* angelegt. Dieser Server-User nutzt einen speziellen Authentifizierungsmechanismus, der dem Server die Ausführung verschiedener Aktionen auf Seiten der normalen Benutzer erlaubt.

Für die Optimierung der Sicherheit steht Ihnen eine einfache Möglichkeit zur Verfügung: Sie ersetzen den Standardtreiber durch *server_x509*. Die Standardkommunikation ist in folgenden Dateien definiert:

- Sunstone: */etc/one/sunstone-server.conf*
- EC2: */etc/one/econe.conf*
- OCCI: */etc/one/occi-server.conf*

Der entsprechende Konfigurationseintrag lautet *:core_auth: cipher*. Um die Kommunikation per X.509 abzusichern, müssen Sie den Authentifizierungstreiber für den Benutzer serveradmin entsprechend neu konfigurieren. Dazu führen Sie die folgenden Kommandos aus:

```
$ oneuser chauth serveradmin
  server_x509
$ oneuser passwd serveradmin -x509
  -cert usercert.pem
```

Mit dem Kommando *oneuser list* können Sie anschließend die Account-Informationen abrufen. Editieren Sie als Nächstes die X.509-Konfiguration in der Datei */etc/one/auth/server_x509_auth.conf* und entkommentieren Sie alle Zeilen. Das Ergebnis sollte in etwa wie folgt aussehen:

```
# User to be used for x509 server
  authentication
:srv_user: serveradmin

# Path to the certificate used by
  the OpenNebula Services
# Certificates must be in PEM format
:one_cert: "/etc/one/auth/cert.pem"
:one_key: "/etc/one/auth/pk.pem"
```

Dann kopieren Sie das Zertifikat und den privaten Schlüssel nach ":one_cert:" sowie ":one_key:" und passen die oben erwähnten Server-Konfigurationsdateien wie folgt an:

```
:core_auth: x509
```

Fazit

OpenNebula ist ein wahres Vorzeigeprojekt, das von Version zu Version immer besser geworden ist. Hier passt einfach sehr viel zusammen – angefangen bei der Funktionalität bis hin zur Handhabung. Version 4.x stellt sicherlich keinen Quantensprung dar, aber es sind die Feinheiten, die ein ohnehin schon ausgereiftes System noch einen Tick besser werden lassen. OpenNebula gehört zudem zu den Open Source-Projekten, die ungewöhnlich gut dokumentiert sind. Unter [3] finden Sie umfangreiche Anleitungen und Hintergrundinformationen. *(ln)*

[1] OpenNebula 4.0 Features and Functionality
DBP01
[2] ISO-Image von Virtio
DBP02
[3] OpenNebula 4.2 Guides
DBP03

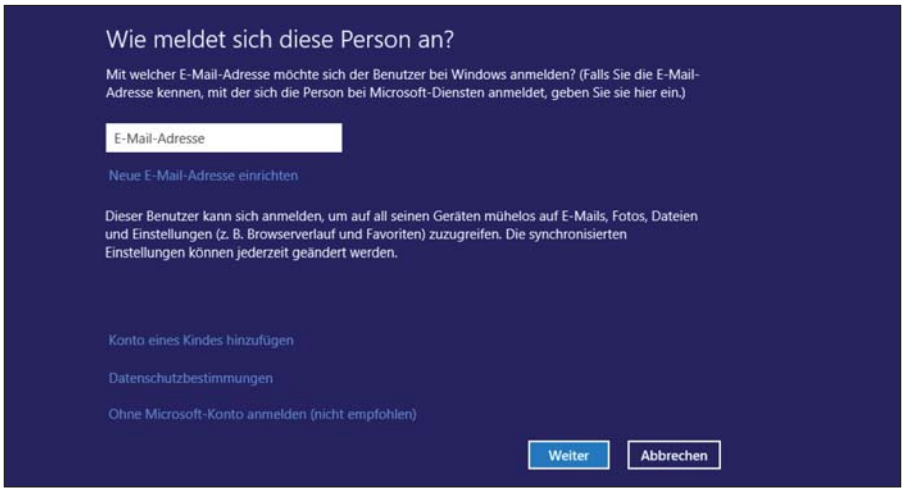
Link-Codes

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.

Alles neu macht **Windows 8.1** – meiner Ansicht nach aber nicht unbedingt immer zum Besten. Beim Upgrade auf die jüngste Version des Betriebssystems ist mir aufgefallen, dass es bei der Einrichtung des Systems **nicht mehr so einfach möglich ist, ein lokales Konto als Benutzerkonto zu verwenden**. Vielmehr besteht Redmond bei der Einrichtung darauf, dass der Benutzer ein Microsoft-Konto hinterlegt. Gibt es hier keine Möglichkeit, weiterhin auf ein lokales Konto zurückzugreifen?

Natürlich existiert auch weiterhin die Möglichkeit, unter Windows 8.1 mit einem lokalen Konto zu arbeiten – allerdings hat Microsoft die dazu nötigen Auswahldialoge gut versteckt. Während der Installation beziehungsweise beim Upgrade besteht Windows 8.1 auf die Eingabe eines Microsoft-Kontos. Nur durch absichtliche falsche Eingaben etwa beim Passwort, das Trennen der Internetverbindung oder Klicken auf Abbrechen fragt das System mit einem Link neben der Eingabemaske für Kontonamen und Kennwort danach, ob der Nutzer ohne Microsoft-Konto fortfahren will. Dann besteht die Möglichkeit, entweder ein vorhandenes lokales Konto weiter zu nutzen oder aber ein neues lokales Konto zu erstellen. Auch im laufenden Betrieb muss der Anwender für das Schaffen eines neuen lokalen Kontos ein paar Klippen umschiffen. Wenn Sie den Weg über die Charms-Leiste gehen ("Einstellungen / PC-Einstellungen ändern / Konten / Weitere Konten / Konto hinzufügen"), findet sich die Option, ein lokales Konto zu erstellen, erst ganz unten am Rand des Bildschirms über den Link "Ohne Microsoft-Konto anmelden (nicht empfohlen)". Ist ein Microsoft-Konto aktiv, können Sie dieses über "Einstellungen / PC-Einstellungen ändern / Konten /Ihr Konto" und den Link "Trennen" deaktivieren und dann zu einem lokalen Konto wechseln. Beachten Sie in diesem Fall allerdings, dass dann einige Features nicht zur Verfügung stehen, etwa die Einbindung von SkyDrive in den Windows Explorer. *(ln)*



Windows 8.1 sieht neue Benutzer am liebsten mit einem Microsoft-Konto verknüpft. Die Alternative eines lokalen Kontos findet sich nur durch den Link ganz unten am Bildschirmrand.

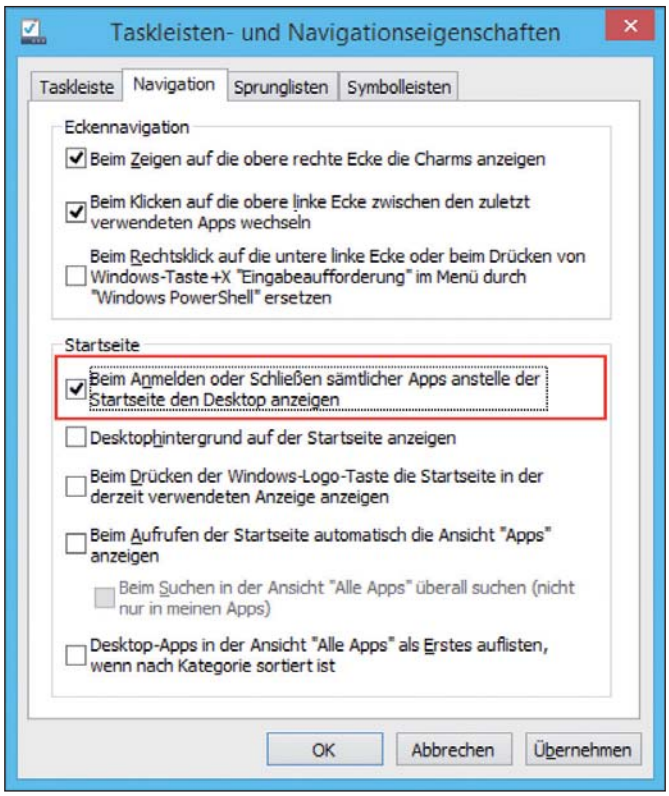
Mit **Windows 8.1** soll es ja angeblich möglich sein, **direkt auf den Desktop zu booten** und die Startseite mit den Kacheln zu überspringen. Jedoch habe ich diese Funktion auf Anhieb nicht gefunden. Können Sie mir hier weiterhelfen?

Auch diese Neuerung hat Microsoft relativ gut versteckt – in der Systemsteuerung werden Sie die Möglichkeit zum Durchstarten direkt auf den Desktop nicht finden. Stattdessen müssen Sie auf dem Desktop mit der rechten Maustaste auf die Taskleiste klicken und "Eigenschaften" auswählen. Im nun folgenden Fenster wechseln Sie zum Reiter "Navigation" und aktivieren dort die Checkbox "Beim Anmelden oder Schließen sämtlicher Apps anstelle der Startseite den Desktop anzeigen". Dass sich diese Option im beschriebenen Menü verbirgt, ist zwar nicht unbedingt logisch, hat aber den gewünschten Effekt. Nach einem Neustart des Rechners erscheint direkt der klassische Desktop. *(ln)*

Datenspeicher in der Cloud sind ja eine feine Sache, aber zusätzlich hätte ich die entsprechenden Files schon gerne **auch auf meiner**

Festplatte. Ist dies mit **SkyDrive** möglich, das in Windows 8.1 ja nun deutlich besser integriert ist? Und wenn ja, funktioniert dies nur mit allen Cloud-Dateien oder auch einzelnen ausgewählten?

