

Administrator

Das Magazin für professionelle System- und Netzwerkadministration

Server-based Computing

Im Test

**H+H Software
NetMan 5**

22

Im Test

**Acceleratio Terminal
Services Log 3.7.5**

32

Workshop

**Remotedesktopdienste
in Windows Server 2012**

44

Systeme

Neues in Exchange Server 2013

50

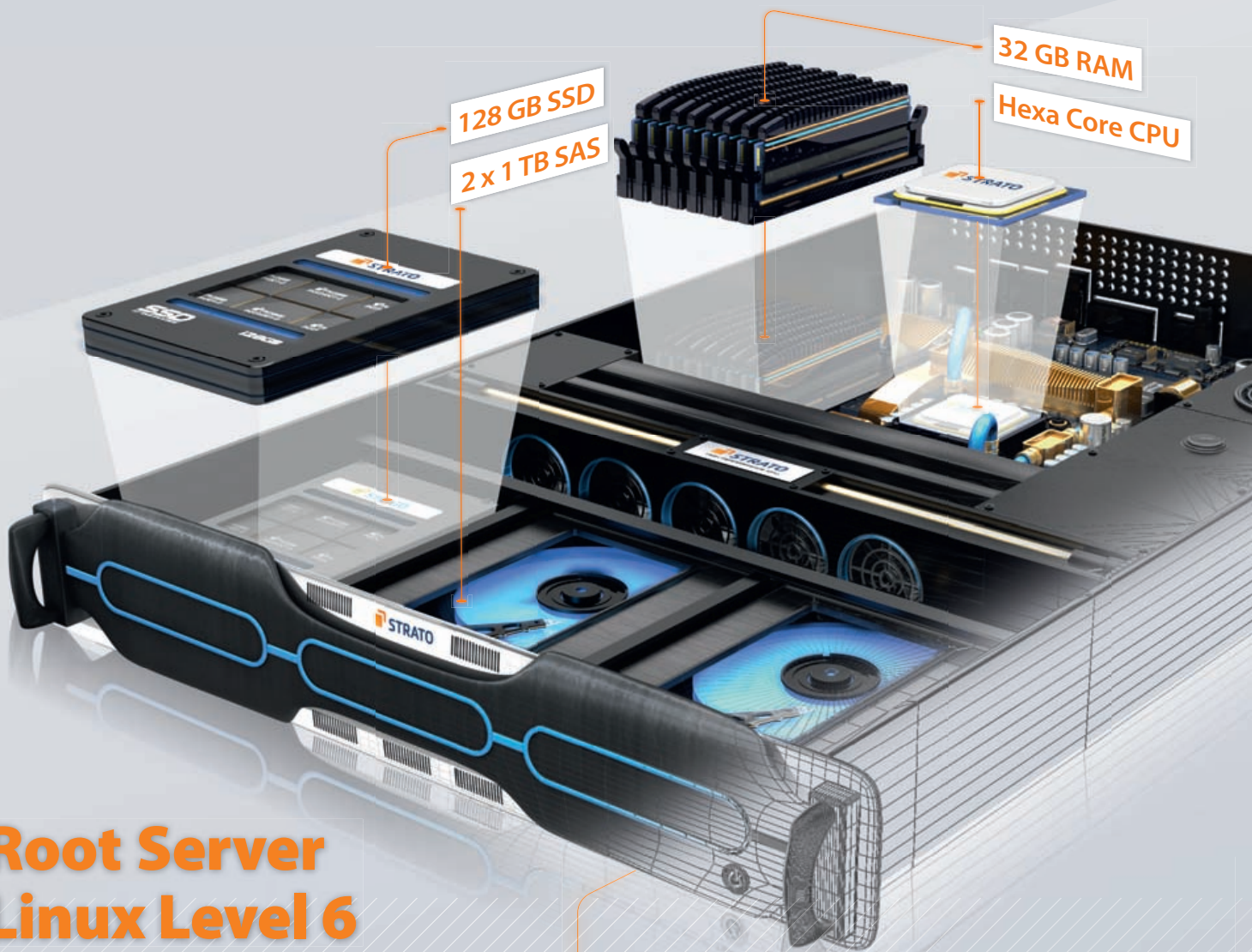
Workshop

**Windows Read-only
Domänencontroller einrichten**

59



PreisRAMbazamba



Root Server Linux Level 6

✓ keine Mindestvertragslaufzeit

✓ keine Einrichtunggebühr

99,00
€/Mon.*

CPU	Intel Xeon E5-1650 (Hexa Core)
Leistung	6 x 3,2 GHz
RAM	32 GB
HDD	1 x 128 GB SSD und 2 x 1 TB SAS
Traffic	Unlimited

HÖCHSTLEISTUNG ZUM KLEINEN PREIS



Der neue Root Server Level 6 punktet mit einem perfekten Zusammenspiel der Hardware. In jeder Situation steht Höchstleistung zur Verfügung.

Dank SSD-Drive starten Anwendungen und Prozesse blitzschnell. Ladezeiten waren gestern! Große Datenmengen finden auf den SAS-Festplatten (RAID 1) Platz. Für satte Beschleunigung sorgt der Intel Hexa-Core-Prozessor, dem ein großes und schnelles RAM zur Seite steht. Minimal ist hier nur eines – der kleine Preis!

* Aktion bis 26.12.2012. Traffic-Unlimited: Keine zusätzlichen Kosten durch Traffic (bei Traffic-Verbrauch über 1.000 GB/ Monat und danach je weitere 300 GB erfolgt eine Umstellung der Anbindung auf max. 10 MBit/s. Erneute Freischaltung der vollen Bandbreite jeweils kostenlos über den Kundenservicebereich). Preis inkl. MwSt.

Zwei und mehr Nullen

Liebe Leser,

was aktuelle Speichertrends angeht, haben sich schnelle SSD-Laufwerke mit aktuell bis zu 100.000 IOPS (!) endgültig aus ihrem Exotendasein befreit. Sie finden inzwischen Verwendung in vielen Rechenzentren und waren auf der Storage Networking World in Frankfurt ein großes Thema. Wie unser Vor-Ort-



Bericht auf Seite 12 zeigt, gibt es diverse Einsatzszenarien für die leistungsfähigen Flash-Speicher – unter anderem gebündelt in einer reinen SSD-Appliance, die VDI-Umgebungen zu mehr Power verhelfen soll. Womit wir beim Thema dieser Ausgabe wären – Server-based Computing. Ein Teilbereich dieser Technologie ist die Virtualisierung von Arbeitsplätzen, die trotz des Siegeszugs der Server-Virtualisierung noch keinen Durchbruch feiern konnte. Denn nicht selten sind es Performance-Probleme, etwa beim gleichzeitigen Hochfahren hunderter virtueller Desktops, die bestehende Storage-Systeme in die Knie zwingen. Dank flinker Flash-Appliances ließe sich dieser Flaschenhals wirkungsvoll weiten.

Server-based Computing ist ein weites Feld, und so beschäftigen wir uns im Workshop ab Seite 54 mit der Konfiguration und dem Betrieb von ThinLinc, einer alternativen Terminalserver-Lösung. Außerdem zeigen wir Ihnen in unserer Praxisrubrik ab Seite 44, wie Sie unter Windows Server 2012 die Remotedesktopdienste und virtuelle Desktops optimal nutzen. Zudem haben wir uns in der Test-Rubrik des Dezember-Hefts ab Seite 22 angesehen, wie sich NetMan 5 von H+H Software bei der Bereitstellung von Remote Desktops schlägt. In einem weiteren Test ab Seite 16 zeigte sich, welche Figur der 2X Application-Server XG 10.5 beim Management von Thin Clients macht.

Zum Schluss noch ein Wort in eigener Sache: Sie halten mit diesem Heft die 100. Ausgabe des IT-Administrator in den Händen. Seit September 2004 versorgen wir Sie mit viel Praxiswissen und konkreten Anleitungen zu den täglichen Aufgaben eines IT-Experten. Bis heute steigende Verkaufszahlen zeigen uns, dass wir mit dieser klar definierten Ausrichtung richtig liegen. Natürlich wollen wir das Jubiläum mit Ihnen feiern und verlosen zu diesem Anlass spannende Profi-Hard- und Software. Sie müssen unser Magazin allerdings ein wenig kennen, um die Chance auf einen der Preise im Wert von über 10.000 Euro zu wahren. Blättern Sie also am besten gleich auf Seite 10 und machen Sie mit beim Run auf heiße Preise – herzlichen Dank an dieser Stelle auch an die Sponsoren.

Viel Vergnügen beim Lesen sowie einen gelungenen Jahresausklang wünscht

Lars Nitsch
Redakteur

Server-based Computing

Im Test: 2X Application-Server XG 10.5



Gerade in homogenen Büroumgebungen sind Thin Client-Systeme eine geeignete und günstige Alternative zu neuer, teurer PC-Hardware. Besonders viel Geld lässt sich sparen, wenn bestehende, ältere PCs auf diesem Weg länger genutzt werden. Voraussetzung ist allerdings ein Werkzeug wie der 2X Application-Server XG, der die schlanken Clients verwaltet und dafür sorgt, dass sie die passenden Applikationen im Zugriff haben. IT-Administrator hat sich genauer angesehen, welche Möglichkeiten diese Zentrale bietet.

Seite 16

Im Test: TSplus 2012

Die Pluspunkte des Remotedesktop-Betriebs unter Windows liegen in der zentralen Bereitstellung, der Vermeidung lokal gespeicherter Daten auf dem Client-System und einer höheren Betriebssicherheit. Wegen dieser zahlreichen Vorteile hat sich der Terminalserver gegen die vielen Angriffe anderer Techniken stets behaupten können. In vielen Unternehmen wird diese Grundlage mithilfe von Citrix XenApp weiter veredelt. Die Kombination aus Microsoft Remotedesktop und Citrix XenApp ist jedoch aufgrund der zahlreich benötigten Lizenzen nicht gerade billig. Für kleinere Umgebungen ist dieser Weg oft zu teuer. Hier springt TSplus 2012 in die Bresche und will das volle Terminalserver-Vergnügen für einen deutlich geringeren Preis liefern. Ob dies gelingt, zeigt unser Test.

Seite 27

AKTUELL

- 06 **News**
- 10 **ITANet aktuell: 100 Ausgaben – IT-Administrator feiert Jubiläum**
- 12 **IT-Administrator vor Ort:**
SNW Europe, 30. und 31. Oktober, Frankfurt/M.
- 14 **IT-Administrator vor Ort:**
VMworld, 9. bis 11. Oktober, Barcelona

PRODUKTE


- 16  **Im Test: 2X ApplicationServer XG**
Mit dem Werkzeug lassen sich Thin Clients verwalten und die passenden Applikationen bereitstellen. Auch der Einsatz älterer PCs als schlanke Clients gehört zum Repertoire der Suite. IT-Administrator hat sich genauer angesehen, welche Möglichkeiten diese Zentrale bietet.
- 22  **Im Test: H+H Software NetMan 5**
Wenn die Remotedesktop-Funktionen von Windows nicht ausreichen, muss nicht unbedingt zu großen Lösungen wie XenApp greifen. Eine günstige Alternative will H+H Software mit NetMan 5 zur Verfügung stellen.
- 27  **Im Test: TSplus 2012**
Die Kombination aus Microsoft Remotedesktop und Citrix XenApp ist nicht gerade billig. Die Lizenzen sind für kleinere Umgebungen oft zu teuer. Hier springt TSplus 2012 in die Bresche und will das volle Terminalserver-Vergnügen für einen deutlich geringeren Preis liefern.
- 32  **Im Test: Acceleratio Terminal Services Log 3.7.5**
Gerade in größeren Terminalserverfarmen ist es für einen effizienten Betrieb überaus wichtig, Nutzung und Auslastung kontinuierlich zu überwachen. Ein äußerst umfassendes Monitoring verspricht hier Terminal Services Log von Acceleratio. IT-Administrator hat die Software getestet.
- 38  **Im Kurzttest: androidVNC 0.5.0**
Die Remote-Software VNC ist mittlerweile auch auf Android-Geräten angekommen. Bei Google Play sind einige VNC Viewer im Angebot. Wir haben einen Blick auf das kostenlose androidVNC geworfen.
- 39  **Einkaufsführer: Auswahlkriterien für KVM-Systeme**
IT-Verantwortliche benötigen einen Rundum-Blick auf alle Server und Prozesse sowie professionelle Managementlösungen. Lesen Sie in unserem Einkaufsführer, worauf es bei der Beschaffung der passenden KVM-Lösung ankommt.

PRAXIS

- 44  **Workshop: Remotedesktopdienste in Windows Server 2012**
Windows Server 2012 und Windows 8 haben neben der neuen GUI auch unter der Haube interessante Neuerungen zu bieten. IT-Administrator zeigt, wie Sie unter Server 2012 die Remotedesktopdienste und virtuellen Desktops optimal nutzen.

- 50  **Systeme: Neues in Exchange Server 2013**
Nach drei Jahren Pause ist die Aktualisierung nahezu aller Microsoft-Serverprodukte in vollem Gange – nun steht das neue Office 2013 an. Neben Lync, SharePoint und Office gehört auch eine Preview des Exchange Server 2013 dazu. Unser Beitrag wirft einen Blick auf die wichtigsten Neuerungen.
- 54  **Workshop: Konfiguration und Betrieb von ThinLinc**
Bei den Terminalservices wird die gesamte Ausführung der Applikationen auf einen Terminalserver verlegt. Wer dabei nicht auf die üblichen Anbieter setzen möchte, sollte einen Blick auf ThinLinc werfen. Unser Workshop erklärt, wie Sie den zentralen Terminalserver in Betrieb nehmen.
- 59  **Workshop: Windows Read-only Domänencontroller einrichten**
Für den sicheren Betrieb in Außenstellen bietet Microsoft den schreibgeschützten Domänencontroller an. Wie Sie diesen Read-only Domänencontroller in der Praxis einsetzen und welche Besonderheiten er mitbringt, lesen Sie in diesem Workshop.
- 64  **Workshopserie: Microsoft System Center 2012 (3)**
Da Microsoft System Center 2012 nur noch als Komplettpaket anbietet, erwerben Unternehmen auch weniger bekannte Werkzeuge der Suite automatisch. Diese dienen dem Virenschutz, dem Backup und dem Support und sind durchaus einen Blick wert, wie der abschließende Teil unserer Systems Center 2012-Reihe zeigt.
- 69  **Workshop: Windows PowerShell 3.0**
Mit der PowerShell 3.0 steht neben vielen anderen Funktionserweiterungen auch der PowerShell Web Access zur Verfügung – eine Funktion, die es ermöglicht, über ein Browserfenster die Serververwaltung von jedem beliebigen Ort aus durchzuführen.
- 70 **Tips, Tricks & Tools**

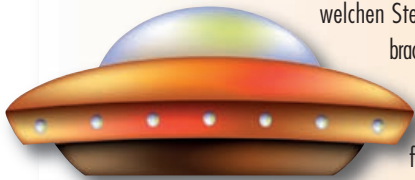
WISSEN

- 74  **Know-how: Application Performance Monitoring**
Moderne Applikationen führen oft zu komplexen Umgebungen und machen es teils unmöglich, den Grund für Performanceengpässe zu ermitteln. Worauf es deshalb beim Application Performance Monitoring ankommt, lesen Sie in diesem Beitrag.
- 78 **Know-how: Veranstaltungskalender**
- 79 **Buchbesprechung "VMware vSphere 5 – Lösungen für Administratoren" und "Wireless LANs, 4. Auflage"**
- 80 **Website & Fachartikel online**

RUBRIKEN

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

Konfiguration und Betrieb von ThinLinc



In Zeiten klammer Kassen loten Unternehmen aus, an welchen Stellen Einsparpotenziale ungenutzt brachliegen. Dabei erleben immer wieder auch längst vergessene Techniken eine Renaissance. Das gilt etwa für die Terminalsdienste, bei denen die gesamte Ausführung der Applikationen auf einen Terminalserver verlegt wird. Wer dabei nicht auf die üblichen Anbieter setzen möchte, sollte einen Blick auf ThinLinc werfen. Unser Workshop erklärt, wie Sie den zentralen Terminalserver in Betrieb nehmen.

Seite 54

Application Performance Monitoring

Die Architektur moderner Applikationen führt oft zu komplexen Umgebungen und macht es sehr aufwändig und zum Teil unmöglich, den Grund für Performance-Engpässe oder Ausfälle zeitnah zu ermitteln. Datenbanken, physische und virtuelle Infrastrukturen, Java oder .NET, Webserver, Netzwerkkomponenten und nicht zuletzt



das Endbenutzer-Verhalten können der Grund für diese Probleme sein und erfordern die Aufmerksamkeit der Administratoren. Worauf es beim Application Performance Monitoring ankommt, lesen Sie in diesem Beitrag.

Seite 74

Themenübersicht

 Server- und Systemmanagement	 Netzwerkmanagement
 Clientmanagement	 Job/Weiterbildung
 Storage	 Virtualisierung
 Sicherheit	 Recht
 Messaging	

www.it-administrator.de

Die große Freiheit

Die neue bintec W-Serie:

Die neuen bintec Access Points für den professionellen Unternehmenseinsatz



- ▶ Single-Radio für 2,4-GHz- oder 5-GHz-Betrieb
- ▶ Bruttoübertragungsraten bis zu 900 Mbit/s
- ▶ Stand-alone-Betrieb oder Betrieb mit WLAN Controller
- ▶ Elegantes, unauffälliges Gehäusedesign für Wand- und Deckenmontage
- ▶ Integrierte Mimo-Antennen für 2,4-GHz und 5-GHz

Mobile Datenkommunikation ist heute ein integraler Bestandteil der modernen Kommunikationskultur. Um den vielschichtigen, unternehmensspezifischen Anforderungen gerecht zu werden, bietet Teldat mit der **bintec W1003/2003 Access Point Serie** die passende Lösung. **Leistungsstark, skalierbar und sicher** - maßgeschneidert auf die individuellen Kundenanforderungen.



Teldat GmbH
Südwestpark 94
D-90449 Nürnberg
Telefon: +49-911-96 73-0

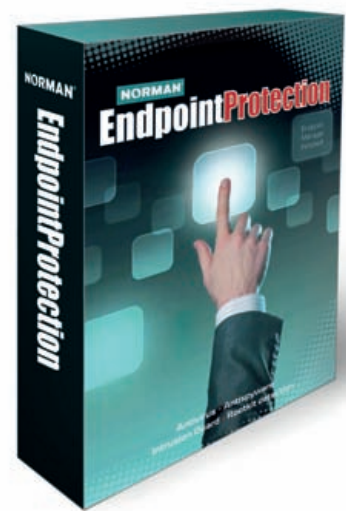


Antivirus auf Diät

Norman bietet die **Anti-Malware-Software Norman Endpoint Protection** (NPRO) in der **Version 9.1** an. Eine **neue Scan-Engine**, in der die Hash-Werte der Virensignaturen in komprimierter Form enthalten sind, soll dabei den **Platzbedarf im Hauptspeicher** erheblich verringern. So soll die Engine nur noch rund 23 MByte an Arbeitsspeicher belegen. Beim Scan-Prozess passt sie ihren Ressourcenbedarf an die Gesamtbelastung des Arbeitsplatzrechners an. Ein **neuer URL-Blocker** ergänzt zudem das signaturbasierte Verfahren und soll zusätzlich vor Malware von Webseiten unabhängig von Signaturen schützen. Weitere Verbesserungen bei der Erkennung bekannter

und unbekannter Malware will der Anbieter durch Neuerungen in der **Norman SandBox** erreichen, die als proaktiver Bestandteil der Scan-Engine in den Virenschutz-Produkten von Norman eingesetzt wird. Für höchstmögliche Stabilität und Performance hat Norman außerdem eine SQLite-Datenbank eingebaut. **Windows 8** wird ebenso unterstützt wie die neuen Versionen von **Microsoft Exchange** durch den Exchange Transport Scanner. Norman Endpoint Protection 9.1 ist ab sofort verfügbar. Eine Ein-Jahres-Lizenz der Standard-Edition für bis zu 50 Clients und Server kostet beispielsweise 1.644 Euro. (dr)

Norman: www.norman.com



Norman Endpoint Protection 9.1 will unter anderem mit einer deutlich schlankeren Engine punkten

Sicher durch die Cloud

SafeNet geht mit einer neuen Sicherheitslösung namens **ProtectV** an den Start. Die Software dient der **Datenverschlüsselung in virtuellen Umgebungen** – von der Erstellung bis zur Archivierung. Nutzer können damit geschäftskritische Anwendungen in virtuelle und Cloud-Umgebungen migrieren und dabei gleichzeitig die Einhaltung von Compliance-Richtlinien, Data Governance sowie die Kontrolle vertraulicher Informationen sicherstellen. ProtectV bietet hierfür eine granulare, vollständige **VM-Verschlüsselung**, **Pre-Boot-Authentifizierung** sowie eine **unternehmensinterne Hardware-basierte Zertifikatsverwaltung**. Alle VMs sowie verbundene Speichervolumina sind dabei verschlüsselt – sowohl VM-Instanzen als auch Snapshots und Backups sowie Disaster Recovery Sites. Selbst Super-User-Administratoren, die eventuell Kontrolle über die Virtualisierungsinfrastruktur haben, können laut Anbieter nicht auf die verschlüsselten VMs zugreifen. Als Bestandteil beinhaltet ProtectV hierfür die **SafeNet Enterprise Key-Management-Lösung KeySecure**. Diese ermöglicht das zentrale und einheitliche Management der Verschlüsselungsschlüssel für eine breite Palette an im Unternehmen eingesetzten Verschlüsselungsplattformen. Schlüssel- und Richtlinienadministration lassen sich so vereinfachen und zentralisieren. ProtectV ist als physikalische und virtuelle Appliance verfügbar. Der Preis für 30 Clients, zwei Management-Server, zehn Volumen-Lizenzen und zwei KeySecure-Appliances beträgt 38.300 Euro. (dr)

SafeNet: www.safenet-inc.de

BULLMAN stellt neben seinem seit August erhältlichen BULLMAN TAB7 MINI ALU eine preiswertere Variante mit Duroden-Gehäuse vor. Das neue Tablet **BULLMAN TAB7 MINI** besitzt dieselben Leistungsdaten der Aluminium-Version, kommt aber kleiner und damit günstiger daher. Das **7.0 Zoll große Android-Tablet** richtet sich in erster Linie an Kunden, denen ein kleinerer Bildschirm ausreicht. Mit Rechenleistung versorgt wird das Gerät durch die **Allwinner A13-CPU** mit 1,2 GHz Taktfrequenz. Zusammen mit dem **Quad Core-Grafikchip Mali 400** treiben die beiden Prozessoren das Multitouch-TFT von LG Electronics an. Das 7-Zoll-Display stellt die Inhalte mit 800 x 480 Bildpunkten dar. Als **TFT-Bildschirm** arbeitet es kapazitiv und reagiert laut Anbieter ohne Verzögerung. Fünf Punkte können dabei gleichzeitig verarbeitet werden. Für das Ablegen von Daten stehen **512 MByte DDR3-Hauptspeicher** sowie ein **4 GByte interner NAND Flash-Datenspeicher** bereit, der sich mittels TF-Card (Micro-SD) auf **32 GByte** erweitern lässt. Für die Aufnahme von Fotos oder für Videokonferenzen ist eine Frontkamera mit 1,3 Megapixeln integriert. Verbindung zum Internet erhalten die Anwender über das eingebaute WLAN im b-, g-

Günstiger Android-Begleiter

und n-Standard. Die UMTS-Funktion lässt sich über einen externen UMTS-Stick oder als Hotspot mit dem Handy integrieren. Für rund 92 Euro ist das BULLMAN TAB7 MINI ab sofort verfügbar. (dr)

BULLMAN: www.bullman.de

Das Tablet BULLMAN TAB7 MINI bietet ein 7-Zoll-TFT-Display



Das Tablet BULLMAN TAB7 MINI bietet ein 7-Zoll-TFT-Display

Vier gewinnt

Mit dem **CM1164** lüftet **ATEN** den Vorhang für ein 4-Port-Split-Screen KVM-Control Center, das mit **2.0 USB-Hub und Audio-Fähigkeit** ausgestattet ist. Das Gerät ermöglicht über einen einzigen Bildschirm **Multi-View-Zugriff auf vier oder mehr Computer** sowie die gemeinsame Nutzung von USB-Peripherie über eine Konsole. Das neue Control Center bietet drei Darstellungsarten: **Quad View, Bild-im-Bild- oder Vollbild-Modus**. Bei der Bild-im-Bild-Anzeige kann der Nutzer zwei bis vier Display-Inhalte auf einem einzigen Monitor mit einer Auflösung bis zu 1.920 x 1.200 Pixel bei 60 Hz betrachten. Über den Maus-Cursor kann er bestimmte Computer auswählen und bedienen und dabei Größe und Platzierung jeder einzelnen Bild-Quelle einstellen. Das Gerät wird über ein mausgesteuertes Menü konfiguriert, das eine große Zahl von Einstellungen wie etwa DCC, Bildschirmmodus, Port-Auswahl, Kanalbearbeitung et cetera zur Ver-

fügung stellt. Damit kann der Nutzer verschiedene Input-Quellen auswählen, steuern, konfigurieren und darstellen. Insgesamt vier CM1164 lassen sich miteinander verbinden und über Daisy Chain Control mit RS-232-Verbindungen steuern. Damit ist der IT-Verantwortliche in der Lage, bis zu vier PC-Gruppen über eine einzige Konsole mit Tastatur und Maus zu steuern. Jede Computergruppe kann aus vier Rechnern bestehen, denen ein bestimmter Monitor zugeordnet ist. Mit Hilfe der integrierten DynaSync-Technologie soll der CM1164 automatisch horizontale oder vertikale Abweichungen in den Einstellungen der einzelnen Computer erkennen und diese mit dem zentralen Monitor synchronisieren. Dadurch will der Hersteller stets die korrekte Bildauflösung bei einem Port-Wechsel sicherstellen. Das KVM-Control-Center CM1164 von ATEN ist ab sofort für 1.235 Euro erhältlich. (In/jp)

ATEN: http://de.aten.com/products/productItem.php?model_no=CM1164



Vier mal vier: Zu einer Vierergruppe zusammengeschlossen, erlaubt das neue VM-Control Center CM1164 die Steuerung von bis zu 16 Rechnern

Alles auf die 8

Langmeier Software stellt **Version 8** seiner **Backup-Software** für kleine und mittelständische Unternehmen vor. Die neue Version bringt zahlreiche Detailverbesserungen mit: Sie soll **einfacher einzurichten** sein und lässt sich mit weniger Einzelschritten installieren. Die **verbesserte Nutzeroberfläche** ist laut Hersteller an **Windows 8** angepasst und durch die selbsterklärende Menüführung intuitiv bedienbar. Anwender können **startfähige Speichermedien** wie bootfähige USB-Sticks oder CDs direkt in Langmeier Backup 8 erstellen. Zum Wiederherstellen startet die jeweils aktuelle Vorinstallations-Umgebung Windows PE (Preinstallation Environment) direkt vom bootfähigen Speichermedium. Ein kompletter Rechner lässt sich inklusive System-Status mit nur wenigen Klicks wiederherstellen. Unter-

nehmen können ihre Backup-Daten mit 128- und 256 Bit-Verfahren verschlüsseln. Dadurch sind sensible Daten sicher und können auch auf Online-Sicherungsservern abgelegt werden. Zur Sicherung lassen sich alle PC-Speichermedien verwenden, etwa lokale oder externe Laufwerke, Magnetbänder, CDs und DVDs, Blue-Ray Disks sowie Ordner im Netzwerk. Vollständige Server-Backups inklusive Microsoft SQL- oder Exchange-Server sowie Oracle Datenbanken-Server sind ebenfalls möglich. Die Backup-Speicherverwaltung warnt vor vollen Sicherungsdatenträgern per E-Mail. Über diese können die Benutzer direkt das Dialogfenster zum Aufräumen und Löschen von Daten öffnen. Für 125 Euro ist Langmeier Backup in der Business-Version verfügbar. (dr)

Langmeier Software: www.langmeier-software.com

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

DeviceLock bringt Version 7.2 der gleichnamigen **Data Leakage Prevention Suite** auf den Markt. Die Software soll verhindern, dass vertrauliche Unternehmensdaten auf mobile Datenträger oder über das Netzwerk kopiert werden und damit das Firmennetz unkontrolliert verlassen. Neu in Version 7.2 ist unter anderem die Unterstützung für RemoteFX. An die Terminalsession weitergeleitete Geräte lassen sich über die "TS Devices"-Gerätekontrolle kontrollieren. Zudem ist eine Inhaltskontrolle der Daten möglich, die zu Cloud-Anbietern wie Amazon oder Google übertragen werden. Auch Skype-Verbindungen lassen sich nun kontrollieren und einschränken. Zum Ende des Jahres soll Version 7.2 erscheinen. Die Preise für eine Einzellizenz liegen bei 28 Euro für 25 bis 49 Lizenzen. (dr)

www.deviceclock.de

Mit **Nitro Pro 8** stellt Nitro eine neue Generation seiner Alternative zu Adobe Acrobat vor. Mit der Software lassen sich **PDF-Dateien erstellen und bearbeiten**. Der Hersteller hat das jüngste Release nach eigenen Angaben an das Ribbon-Layout der aktuellen Microsoft Office-Produkte angelehnt. Neu ist neben der Smart-Alignment-Funktion auch ein automatisches Backup- und Recovery-Feature. Mit Hilfe von voreingestellten oder eigens angepassten Profilen lassen sich zudem Größe und Qualität der PDF-Datei bestimmen. Nitro Pro ist ab sofort in deutscher Sprache zu einem Preis von 120 Euro für eine Einzellizenz verfügbar. (In)

www.nitropdf.com/de/

Von Veeam kommt mit **Veeam ONE 6.5** eine neue Version der Software zum **Monitoring und Reporting in virtualisierten Umgebungen**. Das Werkzeug unterstützt im jüngsten Release mit vSphere 5.1 und Windows Server 2012 Hyper-V die aktuellen Hypervisoren von VMware und Microsoft. Zu den Neuerungen des Tools gehört ferner eine Integration in Veeam Backup & Replication, mit dem Ziel, die Kapazitätsplanung für das Backup in virtuellen Landschaften zu verbessern. Neu sind außerdem zusätzliche Alarm-Features und erweiterte Report-Möglichkeiten, unter anderem ein Flash-basierter Infrastruktur-Wachstumsreport. Die Lizenzgebühren von Veeam ONE 6.5 berechnen sich pro CPU-Socket (ab 400 Euro). (In)

www.veeam.com

Mit **Splunk Enterprise 5** veröffentlicht Splunk die jüngste Ausgabe seiner Software zur Datensammlung und -analyse. Die Berichte sind in der neuen Version laut Hersteller bis zu 1.000 Mal schneller; Dashboards sollen einfacher zu navigieren und zu verteilen sein. Integrierte PDFs ermöglichen den Nutzern, ihre Berichte oder Dashboards auf Anfrage oder nach Zeitplan mit anderen zu teilen. Neu ist auch, dass selbst bei einem Systemausfall Daten kontinuierlich indiziert und bereits indizierte Daten weiterhin durchsucht werden. Das Indexieren eines Datenvolumens von bis zu 500 MByte ist kostenfrei. (In)

www.splunk.com

Magisches Auge

Das **Videoüberwachungs-Portfolio von ALLNET** bekommt Zuwachs. Die **ALL2299 Outdoor PTZ-Kamera** verfügt über eine 360 Grad-Rundumsicht und ist laut Hersteller besonders dafür geeignet, um **große Areale im Außenbereich** im Auge zu behalten. Aufgrund des wetterfesten IP66-Gehäuses sowie der integrierten Heizung lässt sich die neue Kamera innerhalb eines Temperaturbereichs von -40 bis zu +50 Grad Celsius betreiben. Der Neuzugang wird über Highpower-PoE nach IEEE802.3at-Standard mit der benötigten Energie versorgt, womit sich eine von Steckdosen unabhängige Montage realisieren lässt. Lediglich die integrierte Heizung benötigt ein externes, separat erhältliches 24V Netzteil. Die Kamera soll mit Hilfe des eingebauten IR-CUT-Filter selbst bei schlechten Lichtverhältnissen unter 0,01 Lux noch **optisch hervorragende Aufnahmen** bieten und ist sowohl **im Tag- als auch im Nachtbetrieb** einsetzbar. Innerhalb des zu überwachenden Bereiches kann der

Nutzer bis zu 255 Punkte setzen, die die Kamera automatisch abfährt. Zusätzlich kann die Kamera nach festen Zeitplänen, beispielsweise nur außerhalb der Betriebszeiten, aufzeichnen. Die **Motion Detection-Funktion** ermöglicht Überwachungsszenarien, die im Falle eines Alarms unterschiedliche Aktionen, wie FTP-Upload, E-Mailbenachrichtigung oder Aufzeichnung auf einer Micro SD-Karte, starten. Mit der Privacy Mask Funktion lassen sich ferner bis zu 16 unterschiedliche Bereiche markieren, um sicherheits- und datenschutzrelevante Bildbereiche unkenntlich zu machen. Alle Optionen rund um Bildqualität, Helligkeit, Weißabgleich, Sättigung, Schärfe, WDR und 2D-Noise-Reduction lassen sich über die Weboberfläche der Kamera einstellen. Das 2,3 Kilogramm schwere Gerät verfügt neben einem 10/100 MBit-Netzwerkport über einen Micro SD Slot sowie über Alarm Input- und Output-Buchsen. Das Überwachungswerkzeug verbraucht im Normalbetrieb laut ALLNET maximal 20



Keine weißen Flecken auf der Überwachungslandkarte: Die ALL2299 Outdoor PTZ-Kamera bietet eine 360 Grad-Rundumsicht

Watt, durch Zuschaltung der Heizung erhöht sich der Stromverbrauch auf 50 Watt. Die ALL2299 Outdoor PTZ-Kamera ist ab sofort für 1.800 Euro verfügbar. (ln) ALLNET: www.allnet.de

Mehr Storage für den Mittelstand

HP erweitert sein **Speicherangebot für den Mittelstand** um zwei SAN-Lösungen: Bei **HP StoreVirtual Storage 4130 und 4330** handelt es sich um Speicher-Arrays, die bisher unter der Bezeichnung LeftHand HP P4000 erhältlich waren. Die neuen SAN-Speicher unterstützen neben iSCSI zum ersten Mal **8 GBit/s-Fibre Channel** sowie **verschiedene Hypervisoren** und sind laut HP vor allem für virtuelle Umgebungen konzipiert. Die Systeme nutzen dabei die Hardware der ProLiant-Gen8-Server DL360p. Die Neuerscheinung misst eine Höheneinheit, beherbergt vier beziehungsweise acht Festplatten und bietet bis zu 16 TByte Speicherplatz. StoreVirtual Storage lässt sich im Verbund mit der Virtualisierungssoftware Virtual SAN Appliance auf Microsoft Hyper-V und VMware vSphere aufsetzen oder alternativ als physikalische Appliance einsetzen. Unternehmen können damit laut Hersteller im laufenden Betrieb und ohne Unterbrechung physische Cluster-Knoten und Speicher hinzufügen. Die Lösung ist mit ihrem transparenten Failover hochverfügbar und soll selbst mehrere gleichzeitige Fehler überstehen. Auch das

Verschieben von Daten zwischen virtuellem und physischem Speicherplatz soll kein Problem darstellen. Die Listenpreise für StoreVirtual Storage 4130 und 4330 beginnen bei 11.500 US-Dollar. Zudem bringt der Konzern unter dem Namen **HP StoreEasy Storage** neue **NAS-Speicher auf Grundlage von Windows Server 2012** auf den Markt, die es unter anderem ermöglichen sollen, Speicher höher zu skalieren. Mit an Bord sind **native Deduplizierung und Speicher-Pools**. Nutzer können zunächst zwischen drei verschiedenen Varianten von HP StoreEasy Storage wählen: StoreEasy 1000 als Einstiegsserie bietet als Blade oder Tower bis zu 25 2,5

Zoll-Festplatten und stellt Speicherplatz von 5 bis 50 GByte zur Verfügung. StoreEasy 5000 richtet sich an den gehobenen Mittelstand und stellt auf drei Höheneinheiten zwei Knoten mit bis zu 400 GByte Speicherplatz bereit. StoreEasy 3000 schließlich ist als Gateway speziell für den Einsatz mit bereits bestehenden Disk-Systemen ausgelegt. Es unterstützt unter anderem 3PAR Storage und StoreVirtual Storage und soll es dem Nutzer ermöglichen, Datei- und Block-Kapazitäten dynamisch zu verschieben. Der Preis für die neuen NAS-Server startet bei rund 5.200 US-Dollar für ein Gerät mit 8 TByte Kapazität. (ln) HP: www.hp.com/de/



Mit dem StoreVirtual Storage 4130 / 4330 will HP der Speicher-Virtualisierung im Mittelstand einen weiteren Baustein hinzufügen

Globale Verschlüsselung

Applied Security feuert den Startschuss für Version 6.0 der **Verschlüsselungslösung fideAS file enterprise** ab. Die Software verschlüsselt Daten beliebiger internationaler Zeichensätze (Unicode), kann laut Hersteller unternehmensexterne Nutzer in ihr Sicherheitskonzept integrieren und unterstützt die simultane Einbindung mehrerer Windows-Domänen. Auch die Administration des Werkzeugs soll sich im jüngsten Release flexibler gestalten. Unter anderem ist das **Programm nun mandantenfähig**. Einzelne Unternehmens-einheiten können somit innerhalb des Netzwerks ihre Verschlüsselungsrichtlinien sowie die Datenzugriffsrechte selbst verwalten. Ein sogenannter Gruppenadministrator kann sämtliche Verschlüsselungsregeln innerhalb seines Organisationsbereichs vornehmen. Die Software realisiert dabei laut Applied Security ein Vier-Augen-Prinzip für sicherheitskritische Administrations-

aufgaben in Anlehnung an Sicherheitsstandards wie die ISO 27001 oder den BSI-Grundschutz. Neben der **Einbindung mehrerer Active Directory-Domänen** über den globalen Katalog soll die Integration einer externen Public Key-Infrastruktur möglich sein, wenn beispielsweise Smartcards zur Nutzerauthentifizierung benutzt werden sollen. Firmenexterne Nutzer erhalten einen exklusiv für sie konfigurierten Zugang: Mit einer kostenlosen Standalone-Version der Software authentifizieren sich die Nutzer bei der Unternehmensinstallation und können dann, so der Hersteller, in einer Art geschütztem Datenraum sicher auf die vertraulichen Daten zugreifen. Der Preis für fideAS file enterprise 6.0 richtet sich nach der Anzahl der damit ausgerüsteten Arbeitsplätze. Die Ausstattung von 50 Clients etwa schlägt mit rund 2.900 Euro zu Buche. (ln)

Applied Security: www.apsec.de

Disk-Backup reloaded

Fujitsu gibt die Verfügbarkeit einer neuen Generation seiner Data Protection Appliance **ETERNUS CS800 S4** bekannt. Bei dem Gerät handelt es sich um eine **Appliance für die Datensicherung auf Disk**. Nutzer können auf Funktionalitäten wie **Deduplizierung, Replikation und Path-to-Tape** zurückgreifen. Mit der überarbeiteten Technologie zur Deduplizierung will der Hersteller den Speicherbedarf um bis zu 95 Prozent reduzieren und die benötigte Netzwerkbandbreite um den Faktor 20 und mehr senken. Die Einstiegsversion des neu vorgestellten Geräts hat ein **Speichervolumen bis zu 10 TByte**. Bei Bedarf lässt sich die Kapazität schrittweise auf bis **240 TByte erweitern**. Die Appliance ermöglicht es zudem erstmals, Daten entweder in SAN- oder NAS-Umgebungen zu sichern. Die ETERNUS

CS800 S4 arbeitet laut Hersteller mit den Datensicherungslösungen NetBackup und Backup Exec von Symantec sowie Simpana von CommVault zusammen. Die Storage-Komponente ist gemäß Fujitsu zudem eine der ersten Appliances, die Symantec NetBackup OST mit Auto Image Replication unterstützt. Dadurch soll es einfacher sein, **Backups auf Systemen an entfernten Standorten** zu erstellen und so eine effektive Disaster Recovery-Strategie umzusetzen. Nicht zuletzt soll es möglich sein, auf der Appliance einen CommVault-Media-Agent zu installieren. Dadurch lassen sich Daten direkt auf das Gerät übertragen, ohne dass dazu spezielle Server-Hardware erforderlich ist. Die neue Data Protection Appliance ist zu einem Preis von 8.740 Euro erhältlich. (ln)

Fujitsu: www.fujitsu.com/de/

Bastion im Firmennetz

Fortinet bringt sein **Betriebssystem FortiOS in Version 5.0** auf den Markt. Das Sicherheitsbetriebssystem ist die Basis aller **FortiGate-Sicherheitsplattformen**. Die aktualisierte Version soll **über 150 neue Funktionen und Erweiterungen** mitbringen. Ein **Client-Reputationsfeature** bietet Nutzern dabei ein konsolidiertes Sicherheitsranking aller Geräte basierend auf Verhaltensmustern. Administratoren erhalten so gezielte und umsetzbare Informationen, mit denen sich bedrohte Systeme und potenzielle Zero-Day-Attacken in Echtzeit identifizieren lassen sollen. Das neue und verbesserte **Anti-Malware-System**, ergänzt um verhaltensbasierte und heuristische Methoden sowie Cloud-basierte AV-Dienste, sorgt zudem für Schutz. Dies umfasst auch Betriebssystemtests und eine Botnetz-IP-Reputation-Datenbank. Mit den AV-Signaturen soll FortiOS 5.0 eine mehrschichtige Absicherung gegen moderne raffinierte Malware bieten. Eine umfassende Kontrolle mobiler Geräte und **BYOD-Umgebungen** soll zudem durch Geräteidentifizierung und gezielte Zugriffsrichtlinien sowie Sicherheitsprofile je nach Gerätetyp, Gerätegruppe, Ort und Nutzung möglich sein. Auch ist die automatische Anpassung rollenbasierter Richtlinien für Anwender und Gäste basierend auf Einsatzort, Daten und Anwendungsprofil möglich. **Erweiterte Berichts- und Analysefunktionen** geben Administratoren wertvolle Informationen über das Verhalten ihres Netzwerkes, der Anwender, Geräte, Anwendungen und Bedrohungen. Neben dem erweiterten FortiOS 5.0-Betriebssystem für FortiGate-Geräte stellt Fortinet FortiManager 5.0, FortiAnalyzer 5.0 und FortiClient 5.0 vor. Diese neuen Versionen adressieren den stets wachsenden Bedarf an immer anspruchsvolleren Management- und Analysefunktionen für Netzwerkinfrastruktur und Endgeräte – sowohl in Unternehmens- als auch in Carrier-, MSP- und KMU-Umgebungen. Alle FortiGate-Appliances erhalten das FortiOS 5.0-Upgrade im Rahmen des Maintenance-Programms FortiCare kostenlos und automatisch. (dr)

Fortinet: www.fortinet.com



Die neue Data Protection Appliance ETERNUS CS800 S4 richtet sich an kleine und mittelständische Firmen oder den Einsatz in Außenstellen



IT-Administrator feiert Jubiläum Auf die 100!

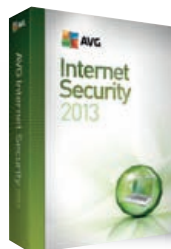
Es gibt etwas zu feiern! Seit 100 Ausgaben begleitet IT-Administrator seine Leser im Arbeitsalltag. Dabei ist das Angebot des IT-Administrator stetig gewachsen – zunächst um das halbjährliche Sonderheft, dann um praxisnahe Workshops und Trainings vor Ort. Und damit ist noch lange nicht Schluss! Zur Feier des Tages verlosen wir unter allen Teilnehmern der IT-Administrator Schnitzeljagd kreuz und quer durch das Heft Preise für alle Aspekte des professionellen IT-Betriebs.