Mit SkyDrive ist es unter Windows 8.1 kein Problem, alle Dateien, die Sie in der Cloud abgelegt haben, auch offline zu nutzen. Öffnen Sie hierfür die SkyDrive-App, bringen Sie am rechten Bildschirmrand die Charms-Leiste ins Bild, wählen Sie "Einstellungen" und zuletzt "Optionen". Hier schieben Sie nun den Regler "Auf alle Dateien offline zugreifen" von "Aus" nach "Ein". Beachten Sie allerdings, dass es einige Zeit dauern kann, bis die Synchronisation durchgelaufen ist. Das Offline-Vorhalten einzelner Cloud-Daten wie etwa bei Google Drive ist derzeit aber nicht möglich. *(ln)*



Die Option, um unter Windows 8.1 direkt auf den Desktop zu starten, verbirgt sich etwas umständlich in den Eigenschaften der Taskleiste

Über **Windows-Updates lädt Windows 8** auch Definitionsdateien von Windows Defender, neue Treiber und Aktualisierungen für andere Microsoft-Programme wie Office herunter – und zwar auch ohne die Nutzung der Windows Server Update Services (WSUS). Können Sie kurz schildern, was beim **Update- und Patch-Management ohne WSUS** zu beachten ist?

Bereits bei der Installation kann der Nutzer von Windows 8 auswählen, dass sich das Betriebssystem automatisch aktualisieren soll, um vor neuen Sicherheitsgefahren gewappnet zu sein. Sie können ohne weiteres auf diesen Schutz vertrauen und sollten ihn auch aktivieren. Die Konfiguration der automatischen Updates nehmen Sie am besten in der Systemsteuerung im Menü "System" und "Sicherheit / Windows Update" vor. Hier steht ein eigenes Menü zur Verfügung, mit dessen Hilfe die installierten Updates angezeigt werden, manuell nach neuen Updates gesucht wird und sich die Konfiguration dieser Funktion anpassen lässt. Zwar gibt es in der Charms-Leiste über "Einstellungen / PC-Einstellungen ändern" auch Möglichkeiten, Windows-Update zu verwalten, allerdings sind diese bei weitem nicht so weitreichend und effizient. So lässt sich zum Beispiel Microsoft Office ständig automatisch aktualisieren. Diese Funktion ist vor allem für den Spamfilter von Outlook interessant. Um die Aktualisierung für weitere Microsoft-Produkte zu aktivieren, gibt es im jeweiligen Installationsfenster des Programms die Möglichkeit, eine Anbindung per Windows Update durchzuführen. Klicken Sie auf den Link "Nach Updates suchen", überprüft Win-dows 8, ob aktuell Updates im Internet oder auf einem WSUS-Server verfügbar sind. Über den Link "Updateverlauf anzeigen" im Update-Fenster oder auf der linken Seite des Fensters können Sie sich anzeigen lassen, welche Updates heruntergeladen und installiert worden sind. Sind neue Updates verfügbar, zeigt Win-dows diese im Update-Fenster an. Sie können über die Schaltfläche "Updates installieren" die Aktualisierung des Rechners starten. Windows installiert dann aber nur die Updates, die im Fenster als wichtig angezeigt werden. Sind optionale Updates verfügbar, klicken Sie auf den Link des optionalen Updates und setzen Sie das Häkchen bei den Updates, die Windows installieren soll. Klicken Sie auf "Installieren", aktualisiert Windows Updates das Betriebssystem. Sie können dann die jeweilige Aktualisierung zur Installation auswählen oder über das Kontextmenü ausblenden, sodass diese nicht mehr angezeigt wird. Neue Systemtreiber zeigt Windows Update oft auch bei den optionalen Updates an. Ein Blick in dieses Fenster lohnt sich also oft. Haben Sie dann alle Updates entweder zur Installation ausgewählt oder über das Kontextmenü mit "Update ausblenden" abgewählt, sehen Sie im Hauptfenster von Windows Update, wie viele Daten das Programm herunterladen und installieren muss. Klicken Sie dann auf "Installieren", beginnt der Assistent mit der Installation des Updates. Über den Link "Einstellungen ändern" im Windows Update-Fenster öffnet sich ein Konfigurationsfenster, in dem Sie einstellen können, wie und wann Updates installiert werden sollen. Grundsätzlich können Sie hier zunächst konfigurieren, ob Windows 8 automatisch aktualisiert werden soll oder ob Sie die automatische Aktualisierung komplett deaktivieren möchten. Wenn Sie Windows 8 so konfigurieren, dass es sich automatisch aktualisiert, können Sie eine Uhrzeit einstellen, zu der die Aktualisierung durchgeführt wird. Wenn der PC zu diesem Zeitpunkt nicht gestartet ist, wird der Aktualisierungsvorgang automatisch im Hintergrund beim nächsten Start durchgeführt. Über den Link "Installierte Updates" links unten im Hauptfenster von Windows Update können Sie sich alle installierten Updates auf dem PC anzeigen lassen und bei Bedarf

einzelne Updates deinstallieren. Hier sehen Sie auch, wann diese Updates eingespielt worden sind. Über den Link "Ausgeblendete Updates anzeigen" bringen Sie die Aktualisierungen auf den Schirm, die nicht in den installierten Updates angezeigt, sondern von Windows 8 automatisch ausgeblendet werden, nachdem Sie diese Auswahl im jeweiligen Kontext der Aktualisierung getroffen haben. *(Thomas Joos/ln)*

CITRIX

Wir nutzen in unserem Unternehmen eine **XenDesktop 7-Infrastruktur**. Beim **Aufrufen einer gehosteten Anwendung**, wie beispielsweise dem Notepad, geschieht nun Folgendes: Das Programm scheint zunächst wie gewohnt zu starten – kurze Zeit später erscheint jedoch eine **Fehlermeldung und die Anwendung wird abgebrochen**. Woran liegt das und wie lässt sich das beheben?

Der Grund für das beschriebene Problem liegt aller Wahrscheinlichkeit nach in der "Time-Out"-Einstellung der Registry. Diese ist standardmäßig auf eine Minute festgelegt. Dauert der Start einer Anwendung in einzelnen Fällen länger, wird die Session automatisch beendet. Um die Einstellungen zu ändern, müssen Sie als Administrator folgende Änderungen in der Registry vornehmen. Suchen Sie nach der Eingabe von *regedit* den Schlüssel "HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ ControllCitrix \ wfshell \ TWI". Ist dieser nicht vorhanden, müssen Sie ihn zunächst erstellen. Dort ändern Sie nun unter "ApplicationLaunchWaitTimeoutMS (Type: REG_DWORD)" unter "Data" den Wert entsprechend. Die zusätzlich benötigte "Time-Out"-Zeit wird in Millisekunden angegeben. Beachten Sie, dass eine Eingabe unter 10.000 immer in 10.000 geändert wird, da der zulässige Mindestwert bei zehn Sekunden liegt. Nach Änderung der Registry müssen Sie die Disk mit den neuen Werten ja nach Provisionierungsmethode über die Machine Creation Services (MCS) oder die Provisioning Services (PVS) für die Benutzer neu bereitstellen beziehungsweise bestehende Kataloge updaten. *(Citrix/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

Ich verwende oftmals das **Tool wget für den Download von großen Dateien** – beispielsweise ISO-Images. Nun muss der Download jedoch **zwingend über einen HTTP-Proxy erfolgen**. Wie kann ich das Werkzeug oder auch andere Tools anweisen, **für den Download der Dateien einen bestimmten Proxy auf einem bestimmten Port** zu verwenden?

Das Problem lässt sich leicht durch das Setzen einer Umgebungsvariable lösen. Die Variable nennt sich "http_proxy". Diese können Sie entweder systemweit oder für einzelne Benutzer definieren. Für die systemweite Definition ist ein Eintrag in der Datei */etc/bashrc* vorzunehmen. Individuelle Benutzer können die Variable in der Datei *~/.bashrc* setzen. Lautet der Proxy beispielsweise "proxy.example.com" und hört auf den Port 3128, so sieht der entsprechende Eintrag in einer der beiden Dateien so aus: "export http_proxy=proxy.example.com:3128". Findet nun ein Zugriff auf der Kommandozeile auf eine HTTP-URL statt, so läuft der Zugriff immer über den definierten Proxy.

(Thorsten Scherf/ln)

Tools

Administratoren sollten auch in kleinen Infrastrukturen jederzeit über einen **vollständigen Überblick über Hardware, Software und Patches** verfügen, um Kosten wie auch Sicherheit der IT unter Kontrolle zu haben. Doch für den großen Wurf – ein Management-Werkzeug, das sich um Monitoring, Patchverteilung und mehr kümmert – fehlt in kleineren IT-Abteilungen oft das Budget. So hantiert der IT-Verantwortliche oft mit den Dashboards einer ganzen Reihe von Tools, um sich Überblick über seine Rechnerlandschaft zu verschaffen. Leider wissen diese Tools dabei oft nichts voneinander und die mit Ihnen gewonnenen Daten lassen sich nicht zu einer noch detaillierteren Sicht der Infrastruktur integrieren.

Dies ändert die Version 7 des Open Source-Tools **Spiceworks**. Die Software, deren Funktionalität es mit jeder Management-Suite aufnehmen kann, adressiert dabei insbesondere **kleine Infrastrukturen mit bis zu 250 Geräten**. Spiceworks kombiniert **Inventur, Monitoring und Helpdesk** in einer einfach zu bedienenden Anwendung. Es ermöglicht, schnell und bequem eine Bestandsaufnahme der Hardware, Software und Patches zu machen, die sich im Netzwerk befinden. So gibt das Werkzeug IT-Verantwortlichen die Möglichkeit an die Hand, das Netzwerk hinsichtlich neuer Software, dem Lizenz-Status, ausreichendem Speicherplatz auf Servern oder auch notwendigen Nachschub an Verbrauchsmaterial an Druckern zu überwachen. Dabei bietet die **Version 7 ein Modul für das Mobile Device-Management** und bringt signifikante Verbesserungen der Inventar- und Help Desk-Funktionen. Mit dem MDM-Modul lassen sich nunmehr alle Smartphones und Tablets genauso überwachen wie übliche PCs und auch das entsprechende Berichtswesen wird mitgeliefert. Ebenfalls neu in Version 7 ist die Fähigkeit von Spiceworks, Cloud-Dienste überwachen zu können. *(jp)*

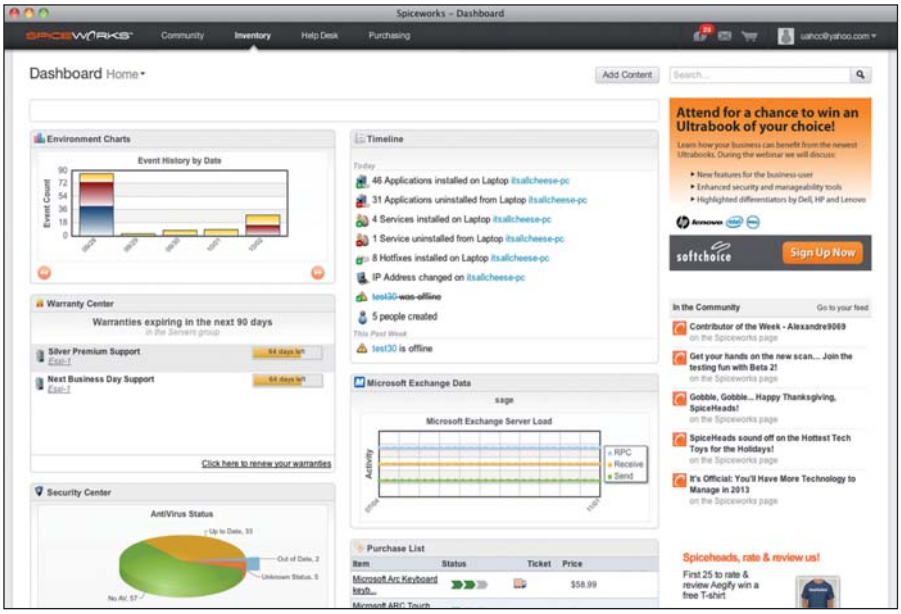
Link-Code: DBPE1

Neben den Klassikern wie "Ich habe mein Passwort vergessen" oder "Mein Monitor ist dunkel" dürfte das **Microsoft Office-Paket nach wie vor einen großen Anteil aller Help Desk-Calls** ausmachen. Dies lässt sich unter Umständen vermeiden, wenn IT-Abteilungen **Muster-Office-Installationen im Vorfeld auf mögliche Probleme untersuchen** könnten. Gleichzeitig wäre dem Support geholfen, wenn dieser genauere Informationen zu dem Problem gewinnen könnte, das sicher für den Endanwender am Telefon nicht immer in all seinen Details und Abhängigkeiten zu durchschauen ist.

Nachdem sich das entsprechende Tool für Outlook – Outlook Configuration Ana-

lyzer – als sehr populär erwiesen hat, stellt Microsoft nunmehr einen Nachfolger bereit, der das komplette Office-Paket unter die Lupe nehmen kann, das **Microsoft Office Configuration Analyzer Tool (OffCAT)**. OffCAT ist in der Lage, **mehr als 300 Office-Konfigurationsprobleme zu erkennen** und die Lösung per Link in die Knowledge Base bereitzustellen. Dabei untersucht das Tool nicht nur die Bestandteile verschiedener Office-Installationen, sondern bietet auch gezielt HotFix-Problemlösungen an, die nicht über Windows Update verfügbar sind. **OffCAT unterstützt alle Office-Versionen ab 2007** (inklusive Access, Excel, InfoPath, OneNote, Outlook, PowerPoint, Publisher, Visio und Word), die auf mindestens Windows XP SP3 laufen, und benötigt das .NET-Framework 3.5. Nach dem Programmstart sucht das Werkzeug nach neuen OffCat-Updates, sodass der Anwender stets mit einem aktuellen Diagnose-Tool arbeitet und ihm die neuesten HotFix-Downloads und Problemlösungen zur Verfügung stehen. Erreicht nun ein Help Desk-Call den Support, erhält dieser **nach einem Scan der problematischen Office-Installation einen ausführlichen Bericht**, der erlaubt, Einstellungen zu verändern oder die angesprochenen HotFixes oder Patches herunterzuladen. Diese Untersuchung lässt sich mit dem Kommandozeilen-basierten Teil von OffCAT sogar ohne Mitarbeit des Anwenders durchführen – üblicherweise wird der IT-Verantwortliche das Tool über die GUI bedienen. Ein solcher Scan ergibt selbstverständlich auch sehr viel Sinn, wenn IT-Verantwortliche ihn auf ein Muster-System loslassen, das später als Basis für den breiten Rollout des Office-Pakets dienen soll. Die OffCAT-Download-Seite bietet sowohl eine portablen ZIP-Download als auch einen MSI-Installer an. *(jp)*

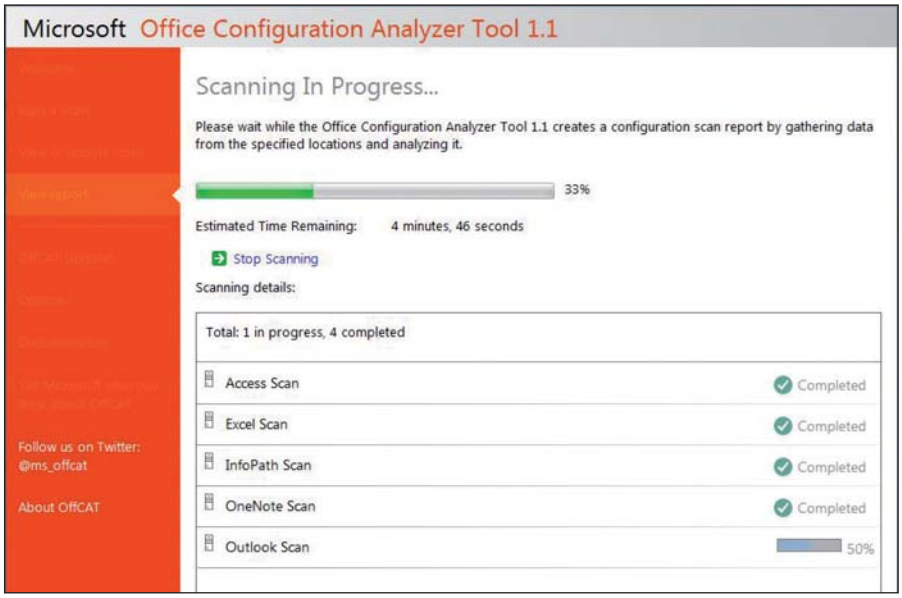
Link-Code: D5PE3



Das Dashboard von Spiceworks begrüßt den Administrator mit den wichtigsten IT-Statusinformationen

Virtualisierte Umgebungen haben besondere Anforderungen an den verwendeten Malware-Scanner, um beispielsweise im Rahmen eines Scans auf unerwünschte Eindringlinge nicht die Performance der Infrastruktur gen Null zu fahren. Aber auch die Möglichkeit, den Netzwerkverkehr verschiedener VMs zu trennen, gehört zu den besonderen Aufgaben eines solchen Scanners. Und wenn ein solches Sicherheitswerkzeug kostenlos zu haben ist wie **5nine Security for Hyper-V**, dann sollte der Administrator zumindest einen prüfenden Blick riskieren. Die Software **sichert Host-basiert und ohne Agenten virtualisierte Infrastrukturen unter Microsoft Hyper-V**. In Dienst genommen, schützt das Tool den Host wie auch die VMs durch sehr schnelle Malware-Scans und eine eingebaute Firewall. 5nine Security for Hyper-V bietet zur Verwaltung eine zentrale Management-Konsole oder den Zugriff per PowerShell beziehungsweise WCF APIs. Dabei lassen sich für jede VM **separate Einstellungen über Policies** vornehmen und diese neu erstellten VMs auch automatisch zuweisen. Auch erlaubt die Software, den Netzwerkverkehr von VMs, die auf demselben Host liegen, zu trennen. Zudem muss nur die Host-AV-Datei regelmäßigen Updates unterzogen werden, was die Ressourcen deutlich schont. Der eingebaute kostenlose Security- und Compliance-Scanner bietet neben den bereits erwähnten Features auch Performance-Checks, IDS und Empfehlungen für eine Optimierung der Sicherheit. Der Download ist nach einer Registrierung kostenlos möglich. *(jp)*

Link-Code: DBPE2



Nur noch Outlook fehlt, dann hat das Office Configuration Analyzer Tool die Analyse der MS Office-Installation abgeschlossen und informiert den Administrator per ausführlichem Bericht

Systemmonitoring bei der Gesellschaft für wissenschaftliche Datenverarbeitung in Göttingen

Neues Cockpit für den Admin

von Jens Michelsons

Die Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen – GWDG – ist eine gemeinsame Einrichtung der Georg-August-Universität Göttingen und der Max-Planck-Gesellschaft. Die GWDG erfüllt die Funktion eines Rechen- und IT-Kompetenzzentrums für die Max-Planck-Gesellschaft und des Hochschulrechenzentrums für die Universität Göttingen. In Sachen IT-Monitoring benötigte die GWDG eine zukunftsfähige Lösung, die die gesamte Infrastruktur – insbesondere ESX, Massenspeicher und Netzwerkkomponenten – umfasst und alle Teilbereiche der Infrastruktur in einem zentralen System konsolidiert.


Quelle: somatuscani – 123RF

Monitoring und Nagios sind für die GWDG keine Fremdworte. Wissen und Erfahrungen mit beiden Themen waren vorhanden, daher wollte die IT-Abteilung eine Nagios-basierte Lösung, um vorhandenes Know-how weiter nutzen zu können. Wichtig war den Verantwortlichen aber auch eine offene, flexible Architektur, die Anpassungen und Erweiterungen mit geringem Aufwand zulässt. Bei der Recherche stieß die GWDG auf das Open Source-Projekt openITCOCKPIT, das auf Nagios aufbaut, aber mit einer grafischen Weboberfläche und verschiedenen Zusatzmodulen für die Überwachung komplexer, heterogener IT-Infrastrukturen ausgestattet ist. Hinter dem Projekt steht der IT-Dienstleister it-novum, der die Entwicklung von openITCOCKPIT maßgeblich vorantreibt und Support sowie zusätzliche Module anbietet. Die GWDG entschied sich daher dafür, das freie Überwachungswerkszeug mit dem Hersteller einzuführen.