Wie gut kennen Sie den IT-Administrator? Um erfolgreich an unserer Schnitzeljagd teilzunehmen, müssen Sie die folgenden fünf Fragen richtig beantworten:

1. In Ausgabe 08/2010 haben wir "WhatsVirtual 1.0 für Ipswitch WhatsUp Gold" getestet. Welcher unserer Autoren hat sich das Produkt angeschaut?
2. Seit Anfang 2008 ergänzen die Sonderhefte die monatlichen Ausgaben. Wie lautete der Schwerpunkt des ersten Sonderhefts (1/2008)?
3. Mit den Jahreszeiten wechseln auch die Titelfarben des IT-Administrator. Welche Farbe markiert typischerweise das Frühjahr?
4. Wie lautet der Name die Rubrik, in der wir jeden Monat einen Administrator interviewen?
5. In welcher Stadt sitzt der Heinemann Verlag, in dem der IT-Administrator erscheint?

Mitmachen können Sie unter dem **Link-Code CBA31** bis 31.12.2012.

Mitmachen und gewinnen!

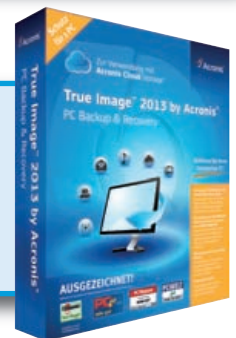


AVG Internet Security 2013 erkennt und blockiert Viren, Bedrohungen und Malware. Die Software hält Viren auf, bevor Sie den PC auch nur erreichen. Sie überprüft Dateien vor dem Öffnen, Facebook-Links vor dem Anklicken und checkt E-Mails, bevor sie eintreffen. Wir verlosen fünf Jahreslizenzen von AVG Internet Security 2013.



Personal Printing ist Cortados Lösung für sicheres, kostensparendes Drucken. Erst nach einer Authentifizierung am Drucker oder einem Multifunktionssystem startet der Nutzer seinen gewünschten Ausdruck, sodass die Vertraulichkeit gesichert ist und Toner- sowie Papierverbrauch gesenkt werden. Dieser Preis umfasst eine 5-Benutzer-Lizenz von Cortado Personal Printing im Wert von etwa 200 Euro.

True Image 2013 von Acronis bietet modernste Technologie für zuverlässiges Backup und Recovery von Systemen, Anwendungen und persönlichen Dateien. Synchronisieren Sie Dateien in lokalen oder Netzwerkverzeichnissen, zwischen mehreren PCs, mobilen Endgeräten und in die Acronis Cloud. Der Try&Decide-Modus erlaubt gefahrloses Testen neuer Anwendungen oder den Besuch von potenziell gefährlichen Webseiten. Wir verlosen insgesamt 10 Lizenzen von Acronis True Image 2013.

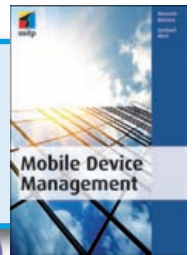


Der **Ultimate USB Hub** vom Online-Versand getDigital sorgt für Ordnung auf dem Schreibtisch! Insgesamt sieben USB-Geräte wie zum Beispiel Drucker, Tastatur oder USB-Gadgets können dort gleichzeitig angeschlossen werden. Dank der externen Stromversorgung via Netzteil stellt es kein Problem dar, alle Anschlüsse zur selben Zeit zu betreiben. Wir verlosen einen Ultimate USB Hub.



Mit der Inventarisierungssoftware **LOGInventory** erfassen Sie lückenlos die im Netzwerk installierte Hard- und Software. Zahlreiche Features wie etwa das integrierte Lizenzmanagement, die Anbindung an die Microsoft PowerShell, Historienauswertungen, das Hinzufügen manueller Eigenschaften und das Erstellen eigener Analysen sorgen für eine detaillierte Interpretation der gesammelten Daten aller physikalischen und virtuellen Assets im Netzwerk. LOGInventory arbeitet agentenlos, das heißt ohne Ausführung einer Client-Komponente auf den zu inventarisierenden Arbeitsplatzrechnern. Wir verlosen eine LOGInventory-Lizenz für 100 Assets mit Webinterface-Lizenz und zwölf Monate Software-Wartung im Wert von 970 Euro.

Das Buch **"Mobile Device Management"** stellt zunächst die Hardware der in der Praxis am häufigsten verwendeten mobilen Endgeräte vor und diskutiert anschließend die jeweiligen Betriebssysteme und ihre Abstammung. Darauf aufbauend untersucht der Autor Besonderheiten zu den Administrationsmöglichkeiten und Sicherheitsfunktionen der mobilen OS. Mobile Device Management ist natürlich auch ein Thema in den wichtigsten Sicherheitsstandards, etwa im Maßnahmen-Katalog des BSI-Grundschutzes. Wir verlosen fünf Exemplare von "Mobile Device Management" aus dem mitp-Verlag.



Der **xPrintServer von Lantronix** ist das richtige Produkt um die fehlende Verbindung zwischen iPhones und iPads und den lokalen Netzwerkdruckern im Büro zu überbrücken. Er unterstützt mehr als 4.000 verschiedene Drucker und ist denkbar einfach einzusetzen: Lediglich über Router, Switch oder LAN anschließen und innerhalb weniger Sekunden erkennt der xPrintServer automatisch alle Drucker im Netzwerk. Für die Verlosung wartet ein xPrintServer Network Edition im Wert von etwa 150 Euro auf den glücklichen Gewinner.



Docusnap ist eine Softwarelösung für IT-Dokumentation, die in der Praxis durch einen umfangreichen und markanten Funktionsmix überzeugt. Zusätzlich zur reinen Inventarisierung erfasst Docusnap auch die Konfigurationen wichtiger Applikationsserver und der Netzwerkdienste. Die Module Berechtigungsanalyse und das Lizenzmanagement erweitern die Funktionalität der Lösung. Der Gewinner dieses Preises erhält eine Docusnap-Lizenz im Wert von 1.500 Euro, je nach Netzwerkgröße als Voll- oder Zeitlizenz und einen Gutschein für eine Docusnap-Tagesschulung.

GFI WebMonitor verfügt in der aktuellen Version über neue Features, die wertvolle Informationen zur Produktivität, Bandbreite und Sicherheit von Unternehmensdaten liefern. Die neueste Version bietet ein Security Dashboard, mit dem IT-Administratoren potenzielle Schwachstellen und Engpässe frühzeitig erkennen und eingrenzen können. Mithilfe des Dashboards lassen sich wichtige Statistiken zur Sicherheit, Bandbreitennutzung und zum Produktivitätsverlust abbilden. Dem Gewinner dieses Preises steht eine 1-Jahres-Lizenz für 50 Seats der Unified Protection-Version von GFI WebMonitor zur Verfügung.



Die aktuelle **Version 10.4 des Solarwinds Network Performance Monitors** vereinfacht die Erkennung, Diagnose und Behebung von Netzwerkproblemen – bevor Ausfälle auftreten. Die Software überwacht Reaktionszeit, Verfügbarkeit und Uptime von Routern, Switches und anderen SNMP-aktivierten Geräten und zeigt Performance-Statistiken in Echtzeit über dynamische, analysierbare Netzwerk-Karten. Im Rahmen der Schnitzeljagd winkt dem Gewinner eine Lizenz im Wert von über 4.000 Euro.

Das **ReadyNAS Pro-D 2** mit 2 x 2 TByte-Festplatten ist der fortgeschrittene Netzwerkspeicher für Unternehmen. Ob ein IT-Verantwortlicher hoch verfügbaren Tier-1-Storage benötigt oder lediglich eine File-Backup-Lösung für eine lokale Arbeitsgruppe sucht, hat enorme Auswirkungen auf die benötigte Performance und das notwendige Budget. NETGEAR bietet hier höchste Flexibilität bei seinen ReadyNAS Pro-Lösungen. Wir verlosen ein ReadyNAS Pro-D inklusive Festplatten im Wert von zirka 680 Euro.



vRanger von Quest Software ist eine führende Datensicherungslösung für VMware-Umgebungen, die zudem physische Windows-Systeme mit hoher Geschwindigkeit und geringen Speicherplatzanforderungen sichert und wiederherstellt. Dabei profitieren Administratoren bei der Sicherung von physischen wie auch virtuellen Systemen von der intuitiv zu bedienenden Oberfläche, die alle Sicherungsaufgaben in einer GUI vereint. Unter allen Teilnehmern unserer Schnitzeljagd verlosen wir drei vRanger-Lizenzen im Wert von über 4.000 Euro.

ShadowProtect IT Edition bietet unlimitierte Wiederherstellung, Datenschutz und System-Migration für jedes Windows-System in Ihrer IT-Umgebung – Server, Desktops und Laptops – ohne vorherige Software Installation. Mit diesem Tool können IT-Verantwortliche von jedem System ein Backup erstellen, einschließlich Betriebssystem, Anwendungen und Daten, und diese auf einem externen Speicher sichern. Der Gewinner dieses Preises kommt in den Genuss einer Jahreslizenz der ShadowProtect IT Edition im Wert von etwa 2.000 Euro.



SNW Europe, 30. und 31. Oktober, Frankfurt/M. It's storage time!

von Lars Nitsch

Frankfurt im Herbst – das bedeutet für die Storage-Familie ihr jährliches Branchentreffen. Auf der SNW Europe gaben sich Speicher-Experten auch in diesem Jahr die Klinke in die Hand. Als besonders heiße Eisen gehandelt wurden der zunehmende Einsatz von SSDs und das Management großer Datenmengen. Was große Aussteller und Besucherzahlen anbetrifft, waren heuer jedoch Abstriche zu machen.



Besonders Vorträge zur Flash-Technologie fanden auf der SNW Europe 2012 regen Anklang

Teilnehmer bezeichnen die SNW gern als Klassentreffen der Storage-Branche. Was die rund 75 Aussteller anging, musste die SNW Europe in diesem Jahr allerdings auf die Klassensprecher verzichten – IBM, HP und EMC blieben der Veranstaltung fern. Ein leichter Rückgang um gut zehn Prozent machte sich auch bei den Besucherzahlen bemerkbar: Wurden im Vorjahr noch 1.850 Teilnehmer gezählt, fanden 2012 nur rund 1.650 Interessierte den Weg nach Frankfurt. Diese teilten sich auf knapp 140 Sessions auf, die wie stets einen soliden Querschnitt durch Storage- und Virtualisierungsthemen boten. Besonders erhellend waren dabei wie so oft die reinen Zahlen – so etwa erstaunte auch langjährige Storage-Veteranen der aus der Mottenkiste der IT gekramte Preis von 1 GByte Flash-Speicher vor nicht einmal 20 Jahren: 20.000 US-Dollar.

SSDs an allen Fronten

Diese hochpreisigen Zeiten sind jedoch passé. Die SSD-Technologie hat sich in der Unternehmens-IT endgültig durchgesetzt, sei es als schneller Cache zur Anwendungs-

beschleunigung oder als hochperformanter Tier 0. Demzufolge gab es zu diesem Thema besonders viele Vorträge. So etwa betonte Esther Spanjer von SMART Storage Systems, dass traditionelle Festplatten zwar nach wie vor Jahr für Jahr mehr Kapazität bereitstellten, die Latenzzeiten mit dieser Steigerung aber bei weiten nicht mithalten könnten. Da SSD-Platten zudem immer günstiger würden, sei mittelfristig zumindest mit einer Ablösung der mit 15.000 Umdrehungen pro Minute arbeitenden Magnetspeicher zu rechnen.

Ansonsten gehe es eher um eine Koexistenz beider Speichersysteme. Arrays, die ausschließlich auf SSDs basieren, seien noch immer die Ausnahme, könnten aber beispielsweise in VDI-Umgebungen – Stichwort Bootstorm – mit überschaubaren Kosten einen hohen Performance-Nutzen entfalten. Die Dozentin warnte jedoch davor, dass mit den schnellen SSDs neue Flaschenhälse entstünden. Nun läge es an der Netzwerk-Infrastruktur, die im Rechenzentrum bevorstehende I/O-Krise zu vermeiden.

Das große Datenwuchern

Nach der Etablierung der Cloud sind viele Hersteller darum bemüht, neue IT-Buzzwords zu schaffen. Das Stichwort "Big Data" umfasst vor allem zwei Teilaspekte: zum einen das langfristige Vorhalten und Archivieren großer Datenmengen, eventuell verbunden mit einem Medienbruch. Zum anderen die Analyse großer Ansammlungen von Informationen, angetrieben vor allem von den Marketing-Abteilungen mit einem Ziel: "to sell you more crap", wie es Shaun Walsh, SVP bei Emulex, recht undiplomatisch ausdrückte. Während Administratoren für letztgenannten Einsatzzweck wohl keine Lanze brechen dürften, sollte es zukünftig auch im Interesse von KMU-Betrieben liegen, den vorhandenen und neu anfallenden Datenbestand zukunftssicher zu verwahren – unter steigendem Kostendruck. Laut Frank Herold, Senior Manager Presales bei Quantum, würden derzeit mehr als die Hälfte aller Kosten im Bereich Tape-Archivierung dafür eingesetzt, die Daten bestehender Bänder durch Umkopieren am Leben zu erhalten.


Fazit

Die SNW erfreute auch 2012 mit einem breiten Themenspektrum im Storage-Sektor, unterstützt durch den Einsatz und die Originalität zahlreicher Branchen-Prominenter. Auch die Möglichkeit für Hersteller, Kunden und Presse, an zwei Tagen konzentriert Erfahrungen auszutauschen, stellte sich wieder als wertvoll dar. Es bleibt allerdings abzuwarten, wie sich die SNW in Zukunft bezüglich der Besucherzahlen und der damit verbundenen Themen gestalten wird. Der Storage-Kongress findet 2013 am 29. und 30. Oktober statt. 

PreisRAMbazamba

Vergleichen lohnt sich richtig!



Anbieter	 STRATO PRO TOP	Hetzner	1&1
Angebotener Preis	99,00 € / Mon.	79,00 € / Mon.	99,99 € / Mon. 1.-3. Monat
Server	Root Server Linux Level 6	Root Server EX 6S	Server XL 12i
CPU	Intel® Xeon® E5-1650	Intel® Xeon® E3-1245	Intel® Xeon® E5-2640
CPU-Benchmark*	13,185	8,278	10,832
CPU-Kerne	Hexa-Core	Quad-Core	Hexa-Core
CPU-Leistung	6 x 3,2 GHz	4 x 3,3 GHz	6 x 2,5 GHz
RAM	32 GB	32 GB	32 GB
Festplatte 1	2 x 1.000 GB SAS	2 x 3.000 GB SATA	2 x 2.000 GB SATA
Festplatte 2	1 x 128 GB SSD	1 x 120 GB SSD (15 €/ Mon.)	nicht verfügbar
Netzunabhängiger RemoteZugriff	✓ Serielle Konsole	19 €/ Mon. (KVM) 15 € (FlexiPack)	✓ Serielle Konsole
FTP-BackupSpace	1.000 GB	100 GB	250 GB
Parallels Plesk Panel	✓ 10 Domains	7,90 €/ Mon. (30 Domains)	✓
Mindestvertragslaufzeit	keine	keine	12 Monate
Einrichtungsgebühr	keine	149 €	keine
Einmalige Kosten	keine	149,00 € (Setup KVM)	keine
Monatliche Kosten inkl. Features	99,00 € / Mon.	135,90 € / Mon.	199,99 € / Mon. ab dem 4. Monat
Im ersten Jahr	1.188,00 €	1.928,80 €	2.099,88 €

VMworld, 9. bis 11. Oktober, Barcelona

Sonne und Wolken

von Jens-Henrik Söldner

Nur gut einen Monat nach der VMworld USA in San Francisco veranstaltete VMware die europäische Version der VMworld im sonnigen Barcelona und lockte immerhin rund 8.200 Besucher und über 125 Aussteller auf die kleinere und um einen Tag kürzere europäische Hausmesse. Die wesentlichen Änderungen wurden bereits in San Francisco Ende August verkündet: Neben dem Wechsel der VMware-Führung von Paul Maritz zum neuen CEO Pat Gelsinger war eine zentrale Ankündigung der VMworld USA die Vorstellung von vSphere 5.1, mit dem auch das im Zuge von vSphere 5.0 eingeführte und bei den Kunden äußerst ungeliebte vRAM-Lizenzierungsmodell nach nur einem Jahr wieder abgeschafft wurde. Paul Maritz übernahm auf der dortigen Pressekonferenz auch die Verantwortung für diesen Schritt, der bei den Anwendern einheitlich einen Aufschrei ausgelöst hatte. Nachdem diese Kehrtwende für gute Stimmung gesorgt hatte, stand in Barcelona die Technologie hinter vSphere 5.1 im Vordergrund.



Quelle: VMware

Auch die Ausstellung im Rahmen der europäischen VMworld konnte beeindrucken

VMwares Strategie ist nun auf die Bereitstellung des "Software-defined Data Center" ausgerichtet, dessen wesentliche Komponente die in San Francisco vorgestellte vCloud Suite 5.1 darstellt. Die Suite umfasst neben vSphere 5.1 in der Enterprise Plus-Variante je nach Edition (Standard, Advanced oder Enterprise) den vCloud Director zur Realisierung von IaaS-Cloud Umgebungen, das Netzwerksicherheitspaket und vShield-Nachfolger "vCloud Networ-

king and Security" (vCNS), die Disaster Recovery-Lösung "vCenter SRM", das Überwachungspaket "vCenter Operations Management Suite" und in der Enterprise Variante noch den "vFabric Application Director".

Auf der VMworld in Barcelona kam dann noch das "vCloud Automation Center" hinzu, das von nun an ebenfalls in der vCloud Suite 5.1 sowie separat erhältlich ist. Bisherige Kunden der vSphere Enter-

prise Plus-Version können im Rahmen einer Upgrade-Promotion ohne zusätzliche Kosten auf die vCloud Suite Standard umsteigen.

Auf Server und Storage folgt Virtualisierung im Netz

Grundidee des Software-definierten Rechenzentrums ist es, durch Virtualisierung die drei Grundzutaten von Rechenzentren – Server, Storage und Netzwerkkomponenten – komplett über Software steuern zu können und mithilfe der Virtualisierungsprinzipien "pooling, abstraction and automation" wie Ressourcen in einer Cloud-Umgebung zu behandeln. Während die Virtualisierung von Server- und Stagesystemen schon recht weit fortgeschritten ist, steckt die Virtualisierung und die damit mögliche Automatisierung der Netzwerkinfrastruktur – das Software-defined Networking (SDN) – noch in den Kinderschuhen. Hier verspricht sich VMware viel von der kürzlich erfolgten Akquisition des Netzwerkvirtualisierungsspezialisten Nicira, die auch aufgrund der ungewöhnlich hohen Summe – 1,2 Milliarden US-Dollar für ein Unternehmen mit gerade einmal 100 Mitarbeitern – für Aufsehen innerhalb der Branche gesorgt hat. Die Produkte von Nicira sollen Netzwerkdienste und die Verwaltung des Netzwerks von der Netzwerkhardware entkoppeln – ganz ähnlich dem, was die

Virtualisierung mit der Entkopplung der Betriebssysteme von der physischen Hardware erreicht hat.

Zur Übernahme von Nicira sind sich die Auguren uneinig. Einige Analysten halten die Übernahme für einen der klügsten Schachzüge, den VMware jemals gemacht hat, da es sich um eine Zukunftstechnologie handelt, die VMware auf Jahre hinweg in eine führende Position bringen soll und die das Geschäftsmodell der Netzkaufrüster, allen voran Cisco, in seinem Kern bedrohen könnte. Andere Branchenkenner wiederum sind weniger optimistisch und äußern sich unsicher, ob VMwares Plan, das Netzwerk genauso zu virtualisieren wie die Server, aufgehen wird und ob der Markt für diese Änderungen bereit ist. Unabhängig davon ist eine strategische Ausrichtung auf neue und zukunftsweisende Technologien auch bei VMware dringend notwendig, da im Markt der klassischen Hypervisoren auf die Dauer nichts mehr zu gewinnen ist – es ist nur noch eine Frage der Zeit, bis andere Hersteller, allen voran Microsoft mit Hyper-V, komplett aufgeschlossen haben oder vSphere technisch sogar überholen werden.

Neuerungen in vSphere 5.1

Das Kernprodukt von VMware ist nach wie vor die Virtualisierungsplattform vSphere, die VMware nun nach dem erfreulichen Wegfall der vRAM-basierten Lizenzierung auch als vCloud Suite 5.1 in Kombination mit anderen Produkten vermarktet. vSphere 5.1 führt die neue Virtual Machine Hardware Version 9 ein, die im Wesentlichen die Anzahl der CPUs einer virtuellen Maschine auf maximal 64 verdoppelt. Andere Einschränkungen, wie die maximale Dateigröße einer virtuellen

Dem lernwilligen Administrator stellte VMware über 36 virtuelle Lernlabore in Barcelona bereit, mit denen Interessierte die neuen Produkte einem Test unterziehen konnten. Bislang war die Benutzung dieser Labore nur während der Konferenz möglich, nun hat VMware aber angekündigt, dass die Labore auch danach verfügbar sein sollen. Interessierte können sich unter Link-Code CBA41 für die Übungsumgebung registrieren, ein genaues Datum, wann sie live geht, ist allerdings noch nicht bekannt.

Labs für daheim



Festplatte von 2 TByte, bleiben unverändert, obwohl zum Beispiel Microsoft daran schon vorbeigezogen ist.

Ansonsten bringt die neue Version zahlreiche Detailverbesserungen mit sich und führt nun den Flash-basierten Web-Client als neues favorisiertes Administrationswerkzeug ein. Alle neuen Features sind nur über den Web-Client zugänglich und nicht mehr über den herkömmlichen, bewährten Windows-basierten vSphere-Client. Hier gibt es für VMware noch viel Arbeit zu erledigen – die Administration mit dem Web-Client hinkt in Sachen Bedienkomfort und Geschwindigkeit noch deutlich hinter dem vSphere-Client hinterher.

Schlimmer noch ist die Tatsache, dass andere bestehende Features wie Host Profiles oder der Update Manager wiederum den herkömmlichen vSphere-Client zur Administration benötigen. Der Administrator muss daher mit zwei unterschiedlichen Werkzeugen arbeiten, was schlicht und ergreifend sehr ärgerlich ist. Auch die Wahl von Flash als Basis des Clients löst oftmals Kopfschütteln aus, da doch mit HTML5 eine plattformunabhängige Technologie zur Verfügung steht, die von VMware in anderen Produkten auch eingesetzt wird.

Für die Kunden angenehm ist, dass Features, die bislang nur in höheren Editionen verfügbar waren, nun die Editions-treppe heruntergefallen sind und nun auch in kleineren Varianten von vSphere bereits lizenziert sind. Hier ist unter anderem Storage vMotion zu nennen oder auch die Backup-Lösung vSphere Data Protection (der Nachfolger von Data Recovery), das ab der Essentials Plus-Edition enthalten ist. Ganz von ungefähr kommt diese Kundenfreundlichkeit allerdings nicht, denn mit der Verfügbarkeit von Windows Server 2012 wird der Riese aus Redmond zunehmend zu einer Bedrohung, der VMware nicht in einem Preiskrieg begegnen kann, sondern mit technologischer Überlegenheit der eigenen Produkte kontern muss. Diese ist zwar im Wesentlichen noch gegeben, aber in einzelnen technischen Aspekten hat Microsoft bereits gleichgezogen beziehungsweise VMware überholt.


Fokus auf die Desktops

Im Mittelpunkt der Keynote von CTO Steve Herrod am zweiten Tag der VMworld in Barcelona standen Neuerungen im Bereich "End User Computing", dem Geschäftsbereich, der bei VMware Produkte wie View, ThinApp und den Horizon Application Manager umfasst. VMware View ist inzwischen zu einer mächtigen und performanten VDI-Lösung gereift, allerdings macht der VDI-Markt trotz aller technologischen Fortschritte nur einen Bruchteil des Desktop-Marktes aus. Hier erweitert VMware seine Marktdurchdringung mit der im Mai erfolgten Akquisition von Wanova, das die Basis des neuen VMware Mirage darstellt.

Mirage ist eine Lösung, die die enge Kopplung von Userprofilen, Betriebssystem und Hardware bei Windows-Desktops durchbricht, Migrationen auf neue Windows Versionen deutlich erleichtert und das Verwalten von Desktops, egal ob physisch oder virtuell, über ein einziges Image abdeckt.

Lebendiges Ökosystem rund um VMware

Ebenfalls einen ausführlichen Besuch wert war die große Ausstellung, auf der neben Mitbewerbern wie Citrix – die eine Woche später mit ihrer Synergy-Konferenz ebenfalls in Barcelona vertreten waren – viele Partner mit neuen und spannenden Entwicklungen aufwarteten.

Besonders beeindruckend waren aus unserer Sicht die Lösungen des Netzwerk-Performance-Optimierers Riverbed, der Backup-Spezialisten Quantum, Acronis und Veeam und vieler anderer Anbieter, die im Storage- oder VDI-Bereich Innovationen vorantreiben. Auch kleinere deutsche Anbieter waren vertreten, wie etwa das Unternehmen "protected networks", das sein Berechtigungsmanagement "8man" auf die Analyse von vSphere-Umgebungen erweitert hat. (jp) 

Jens-Henrik Söldner ist Dozent für Wirtschaftsinformatik an der FOM Hochschule für Oekonomie und Management in Nürnberg und leitet das Infrastruktur-Consulting bei der Söldner Consult GmbH in Nürnberg.



Im Test: 2X ApplicationServer XG 10.5

Dickes Plus mit dünnen Clients

von Jürgen Heyer



Hersteller 2X hat sich ganz dem Server-based Computing (SBC) verschrieben und ist mit Produkten wie dem ApplicationServer und dem VirtualDesktopServer (siehe IT-Administrator-Test in der Ausgabe Mai 2011) recht erfolgreich. Den gerade erschienenen ApplicationServer XG 10.5, abgekürzt AS, hat 2X deutlich aufgewertet, indem ein umfassendes Thin Client-Management integriert wurde. Diese Funktion wurde bisher als eigenes Produkt namens ThinClientServer angeboten und ist jetzt eine Option des AS. In unserem Test haben wir den besonderen Fokus auf diese Thin Client-Features gelegt, aber auch die übrigen Funktionen des AS betrachtet, da letztendlich alles zusammenspielt.

Ein Werkzeug für alle Clients

Durch die Integration ist der AS noch universeller einsetzbar geworden. Seine Kernfunktion besteht in der Bereitstellung von Applikationen oder Desktops mit Hilfe von Terminalservern unter Windows Remote Desktop Services und Citrix XenApp sowie VDI-Clients. Auf der Clientseite wiederum lassen sich normale PCs verwenden, auf denen ein Software-Client zu installieren ist, oder jetzt eben auch

Gerade in homogenen Büroumgebungen sind Thin Client-Systeme eine geeignete und günstige Alternative zu neuer, teurer PC-Hardware. Besonders viel Geld lässt sich sparen, wenn ältere PCs auf diesem Weg länger genutzt werden können als ursprünglich vorgesehen. Voraussetzung ist allerdings ein Werkzeug wie der 2X Application-Server XG, der die schlanken Clients verwaltet und dafür sorgt, dass sie die passenden Applikationen im Zugriff haben. IT-Administrator hat sich genauer angesehen, welche Möglichkeiten diese Zentrale bietet.

Thin Clients. Letzteres sorgt für eine Optimierung des SBC, indem sich durch deren Verwendung praktisch alle Funktionen auf zentrale Terminalserver verlagern lassen. Der AS stellt mit dem neuen ClientManagerModule auch die zentrale Leitstelle für die Thin Clients dar und sorgt dafür, dass alle Benutzer Zugriff auf die ihnen zugewiesenen Applikationen erhalten.

Sofern Thin Clients zum Einsatz kommen, booten diese mit 2XOS, auch ThinClientOS genannt. Hierbei handelt es sich um einen schlanken Linux-Client, den 2X zur Verfügung stellt. Damit entfallen Tätigkeiten wie das ungeliebte Patchmanagement und der Client-Virenschutz. Über eine weitgehende Bereitstellung der Applikationen über Terminalserver lässt sich das Angebot vereinheitlichen, was schließlich den Helpdesk entlastet, da der Support für individuelle Arbeitsplätze reduziert wird oder gar wegfällt. Auch lässt sich ein Datendiebstahl einfacher verhindern ebenso wie ein unerwünschtes Einspielen von Daten, die Anwen-

der mitgebracht haben, bis hin zur Installation unerwünschter Software.

Ziel des AS ist es, den Administrationsaufwand auf der Endanwenderseite zu reduzieren und einheitliche Arbeitsplätze mit fest umrissenem Applikationsumfang zur Verfügung zu stellen.

Redundanz durch Backup-Server

Die Installation des AS auf einem Windows Server 2008 R2 bereitete im Test keinerlei Probleme. Der Server, auf dem AS zuerst installiert wird, fungiert standardmäßig als Master Publishing-Server (Broker). Dies bedeutet, dass alle Clientanfra-

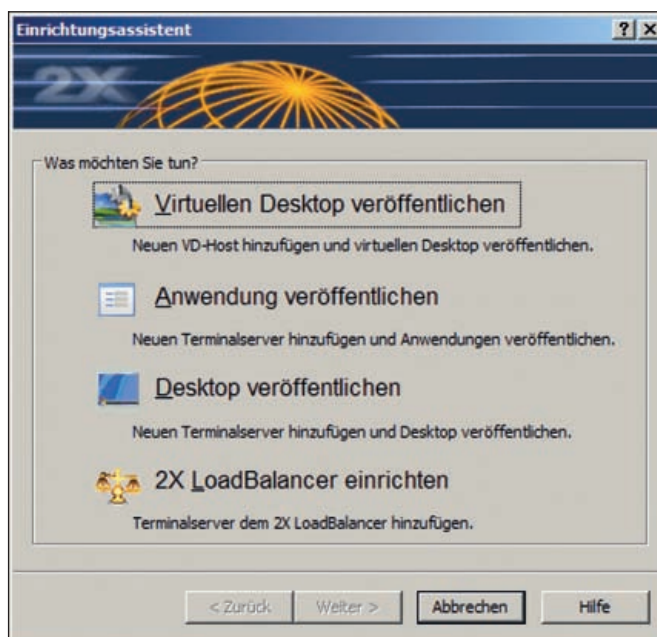


Bild 1: Mit Hilfe eines Assistenten lassen sich sehr leicht Applikationen, Desktops sowie virtuelle Desktops veröffentlichen



gen zuerst zu diesem Server gelangen, der sie dann an das eigentliche System weitergibt, über den die gewünschte Applikation beziehungsweise der Desktop bereitgestellt wird. Das bedeutet aber, dass bei Ausfall des Masters die gesamte Bereitstellung ausfallen würde. Um hier Redundanz zu schaffen, lassen sich ein oder mehrere Backup-Server definieren, die dann die Verteilung übernehmen.

Sollte der Master auf Dauer ausfallen, kann der Administrator jederzeit einen Backup-Server zum Master hochstufen. Damit die Backup-Server im Normalbetrieb nicht nur weitgehend untätig auf einen Ausfall des Masters warten, lassen sie sich zusätzlich als sogenannte Secure Client Gateways nutzen. Diese dienen dazu, vor allem in Umgebungen mit erhöhten Sicherheitsanforderungen und in durch Firewalls segmentierten Netzwerken den gesamten Datenverkehr über einen Port (Standard ist Port 80) zu tunneln und auf Wunsch zusätzlich mit SSL zu verschlüsseln. Standardmäßig wird SSL2 und SSL3 unterstützt, dies kann aber auf SSL3 beschränkt werden. Der Gateway-Zugriff lässt sich über MAC-Adressen filtern, indem der Administrator entweder eine Ausschlussliste ("Alle Adressen außer ...") oder eine Einschlussliste ("Nur die Adressen ...") pflegt.

Übersichtliches Port-Management

Sehr von Vorteil für die Umsetzung individueller Sicherheitsanforderungen ist die Möglichkeit, dass alle genutzten Ports für RDP, Citrix, die Verwendung von Secure Client-Gateways, den Einsatz von SSL/TLS und die Kommunikation mit den Agenten geändert werden können. Vorteilhaft ist zudem, dass der Administrator an allen Stellen, wo sich die Ports anpassen lassen, eine Schaltfläche zur Rückkehr auf die Standardeinstellungen vorfindet. Hat er einmal falsch konfiguriert, stellt es somit kein Problem dar, wieder zum Normalzustand zurückzukehren.

Auf allen Systemen, die der AS für die Applikations- beziehungsweise Desktopbereitstellung nutzen können soll, ist der 2X Publishing-Agent zu installieren. Das kann über ein Setup erfolgen, ebenso aber remote über die nachfolgend beschriebene

Konsole des AS. Diese erlaubt es auch, bereits installierte Agenten auf Erreichbarkeit und Funktion zu prüfen sowie gegebenenfalls zu deinstallieren oder auf eine neuere Version zu aktualisieren.

Eine Stärke des AS ist die Lastverteilung wahlweise per Round Robin oder Ressourcen-basiert. Gerade bei der Nutzung vieler verschiedener Applikationen ist in der Regel die Ressourcen-basierte Vorgehensweise effizienter, bei der der AS die Anzahl der Benutzer-Sitzungen, den Arbeitsspeicher und die CPU-Last als Indikatoren verwendet und neue Sitzungen entsprechend zuweist. Der Administrator hat hier die Möglichkeit vorzugeben, welche der genannten Leistungsindikatoren berücksichtigt werden. Unabhängig davon achtet der AS auf Wunsch darauf, dass getrennte Sitzungen bevorzugt wiederhergestellt werden, indem sie wieder dem gleichen Server zugewiesen werden. Um die Anzahl der aktiven Sitzungen pro Desktop in Grenzen zu halten, ist es möglich, diese auf eine pro Benutzer zu beschränken. Zusätzlich gibt es für spezielle Anforderungen noch weitere Optionen für eine individuelle Verteilung, deren Beschreibung hier aber zu weit führt.

Gefallen hat uns, dass der AS jederzeit eine detaillierte Übersicht zum aktuellen Stand der Lastverteilung und zur Verteilung der Sitzungen liefert. Damit es selbst bei weiter verzweigten Netzen gegebenenfalls mit WAN-Strecken zu keinen Problemen kommt, lassen sich die Timeouts für die Aktualisierung und die Werte der Inaktivitätserkennung verändern.

Zentrale Steuerung über eine Konsole

Erfreulich übersichtlich präsentiert sich die Konsole des AS, die alle Einstellmöglichkeiten sehr kompakt in einer Oberfläche zusammenfasst. Auf der rechten Seite findet der Administrator ein Menü mit den neun Hauptrubriken (Server-Farm, Lastverteilung, Veröffentlichung, Universal Printing, Universal Scanning, Verbindung, Client-Management, Information und Lizenzierung).

Der wichtigste Schritt ist nun, in der Rubrik Server-Farm zumindest ein System

zu erfassen, da andernfalls bei allen anderen Punkten der Hinweis erscheint, dass noch kein aktiver Server konfiguriert ist. Letztendlich sind sämtliche Server einzutragen, von denen Desktops oder Applikationen verteilt werden sollen. Das können Terminalserver sein, entweder von Microsoft, Citrix oder Linux NX, Virtual Desktop Hosts (VDI-Hosts) und dedizierte PCs, um diese über RDP zu veröffentlichen. Weiterhin gibt der Administrator hier die schon erwähnten Secure Client Gateways sowie vorhandene Backup-Server an.

Praktische Server-Gruppen

Innerhalb der erfassten Terminalserver ist eine Gruppierung implementiert, um diese bedarfsgerecht zu unterteilen, um beispielsweise bestimmte Applikationen oder Desktops nur über einen Teil der Server zu veröffentlichen. Das bedeutet auch, dass nicht alle Terminalserver identisch konfiguriert sein müssen. Vielmehr kann der Administrator beispielsweise für eine spezielle Applikationsbereitstellung eine Servergruppe definieren und diese wiederum nur an eine bestimmte Benutzergruppe freigeben.

Damit hat er die Möglichkeit, eventuelle Lizenzvorgaben besser zu kontrollieren und die Lizenzen effizienter zu verwenden. Weiterhin kann er bei Bedarf Benutzergruppen priorisieren, indem er eine Applikation für eine Gruppe nur über wenige Terminalserver zur Verfügung stellt, für eine andere Gruppe aber über zusätzliche, sodass diese auch bei einer hohen Auslastung immer

Publishing Server und Secure Client Gateway laufen unter Windows Server 2003/2008 (R2) Standard oder Enterprise, der Terminalserver-Agent unter Windows Server 2003/2008 (R2) Standard oder Enterprise mit aktivierten Terminalservices. Der 2X-Client ist in einer 32 Bit- und 64 Bit-Version verfügbar für Windows Server 2003, Windows 2000, XP, Vista, 7, CE und Embedded; Mac ab 10.5.x, außerdem für die 32 Bit-Linux-Distributionen Ubuntu 8.04/8.10/9.04/9.10, OpenSuse 11.1, Fedora Core 9/11, CentOS 5.2, VectorLinux 6.0, weiterhin Blackberry Playbook, Android und iOS. Darüber hinaus ist der Client in einer Portable-Version und als Java-basierte Facebook-App erhältlich.

Systemvoraussetzungen



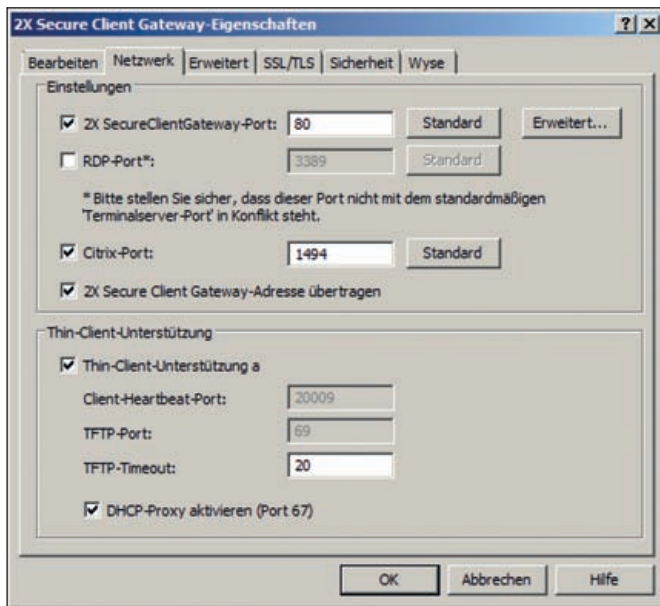


Bild 2: Die Thin Client-Unterstützung ist beim AS explizit zu aktivieren, damit Boot-Images per TFTP-Server angeboten werden und auch der DHCP-Proxy arbeitet

noch eine Sitzung bekommt. Sofern ein Benutzer auf mehrere Serverfarmen berechtigt ist, kann er sich durchaus gleichzeitig zu mehreren verbinden.

Breite Hypervisoren-Unterstützung

Ist die Server-Farm definiert, kann der Administrator einen Assistenten verwenden, der die Veröffentlichung von virtuellen und Terminalserver-Desktops sowie Anwendungen erleichtert. Bei der Veröffentlichung virtueller Desktops werden alle verbreiteten Hypervisoren unterstützt, darüber hinaus auch weniger bekannte wie Virtual Iron oder QEMU. Im Rahmen der Veröffentlichung eines Desktops oder einer Applikation von einem Terminalserver ist es möglich, neue Server zu erfassen. Außerdem kann der Nutzer vorgeben, ob die Veröffentlichung von allen Servern, einer Gruppe oder einzelnen, individuell auszuwählenden Servern erfolgen soll.

Diese Flexibilität macht den Ablauf sehr komfortabel und hilft vor allem dann, wenn die Server innerhalb einer Farm für unterschiedliche Aufgaben oder Benutzergruppen gedacht sind. Neben dem Assistenten, der die am häufigsten benötigten Anforderungen abdeckt, besteht noch die Möglichkeit, über weitere Schaltflächen im Kopfbereich der AS-Konsole ein Verzeichnis oder ein Dokument zu veröffentlichen.

Bei der Veröffentlichung eines Desktops lässt sich die gewünschte Auflösung oder ein Vollbild auswählen, unter den erweiterten Einstellungen kann der IT-Experte vorgeben, ob für den Aufruf eine Verknüpfung auf dem Desktop, im Start-Ordner oder im Autostart-Ordner angelegt werden soll.

Soll eine Anwendung veröffentlicht werden, so ermöglicht die Auswahl "Einzelne Anwendung" eine in-

dividuelle Vorgabe aller Einstellungen. Schneller geht es, wenn es sich um eine Anwendung handelt, die auch auf dem AS zu finden ist, indem sich der Administrator alle dort installierten Anwendungen auflisten lässt. Eine dritte Option, die Auswahl einer vorgegebenen Anwendung, springt zu einer Liste systemnaher Tools wie Internet Explorer, Netzwerkverbindung sowie diversen Inhalten der Systemsteuerung.

Insgesamt empfanden wir die gesamte Erfassung der Server sowie den Veröffentlichungsprozess als recht einfach und intuitiv bedienbar. Positiv fiel uns zudem auf, dass letztendlich wenige Eingaben für eine grundlegende Inbetriebnahme und die erste Veröffentlichung reichen.

Einfache Client-Integration

Hinsichtlich des allgemeinen Client-Supports – gewöhnliche Arbeitsplätze werden über den sogenannten 2X Client angebunden – ist 2X sehr breit aufgestellt (siehe Kasten "Systemvoraussetzungen"). Nach der 2X-Client-Installation ist die Verbindung zum AS zu konfigurieren, anschließend hat das jeweilige System Zugriff auf die bereitgestellten Anwendungen. Dank der Möglichkeit, ein Single Sign-On einzurichten, erfolgt die Authentifizierung im Hintergrund. Beim Click auf das 2X-Icon – je nach gewählter Option im Startmenü der Taskbar oder auf dem Desktop zu sehen

– öffnet sich ein Fenster mit den Icons der freigegebenen Anwendungen. Startet der Anwender darüber nun eine nahtlos eingblendete Anwendung, merkt er kaum, dass er nicht lokal, sondern remote arbeitet.

Vereinheitlichung durch Thin Clients

Statt das jeweilige System mittels 2X Client um den komfortablen Zugriff auf die durch den AS bereitgestellten Ressourcen zu erweitern, lässt sich die Applikationsnutzung komplett auf die Terminalserver verlagern und an den Arbeitsplätzen mit Thin Clients arbeiten. Das hat in stark vereinheitlichten Umgebungen diverse Vorteile, denn die Anwender haben dann nicht mehr die Möglichkeit, am lokalen System etwas zu verändern oder zusätzlich eigene Applikationen zu nutzen. Gestartet wird vielmehr nur ein Linux-basiertes Grundbetriebssystem, genannt 2XOS, das den Zweck hat, die Verbindung zum AS herzustellen. Die Stärke von 2XOS besteht darin, dass diverse Verbindungsclients wie 2X RDP, Citrix ICA, VMware View, VNC und Linux NX integriert sind, um es optimal an die Funktionalität des ApplicationServer anzupassen.

2XOS lässt sich über verschiedene Möglichkeiten auf einen Thin Client bringen und per USB-Medium, Flash-Speicherkarte, CD sowie von der lokalen Festplatte starten. Auch ist ein PXE-Boot möglich, welchen wir uns genauer angesehen haben. Um die Thin Client-Unterstützung mit PXE-Boot zu nutzen, ist diese Option zuerst am 2X Secure Client Gateway zu aktivieren. Dadurch fungiert es als TFTP-Server. Weiterhin ist bei Bedarf die DHCP-Proxy-Funktion nutzbar, wodurch sich eine Modifikation des eigentlichen DHCP-Servers erübrigt. Andernfalls sind am DHCP-Server der Boot-Server und der Name der Boot-Datei zu hinterlegen (DHCP-Optionen 66 und 67). Im Test wendeten wir beide Möglichkeiten erfolgreich an.

Weitere Einstellungen sind in der Rubrik Client-Management vorzunehmen, die mit der Version 10.5 erweitert wurde. Eine wichtige Voraussetzung ist es, das Betriebssystem 2XOS in der richtigen Ausprägung bereitzustellen. So ist 2XOS für typische



webtropia.com

Beste Performance zum unfassbaren Preis!



	ECO i5-3450	ECO i7-3770	ECO i7-3930k
CPU	Intel i5-3450	Intel i7-3770 mit HT	Intel i7-3930k mit HT
Leistung	4 x 3,10 GHz	4 x 3,50 GHz	6 x 3,20 GHz
Arbeitsspeicher	Neu! 16 GB DDR3	Neu! 32 GB DDR3	Neu! 64 GB DDR3
Festplatten	2 x 1.000 GB	2 x 2.000 GB	2 x 3.000 GB
Datentransfer enthalten	✓	✓	✓
IPv4 Adresse inkl.	✓	✓	✓
IPv6 Subnetz (/64) inkl.	✓	✓	✓
Backup-Speicherplatz	50 GB	50 GB	50 GB
Betriebssysteme	Debian 6.0, CentOS 6.3, openSUSE 12.2 Neu! , Ubuntu 12.04, VMware vSphere 5 & Windows 2012 Neu! (19,99 € Aufpreis im Mon.)		
Admin-Panel inkl.	Plesk 11 oder Confixx 3.3		
Extras Live 24/7 inkl.	Domain-Robot, DNS-System, RDNS-Verwaltung, Reboot, Rescue- und Neuinstallations-System		
Monatsgrundgebühr ab	44,99 €	54,99 €	99,99 €
Setup-Gebühr	0,00 €	0,00 €	0,00 €

Jetzt informieren & bestellen Tel.: 0211 / 545 957 - 330 www.webtropia.com



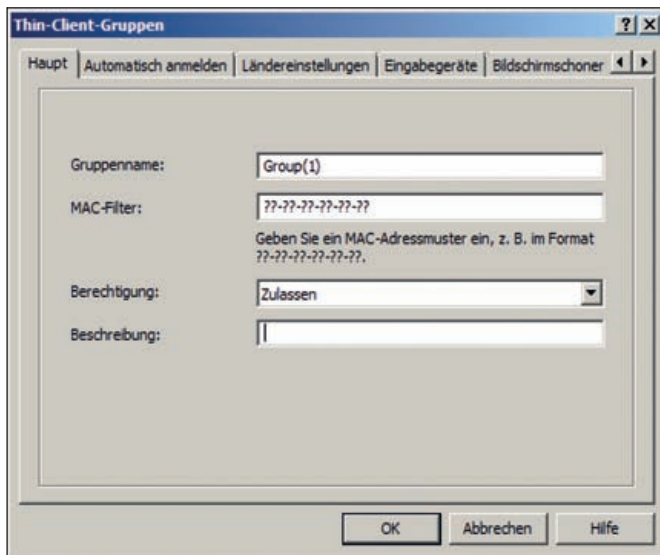


Bild 3: Durch Angabe von Teilen der MAC-Adresse lassen sich die Thin Clients anhand der Hardware unterschiedlichen Gruppen zuordnen

PC-Hardware mit einer breiten Unterstützung verschiedenster Chipsätze verfügbar. 2X hat dazu auf seiner Website eine detaillierte Kompatibilitätsliste veröffentlicht und aktualisiert die Hardwareunterstützung regelmäßig.

Maßgeschneidert für jede Hardware

Neben einer 2XOS-Standardversion für PC-Hardware gibt es noch drei Varianten für den Einsatz in einer virtuellen Umgebung unter VirtualBox, VMware oder Hyper-V. Und schlussendlich produziert 2X für die Vielzahl an verbreiteten Thin Clients speziell angepasste Versionen. Die diversen Versionen sind stets als ZIP- und ISO-Datei verfügbar. Letztere dient zur manuellen Installation, die ZIP-Datei zur Nutzung durch den AS.

Der Administrator muss nun alle benötigten Versionen herunterladen und in den AS importieren, was sich aber sehr einfach gestaltet, indem er nur den Pfad zur besagten ZIP-Datei angibt. Alle importierten Versionen sind anschließend in einer Liste aufgeführt, eine ist als Standard festzulegen. Um nun bei der Verwendung unterschiedlicher Hardware jeweils die passende Version aufzurufen, lassen sich Thin Client-Gruppen anlegen, die sich an der MAC-Adresse orientieren. Das ist insofern sehr sinnvoll, da sich so die herstellereinspezifische Kennung in der MAC-Adresse zur Unterscheidung der Hardware nutzen lässt. Nur falls sich ein Thin Client verbinden will, der

in keine der Gruppen passt, erhält er die Einstellungen der "Default"-Gruppe, die sich nicht löschen lässt, zugewiesen.

Übrigens kann der Administrator die Thin Clients gruppenweise ausschalten, neu starten oder die Anwender abmelden. Erwähnenswert ist ferner, dass das Client Management zum AS als günstige Option angeboten wird.

Individuelle Thin Client-Einstellungen

Bezüglich der Vorgabe einheitlicher Einstellungen hat der Administrator verschiedene Möglichkeiten zur Anpassung. Hier fiel uns auf, dass es wichtig ist, überlegt vorzugehen und das Konzept ein wenig zu planen. Andernfalls kann es schnell unübersichtlich werden.

Auf diese Weise lassen sich für jede Thin Client-Gruppe individuelle Einstellungen über mehrere Registerblätter pflegen. Dies umfasst eine automatische Anmeldung mit einem einheitlichen Benutzer, was beispielsweise für einen öffentlichen Client sinnvoll ist. Dann lassen sich die Ländereinstellungen vorgeben, die Eingabegeräte definieren (Tastaturmodell und -layout, Mausmodell) und sich ein Bildschirmschoner aktivieren. Auch kann der Administrator das Layout des Desktops bestimmen. Stehen hier alle Einstellungen auf "Einfach" beziehungsweise "Standard", sieht der Anwender nur einen einfarbigen Hintergrund und kann praktisch nur die durch den AS bereitgestellten Applikationen aufrufen. Bei der Wahl "Erweitert" hat der Anwender Zugriff auf einen Fenster-Manager und besitzt lokal einige grundlegende Tools wie einen Taschenrechner, einen Bildbetrachter, einen einfachen Texteditor und einen Media Player. In der Praxis dürften diese Tools aber kaum genutzt werden.

Wichtig für das Bootverhalten ist die Parametrisierung auf dem Registerblatt "Hardware", denn hier ist anzugeben, welches der importierten Clientbetriebssysteme und welche Bootmethode zu verwenden ist. Hier stehen wahlweise die Festplatteninstallation und der Netzwerkboot zur Verfügung. Die erste Option ist dann sinnvoll, wenn die Systeme noch über lokale Festplatten verfügen. Dann wird nur beim ersten Mal mittels PXE gebootet und es startet eine Routine zur Installation des 2XOS auf die Platte. Beim Netzwerkboot startet der Thin Client jedes Mal mit PXE, auch dann, wenn er eine eigene Platte hat. Schlussendlich lassen sich noch die RDP-Einstellungen festlegen und ein VNC-Zugriff aktivieren, also eine Aufschaltung eines anderen Nutzers auf den Desktop.

Sind Einstellungen über die Thin Client-Gruppen vorgegeben, so lassen sich nun wieder für einzelne Clients Ausnahmen definieren. Wenn der Administrator unter dem Reiter "Geräte" einen Client markiert, kann er die oben genannten Einstellungen nochmals individuell verändern, nachdem er auf der entsprechenden Registerseite den Haken bei der Option "Gruppeneinstellungen verwenden" weggenommen hat. Letztendlich besteht wahlweise die Möglichkeit, mit möglichst einheitlichen Einstellungen zu arbeiten oder zu individualisieren.

Laut 2X sind für den Einsatz von 2XOS nur 1 GByte Speicherplatz und 512 MByte Arbeitsspeicher erforderlich. Im Test erwiesen sich die erstellten virtuellen Thin Clients dann aber doch als recht träge. Mit 1 GByte Arbeitsspeicher liefen die Clients deutlich flüssiger.

Optionale Zwei-Faktor-Authentifizierung

AS verfügt noch über diverse Funktionen und Features, die den Leistungsumfang abrunden und selbst spezielle Wünsche abdecken. Wie in normalen Terminalserverumgebungen üblich, unterstützt der AS das Drucken über einen universellen Treiber sowie das Scannen über die TWAIN-Schnittstelle über den lokalen Treiber. Gegeben ist ferner ein Multimedia-Support über RDP 7 und RemoteFX.

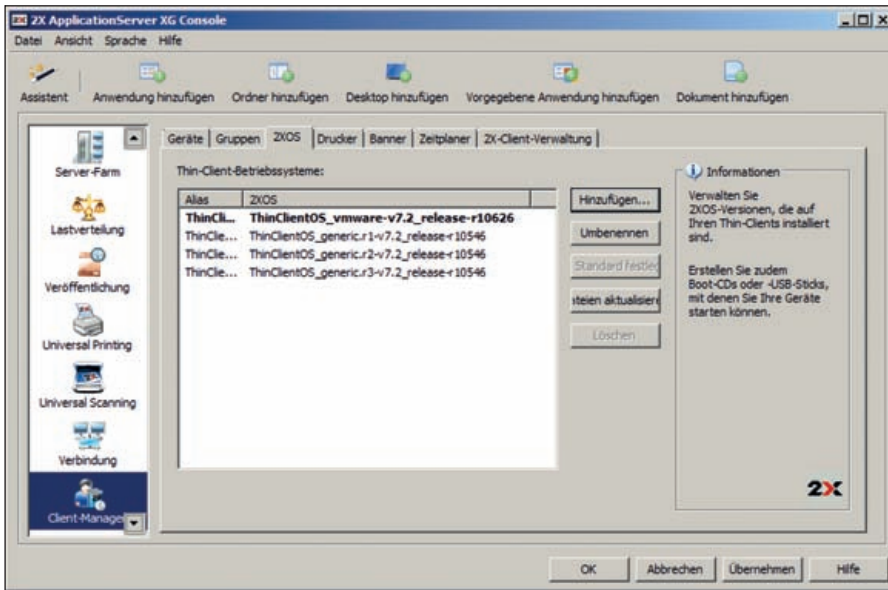


Bild 4: In den AS lassen sich mehrere 2XOS-Versionen importieren, eine wird dann als Standard festgelegt

Durch eine automatische Dateizuordnung lässt sich sicherstellen, dass beim Klick auf eine Datei die passende Applikation gestartet wird. Eine weitere, durchaus sinnvolle Funktion ist eine Versionskontrolle des 2X-Clients. Wenn ein Client einen zu alten Versionsstand hat, kann das Starten von Applikationen oder Desktops verweigert werden. Für besondere Sicherheitsanforderungen unterstützt der AS eine Zwei-Faktor-Authentifizierung über Radius, Deepnet und Safenet.

Damit ein Administrator auch bei Nutzung aller Bereitstellungsarten nicht den Überblick über die Gesamtstruktur verliert, ist schließlich noch ein Farm Designer integriert, mit dem sich diese relativ leicht übersichtlich grafisch darstellen lässt.

Fazit

Der ApplicationServer XG von 2X vereint die Veröffentlichung von Applikationen und Desktops über Microsoft Terminalserver, Citrix sowie Linux NX und die Bereitstellung von virtuellen Desktops in einem Produkt. Darüber hinaus lassen sich die Desktops eigenständiger PCs veröffentlichen. Beeindruckend ist der sehr breite Hypervisor-Support, da neben allen namhaften Produkten auch weniger bekannte Berücksichtigung finden. Mindestens ebenso beeindruckend ist die Client-Palette, die nicht nur Windows-Systemen und mehreren Li-

nux-Derivaten den Zugriff erlaubt, sondern zudem einen allgemeinen Java-Client sowie Unterstützung für mobile Geräte umfasst.

Sehr gut gefallen hat uns die zentrale Konsole, über die alle Administrations-schritte erfolgen. Sehr von Vorteil ist, dass sich mit AS mehrere Terminalserver-Farmen sowie VDI-Hosts administrieren und für unterschiedliche Benutzerzugriffe gruppieren lassen. Damit ist eine Betreuung einer überaus heterogenen Umgebung mit unterschiedlichen Anforderungen der einzelnen Anwender von einem zentralen Punkt aus gegeben. Die Einrichtung mehrerer Publishing-Server im Master-/Backup-Prinzip sorgt für eine hohe Verfügbarkeit. Die Nutzung von Secure Client Gateways, bei denen der gesamte Datenverkehr über einen Port getunnelt und bei Bedarf verschlüsselt wird, prädestiniert das Produkt für den Einsatz in Umgebungen mit erhöhten Sicherheitsanforderungen.

Ein umfassendes Thin Client-Management unterstützt sowohl den Betrieb von zu Thin Clients umgewandelten PCs als auch typische Thin Clients diverser Hersteller. Mit 2XOS liefert 2X das passende Mini-Betriebssystem, das alle Funktionen besitzt, um die Thin Clients optimal in eine AS-Umgebung zu integrieren. Durch die Unterstützung eines PXE-Boots lassen

sich die Systeme sehr einfach mit 2XOS bestücken, wahlweise als lokale Installation oder per dauerhaften Netzwerkboot. Bei Bedarf lässt sich so eine SBC-Infrastruktur aufbauen, bei der alle Applikationen und Desktops von zentralen Systemen kommen und am Arbeitsplatz nichts mehr zu pflegen ist. (In)

Produkt

Programm zur Bereitstellung von Applikationen und Desktops für Remotezugriffe und VDI über Arbeitsplätze und Thin Clients.

Hersteller

2X
www.2x.com/de/

Preis

AS Small Business (ein Server, 80 Desktops, ein Gateway) kostet 900 Euro, AS Professional (zwei Server, 160 Desktops, zwei Gateways) 2.550 Euro, AS Enterprise (drei Server, unlimitierte Desktops und Gateways) 5.150 Euro. Das ClientManagerModule schlägt für zehn Clients mit 370 Euro zu Buche.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für den Einsatz in heterogenen Umgebungen, wo Desktops und Applikationen von verschiedenen Quellen an unterschiedlichen Clients bereitgestellt werden sollen. Der Einsatz von Thin Clients kann die Investitionen bei den Arbeitsplätzen reduzieren.

bedingt für reine Terminalserver-Umgebungen mit einheitlicher Bereitstellung. Hier reicht gegebenenfalls auch der Betrieb einer nativen Farm mit Windows Terminalserver oder Citrix.

nicht für Umgebungen, die ausschließlich mit lokalen Ressourcen arbeiten und in denen keine Anwendungen oder Desktops zu veröffentlichen sind.

2X Application Server XG 10.5

Im Test: H+H Software NetMan 5

Komfort für den Terminalserver

von Markus Wittwer



Terminalservices haben in vielen IT-Konstellationen ihre unangefochtene Daseinsberechtigung. Die Loslösung des Desktops von der lokalen Hardware, gepaart mit dem etablierten und robusten RDP (Remote Desktop Protocol), und die Tatsache, dass sehr viele Branchenlösungen für Terminal-Umgebungen freigegeben sind, sorgen dafür, dass SBC (Server-based Computing) auch im Jahr 2012 insgesamt sehr beliebt ist. Doch die Basismittel, die Microsoft mit dem Windows Server Betriebssystem bereitstellt, haben ihre Grenzen. Sobald es darum geht, die Desktop-Anpassung flexibel zu gestalten, einzelne Applikationen in einer Terminalsitzung bereitzustellen oder gar in einen lokalen Desktop zu integrieren, zeigen sich gewisse Schwächen.

Traditionell ist es die Firma Citrix, die seit Jahren eine Lösung für derlei Herausforderungen bietet. Was einst unter dem Namen "MetaFrame" oder "Presentation Server" vermarktet wurde, heißt heute "Citrix XenApp". Auch XenApp setzt auf die Terminalserver-Funktionen von Windows auf und erweitert die Fähigkeiten der Technik hinsichtlich der Benutzerschnittstelle, Integration und der Leistung. Citrix ist je-

Remotedesktops sind für viele Unternehmen eine wichtige Technik, um die Benutzerarbeitsumgebung einfach und zentral bereitzustellen. Wem dabei die Basisfunktionen von Windows nicht ausreichen, der muss nicht unbedingt zu großen Lösungen wie XenApp greifen. Eine günstige Alternative stellt H+H Software mit NetMan 5 zur Verfügung. Was die Software tatsächlich leistet, hat sich IT-Administrator im Test genauer angesehen. Besonders bei der Bedienbarkeit und der Performance überraschte die Lösung.

doch nicht der alleinige Heilbringer. H+H Software mit "NetMan 5", aber auch andere Konkurrenten haben sich der Optimierung der Remotedesktopdienste mit ähnlichem Erfolg verschrieben.

Neues in NetMan 5

H+H NetMan ist eine Erweiterung der Basis-Remotedesktop-Dienste von Windows und versucht, die erwähnten Schwachpunkte auszugleichen. Die aktuelle Version 5 ist im Sommer dieses Jahres erschienen und soll insbesondere bei der Geschwindigkeit der Sitzungen Vorteile bieten. Der Wechsel

auf eine NoSQL-Datenbank soll sowohl die Reaktionsgeschwindigkeit der Administrationsoberfläche als auch den Session-Aufbau und den Start der Anwendungen deutlich beschleunigen. Besonders weist der Hersteller jedoch auf die optionale "NDM RDA" (Remote Desktop Acceleration) hin. Gemäß der herstellereigenen Messungen wird das RDP-Protokoll dank Kompression maximal um den Faktor 25 beschleunigt. So sei der Einsatz von mobilen Zugriffen über WAN-Strecken möglich, ohne dass es zu Einschränkungen der Nutzbarkeit kommt. Ansonsten gibt es in der

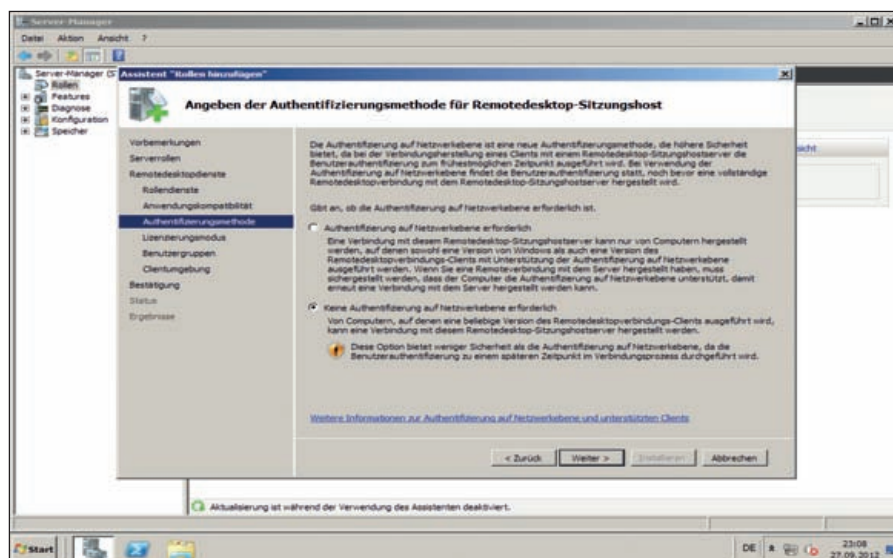


Bild 1: Die Installation von NetMan NDM5 beginnt mit der Einrichtung eines gewöhnlichen Windows-Terminalservers. Die Sicherheitsfunktionen der Windows-Remotedesktop-Server müssen hierzu deaktiviert werden.



jüngsten Version einige kleinere Optimierungen, wie das neu überarbeitete Web-Fenster, ein überarbeitetes Lizenzmodell mit "User" und "Device", die Unterstützung virtualisierter Anwendungen, wie beispielsweise Microsoft App-V, und die Verwendbarkeit von IPv6.

Einfache Installation

Wir integrierten die Software in eine Active Directory-Umgebung auf Basis von Windows Server 2008 R2. Alle beteiligten Systeme virtualisierten wir mit VMware. Der Test der Software begann mit dem Download des rund 400 MByte großen Installationspakets. Die Installation startet mit dem Hinzufügen der Rolle "Remotedesktopdienste" auf dem künftigen Terminalserver. Der als PDF-Dokument bereitgestellten Schritt-für-Schritt-Anleitung folgend ist dies zügig erledigt. Da NetMan eigene Techniken wie Webzugriffe, Gateway und Load Balancing mitbringt, darf der Administrator diese Funktionen nicht unter Windows aktivieren. Im Installationsschritt "Authentifizierungsmethode" gilt es, die Auswahl "Keine Authentifizierung auf Netzwerkebene erforderlich" zu markieren und den Lizenzmodus auf "Pro Gerät" einzustellen. Einen Neustart später mussten wir in den Einstellungen für das RDP-Protokoll im Register "Allgemein" ebenfalls die "Authentifizierung auf Netzwerkebene" deaktivieren. Im Register "Sitzungen" folgten wir ebenfalls der Anleitung und stellten mithilfe des Optionsfelds "Sitzung beenden" sicher, dass mit dem Erreichen des Sitzungslimits die Session nicht nur getrennt, sondern wirklich beendet wird.

Server

Terminal-Server mit Windows Server 2003/2008 x86/x64, Windows Server 2008 R2 x64. Der NetMan-Server selbst benötigt Windows Server 2003 x86 oder höher, 1 GByte freien Plattenplatz für die Installation und zusätzlichen Speicher für die Statistik- und Reporting-Datenbanken.

Client

Clientseitig unterstützt die Software Windows ab Version 2000 Professional als Web-Client, Windows XP und höher für lokale Installationen. Thin Clients, Apple MacOS, Linux über Java oder RDP, Android- und Apple iOS-Geräte über RDP oder den AccessToGo-Client.

Systemvoraussetzungen

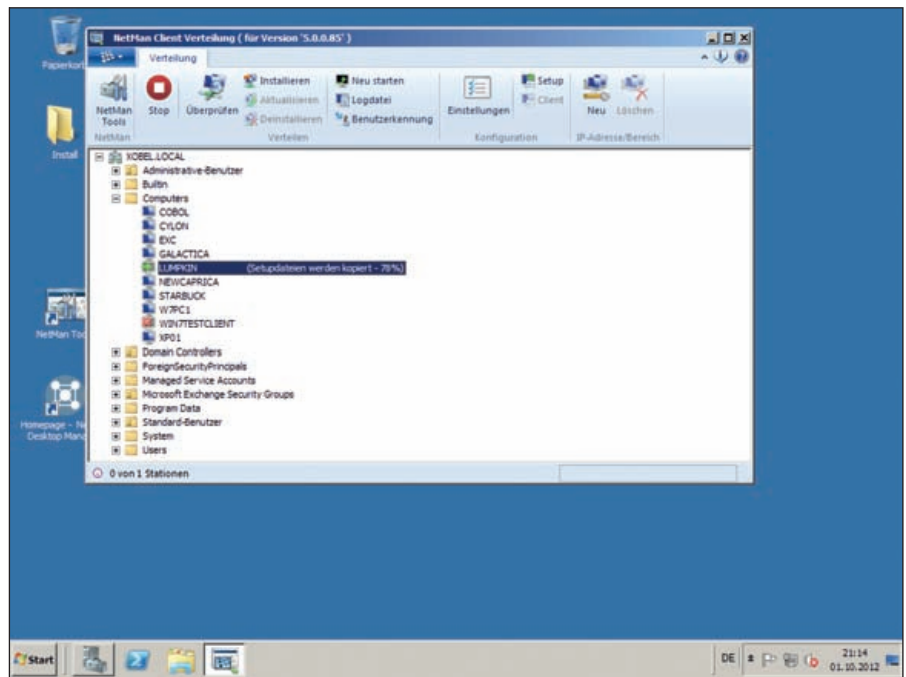


Bild 2: Die Agenten-Komponente kann entweder per Push-Kommando verteilt, über das Webinterface heruntergeladen oder über das Anmeldeskript installiert werden

Nach Einrichtung der Windows Remotedesktop-Server begann die eigentliche Installation von NetMan. Interessanterweise ist die Organisation rund um die von uns genutzte 30-Tage-Testlizenz in der Summe aufwändiger als die eigentliche Installation. Die Lizenzdatei erhält der Interessent nur nach Anmeldung in einem Webinterface und durch die Eingabe eines Codes, der per E-Mail versendet wird. Zur Installation von NetMan selbst muss der Administrator eigentlich nur die Setup-Datei starten, den Zielordner bestimmen und einige Minuten warten, bis die Einrichtung abgeschlossen ist. Der NetMan-Server war nach dieser kurzen Zeitspanne einsatzbereit auf dem Terminalserver installiert. Gemäß der Anleitung spielten wir auf zwei Windows-Clients noch den NDM5-Agenten per Push-Kommando auf. Das funktionierte im Test ohne Tadel, nachdem die Firewall-Regeln angepasst worden waren. Eine manuelle Einrichtung oder die Installation per Anmeldeskript oder Softwareverteilung eines Drittherstellers ist ebenfalls möglich.

Gut gestaltete Oberfläche unterstützt die Administration

NetMan5 wirkt gleich auf den ersten Blick aufgeräumt. Die Zeiten, in denen Administratoren mit tausenden von Funktionen erschlagen wurden, scheinen vor-

bei zu sein. Ein Doppelklick auf die "NetMan Tools" öffnet ein kleines Menü mit sechs Rubriken: z. B. "Center" zur Datenverwaltung von Programmen, Stationen und Benutzern, die "Einstellungen" und der "Monitor". Während es beim Monitor um den Echtzeitzugriff auf Sitzungen oder Lizenzen geht, handelt es sich beim "Report Center" um die Auswertung all dieser Informationen über einen längeren Zeitraum. Die "Client-Verteilung" pusht den Client wie bereits erwähnt über das Netzwerk auf den PC. Der "NetMan Prozessrekorder" erlaubt das Aufzeichnen von Installationsprozessen.

Die Auswahl führt den Administrator in ein modernes Programmfenster mit Ribbon-Technik und einem dreigeteilten Fenster. Die rechte Spalte beinhaltet "Dynamische Informationen", hierbei handelt es sich um kontextabhängige HTML-Hilfstexte vom NetMan-Server. Die Erklärungstexte sind gut geschrieben und bebildert. Insgesamt fällt die Arbeit mit der Software leicht – alle Funktionen scheinen auf Anhieb logisch aufgebaut. Dass es sich bei einer "Kollektion" um eine Zusammenfassung von Programmen und Einstellungen handelt, erschließt sich dem Anwender von allein. Das Wort "Skripte" verwundert zunächst, nach einem Mausklick ist aber klar, dass es sich

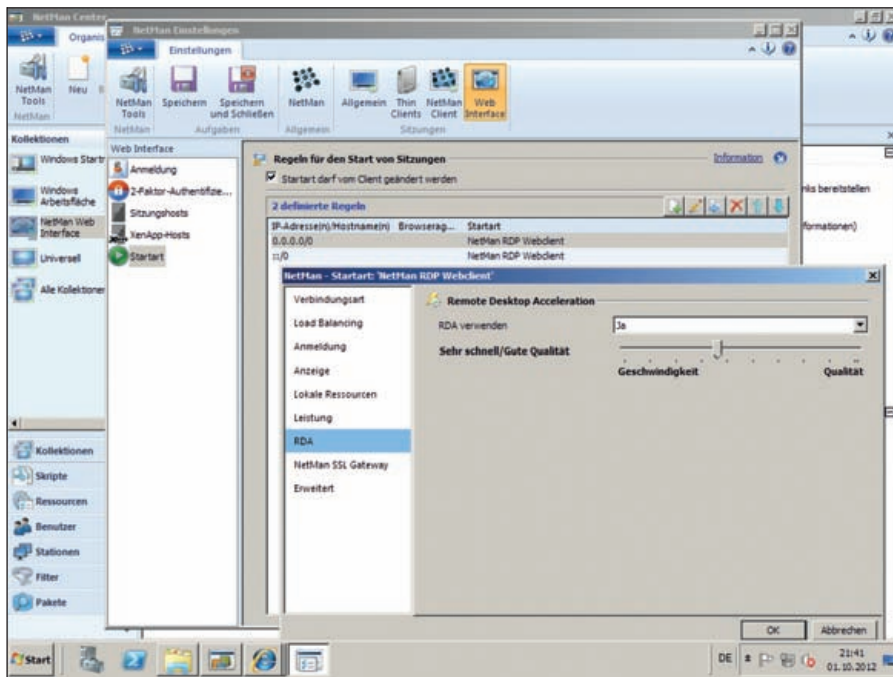


Bild 3: Die optionale Remotedesktop-Beschleunigung erzielt im Test eine Performance-Verbesserung von bis zu 55 Prozent in einer simulierten WAN-Umgebung

um "Programme", "Installationsjobs" oder "URL-Verweise" handelt, die in den Kollektionen zu verknüpfen sind. Bereits nach wenigen Minuten war es im Test möglich, eigene Programme in eigenen Kollektionen für Benutzer beziehungsweise Benutzergruppen freizuschalten. Die knapp 400 Seiten PDF-Dokumentation hatten wir zu diesem Zeitpunkt noch nicht einmal angelesen.

Die Erstellung eines eigenen "Skripts" besteht aus der Beantwortung einiger Options- und Eingabefelder im Dialogfenster "Skripteditor". Diese lauten beispielsweise "Name", "Starteinstellungen", "Symbol", "Programmpfad" oder "Ausführung in Normal / Maximiert / Minimiert / Versteckt". Wer schon einmal Programme in anderen Skript-Sprachen gestartet und bereitgestellt hat, für den ist das alles kein Hexenwerk. Auch andere Optionen sind selbsterklärend: "Mehrere Instanzen in einer Sitzung erlauben" oder "Als Administrator ausführen (VISTA oder höher)". Das, was der Administrator zusammengestellt hat, kann er jederzeit mit den Befehlen "Debug" und "Start" sofort ausprobieren. Ist mehr als eine Standardbereitstellung erforderlich, so muss der Nutzer in das "Erweiterte Skript" wechseln. Anschließend stehen Funktionen wie das applikationsabhängige Mapping von

Druckern und Laufwerken, das Schreiben und Lesen von INI-Dateien, der Zugriff auf Active Directory-Eigenschaften oder die Bearbeitung der Registry-Datenbank zur Verfügung.

Voller Komfort für den Anwender

Auf einem Windows-PC erweitert der NetMan-Client das Startmenü und den Task-Tray. Die per Terminaltechnik be-

reitgestellten Applikationen, beispielsweise ein Office-Programm oder eine Branchensoftware, werden so in das Startmenü integriert, als sei die Software lokal installiert. Der Anwender bemerkt keinen Unterschied in der Gestalt der Software. Erst beim Start der Applikation erscheint, sofern es sich um die erste Verbindung zum Server handelt, für zirka zehn Sekunden ein Dialogfenster von H+H, in dem verkleinert der Desktop des Servers zu erkennen ist. Single Sign-On (SSO) sei Dank wird dem Anwender, sofern in den Stammdaten von NetMan aktiviert, eine manuelle Anmeldung erspart und das gewünschte Programm sofort gestartet.

Programmfenster in einer Remotedesktopverbindung, die sich nahtlos auf dem lokalen Desktop darstellen, heißen gemeinhin "Seamless Windows". Diese nahtlose Darstellung ist bei NetMan5 sehr gut gelungen. Programmfenster lassen sich zügig verschieben und in der Größe anpassen. Die Zwischenablage wird synchronisiert und Menüerweiterungen, die beispielsweise zur Laufzeit der Software am "Task-Tray andocken", stellt das Programm ebenfalls korrekt dar. Auch die Umleitung von Dateien eines bestimmten Typs zu einer bestimmten Software beherrscht NetMan5. Ein Doppelklick auf

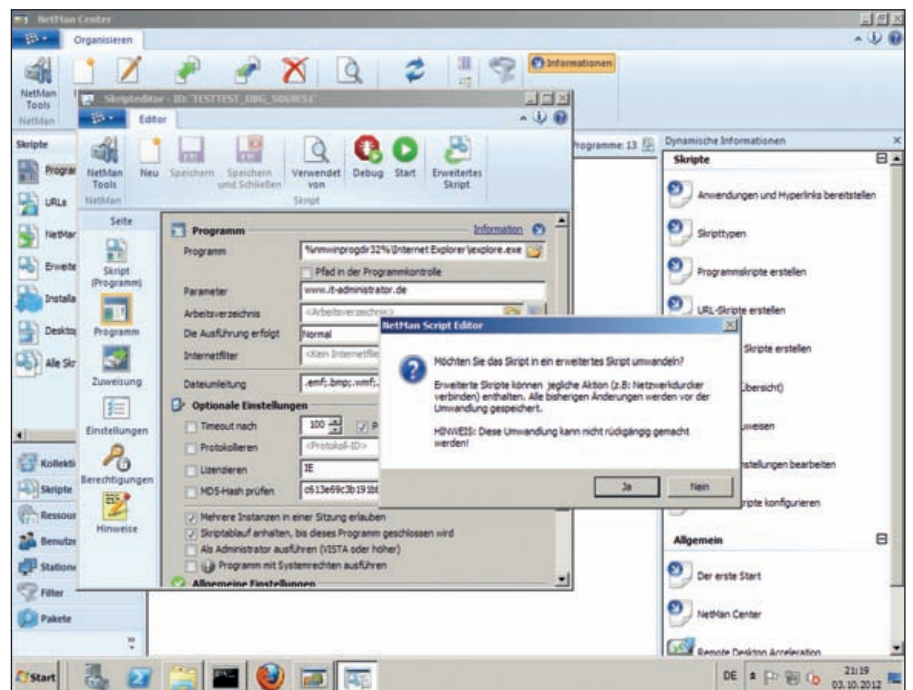
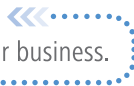


Bild 4: Programme, Konfigurationen oder Links für den Benutzer fasst NDMS in so genannten "Skripts" zusammen, die der Administrator zusammenstellt



LANCOM

Systems

NEU SMART. SCHNELL. INNOVATIV.

Die neue LANCOM Smart Access Point Serie für High-Performance WLAN.

Noch mehr Speed für Ihr Enterprise WLAN!



- Bis zu 900 MBit/s brutto Datendurchsatz
- Mehr Leistung im WLAN – über 430 MBit/s netto Datendurchsatz (TCP)



- Höherer Datendurchsatz dank Band Steering (automatische Entlastung des 2,4 GHz Bandes – flexibel konfigurierbar)
- Paralleler Funkbetrieb in 2,4 und 5 GHz für heterogene Clientumgebungen



- STBC und beste Funkverbindung
- Verbesserte WLAN-Performance im Randbereich einer Funkzelle



- Spectral Scan für mehr Netzwerkübersicht
- Identifikation von WLAN-Störquellen (z. B. Bluetooth-Geräte) für ein effizientes Netzwerk-Troubleshooting

WLAN-Lösungen von LANCOM:

Kabellos glücklich.



- Sichere Integration von Tablets, Smartphones und Notebooks in Unternehmensnetze
- Optimaler Durchsatz dank Smart WLAN Controlling
- Perfekte Sicherheit durch hohen Verschlüsselungsstandard und überwachte Sicherheitspolicies

Informieren Sie sich jetzt unter:

www.lancom.de/smartwlan





eine so verknüpfte Datei auf dem Client-Rechner startet das Programm auf dem Sitzungs-Host. Eine neuere Variante hiervon ist die "Protokollumleitung", bei der Protokollaufrufe, beispielsweise "http:" oder "mailto:", an bestimmte Programme umgeleitet werden können. Die Akzeptanz der Lösung dürfte durch die gute Desktop-Integration bei Anwendern im Unternehmen recht hoch sein. Je nachdem, was für ein Client-Betriebssystem der Anwender nutzt, mag vielleicht auffallen, dass die typischen Remotedesktop-Programme keine Aero-Optik nutzen, Vista beziehungsweise Windows 7 aber schon. Neben den Seamless-Windows hat der Anwender

natürlich auch noch den "kompletten Remote-Desktop" zur Auswahl.

Neben dem lokalen Client verwendet die Software eine webbasierte Verteilung. Hierfür startet der Anwender die Intranetseite der NetMan5-Installation, meldet sich mit seinen Login-Daten an und erhält im Browserfenster die ihm zugewiesenen Programme. Der Vorteil des NetMan RDP-Webclients ist seine Plattformunabhängigkeit. Auf der Maschine muss lediglich die Java-Laufzeitumgebung 6.x installiert sein. Im Test konnten wir erfolgreich und ohne Probleme mit Windows 7, XP, XP Embedded und Mac OS 10.6 auf die Applikationen zugreifen. Auf Nachfrage erklärte der Hersteller, dass beispielsweise auf Igel-Thin Clients die Clientsoftware auf die Custom-Partition installiert werden kann.

ner Bitmap-Darstellung ohne RDA-Kompression in der WAN-Umgebung beinahe zehn Sekunden dauert, ist der Aufbau mit aktiviertem RDA in rund drei Sekunden erledigt.

Ein kleines Prüfprogramm, das einen kontrollierten Ablauf von Programmstart, Speicherkommando und Öffnen einer Bitmap-Datei mit Zeitmessung durchführte, ermittelte in unserem Test eine Performance-Verbesserung von rund 55 Prozent in der simulierten WAN-Umgebung. Treten im Netzwerk simulierte zwei Prozent Paketverluste auf, so ist die Leistung mit aktivem RDA zwar besser, aber im Vergleich zur Standard-RDP-Verbindung sind die Zugewinne nicht mehr so deutlich.

Fazit

Der NetMan Desktop Manager 5 ist eine professionelle Software zur Bereitstellung von Desktops in Unternehmen. Auch wenn die Installation der Software nur einige Minuten dauert und bereits nach weniger als einer halben Stunde die ersten angepassten Umgebungen festgelegt sind, darf der Administrator das Programm keinesfalls unterschätzen. Die umfangreiche Produktdokumentation offenbart eine Vielzahl an Einstellungsmöglichkeiten. Doch trotz der vielen Möglichkeiten, die dieses Programm bietet, fällt die Bedienung für den Administrator leicht. Anstelle sich mit einem der vielen selbstgeschriebenen Anmeldeskripten herumzuplagen, erscheint der Einsatz von NDM5 doch deutlich einfacher. (dr)



Produkt

Software zur Desktop-Bereitstellung auf Basis der Windows-Terminaldienste.

Hersteller

H+H Software
www.hh-software.de

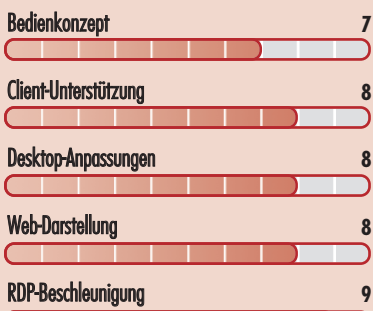
Preis

Der Basispreis der Software mit fünf Lizenzen startet bei 831,81 Euro. Bei Abnahme von 500 Lizenzen liegt der Einzelpreis bei rund 31 Euro pro Gerät. Die optionale NDM Remote Desktop Acceleration kostet 70,21 Euro pro Benutzer.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für Unternehmen, denen die Remotedesktop-Bordmittel von Windows nicht ausreichen.

bedingt für kleine Unternehmen, die nur geringe Anpassungsanforderungen im Remotedesktop-Umfeld haben.

nicht für Firmen, die keinen Bedarf an Terminaltechnik haben oder denen die Bordmittel gut ausreichen.

NetMan Desktop Manager 5

Beachtliches Tempo

Letztendlich ist die große Frage, wie sich die Software dank der beworbenen optionalen RDP-Beschleunigung NDM RDA im Geschwindigkeitstest schlägt. Das Ergebnis dieser Datenstromkompression mit "Packet Shaping" ist wahrlich beachtlich. Die typischen negativen Effekte wie das Ruckeln bei Animationen oder in gescrollten Dokumenten mit Bildern sind deutlich reduziert. In einer simulierten, schmalbandigen Verbindung mit einer Latenz von 100 ms und einer Datendurchsatzrate von 2 MBit/s fühlt sich eine Terminalsitzung an wie in einem lokalen Netzwerk mit 100 MBit/s ohne nennenswerte Latenz. Während der Bildaufbau ei-



Bild 5: Der Anwender genießt mit NetMan den vollen Komfort eines Fat-Clients, auch dank RDP-Beschleunigung


Im Test: TSplus 2012

Beinahe original

von Thomas Bär

Die Pluspunkte des Remotedesktop-Betriebs unter Windows liegen in der zentralen Bereitstellung, der Vermeidung lokal gespeicherter Daten auf dem Client-System, einer höheren Betriebssicherheit und mehr. Wegen dieser zahlreichen Vorteile hat sich der Terminalserver gegen die Angriffe anderer Techniken stets behaupten können. In vielen Unternehmen wird diese Grundlage mithilfe von Citrix XenApp weiter veredelt. Die Kombination aus Microsoft Remotedesktop und Citrix XenApp ist jedoch nicht gerade billig. Um die Technik zu erhalten, muss ein Unternehmen viel Geld für Lizenzen ausgeben. Für kleinere Umgebungen ist das oft zu teuer. Hier springt TSplus 2012 in die Bresche und will das volle Terminalserver-Vergnügen für einen deutlich geringeren Preis liefern. Ob dies gelingt, zeigt unser Test.



Dass ein Standard-Windows-PC nicht gleichzeitig von verschiedenen Anwendern genutzt werden kann, ist eine von Microsoft künstlich eingebaute Begrenzung. Der technische Unterschied des Betriebssystemkerns oder der wichtigsten Windows-Komponenten zwischen Client- und Serverfassung ist nicht so groß, dass es eine Erklärung für diese Begrenzung gibt. Windows XP, Vista, 7 oder 8 sind als Einzelplatzsystem ausgelegt und für die Bedürfnisse eines Einzelbenutzers getrimmt. Windows Server mit aktivierten Remotedesktop-Diensten, vormals Terminalserver, ist indes auf den gleichzeitigen Mehrbenutzerbetrieb optimiert. Wer in die technischen Referenzdokumente von Microsoft schaut, sieht, dass sich viele Grundwerte zwischen den Betriebssystemausprägungen unterscheiden.

Der PC wird zum Terminalserver

TSplus 2012 für Windows (TSP) ist eine Software des französischen Herstellers TSplus, die einen Standard-PC in einen Terminalserver verwandelt und für den Betrieb in einer Mehrbenutzerumgebung optimiert. Das Programm enthält eine Vielzahl von Funktionen, wie Multi-Session, Multi-User (ab Windows 7), Load Balancing, Universal Printer, Seamless-Client, USB-Client (optional), RDP-Client, Web-Client, Seamless Remote-Applikation, Application-Control und eine zentrale Benutzer-

verwaltung. Die Besonderheit ist, dass all diese Funktionen, die gewöhnlich von einem Terminalserver geboten werden, ein Standard-PC mit Windows XP SP3 oder höher bereitstellt. Freigegebene Applikationen werden, genau wie auf einem echten Terminalserver, als kompletter Remote-Desktop dargestellt oder als Seamless-Fenster, das sich in einen lokalen Desktop integriert.

Nun stellt sich dem Interessenten die Frage, ob die Mehrfachnutzung eines Einzelplatz-Betriebssystems überhaupt zulässig ist. Auf Nachfrage antwortete der Hersteller, dass er die Technik zur Mehrfachnutzung ohne die typischen Microsoft-Softwarekomponenten realisiert und es daher zu keinem EULA-Lizenzverstoß komme. Wie die Lizenzrechte für die auf dem TSplus-Server bereitgestellten Softwareanwendungen im Terminalserver-Umfeld lauten, hängt, so der Hersteller weiter, von den Lizenzbestimmungen der jeweiligen Softwarehersteller ab. Im Zweifelsfall ist für jeden Benutzer sicherlich eine Windows-CAL erforderlich. Einen Remotedesktop-Lizenzserver vermissen die TSplus-Terminalserver jedoch im Testnetzwerk nicht.