Pilotprojekt zeigt notwendige Anpassungen auf

Die Einführung von openITCOCKPIT wurde in zwei Schritten realisiert, der Durchführung eines Proof of Concepts (PoC) und der Implementierung und Anpassung der Software. Im Rahmen des PoC richtete der Dienstleister grundlegende Eigenschaften wie die Überwachung von Windows- und Linux-Betriebssystemen, der ESX-Farm und des Windows-Eventlogs sowie die Umsetzung des Provisioning von Systemen ein. Die Provisionierung sollte aus einer durch die GWDG selbst entwickelten Configuration Management Database (CMDB) erfolgen. Diese CMDB dient auf Basis einer Oracle-Datenbank zur Inventarisierung von Geräten. Daher musste die Lösung so konfiguriert werden, dass neu angelegte oder geänderte Assets automatisiert angepasst und erstellt werden. Dazu gehört auch das Anlegen von Hosts im Monitoringsystem. Durch die in openITCOCKPIT integrierte Provisioning-API ließ sich dies über definierte Schnittstellen schnell umsetzen.

Der Prototyp wurde zunächst noch sehr rudimentär gehalten: Die Aufnahme eines neuen Systems in die CMDB erzeugt eine E-Mail an openITCOCKPIT. Ein Parsing-Mechanismus übergab die erforderlichen Daten dann an die Provisioning-Schnittstelle. Problematisch an dieser Umsetzungsvariante war, dass diese E-Mailzustellung nicht sichergestellt werden konnte. Es zeigte sich schon zu diesem Zeitpunkt, wie Systeme automatisiert übernommen werden können. Doch wurde im Rahmen des Proof of Concept auch klar, dass die Schnittstelle in einem Folgeprojekt erweitert werden musste, um sicherzustellen, dass auch alle Systeme der CMDB in das Monitoring mit aufgenommen werden.

Dr. Konrad Heuer, Leiter der Arbeitsgruppe Nutzerservice und Betriebsdienste bei der GWDG: "Wir waren auf der Suche nach einer Open-Source-Monitoring-Lösung, die sich durch einfache Bedienbarkeit auszeichnet."

Die GWDG war mit dem PoC sehr zufrieden. Dr. Konrad Heuer, Leiter der Arbeitsgruppe Nutzerservice und Betriebsdienste bei der GWDG, kommentiert diesen Projektabschnitt: "Wir waren auf der Suche nach einer Open Source-Monitoring-Lösung, die sich durch einfache Bedienbarkeit auszeichnet. Schon der PoC zeigte, dass wir mit openITCOCKPIT auf dem richtigen Weg waren." Die GWDG beauftragte it-novum daher mit der Einführung der Überwachungslösung.

Integration mit Ticketsystem OTRS

In der ersten Projektphase ging es anschließend darum, das PoC-System erfolgreich zu migrieren und zu erweitern, ohne dass Funktionen der Infrastruktur, wie das ESX-Monitoring oder Windows-Eventlogs, ausfielen. Daneben mussten die Techniker sicherstellen, dass die Überwachung des Dateialters und die Kopplung mit dem intern betriebenen Ticketsystem OTRS reibungslos funktionierten. Große Bedeutung hatte dabei für die GWDG, dass Tickets automatisiert eröffnet, geschlossen und bei Folgenachrichten erweitert werden. it-novum musste daher entsprechende Konfigurationen und Mechanismen vornehmen, um zu vermeiden, dass eine Flut an Tickets automatisiert erstellt, aber im weiteren Verlauf nicht geschlossen wurde.

Diese Anforderung ließ sich mit dem Systemmonitoring-Modul in OTRS abbilden. So entscheidet OTRS anhand von regulären Ausdrücken logisch, um welche Art von Nachricht es sich handelt. Bei einem bereits zu diesem Problem offenen Ticket wird ein Follow-Up auf das bestehende Ticket generiert und die Statusinformationen in den Ticketverlauf mit übernommen. Erfolgt hingegen eine Wiederherstellungsmeldung durch openITCOCKPIT, wird das Ticket automatisiert mit der entsprechenden E-Mail geschlossen und bei neuen Problemen ein neues Ticket erzeugt. Einen zusätzlichen Mehrwert stellten zudem die bidirektionalen HTML-Verlinkungen zwischen den Monitoring-Services und den Tickets in OTRS dar, die it-novum einrichtete. Sie erleichtern es, einen Bezug zwischen Problem und aktuellem Status herzustellen. Die Integration beider Systeme liess sich durch die offenen Schnittstellen mit wenig Zeitaufwand vornehmen.

Customizing und hohe Anwenderakzeptanz

Die erste Projektphase verlief damit erfolgreich: Die GWDG verfügte innerhalb kurzer Zeit über eine zentrale Überwachungseinheit, die sich durch die Kopplung mit OTRS harmonisch in die Arbeitsabläufe der Wissenschaftsgesellschaft integrierte. Die Anwenderakzeptanz war von Anfang an sehr hoch, weil openITCOCKPIT als sehr übersichtlich und einfach in der Handhabung wahrgenommen wurde: Die Wizard-gesteuerten Möglichkeiten für die Konfiguration neuer Hosts und Services über die grafische Weboberfläche erleichtern den Mitarbeitern die Arbeit. Auch Personen, die über keine oder nur geringe Linux-Kenntnisse verfügen, können problemlos mit dem Monitoring-Tool arbeiten und Hosts und Services anlegen. Das trug im Wesentlichen dazu bei, dass sich openITCOCKPIT als zentrales Monitoringsystem etablieren konnte.

Im zweiten Projektschritt passte it-novum die Open Source-Software an die speziellen Anforderungen der GWDG an und erweiterte die Funktionen. Im Closed Source-Bereich sind dies in der Regel die schwierigsten Anforderungen, da die Anbindung eigener Entwicklungen meist nicht durch den Hersteller unterstützt wird oder mit hohen Kosten verbunden ist. Ein Open Source-basiertes System hat hier große Vorteile, da es sich aufgrund des offenen Sourcecodes und der Standardschnittstellen leicht anpassen oder erweitern lässt. Eine Herausforderung dabei war, sicherzustellen, dass auch alle Hosts in der CMDB angelegt werden. Dazu entwickelte der Dienstleister einen Importer, der alle neu angelegten Hosts in einem definierbaren Zeitraum aus der CMDB heraussucht und in openITCOCKPIT anlegt. Durch die direkte Verbindung zur Datenbank wird sichergestellt, dass alle Hosts auch wirklich angelegt wurden.

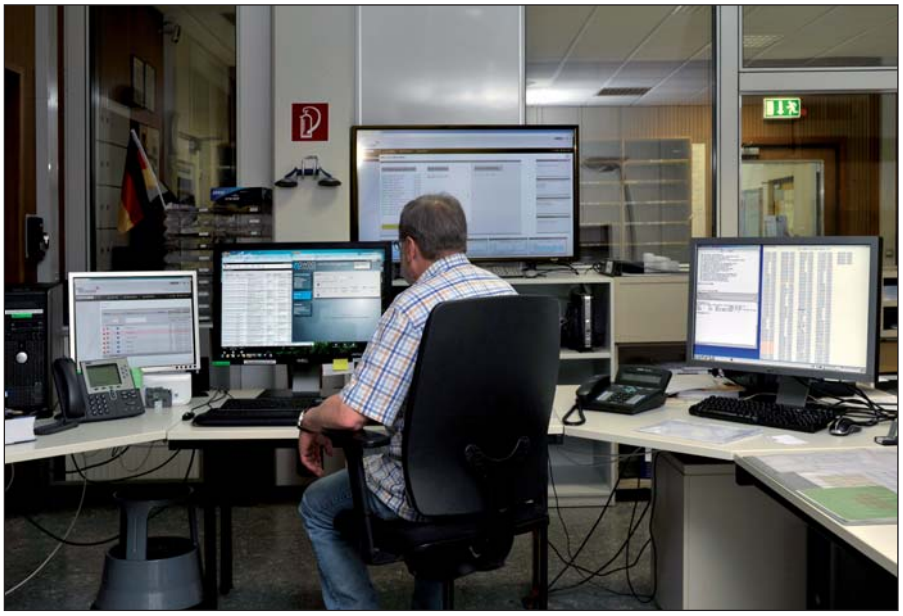


Bild 2: Auch Personen mit keinen oder geringen Linux-Kenntnissen können mit openITCOCKPIT arbeiten und Hosts und Services anlegen

Eine weitere Herausforderung bestand in der Validierung der Daten, da in der CMDB beispielsweise auch Umlaute und für Nagios nicht erlaubte Zeichen gespeichert werden können. Der Importer wurde daher so konfiguriert, dass er zuerst eine Validierung und Anpassung der Daten durchführt, bevor die Systeme angelegt werden. Da die CMDB eine Vielzahl an Informationen liefert wie Systeminformationen, Notfallpläne oder Ansprechpartner, legten die Verantwortlichen neben der geforderten Grundfunktionalität, die Hosts in openITCOCKPIT aufzunehmen, auch noch automatisiert eine Seite pro Host im DokuWiki an, die weitere Zusatzinformationen enthält. Für die GWDG war das ein großer Vorteil, denn dadurch lassen sich Informationen wie Kontaktdaten und Notfallpläne für die einzelnen Systeme weiterhin zentral pflegen, sie sind aber immer mit einem aktuellen Stand im zentralen Monitoringsystem vorhanden.

Überwachung des gesamten Netzwerks

Die GWDG betreut das Übertragungsnetz GÖNET, das die Göttinger Institute mit dem nationalen Wissenschaftsnetz X-WiN und dem Internet verbindet. Eine weitere Grundanforderung an neue Überwachungssoftware war daher die Überwachung des gesamten Netzwerks. Schwierig daran war, dass ein geeigneter Weg gefunden werden musste, um alle Performancedaten (Antwortzeiten, Paketverlust, Traffic, Errors & Discards) für die rund 75.000 Netzwerkinterfaces der Router und Switche des GÖNET aufzuzeichnen und darzustellen. Das bedeutet, dass alle fünf Minuten 280.000 Performancedaten gesammelt und verarbeitet werden müssen. Gleichzeitig sollte sich aber die eingesetzte Hardware auf ein Minimum beschränken. Die Idealvorstellung sah den Einsatz eines Mastersystems ohne Satellitensysteme zur Lastverteilung vor.