Sehr einfache Installation binnen Minuten

Die Installation der Software ist denkbar einfach. Der Installer besteht aus einer 115

MByte großen Datei, die wir per Doppelklick auf dem künftigen Terminalserver starteten. Die einzige Frage, die wir bei der Installation zu beantworten hatten, war die nach dem Zielverzeichnis. Nach dem Installationsvorgang, der lediglich drei Minuten dauerte, mussten wir den Computer neu starten. Die Anforderung an den Rechner, der als Terminalserver zum Einsatz kommen soll, ist gering. Ab Windows XP SP3 ist eine Nutzung möglich. Neben Windows wird lediglich eine aktuelle Java-Installation auf dem PC verlangt. Ist diese Voraussetzung nicht erfüllt, so verweigert der Installer seinen Dienst.

Die Hardware-Anforderungen sind abhängig von der zu erwartenden Systemlast. Sollen lediglich fünf Benutzer auf dem System gleichzeitig arbeiten, so ist eine Single Core-CPU mit 512 MByte

Windows XP SP3 und höher auf der Seite des TSplus-Terminalservers mit aktueller Java Runtime-Installation. Aktuelle Windows Server-Betriebssysteme, auch Small Business Server, werden unterstützt. Clientseitig arbeitet die Software mit allen gängigen Windows-Versionen und über den Java-Agenten auch mit Linux-Systemen. iOS- und Android-Unterstützung ab der neuesten Version, die jedoch im Test nicht verifiziert werden konnte.

Systemvoraussetzungen



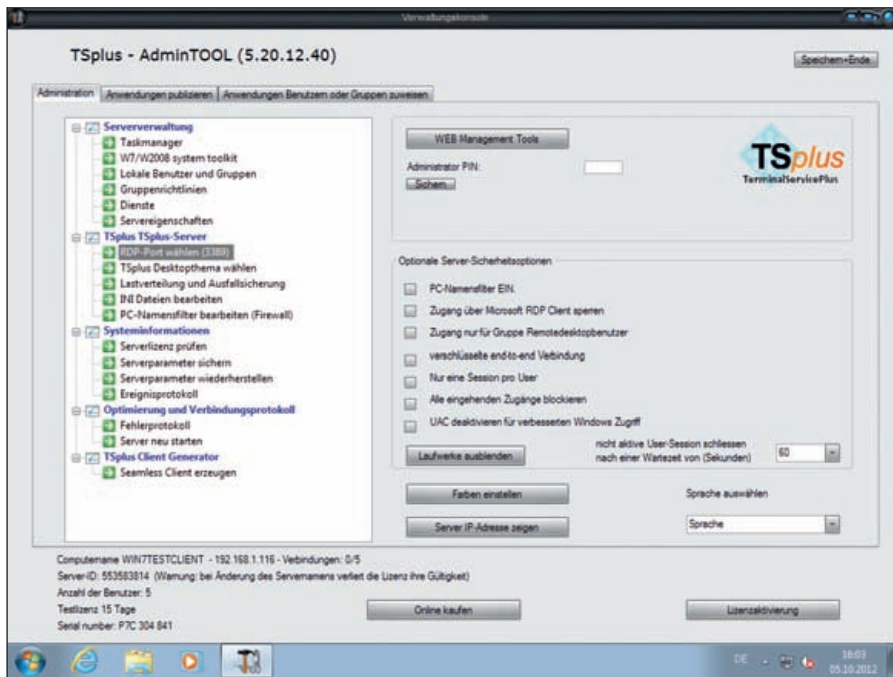


Bild 1: TSPplus 2012 ermöglicht es, einen Standard-PC in einen Terminalserver umzuwandeln

DDR2-Speicher oder schneller ausreichend, sofern Windows XP als Betriebssystem genutzt wird. Für das deutlich modernere Windows 7 empfiehlt der Hersteller bei derselben Auslastung bereits eine Dual Core-CPU mit mindestens 2 GHz Taktfrequenz und 2 GByte DDR3-RAM. Bei 20 gleichzeitig aktiven Benutzern steigt die Anforderung für Windows 7/2008 SBS oder Server 2008 auf zwei Quad Core-CPU's mit 4 GByte RAM.

Remotezugriff problemlos etabliert

Für den Test installierten wir die 15-Tage-Testversion, die jedem Interessenten auf der Homepage zur Verfügung gestellt wird, auf einem unter VMware ESX5 virtualisierten Windows 7 Enterprise SP1 x64-System mit zwei CPU-Kernen und 2 GByte zugewiesenem Arbeitsspeicher. Beim Design der Fenster haben sich die Entwickler etwas Besonderes einfallen lassen: Die Fenster-rahmen sind grafisch aufgewertet und der Administrator hat das Gefühl, er würde ein Computerspiel oder ein System-Gimmick installieren. Das Hauptfenster der Software, das "AdminTOOL", vermittelt ebenfalls diesen Charme.

Der folgende erste Funktionstest, zu dem die deutschsprachige PDF-Kurzanleitung rät, ist ein Zugriffsversuch mit dem Standard-Remote-Desktop-Client von Mi-

crosoft von einem anderen PC im Netzwerk. Bis auf ein für nur einen Augenblick sichtbares Fenster von TSP verhielt sich der Windows 7-Terminalservers wie ein ganz gewöhnlicher Server mit Remote-Desktop-Diensten im Netzwerk. In punkto Geschwindigkeit gab es ebenfalls keine erkennbaren Unterschiede.

Schaut der Remote-Desktop-Benutzer ohne Administrationsrechte in das Startmenü, so kann er die Verwaltungssoftware von TSP zudem nicht finden. Die Grund-

funktionalität liefert die Software somit ohne jegliche Probleme. Mehrere Benutzer können sich im RDP-Vollbildmodus am TSP-Terminalservers anmelden, ohne dass es zu unerwünschten Interaktionen kommt. Ein Blick in den Task-Manager offenbart im Register "Benutzer", dass es sich um ganz gewöhnliche RDP-Sitzungen mit eigener Session ID handelt.

Erschwerte Administration

Das AdminTOOL des TSP besteht aus den drei Registern "Administration", "Anwendungen publizieren" und "Anwendungen Benutzern oder Gruppen zuweisen". Die Administrationssoftware, die direkt auf TSP installiert ist und sich auch nicht von einem anderen PC aus starten lässt, bietet unterschiedliche Oberflächensprachen – unter anderem Englisch und Deutsch.

In der "Administration" ist der Anwender in der Lage, die Grundkonfiguration vorzunehmen, beispielsweise die Port-Adresse für RDP/HTTP oder HTTPS zu verändern. Über einzelne Checkboxes legt der Administrator fest, ob pro Benutzer nur eine Verbindung zulässig ist, UAC und die Firewall generell ausgeschaltet bleiben oder ein PC-Namensfilter aktiv ist. Einzelne Laufwerksbuchstaben kann der IT-Verantwortliche in der Explorer-Ansicht für Benutzer ausblenden, ohne dass jedoch ein direkter Zugriff komplett unmöglich wäre.

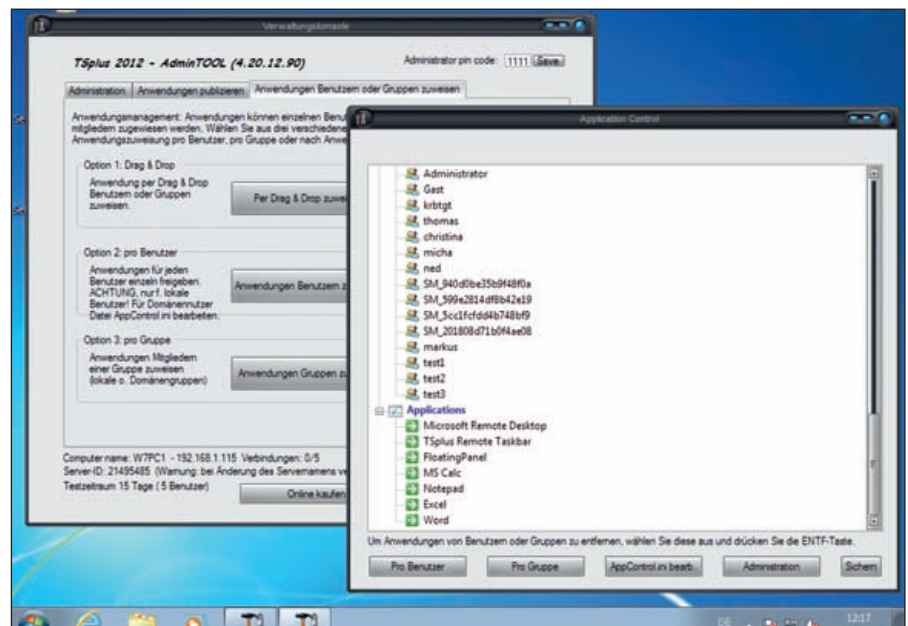


Bild 2: Welche Benutzer/Benutzergruppen welche Applikationen erhalten, wird über die grafische Oberfläche oder direkt in einer INI-Datei festgelegt



EXPERTeach

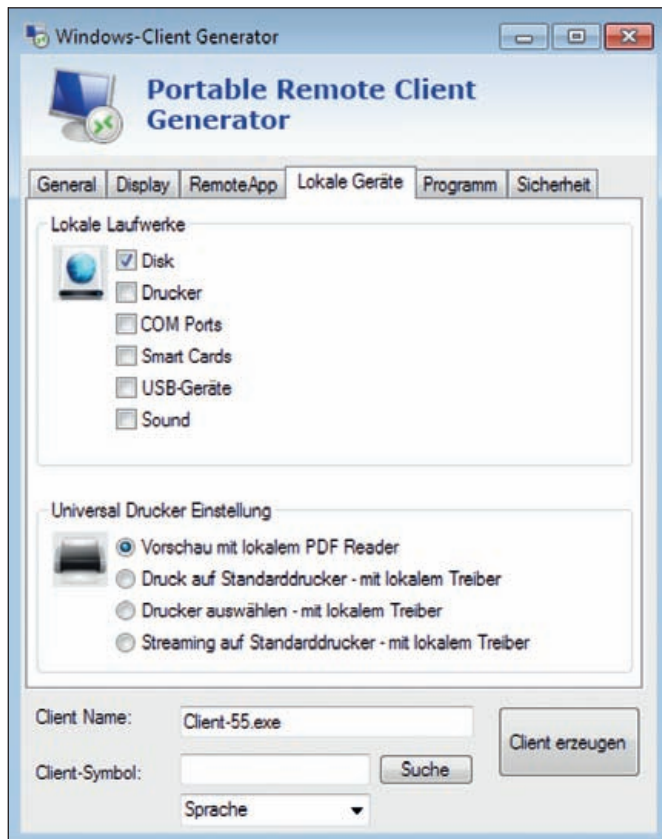


Bild 3: Eine Besonderheit von TSPplus: Der Windows-Zugriffscient wird als EXE-Datei nach den Anforderungen des Administrators generiert

Das Desktop-Farbschema für Benutzer kann auf Wunsch zwischen Blau und Silber umgestellt werden, Menü-Optionen im Benutzer-Menü ausgeblendet oder das Logo und der Desktophintergrund angepasst werden. Viele Befehle im Menü des AdminTOOLS führen einfach zu den Standard-Fenstern von Windows wie Taskmanager, lokale Benutzer und Gruppen, Gruppenrichtlinien, Dienste oder die Servereigenschaften. Bei komplexeren Konfigurationsanforderungen verweisen die insgesamt nicht sehr aussagekräftigen PDF-Dokumente auf INI-Dateien, die manuell anzupassen sind. Was uns jedoch sehr gut gefiel, war die Möglichkeit, die Oberfläche mit einem Administrator-PIN-Code zu versehen, um unerwünschten Personen den Zugriff zu verweigern.

Leider gibt es gewisse Seltsamkeiten in der Bedienung der Administrationsoberfläche. Soll beispielsweise eine neue Applikation bereitgestellt werden, ohne dass der Benutzer den kompletten Desktop zu Gesicht bekommt, so wechselt der Administrator in das Register "Anwendungen publizieren" und füllt die Felder "Angezeigter Name", "Pfad/Dateiname", "Startverzeichnis" und "Befehlszeile" aus. Lediglich vier Optionen bietet das Programm für weitere Einstellungen: "Anwendungen maximiert oder minimiert starten", "Anwendung für alle Benutzer freigeben" und "Starten + Verbergen der Anwendung". Gibt der Administrator eine Applikation ein, beispielsweise "Winword", klickt dann auf "Sichern" und möchte nun mit "Excel" fortfahren, so überspeichert er leider "Winword". Im Test war stets ein Doppelklick auf "Hinzufügen" notwendig, ehe eine neue, leere Anzeige durch das Programm dargestellt wurde.



IT & TK Training



Geförderte Cisco Zertifizierungen

**Mittelständler (unter 250 Mitarbeiter)
erhalten Fördergelder bis 100%!**

Associate Level

CCENT – Kurs ICND1

CCNA – Kurse ICND1 + ICND2

CCNA Voice – Kurse ICND1 + ICND2 + ICOMM

CCNA Security – Kurse ICND1 + ICND2 + IINS

CCNA Wireless – Kurse ICND1 + ICND2 + IUWNE

CCDA – Kurse ICND1 + ICND2 + DESGN

Professional Level

CCNP – Kurse ROUTE + SWITCH + TSHOOT

CCNP Voice – Kurse CVOICE + CIPT1 + CIPT2 + TVOICE + CAPPS

CCNP Security – Kurse SECURE + FIREWALL + IPSv7 + VPN

CCDP – Kurse ROUTE + SWITCH + ARCH

... und alles mit garantierten Kursterminen! 



Scannen Sie unsere vCard
oder rufen Sie einfach an:
Tel. 06074 4868-0



Applikationen weist TSP entweder lokalen Benutzern oder Gruppen zu oder nutzt die Anbindung an das Active Directory, der direkte Verweis auf OUs ist nicht möglich. Jedes Programm, das im Vorfeld angelegt wurde, steht anschließend als Checkbox zur Verfügung, die dem Benutzer oder einer Gruppe zugeordnet wird. Es versteht sich von selbst, dass bei einer kompletten Freischaltung des Desktops eine derlei genaue Zuordnung überhaupt nicht möglich wäre. Hierfür setzt TSP auf einen eigenen Windows-Agenten, der die Verbindung aufbaut, oder auf eine Anmeldung per Webinterface, das einen Java-Agenten aktiviert. In den Server-Stammdaten hat der Administrator die Möglichkeit, den freien Zugriff per Standard RDP-Clients auf den Server zu sperren, um so eine Umgehung der Richtlinie zu verhindern.

Selbstgebaute Agenten erhöhen Sicherheit und Komfort

Um die Verwendung von Seamless-Windows-Applikationen auf einem Windows-Client-System zu erzwingen und gleichzeitig dem Benutzer den Aufruf so einfach wie möglich zu machen, erlaubt TSP, einen Windows-Zugriffs-Client als ausführbare Datei zu erzeugen. Alle Parameter, etwa den Benutzernamen, die Farbtiefe, Zugriff auf lokale Ressourcen oder die Art des Ausdrucks, legt der Administrator in diesem selbsterklärenden Programm fest. Es ist sogar möglich, das Zugriffspasswort direkt einzuspeichern. Besonders praktisch in Bezug auf die Sicherheit: Der Administrator legt auf Wunsch fest, von welcher USB-Stick-Seriennummer sich der Client ausschließlich starten lässt und auf welchem PC-Namen das Programm funktionieren soll. Somit kann der IT-Verantwortliche bei Bedarf einen zusätzlichen Dongle in Form ei-

nes USB-Sticks erzeugen. Aber auch ohne von einem USB-Laufwerk zu starten, arbeitet das Programm im Test einwandfrei.

Wird das Programm gestartet, so dauert es zirka 30 Sekunden, bis die Verbindung komplett aufgebaut ist. Auf der rechten Fensterseite wird ein optisch an Windows angelehntes Menü mit den freigegebenen Applikationen angezeigt. Je nach Konfiguration bieten sich zwei Farbmodelle und zwei Darstellungsformen an, die sich jedoch nur optisch voneinander unterscheiden. Die Seamless-Windows-Applikationen arbeiten wie gewohnt, lassen sich maximieren oder minimieren und in der Größe anpassen.

Zugriff per Webservice


Neben dem eigenen Agenten für Windows-Computer und dem Standard-RDP-Aufruf erlaubt die Software die Verwendung eines internen Webservers, um einen Java-Agenten auf einem Client-System zu starten. In der Teststellung weigerte sich die aktuelle Version 5 jedoch vehement, den eingebauten Webserver so zu starten.

Wegen dieser Auffälligkeit luden wir die Software noch einmal von der französischen Hauptseite herunter. Dort stand, entgegen der auf der deutschsprachigen Seite zu findenden Version 5.20, noch die frühere Version 4.20 zum Download bereit. Die Version 4.20 trägt jedoch im Administrationsinterface den Namenszusatz "TSplus 2012" – die Verwirrung war nun komplett. Kurzerhand installierten wir die 4.20-Fassung, stellten die Sprache auf "Deutsch" um und konnten problemlos auf den Webserver zugreifen. Anschließend war es uns im Test möglich, auf die Webseite zuzugreifen und die definierten Applikationen zu öffnen. Der so gestartete Java-Client zeigte die Seamless-Windows-Applikationen in derselben Art an wie der zuvor beschriebene EXE-Agent.

Fazit

Das Kernsystem von TSplus 2012 arbeitet exakt so, wie es der Hersteller verspricht. Die Management-Software der aktuellen Version 5.20 konnte im Test nicht so recht überzeugen und scheint hier und da noch mit der heißen Nadel gestrickt zu sein. Der Webserver für die Verwendung des Java-Zugriffs auf bereitgestellte

Applikationen funktionierte erst gar nicht. Erst ein Rücksprung auf die Vorgängerversion ermöglichte es, überhaupt mit dem Test fortzufahren.

Das seltsame Software-Design ist sicherlich Geschmacksache, die Steuerung über INI-Dateien ist im Jahr 2012 jedoch garantiert antiquiert. Dass es keine Verwaltungskonsole für die Workstation des Administrators gibt, ist auch nicht gerade zeitgemäß. Der Blick in die Referenzliste zeigt jedoch, dass sich weltweit teilweise namhafte Unternehmen für TSPlus entschieden haben. (jp) 

Produkt

Software für Remotedesktop-Dienste und Mehrbenutzerzugriff.

Hersteller

TSPlus Germany Distribution
www.terminalserviceplus.de

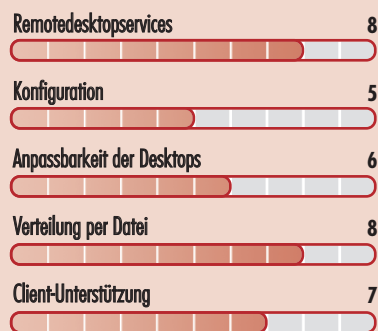
Preis

Der Preis ist gestaffelt nach Leistungsumfang und beginnt bei 71,40 Euro für eine Basisversion der 3-Benutzer-Lizenz. In der maximalen Ausbaustufe ohne Benutzer-Begrenzung kostet die Software in der "TSPlus Unlimited Corporate Edition" mit Universal Printing, HTTPS/SSH-Tunneling, HTML5 iPad/Android-Access und Server Gateway rund 1.120 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für Unternehmen, die in kleinen Umgebungen möglichst identische Desktops mit geringen Kosten bereitstellen wollen.

bedingt für Unternehmen, die eine komplexere Terminalservice-Umgebung betreiben müssen.

nicht für Unternehmen, die keinen Bedarf an Remotedesktops haben.

TSPlus 2012

In Terminalservice-Umgebungen gibt es immer wieder das Problem der Druckerzuordnung. An dieser Stelle haben sich die Entwickler von TSP galant aus der Affäre gezogen. Der "Universalprinter" druckt einen Auftrag in eine PDF-Datei und zeigt diese in einem lokal installierten PDF-Viewer an. Von dort aus druckt der Benutzer das Dokument tatsächlich auf seinem Drucker. Alternativ bleibt die Möglichkeit, den lokal am Client-Computer angeschlossenen Drucker direkt zu nutzen, sofern die Treiber verfügbar sind.

Druck per PDF



1&1 DOMAINS

DIE GRÖSSTE AUSWAHL FÜR IHRE WUNSCH-DOMAIN.

.de .com .net

VERTRAUEN SIE DER NUMMER 1

1&1 ist einer der größten Webhoster weltweit. Mit über 11 Mio. Kundenverträgen, 2 Milliarden € Jahresumsatz, 5.000 Mitarbeitern und 5 Hochleistungs-Rechenzentren. Und weil wir mit mehr als 18 Mio. registrierten Domains auch ein führender Registrar sind, profitieren Sie von außerordentlich günstigen Preisen!



GRÖSSTE AUSWAHL

Mehr als 30 Domainendungen verfügbar: .de, .eu, .com, .net, .org, .us, .at, .info, .biz, .mobi, .name, .ch, .li, .co.uk, .me.uk, .org.uk, .co, .tv, .ws, .cc, .be, .as, .lt, .lv, .nu, .ph, .hn, .vc, .sc, .ag, .to, .vu



1&1 DOMAIN APP

Domaincheck und Domainregistrierung mit der 1&1 Domain App auch mobil möglich.



VOLLE DNS-KONTROLLE

Einfach über Verwaltungstool.



INKLUSIVE-LEISTUNGEN

- Kostenlose Domain-Umleitung
- Domain Kontakt-Management
- Kostenlos Subdomains einrichten und umleiten



24/7 SUPPORT

Unser Experten-Team ist rund um die Uhr per Telefon und E-Mail erreichbar.

.de
.com
.net
.org
.info

12 MONATE

ab **0,29** €/Monat*

1 Jahr ab 0,29 €/Monat,
danach ab 0,49 €/Monat*

**AKTION: JETZT OHNE
EINRICHTUNGSGEBÜHR!**



DOMAINS | E-MAIL | WEBHOSTING | E-SHOPS | SERVER

 0 26 02 / 96 91

 0800 / 100 668

www.1und1.info

* Aktion bis 30.11.2012 : Pro Neuvertrag eine Domain zum Vorzugspreis, z.B. .de, .info 12 Monate 0,29 €/Monat, .com, .net, .org 12 Monate 0,69 €/Monat. Normalpreis .de 0,49 €/Monat, .info 1,99 €/Monat, .com, .net, .org 1,49 €/Monat. Einrichtungsgebühr von 9,60 € entfällt im Rahmen der Aktion. 12 Monate Mindestvertragslaufzeit. Preise inkl. MwSt.



Im Test: Acceleratio Terminal Services Log 3.7.5 Stiller Beobachter

von Jürgen Heyer



Quelle: Visty - Fotolia.com

Gerade in größeren Terminalserverfarmen ist es für einen effizienten Betrieb überaus wichtig, sowohl die Nutzung als auch die Auslastung kontinuierlich zu überwachen. Nur so kann ein Administrator rechtzeitig auf Veränderungen reagieren und bei Bedarf erweitern oder reduzieren. Ein äußerst umfassendes Monitoring verspricht hier Terminal Services Log von Acceleratio. IT-Administrator hat die Fähigkeiten der Software genauer untersucht.

Die Bezeichnung einer Monitoring-Software als "Terminal Services Log" (TSL) mag etwas ungewöhnlich klingen, sie beschreibt aber die Funktion recht gut, denn im Fokus steht die Überwachung von Terminalserverfarmen unter Windows Remote Desktop Services und Citrix XenApp. Dabei handelt es sich nicht um eine typische Ereignis-Überwachung zum schnellen Aufdecken von Fehlfunktionen, sondern um die Aufzeichnung aller Aktivitäten sowie der Nutzung und Auslastung. Das Resultat ist ein umfassendes Reporting mit diversen vorgefertigten, sehr detaillierten, dynamischen Berichten sowie der Möglichkeit, eigene Auswertungen zu definieren.

Je größer eine Terminalserverfarm ist, desto wichtiger ist es, die Auslastung im Auge zu behalten. Zum einen liegt es im Interesse eines jeden Unternehmens, nur so viele Ressourcen bereitzustellen, wie tatsächlich benötigt werden, sodass es sehr hilfreich ist, die Auslastung über den Tages- und Wochenverlauf zu kennen. Zum anderen sollten sich Ände-

rungen an den Nutzergewohnheiten, die für eine steigende oder sinkende Auslastung verantwortlich sind, erkennen lassen, um rechtzeitig zu reagieren.

Kein Bedarf an Agenten

Terminal Services Log ist in drei Versionen verfügbar: Die Standard Edition eignet sich für einzeln betriebene Terminalserver und die Professional Edition für mittelgroße Farmen mit ein bis zehn

Servern. In diesen beiden Fällen erfolgt die Installation auf jedem Server. Die Enterprise Edition letztendlich richtet sich an größere Farmen, wo die Software auf einem unabhängigen Monitoring-System installiert wird und von dort alle zu überwachenden Server abfragt. Darüber hinaus besitzt die Enterprise Edition einen deutlich größeren Funktionsumfang. So erlaubt sie das Erstellen eigener Berichte und arbeitet mit rollenbasierten Zugriffsrechten. Ein gro-

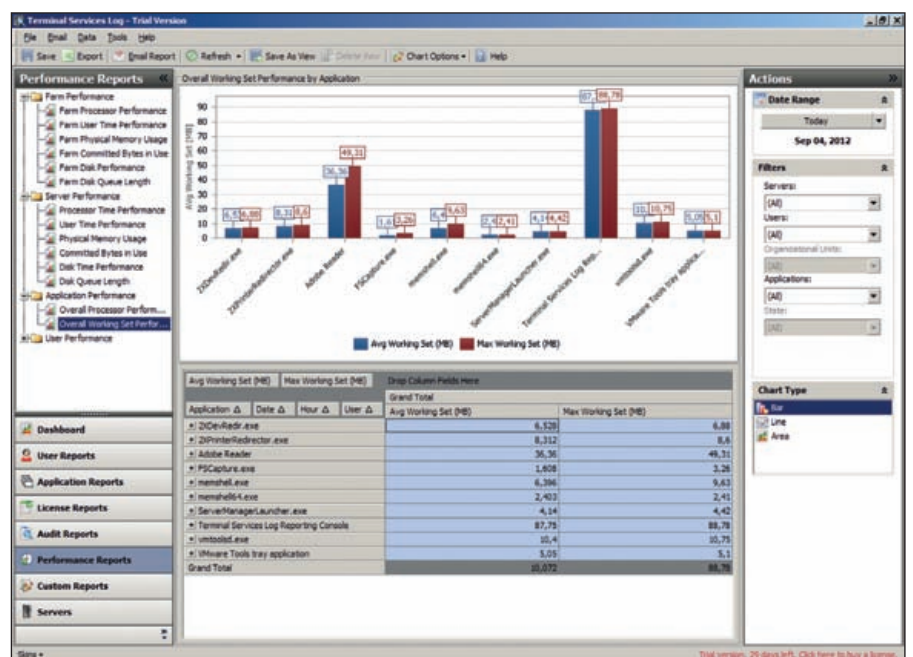


Bild 1: Für die aufgerufenen Programme liefert TSL die minimale und maximale Arbeitsspeicherbelegung



ßer Vorteil ist die agentenlose Arbeitsweise, sodass auf den überwachten Terminalservern nichts zu installieren ist.

Getestet haben wir die TSL Enterprise-Version, installiert auf einem Windows Server 2008 R2. Überwacht wurden zwei Terminalserver ebenfalls unter Windows Server 2008 R2, auf denen diverse Applikationen freigegeben waren, auf die eine Handvoll Clients zugriff. Alle Systeme waren Mitglied einer Windows-Domäne.

Am Anfang steht die Datenbank

TSL kommt mit einer integrierten Datenbank, im Handbuch als SQL Compact bezeichnet. Diese eignet sich unserer Meinung nach aber bestenfalls für einen Ressourcen-schonenden Betrieb der Standard Edition. Laut Handbuch ist der Umfang der Berichte mit dieser Datenbank recht eingeschränkt und der volle Funktionsumfang steht erst mit einer externen MS SQL-Datenbank zur Verfügung. Das bedeutet übrigens nicht, dass hier unbedingt noch zusätzliche Investitionen fällig sind, da es auch legitim ist, die kostenlose Express-Version zu verwenden. So nutzten wir im Test MS SQL 2005 Express mit einer Standardinstallation und Windows-Authentifizierung.

Die Installation des knapp 40 MByte großen Pakets verlief problemlos, anschließend startete ein Assistent, um die beschriebene Datenbank auszuwählen und um festzulegen, ob nur ein oder mehrere Server überwacht werden sollen. Gut gefiel uns, dass sich der Datenbankzugriff gleich überprüfen lässt und die Software auf Wunsch im Netz nach SQL-Servern sucht. Sofern noch keine SQL-Instanz angelegt ist, übernimmt dies TSL, sodass spezielle SQL-Kenntnisse nicht erforderlich sind.

Windows Server 2003/2008 (R2), Microsoft SQL Server 2005/2008 (Express Edition) empfohlen, Windows Terminal Services beziehungsweise Remote Desktop Services, Citrix XenApp 5, 6 oder 6,5 oder Presentation Server 4.0/4.5, Citrix Metaframe XP.

Systemvoraussetzungen

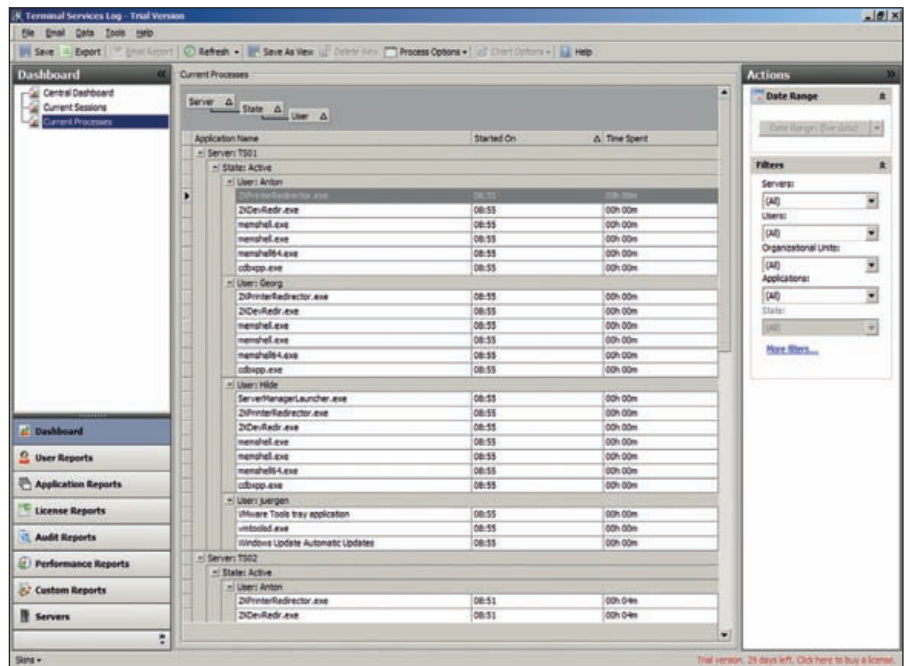


Bild 2: TSL ermittelt pro Terminalserver-Benutzer auch die gestarteten Prozesse

Schneller Start über zentrale Konsole

Die zentrale Administration erfolgt bei der Enterprise Edition über eine Konsole, die auf dem Server aufzurufen ist, auf dem TSL installiert ist. Gefallen hat uns hier die intuitiv bedienbare, dreispaltig aufgebaute Oberfläche. In der rechten Spalte sind die verschiedenen Berichtsarten thematisch gruppiert aufgelistet. Die mittlere, breite Spalte enthält den jeweils ausgewählten Bericht in Textform sowie als Grafik und die rechte Spalte erlaubt eine Filterung sowie die Wahl der grafischen Darstellung. Ist in der mittleren Spalte keine Grafik zu sehen, muss der Administrator nur weiter nach unten scrollen. Die Spalte ist bei den meisten Berichten schlichtweg deutlich länger, als auf den Monitor passt.

Nach Abarbeiten des Assistenten für die Datenbankwahl sind nur noch wenige Einstellungen zu tätigen. So lässt sich das Abfrageintervall an die gewünschte Mess-Auflösung sowie an die Anzahl der abzufragenden Server anpassen. Standardmäßig sind 90 Sekunden eingestellt, wobei der wählbare Bereich zwischen 15 und 360 Sekunden liegt. Der Hersteller empfiehlt allerdings, das Intervall nicht kleiner als 60 Sekunden zu wählen. Letzten Endes hängt die Einstellung mit davon ab, wie viele Server zu überwa-

chen sind, damit sich in einem Zyklus alle Informationen einsammeln lassen.

Weiterhin lässt sich einstellen, ab welcher Zeit der Inaktivität eine Remote-Verbindung als untätig gezählt werden soll. Erfreulicherweise ermöglicht die Enterprise Edition auch eine anonyme Aufzeichnung der Aktivitäten, bei der eine Sicht auf einen individuellen Benutzer nicht möglich ist.

Sinnvolle Filtermöglichkeiten

Damit sich Auswertungen später besser interpretieren lassen, kann der Administrator Arbeitszeitrahmen festlegen. Damit ist es dem Programm möglich, Berichte bezogen auf die Arbeitszeit ausgeben zu lassen. TSL überwacht prinzipiell die Nutzung aller ausführbaren Dateien, was aber zur Folge hat, dass beispielsweise systemnahe Applikationen wie Windows Update oder die VMware Tools in den Auswertungen erscheinen. Verständlicherweise sind diese in der Regel für eine Auswertung nicht relevant, weshalb TSL die Möglichkeit bietet, eine entsprechende Filterung durchzuführen. Ähnliches gilt für die laufenden Prozesse, wobei die Windows-Systemprozesse bereits standardmäßig ausgefiltert sind. Sie lassen sich aber bei Bedarf mit in die Auswertung aufnehmen.

Zu beachten ist, dass TSL zu den ausgefilterten Dateien und Prozessen keinerlei

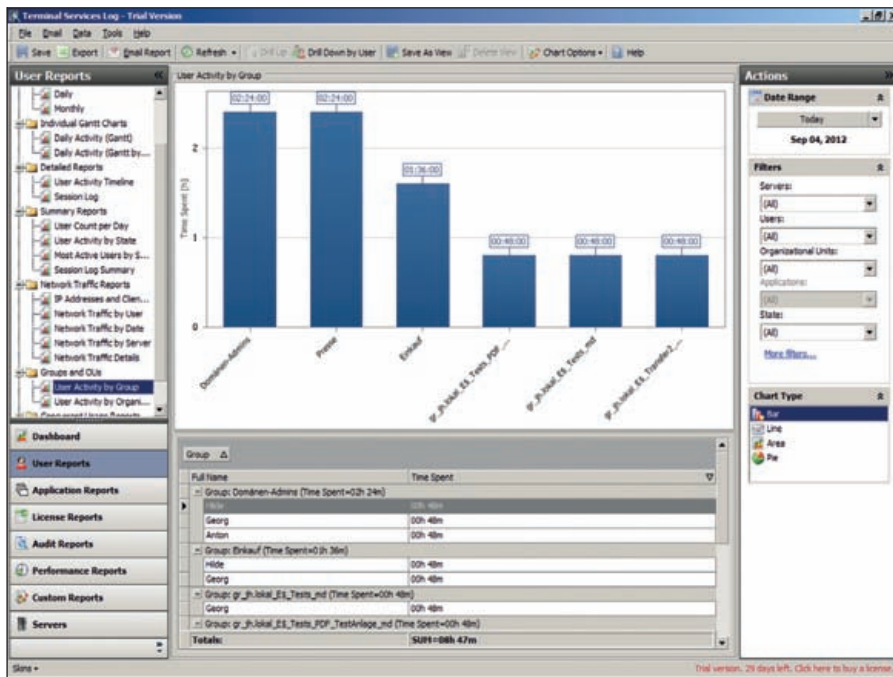


Bild 3: Bei Einbindung in ein Active Directory gruppiert TSL die Daten auch über dort angelegte Gruppen

Informationen speichert, auch nicht im Hintergrund. Das vermeidet ein unnötiges Aufblähen der Datenbank, bedeutet aber im Umkehrschluss, dass es nicht möglich ist, für eine gefilterte Applikation im Nachhinein doch noch eine Auswertung zu bekommen, indem sie einfach nachträglich wieder aus der Filterung herausgenommen wird. Vielmehr kann eine Auswertung dann erst ab dem Zeitpunkt erfolgen, ab dem die Filterung beendet wurde.

Um zu ermitteln, aus welchen IP-Bereichen sich die Benutzer anmelden, ist es möglich, einzelne Bereiche zu definieren und die laufenden Anmeldungen dahingehend zu analysieren. Dann erstellt die Software entsprechende Auswertungen. Neben dem Filtern auf Applikationsebene enthält TSL einen sogenannten Filepath Manager, mit dem sich großzügig ganze Programmpfade ausschließen lassen, für die kein Audit erfolgen soll. Damit ist es in der Regel noch einfacher möglich, sich genau auf die Software zu konzentrieren, für die eine Auswertung erstellt werden soll, und alles andere beiseite zu lassen.

Komfortable Benachrichtigung und AD-Integration

Um die Benachrichtigung zu automatisieren, ist ein Zeitplaner zum Mailversand von Berichten integriert. Dieser verschickt

täglich, wöchentlich, monatlich oder vierteljährlich seine E-Mails. Als komfortabel empfanden wir den dazugehörigen Subscription Manager, der es erlaubt, mit einer Mail mehrere Berichte zu versenden, und der bei Bedarf unterschiedliche Berichte an verschiedene Mailadressen verschickt. So kann der IT-Verantwortliche recht bequem verschiedene Empfänger mit unterschiedlichen Berichten adressieren. Voraussetzung für den Mailversand ist natürlich die Einrichtung des SMTP-Mails innerhalb von TSL.

Die Aufnahme der Server in TSL zur Überwachung kann über eine Suchfunktion erfolgen. Sehr gefallen hat uns dabei wie schon erwähnt, dass die zu überwachenden Server ohne Agent abgefragt werden, sodass nichts zu installieren ist.

TSL besitzt eine Active Directory-Integration und kann Auswertungen in Relation zu den Gruppen- und OU-Zugehörigkeiten erstellen. Gesammelt werden die Informationen allerdings nur für Gruppen und OUs, die Mitglieder in der Terminalserverfarm haben. Informationen zu Benutzern, die nicht als Terminaldienst-Benutzer angemeldet sind, werden nicht erfasst.

Bezüglich der Verwendung von TSL gibt es in der Enterprise Edition eine Benut-

zerrollenverwaltung, die allerdings recht einfach gestaltet ist. So existieren nur drei Rollen und ein Benutzer hat entweder keine Nutzungsrechte, er kann nur betrachten oder in vollem Umfang administrieren.

Ordnung durch Aufräum-Job

Damit die Datenbank nicht unkontrolliert wächst, lässt sich ein Aufräumjob definieren, der Einträge entsprechend des Alters löscht. Ab welchem Alter die Daten gelöscht werden, kann der Administrator beliebig vorgeben. Dieser Job ist übrigens nur einer von mehreren, denn TSL führt diverse Aktualisierungen und Aufgaben Job-orientiert durch. Dazu gehören unter anderem der Versand von E-Mails, der Import bei einer AD-Integration sowie die Auswertung der Performance-Counter und der gleichzeitigen Applikationsnutzung. In einer Übersicht sind alle System-Jobs übersichtlich aufgelistet mit dem Zeitpunkt der letzten und nächsten Ausführung sowie dem Intervall.

Abschließend mussten wir feststellen, dass TSL auf jeden Fall mehr Einstellungsmöglichkeiten besitzt, als wir zu Beginn registrierten. Das hing sicher auch damit zusammen, dass bei der Inbetriebnahme nur wenige Angaben erforderlich sind und ein Anfang mit den Standardeinstellungen durchaus möglich ist. Nach und nach wird ein Administrator sicher ein Feintuning durchführen wollen, dies ist jedoch nicht Voraussetzung für eine Inbetriebnahme. Was die Aktualisierung von TSL anbetrifft, so prüft die Software regelmäßig auf die Verfügbarkeit eigener Updates.

Berichte in Hülle und Fülle

Der von TSL standardmäßig bereitgestellte Berichtsumfang ist beeindruckend. Der Übersicht halber ist er in die Rubriken Dashboard, Benutzer, Applikationen, Lizenzen, Auditing, Performance und eigene Berichte unterteilt. In jeder Rubrik außer den eigenen Berichten finden sich diverse vorgefertigte Berichte, in der Summe sind es rund 60 Reports. Diese bestehen erfreulich systematisch und fast durchgehend aus einer doppelten Ansicht, nämlich einer dynamischen Pivot-Tabelle und einer grafischen Darstellung.



Druckerupdates: eine Sache von Minuten, keine Wochenendschicht.

Der MFP. Neu definiert von HP. Unsere Ausgangsbasis war die bekannte Zuverlässigkeit von HP LaserJets. Ergänzt haben wir ein preisgekröntes, zeitsparendes Tool für das Management Ihrer Druckerflotte. HP Web Jetadmin gibt Ihnen die nötige Flexibilität und Kontrolle, um mehr Drucker mit deutlich weniger Aufwand zu verwalten und zu sichern.¹ Lernen Sie die neuen HP LaserJet Multifunktionsdrucker kennen: hp.com/de/mfp



Make it matter.



¹ HP Web Jetadmin wurde von Buyer's Laboratory Inc. mit der Höchstbewertung von 5 Sternen ausgezeichnet. Besuchen Sie www.hp.com/go/wja, um den BLI-Bewertungsbericht für April 2011 anzusehen. HP Web Jetadmin ist kostenlos und steht unter www.hp.com/go/webjetadmin zum Download bereit. Abgebildetes Modell: HP LaserJet Enterprise 500 color flow MFP M575c, inklusive zusätzlicher 500 Blatt Papierzuführung (CF084A) und Printer Cabinet (CF085A).
© 2012 Hewlett-Packard Company, L.P.

Die Entscheidung für eine dynamische Pivot-Tabelle hat den Vorteil, dass sie sich sehr einfach gruppieren und somit in der Betrachtungstiefe verändern lassen. Für die grafische Darstellung stehen wiederum die vier Typen Balken, gestapelte Balken, Linien und Flächen zur Verfügung. Darüber hinaus fanden wir vorbereitete Gantt-Diagramme. Weiterhin kann der Nutzer zwischen einer Vielzahl an unterschiedlichen Farbkombinationen wählen und hat diverse Möglichkeiten zur Positionierung der Legende. Möglich ist außerdem eine Darstellung in TopN-Form, bei der immer nur die Spitzenreiter angezeigt werden. Wie viele Einträge dabei sichtbar sein sollen, ist frei wählbar.

Um bei der Enterprise Edition leichter eigene Berichte zu erstellen, hilft ein Assistent, der in mehreren Schritten die Kriterien abfragt. Letztendlich erzeugt der Assistent daraus eine SQL-Abfrage, die gespeichert wird. Auch in Verbindung mit den vorbereiteten Berichten kann der Administrator einen bestimmten Satz an Einstellungen als sogenannte View unter einem frei wählbaren Namen speichern. Die Views sind dann im Dashboard zu finden. So sind die für den Nutzer wichtigsten Auswertungen auf einen Blick erreichbar.

Sehr umfassend stellen sich die Möglichkeiten zur Performancemessung dar. Dabei ermittelt TSL neben den Performancedaten für einen Server wie Prozessorauslastung, Nutzungszeit, Speicherauslastung auch die Werte für mehrere Server in einer Farm und stellt diese nebeneinander dar. So lassen sich beispielsweise unterschiedliche Auslastungen recht leicht aufdecken.

Nachdem TSL sehr genau dokumentiert, wer welche Applikationen aufruft, resultiert daraus eine integrierte Lizenzverwaltung. Zusätzlich kann der Administrator erfassen, für welche Applikation wie viele Lizenzen vorhanden sind, sodass TSL dann einen Bericht liefert, der detailliert jede Unter- und Überlizenzierung entsprechend unterschiedlich farbig unterlegt ausgibt. Dabei beherrscht TSL unterschiedliche Lizenzmodelle wie Client-bezogene Lizenzen oder die parallele Nutzung (Concurrent Use). Für eine weitere

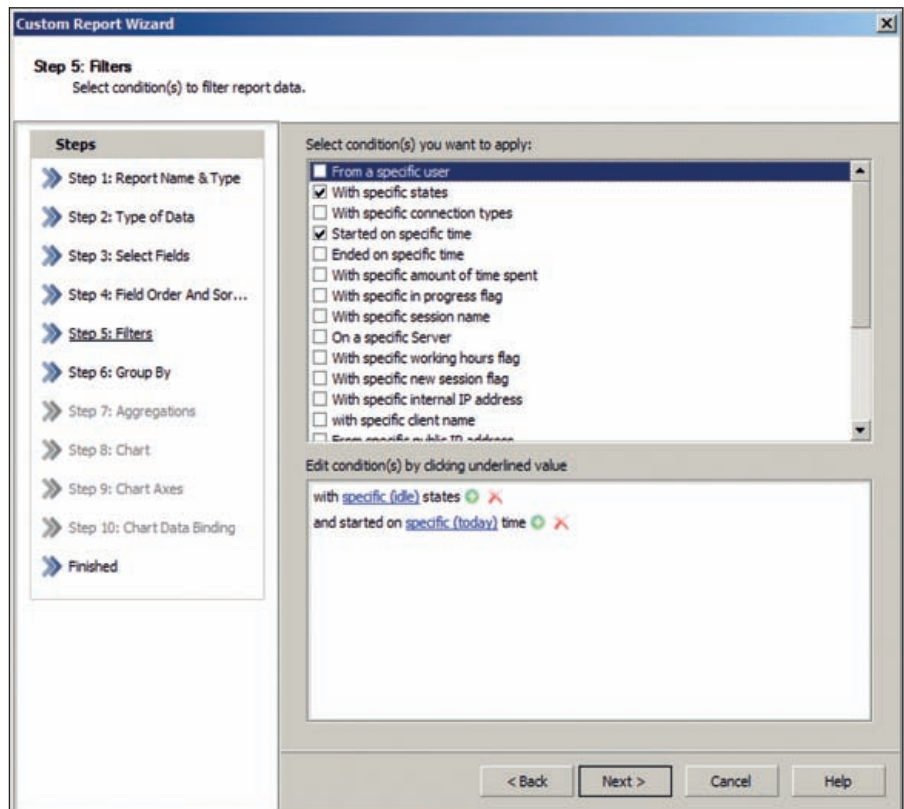


Bild 4: Dank eines komfortablen Assistenten lassen sich eigene Abfragen erfreulich leicht erstellen

Auswertung liefert das Programm zusätzlich die Informationen, an welchem Client welche Lizenzen benutzt wurden.

Bei der genaueren Betrachtung der Berichte fiel uns auf, dass TSL standardmäßig sehr detaillierte benutzerbezogene Auswertungen erstellt. Um mögliche Konflikte mit einer unzulässigen Arbeitskontrolle der Anwender zu vermeiden, ist eine optionale Anonymisierung wie schon oben erwähnt vorgesehen. Diesbezüglich sollten hierzulande unbedingt die Bestimmungen beachtet und gegebenenfalls der Betriebsrat mit eingebunden werden.

Individuelle Suchfilterung

Vorteilhaft für die Suche nach bestimmten Ereignissen ist die Möglichkeit, das Zeitbetrachtungsfenster frei zu wählen, sodass sich ein beliebiger Zeitraum relativ einfach eingrenzen und gestreckt darstellen lässt. Das Maß der möglichen Streckung bestimmt natürlich maßgeblich das gewählte Abfrageintervall, da eine Analyse nicht genauer sein kann. Weiterhin lässt sich nach Servern, Benutzern, Organisationseinheiten, Applikationen, der Verbindungsart, der Arbeitszeit, nach einer angelegten Gruppierung und nach dem Sitzungsstatus filtern.

In Verbindung mit den vielen vorbereiteten Auswertungen und den beschriebenen Filtermöglichkeiten liefert TSL sehr detaillierte Daten mit individuell wählbarem Fokus. Unserem Eindruck nach stellt TSL eine wertvolle Hilfe bei der Auswertung dar. Um die Berichte außerhalb von TSL nutzen zu können, findet ein Export nach Excel Unterstützung, und zwar wahlweise als statisches oder dynamisches Arbeitsblatt sowie als Pivot-Tabelle. Dies hat den Vorteil, dass auch jemand, der nicht direkt auf TSL Zugriff hat, die Messwerte analysieren und weiterverarbeiten kann. Neben einem Excel-Export bietet TSL das Speichern als PDF-Datei an. Dies umfasst sowohl die Tabellenansichten als auch die Grafiken.

Kein Blick in die Zukunft

Zu beachten ist, dass TSL in erster Linie ein passives Monitoring und Reporting in vorgegebenen Intervallen durchführt, ohne über die Angabe und Überwachung von Schwellenwerten gleich eine Alarmierung durchzuführen. Das hängt mit dem Job-orientierten Betrieb zusammen. Trotzdem unterstützt TSL in Verbindung mit den eigenen Berichten eine Echtzeit-Alarmierung. Dann wird bei Überschrei-

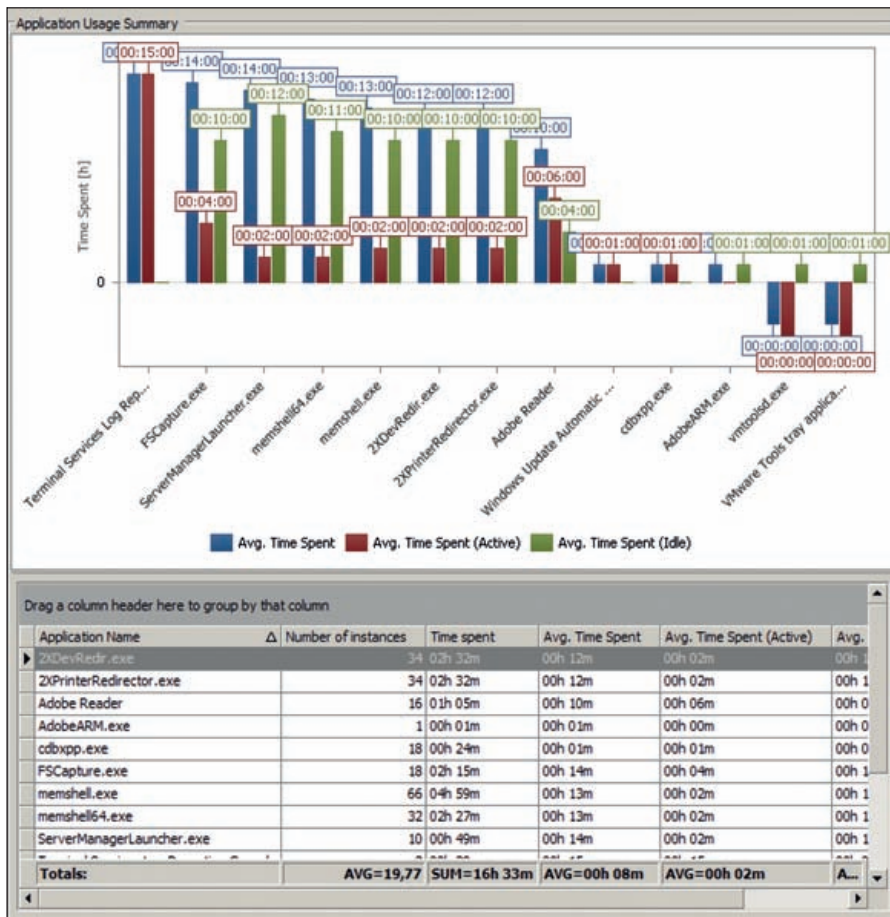


Bild 5: Bei der Auswertung der Applikationsnutzung unterscheidet TSL zwischen aktiver Nutzung und Leerlaufzeiten

ten eines Schwellenwertes sofort eine E-Mail versendet. Letztendlich aber ersetzt TSL damit kein Überwachungstool, das auch noch die Events verarbeitet. Es ist aber bei wichtigen Schwellenwertüberschreitungen für eine zusätzliche Alarmierung einsetzbar.

Auch verhält sich TSL insgesamt recht passiv: Es stellt die erfassten Messwerte ansprechend und übersichtlich dar, führt jedoch keine weitere Analyse durch, um anhand derer selbst Hinweise für empfehlenswerte Aktionen zu geben. Letztendlich vermissen wir eine Trendanalyse anhand der Fülle der erfassten Daten, die bei der Planung unterstützen könnte. Hier sehen wir für TSL noch Entwicklungspotential. Nichtsdestotrotz steht es dem Nutzer natürlich frei, die exportierten Daten beispielsweise in Excel weiterzuverarbeiten und eigene Trendanalysen fortzuschreiben.

Obwohl TSL die Nutzungsdaten genauestens erfasst, gibt es keine Billing-Funktion, um diese bei Bedarf für eine Abrech-

nung nutzen zu können. Hier sehen wir eine weitere Möglichkeit für eine funktionale Erweiterung.

Fazit

Terminal Services Log von Acceleratio erfasst in frei wählbaren Intervallen eine Vielzahl an Parametern von den Servern und speichert diese in einer SQL-Datenbank für anschließende Auswertungen. Das Programm hat damit einen klaren, relativ eng begrenzten Fokus, den es aber mit Bravour beherrscht. Die umfassenden und detaillierten Berichte haben uns in jeder Hinsicht überzeugt. Weiterhin lassen sich mit der Enterprise Edition eigene Berichte definieren. Durch die Aufbereitung als Pivot-Tabellen sind innerhalb der Berichte wiederum eigene Gruppierungen möglich. Für einen schnellen Blick eignet sich zudem das Dashboard, für das sich aus den vorhandenen Berichten eigene Ansichten speichern lassen.

Vermisst haben wir allerdings die Möglichkeit, dass TSL die Zahlen selbst hinsichtlich erkennbarer Trends analysiert, um

von sich aus auf drohende Engpässe oder eine ineffiziente Nutzung hinzuweisen. Dank der detaillierten Analyse der Applikationsnutzung eignet sich TSL recht gut für eine Lizenzüberwachung. Hinsichtlich der Benutzer-bezogenen Auswertungen sind allerdings hierzulande die einschlägigen Regeln zu beachten, damit dies nicht zu einer unzulässigen Überwachung von Mitarbeitern führt. Erfreulicherweise lassen sich die Auswertungen diesbezüglich anonymisieren. (In)



Produkt

Monitoring-Werkzeug für Terminalserverfarmen unter Windows Remote Desktop Services und Citrix XenApp.

Hersteller

Acceleratio
www.terminalserviceslog.com

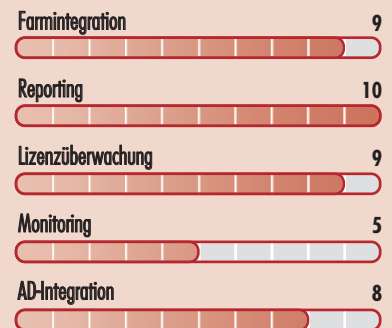
Preis

Die Standard Edition kostet 299 US-Dollar pro Server, die Professional Edition 499 US-Dollar und die Enterprise Edition 2.499 US-Dollar pro Farm sowie 199 US-Dollar pro Server in der Farm.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für mittlere und größere Terminalserverfarmen, die mehrere Desktops und Applikationen bereitstellen und die aufgrund der Größe und Nutzungsintensität einer ständigen Überwachung bedürfen.

bedingt für kleine Farmen mit sehr wenigen Applikationen, da der Nutzen unserer Meinung nach dann begrenzt ist.

nicht für Umgebungen, die keine Terminalserverfarmen im Einsatz haben, sondern auf andere Techniken setzen.

Acceleratio Terminal Services Log 3.7.5

Im Kurzttest: androidVNC 0.5.0

Fern und doch ganz nah

von Sandro Lucifora

VNC hat sich zu einem der meistgenutzten Fernsteuerungs-Tools gemauert. Es ist kostenlos und beschränkt sich auf die wichtigste Funktion: Die Fernbedienung von Computern. VNC ist mittlerweile auf zahlreichen Betriebssystemen einsetzbar, unter anderem auch auf Android. Bei Google Play sind einige VNC-Viewer im Angebot, von denen wir uns mit dem kostenlosen androidVNC den am meisten heruntergeladenen genauer angesehen haben.

Wir haben androidVNC sowohl auf einem 4 Zoll-Smartphone mit Android 2.3 als auch einem 7 Zoll-Tablet mit Android 4.0 getestet. Nach dem Start erscheint im festen horizontalen Layout eine Eingabemaske für die benötigten Parameter. Neben einer beschreibenden Bezeichnung erwartet der Dialog die Eingabe der IP, des VNC-Kennworts sowie des Ports, sofern dieser vom Standard abweicht. Optional ist auch das Hinterlegen eines Usernamens samt Passwort für die Windows-Authentifizierung möglich. Als weitere Parameter stehen die Farbtiefe, das Einschalten der Ansicht des lokalen Mauszeigers sowie die Angabe eines Repeaters zur Verfügung. Letzterer wird von UltraVNC verwendet und erlaubt den Zugriff auf mehrere VNC-Hosts über eine IP und einen Port.


Im Test haben wir das ebenfalls kostenlose TightVNC auf einem Server sowie einer Workstation installiert und als Host eingesetzt. Die Verbindung wurde sehr schnell aufgebaut und die Darstellung des Desktops war klar und deutlich. Überzeugt hat uns, dass sich der Bildschirmausschnitt mit dem Finger bewegen lässt. Ebenso kann der Nutzer den Mauszeiger mit der Fingerspitze positionieren. Diese Arbeitsweise gleicht der in einem Android-Browser.

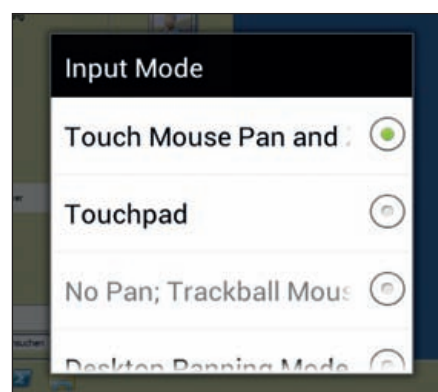
Schwieriger war es jedoch zum Beispiel, ein im Vollbildmodus geöffnetes Fenster zu schließen, da das genaue Positionieren des Mauszeigers durch die breite Fingerkuppe, besonders in der Display-Ecke, zu ungenau wird. Um auch dies zu bewerkstelligen, wechselten wir den Input-Mode auf Touchpad. Dadurch wird der entfernte

Mauszeiger über den Bildschirm gesteuert wie mit einem Touchpad. Das Festlegen und Senden von Tastaturkombinationen aus Shift, Ctrl, Alt plus einer beliebigen Taste erleichtert den Zugriff auf besondere Funktionen des Rechners.

Grundsätzlich ist der Einsatz von VNC als globale Helpdesk-Applikation in Firmen jedoch problematisch, da so gut wie keine Rücksicht auf Datenschutz genommen wird: Fehlende Features wie Benutzerbestätigung, akustische Signalisierung und Protokollierung sind vor dem Datenschutzbeauftragten sicher schwer zu rechtfertigen. Diese Tatsache ist jedoch für VNC allgemein bekannt und trübt nicht die gute Funktion der App.

Fazit

VNC wurde ursprünglich für den Einsatz im Intranet entwickelt und ist aus Sicherheitsgründen nicht zur direkten Verwendung über das Internet geeignet. Wer von zuhause oder unterwegs mit androidVNC auf Server und Workstation zugreifen möchte, sollte dazu einen sicheren VPN-Zugang nutzen. Über das lokale (W)LAN sind Sicherheitsbedenken ausgeräumt und der Zugriff mittels androidVNC-Viewer auf die Hosts außerordentlich schnell und komfortabel. Die schlanke App ist intuitiv zu bedienen. Lediglich die Umstellung der Input-Modi könnte einfacher erfolgen, da diese im Test öfters gebraucht wurde. Um Einstellungen am Server vorzunehmen, ihn neu zu starten oder mal einen Blick auf den Arbeitsplatz der Kollegen zu werfen, eignet sich androidVNC hervorragend. (In) 



Über die verschiedenen Input-Modi lässt sich der entfernte Mauszeiger optimal steuern

Produkt

Software zur Fernsteuerung von Computern von einem Android-Gerät aus.

Hersteller

androidVNC-Team

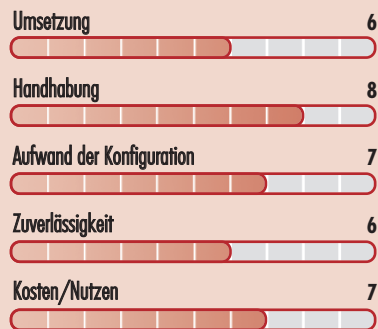
Preis

Kostenlos.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



androidVNC 0.5.0



Einkaufsführer: Auswahlkriterien für KVM-Systeme

Zugriff von nah und fern

von Marc Salimans

Die Administration wachsender dezentraler IT-Infrastrukturen entpuppt sich schnell als echte Herausforderung. Unabhängig von Plattform, Schnittstelle, Standort oder Größenordnung der Infrastruktur benötigen IT-Verantwortliche einen Rundum-Blick auf alle Server und Prozesse sowie professionelle Managementlösungen. Nach wie vor ist für diese Aufgabe der Einsatz von KVM-Hardware in unterschiedlicher Ausprägung die gängigste Lösung. Lesen Sie in unserem Einkaufsführer, worauf es bei der Beschaffung der passenden KVM-Lösung ankommt.

zentrum vornehmen müssen. Nur so können die eingesetzten Werkzeuge optimal auf die IT-Anforderungen abgestimmt werden und garantieren später eine reibungslose Fernadministration. Vor allem die Zahl der zu verwaltenden Server – und deren erwartetes Wachstum – sowie die zu überbrückenden Distanzen sind wichtige Auswahlkriterien. Deswegen sollten IT-Verantwortliche zunächst folgende Fragen klären:

- Wie viele Server sind im Einsatz?
- Welches Serverwachstum erwarten Sie in den nächsten Jahren?
- Aufbau der IT-Umgebung (Anzahl der physischen / virtuellen Server)?
- Wie groß ist die Distanz zwischen den einzelnen Servern?
- Wie viele Administratoren benötigen einen Zugang zum Rechenzentrum?
- Wird von entfernten Standorten auf die Server zugegriffen?

Ist dies geklärt, kann sich der IT-Verantwortliche an die basale Auswahl der Gattung von KVM-Lösungen machen, aus der die dann auszuwählenden Geräte stammen sollen. Hier lassen sich – grob zusammengefasst – folgende Gattungen/Familien feststellen:

- Analoge KVM-Hardware
- LCD KVM-Lösungen
- KVM over IP-Lösungen
- Fernmanagement für virtuelle Umgebungen
- Software-Produkte
- Kombinationen aus Soft- und Hardware

Analog oder IP-basiert

Klassische analoge KVM-Lösungen sind besonders für IT-Umgebungen geeignet, in denen viele Server an einem Standort von wenigen Anwendern bedient werden müssen. Hier eignen sich KVM-Switches mit integrierter LCD-Konsole, die direkt in das Rack (1U-Einschub) eingebaut werden. Eine solche LCD-Konsole macht die Installation eines separaten Monitors überflüssig und erlaubt dem Administrator, die angeschlossenen Server über die Rack-Konsole zu steuern. Jedoch kann die Entfernung zwischen dem System und der Konsole – in Kombination mit einem KVM-Extender-Kabel – auch bis zu 100 Meter betragen, wodurch die Administratoren die Serverlandschaft bequem vom Büroschreibtisch administrieren können. Ein Höchstmaß an Flexibilität bieten KVM-Switches mit Skalierungsfunktion, was diese Geräte für wachstumsorientierte Rechenzentrumsstrukturen unverzichtbar macht. Mittels Kaskadierung und Reihenschaltung können dann über eine Konsole zig Server zentral verwaltet werden.

Doch für weiter verzweigte Unternehmen, die außerdem Virtualisierungsansätze integrieren, reichen reine analoge KVM-Lösungen nicht mehr aus. Zur zentralen Verwaltung solcher größerer und weiter verzweigter Serverlandschaften können IP-basierte KVM-Lösungen zum Einsatz kommen, die einen sicheren Zugriff auf die Serverumgebung unabhängig vom

In Form von Switches, Extendern oder Konsolen ermöglichen KVM-Systeme (Keyboard-Video-Maus) Zugriff auf mehrere Server und Computer über einen Monitor, eine Tastatur und eine Maus. KVM-Lösungen steigern so die Effizienz in Rechenzentren jeder Größe, da sie nicht nur kostbaren Rechenzentrumsplatz einsparen, sondern auch die Wege des Administrators zu den physischen Servern verkürzen, was bei weit verteilten Rechenzentren viele Reisekosten unnötig macht. Mittlerweile ist die Zahl der angebotenen KVM-Lösungen nahezu unüberschaubar – die Palette reicht von purer KVM-Hardware über Softwarelösungen bis hin zu komplexen Kombinationen aus KVM und Managementsoftware.

Suche nach der passenden Managementlösung

Welches System am besten zum Einsatz kommt, hängt von den Einzelfallbedingungen ab, weswegen Administratoren vor einer Investitionsentscheidung eine genaue Analyse der IT-Situation im jeweiligen Rechen-





Standort gewährleisten. Restriktionen bei der Entfernung sind hier nicht mehr gegeben. Die Fernsteuerungstechnik "KVM over IP" bietet entscheidende Vorteile gegenüber analogen Remote-Desktop-Lösungen: Sie ermöglicht neben der Echtzeitsteuerung der angeschlossenen Server mittels Tastatur, Monitor und Maus über TCP/IP-Verbindungen auch wichtige Managementfunktionen. Solche IP-basierten KVMs sind nahezu unbegrenzt erweiterbar, weswegen sie sich gerade dann anbieten, wenn es um eine ohnehin große Anzahl von Servern geht, sowie bei der Anschaffung eines neuen KVM-Switches für einen neuen Serverraum, wenn der Serverraum erweitert werden muss oder wenn mehrere Serverräume an verschiedenen Standorten aufgebaut werden sollen.

Gängige IP-basierte KVMs sind mit acht, 16, 24, 32 oder 40 Ports ausgestattet und eignen sich für nahezu alle Umgebungen ab einem Server. Die Switches werden in einem 1U-Rack installiert und unterstützen gängige Betriebssysteme und Plattformen. Über den Netzwerkport lassen sich die digitalen KVMs einfach in das bestehende Netzwerk integrieren und ermöglichen so eine Fernkontrolle über WAN, LAN, Internet oder Intranet. Solche Geräte sollen IT-Administratoren die Möglichkeit bieten, mit einem beliebigen Web-Browser über einen vernetzten PC – den Remote Client – jederzeit und von jedem Ort aus auf den KVM-Switch und die angeschlossenen Server zuzugreifen, diese autark zu booten und im Notfall, selbst bei totalem Netzwerkausfall, zur Fehlersuche auf ihre BIOS-Ebene zuzugreifen.

Über den Fernzugriff kann dabei auch wichtige Software wie Anwendungs- und Betriebssystempatches von einem zentralen Standort auf allen Servern eines dezentralen Netzwerks installiert sowie Diagnosen durchgeführt werden. Dies erhöht die Sicherheit im Unternehmensnetzwerk, da Fehler durch unautorisierte Zugriffe am Server ausgeschlossen sind und damit das unbemannte Rechenzentrum realisiert werden kann. Zwingend notwendig sind allerdings Sicherheitsfeatures wie Passwortschutz und Verschlüsselung, konfigurierbare Benutzerrechte, protokollierte Zugriffe und eine im Panel-Array-Modus verfü-

bare Echtzeitüberwachung aller angeschlossenen Server. Sind mehrere Administratoren an verschiedenen Standorten tätig, empfehlen sich IP-KVM-Modelle, die ein Nachrichten-Board, ähnlich einem Internet-Chat-Programm, integrieren und den Informationsaustausch, beispielsweise über den Status der IT-Umgebung, untereinander ermöglichen. Kommunikation sollte dabei stets durch Verschlüsselungs-, Authentifizierungs- und Autorisierungsanwendungen geschützt sein.

Fernmanagementlösungen für virtuelle Umgebungen

Heterogene IT-Umgebungen im Rahmen der Virtualisierung stellen eine besondere Herausforderung für das Fernmanagement dar. Selbst wenn durch die Virtualisierung die Hardware im Rechenzentrum auf ein Minimum reduziert wird, bleibt der Bedarf nach einer direkten Verbindung zu den bestehenden physischen Servern, weswegen auch die Notwendigkeit von Verbindungs- und Steuerungslösungen weiterhin existiert. Doch nicht nur das: So ermöglicht Virtualisierung zwar sehr schnelles Implementieren von Entwicklungs- und Testumgebungen neuer Anwendungen. Diese Testumgebungen auf virtuellen Maschinen verbrauchen sehr geringe IT-Ressourcen und bieten Unternehmen die Flexibilität, mit vielen verschiedenen Anwendungen zu experimentieren. Sobald jedoch eine neue Anwendung in der Unternehmensrealität zum Einsatz kommt, wird eine erhebliche Rechenleistung erforderlich, die dann nur von physischen Servern geboten werden kann.

Hochverfügbarkeit der Server und Komponenten ist besonders in virtualisierten IT-Infrastrukturen essenziell und daher der Einsatz einer zuverlässigen Remotemanagementlösung für IT-Administratoren unverzichtbar. Um die Leistung und Vorteile dieser virtuellen IT-Umgebung ausschöpfen zu können, benötigen Administratoren intelligente Zusatzfunktionen für das Fernmanagement. Zur zentralen Verwaltung der physischen und virtuellen Maschinen müssen KVMs mit speziellen Plattformen kompatibel und mit Managementsoftware ausgestattet sein.

Zudem müssen die KVMs in der Lage sein, die komplette IT-Umgebung mit

sämtlichen installierten Geräten, einschließlich Blade-Servern und virtuellen Maschinen, aus der Ferne zu überwachen und zu steuern. Dabei ist eine Unterstützung und Integration virtueller Server-Hypervisoren und Plug-Ins wie VMware Remote Console, Citrix Xen Console, Microsoft Hyper-V, HP Integrity VM und IBM Power VM unverzichtbar. In diesen Fällen sollten sich Administratoren für eine Kombination aus IP-basiertem KVM und Remote Control-Software entscheiden.

Software-basierte Systeme

Eine Alternative zu Hardware-basierten KVM-Lösungen sollen Remote-Control-Softwarepakete darstellen, deren Einsatz jedoch vor allem in großen heterogenen Umgebungen nur eingeschränkt empfehlenswert ist. Der entscheidende Nachteil ist, dass jede reine Softwarelösung nur effektiv arbeiten kann, wenn Hardware und Betriebssystem problemlos laufen. In einem fundamentalen Störfall kann die Software nicht reagieren und bleibt wirkungslos; über einen KVM-Switch hingegen – da völlig unabhängig – kann sogar dann auf das BIOS des Systems zugegriffen werden. Dazu kommt noch der Nachteil der aufwendigen Installation, die beim KVM-Switch vollkommen entfällt, denn dieser ist unmittelbar einsatzfähig und belegt keine Prozessorressourcen.

In komplexen Netzwerkumgebungen verbindet sich der Bedarf an Hardware- und Software-basierter Steuerung, die über ei-

1. Wie viele Server werden kontrolliert?
2. Wie groß ist die Distanz zwischen den Servern?
3. An wie vielen Standorten werden Server betrieben?
4. Welche Schnittstellen für Tastatur, Monitor, Maus werden benötigt?
5. Wie hoch ist die maximal benötigte Video-Auflösung?
6. Müssen Audio-Geräte unterstützt werden?
7. Sind virtuelle Maschinen oder Blade-Server in der IT-Umgebung zu finden?
8. Wird ein IP-Zugriff benötigt?
9. Wie viele Benutzer benötigen simultanen Zugriff auf die KVMs?
10. Ist eine eingebaute LCD KVM-Konsole für den lokalen Zugang erforderlich?

Zehn grundlegende Fragen zur Auswahl einer KVM-Lösung





Mit KVM-Systemen haben Administratoren direkten Zugriff auf Server auch über das IP-Netzwerk – doch auf die richtige Auswahl kommt es an

ne Kombination von KVM-Switch und intelligenter Management-Software geleistet wird; wo eine Vielzahl von IP-basierten IT-Geräten zum Einsatz kommt, zu deren Verwaltung und Kontrolle Administratoren den Überblick über alle IP-Adressen aller internetfähigen Geräte behalten müssen, ist dies ein zentrale Notwendigkeit. Intelligente Kontrollsoftware ermöglicht es, sämtliche IP-fähigen KVM-Switches, Gerätekonsolen und Energieverwaltungseinheiten (Power Distribution Units, PDU) über eine Plattform zentral zu verwalten. Gleichzeitig bietet eine softwarebasierte Managementplattform jederzeit und überall Zugriff auf das Equipment des Netzwerks, dies gilt auch für Blade-Server und virtualisierte Maschinen. Alle Geräte lassen sich über nur eine einzige IP-Adresse steuern, konfigurieren und verwalten. Solche intelligente Managementsoftware wird meist in einer Master-Slave-Architektur konzipiert und garantiert eine sichere Datenübertragung durch mehrere Redundanzebenen.

Um das Session-Management in komplexen Netzwerkumgebungen und ein noch sichereres und effizienteres Gerätemanagement zu gewährleisten, sollte eine moderne Verwaltungssoftware mit umfangreichen Funktionen für Multi-Sessions Blade- oder VMware-Server oder PDUs ausgestattet sein. Dabei kann beispielsweise die Stromabgabeleistung je nach Port auf dem Bildschirm kontrolliert werden.

Dabei stellt die Master-Slave-Architektur die Verfügbarkeit der IT-Umgebung sicher. Fällt der Master-Server aus, übernimmt der Slave-Server sämtliche Funk-

tionen und gewährleistet so die Ausfallsicherheit der Systeme. Zusätzliche Features, wie beispielsweise ein Quick Install-Wizard, die erweiterte Suchfunktion für Log-Einträge oder NTS-Unterstützung für die zentrale Zeiteinspeisung, erleichtern die Arbeit des Administrators zusätzlich. Der Datenaustausch erfolgt dabei in Echtzeit oder nach Programmierung. Die aktuellen Sicherheitsstandards schließlich sollten mit IPv6-Support, AES/DES-Verschlüsselung für den Datenexport und OOB-, PAP- und CHAP-Authentifizierung erfüllt werden.

Fazit

Moderne IT-Umgebungen werden nicht zuletzt durch die zunehmende Virtualisierung immer komplexer und heterogener, wobei das eminente Anwachsen der virtuellen Server nicht zu einer Abnahme der physischen Maschinen führt, eher das Gegenteil scheint der Fall. Die Verwaltung, Steuerung und Kontrolle der virtuellen wie physischen Server stellen wachsende Herausforderungen an den Administrator, die bei weiter steigendem Kostenminimierungsdruck besonders abgewogene Entscheidungen für den Einsatz entsprechender Werkzeuge fordern. Moderne KVM-Lösungen bieten eine kostengünstige und zukunftssichere Möglichkeit, die Kontrolle über die IT-Landschaft zu gewährleisten. Voraussetzung für eine befriedigende Implementierung ist eine klare Analyse der bestehenden IT-Umgebung und vernünftige Abschätzung künftigen Bedarfes. (dr)



Marc Salimans ist Vertriebsleiter bei ATEN Belgien.

Windows 8 für Administratoren



- Konzepte und Lösungen für den Einsatz von Windows 8 in Unternehmen
- Automatisiertes Deployment des Betriebssystems
- Gruppenrichtlinien, Sicherheit, Mobilitäts-Features, Virtualisierung u. v. m.

712 S., 2. Auflage 2012, 49,90 €
» www.galileocomputing.de/3261



Linux-Server



- Linux-Server distributions-unabhängig einrichten und administrieren
- Backup, Sicherheit, Samba, LDAP, Webserver, Mailserver, Datenbanken
- Inklusive sofort einsetzbarer Praxislösungen

948 Seiten, 2. Auflage 2012, 49,90 €
» www.galileocomputing.de/3051



LPIC-2



- Vorbereitung auf die Prüfungen 201 und 202
- Kommentierte Testfragen für beide Prüfungen
- Prüfungssimulator mit sofortiger Auswertung

552 S., 2012, mit DVD, 39,90 €
» www.galileocomputing.de/2886



Microsoft Office 365



- Umfassendes Know-how zur Anbindung des Cloud-Dienstes an Ihre IT
- Exchange-, SharePoint- und Lync-Online-Integration
- Single Sign-on mit AD FS, PowerShell-Automation u. v. m.

752 S., 2012, mit Poster, 49,90 €
» www.galileocomputing.de/2908



www.GalileoComputing.de

booksonline

» facebook.com/GalileoPressVerlag

» twitter.com/Galileo_Press

» gplus.to/GalileoPress

AIDA64 Business Edition – die Netzwerklösung

Der schnelle Weg zu mehr Sicherheit!

Noch nie war es so einfach, die Sicherheit und das Management Ihres Netzwerks zu gewährleisten. Unser Angebot an alle IT-Administratoren: Testen Sie die AIDA64 Business Edition kostenlos und völlig unverbindlich. Wir sind uns sicher: Sie werden begeistert sein!

Die AIDA64 Business Edition vereint alle wichtigen Funktionen, die für eine professionelle Netzwerk-Administration notwendig und wünschenswert sind. Mit AIDA64 können Sie blitzschnell eine äußerst genaue Software- und Hardware-Inventur Ihres gesamten Netzwerks erstellen, über die Änderungsmanagement-Funktion erfahren Sie umgehend, ob und was sich in Ihrem Netzwerk verändert hat, sei es im Bereich der Hard- oder Software. Eine enorme Hilfe bei eventueller Fehlersuche.

Mit AIDA64 Business Edition können Sie sämtliche Rechner im Netz auch aus der Ferne verwalten (Remote Desktop Funktion, Prozesse starten oder beenden usw., usw., usw.). Dazu müssen Sie das Programm noch nicht einmal auf allen Rechnern installieren. Es genügt, AIDA64 auf einem zentralen Rechner freizugeben und von dort aus zu starten.

Die Konfiguration lässt sich einfach und effizient durchführen, dabei helfen Ihnen das ZIP-Paket sowie unsere ausführliche **Konfigurationsanleitung**, die Sie beide von unserer Website herunterladen können.

So testen Sie AIDA64 kostenlos und unverbindlich:

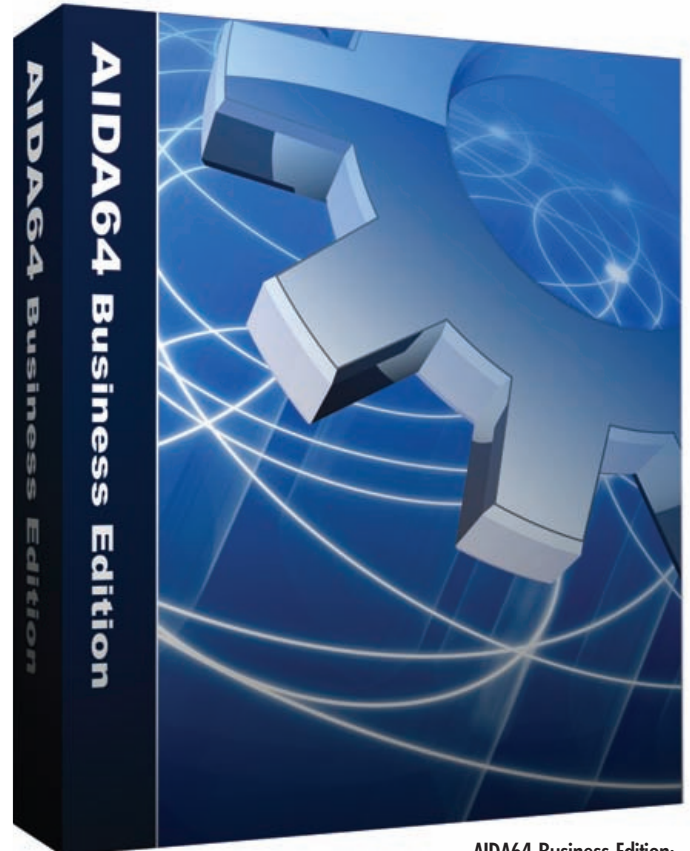
Niemand muss bei uns die Katze im Sack kaufen! Unser Angebot an Sie: Testen Sie AIDA64 Business Edition kostenlos und ohne jegliche weitere Verpflichtung auf Herz und Nieren. Und das ganz ohne irgendeine Funktionseinschränkung! Nehmen Sie bitte über unsere Homepage

www.aida64.de

Kontakt mit uns auf und fordern Sie eine kostenlose, personalisierte Testlizenz an, damit Sie das Produkt mit der gesamten Funktionalität testen können. Das Programm kann auch ohne aktive Internetverbindung aktiviert werden, danach kann es bis zum Ende der Lizenzdauer mit voller Funktionalität benutzt werden und es stehen alle Programmupdates und Aktualisierungen zur Verfügung, diese werden sogar automatisch gesucht und zur Installation angeboten.

Die Aktivierung von AIDA64 Business Edition erfolgt auf einem Netzwerk am Einfachsten über den Domainkontroller. In diesem Fall muss man im Logon-Skript der Clients den Start von AIDA64 Business Edition einfügen. So wird das Programm sofort aktiviert, wenn sich die Clients in der Domain anmelden.

Als ersten Schritt entpacken Sie das ZIP-Paket auf einem Netzlaufwerk, wo alle Clients einen Lesezugriff und Änderungsrechte (NTFS) haben. Zum Beispiel `\\Server\I\Share\AIDA64`. Natürlich kann man auch den Servernamen statt der IP-Adresse verwenden, mit dieser Variante muss man aber nicht einmal auf die Namensauflösung warten. Falls Sie die Berichte auch in das „Share“-Verzeichnis ablegen möchten, müssen auch die entsprechenden Änderungsrechte vergeben werden, ansonsten muss das Verzeichnis nur Leserechte haben. Sie können aber auch eine eigene Freigabe für die Berichte erstellen.



AIDA64 Business Edition:
Volle Kontrolle über jedes Netzwerk!

Unser Tipp: Wenn Sie das Verzeichnis „Share“ als „Share\$“ freigeben, wird dies eine versteckte Freigabe. Das ist deshalb empfehlenswert, weil auf diese Art und Weise keiner Ihrer Client-Anwender die Freigabe bemerkt und somit jeglicher Missbrauch ausgeschlossen ist.

Die AIDA64 Business Edition eignet sich für alle Windows-Netzwerke einschließlich Windows 8 und Windows Server 2012.

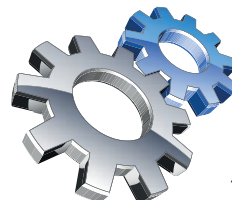
Die Systemanforderungen im Einzelnen

Prozessor: Intel Pentium oder neuer

Arbeitsspeicher: mindestens 32 MB

Festplattenspeicher: 20 MB

Betriebssystem: Windows 95/98/Me, Windows NT4, Windows 2000/XP, Windows PE, Windows Server 2003, Windows Vista, Windows Server 2008/R2, Windows 7/8, Windows Server 2012



AIDA64

Netzwerk-Sicherheit: Vertrauen ist gut, Kontrolle ist besser!



AIDA64

**DIE LÖSUNG FÜR IHR
NETZWERK-MANAGEMENT**

HARDWARE-DIAGNOSE

AIDA64 hat die präzisesten Erkennungsfähigkeiten seiner Klasse und erstellt blitzschnell und lückenlos einen Überblick über die gesamte Hardware jedes PC und damit des gesamten Netzwerks. Streßtests warnen rechtzeitig vor Problemen.

SOFTWARE-ANALYSE

AIDA64 bietet einen Überblick über alle installierten Programme, Software-Lizenzen, die Sicherheit von Anwendungen und Windows-Einstellungen. Dazu eine Liste aller gestarteten Prozesse, Dienste, DL-Dateien, Autostarts und besuchte Web-Sites.

ÜBERWACHUNG

AIDA64 sammelt Informationen über Hard und Software der vernetzten Computer über Kommandozeilen-Automatisierung und speichert die Daten in CSV-, XML-Dateien oder in einer SQL-Datenbank. Dabei meldet AIDA64 jede Veränderung an Hard- und Software.

(FERN-)WARTUNG

Mit der AIDA64-Fernverwaltung überwachen Sie jeden Computer Ihres Netzwerks, egal wo dieser steht. Dabei bietet AIDA64 die volle Kontrolle über den ferngesteuerten PC, um administrative Aufgaben durchzuführen oder Dateien zu übertragen.



DIE NEUE VERSION V2.70 DER AIDA64 BUSINESS EDITION IST AB SOFORT IM HANDEL. AIDA64 BUSINESS EDITION UNTERSTÜTZT ALLE 32- UND 64-BIT WINDOWS-BETRIEBSSYSTEME INKLUSIVE WINDOWS 8 UND WINDOWS SERVER 2012. AIDA64 BUSINESS EDITION - MEHR KOMFORT FÜR IHR NETZWERK-MANAGEMENT GEHT NICHT! WEITERE INFORMATIONEN UNTER WWW.AIDA64.DE



Remotedesktopdienste in Windows Server 2012

Windows aus der Ferne

von Christian Knerrmann

Windows Server 2012 bricht durch das Metro-UI nicht nur radikal mit bisherigen Bedienkonzepten, der neue Server bringt auch in Sachen Remote Desktop deutliche Verbesserungen. So wurde die zentrale Administration mehrerer Terminalserver erleichtert und RDP steht in Version 8 bereit.

Letzteres ist aktuell jedoch auf Windows 8-Clients beschränkt. IT-Administrator zeigt, wie Sie unter Windows Server 2012 die Remotedesktopdienste einrichten, konfigurieren und betreiben.

Bereits mit der Einführung von Windows Server 2008 R2 hatte Microsoft die klassischen Terminaldienste in Remotedesktopdienste (RDS) umbenannt. Der Terminalserver wurde zum Remote Desktop Session Host (RDSH), dem weitere Rollendienste zur Seite gestellt wurden. Der Verbindungsbroker kümmert sich um die Ausfallsicherheit. Web Access sorgt für den Browser-basierten Zugriff auf Desktops und einzelne Applikationen, von Microsoft als RemoteApps bezeichnet, und das Remote Desktop Gateway erlaubt den sicheren Zugriff auch von extern. Der Remote Desktop Virtualization Host (RDVH) ergänzt die herkömmlichen Terminaldienste, bei denen sich mehrere Benutzer ein Server-Betriebssystem teilen, um virtuelle Desktops, also separate Betriebssystem-Instanzen für einzelne Benutzer (siehe Bild 1).