Um dieses Problem zu lösen, integrierte das Projektteam einen Datensammler, der sich ausschließlich um die Verarbeitung der Daten für das GÖNET kümmert, und "mod_gearman" zur Durchführung der Host- und Servicechecks. Durch die Erweiterung des Frontends von openITCOCKPIT integriert sich der Datensammler vollständig in das Monitoring- Framework. Die Software überwacht dadurch etwa 2.000 Hosts und 3.000 Services und verarbeitet 280.000 Performancedaten auf nur einer physikalischen Hardware. Durch die Einbindung des Datensammlers und mod_gearman ist das System außerdem so ausgelegt, dass es auch noch im weiteren Projektverlauf skalieren kann. Hier zeigt sich das Leistungspotenzial im Vergleich zu einem reinen Nagios-System: Nagios wäre angesichts der Menge an Checks in Kombination mit einer möglichst schlanken Hardware schnell an seine Grenzen gestoßen.

Zukunftsmusik: Umfassendes Servicemonitoring

openITCOCKPIT dient der GWDG als zentrales Monitoringsystem: "Inzwischen sind alle zentralen Systeme bei uns mit openITCOCKPIT überwacht, auch wenn der Umfang der Überwachung im Detail noch ausbaufähig ist", bemerkt Dr. Heuer. Die Forschungseinrichtung will daher den nächsten Schritt wagen. Geplant ist, die Infrastruktur immer weiter in Richtung eines umfassenden Servicemonitorings auszubauen. Dazu gehören für die GWDG neben einem umfassenden Monitoring auch die Themen Eventkorrelation und SLA-Reporting, eine Anforderung, aufgrund derer die GWDG sich ursprünglich auch für openITCOCKPIT entschieden hatte: Das System verfügt über die entsprechenden funktionalen Erweiterungen. Dr. Heuer bemerkt dazu: "Es zeigt sich, dass das Reporting über Ausfallzeiten immer wichtiger wird. Wir planen daher, die Qualitätsmanagementerweiterung zum SLA-Nachweis noch in diesem Jahr in Betrieb zu nehmen."

Um spezielle Ansichten für einzelne Anwender und Teilbereiche aufbauen zu können, denkt die GWDG langfristig auch über Visualisierungsmöglichkeiten durch NagVis und die bereits in der Community-Version verfügbaren Mandantenfähigkeit nach. Indem die Statusinformationen einzelner Checks und von korrelierten Zuständen genutzt werden, lassen sich vollständige Dashboards erstellen, auch speziell für einzelne Abteilungen. Durch die Bereitstellung diverser Services ist ferner eine Ende-zu-Ende-Überwachung angedacht. Auch ohne das Umsetzen dieser Funktionen verfügt die GWDG über ein organisationsweites Überwachungssystem für ihre Infrastruktur, das durch die offene Architektur zukunftssicher ist, weil es sich einfach und flexibel an sich verändernde Anforderungen anpassen lässt. *(dr)*

Jens Michelsons ist Senior Consultant bei der it-novum GmbH.

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.

iladministrator
Das Magazin für professionelle System- und Netzwerkadministration

Sicherer Datenaustausch bei MR-Datentechnik

Virtueller Tresor

von Tom Zeller

Der gesicherte Dateiaustausch zwischen Teams im Unternehmen oder mit Kunden und Geschäftspartnern wird immer häufiger auf dem kleinen Dienstweg per privatem Account bei einem Online-Speicher realisiert. Doch sind diese weder besonders gesichert noch von der IT gemanagt. Das IT-Systemhaus MR Datentechnik stand ebenfalls vor der Herausforderung, den reibungslosen Austausch von Daten für die Mitarbeiter bereitzustellen. Für welches Werkzeug sich das Unternehmen entschied, zeigt unsere Reportage.

Die MR-Datentechnik Vertriebs- und Service GmbH, ein inhabergeführtes Systemhaus mit Stammsitz in Nürnberg, wurde 1994 gegründet und verfügt heute neben der Zentrale in Nürnberg über neun weitere Niederlassungen in Deutschland und beschäftigt rund 360 Mitarbeiter.

Datenaustausch als Anforderung aus den Fachabteilungen

Im Jahr 2011 formulierten verschiedene Abteilungen der MR-Datentechnik die Anforderungen hinsichtlich einer zentralen und sicheren Plattform für den Daten-Austausch. In der Support-Abteilung etwa mussten täglich Updates, Patches, Fixes und so weiter für Kunden bereitgestellt werden, die oft die Größe der erlaubten Anhänge im Exchange überschritten oder gar nicht verschickt werden konnten, da ein Dateityp (zum Beispiel EXE) blockiert wurde. Die bislang genutzten Möglichkeiten von FTP stießen an Grenzen der Bedienbarkeit und Sicherheit.

Ein weiteres Beispiel war der Wunsch der Projektabteilung, die sich für die Abwicklung von Großprojekten mit komplexen Transition-Phasen ein einfaches und sicheres Tool zum Austausch auch von großen Datenmengen vorstellte. In diesem sollten die Mitarbeiter ebenso wie die Kunden jederzeit Zugriff auf den aktuellsten Stand der Dokumente haben. Dabei war ebenfalls wichtig, dass die verschiedenen Benutzer (interne, externe) über die Berechtigung unterschiedliche Zugriffsrechte auf die Inhalte haben.

Somit standen die Projektverantwortlichen Thomas Thiele und Thomas Heinke vor der Aufgabe, die Anforderungen zu definieren. Im Lastenheft stand an erster Stelle die zentrale Vergabe von Rechten und Benutzerrollen durch den Administrator. Es galt, die unterschiedlichen Gruppen wie Niederlassungen, die internen Projektteams sowie Kunden in die Lösung zu integrieren. Weiterhin musste das System sowohl für PCs und Notebooks mit unterschiedlichen Windows-Versionen als auch für Smartphones und Tablets mit den verschiedenen Betriebssystemen zur Verfügung stehen, damit die Daten von allen Nutzern plattformunabhängig genutzt werden können. Ein zentraler Virenscanner zur automatischen Überprüfung der Inhalte auf Schadcode war ebenfalls ein Muss. Auch wurde auf die Verschlüsselung und schon damals auf ein Angebot "hosted in Germany" geachtet.

Kostenrechnung entscheidet Evaluierungsphase

Die Evaluierung erfolgte primär durch IT-Leiter Thomas Thiele und sein Team sowie in einzelnen Projektgruppen. Im Rahmen der Evaluierung kam es auch zu der Frage, ob die Lösung inhouse betrieben werden soll oder als Software-as-a-Service. Die Lizenz- beziehungsweise Softwarekosten sowie die angebotenen Leistungen für Cloud-Speicher variierten zu diesem Zeitpunkt zwischen den unterschiedlichen Anbietern um bis zu 100 Prozent. Aus diesem Grund wurde eine Gesamtkostenrechnung durchgeführt und eine Verfügbarkeit von 24/7 inklusive Supportleistung zugrunde gelegt. Im Vergleich mit der Installation einer eigenen Infrastruktur konnte in der Vollkostenrechnung das Outsourcing unter Berücksichtigung des Support-Aspekts und leistungsfähiger Internetanschlüsse punkten.

Entscheidung für Secure Data Space

Nach Begutachtung verschiedener Angebote und Produkte fiel die Wahl bei MR-Datentechnik auf den Cloud-Speicher Secure Data Space der SSP Europe GmbH. Die Entscheidung machten die Verantwortlichen an drei Punkten fest:

1. Zentrale Verwaltbarkeit über eine eindeutige Adminrolle (Data Space Admin) im Secure Data Space und ein Rechte- und Benutzerkonzept, das ermöglicht, verschiedene Abteilungen, Organisationen und Personen in ein zentrales System einzubinden. Dabei war ebenfalls wichtig, dass der zentrale Admin über eine Zwischenrolle (Data Room Admins) Rechte zur Selbstverwaltung in die Abteilungen vergeben kann, sodass er nicht jede Änderung von Benutzern oder Neuanlage eines Datenraums selbst durchführen muss. Der Data Space Admin sollte aber nie die Hoheit über das Gesamt-System verlieren. In diesem Punkt überzeugte SSP Secure Data Space gegenüber dem Wettbewerb.
2. Ein attraktives und flexibles Lizenzmodell, das monatliche Änderungen in Stückzahl und Speicherplatz erlaubt und keine versteckten Kosten für Zusatzfunktionen beinhaltet.
3. Für ein Systemhaus sind die Sicherheit und Verschlüsselung von Daten ein "Muss". Im Rahmen des Geschäftsbetriebs werden sehr viele vertrauliche Daten mit Geschäftspartnern ausgetauscht. Secure Data Space hatte zum Entscheidungszeitpunkt bereits die serverseitige Verschlüsselung und die Verschlüsselung der Übertragung implementiert. Aktuell wird die Verschlüsselungstechnik des SSP Secure Data Space auf die Clientseite erweitert. Die Technologie bezeichnet der Anbieter als Triple-Crypt-Technologie. Die Datenverschlüsselung wird bei dieser Methode direkt durch die Anwendung auf dem jeweiligen Gerät durchgeführt. Die Verschlüsselung ist damit durchgängig vom Device (Local Encryption) über die Datenübertragung (Channel Encryption) bis hin zum Server, wo die Daten gespeichert werden (Server-Side-Encryption). Dies erfolgt in der ersten Version über den Web-Client (gängige Browser) und in Kürze auch über die nativen Clients (Windows, iOS, Andoid, BlackBerry 10).

Zum Einsatz kam der SSP Secure Data Space in der "dedicated"-Variante. Die Anwendung und die Daten liegen somit in den deutschen Rechenzentren von SSP Europe. Die Rechenzentren und die relevanten Prozesse sind nach DIN ISO 27001 zertifiziert.

Kurze Einführungsphase

Nach der Entscheidung für das Produkt SSP Secure Data Space wurden die notwendigen Parameter und Daten für die Erstinstallation von MR-Datentechnik bereitgestellt. Innerhalb einer knappen Woche war SSP Secure Data Space dedicated installiert, obwohl diese Instanz speziell für MR Datentechnik unter einer eigenen URL und abgesichert durch ein SSL-Zertifikat aufgesetzt wurde.