Diese Rollendienste finden sich auch im Windows Server 2012, wobei nach Angaben von Microsoft insbesondere Management und Ausfallsicherheit wesentliche Verbesserungen gegenüber früheren Versionen erfahren haben. So war es in älteren



Quelle: sypher5 - 123RF

Ausgaben des Servers erforderlich, die als RemoteApps freigegebenen Anwendungen pro Server zu konfigurieren. Dies wurde zwar durch eine Import-/Export-Funktion etwas vereinfacht, erübrigte aber leider nicht, jeden Server separat zu betreiben. Ebenso fehlte eine zentrale Übersicht, um die Sitzungen aller Benutzer auf allen Terminalservern und virtuellen Desktops anzuzeigen und zu verwalten. Windows Server 2012 setzt an eben dieser Stelle an und soll den Server-Manager als zentrale Administrationskonsole etablieren, die zusammen mit dem Verbindungsbroker eine Übersicht über sämtliche Terminalserver und Desktops innerhalb einer Infrastruktur bietet. Welche Unterschiede sich gegenüber dem Windows Server 2008 R2 im Bereich der Remotedesktopdienste ergeben, haben wir uns anhand der Vorabversion des Windows Server 2012 bereits angesehen. Dieser Artikel basiert auf den

Erfahrungen aus dem Test der Release Preview von Windows Server 2012 (Build 8400). Einzelne Funktionen könnten in der finalen Version abweichend implementiert sein.

Installation und Konfiguration

Wir installieren für unseren Workshop zwei Server mit dem Ziel, diese als RDSH zu betreiben. Die Basisinstallation verläuft ähnlich, wie Sie es von Windows Server 2008 R2 gewohnt sind. Nachdem die Einstellungen für Sprache, Zeitzone und Tastaturlayout gewählt sind, können Sie sofort mit einem Klick auf die Schaltfläche "Jetzt installieren" beginnen. Im nächsten Schritt ist die gewünschte Variante des Betriebssystems festzulegen. Da die Release Preview grundsätzlich als Datacenter Edition daherkommt, steht hier nur zur Wahl, ob die Core Variante oder die vollständige Installation mit grafischer Be-

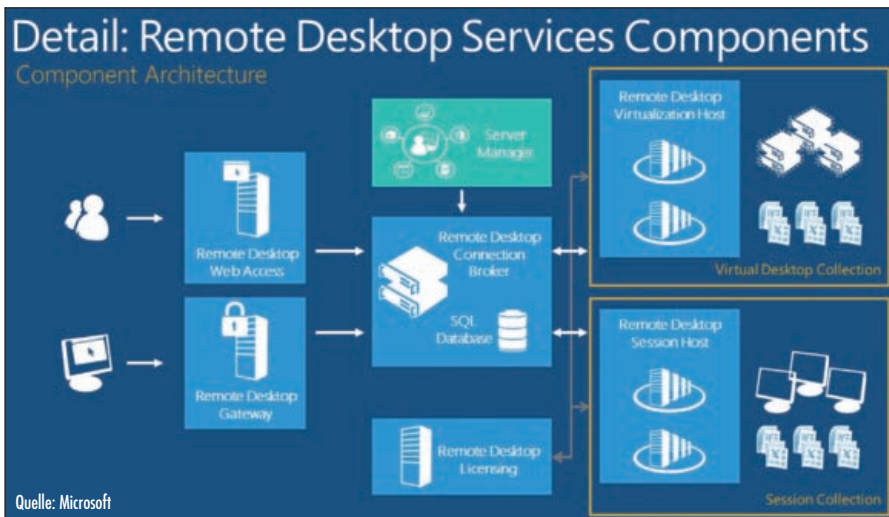


Bild 1: Die RDS sind zu einer kompletten Infrastrukturlösung gewachsen

nutzeroberfläche auf der Platte landen soll. Wir entscheiden uns für letztere Option.

Daraufhin sind noch die Lizenzbestimmungen abzunicken und es steht die Entscheidung zwischen Upgrade und benutzerdefiniertem Setup an. Ist auf den Systemen noch kein vorheriges Windows installiert, ergibt hier nur die zweite Option Sinn. Der Dialog zur Partitionierung der Festplatte funktioniert analog zu dem von Windows 2008 R2 bekannten. Wir entscheiden uns, den gesamten verfügbaren Platz zu verwenden. Es folgt der Installationsprozess und abschließend legen Sie noch das Administrator-Passwort fest.

Nun dürfte Ihnen ein ähnlicher Kulturschock bevorstehen wie auch beim Test der Vorabversionen von Windows 8: Auch der Desktop des Servers präsentiert sich in neuer reduzierter Optik mit eckigen Fenstern ohne Transparenzeffekte, vor allem aber auch ohne Startmenü. Sollen Anwendungen gestartet werden, die nicht bereits mit einer Verknüpfung auf dem Desktop oder in der Taskleiste präsent sind, bringt der Mauszeiger in der rechten unteren Bildschirmcke vom rechten Rand eine Leiste mit drei Optionen zum Vorschein.

Die oberste Option "Suchen" blendet eine Übersicht aller installierten Apps ein mit der Möglichkeit, diese zu durchsuchen, wie Sie es auch vom Suchfeld des Startmenüs unter Windows 7 her kennen. Der mittlere Punkt "Start" bringt die von Windows 8 bekannte Kachel-Optik auf

den Schirm. Hier können die auf dem Startschirm verknüpften Apps aufgerufen werden, was derzeit stets zur Folge hat, dass die entsprechende Anwendung auf dem Desktop gestartet wird. Metro-Apps, wie der in Windows 8 enthaltene Internet Explorer, sind im Server nicht an Bord. Die untere Option "Einstellungen" erlaubt schließlich den Schnellzugriff auf die Systemsteuerung sowie auf weitere systemnahe Einstellungen wie beispielsweise die Netzwerkkonfiguration.

Dies sei jedoch nur erwähnt, um einen ersten Überblick über die Bedienung des neuen Systems zu bieten. Für unser Workshop-Vorhaben, einen Terminalserver aufzusetzen, können wir zunächst auf dem Desktop bleiben, da der neue Server-Manager dort nach der Installation automatisch startet und uns mit einem Assistenten beim weiteren Setup unterstützt. Der anfängliche Schritt besteht darin, das erste unserer Systeme in die Active Directory Domäne aufzunehmen.

Dies ist insbesondere für die Remotedesktopdienste wichtig, da deren Setup mit einer Fehlermeldung abbricht, wenn der Server in einer Arbeitsgruppe ist. Nach dem obligatorischen Neustart installieren Sie sämtliche angebotenen Windows-Updates (vier an der Zahl), denn auch die Release Preview wird von Microsoft bereits mit Updates versorgt. Anschließend können Sie sich dem zweiten Schritt des Konfigurationsassistenten widmen: "Rollen und Features hinzufügen".

Neu ist an dieser Stelle, dass sich im entsprechenden Assistenten neben der Installation von Rollen, Rollendiensten und Features nun der separate Punkt "Installation von Remotedesktopdiensten" findet. Diesen wählen wir und setzen die Einrichtung mit einem Klick auf "Weiter" fort. Im folgenden Dialogschritt begegnet uns in der Release Preview noch eine Mischung aus englischen und deutschen Textbausteinen. Ein "Standard deployment" sieht vor, die verschiedenen Rollendienste der RDS auf mehrere Server zu verteilen, der "Schnellstart" installiert die Remotedesktopdienste mitsamt Verbindungsbroker und Web Access auf einer Maschine. Um uns davon zu überzeugen, ob Microsofts Versprechen der deutlich vereinfachten Bereitstellung hält, versuchen wir es mit dem Schnellstart.

Im nächsten Schritt müssen Sie sich zwischen Desktop-Virtualisierung oder sitzungsbasierter Desktopbereitstellung entscheiden. Da unser Interesse dem klassischen Terminalserver gilt, wählen wir Letzteres. Daraufhin können Sie die Maschine auswählen und im folgenden Dialog mit einem Klick auf "Bereitstellen" die Installation beginnen, nachdem Sie die Checkbox vor der Option "Zielserver bei Bedarf automatisch neu starten" gesetzt haben. Die Installation der Rollendienste erfolgt automatisch, woraufhin der Setup-Assistent beim Erstellen einer Sitzungssammlung einen nicht näher spezifizierten Fehler meldet und somit auch das Veröffentlichen von Remote-Apps abbricht. Sie können diesen Fehler jedoch relativ leicht umgehen, indem Sie im Server-Manager zu den Remotedesktopdiensten wechseln und manuell die Aufgabe "Sitzungssammlungen erstellen" starten.

Assistenten-geführt legen Sie daraufhin einen Namen für die Sammlung fest. Hier wählen Sie zunächst "Windows-Desktop", um eine komplette Desktop-Sitzung bereitzustellen. Im nächsten Schritt wählen Sie Ihren Server aus und legen daraufhin fest, welche Benutzer Zugriff haben sollen. Wir entscheiden uns hier für die Gruppe der Domänen-Benutzer. Weiterhin wird angeboten, die neue Option des Benutzerprofil-Datenträgers zu aktivieren. Es

Worüber Administratoren morgen reden

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

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

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

Jetzt einfach und kostenlos bestellen unter:



www.it-administrator.de/newsletter

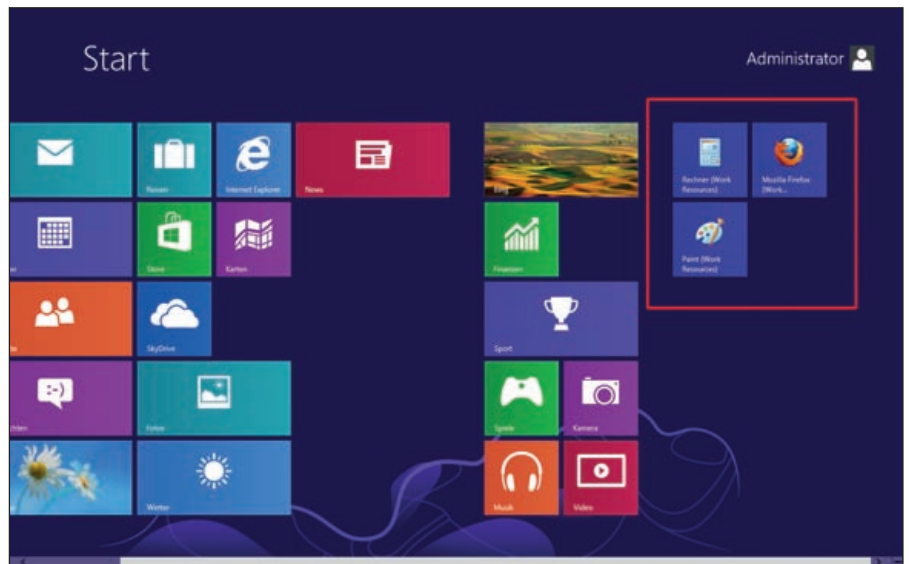


Bild 2: Auch RemoteApps integrieren sich in die Kachel-Optik von Windows 8

handelt sich dabei um eine Alternative zur Ordner-Umleitung mittels Gruppenrichtlinien, die es ermöglichen soll, das Benutzerprofil und frei definierbar weitere Ordner in eine separate Freigabe umzuleiten. Diese Option lassen wir jedoch vorerst unkonfiguriert und schließen das Erstellen der Sammlung ab. Damit sind wir bereits in der Lage, einen Benutzer an der Web Access-Seite unter <https://servername/RDWeb> anzumelden. Dabei ignorieren Sie die Warnung, die das selbstsignierte Zertifikat des Servers im Browser erzeugt. Im Rahmen einer produktiven Implementierung sollten Sie ein solches allerdings durch ein Zertifikat einer anerkannten PKI ersetzen.

Der Web Access bietet optisch keine Überraschungen und präsentiert sich ähnlich der vom Windows Server 2008 R2 bekannten Seite. Die Webseite setzt nun allerdings nicht mehr auf ActiveX und funktioniert somit auch in alternativen Browsern. Nach erfolgreicher Anmeldung wird Ihnen der zuvor erstellte Windows-Desktop angeboten, den Sie nun starten können. Dabei erhalten Sie allerdings umgehend eine Warnmeldung, dass der Terminalserver keine passende Lizenz finden konnte.

Probleme mit älteren Lizenzservern

Die auch unter Windows Server 2012 zwingend erforderliche Remotedesktoplizenzierung installiert der Assistent im

Rahmen des "Schnellstart"-Setups nicht mit und mit einem bereits vorhandenen Lizenzdienst unter Windows Server 2008 R2 möchte der neue Server nicht kommunizieren. Hier gilt nach wie vor, dass die Remotedesktoplizenzierung nicht aufwärtskompatibel ist und mindestens unter dem Betriebssystem laufen muss, das auch der Terminalserver verwendet.

Ein Probebetrieb ist zwar für 120 Tage auch ohne Lizenz-Server möglich. Es ist jedoch zu empfehlen, sich schnellstmöglich um diesen Punkt zu kümmern. Nicht wenigen Administratoren ist es bereits passiert, dass diese Aufgabe in Vergessenheit gerät und dann nach Ablauf der Frist hektisch ausbricht, weil die Terminalserver plötzlich keine Verbindungen mehr akzeptieren.

Das Problem können wir in unserer Beispielumgebung relativ einfach beheben, indem wir im Server-Manager über die "Bereitstellungsübersicht" die RD-Lizenzierung hinzufügen. Hierzu ist lediglich der Zielserver zu wählen, woraufhin der Rollendienst automatisch mit auf dem Terminalserver installiert wird. Anschließend können Sie den Remotedesktoplizenzierungs-Manager starten, den Lizenz-Server online beim Microsoft Clearinghouse aktivieren und anschließend Lizenzen installieren. Dazu ist ein bestehender Vertrag mit Microsoft erforderlich, beispielsweise im Open License- oder Campus-Lizenzmodell.



Nach Angabe Ihrer Vertragsnummer finden Sie in der Auswahlliste der Produktversionen die Server-Betriebssysteme von Windows 2000 Server bis hin zum Windows Server 2012 Release Candidate vor. Als Lizenztyp stehen "Remote Desktop Services Client Access Licenses (RDS-CAL)" pro Benutzer oder pro Endgerät sowie für virtuelle Desktops auch die VDI Suite zur Wahl. Ein Lizenzserver kann unterschiedliche Lizenzpakete hosten, während je Terminalserver zu entscheiden ist, ob dieser Lizenzen pro Gerät oder pro Benutzer verwenden soll. Wir installieren für unseren Workshop zehn "Pro Benutzer"-RDS-CALs. Anschließend gibt der Lizenzserver noch eine Warnung aus, da er der Domänen-Gruppe der "Terminalserver-Lizenzser-

ver" angehören muss, damit er "Pro Benutzer"-Lizenzen ausstellen kann. Dies lässt sich über die Schaltfläche "Zu Gruppe hinzufügen" direkt aus der Konsole heraus bewerkstelligen.

Daraufhin konnten wir uns ohne weitere Warnmeldungen mit dem Desktop des Terminalservers verbinden. Hierzu müssen Sie allerdings beim Verbindungsaufbau erneut die Anmeldeinformationen des Users eingeben, mit dem Sie sich zuvor bereits am Web Access angemeldet haben. Im Zusammenspiel der Server Release Preview mit der finalen Version von Windows 8 (Build 9200) funktioniert der von Microsoft versprochene transparente Single Sign-On [1] nämlich nicht.

RemoteApps bereitstellen

Sofern es sich bei den Endgeräten um vollwertige Arbeitsstationen mit Windows 8 handelt, ist es in der Regel nicht gewünscht, einen kompletten Desktop vom Terminalserver zu verbinden, da zwei verschiedene Desktops die Endanwender eher verwirren. In einem solchen Fall ist es stattdessen gefragt, einzelne Anwendungen als RemoteApp zu veröffentlichen, die sich nahtlos in den Client-Desktop integrieren und so erscheinen, als seien sie lokal installiert. Auf unserem Beispielserver installieren wir zunächst Mozilla Firefox und navigieren dann im Server-Manager innerhalb der Remotedesktopdienste zu unserer Sammlung "Windows-Desktop". Dort können Sie im Bereich "RemoteApp-Programme" die Aktion "RemoteApp-Programme veröffentlichen" ausführen. Dies ist allerdings mit dem Hinweis verbunden, dass innerhalb der Sammlung anschließend nur noch RemoteApps und kein kompletter Desktop mehr bereitgestellt werden.

Im folgenden Dialog wählen Sie aus den auf dem Server vorhandenen Programmen aus und veröffentlichen dabei je nach Bedarf gleich mehrere RemoteApps in einem Schritt. Wir entscheiden uns an dieser Stelle für den zuvor installierten Firefox sowie Paint. Im nächsten Schritt sind die Pfade zu den Programmen zu bestätigen. Sofern der Sammlung mehrere Terminalserver zugeordnet sind, ist sicherzustellen, dass die Programme auf allen Servern im

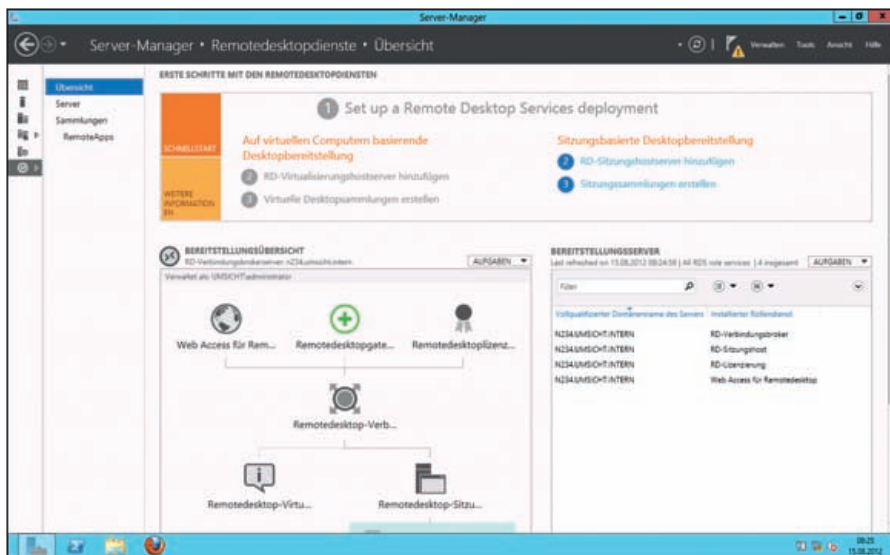


Bild 3: Der Server-Manager erlaubt die zentrale Administration der kompletten Infrastruktur



Und wann kaufen Sie Ihre Server bei uns?



SERVER MEILE

DIE SERVER-FERTIGUNG

- ▶ **Fertigung der neuen Romley Intel Serversysteme mit Sandy Bridge EP Prozessoren und bis zu 768GB DDR3 RAM**
- ▶ **Deutschlandweiter 24h Vor-Ort-Service bis zu 5 Jahren**
- ▶ **Eigenes Rechenzentrum für Server Housing und Managed Server**
- ▶ **Firmen Niederlassungen in Berlin und Schwäbisch Gmünd**

Server online konfigurieren unter <http://www.servermeile.com> und PDF Angebot ausdrucken

Telefonischer Kontakt: **030 – 2000 50 500**





gleichen Pfad zu finden sind. Damit ist die Veröffentlichung der RemoteApps bereits erledigt. An Stelle des Windows-Desktops finden wir im Web Access bei der nächsten Anmeldung entsprechend die beiden Anwendungen vor. Passend zur geänderten Konfiguration benennen wir unsere Sammlung von "Windows-Desktops" in "RemoteApps" um.

Über den Eigenschaften-Dialog können Sie pro RemoteApp anschließend detailliertere Einstellungen vornehmen. Dies betrifft die Fragen, ob die App im Web Access angezeigt werden soll und ob sie dort in einen definierbaren Unterordner einsortiert wird. Weiterhin können dort bei Bedarf Befehlszeilenparameter zugelassen werden. Auch ist pro App möglich, den Zugriff auf Gruppen oder Benutzer einzuschränken. Zu guter Letzt kann die Dateitypenzuordnung aktiviert werden. Dies ist hilfreich für Programme, die ausschließlich per Terminalserver bereitgestellt werden und nicht auf den Clients installiert sind. In diesem Fall lassen sich Client-seitig die Dateieinstellungen mit der RemoteApp auf dem Terminalserver verknüpfen. Klickt ein Anwender beispielsweise auf eine entsprechende Datei, so wird diese automatisch in der passenden Applikation auf dem Terminalserver geöffnet. Damit dies funktioniert, muss der Client-Computer allerdings via RSS-Feed auf die Ressourcen des Terminalservers zugreifen.

Die Variante "RSS-Feed" findet sich in der Systemsteuerung von Windows 7 und Windows 8 Clients unter dem Punkt "RemoteApp- und Desktopverbindungen". Im entsprechenden Dialog starten Sie in der linken Fensterhälfte die Aktion "Auf RemoteApp und Desktops zugreifen" und geben im folgenden Fenster den Pfad "https://servername/RDWeb/Feed/webfeed.aspx" ein. Da-

Installation und Verwaltung der Remotedesktopdienste sind mittels PowerShell weiter automatisierbar. Über ein entsprechendes PowerShell Modul [2] können Sie die RDS-Infrastruktur weitestgehend per Kommandozeile beziehungsweise per Skript bedienen.

RDS via PowerShell



raufhin können Sie die Verbindung einrichten. Entsprechend zeigt das System in der Systemsteuerung die Verbindung als aktuell an und es werden die Serverseitig konfigurierten RemoteApps eingerichtet. Diese finden sich anschließend automatisch neben den lokal installierten Anwendungen auf dem Start-Bildschirm wieder (siehe Bild 2).

Damit dies alles im Probebetrieb übrigens mit einem selbstsignierten Server-Zertifikat funktioniert, muss das Zertifikat zuvor in den Zertifikat-Speicher des Clients importiert werden, da ansonsten die Verbindung fehlschlägt.

Einfacher Aufbau einer RDSH-Farm

Dass die Bereitstellung einer Terminalserver-Infrastruktur mit dem Windows Server 2012 tatsächlich deutlich einfacher geworden ist, stellen Sie fest, wenn Sie Ihre Umgebung um einen weiteren Server erweitern möchten. Dies lässt sich bewerkstelligen, ohne auf dem zweiten Server lokal aktiv zu werden. Dazu rufen Sie aus dem Server-Manager des ersten Systems (siehe Bild 3) unter "Sitzungsbasierte Desktopbereitstellung" die Aktion "RD-Sitzungshostserver hinzufügen" auf und wählen im folgenden Dialog den zweiten Server aus. Anschließend müssen Sie lediglich bestätigen, dass das Zielsystem bei Bedarf neu gestartet werden darf. Den Rest erledigt der Assistent vollautomatisch – die RDSH-Rolle wird installiert und dem Verbindungsbroker-Verbund hinzugefügt.

Neben der vereinfachten Installation stellt sich hier eine weitere wesentliche Verbesserung heraus: RemoteApps werden nicht mehr pro Server, sondern pro Sammlung definiert. Eine Sammlung dient dabei als Organisationseinheit, die wiederum beliebig viele Terminalserver enthält. Einstellungen, die ehemals pro Server vorzunehmen waren, lassen sich nun zentral für sämtliche Server in der Sammlung vorgeben. Dies betrifft beispielsweise die Einstellungen zum Trennen und Wiederverbinden von Sitzungen oder auch die Client-Ressourcen wie die Umleitung von Laufwerken oder der Zwischenablage.

Die RDS sind darüber hinaus unter Windows Server 2012 nun auch vollständig per Gruppenrichtlinien konfigurierbar. Somit verwalten Sie auch eine größere Anzahl von Terminalservern bequem zentral. Die Lastverteilung der Sessions erledigt der Verbindungsbroker. Dabei werden Sie automatisch bei Verbindungsaufbau immer zum Terminalserver mit der geringsten Auslastung basierend auf der Anzahl der aktiven Sitzungen geleitet. Welche Sessions auf welchem Server aktiv sind, überblicken Sie komfortabel in einer zentralen Ansicht und können einzelne Sessions aus dieser Ansicht heraus auch trennen oder abmelden.

Im Umkehrschluss bedeutet dies allerdings auch, dass es Ihnen als Administrator nicht mehr ohne Weiteres möglich ist, sich zu Wartungszwecken gezielt mit einem der Terminalserver zu verbinden. Selbst wenn Sie eine RDP-Verbindung auf die IP-Adresse eines bestimmten Servers versuchen, nimmt dieser zunächst Kontakt zum Verbindungsbroker auf und leitet Sie zum anderen Server um, falls dessen Auslastung gerade niedriger ist. Um den Server dennoch administrieren zu können, müssen Sie explizit die Verbindung zur Konsole des Servers aufbauen. Dies lässt sich erreichen, indem Sie die Remotedesktopverbindung mit folgendem Befehl über die Kommandozeile starten:

```
mstsc.exe /v:servername/admin
```

Verbindungsbroker als Schnittstelle

Sind mehrere Terminalserver in einer Farm präsent, kommt dem Verbindungsbroker

- [1] Single Sign-On unter Server 2012
CBP11
- [2] PowerShell-Modul für RDS
CBP12
- [3] RD Connection Broker-Hochverfügbarkeit
CBP13
- [4] RemoteFX-Anpassungen unter Server 2012 und Windows 8
CBP14
- [5] Anpassung der Grafikleistung bei RemoteFX
CBP15

Link-Codes





broker besondere Bedeutung zu. Noch unter Windows Server 2008 R2 war der Verbindungsbroker eher umständlich einzurichten und zudem ein Single Point of Failure. Beim Ausfall des Brokers war das Wiederverbinden getrennter Sitzungen nicht mehr möglich und die Lastverteilung erfolgte lediglich noch per DNS Round-Robin, ohne auf die tatsächliche Auslastung der Server Rücksicht zu nehmen. Unter Windows Server 2012 ist die Verankerung im DNS nicht mehr nötig. Lastverteilung und Ausfallsicherheit sind quasi ab Werk eingebaut, benötigen aber nichtsdestotrotz den Rollendienst des Verbindungsbrokers.

Dieser sollte in produktiven Umgebungen nicht wie in unserer Beispielumgebung mit auf einem RDSH, sondern als separates System installiert werden. Um die Ausfallsicherheit zu gewährleisten, können mehrere Verbindungsbroker als Aktiv-/Aktiv-Cluster betrieben werden. Dies setzt allerdings wiederum mindestens einen SQL Server 2008 R2 voraus, der seinerseits ebenfalls als Cluster ausgelegt sein sollte. Eine solche Umgebung ist entsprechend komplex im Aufbau [3], allerdings nicht nur redundant, sondern auch skalierbar, sodass sich der Aufwand für größere Produktivumgebungen durchaus lohnt.

Vielversprechender Rollendienst

Den Rollendienst des RVDH haben wir nicht selbst erprobt, da dies den Zeitrahmen unseres Workshops gesprengt hätte. Die

Desktop-Virtualisierung auf Basis eines oder mehrerer RVDH verspricht jedoch, ähnlich einfach einzurichten zu sein. Wird ein Host zum RVDH bestimmt, so schiebt der Setup-Assistent dem Server automatisch den Typ-1-Hypervisor Hyper-V 3.0 unter, der anschließend als Plattform für virtuelle Desktops dient und ebenso wie die RDSH unter die Kontrolle der zentralen Administrationskonsole wandert.

Auch das Remote Desktop-Protokoll (RDP) hat in der neuen Version 8.0 einige Verbesserungen erfahren. Um der steigenden Bedeutung von Tablets gerecht zu werden, ist das Protokoll für die Multi-Touch-Bedienung optimiert und der neue Client bringt mit dem "Touch Pointer" ein virtuelles Track-Pad mit, wie man es in ähnlicher Weise bereits von iOS- und Android-Clients von Herstellern wie Citrix, VMware und WYSE kennt. Das bedeutet, auch im Tablet-Betrieb wird in einer Remote-Sitzung ein Cursor eingeblendet, der sich über Gesten auf dem Touch-Screen verschieben lässt. RDP 8.0 soll nun automatisch die Darstellungsqualität an die verfügbare Bandbreite und weitere Rahmenbedingungen anpassen [4] und dabei insbesondere Grafiken und Text separat behandeln, so dass Text immer scharf dargestellt wird und nur Grafiken gegebenenfalls mehrstufig aufgebaut werden, wenn die Bandbreite dies erfordern sollte [5].

Sofern Server-seitig keine spezielle Grafik-Hardware vorhanden ist, greifen Ter-

minalserver und virtuelle Desktops auf eine virtuelle Grafikkarte zurück, die eine DirectX 11-fähige GPU emuliert, was natürlich zu Lasten der physischen CPU geht. Grundlegende 3D-Darstellungen sind auf diesem Wege jedoch möglich. Um höheren Ansprüchen zu genügen, insbesondere für 3D-Grafik-intensive Applikationen, kann auf die RemoteFX vGPU zurückgegriffen werden. Dabei handelt es sich um eine ebenfalls virtualisierte, jedoch Hardware-beschleunigte DirectX 11-fähige GPU für den VDI-Einsatz. Die RemoteFX vGPU setzt allerdings voraus, dass eine physische DirectX 11 GPU im Virtualisierungshost verbaut ist.

Fazit

Die RDS im neuen Server-Betriebssystem von Microsoft haben signifikante Optimierungen erfahren. Die mangelnden Möglichkeiten zentraler Installation und Administration wurden wesentlich verbessert, sodass nun der Überblick auch über mehrere Terminalserver einfacher gelingt. Sämtliche Vorteile der neuen Plattform, insbesondere die Neuerungen in RDP, lassen sich jedoch nur nutzen, wenn sowohl Server als auch Client RDP 8.0 sprechen. Aktuell setzt dies auf dem Client Windows 8 voraus. Somit bleibt abzuwarten, wie dieses Betriebssystem im Unternehmensumfeld angenommen wird und inwieweit RDP 8.0 beispielsweise in Thin Clients und auf anderen (Tablet)-Betriebssystemen Einzug hält. (dr)



IGEL'S NEUER SYSTEM-ON-CHIP THIN CLIENT UD2-LX MULTIMEDIA

Geballte Power für Citrix HDX und
Microsoft RemoteFX

Perfekte Ausstattung bei minimalen Maßen:

- ▶ Multiprotokoll System-on-Chip (SoC)-Device
- ▶ Performante Multimediabeschleunigung für Citrix® HDX™ und Microsoft® RemoteFX™
- ▶ Jetzt schon in der Thin Client-Einstiegsklasse Full-HD Videos abspielen
- ▶ Hervorragendes Preis-/Leistungsverhältnis
- ▶ Intelligente Remote Management Software – IGEL Universal Management Suite (UMS)



Fordern Sie jetzt Ihre kostenlose Teststellung an:
www.igel.com/de/testen

IGEL Technology – Thin Client Software & Hardware





Neues in Exchange Server 2013

Kommunikativ und sicher

von Christian Schulenburg



Nach drei Jahren Pause ist die Aktualisierung nahezu aller Microsoft-Serverprodukte in vollem Gange. Nach SQL Server 2012, Windows Server 2012 und System Center 2012 steht nun das neue Office 2013 an. Neben Lync, SharePoint und Office gehört auch Exchange Server 2013 dazu. Unser Beitrag wirft einen Blick auf die wichtigsten Neuerungen in der Exchange-Preview. Auch wenn es noch die eine oder andere Änderung bis zur finalen Fassung geben mag, zeichnet sich bereits deutlich ab, was der neue Server alles zu bieten hat.

Seit Exchange 2007 hat Microsoft auf ein Konzept bestehend aus den fünf Rollen Mailbox, Client-Access, Hub-Transport, Unified Messaging und Edge gesetzt. Dies sollte vor allem der besseren Skalierbarkeit und der Sicherheit dienen. Exchange Server 2013 bricht mit diesem Konzept und verteilt die Rollen Unified-Messaging / Hub-Transport auf die Rollen Mailbox und Client-Access. Die Mailbox-Rolle übernimmt dabei alle aktiven Komponenten, die auf die Mailbox zugreifen, während sich die Rolle Client-Access (CAS) nur noch um die Authentifizierung sowie das Redirect und das Proxying der verschiedenen Dienste kümmert. Es entspricht einer Frontend-Backuptopologie, bei der der vorgelagerte CAS weder Daten rendert noch Daten in Queues zwischenspeichert.

Die Mailbox-Rolle ist dann unter anderem für den klassischen Zugriff auf die Mailbox, das OWA-Rendering und die Unified Messaging-Funktionalität zuständig. Ziel ist es, die Installationen zu vereinfachen, Updateprozesse zu optimieren und mehr Flexibilität bei der Rollenverteilung zu ermöglichen. Was mit den

Edge-Servern passiert, lässt Microsoft bisher offen. Exchange 2013 unterstützt den Exchange 2010 Edge bisher im vollen Umfang. Ein Update der Edge-Rolle ist mit SP1 zu erwarten.

Ändern wird sich auch der Zugriff zwischen den Servern und den Clients. RPC over HTTP ist bereits weit verbreitet, doch ist RPC over TCP oft weiter aktiv. Mit dem neuen CAS werden nur einfache und statusfreie Protokolle unterstützt, wodurch RPC over TCP als Zugriffsprotokoll entfällt. Outlook nutzt zwingend RPC over HTTP und es werden nur noch Clients ab Outlook 2007 unterstützt. Infolge kann das Routing auf Load Balancern auch auf Layer 4 erfolgen und auch DNS-Round Robin wird zukünftig zur CAS-Ausfallsicherheit unterstützt. Ein Hardware-Load-Balancer ist aber auch weiterhin zu empfehlen.

Exchange unter Kontrolle

Nach der Installation suchen Sie zunächst vergebens nach einer Konfigurationsoberfläche, denn im Windows-Startmenü sind nur die Exchange Management Shell und die Toolbox zu finden. Der Weg zur Administration führt zukünftig über den Browser und das Exchange Administration Center (EAC).

Aufrufen können Sie die neue Konsole über <https://servername/ecp>. Das neue Center ersetzt die Exchange Management Console (EMC) sowie das Exchange Control Panel (ECP) und ermöglicht eine zentrale Administration über das Intranet oder das Internet. Das EAC macht im Gegensatz zu den vorhergehenden Konsolen, die noch auf die MMC aufbauten, einen sehr schlanken und schnellen Eindruck. Durch den Technologiewechsel gehören Startschwierigkeiten und WinRM-Fehler der Vergangenheit an. EAC unterstützt alle gängigen Browser. Kompatibilitätsprobleme wie etwa bei Einführung des Internet Explorer 9 sollten der Vergangenheit angehören. Microsoft nutzt ferner die Erfahrungen mit Office 365, das über ein ähnliches Interface administriert wird. Eine Übersicht aller gängigen Browser finden Sie unter [1].

Praktisch ist der Export von Listen, der es beispielsweise ermöglicht, Übersichten aller Mailboxen zu generieren. Auch wurde die Role Based Access Control (RBAC) in das EAC aufgenommen, wodurch ein schnelles Vergeben von angepassten Rechten möglich ist. Administratoren mit angepassten Rechten melden sich ebenfalls über das EAC an, erhalten aber nur ein angepasstes Menü, für das sie die entspre-



Bild 1: Der Aufbau des Exchange Administration Centers ist klar strukturiert

chenden Berechtigungen besitzen. In der EMC wurden bisher immer alle Funktionen angezeigt, was des Öfteren zu Fehlermeldungen führte, wenn ein Zugriff nicht möglich war.

Wie erwähnt ist die Exchange-Management-Shell weiterhin ein wichtiger Bestandteil der Administration. Der Befehlsumfang hat sich um zirka 200 Kommandos erweitert, während 13 Befehle weggefallen sind. Vor allem im Bereich der Öffentlichen Ordner hat sich viel verändert und auch für die neuen Funktionen kommen einige Cmdlets dazu. Die Powershell wird nun in Version 3 unterstützt. Dadurch vereinfacht sich die Syntax weiter und es kommen einige Features wie Tasks hinzu:

```
Get-Command -Module PSScheduledJob |
Sort-Object Noun, Verb
```

Wer Kommandos aufeinander aufbauen lässt, kommt künftig einfacher voran. So verkürzt sich etwa die Syntax zum Suchen eines Namens von

```
Get-Mailbox | where {$_.Name -like
"*Chris*"}
auf
```

```
Get-Mailbox | where name -like
"*Chris*"
```

Mehr Informationen zur neuen Powershell finden Sie unter [2].

Nachdem Sie sich an die neue Struktur und das Design gewöhnt haben, dürften Sie nur die PowerShell Learning-Erweiterung und die rechte Maustaste vermissen. Die kontextbasierten Menüs über die rechte Maustaste hat Microsoft im EAC bisher nicht implementiert. Dass dies prinzipiell möglich ist, zeigt das neue OWA 2013, bei dem Sie verschiedene Aktionen über die rechte Maustaste auslösen können. Die Überführung der Funktion in das EAC sollte nur ein kleiner Schritt sein, der in einem kommenden Service-Pack hoffentlich berücksichtigt wird. Ein weiteres Feature, das zu einem späteren Zeitpunkt auch den Weg zurück in die Verwaltung finden sollte, ist die PowerShell Learning-Erweiterung. Mit der Funktion wurde Ihnen der Befehl zu einer EMC-Aktion aufgezeigt, was vor allem das Know-how über die Cmdlets nebenbei erweiterte.

Wiedergeburt der Öffentlichen Ordner

Das Ende der Öffentlichen Ordner wurde nach Exchange 2007 oft vorausgesagt. Doch der Protest gegenüber Microsoft war anscheinend groß genug, um sie zu erhalten. Zunächst schafften es die Öffentlichen Ordner ohne GUI-Verwaltung in die erste Version von Exchange 2010. Mit Service Pack 1 für Exchange 2010 reichte Microsoft dann die Öffentliche Ordner-Verwaltung über die GUI nach. In Exchange 2013 sind die Öffentlichen Ordner dabei und sie werden uns wohl nach den Veränderungen auch länger erhalten bleiben. Das Konzept wurde komplett überarbeitet

und der Inhalt wird jetzt in speziellen Öffentlichen Ordner-Postfächern abgelegt. Öffentliche Ordner-Datenbanken gehören damit der Vergangenheit an und auf die Replikation zwischen verschiedenen Datenbanken wird künftig verzichtet. Unterschiedliche Versionsstände und Probleme bei der Replikation, die vor allem bei Migrationen oft zu Problemen führten, sind damit obsolet geworden. Durch das neue Design nutzen Öffentliche Ordner fortan die DAG-Architektur. Die Nutzung verteilter Strukturen über verschiedene Sites wird jedoch erschwert.

Bei den neuen Postfächern wird zwischen einem beschreibbaren Master Hierarchie-Postfach, das die Struktur hält, und den reinen Öffentliche-Ordner-Postfächern, die den Inhalt führen, unterschieden. Bei dem Master Hierarchie-Postfach handelt es sich standardmäßig um das erste Öffentliche-Ordner-Postfach. Alle weiteren Postfächer enthalten eine Kopie der Hierarchie. Der Inhalt der Öffentlichen Ordner verteilt sich über die verschiedenen Inhaltspostfächer. Der Technologiewandel erschwert allerdings die Migration auf den neuen Server. So müssen Sie die Struktur zunächst über eine CSV-Datei portieren, bevor ein Abgleich zu den neuen Öffentlichen Ordnern stattfindet. Für die Migration müssen sich die User bereits auf Exchange 2013 befinden, da Exchange 2013 auf Öffentliche Ordner unter Exchange 2010 zugreifen kann, aber nicht umgekehrt.

OWA jetzt offline

Outlook Web App hat sich dem Kachel-Design (Modern UI Style, vormals Metro) angepasst und kommt in der Preview sehr einfach daher. Die neue Oberfläche gleicht noch stärker der lokalen Offline-Version Outlook 2013, sodass eine Umstellung für User in der neuen Version sehr einfach ist. OWA unterstützt die drei Standardgeräteklassen (Desktop, Tablet und Mobile), für die automatisch drei verschiedene Layouts geladen werden. Outlook Mobile Access, das erst mit Exchange 2010 SP2 dazugekommen ist, gehört damit wieder der Vergangenheit an.

Eine der größten Änderungen in OWA ist die Offline-Verfügbarkeit. Dabei wird das Postfach über den Browser gecached, sodass



Bild 2: OWA 2013 bringt ein für jeden Gerätetyp angepasstes Layout

auch ohne Zugriff auf das Firmennetzwerk ein Arbeiten möglich ist. Diese Funktion lässt sich mit dem Internet Explorer 10, aber auch mit Safari 5.1 und Chrome 18 nutzen. In diesen Versionen aktivieren Nutzer die Funktion oben rechts und nach einer kurzen Synchronisation lässt sich das Postfach auch offline nutzen. Eine Übersicht zu den nutzbaren Browsern finden Sie unter [3].

Mailbox für SharePoint

Öffentliche Ordner wurden nicht in SharePoint überführt, aber dennoch rücken Exchange und SharePoint über die Site Mailbox näher zusammen. Dabei ist ein Zugriff direkt auf SharePoint 2013 über Outlook-Clients möglich. Die SharePoint-Site wird ähnlich einem zusätzlichen Postfach in der Baumstruktur angezeigt. Ziel ist es, verschiedene projekt-bezogene Daten zusammenzufassen und sowohl Dokumente als auch E-Mails zentral zu verwalten. Der Zugriff erfolgt dabei über

Outlook oder die SharePoint-Website. Voraussetzung sind neben der aktuellen Exchange-Version die aktuelle SharePoint-Version 2013 und der aktuelle Outlook-Client 2013. Durch die umfangreichen Voraussetzungen dürfte es allerdings noch etwas dauern, bis die neue Funktion im produktiven Einsatz zu finden ist.

Auch den Store-Prozess hat Microsoft komplett neu geschrieben. Jede Datenbank läuft nun in einem eigenen Prozess, wodurch der Absturz einer Datenbank andere Datenbanken nicht zwingend in Mitleidenschaft zieht. Durch den Entwicklungsprozess und die Optimierung wurde die I/O-Last weiter optimiert und auch die Größe der unterstützten Postfachgröße nimmt auf 100 GByte zu. Microsoft spricht von einer Reduzierung der IP-Last um 95 Prozent gegenüber Exchange 2003. Nachdem sich die FAST-Suche bereits bei SharePoint bewährt hat, findet sie nun Einzug in den Exchange Server. Das gelegentliche Zurücksetzen des Suchindexes gehört damit hoffentlich der Vergangenheit an.

Ein Auge auf sensible Daten

Eine weitere erwähnenswerte Funktion ist die Data Leak Prevention (DLP). Microsoft macht sich auch um den Umgang sensibler Daten wie Kreditkarten Gedanken. In Produkten wie Forefront wurde es bereits hinzugefügt und Exchange zieht nun nach. Die Funktion filtert den Emailverkehr auf bestimmte Wörter. Bis zum RTM soll es vordefinierte DLP-Pakete geben, die eine branchenbezogene Regelsammlung ent-

halten und die Erstellung von Regelsammlungen erleichtern. Bevor der Benutzer eine E-Mail sendet, erhält er eine Information direkt in Outlook 2013 über "Mail-Tips". Das Ergebnis einer Regelverletzung wird weiterhin ins Nachrichtentracking geschrieben. Eine Verletzung lässt sich dadurch schnell erkennen und im Nachhinein nachvollziehen. Gerade die Nachvollziehbarkeit von Verletzungen war mit angepassten Transportagenten immer ein schwieriger Weg. Den Abfluss auf anderem Wege verhindert DLP nicht, sodass das Thema Rights Management Service auch weiterhin eine wichtige Rolle spielt.

Testinstallation aufbauen

Sollten Sie nun Lust bekommen haben sich Exchange 2013 näher anzuschauen, können Sie sich die aktuelle Version unter [4] herunterladen. Die Installation in eine vorhandene Exchange-Struktur ist zurzeit nicht möglich. Hierfür sind noch Anpassungen in der vorhandenen Umgebung nötig, die über das Exchange 2010 Service-Pack 3 nachgeholt werden. Auch für das Upgrade von Exchange 2007 wird es ein Update geben, das zusammen mit dem Service-Pack kurz nach mit der RTM von Exchange 2013 erscheint. Ein Inplace-Upgrade wird auch in Exchange 2013 nicht möglich sein. Weiterhin wird die Organisation Exchange 2003 nach dem Upgrade nicht mehr supportet. So ist von Exchange 2003 kein direkter Mailbox-Move möglich und die Migration muss über den Zwischenschritt Exchange 2007/2010 gehen. Eine Übersicht über die Voraussetzungen ist unter [5] zu finden.