Wichtig für eine professionelle Einführung war der interne Workshop, in dem sämtliche Anforderungen der Abteilungen aufgenommen wurden und daraufhin die Raumstruktur inklusive der nötigen Berechtigungen festgelegt wurde. Im Anschluss erfolgte die Einweisung und Schulung der Schlüsselpersonen im Umgang mit der Lösung.

Der Secure Data Space ermöglicht nun durch die "Teamfunktion" eine zentrale Benutzer- und Rechtesteuerung. So bildet MR-Datentechnik Projektstrukturen über sogenannte Data Rooms ab. Dateien können somit innerhalb von Abteilungen oder Niederlassungen, aber auch übergreifend mit Kunden und Partnern, einfach und sicher ausgetauscht werden. Über die zentrale Adminfunktion werden die Rechte für Data Rooms, Subrooms und die verschiedenen Adminrollen gemanagt.

Erste Erfahrungen zeigen Nutzen für Vertrieb und Projektteams

Der Vertrieb nutzt den Dateiaustausch zur Information von Kunden in Form von Preislisten, Infobroschüren, Whitepaper oder technischen Datenblättern. Ein zentraler Downloadbereich kam hierfür nicht in Frage, da jedem Kunden individuell Unterlagen oder Angebote bereitgestellt werden müssen. Den Versand per E-Mail kann sich MR Datentechnik bei vertraulichen Informationen aus Sicherheitsgründen nicht erlauben. Große Dateien per E-Mail zu versenden, stößt bei Kunden immer wieder auf Schwierigkeiten, da die Server Anhänge dieser Größe nicht annehmen. Dies lässt sich inzwischen sehr komfortabel lösen.

Mit dem Secure Data Space erfolgt der Dateiaustausch in Form von Down- und Uploadlinks/Quicklinks, die optional passwortgeschützt und zeitlich limitiert sind. Der Mitarbeiter markiert eine Datei, vergibt ein Passwort und ein zeitliches Limit und wählt den Empfänger aus. Dieser erhält eine E-Mail und kann sich die Datei herunterladen. Das Passwort wird dem Kunden je nach Sicherheitslevel über einen Zweitweg wie etwa eine separate E-Mail, am Telefon oder als SMS mitgeteilt. Nach dem Download durch den Kunden erhält der Vertriebsmitarbeiter eine Benachrichtigung.

Die Projektteams von MR Datentechnik greifen in der Zusammenarbeit mit Kunden und deren Projektverantwortlichen auf die Daten im Cloud-Speicher über Notebooks, inzwischen aber auch immer mehr über Tablets und Smartphones zu. Der Zugriff über die mobilen Geräte erfolgt über Apps (derzeit hat MR Datentechnik iOS- und Android-Geräte im Einsatz) und auf PCs oder Notebooks über eine Laufwerkseinbindung, alternativ über ein Webfrontend aller gängigen Browser.

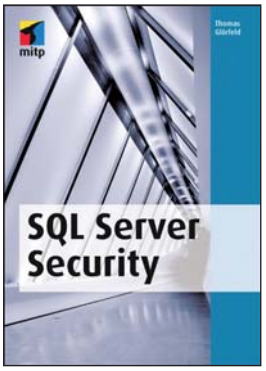
Sowohl die Laufwerkseinbindung als auch der Secure Data Space Windows-Client ist für die Projektteams inzwischen die effizienteste Form der Anbindung von Secure Data Space. Da sich das Notebook permanent mit dem Secure Data Space abgleicht, befinden sich immer die aktuellsten Projektdaten auf dem Notebook. Der Mitarbeiter muss nicht mehr vor jedem Termin prüfen, ob seine Unterlagen aktuell und vollständig sind.

Fazit

Secure Data Space hat sich im täglichen Gebrauch etabliert und ist ein gern genutztes Tool, um den modernen Arbeitsalltag mit dem nötigen Maß an Sicherheit zu erleichtern. Die Gesamtkosten inklusive der Einführung und Schulung der Mitarbeiter beliefen sich in den ersten zwölf Monaten auf einen mittleren vierstelligen Betrag für rund 60 User. Der Gesamtaufwand mit Evaluierung, Test, Einführung und Schulung belief sich geschätzt auf zehn Manntage. *(jp)*

Dipl. Ing (FH) Tom Zeller ist Business Development Manager bei SSP Europe.

SQL Server Security



Bei SQL spielt die Server-Sicherheit eine große und zum Teil manchmal vernachlässigte Rolle. Sieht der Administrator die Pflicht und Notwendigkeit, sich dieser anzunehmen, wird er vom Großteil der vorhandenen SQL-Literatur eher enttäuscht sein, da das Thema Sicherheit zumeist ausschließlich aus Softwaresicht oder der Anwendungsentwicklung im Allgemeinen behandelt wird. Diese Lücke soll das Buch "SQL Server Security" schließen, indem es sich den Gegebenheiten der Datenbanken und den Datenzugriffen selbst widmet.

Nach einer kurzen Einführung legt Autor Thomas Glörfeld die verschiedenen Möglichkeiten zur Authentifizierung und Autorisierung dar, die der SQL-Server bietet. Darauf aufbauend werden User und Rollen näher untersucht, die wiederum mit verschiedenen Rechten ausgestattet sind. Die Rechte-Thematik umfasst auch Beschreibungen zu Besitzverkettungen und datenbankübergreifenden Rechten. Im Anschluss werden alle Authentifizierungsmethoden mit den jeweiligen Architekturen in Verbindung gebracht. Die Wahl der richtigen Authentifizierung wird über die Architektur des DB-Zugriffs bestimmt.

Der SQL-Injection widmet Glörfeld sogar ein eigenes Kapitel, das insbesondere für SQL-basierte Webdienste äußerst interessant ist. Verschlüsselung mit asymmetrischen und symmetrischen Schlüsseln, der Einsatz von Zertifikaten und Hashing werden ausführlich in Bezug auf den Einsatz beim SQL-Server aufgezeigt. Expertenwissen präsentiert der Autor dann in den letzten drei Kapiteln, in denen er selten genutzten Security-Features, Auditing mit "SQL Audit" und Root-Kits im SQL-Umfeld Aufmerksamkeit schenkt. Zum Schluss noch lesenswert ist ein aufbereiteter Beitrag zum OS-übergreifenden Thema "Welche Rechte werden für das Debugging benötigt?"

Fazit

Administratoren müssen für den sicheren Umgang mit SQL-Diensten sorgen. Auf Basis des SQL Server 2012 findet der Interessierte in diesem Buch sicherheitsrelevante Themen zu SQL-Datenbanken und deren Zugriff. Die Aufbereitung ist umfassend und schlüssig dargestellt. Einziges Manko ist die Bindung: Aufgrund der vielen Codebeispiele kann das Buch kaum ohne praktische Umsetzung am PC durchgearbeitet werden. Leider ist die Bindung dafür nicht geeignet, da das geöffnete Buch irgendwie beschwert werden muss, um gleichzeitig am PC arbeiten zu können. *Frank Große*

Autor	Thomas Glörfeld
Verlag	mitp
Preis	39,95 Euro
ISBN	978-3826694219
Bewertung *(max. 10 Punkte)*	**9**

IT-Controlling für die Praxis

IT-Controlling ist nicht gleich IT-Kontrolle. Denn das Controlling umfasst vielmehr operative, administrative und strategische Aufgaben, die grob wie folgt zusammengefasst werden können: Sicherstellung der Unternehmensziele im Einklang mit IT-Zielen (strategisch), Koordination der Aufgaben der Planung, Steuerung, Kontrolle (administrativ) und Wirtschaftlichkeitsbeurteilung von IT-Investitionen und IT-Einsatz (operativ). Dr. Martin Kütz, Professor für Wirtschaftsinformatik an der Hochschule Anhalt, demonstriert in seinem Buch "IT-Controlling für die Praxis" die Notwendigkeit der betrieblichen Führungs- und Führungsunterstützungsfunktion eines IT-Controllers. Damit die Begriffswelten geklärt sind, stellt der Autor IT-Controlling zunächst als System vor, indem er die einzelnen Schwerpunkte sowie deren Adressaten erläutert. Ferner werden Prozessmodelle, ein kurzer Anriss zum Benchmarking und die Instanzen dargelegt. Als Sonderfälle separat behandelt Dr. Kütz die Ausgliederung und Auslagerung der IT, E-Business und E-Government sowie den Transfer von IT-Organisationen. Nach diesen Abgrenzungen besteht die Hauptaufgabe der folgenden zweihundert Seiten darin, die einzelnen Controlling-Methoden systematisch vorzustellen. Hier bringt der Autor dem Leser die Kosten- und Leistungsrechnung sowie Kennzahlen und Wirtschaftlichkeit aus der speziellen Sicht der IT näher. Auch wenn das Buch praktische Anwendungsmöglichkeiten vorweisen kann, bleiben die Hauptinhalte theoretischer Natur.

Fazit

In der vorliegenden zweiten, überarbeiteten Auflage seines Buches hat der Autor keine Veränderung an der Struktur vorgenommen, aber die einzelnen Kapitel zum Teil stark überarbeitet. Hintergrund sind die permanenten Änderungen an die Anforderungen im IT-Management aufgrund neuer Technologien wie Cloud oder E-Business, die in die Neuauflage eingeflossen sind. Administratoren mit Projektverantwortung sind bisweilen in das IT-Controlling einbezogen und können mit diesem Buch das Verständnis für die Terminologie und Hintergründe der zumeist wirtschaftlichen Begrifflichkeiten erlesen. Die vorgestellten Methoden beziehen sich auf die Bereiche der Kosten- und Leistungsrechnung und Verfahren der Bewertung und Entscheidungsfindung. In der zweiten Auflage ist auch ein Berechnungsverfahren für den IT-Wertbeitrag hinzugekommen. *Frank Große*

Autor	Dr. Martin Kütz
Verlag	dpunkt Verlag
Preis	44,90 Euro
ISBN	978-3864900037
Bewertung *(max. 10 Punkte)*	**8**

www.cloudtweaks.com

Crashkurs "Wolke"

Wenn in IT-Abteilungen oder in Gesprächen des IT-Verantwortlichen mit der Geschäftsführung das Thema "Cloud" aufkommt, haben die Gesprächspartner nicht selten völlig unterschiedliche Vorstellung von dem, was sich dahinter genau verbirgt. Der Geschäftsführer verspricht sich vielleicht eine Kostenreduktion durch die Möglichkeit, gewisse Dienste extern günstig einzukaufen und so das Geschäftsergebnis zu verbessern. Der IT-Verantwortliche hingegen möchte gern die interne IT automatisieren oder durch Virtualisierung Wege finden, IT-Dienste besser an die Anwender zu bringen. Oder beide Seiten sind sich einig in der Tatsache, dass für den Datenaustausch unter den Mitarbeitern ein regional nicht zu spezifizierender Dienst nicht in Frage kommt.

Wie auch immer die Diskussionen laufen, die Cloud wird aufgrund ihrer zahlreichen Aspekte auch zukünftig immer erklärungsbedürftig bleiben – und sei es allein, um sicherzustellen, dass alle Beteiligten über das gleiche sprechen. Hier kommt unsere Website des Monats unterstützend ins Spiel. Cloudtweaks.com liefert IT-Verantwortlichen und interessierten Geschäftsführern gleichermaßen anschauliches Infomaterial und Know-how rund um die Cloud.

Begrüßt wird der Besucher der Website mit Blog-artigen Newsmeldungen rund um Cloud- und Virtualisierungsthemen, die die Betreiber in Kategorien wie "Business", "How to", "SaaS", "Security" oder "Storage" einteilen. Schon hier zeigt sich, dass die mehr als 20 regelmäßigen Autoren technische wie auch geschäftliche Aspekte der Cloud-Nutzung betrachten. Besonders anschaulich stellt Cloudtweaks diese Themen in "Infographics" dar, die Aspekte des Cloud Computing komprimiert in einer anschaulichen Grafik darstellen. Ideal zur Schaffung einer gemeinsamen Basis in den eingangs erwähnten Gesprächen mit der Geschäftsleitung.

Erfrischend – und daher lobend hervorzuheben – ist die Integration von Humor in das technische Thema. Dazu bietet die Website eine eigene Sektion mit zahlreichen Comic-Strips. Gleichzeitig finden sich aber auch Fachartikel wie "5 New Technologies To Manage A Zombie Apocalypse". Dies macht die Seite eigentlich für jeden IT-Profi empfehlenswert. Denn wer sich selbst mit Cloud-Technologien herumschlagen muss, hat hier zumindest immer wieder die Gelegenheit zu einem Schmunzler. Und vieles lässt sich mit Humor auch leichter erklären. *(jp)*

Technisches wie auch Geschäftliches zum Thema Cloud bringt cloudtwaeks.com auf den Bildschirm

Unser Internetauftritt versorgt Sie jede Woche mit einem neuen interessanten Fachartikel. Diesen Monat erfahren Sie auf unserer Webseite mehr zu folgenden Themen:

Nutzung Array-basierter Snapshots beim Disaster Recovery

Analysten gehen davon aus, dass innerhalb der nächsten zwei Jahre 20 Prozent der großen Unternehmen von traditionellen Backup- und Recovery-Werkzeugen zu Technologien wechseln werden, die mit Snapshot- und Replikationstechniken arbeiten. Besonders Array Snapshots eignen sich für bisher unerreichte Recovery Point Objectives und Recovery Time Objectives. Unser Online-Beitrag führt auf, welche Punkte vor der Nutzung von Array Snapshots zu beachten sind – etwa deren Auswirkungen auf die Storage- und Netzwerk-Performance.

Link-Code: DBW51

Datenschutz bei inländischen Cloud-Diensten

Der Markt für Cloud-Dienstleistungen wird täglich größer – und unüberschaubarer. Vor allem Anbieter aus den USA wie Apple oder Amazon gelten in Deutschland derzeit noch als Marktführer und locken mit günstigen Offerten. Wie es dort jedoch zum Teil um die Sicherheit der Daten bestellt ist, ging in den vergangenen Wochen durch die Presse. Immer größerer Beliebtheit erfreut sich daher die deutsche Wolke. In unserem Fachartikel im Web analysieren wir die Vorteile von Cloud-Lösungen "Made in Germany".

Link-Code: DBW52

Sichere Datenlöschung in SAN-Umgebungen

Storage Area Networks sind die erste Wahl, wenn extrem viel Speicherplatz mit flexibler Zuteilung benötigt wird. Doch auch hier stehen Unternehmen regelmäßig vor der Herausforderung, SAN-Komponenten auszutauschen, da die Hardware nicht mehr den Anforderungen genügt. Doch wie können IT-Verantwortliche diese komplexen Systeme, die häufig auf unterschiedlichsten Technologien aufbauen und meist die gesamten Unternehmensdaten enthalten, zuverlässig löschen? Unser Online-Artikel geht genau dieser Frage nach.

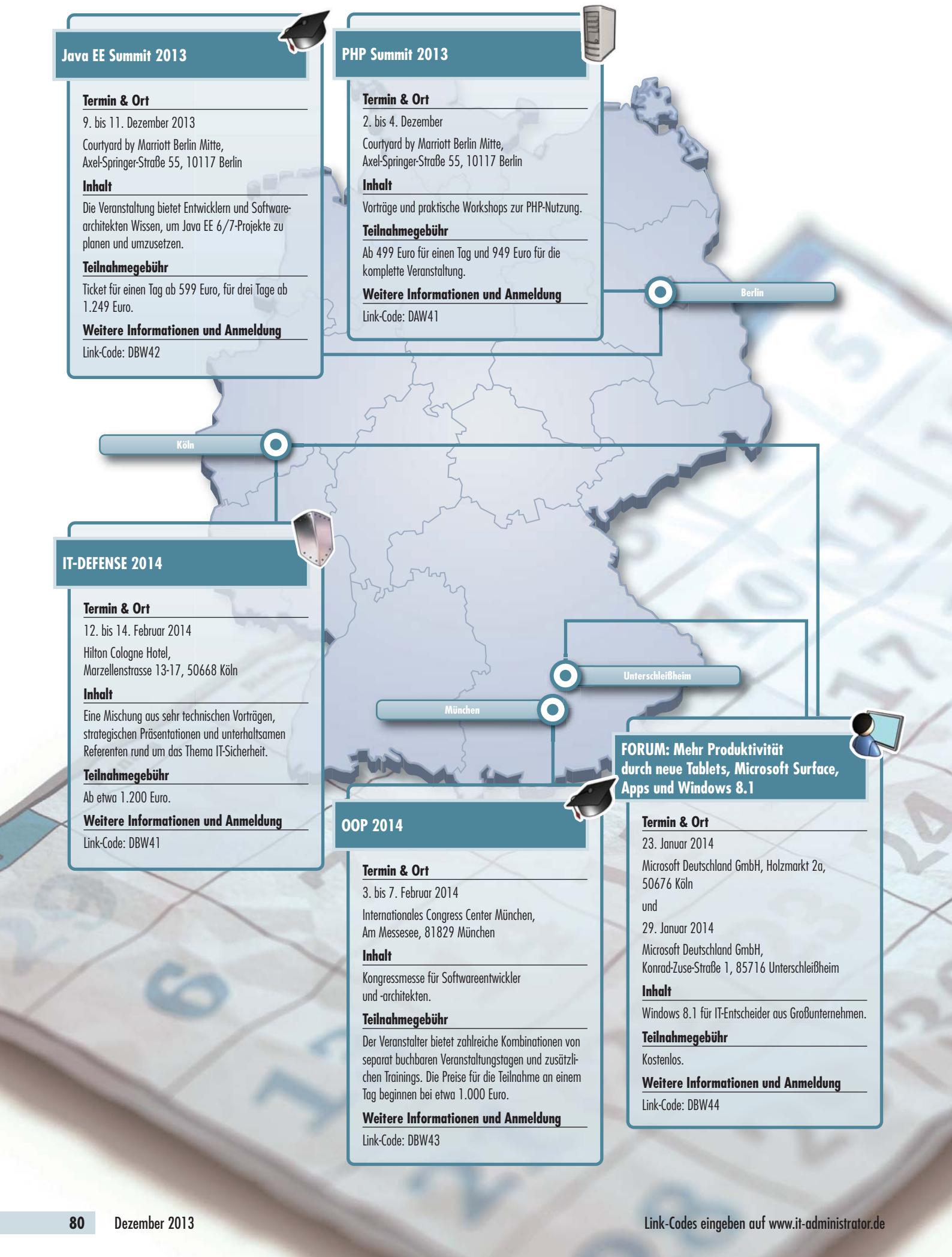
Link-Code: DBW53

Anwenderbericht: Monitoring der Webseiten-Performance

Als führendes Immobilienportal im deutschsprachigen Raum verzeichnet ImmobilienScout24 mehr als zehn Millionen User monatlich auf seinen Webseiten. Besonders der Zugriff über mobile Kanäle hat in den letzten Jahren immer mehr zugenommen und besitzt inzwischen einen Anteil von über 40 Prozent. Damit Nutzer immer auf die gewünschten Informationen zugreifen können, überwacht das Unternehmen die Performance seiner Website und mobilen Applikationen mit einem speziellen Werkzeug. Unser Online-Anwenderbericht wirft einen Blick darauf.

Link-Code: DBW54

Besser informiert: Mehr Fachartikel auf der Website des IT-Administrator



Java EE Summit 2013

Termin & Ort

9. bis 11. Dezember 2013

Courtyard by Marriott Berlin Mitte,
Axel-Springer-Straße 55, 10117 Berlin

Inhalt

Die Veranstaltung bietet Entwicklern und Softwarearchitekten Wissen, um Java EE 6/7-Projekte zu planen und umzusetzen.

Teilnahmegebühr

Ticket für einen Tag ab 599 Euro, für drei Tage ab 1.249 Euro.

Weitere Informationen und Anmeldung

Link-Code: DBW42

PHP Summit 2013

Termin & Ort

2. bis 4. Dezember

Courtyard by Marriott Berlin Mitte,
Axel-Springer-Straße 55, 10117 Berlin

Inhalt

Vorträge und praktische Workshops zur PHP-Nutzung.