Fazit

Der erste Blick auf die neue Exchange-Version bietet zahlreiche interessante Neuerungen, die Lust auf mehr machen. Gerade im Design der Rollen, der Administration und den Öffentlichen Ordnern fallen die Änderungen sehr gravierend aus. War das große Thema bei Exchange 2010 die Hochverfügbarkeit, die auch Mittelständlern den einfachen Einstieg in HA ermöglichte, fehlt zumindestens beim Einsatz von Exchange 2010 ein zwingender Migrationsgrund. Sofern Sie noch eine ältere Exchange-Version im Einsatz haben, empfiehlt sich das Technologieupgrade im Rahmen des Life-Cycles. (dr)



- [1] Office 365-fähige Browser
CAP11
- [2] Informationen zu PowerShell 3.0
CAP12
- [3] OWA-fähige Browser
CAP13
- [4] Exchange 2013 Trial
CAP14
- [5] Voraussetzungen für Exchange 2013
CAP15

Link-Codes





Bestellen Sie jetzt das IT-Administrator Sonderheft II/2012!

180 Seiten Praxis-Know-how rund um das Thema

Virtualisierung

Betrieb und Management
virtualisierter Infrastrukturen

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

* IT-Administrator Abonnenten erhalten das Sonderheft II/2012 für € 24,90. Nichtabonnenten zahlen € 29,90.
Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

IT-Administrator
Das Magazin für professionelle System- und Netzwerkadministration

Einfach kopieren und per Fax an den Leserservice IT-Administrator senden: 06123/9238-252

Ja, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft II/2012 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

Ja, ich bestelle das IT-Administrator Sonderheft II/2012 zum Preis von **€ 29,90** inkl. Versand und 7% MwSt.

Der Verlag gewährt mir ein Widerrufsrecht. Ich kann meine Bestellung innerhalb von 14 Tagen nach Bestelldatum ohne Angaben von Gründen widerrufen.*

Ich zahle per Bankeinzug

Firma: _____

Geldinstitut: _____

Name, Vorname: _____

Kto.: _____ BLZ: _____

Straße: _____

oder per Rechnung

Land, PLZ, Ort: _____

Datum: _____

Tel: _____

Unterschrift: _____

E-Mail: _____

* Zur Fristwahrung genügt die rechtzeitige Absendung einer E-Mail an leserservice@it-administrator.de oder einer kurzen postalischen Mitteilung an Leserservice IT-Administrator, 65341 Etlville.

So erreichen Sie unseren
Vertrieb, Abo- und
Leserservice:

Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Etlville

Tel: 06123/9238-251
Fax: 06123/9238-252

leserservice@it-administrator.de

Diese und weitere Aboangebote
finden Sie auch im Internet
unter www.it-administrator.de



H
Heinemann Verlag

Leopoldstraße 85
D-80802 München
Tel: 089-4445408-0
Fax: 089-4445408-99

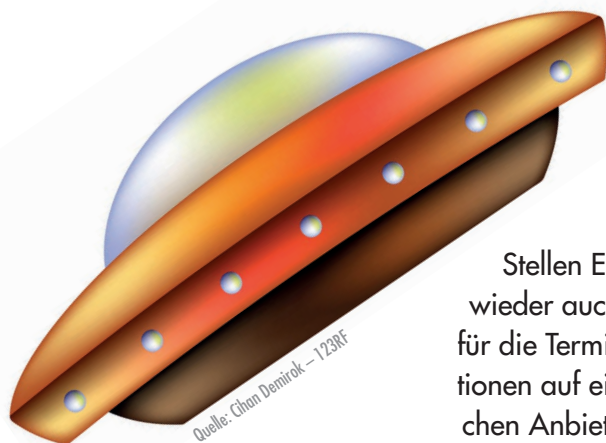
Geschäftsführung:
Anne Kathrin Heinemann
Matthias Heinemann

Amtsgericht München HRB 151585

ITA 1212

Konfiguration und Betrieb von ThinLinc Terminaldienste der dritten Art

von Dr. Holger Reibold



In Zeiten klammer Kassen loten Unternehmen aus, an welchen Stellen Einsparpotenziale ungenutzt brachliegen. Dabei erleben immer wieder auch längst vergessene Techniken eine Renaissance. Das gilt etwa für die Terminal Services, bei denen die gesamte Ausführung der Applikationen auf einen Terminalserver verlegt wird. Wer dabei nicht auf die üblichen Anbieter setzen möchte, sollte einen Blick auf ThinLinc werfen. Unser Workshop erklärt, wie Sie den zentralen Terminalserver in Betrieb nehmen.

Auf der Website des Entwicklers Cendio finden Sie die verschiedenen Downloads [1], die Sie einer ausgiebigen Evaluierung unterziehen können. Für ein Open Source-basiertes Projekt ist ThinLinc ausgesprochen gut dokumentiert. ThinLinc nutzt zwar etablierte freie Werkzeuge, ist selbst aber ein kommerzielles Produkt, bei dem die Entwickler ihren Kunden insbesondere mit Support zur Seite stehen. Die Preisgestaltung ist moderat: Für zehn User fallen bei einem zwölfmonatigen Engagement 65 Euro pro User an, ab 100 User sind es 40 Euro pro Nutzer.

ThinLinc im Überblick

Die Lösung sollte laut Angaben der Entwickler vorzugsweise auf einem Red Hat Enterprise Server, auf Ubuntu oder SuSE Enterprise ausgeführt werden. Die Umgebung basiert auf zwei zentralen Komponenten: dem ThinLinc Master und dem ThinLinc Agent. Beide lassen sich bei kleineren Umgebungen auf dem gleichen Server unterbringen, bei größeren Landschaften empfiehlt sich jedoch die Verteilung auf mehrere Systeme.

In Business-kritischen Infrastrukturen ist meist Hochverfügbarkeit gefragt. Um diese

Anforderung zu erfüllen, haben die ThinLinc-Entwickler einen speziellen Mechanismus entwickelt, der im Falle des Ausfalls eines aktiven ThinLinc-Servers die Sessions automatisch an einen Ausfallserver übergibt. So ist die Verfügbarkeit bei Updates oder dem Austausch beziehungsweise Ausfall von kritischen Komponenten sichergestellt.

Für die Desktop-Virtualisierung mit ThinLinc stehen Ihnen spezielle Clients für die drei wichtigsten Desktop-Plattformen zur Verfügung: Linux, Mac OS X und Windows. Außerdem ist der Zugriff über einen Webbrowser möglich. Dabei ist die Virtualisierung von aufwändigen grafischen Applikationen wie CAD, aber auch Bild-

und Videobearbeitung möglich. ThinLinc macht sich dabei die VNC-Implementierung TigerVNC zu Nutze.

Im Unterschied zu Microsoft, das bei seinem Terminalserver in erster Linie auf RDP für die Client-Server-Kommunikation setzt, verwendet ThinLinc das sichere SSH-Protokoll. Der Terminal Service setzt auf etablierte Open Source-Lösungen und unterstützt verschiedene Authentifizierungsmechanismen wie beispielsweise Smartcards. Für Unternehmen ist bei der Evaluierung von neuen Lösungen stets relevant, wie sie sich in eine bestehende IT-Infrastruktur einfügen beziehungsweise diese integrieren. Auch hier ist ThinLinc gut vorbereitet, denn Sie können etwa



Bild 1: Der Remote-Zugriff mit dem ThinLinc-Client erfolgt nicht über RDP, sondern SSH



Active Directory- und eDirectory-Services, RADIUS und File-Server einbinden.

Auf Seiten der Remote-Clients können die Linux-Desktop-Virtualisierung und ein Windows-Betriebssystem parallel ausgeführt werden. Für die Clients ist es möglich, unterschiedliche Desktop-Umgebungen anzulegen, die auf die speziellen Anforderungen bestimmter Benutzergruppen ausgerichtet sind. Mit dem ThinLinc Client Operation System, kurz TLCOS, haben die Entwickler außerdem ein spezielles System geschaffen, das einen älteren Desktop-Rechner in einen dezierten Thin Client verwandelt.

Aufbau einer ThinLinc-Session

Für den Betrieb einer ThinLinc-Umgebung benötigen Sie einen Linux-Server samt ThinLinc-Terminalserver-Installation und ein gängiges Client-Betriebssystem, auf dem entweder ein spezieller ThinLinc-Client, ein Java-fähiger Browser oder aber TLCOS ausgeführt wird.

Versucht ein Client eine Verbindung mit dem Terminal Service herzustellen, so passiert vereinfacht dargestellt Folgendes:

1. Zunächst generiert der Client einen SSH-Tunnel zum ThinLinc-Server. Der Client übermittelt seine Zugangs-kennung. Schlägt der Login-Versuch fehl, wird der Vorgang abgebrochen und eine entsprechende Fehlermeldung ausgegeben.
2. Als Nächstes versucht der Client, sich bei dem VSM-Server (VNC Session Manager) über den SSH-Tunnel zu authentifizieren. Der VSM-Server ist der Hauptprozess von ThinLinc. Er ist für die Allokation und Überwachung der Benutzer zuständig.
3. Gelingt die Authentifizierung, prüft der Terminalserver, ob es bereits eine Session mit dem Client gibt. Ist das der Fall, werden die Session-Informationen an den Client zurückgegeben. Ist das nicht der Fall, wird eine neue Session angelegt. Sollten Sie mehrere Terminal-Server aufgesetzt haben, wird der Server herausgepickt, der aus Sicht der Lastverteilung der optimale ist.
4. Der Client beendet dann den SSH-Tunnel zu dem VSM-Manager und prüft die Informationen, die er erhalten hat, um

den Terminalserver zu bestimmen, zu dem eine Terminal-Session aufgebaut wird.

5. Im nächsten Schritt erzeugt der Client einen neuen SSH-Tunnel zu dem VSM-Agent-Server, der von dem VSM-Manager für die Verbindungsaufnahme vorgeschlagen wurde. Sofern die Konfiguration es vorsieht, erzeugt die Plattform weitere Tunnel für die Sound-Übertragung und andere Dienste. Außerdem wird ein VNC-Tunnel generiert, es sei denn, die ThinLinc-Konfiguration sieht keine Verschlüsselung des VNC-Traffics vor. Alle diese Tunnel werden gebündelt über eine SSH-Verbindung gelegt.
6. Im letzten Schritt startet der Client den VNC-Viewer. Die gesamte weitere Kommunikation und der Datenaustausch werden über die gesicherte VNC-Verbindung ausgeführt, bis der Client die Verbindung zum Terminalserver beendet beziehungsweise die Verbindung beispielsweise nach einem inaktiven Zeitintervall beendet wird.

ThinLinc-Server installieren

Bevor Sie sich an die Installation des ThinLinc-Terminalservers machen, ist die Frage zu klären, ob Sie ThinLinc als einzigen Terminalserver in Ihrer Infrastruktur verwenden wollen oder ob dort bereits ein solcher Server zum Einsatz kommt, beispielsweise ein MS Windows Terminalserver. Wenn Sie den MS-Server ebenfalls verwenden wollen beziehungsweise bereits eine solche Server-Installation besteht, sollten Sie auf dem Windows-Server das WTS Tools Package installieren.

Bei einem einfachen ThinLinc-Setup richten Sie einen oder mehrere ThinLinc-Server ein, auf die über LAN oder WLAN verschiedene ThinLinc-Clients zugreifen. Die Clients kommunizieren standardmäßig über Port 22 mit dem Server. Wenn Sie keine verschlüsselten grafischen Sessions erzeugen, kommen die Ports 5900 bis 6000 und Ports unterhalb von 32767 zum Einsatz.

Wenn Sie ThinLinc in ein Novell-Netzwerk integrieren, kommuniziert der ThinLinc-Server über Port 636 verschlüsselt mit dem eDirectory. ThinLinc muss zudem mit dem Netware-Dateiserver per TCP oder UDP über Port 524 kommunizieren können. Wenn Sie ThinLinc in eine Win-

dows-Infrastruktur mit einem Windows Domain Controller und Windows-Dateiserver integrieren wollen, so muss ThinLinc mit dem Controller per TCP über Port 139 kommunizieren können. Bei der Kommunikation mit dem Dateisystem kommen typischerweise die TCP-Ports 139 und/oder 445 zum Einsatz.

Mit diesen Informationen im Hinterkopf können Sie sich an die eigentliche Installation des ThinLinc-Servers machen. Dazu laden Sie sich von der Projektseite das Server-Bundle herunter und entpacken es. Das Installationsprogramm starten Sie mit folgendem Befehl:

```
# sh ./install-server
```

Nach der Ausführung dieses Befehls ist ThinLinc bereits installiert und Sie können sich an die Konfiguration machen. Dazu führen Sie das Setup-Programm aus:

```
/opt/thinlinc/sbin/tl-setup
```

Damit steht Ihnen die Basiskonfiguration zur Verfügung und Sie können sich im nächsten Schritt dem Feintuning widmen.

Einstieg in die ThinLinc-Server-Konfiguration

Der ThinLinc-Server verwendet für die Konfiguration und die Speicherung der

VDI-Lösungen erlauben den Nutzern den Zugriff auf ihre eigene dezidierte virtuelle Maschine – im Unterschied zu einem Account auf einem Shared Server. Die VDI-Technik stellt Ihnen hierfür bekannte Funktionen wie den Ein-/Aus-Schalter, das Einfrieren von Installationen, das Verwalten von Berechtigungen und die gemeinsame Verwendung der Peripherie zur Verfügung. In manchen Szenarien ist es sinnvoll, statt der klassischen Terminal-Services (TS) besser VDI zu nutzen. Das Gute dabei: ThinLinc unterstützt beide Möglichkeiten, also VDI- und TS-Konfigurationen sowie gemischte Konfigurationen. Die VDI-Unterstützung von ThinLinc erlaubt es den Benutzern, auf virtuelle Maschinen zuzugreifen, die auf einer VMware-Umgebung ausgeführt werden. Für den Benutzer ist dabei nicht zu erkennen, auf welche Umgebung er zugreift. Mit speziellen Tools ist auch die Integration von VirtualBox-VMs möglich. Die VDI-Integration gestaltet sich recht einfach, denn Pools und Benutzer lassen sich auch über das ThinLinc-Webinterface anlegen und verwalten.

ThinLinc und VDI



Konfigurationsparameter "Hiveconf". Dabei handelt es sich nicht um ein ThinLinc-spezifisches Modul, sondern vielmehr um ein generisches Konfigurations-Framework, das Schlüsselwert-Paare in einer einfach lesbaren und verständlichen Form speichert. Die Konfiguration ist so einfach verständlich wie jede Windows-INI-Datei oder die Samba-Konfigurationsdatei *smf.conf*. ThinLinc verwendet eine Ordnerstruktur, in der die verschiedenen Konfigurationsdateien abgelegt sind:

- /vsm: In diesem Verzeichnis sind die Parameter für den VSM-Agent und den VSM-Server hinterlegt. Der Pfad der Konfigurationsdatei lautet typischerweise */opt / thinlinc / etc / conf.d / vsm.hconf*.
- /vsmagent: Diese Konfigurationsdatei beinhaltet spezifische Parameter für den VSM-Agent und ist unter */opt / thinlinc / etc / conf.d / vsmagent.hconf* zu finden.
- /vsmserver: Konfiguriert spezifische Parameter des VSM-Servers. Die Konfigurationsdatei ist unter */opt / thinlinc / etc / conf.d / vsmserver.hconf* erreichbar.
- /appservergroups: Wird für den Zugriff auf Anwendungsserver und VDI-Hosts benötigt. Die Config-Datei liegt unter */opt / thinlinc / etc / conf.d / appservergroups.hconf*.
- /profiles: Konfiguriert die verschiedenen Session-Profile. Zu finden unter */opt / thinlinc / etc / conf.d / profiles.hconf*.
- /utils: Dient der Konfiguration verschiedener ThinLinc-Utilities. Jedes Tool besitzt eine Konfigurationsdatei.
- /sessionstart: Beinhaltet verschiedene Parameter, die für den Session-Aufbau relevant sind.
- /vdi: In diesem Ordner finden Sie die VDI-Einstellungen.
- /tlwebadm: In diesem Ordner konfigurieren Sie die Webschnittstelle.

Die wichtigsten Konfigurationen der ThinLinc-Umgebung finden Sie in den Verzeichnissen *vsm*, *vsmagent* und *vsmserver*. In *vsmagent* können Sie mit *agent_hostname* den Hostnamen öffentlichen Hostnamen anpassen. Standardmäßig ist diese Konfiguration leer und ThinLinc verwendet dann die IP-Adresse des Computers, auf dem Sie den Server ausführen. Der Vorteil: Das DNS muss nicht sauber konfiguriert sein. Wenn Sie allerdings NAT verwenden,

müssen Sie diese Einstellungen beispielsweise wie folgt vornehmen:

```
agent_hostname = thinlinc.server.de
```

In "/vsmagent/allowed_clients" geben Sie die Liste der VSM-Server an, die eine Verbindung zu dem VSM-Agent herstellen dürfen und Sessions erzeugen können. Localhost darf standardmäßig immer Verbindungen zu dem Agent initiieren.

Im Unterordner "/vsmagent/default_environment" bestimmen Sie die Umgebungsvariablen für User-Sessions. Damit legen Sie beispielsweise die Standardsprache und die Kodierung fest. Mit der Konfiguration bei "vsmagent/listen_port" setzen Sie den TCP-Port des VSM-Agenten für eingehende Requests. Dieser sollte den gleichen Wert wie in "/vsm/vsm_agent_port" besitzen. Setzen Sie die Option "vsmagent/make_homedir" auf "true", damit für die Benutzer automatisch ein Home-Verzeichnis erstellt wird. Das eigentliche Verzeichnis legen Sie mit dieser Option an:

```
/vsmagent/make_homedir_mode
```

Über den Parameter "vsmagent/single_signon" bestimmen Sie, ob das Benutzerpasswort gespeichert werden soll, um in Zukunft den Zugriff per Single Sign-on zu vereinfachen.

Anpassungen des VSM-Servers

Für die Konfiguration des VSM-Servers sind die Konfigurationsdateien im Verzeichnis "/vsmserver" relevant. Geben Sie zunächst über "vsmserver/admin_email" die E-Mailadresse des Administrators an. Den Hostnamen für ausgehende Requests vom VSM-Server zum VSM-Agent bestimmen Sie über:

```
/vsmserver/agentcomm_bind_hostname
```

Die Verwendung dieser Konfiguration ist dann wichtig, wenn der VSM-Server verschiedene Schnittstellen für die Kommunikation verwendet. Auch für den VSM-Server kann eine Host-Liste mit den Systemen angelegt werden, die privilegierte Operationen ausführen dürfen. Zu diesen Operationen gehört beispielsweise das De-

Damit Sie ausrangierte Computersysteme wieder zum Leben erwecken können, haben die Cendio-Entwickler ein spezielles Thin Client-Betriebssystem entwickelt, das für das Zusammenspiel mit dem Terminal konzipiert ist. Bei TLCOS handelt es sich um ein auf Fedora 8 basiertes Betriebssystem, das auch den ThinLinc-Client beinhaltet. Laut Angaben der Entwickler handelt es sich dabei um ein schlankes Betriebssystem, doch deutet der Download des 457 MByte großen ISO-Pakets auf etwas anderes hin. Dennoch dürfte der Einsatz von TLCOS für viele Unternehmen interessant sein, da es leistungsschwächeren Rechnern einer neuen Bestimmung zuführen kann: der Verwendung als Thin Client.

Nach der Installation des Betriebssystems, das Sie lokal, aber auch per PXE über das Netzwerk aufspielen können, erfolgt ein Neustart des Systems und der ThinLinc-Client wird bei jedem Neustart automatisch gestartet. Für die Installation benötigen Sie einen Rechner, der mit 128 MByte RAM und etwa 3 GByte freien Festplattenspeicher ausgestattet ist. Wenn Sie TLCOS auf einem Testrechner evaluieren wollen, laden Sie sich die ISO-Datei von der Cendio-Website herunter und installieren Sie diese auf dem System. Der Installationsvorgang wird über die Kickstart-Konfigurationsdatei *ks.cfg* gesteuert. Sie finden die Datei im Root-Verzeichnis der Installations-CD, die Sie mit der ISO-Datei erzeugen können. Die Installation von CD ist denkbar einfach: Sie legen das Installationsmedium in ein CD-ROM-Laufwerk, starten den Rechner und folgen den Anweisungen auf dem Bildschirm.

Wenn Sie TLCOS auf mehreren oder gar vielen Clients installieren wollen, ist die CD-basierte Installation unpraktisch. Da die meisten Netzwerkadapter über PXE-Unterstützung verfügen, sollten Sie die netzwerkbasierende Installation wählen. PXE-Implementierungen verwenden typischerweise *bootp*, sodass Sie einen DHCP-Server für die netzwerkweite Installation verwenden können. Sie benötigen außerdem einen TFTP-Server, von dem sich PXE die Konfigurationsdatei und den Kernel holt. Konnte der Kernel auf den Client übertragen werden, prüft dieser die Kickstart-Konfigurationsdatei und bezieht die weiteren Daten per HTTP von einem Webserver.

Das Installationsprogramm verwendet standardmäßig den Host *thinlinc* für die TLCOS-Installation. Sie sollten Ihre DNS-Konfiguration entsprechend anpassen. Alternativ editieren Sie die Dateien *images/pxeboot/pxelinux.cfg/default* und *ks.cfg*. Auch auf Seiten des DHCP-Servers sind einige Anpassungen erforderlich. Er ist für die Verwendung von *bootp* zu konfigurieren. Eine entsprechende Konfiguration in den DHCP-Settings könnte wie folgt aussehen:

```
host dhcp_server {
  hardware ethernet 01:03:a3:56:ef:8d;
  fixed-address 10.0.0.1;
  next-server tlinstallhost;
  filename "pxelinux.0";
  allow bootp;
  allow booting;
}
```

Der DHCP-Server benötigt nicht notwendigerweise eine statische IP-Adresse, Sie können auch eine dynamische verwenden. Den TFTP-Server sollten Sie so konfigurieren, dass er die Dateien der TLCOS-Installations-CD unter "/images/pxeboot" bereitstellt. Da die weiteren Daten per HTTP übertragen werden, müssen Sie den CD-Inhalt außerdem über einen Webserver verfügbar machen. Kopieren Sie dazu die CD-Daten in das Verzeichnis TLCOS, ein Unterverzeichnis von "/var/www/html". Damit haben Sie alle notwendigen Schritte für die PXE-basierte Installation vorgenommen.

**TLCOS – ThinLinc
Client Operating System**



aktivieren von Sessions. Diese Liste ist standardmäßig leer, allerdings besitzt localhost die entsprechenden Berechtigungen:

```
/vmsserver/allowed_clients
```

Sie können die Verwendung der Umgebung außerdem auf bestimmte Gruppen beschränken. Weist die Konfiguration "allowed_groups" keinen Eintrag auf, werden alle Benutzer akzeptiert. Alternativ legen Sie Gruppen an und hinterlegen diese wie folgt in der Konfigurationsdatei:

```
allowed_groups = administratoren
```

Die Parameter "/vsm" wirken auf den VSM-Agent und den VSM-Server. In der Regel sind hier keine Änderungen notwendig, dennoch sollten Sie wissen, welche Einstellungen hier konfiguriert sind. Über "/vsm/tunnel_bind_base" bestimmen Sie den niedrigsten Port, der vom VSM-Agent verwendet wird. Bei "/vsm/tunnelservices" sind verschiedene Tunnel-spezifische Parameter definiert.

Die Port-Basis für die VNC-Kommunikation wird in "/vsm/vnc_port_base" bestimmt. Das VNC-Protokoll verwendet für jeden Benutzer einen Port. Der erste VNC-User bekommt den Port zugewiesen, der eins größer als der hier hinterlegte Wert ist, der nächster User dann vnc_port_base + 2 et cetera.

Der ThinLinc-Client

Für den Zugriff auf den ThinLinc-Terminalserver steht Ihnen der ThinLinc-Client zur Verfügung. Er ist für alle relevanten Plattformen verfügbar. Um sich erfolgreich von einem Client-Betriebssystem auf dem ThinLinc-Server einloggen zu können, installieren Sie den Client und geben im Login-Dialog den Hostnamen des Terminalservers, die Benutzerkennung und das Passwort an.

Beim Login-Versuch prüft der Terminalserver, ob der Client über eine entsprechende Zugangsberechtigung verfügt. Anstelle des Hostnamens können Sie eine IP-Adresse angeben. Sofern Sie sich für die passwortgeschützte Authentifizierung entschieden haben, genügt die Angabe der Kennung und des Passworts.

Verwenden Sie hingegen die Public Key-Authentifizierung oder SmartCards, müssen Sie den Pfad zum Schlüssel beziehungsweise ein Zertifikat angeben. Der Client speichert den Servernamen, den Benutzernamen, den Schlüsselpfad und der Zertifikatnamen, damit diese Eingaben beim nächsten Verbindungsaufbau nicht erneut anzugeben sind. Mit einem Klick auf "Verbinden" stellen Sie die Verbindung zum Server her.

Über die "Erweitert"-Schaltfläche ist der Zugriff auf zwei weitere Funktionen möglich: Mit "Session beenden" erzwingen Sie das Beenden der Verbindung und initiieren einen neuen Verbindungsaufbau, mit "Optionen" greifen Sie auf die Client-Optionen zu. Hier steht Ihnen eine Fülle an erweiterten Funktionen zur Verfügung. Auf der Registerkarte "Optionen" können Sie beispielsweise das zu startende Programm bestimmen, das

Kompetentes Schnupperabo sucht neugierige Administratoren



www.it-administrator.de

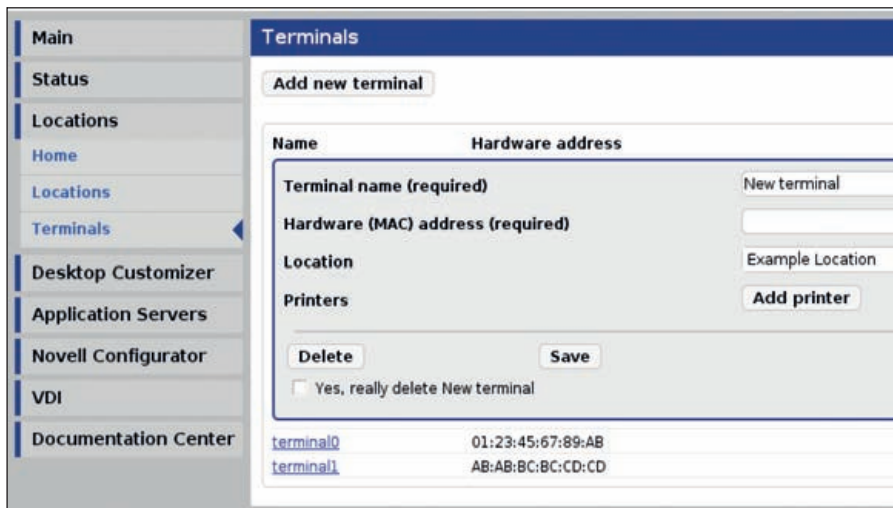


Bild 2: Schmucklos, aber praktikabel: Das ThinLinc-Webinterface vereinfacht die Administration

automatisch beim Session-Aufbau geladen wird. Auf der Registerkarte "Lokale Geräte" legen Sie fest, ob neben dem Drucker, dem Soundmodul und einem optionalen SmartCard-Lesegerät auch die serielle Schnittstelle und weitere Laufwerke freigegeben werden. Theoretisch können Sie alle verfügbaren Laufwerke einbinden. Für die Anpassung der Bildschirmauflösung verwenden Sie die Registerkarte "Bildschirm".

Den Client-Zugriff auf den Terminalserver können Sie außerdem über die Registerkarte "Optimierung" bei der bevorzugten Kodierung, dem Farblevel und der Komprimierung manuell anpassen.

Es geht auch hochverfügbar

Bereits in recht kleinen Umgebungen, in denen nur einige Duzend Clients mit dem Terminalserver arbeiten, ist es sinnvoll, die Funktionen für die Ausfallsicherheit von ThinLinc zu verwenden, denn nichts ist schlimmer als unnötige Ausfallzeiten.

Das Grundprinzip: Sie richten zwei identische Terminalserver ein, auf denen der VSM-Server ausgeführt wird. Fährt einer der Server aus irgendwelchen Gründen herunter, übernimmt der zweite Server

alle Sessions und sorgt dafür, dass die Clients weiter mit den benötigten Daten versorgt werden – im Idealfall, ohne dass die Clients etwas davon bemerken.

Sie realisieren die HA-Funktionalität durch einen Synchronisierungsmechanismus, der die Session-Daten über mehrere VSM-Server hinweg abgleicht und permanent aktualisiert. Die hierfür benötigten Komponenten sind nicht Bestandteil von ThinLinc, sondern müssen gesondert installiert und konfiguriert werden. ThinLinc greift dabei auf die Lösung des Linux-HA-Teams [2] zurück. Um Ihre ThinLinc-Installation mit dieser Lösung abzusichern, müssen Sie zumindest eine weitere ThinLinc-Installation aufsetzen. Wichtig ist dabei, dass Sie auf beiden die gleichen SSH-Schlüssel verwenden. Kopieren Sie dazu das Verzeichnis `"/etc/ssh/ssh_host_*"` auf das Zweitsystem und starten Sie das SSH-Modul erneut.

Nehmen Sie als Nächstes Linux-HA in Betrieb und konfigurieren Sie es so, dass es den Status der beiden Systeme überwacht. Dann stellen Sie den VSM-Agent so ein, dass er privilegierte Aktionen von den beiden Terminalserver-Installationen zulässt. Mit dem folgenden Schritt gewährleisten Sie, dass der VSM-Server auf beiden Systemen korrekt ausgeführt wird. Wichtig ist dabei, dass beide die gleiche Agent-Liste verwenden. Besonders wichtig ist außerdem, dass 127.0.0.1 nicht in der Liste der Terminalserver auftaucht. Auf Seiten der VSM-Server-Installationen sind außerdem die HA-Funktionen zu aktivieren.

Um sicherzugehen, dass Ihre Konfiguration den gewünschten Zweck erfüllt, sollten Sie die Ausfallsicherheit prüfen. Ziehen Sie dazu einfach das Kabel von dem Standard-Terminalserver und vergewissern Sie sich, ob die verbundenen Clients weiter bedient werden.

Das Web-Interface

Der ThinLinc-Terminalserver verfügt über eine webbasierte Administrationsschnittstelle, auf die Sie über `https://hostname:1010` zugreifen. Sie trägt die Bezeichnung `tlwebadm` und lässt sich mithilfe verschiedener Optionen anpassen. Editieren Sie dazu die Konfigurationsdatei `/opt/thinlinc/etc/conf.d/tlwebadm.hconf`.

Bevor Sie sich über die Webschnittstelle auf die Terminalserverkonfiguration verbinden können, müssen Sie den Benutzernamen und das Passwort bestimmen. Dazu verwenden Sie diese Einstellungen:

```
/tlwebadm/username
/tlwebadm/password
```

Sie können auch das Tool `/opt/thinlinc/sbin/tl-gen-auth` verwenden, um Hash-Werte zu erstellen.

Den Pfad zur Zertifikatdatei, die für die SSL-Verschlüsselung verwendet wird, geben Sie mit `/tlwebadm/cert` an. Den Standardport ändern Sie mit `/tlwebadm/listen_port`. Außerdem können Sie den Pfad zur Protokolldatei mit `/tlwebadm/logging/logfile` ändern. Standardmäßig verwendet das Web-Interface die Datei `/var/log/tlwebadm.log`. Über das Web-Interface selbst sind überwiegend einfache Aktionen wie das Anlegen eines neuen Terminals möglich. Außerdem können Sie verschiedene statistische Informationen abrufen.

Fazit

ThinLinc ist eine einfach zu bedienende und funktional vollständige Terminalserver-Lösung, die alles bietet, was von einem Werkzeug dieser Art zu erwarten ist. Dank der Unterstützung von etablierten Terminal-Lösungen ist auch die Integration in bestehende IT-Infrastrukturen einfach möglich. Nicht zuletzt wegen der moderaten Preisgestaltung ist ThinLinc eine interessante Alternative. (In)



[1] ThinLinc Download
CBP61

[2] Linux HBA
CBP62

Link-Codes



Read-only Domänencontroller einrichten Aus der Schusslinie

von Ulf B. Simon-Weidner

Domänencontroller spielen eine grundlegende Rolle in Windows-Umgebungen. Aufgrund ihrer Bedeutung müssen die Server besonders geschützt werden. In Außenstellen manchmal ein schwieriges Unterfangen. Deshalb bietet Microsoft den schreibgeschützten Domänencontroller an. Das Ziel: eine dezentrale DC-Verfügbarkeit bei höchstmöglicher Sicherheit. Wie Sie diesen Read-only Domänencontroller in der Praxis einsetzen und welche Besonderheiten er mitbringt, lesen Sie in diesem Workshop.



Quelle: piren - 123RF

Der Domänencontroller (DC) ist in IT-Infrastrukturen eine der wichtigsten Komponenten: Er stellt die Active Directory-Domänendienste zur Verfügung und kümmert sich darum, dass sich die Benutzer an beliebigen Systemen anmelden können und etwa ihre Berechtigungen erhalten, um auf E-Mailpostfach, Dateiserver, Drucker und Anwendungen zuzugreifen. Daneben stellt der DC Adressbuchdaten und Hierarchieinformationen zur Verfügung, verwaltet die Sicherheitseinstellungen und Systemvorgaben von Laptops, Desktops und weiteren Servern und regelt, mit welchen weiteren Domänen eine möglichst integrierte Zusammenarbeit möglich ist. Anwendungen wie DNS, Zertifikatsdienste oder Exchange integrieren sich in die Active Directory-Domänendienste, die von Haus aus redundant identisch von allen DCs der gleichen Domäne zur Verfügung gestellt werden.

Daher ist es ratsam, auch in kleinen Umgebungen mehr als einen DC zu verwenden, um Ausfallsicherheit und Redundanz zu schaffen. Außerdem sollen die Anmeldedienste in unterschiedlichen Standorten

des Unternehmens performant und teilweise unabhängig von der Leistung und Zuverlässigkeit der WAN-Anbindung funktionieren. Aber besonders die physikalische Sicherheit von DCs ist ein wichtiges Thema. Da diese die Informationen über alle Benutzer und deren Passwörter sowie zahlreiche weitere infrastrukturelle Daten enthalten, müssen Sie sicherstellen, dass diese Informationen nicht in falsche Hände geraten. Und ein Datenklau ist bei fehlender physikalischer Sicherheit, zum Beispiel mangels eines dedizierten Serverraums, relativ einfach zu bewerkstelligen.

Besonderheiten des RODC

Seit Windows Server 2008 gibt es eine Option für weniger vertrauenswürdige Umgebungen: den schreibgeschützten Domänencontroller (Read-only Domain Controller, RODC). Dieser enthält alle Daten eines vollen DCs, nicht jedoch die "Shared Secrets" wie Passwörter. Zum einen bietet der RODC eine schnelle Anmeldung für die Anwender, die sich im gleichen Standort befinden. Er hält nämlich nahezu alle Daten vor, die auch ein normaler DC enthält, und repliziert ferner alle

Gruppenrichtlinien. Gerade diese beeinflussen die Anmeldezeiten erheblich, insbesondere über WAN-Leitungen. Die Überprüfung des Benutzerkontos und Passwortes hingegen benötigt sehr geringen Netzwerkverkehr. Die Anmeldezeiten zwischen einem Standort mit vollwertigem DC gegenüber denen eines Standorts mit RODC unterscheiden sich unmerklich, wohingegen die Anmeldezeiten bei einem Standort ohne DC erheblich von der Geschwindigkeit der WAN-Leitungen sowie der Menge und dem Inhalt der Gruppenrichtlinien abhängt.

Die Active Directory-Datenbank des RODCs ist nur lesbar. Änderungen werden lediglich über die eingehende Replikation von vollwertigen DCs zugelassen. Versucht eine Anwendung, auf einen RODC zu schreiben, erhält sie einen "LDAP write-referral", also eine Umlenkung auf einen DC. RODCs replizieren auch keine Informationen nach außen, sie nutzen nur eingehende Replikationsverbindungen. Sollte es tatsächlich jemand schaffen, Änderungen in der lokalen Datenbank durchzuführen, werden diese nicht auf weitere DCs des Unternehmens repliziert.

Passwörter werden standardmäßig nicht auf dem RODC gespeichert. Sie können dies jedoch ändern, indem Sie es zulassen, dass die Passwörter bestimmter Benutzer auf dem RODC gecached werden. Meldet sich dann ein Benutzer an einem RODC an, prüft dieser zunächst, ob er das Passwort des Anwenders selber verifizieren kann. Liegt das Passwort lokal nicht vor, leitet der RODC die Kerberos-Ticketanfrage an einen DC weiter. Dieser überprüft den Benutzer und stellt ein Ticket aus, das der RODC durch sein eigenes Ticket ersetzt und dem Benutzer aushändigt. Im Anschluss fragt der RODC den DC über einen sogenannten "Replicate Single Object Request" mit der Option "Secrets-Only", ob er das Passwort für den Benutzer erhalten darf. Der DC überprüft anhand von "Erlaubt- und Verboten-Listen", ob der RODC das Passwort erhalten darf, und lässt die Replikation gegebenenfalls zu. Beachten Sie hierbei, dass es sich zwar um eine Replikation handelt, das Passwort jedoch nicht fortlaufend mitrepliziert wird. Ändert der Benutzer das Passwort in einem anderen Standort, wird es nicht repliziert, sondern auf dem RODC gelöscht. Erst wenn der Anwender sich wieder an dem RODC authentifiziert, beginnt der Prozess von vorn und das neue Passwort wird angefordert. Aber bereits parallel zur Passwortanfrage des RODCs kann der Benutzer

mit seinem Client die weitere Anmeldung durchführen und die Gruppenrichtlinien laden und anwenden.

Aber auch in weiteren Szenarien kann ein RODC nützlich sein. In einer demilitarisierten Zone etwa lassen sich Computerkonten in die Active Directory-Verwaltung einbinden und über GPOs zentral konfigurieren. Da der RODC nur eine eingehende Replikation nutzt, spart er zudem Replikationsverkehr. Auf einem RODC können ferner keine "Lingering Objects" oder sonstige Effekte auftreten, die Auswirkungen auf andere Teile des Active Directory hätten. Schließlich ist der RODC bei Domänen oder Forest-Recoveries einigermassen unkritisch, da er keine Informationen in die restliche Domäne repliziert. Er kann also im Gegensatz zu DCs zunächst dazu dienen, während einer Wiederherstellung noch Benutzeranmeldungen durchzuführen, und muss erst danach neu eingerichtet werden.

Nicht alle Anwendungen sind kompatibel

Was müssen Sie nun bezüglich Anwendungen bei Nutzung eines RODC beachten? Zunächst sollten nahezu alle Applikationen auch im Zusammenhang mit RODCs funktionieren. Wenn Schreibzugriffe versucht werden, erhält die Anwendung den bereits erwähnten LDAP

write-referral. Diese Methode ist in dem LDAP RFC 2251 von 1997 hinterlegt und existiert auch in anderen Verzeichnisdiensten oder bei Globalen Katalogservern, wenn Informationen anderer Domänen angefragt werden. Anwendungen sollten also keine Schwierigkeiten hiermit haben. Eine Ausnahme bilden allerdings Programme, die weder über Standard-APIs noch LDAP auf dem DC schreiben wollen. Hierzu gehört auch Microsoft

Exchange, wodurch es nicht möglich ist, Exchange-Server an Standorten zu betreiben, die von einem RODC bedient werden. Exchange benötigt einen vollwertigen DC. Ob es sinnvoll ist, einen Exchange-Server in einem eventuell unsicheren Außenstandort zu betreiben, ist natürlich die andere Frage.

DCs in Windows-Infrastrukturen beheimaten oft auch DNS-Server und Windows bietet die häufig genutzte Option, DNS in das Active Directory zu integrieren. Alle DCs und Domänenmitglieder nutzen DNS, um sich zu registrieren: DCs bieten ihre Dienste hierüber an und alle Domänenmitglieder sind hierüber auffindbar, indem sie ihren Namen und die IP-Adresse registrieren. Auch mit dem RODC ist dies einfach gelöst: das klassische DNS-Protokoll sieht normalerweise einen schreibfähigen, primären DNS-Server pro Zone vor und mehrere nur-lesbare, sekundäre Server. Ist der DNS-Dienst in das Active Directory integriert, wird in Windows-Infrastrukturen das AD für die Replikation der DNS-Informationen verwendet und es ist nicht notwendig, nur einen beschreibbaren DNS-Server zu nutzen – DNS wird plötzlich Multi-Master-fähig und jeder Server gibt bei der Frage nach dem beschreibbaren DNS-Server einfach sich selbst an. Daher ist die Lösung für DNS auf dem RODC naheliegend: Er verhält sich wie ein klassischer, sekundärer DNS-Server. Erhält er eine Anfrage nach einem schreibbaren DNS-Server, wird er nicht wie andere AD-integrierte DNS-Server selbst anbieten, sondern einen DC, auf dem das Domänenmitglied seine Einträge dann vornehmen lässt. Da der RODC aber zuvor nach einem beschreibbaren DNS-Server gefragt wurde, informiert er sich kurz darauf bei diesem nach dem neuen oder geänderten DNS-Eintrag und repliziert diesen. Damit hat er gegenüber klassischen sekundären DNS-Servern den Vorteil, sehr aktuell bezüglich der Einträge seiner "eigenen Clients" zu sein. Die DNS-Einträge anderer Server erhält er über die normale Active Directory-Replikation.

Anwendungen sollten also üblicherweise weder mit AD noch DNS auf den RODCs ein Problem haben. Ein Thema taucht allerdings hin und wieder auf: Für

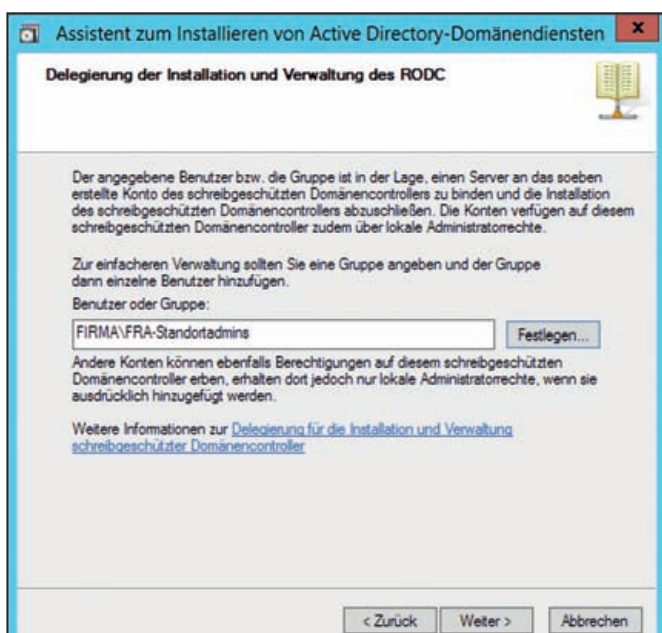


Bild 1: Wird der RODC in zwei Stufen installiert, gibt der Domänenadministrator die Einstellungen vor und ermächtigt ein Konto oder eine Gruppe, den RODC zur Domäne hinzuzufügen und lokal zu verwalten



den RODC legt das “Filtered Attribute Set (FAS)” fest, dass einige sicherheitsrelevante Attribute nicht auf einen RODC repliziert werden sollen. Dies sind standardmäßig zum Beispiel die Bitlocker Recovery Keys, wenn die Festplatten von Domänenmitgliedern per Bitlocker verschlüsselt werden. Sollte es Anwendungen geben, die das FAS verwenden, oder Sie als Administrator das FAS auf weitere Attribute ausdehnen, ist wichtig, dass diese Anwendungen auch den RODC verstehen. Wird der RODC nach einem Attribut aus dem FAS gefragt, gibt er nämlich einen leeren Wert zurück. Der RODC weiß, dass das Attribut existiert, hat aber keinen Wert dafür. Die Anwendung muss sich dessen bewusst sein und Anfragen nach Attributen, auch dem Filtered Attribute Set, explizit von vollen DCs verlangen. Dieses “Feature” sollte aber auch nicht zu Problemen führen, solange Sie keine Änderungen durchführen.