Teilnahmegebühr

Ab 499 Euro für einen Tag und 949 Euro für die komplette Veranstaltung.

Weitere Informationen und Anmeldung

Link-Code: DAW41

IT-DEFENSE 2014

Termin & Ort

12. bis 14. Februar 2014

Hilton Cologne Hotel,
Marzellenstrasse 13-17, 50668 Köln

Inhalt

Eine Mischung aus sehr technischen Vorträgen, strategischen Präsentationen und unterhaltsamen Referenten rund um das Thema IT-Sicherheit.

Teilnahmegebühr

Ab etwa 1.200 Euro.

Weitere Informationen und Anmeldung

Link-Code: DBW41

OOP 2014

Termin & Ort

3. bis 7. Februar 2014

Internationales Congress Center München,
Am Messesee, 81829 München

Inhalt

Kongressmesse für Softwareentwickler und -architekten.

Teilnahmegebühr

Der Veranstalter bietet zahlreiche Kombinationen von separat buchbaren Veranstaltungstagen und zusätzlichen Trainings. Die Preise für die Teilnahme an einem Tag beginnen bei etwa 1.000 Euro.

Weitere Informationen und Anmeldung

Link-Code: DBW43

FORUM: Mehr Produktivität durch neue Tablets, Microsoft Surface, Apps und Windows 8.1

Termin & Ort

23. Januar 2014

Microsoft Deutschland GmbH, Holzmarkt 2a,
50676 Köln

und

29. Januar 2014

Microsoft Deutschland GmbH,
Konrad-Zuse-Straße 1, 85716 Unterschleißheim

Inhalt

Windows 8.1 für IT-Entscheider aus Großunternehmen.

Teilnahmegebühr

Kostenlos.

Weitere Informationen und Anmeldung

Link-Code: DBW44

»Fehlende Cloud-Sicherheit verursacht Bauchschmerzen«

Wolfgang Zwiefelhofer (50) stellt gemeinsam mit einem Kollegen bei der Münchner GULP Information Services den laufenden IT-Betrieb sicher. 1996 als Internet-Jobbörse von zwei Studienfreunden gegründet, vermittelt das Unternehmen heute als klassische Personalagentur Spezialisten in Projekt- und Interim-Management-Positionen. GULP beschäftigt derzeit über 210 interne Mitarbeiter und hat neben der Zentrale Niederlassungen in Frankfurt, Hamburg, Köln und Stuttgart sowie in Zürich.

Warum sind Sie IT-Administrator geworden?

Ein IT-Administrator steht jeden Morgen auf und weißt nicht, was der Tag bringen wird. Diese Spannung brauche ich, sonst wird mir langweilig. Mir gefallen auch die große Verantwortung und der tägliche Umgang mit den unterschiedlichsten Benutzern und ihren Bedürfnissen.

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

Zunächst würde ich jedem jungen Menschen raten, in sich hineinzuhören. Bin ich technikaffin? Komme ich mit der hohen Verantwortung zurecht? Bleibe ich auch unter Stress und Zeitdruck cool? Bin ich bereit in einem Beruf zu arbeiten, in dem das Lernen nie aufhört? Wer diese Fragen mit "ja" beantworten kann, hat sicherlich gute Chancen, in einem der spannendsten, abwechslungsreichsten und anspruchsvollsten Jobs der IT-Branche zu arbeiten.

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

Der tägliche Umgang mit Menschen und deren IT-Problemen bereitet mir am meisten Freude. Ich mag es aber auch, wenn ich durch knifflige und anspruchsvolle Aufgabenstellungen gefordert werde. Weniger Spaß macht es mir, kaufmännischen Entscheidern darzulegen, dass eine moderne und funktionierende IT auch Geld kostet.

Haben die Spionage-Enthüllungen zu einem Umdenken bezüglich Cloud-Nutzung im Unternehmen geführt?

Wir denken trotzdem weiter über eine Verlagerung von Daten in die Cloud nach. Ich bin hier aber sehr konservativ diesbezüglich eingestellt. Sensible Daten eines Unternehmens haben aus meiner Sicht in der Cloud nichts zu suchen. Ein gesundes, gewachsenes Unternehmen sollte sehr genau Vor- und Nachteile sowie die Risiken abwägen.

Woran hapert es in Bezug auf Webdienste und Cloud Computing am meisten?

Ich bekomme Bauchschmerzen, wenn ich an die fehlende Transparenz denke. So müssen internationale Provider viel deutlicher aufschlüsseln, wo ihre Server und Backup-Systeme stehen und welche Rechtssprechung gilt. Für problematisch halte ich auch eine mögliche Abhängigkeit des Kunden vom Anbieter und seiner Infrastruktur.

In welchem Projekt werden Sie in nächster Zeit arbeiten?

Das werden mehrere gleichzeitig sein. Zunächst wollen wir BlackBerry Enterprise Server 10 implementieren, verbunden mit einem Rollout von Z10-Geräten. Außerdem müssen wir uns mit der kniffligen Frage Cloud oder nicht Cloud beschäftigen.

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

Ganz klar unsere neue Swyx-Telefonanlage im Modus "Telefonkonferenzen". Diese werden permanent zerstückelt, die Sprache dadurch abgehackt. Seit einem halben Jahr gelingt es uns nicht, dieses Phänomen zu beseitigen.

Welches Netzwerk- und Systemmanagement nutzen Sie?

Die gängigen Microsoft-Tools, SCCM 2008 und PRTG. Aktuell teste ich gerade OpUtils als mögliche Ergänzung.

Welches ist der lustigste Anwenderfehler, der Ihnen untergekommen ist?

Anruf einer Mitarbeiterin: Meine Tastatur ist kaputt, ich kann nichts mehr eintippen. Nachdem ich mich über mehrere Stockwerke auf den Weg zu ihr gemacht hatte, reichte ein kurzer Blick auf die Tastatur, um einen Lachkrampf zu bekommen. Ich fragte die Mitarbeiterin: Was macht denn Ihr Locher auf der ESC-Taste? Daraufhin sie: Was hat das damit zu tun, dass meine Tastatur nicht mehr geht? Nachdem sie den Locher weggestellt hatte, funktionierte die Tastatur erwartungsgemäß.

Wie finden Sie den nötigen Ausgleich zu Ihrer Arbeit?

Im Sommer sitze ich gerne in Straßencafés und Biergärten und beobachte die Menschen. Im Winter bin ich dann mehr zu Hause und höre Musik von AC/DC, U2 und Bon Jovi. Dazu ein gut gebratenes Steak und die Welt ist in Ordnung.

Das Interview führte Petra Adamik.

Geburtstag: 26.09.1963
Admin seit: 17 Jahren
Hobbys: Fußball, Kochen, Reisen, Computer

Wolfgang Zwiefelhofer, IT-Administrator

Ausbildung und Tätigkeit

- Ursprünglich aus der Elektrobranche, 1991 Prüfung zum Industriemeister Elektrotechnik in der Fachrichtung Nachrichten- und Kommunikationstechnik
- Später Ausbildungen zum Organisationsprogrammierer und Netzwerkspezialisten
- Im Laufe der Jahre diverse Qualifizierungen als Microsoft Certified System Engineer (MCSE), Microsoft Certified Technology Specialist (MCTS) und für Citrix MetaFrame
- Heute IT-Systemadministrator

Betreute Umgebung

- Windows-Rechner und Windows-Server
- Active Directory, Exchange Server, Windows Terminal Server, Citrix Xen sowie
- Firewall, Backupsystem, Netzwerkverwaltung, Alcatel- und Swyx-Telefonanlage

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 01/14 erscheint am 30. Dezember 2013

Schwerpunktthema

Server-based Computing

Das lesen Sie in den nächsten Ausgaben des IT-Administrator:

Im **Februar** befasst sich IT-Administrator mit dem Schwerpunkt **Sicherer IT-Betrieb**. In den Tests beweisen unter anderem die virtuelle Appliance von AlienVault sowie BitDefenders GravityZone in a Box ihr Können. Im Praxisteil zeigen wir Ihnen, wie Sie Ihre Dateien unter Windows Server 2012 richtig klassifizieren und verwalten. Zudem lesen Sie, wie der sichere Umgang mit PowerShell-Credentials funktioniert und wie Sie mit TeamDrive Ihre eigene sichere Cloud betreiben.

Den Schwerpunkt im **März** bildet das **Management virtualisierter Server**.

Im Test: Citrix XenClient Enterprise 5

Im Test: SecureGUARD Office Cloud-Appliance

Workshop: Hyper-V-Host auf Windows Server 2012 R2 aktualisieren

Systeme: Open Source Business-Server Zentyal: Funktionen und Administration

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

Redaktion
John Pardey (jp), *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, Frank Große, Jürgen Heyer, Thomas Joos, Christian Knermann, Sandro Lucifora, Jens Michelsons, Dr. Holger Reibold, Thorsten Scherf, Christian Schulenburg, Matthias Wessner, Bertram Wöhrmann, Tom Zeller

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
Lightrays: 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-Hohestadt

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

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
Konto 174 966 462 bei der
Postbank Dortmund, BLZ 440 100 46
Kontoinhaber: Vertriebsunion Meynen

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

INSERENTENVERZEICHNIS

Die Ausgabe enthält eine Gesamtbeilage der Firma ppedv.

Das IT-Administrator Komplettprogramm!!!

NEU! Jetzt auch inklusive E-Paper!

Sichern Sie sich jetzt das **IT-Administrator Jahresabo All-Inclusive** mit allen Monatsausgaben 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 Abonummer 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/

Oder Sie sind Neukunde? Hier können Sie bestellen:

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

Virtuelle Systeme von transtec:
flexibel. sicher. einfach.

33 JAHRE PROFESIONELLE IT-SYSTEME UND LÖSUNGEN „MADE IN GERMANY“

- Erhöhen Sie die Flexibilität Ihrer IT-Infrastruktur
- Sparen Sie sich Pflege und Wartung Ihrer Hardware
- Profitieren Sie von einer hochverfügbaren, ausfallsicheren Lösung

intel inside XEON

Intel® Xeon ® Prozessor

transtec
accelerate productivity