Standortüberlegungen

Also bestimmen zumindest die Exchange-Standorte schon einmal, wo RODCs stehen dürfen und wo nicht. Aber auch beim Einrichten von RODCs müssen Sie sich detailliertere Gedanken zu Ihren Standorten machen:

- Wie zuverlässig sind die Netzwerkverbindungen an den Standort?
- Wie viele Benutzer arbeiten an dem Standort?
- Gibt es einen gesicherten Serverraum?
- Wie viele Domänencontroller werden für den Standort benötigt?
- Gibt es RODC-inkompatible Anwendungen an dem Standort?
- Mit welchen Anwendungen kann der Benutzer an dem Standort arbeiten, wenn eine WAN-Leitung ausgefallen ist? Benutzer können sich über gespeicherte Profile an den bisherigen Rechnern anmelden und kommen gegebenenfalls sogar auf lokale Applikations-, Datei- und Druckserver (solange dezentrale Namensauflösung möglich ist beziehungsweise nur ein Netzwerksegment per Broadcast). Alle zentralen Dienste stehen in diesem Fall ohnehin nicht zur Verfügung.
- Macht ein RODC möglicherweise aus weiteren Gründen Sinn – etwa zur Entlastung der Anmeldezeiten?

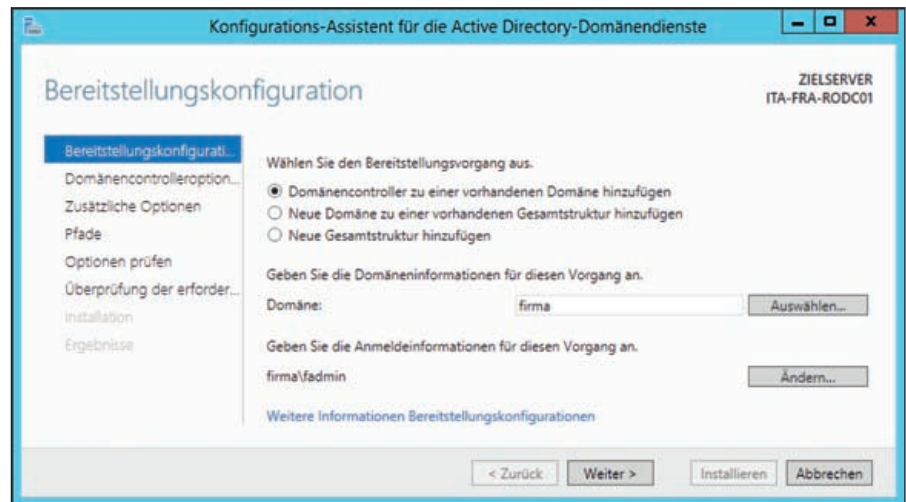


Bild 2: Im Server Manager fügt der Administrator die Rolle mit abhängigen Funktionen für die Domänendienste hinzu. Danach muss er die Konfiguration des RODC durchführen.

Haben Sie diese Daten pro Standort erhoben, können Sie sich überlegen, für welche Standorte der Einsatz eines RODCs sinnvoll sein könnte. Bei zuverlässigen und schnellen Netzwerkleitungen und wenigen Benutzern können Sie gegebenenfalls auf einen DC oder RODC am Standort ganz verzichten. Falls es dort einen gesicherten Serverraum gibt, bietet sich auch der Einsatz eines vollwertigen DCs an. Benötigen Sie mehrere DCs an einem Standort, ist ein RODC unter Umständen auch weniger sinnvoll: Jeder RODC kennt nur sich und seinen DC als Replikationspartner und würde daher Informationen immer über die WAN-Leitung replizieren. Auch liegen die zwischengespeicherten Passwörter auf jedem RODC separat vor; ein Anwender, der sich also nur an einem Server authentifiziert hat, könnte sich bei einem Ausfall der WAN-Leitung nicht an einem anderen RODC authentifizieren.

Sichere RODC-Einrichtung

Das Einrichten eines RODCs kann auf zwei Wegen erfolgen: Analog zur bisherigen Installation eines Domänencontrollers stufen Sie den Mitgliedsserver hoch und wählen hierbei die Option “RODC”. Der zweite Weg ist noch interessanter und zu bevorzugen: Sie erstellen als Domänenadministrator das Computerkonto für den RODC in der Domänencontroller-OU. Dabei machen Sie alle notwendigen Vorgaben und legen im Vorfeld fest, ob der RODC einen Globalen Katalog besitzen soll, DNS zur Verfügung stellt und in wel-

chem Standort er stehen soll. Des Weiteren können Sie das Verbinden und Hochstufen des RODCs zur Domäne dann an einen Benutzer oder eine Gruppe delegieren. Hierfür sind dann keine Domänenadministratorenrechte mehr notwendig. Die hierfür verwendete Gruppe erhält vielmehr lokale Administratorenrechte und kann den RODC nur mit den vorgegebenen Optionen hinzufügen. Dies ist sehr interessant, da in der Vergangenheit eine Trennung von lokaler Administration eines Servers und der Domänenadministration bei Domänencontrollern nur schwer und nicht sicher genug durchgeführt werden konnte.

Der RODC ist aber eine grundlegende Änderung gegenüber dem bisherigen Domänencontroller und entspricht von der Grundarchitektur eher einem Mitglieds-server, der zusätzlich Domänendienste zur Verfügung stellt. Dadurch kann erstmals die lokale Administration des RODCs delegiert werden, sodass der Administrator eines Standortes die IP-Adresskonfiguration durchführen und auch ansonsten sicherstellen kann, dass der Server entfernt verwaltbar ist, während sich die Domänenadministratoren darum kümmern, dass der RODC in der Replikationsinfrastruktur teilnimmt und korrekt funktioniert.

Dies geht sogar noch etwas weiter: Aus Sicherheitsgründen sollte sich ein Domänenadministrator nie direkt oder via Remote Desktop-Dienste an einem nicht-vertrauenswürdigem Gerät anmelden – also an einem Gerät, dessen physikalische



Sicherheit nicht gewährleistet ist, da üblicherweise auf den Systemen die lokale Anmeldung der letzten zehn Benutzer zwischengespeichert wird. Bei einem abhandengekommenen Gerät (oder einem abgezogenen Image) könnte ein Angreifer versuchen, das Domänenadministratorkonto mit dessen Passwort herauszubekommen. Daher ist es empfehlenswert, den RODC in den beschriebenen zwei Stufen einzurichten. Den Administratoren in Ihrem Team sollte bewusst sein, dass sie sich niemals mit einem Domänenadministratorkonto oder sonstigem Konto mit höheren als den delegierten Rechten am RODC anmelden.

Zu beachten bleibt allerdings, dass der Server bei der zweistufigen Installation den gleichen Namen haben muss wie das erstellte Computerkonto, aber noch nicht in der Domäne beigetreten sein darf, da es keine zwei Computerkonten mit dem gleichen Namen geben darf. Möchte der delegierte Administrator also den zweiten Teil durchführen, loggt er sich lokal an dem Server ein, der zu dem Zeitpunkt zwar genauso heißt wie der spätere RODC, aber noch nicht Teil der Domäne ist. Über den Server Manager fügt er dann die Rolle "Active Directory Domänendienste" mit ihren Abhängigkeiten hinzu.

Anschließend wählt er in den Benachrichtigungen des Server Managers die Option "Server zu einem Domänencontroller heaufstufen". Danach kann er im Konfigurations-Assistent für Active Directory-Domänendienste den Server zu einer existierenden Domäne hinzufügen und die Domäne sowie die Daten des delegierten Kontos angeben. Nun bemerkt der Konfigurations-Assistent, dass bereits ein Konto für den RODC vorhanden ist und bietet an, dieses zu verwenden. Da der delegierte Administrator sowieso keine Berechtigung hat, einen anderen DC zur Domäne hinzuzufügen, muss er auch diese Option wählen. Nach wenigen weiteren Angaben wird der RODC dann eingerichtet.

Zwischenspeichern von Passwörtern

Wie lässt sich nun steuern, welche RODCs welche Passwörter cachen dürfen? Erhält der RODC eine Anmeldean-

forderung, die typischerweise von einem Client oder Benutzer kommt, prüft er zunächst, ob er das Passwort vorhält und die Anfrage beantworten kann. Ist dies der Fall, stellt er dem Anwender einen Token (Kerberos-Ticket sowie Anmeldetoken mit Gruppenmitgliedschaften) aus. Ansonsten leitet der RODC die Anmeldeanforderung an einen DC weiter, erhält das Kerberos-Ticket, wandelt dieses in ein eigenes Ticket um und stellt dem Benutzer den Anmeldetoken aus. Danach fordert er beim DC eine Passwortreplikation an.

Der DC überprüft daraufhin, ob der RODC berechtigt ist, das Passwort zu erhalten. Standardmäßig darf der RODC nur das Passwort seines eigenen Computeraccounts sowie seines Kerberos-Dienstes erhalten. Sie haben jedoch die Möglichkeit zu bestimmen, welche Passwörter der RODC auf Anforderung erhalten darf. Hierzu steht Ihnen die Konfiguration im Computerobjekt des RODC zur Verfügung, in der standardmäßig schon zwei Gruppen enthalten sind:

- Denied RODC Password Replication Group
- Allowed RODC Password Replication Group

Des Weiteren sind einige Gruppen parallel zur Denied RODC Password Replication Group vorhanden, die Microsoft für schützenswert erachtet und daher parallel zur Gruppe die Passwortreplikation verweigert. Diese sind Administratoren, Serveroperatoren, Backup-Operatoren und Kontenoperatoren.

Und auch innerhalb der Denied-Gruppe finden sich noch weitere Konten, deren Passwörter nicht auf den RODC dürfen:

- Cert Publishers
- Domänenadministratoren
- Domänencontroller
- Organisationsadmins
- Group Policy Creators
- Krbtgt
- Read-only Domain Controllers
- Schema Administratoren

Bei der Überprüfung der Passwort-Berechtigung des RODCs gilt vorrangig die "Deny-Liste". Befindet sich das Konto in dieser Liste, wird das Passwort nicht an

den RODC repliziert. Ist das Konto nicht in der Deny-Liste, aber in der Allow-Liste, kann der RODC das Passwort auf Anfrage (eine Anforderung, ein einzelnes Objekt und auch nur die "Secrets" dessen zu replizieren) erhalten. Diese Gruppen dienen dazu, zu steuern, wer sich an der Domäne anmelden kann, sollte die WAN-Leitung einmal nicht funktionieren.

Sollte es einen sicherheitsrelevanten Vorfall auf einem RODC geben – sei es, dass ein Abbild von der Festplatte erstellt wurde oder eine Festplatte oder sogar der RODC komplett verschwunden sind – wird im AD protokolliert, wessen Passwörter an welchem RODC zwischengespeichert wurden. Löschen Sie ein solches RODC-Konto, berichten die Managementoberflächen, welche Passwörter alle auf diesen RODC repliziert wurden, und bieten an, die Passwörter zurückzusetzen oder zumindest eine Liste zur Verfügung zu stellen, damit Sie den Anwendern nahelegen, ihr Passwort schnellstens zu ändern.

Best Practices der Kennwortreplikation

Jetzt könnten Sie natürlich alle Domänenbenutzer in der Erlaubt-Liste aufnehmen, was die einfachste Option wäre. Wie sehen aber die Best Practices hierfür aus? Zunächst sollte es in vielen Umgebungen ausreichen, nur eine Deny-Liste zu pflegen. Neben den standardmäßig vorgegebenen Konten sollten Sie hier insbesondere Gruppen hinzufügen, die Administrative Konten enthalten, die nicht in einer der bereits verweigerten Gruppen mit aufgeführt sind. Ein klassisches Beispiel hierfür sind Konten, die für die Delegation von Berechtigungen im Active Directory verwendet werden, um die Administration im Unternehmen aufzuteilen. Deren Passwörter sollten nicht auf RODCs repliziert werden.

Erstellen Sie die Erlaubt-Liste am besten einmal pro Standort. Damit vermeiden Sie, dass reisende Benutzer ihr Passwort auf jedem RODC ablegen und damit zwangsweise zurückgesetzt würden, wenn mit einem RODC etwas passiert. Erstellen Sie deshalb sinnvollerweise eine Gruppe mit den Anwendern, die einem bestimmten Standort zugeordnet sind. Häufig existiert in Unternehmen sowieso schon eine

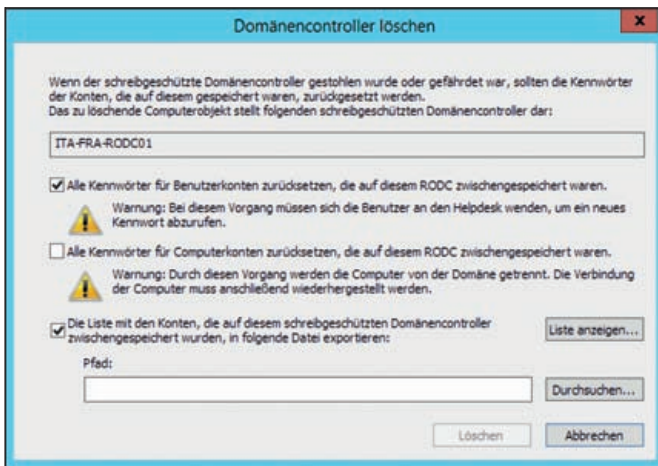


Bild 3: Wird der RODC gelöscht, erhält der Administrator automatisch die Aufforderung, die zwischengespeicherten Passwörter der Konten zurückzusetzen

Verteilerliste für die Anwender pro Standort, um lokale Events kommunizieren zu können. Kann diese Verteilerliste auch für Sicherheitsgruppen verwendet werden – beziehungsweise umgewandelt werden, denn Sicherheitsgruppen können als Verteilerlisten dienen –, können Sie auch gleich diese verwenden.

Des Weiteren dürfen Sie die Konten der Domänenmitglieder nicht vergessen, die sich in dem Standort befinden. Wird ein Computer gestartet, authentifiziert er sich zunächst gegenüber dem AD, bevor seine gesicherte Verbindung verwendet wird, um Benutzer zu authentifizieren. Es würde also nichts bringen, nur Benutzerkonten in die Erlaubt-Liste mit aufzunehmen. Bei den Computerkonten können Sie sich überlegen, ob Sie diese in die Erlaubt-Liste pro Standort aufnehmen oder ob Sie diese dann doch in die globale Erlaubt-Liste setzen, da die Computerkonten gegebenenfalls schneller zurückgesetzt sind und Desktops seltener reisen.

tigen. Standardmäßig wird dies nicht gemacht, doch dient die Gruppe genau dem Zweck, den Server zu verwalten, wenn er nicht mit einem vollen DC kommunizieren kann. Daher muss der Gruppe erlaubt werden, das Passwort auf dem RODC vorzuhalten. Sollte dies nicht bei der Installation passiert sein, können Sie über die Computereigenschaften des RODCs in der Registerkarte "Kennwortreplikationsrichtlinie" die Gruppe noch hinzufügen. Bei der neuen Active Directory-Verwaltungskonsole (oder Active Directory Administrative Center) finden Sie die Registerkarte unter den Erweiterungen in den Computereigenschaften.

Kennworte im Noffall zurücksetzen

Der RODC ist für unsichere Umgebungen vorgesehen. Daher wird für jeden RODC wie erwähnt protokolliert, welche Anwender sich gegen ihn authentifiziert haben und welche Passwörter dorthin repliziert wurden. Den Vergleich beider Lis-

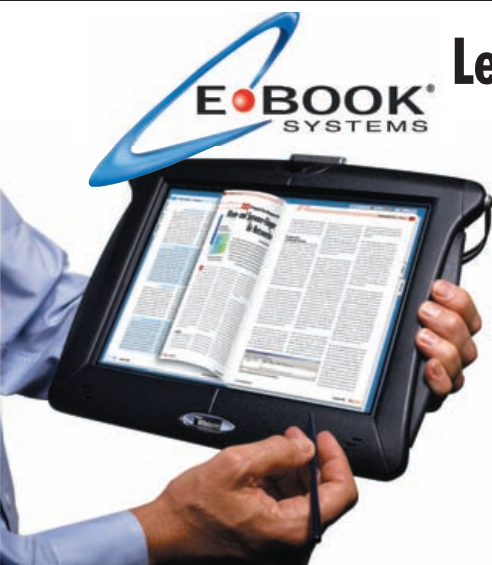
ten kann der Administrator auch verwenden, um zu überprüfen, dass die Erlaubt-Liste richtig gepflegt ist. Sollte der RODC aus der Domäne entfernt werden müssen, erhalten Sie automatisch die Warnung, dass alle Kennwörter der Konten, die auf dem RODC gespeichert waren, zurückgesetzt werden sollten. Sie können dann wählen, die Kennwörter für Benutzerkonten oder von Computerkonten zurückzusetzen, eine Liste anzuzeigen oder zu exportieren. Auch außerhalb des Löschdialogs können Sie die Informationen erhalten, indem Sie in der Registerkarte "Kennwortreplikationsrichtlinie" die Schaltfläche "Erweitert" drücken.

ten kann der Administrator auch verwenden, um zu überprüfen, dass die Erlaubt-Liste richtig gepflegt ist. Sollte der RODC aus der Domäne entfernt werden müssen, erhalten Sie automatisch die Warnung, dass alle Kennwörter der Konten, die auf dem RODC gespeichert waren, zurückgesetzt werden sollten. Sie können dann wählen, die Kennwörter für Benutzerkonten oder von Computerkonten zurückzusetzen, eine Liste anzuzeigen oder zu exportieren. Auch außerhalb des Löschdialogs können Sie die Informationen erhalten, indem Sie in der Registerkarte "Kennwortreplikationsrichtlinie" die Schaltfläche "Erweitert" drücken.

Fazit

Der Read-Only Domänencontroller ist eine gute Option, um unsichere Standorte abzusichern, in denen keine physikalische Sicherheit mit Zutrittskontrolle für volle Domänencontroller gegeben ist, aber trotzdem die Anmeldezeiten kurz gehalten werden sollen, oder in denen die WAN-Verbindungen nicht zuverlässig genug arbeiten.

Vor der Implementation der RODCs müssen Sie allerdings prüfen, ob kritische Anwendungen wie Exchange einen vollwertigen Domänencontroller benötigen. Des Weiteren muss geprüft werden, inwieweit der Einsatz eines RODCs sinnvoll ist, wenn keine zentrale Anbindung möglich ist. Und vor allem sollten Sie sich Gedanken darüber machen, wie Sie mit den Konten umgehen, die sich anmelden können, wenn das WAN nicht verfügbar ist, sowie wessen Kennwörter niemals gecached werden sollen und wie mit der Administration des RODC umgegangen werden soll. (dr)



Lesen Sie den IT-Administrator als E-Paper

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

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

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

www.it-administrator.de/magazin/epaper



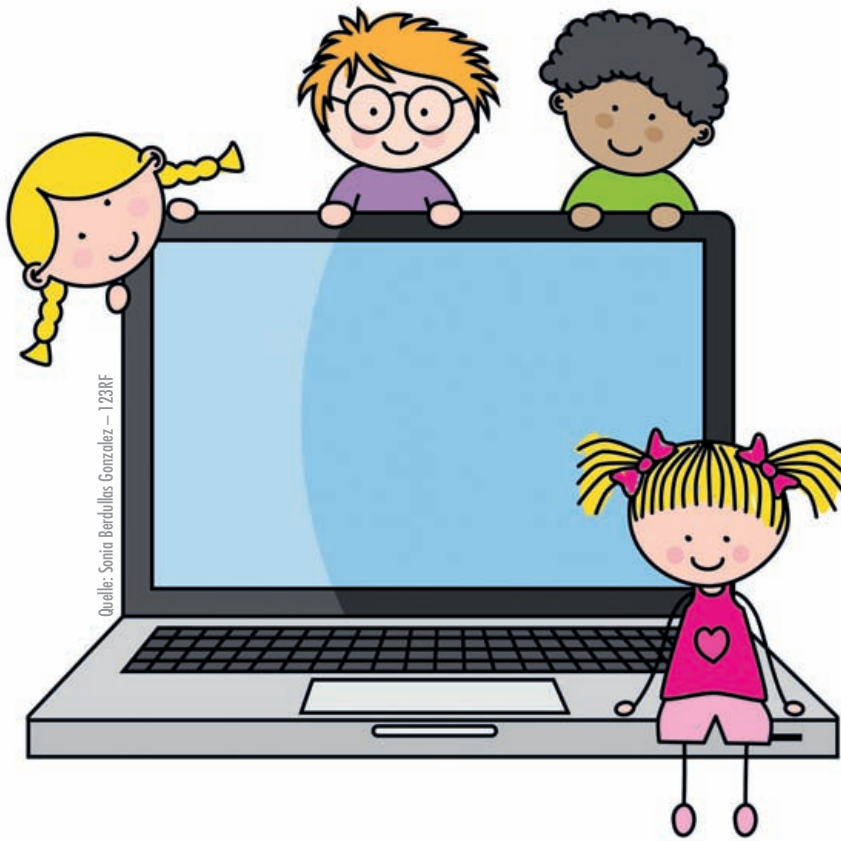
NEU! Jetzt auch mit App fürs iPad!



Microsoft System Center 2012 (3)

Die kleinen Geschwister

von Thomas Joos



Quelle: Sonia Berdullas Gonzalez - 123RF

Die ersten beiden Teile unserer Workshopserie brachten Ihnen die bekannten Managementwerkzeuge wie Configuration Manager oder Virtual Machine Manager in ihren neuesten Ausprägungen näher. Doch da Microsoft das System Center 2012 nur noch als Komplettpaket anbietet, erwerben Unternehmen auch weniger bekannte Werkzeuge der Suite automatisch. Diese dienen dem Virenschutz, dem Backup und dem Support und sind durchaus einen Blick wert, wie der abschließende Teil unserer Systems Center 2012-Reihe zeigt.

Da nach der neuen Lizenzierung des System Center 2012 ohnehin immer alle Produkte im Gesamtpaket integriert sind, sollten sich Unternehmen auch die Bestandteile näher ansehen, die sie bisher nicht genutzt haben. Vor allem die Sicherungslösung Data Protection Manager (DPM) und der Virenschutz Forefront Endpoint Protection (FEP) bieten einen echten Mehrwert für Unternehmen, die ohnehin schon das System Center einsetzen. Aber auch andere, meist wenig bekannte Werkzeuge sind unter Umständen sehr nützlich:

- Der System Center Data Protection Manager 2012 stellt die Datensicherungslösung im System Center dar. Das Werkzeug sichert alle Server im Netzwerk und erlaubt, die Sicherungen zentral zu verwalten. Insbesondere ist die Software für die Sicherung und Wiederherstellung von Exchange, SQL und SharePoint sowie Hyper-V optimiert.
- System Center Endpoint Protection 2012 bietet Virenschutz, der sich mit SCCM verwalten und verteilen lässt.
- Im System Center Service Manager

2012 liegt der Fokus auf der Anbindung als zentrale Verwaltungsoberfläche und Knotenpunkt für alle System Center-Produkte im Unternehmen sowie der Bildung von Schnittstellen und deren Verknüpfung und Automatisierung.

- Der System Center Orchestrator 2012 ermöglicht die Automatisierung von IT-Prozessen.
- System Center App Controller 2012 soll dabei helfen, Anwendungen im Unternehmen zentral zu verwalten.

Backup & Recovery mit Data Protection Manager 2012

Mit System Center Data Protection Manager 2012 bietet Microsoft die neue Version seiner Lösung zur Datensicherung im Unternehmen. Neben herkömmlichen Dateien unterstützt das Produkt auch die Online-Datensicherung von Exchange-Datenbanken, SharePoint oder SQL Server. DPM ist daher eine ernst zu nehmende Alternative zu gängigen Datensicherungsprodukten von Drittherstellern. In der neuen Version lassen sich sogar einzelne Items in SharePoint 2010

sehr leicht wiederherstellen. DPM ist vor allem für die Datensicherung auf Festplatten und Backup-To-Disk optimiert. Das Tool kann aber auch, wie seine Vorgänger, weiterhin Daten auf Band sichern. Bei der Backup-To-Disk-Variante repliziert DPM Dateien auf den verwalteten Festplattenspeicher. Unternehmen, die bereits den Vorgänger DPM 2010 einsetzen, können die Server direkt zu DPM 2012 aktualisieren. In DPM 2012

Unternehmen, die bisher System Center noch nicht einsetzen, können die einzelnen Anwendungen auch testen. Dazu stellt Microsoft Testversionen der einzelnen Programme zur Verfügung [1]. Die einzelnen System Center-Programme unterstützen allerdings noch nicht oder zumindest eingeschränkt Windows Server 2012 und Windows 8. Erst durch das Service Pack 1 für die verschiedenen System Center-Produkte lassen diese sich auch an Windows Server 2012 anbinden. Das ist vor allem für die Produkte Configuration Manager, Operations Manager und Virtual Machine Manager wichtig. Wichtige Informationen und Anleitungen zum System Center sind auch im Technet zu finden [2].

System Center 2012 testen



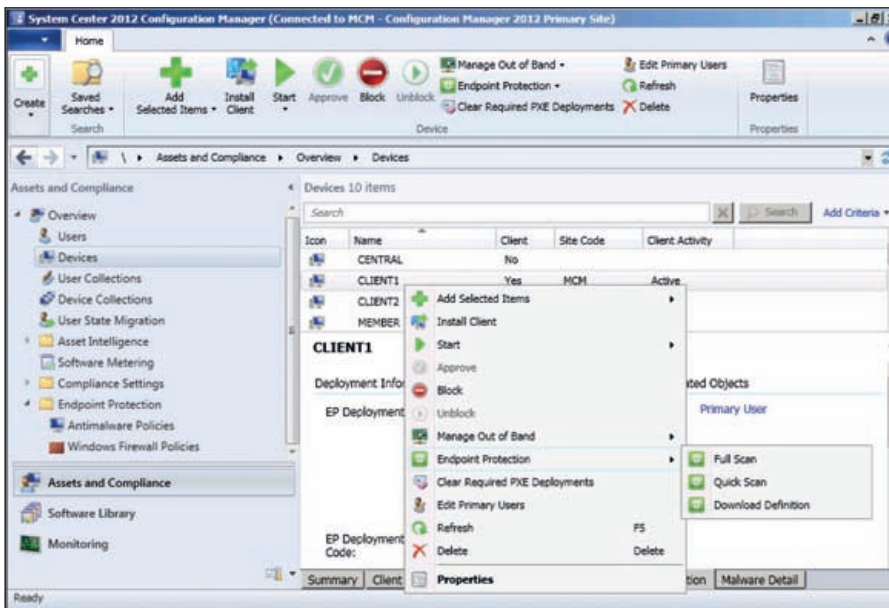


Bild 1: Der Virenschutz von Forefront Endpoint Protection 2012 integriert sich in den Configuration Manager und erlaubt so beispielsweise einen zentralen Scan der Clients auf Malware

arbeiten mehrere Server jetzt deutlich besser zusammen.

Der große Unterschied zu vielen anderen Sicherungsprodukten ist, dass DPM nicht die kompletten geänderten Da-

teien, zum Beispiel Exchange-Datenbanken, erneut überträgt, sondern nur die geänderten Datenblöcke innerhalb dieser Dateien. Bereits übertragene Datenblöcke überspringt DPM. Um die geänderten Blöcke zu erkennen, ver-

wendet DPM nicht das NTFS-Journal des Dateisystems, sondern direkt die Bitmap. So kann der Server sehr schnell und zuverlässig erkennen, welche Blöcke auf der Festplatte geändert sind und diese sichern. Setzen Unternehmen mehrere DPM-Server ein, lassen sich diese zentral verwalten und über die Verwaltungskonsole remote konfigurieren und verwalten. Mehrere DPM-Server können in DPM 2012 außerdem auf eine einzelne Datenbank zur Konfiguration zugreifen (DPMDB).

Damit DPM eine Sicherung durchführen kann, muss auf allen geschützten Servern ein Agent vorhanden sein, der mit dem DPM-Server eine Verbindung aufbaut. Die Clients lassen sich übrigens einfach über die Verwaltungskonsole von DPM im Netzwerk verteilen. Neben der manuellen Installation über die Konsole besteht auch die Möglichkeit, den DPM-Client per Softwareverteilung auszubringen.

Gemeinsame Systemdaten mehrerer Server fasst DPM zusammen und sichert nur

Bestellen Sie jetzt das IT-Administrator Sonderheft 1/2012!

180 Seiten Praxis-Know-how rund um das Thema

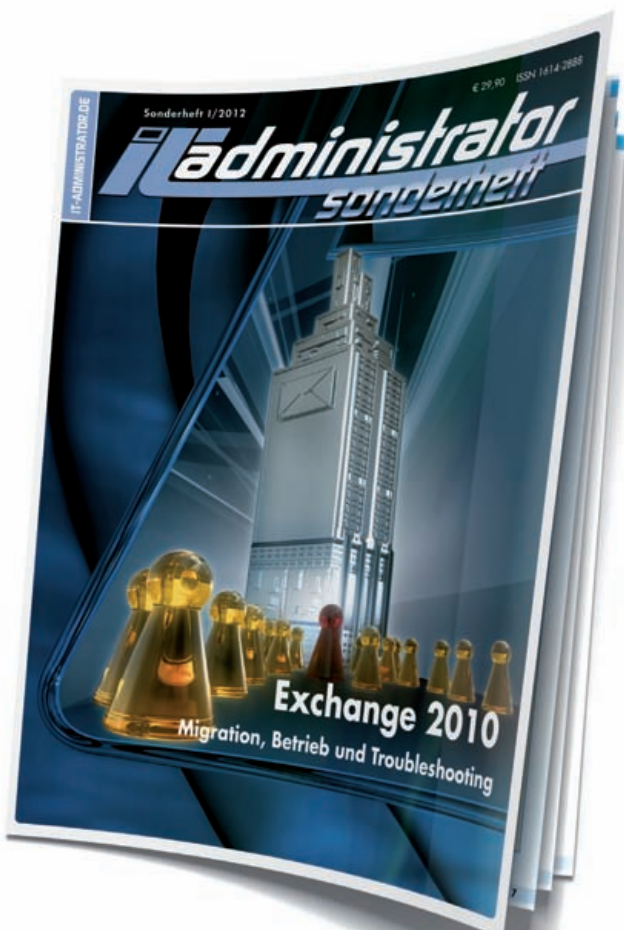
Exchange 2010

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

* IT-Administrator Abonnenten erhalten das Sonderheft 1/2012 für € 24,90. Nichtabonnenten zahlen € 29,90.
Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier
www.it-administrator.de/kiosk/sonderhefte/



beim ersten Server das komplette Betriebssystem. Das hat den Vorteil, dass sich neben den Daten auch ganze Server wiederherstellen lassen, aber nur so wenige Daten wie möglich in der Sicherung vorhanden sind. Das ist vor allem bei der Sicherung von Hyper-V-Hosts eine wichtige Funktion. Generell unterstützt die neue Version Hyper-V wesentlich besser und kann zwischen Hosts und virtuellen Maschinen besser unterscheiden. Das erspart Daten in der Sicherung und beschleunigt die Sicherungszeit.

DPM ist in der Lage, die Sicherungs-Volumen automatisch zu verwalten und zu vergrößern, wenn der Plattenplatz für die Sicherung nicht mehr ausreicht. Administratoren können dazu bei der Einrichtung festlegen, welche Volumes DPM verwalten soll und auf welchen Datenträgern DPM über das Recht verfügt, Volumes zu vergrößern. Neben der Sicherung und Wiederherstellung von Daten lassen sich mit DPM 2012 auch Disaster Recovery-Vorgänge durchführen, zum Beispiel die vollständige Wiederherstellung einer Share-Point-Farm. DPM sichert auf Wunsch alle 15 Minuten die Daten von Exchange-Servern ab Version 2003 SP2 bis 2010 SP2 im laufenden Betrieb. Genauso leicht wie die Sicherung ist die Wiederherstellung dieser Daten. Da DPM immer die ganze SQL-Instanz sichert, erkennt DPM neue Datenbanken und integriert diese automatisch in die Datensicherung.

DPM kann auch Daten von virtuellen Computern sichern, die zur Live Migration vorgesehen sind. Ebenfalls möglich ist die Wiederherstellung einzelner Daten innerhalb von virtuellen Festplatten (VHD). Virtuelle Computer lassen sich nicht nur auf der ursprünglichen Host-Maschine wiederherstellen, sondern auf jedem anderen Hyper-V-Host in der Infrastruktur. Daten von Arbeitsstationen mit Windows Vista, XP und Windows 7/8 lassen sich ebenfalls sichern.

Virenschutz mit Forefront Endpoint Protection 2012

Bestandteil des System Center-Pakets ist Microsoft Forefront Endpoint Protection 2012 (FEP). Hierbei handelt es sich um einen Virenschutz für PCs und Server, der



Bild 2: Auch Berichte zu Alarmen und Virenmeldungen lassen sich zentral verwalten und anzeigen – eine eigene Verwaltungskonsolle für Malwareschutz ist also nicht notwendig

sich mit den anderen Produkten im System Center überwachen lässt. FEP bietet aber keine eigene Verwaltungsoberfläche, sondern verwendet den System Center Configuration Manager. Mit Endpoint Protection 2012 können Administratoren den Virenschutz direkt aus System Center Configurations Manager 2012 steuern und mit Operations Manager 2012 überwachen. Wer FEP einsetzt, muss allerdings auch auf System Center Configurations Manager setzen. Als alleinstehendes Produkt macht FEP mangels fehlender eigener Server-Infrastruktur keinen Sinn.

Basis von FEP sind die Antimalware-Policies. Diese steuern Sie in der Verwaltungsoberfläche des System Center Configuration Managers. In der Konsole lassen sich verschiedene Richtlinien erstellen und damit individuell an die verschiedenen Server und Computer im Unternehmen anpassen. Eine Richtlinie besteht aus einem Satz von Einstellungen, in denen sich festlegen lässt, wann ein Client nach Viren suchen soll, wie das Verhalten der Software ist, wenn ein Virus entdeckt wird und ob die Software auch Netzlaufwerke und E-Mails nach Viren durchsuchen soll.

FEP bindet sich in die Verwaltungswerkzeuge des System Center ein und erlaubt über das Netzwerk den Scan von Computern. Neben dem Virenschutz kann FEP über die Configurations Manager-Konsole

auch Firewall-Einstellungen auf Rechnern vorgeben. Auf diese Weise ist sichergestellt, dass auf den PCs nicht nur der Virenschutz läuft, sondern auch die Firewall. Auch hierbei sind wieder Policies im Einsatz, die sich verschiedenen Sammlungen zuordnen lassen. Die Überwachung findet in einer einheitlichen Konsole statt. Hierzu hat Microsoft in der neuen Version auch die Berichte deutlich verbessert.

Erstellen Sie verschiedene Policies für den Virenschutz oder die Firewall-Konfiguration, lassen sich diese direkt in der Konsole verschiedenen Sammlungen zuordnen und auch die Prioritäten entsprechend anpassen. Neben den Standardsammlungen können Sie auch zusätzliche Sammlungen anlegen und manuell entsprechende Endgeräte hinterlegen. Durch die Integration des Virenschutzes in das System Center ist keine getrennte Überwachung von Alarmen notwendig, sondern Informationen und Benachrichtigungen des Virenschutzes sind direkt in das System Center eingebunden und lassen sich über eine einheitliche Konsole abrufen. Außerdem können Sie eigene Berichte erstellen, die den Virenschutz berücksichtigen.

Administratoren können im System Center die Verwaltung verschiedener Aufgaben an Benutzer delegieren. Dazu bietet das System Center vorgefertigte Verwaltungsrollen an, zum Beispiel zur Verwaltung von FEP. Na-



türlich lassen sich auch eigene Rollen mit entsprechenden Rechten anlegen. Das Prinzip ist ähnlich zu Exchange Server 2010.

Zentraler Support mit dem Service Manager

Mit System Center Service Manager (SCSM) bietet Microsoft eine zentrale IT-Service-Desk-Lösung an, die die verschiedenen System Center-Produkte miteinander verbindet und eine zentrale IT-Prozess-Verwaltung auf Industriestandards ermöglicht. SCSM stellt Prozesse zur Incident- und Problemlösung, für das Change-Management und für das Asset-Lifecycle-Management bereit. Als Plattform für die Automatisierung von IT-Prozessen basiert SCSM auf Industrie Best Practices wie dem Microsoft Operations Framework (MOF) oder der IT Infrastructure Library (ITIL) und verbindet andere Produkte aus der System Center-Reihe mit den IT-Prozessen in Unternehmen. Auch die Integration der Produkte anderer Hersteller in die Prozessreihe ist möglich, sodass Unternehmen eine zentrale Verwaltungsplattform und Reportinglösung erhalten, die eng mit System Center-Produkten zusammenarbeitet.

Meistens liegt das Problem vor allem in größeren Umgebungen darin, diese Produkte mit den IT-Prozessen und den ITIL- oder MOF-Reglements zu verbinden. Aus diesem Grund ist eine zentrale Schnittstelle für technische Produkte und Anwendungen zur Überwachung der IT-Prozesse notwendig, vor allem im Bereich Change-Management oder Incident-Management. Dabei geht es nicht um eine technische Konsole, sondern die effiziente Verbindung von Überwachung, Konfiguration und damit einhergehendem Change-Management. SCSM bildet Schnittstellen zwischen den verschiedenen Produkten in der System Center-Reihe, verknüpft und automatisiert Vorgänge. Requests kann SCSE auf Wunsch selbständig erstellen, Änderungen durchführen und Maßnahmen dokumentieren. Verwalten und konfigurieren können Sie die Anwendungen über eine übersichtliche und einheitliche Benutzeroberfläche.

Die Software hat die Aufgabe, Supportanfragen von Benutzern zu verwalten und

deren Bearbeitung im Unternehmen zu verbessern, zu überwachen, zu dokumentieren und nachvollziehbar zu machen. Bestandteile sind Incident-, Problem-, Change- sowie Asset- und Konfigurationsmanagement. Administratoren erkennen schnell die enge Anbindung an MOF oder ITIL. Allerdings ist einiges an Wissen um SCOM und SCCM sowie eine bereits erfolgte Integration von ITIL oder MOF im Unternehmen notwendig.

Mithilfe von Service Manager-Konnektoren lassen sich Prozesse der System Center-Produkte zusammenfassen, es kann auf deren Daten zugegriffen werden und es ist möglich, Dienste beziehungsweise Prozesse zu automatisieren. Zusätzlich bindet

sich die Software in das Active Directory ein, um Workflows leichter und konsistenter zu unterstützen sowie Vorfälle direkt mit Benutzerkonten von IT-Mitarbeitern oder Anwendern zu verknüpfen. Im Fokus stehen dabei Service-Desk-Funktionen, die sich leicht nutzen und anpassen lassen, aber dennoch umfassend sind und eine End-to-End-Automatisierung von IT-Prozessen bieten – unabhängig von der eingesetzten Hard- und Software.

Ein interessantes Szenario ist die Anbindung an Hyper-V zusammen mit System Center Virtual Machine Manager. Bei der Integration von SCSM und SCVMM wird zum Beispiel ein Change-Request für die Aktualisierung eines Servers initi-

Fast Lane, die Spezialisten für:

Training und Consulting rund um Virtualisierung, Cloud- und Data Center-Technologien



Cloud Computing, Data Center und Virtualisierungs-Trainings, z.B.:

- FlexPod for Account Managers (FPAM)
- FlexPod for VMware Essentials (FPVE)
- FlexPod for VMware Administration (FPVA)
- FlexPod for VMware Design & Implementation (FPVI)
- Implementing Enhanced Secure Multi-Tenancy Solutions (IESMT)
- Cisco Virtualization Experience Infrastructure (VXI) Curriculum
- Virtualisierung: Konzepte, Potenziale & Risiken (VIRT)
- Cloud Computing Overview (CLOUD)
- Cloud Computing Security Knowledge - Plus (CCSKP)
- Data Center Unified Computing Implementation (DCUCI)
- Implementing Cisco Data Center Unified Fabric (DCUFI)
- Implementing Cisco Storage Networking Solutions (ICSNS)
- VMware vSphere 5: Install, Configure, Manage (VICM)
- VMware vCloud: Deploy & Manage the VMware Cloud (VCDM)
- VMware View: Install, Configure, Manage (VIEW)
- Data ONTAP 8.0 7-Mode Administration (D7ADM)
- Data ONTAP Cluster-Mode Administration (DCADM)
- Symantec Backup Exec Administration (BE2010)
- Symantec NetBackup Administration (NBUW7)

Erfahren Sie mehr unter www.flane.de oder rufen Sie uns an: **040 25334610**.



Cisco Top Relevance Award EMEAR 2012 • Cisco European Learning Partner of the Year 2009, 2010 & 2011
NetApp Partner Award 2011 • VMware EMEA Training (VATC) Partner of the Year 2012

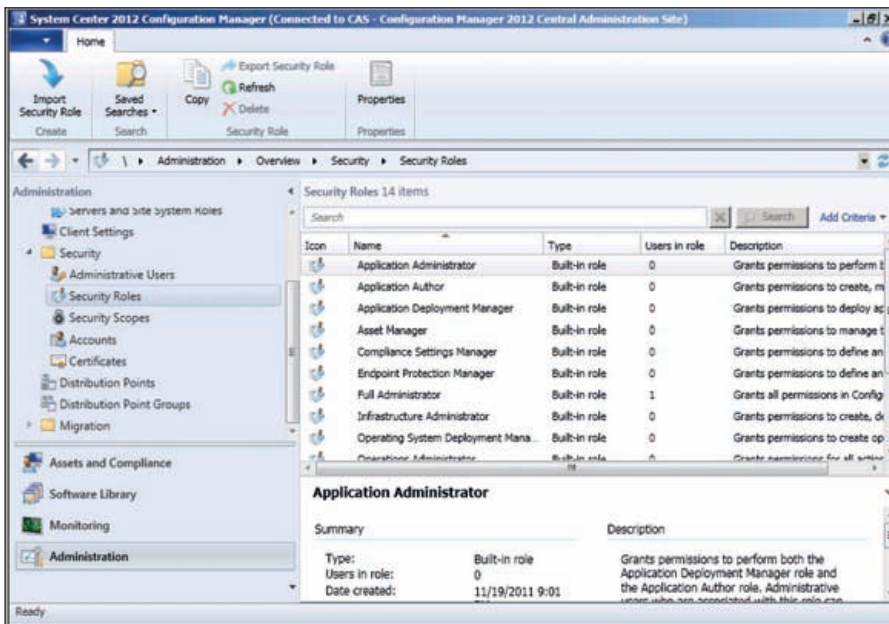


Bild 3: Berechtigungen lassen sich im System Center 2012 über vordefinierte Rollen an Anwender vergeben, um so gezielt Administrationsaufgaben zu delegieren

iert. SCVMM kann den entsprechenden Host automatisch in den Wartungsmodus versetzen, während SCSM die Aktualisierung dokumentiert.

Für die Endbenutzer-Unterstützung betreiben Sie das zentrale Serviceportal mit einer Wissensdatenbank und können Software verteilen, Kennwörter zurücksetzen sowie Incidents erstellen und verwalten. Anwender unterstützen Sie durch die verknüpfte Wissensdatenbank und die Möglichkeit, Probleme eigenständig zu lösen. SCSM dokumentiert dabei auch diese Änderungen entsprechend.

Orchestrator 2012 automatisiert Workflows

System Center Orchestrator (SCO) ermöglicht die Erstellung von automatisierten Workflows der verschiedenen System Center-Produkte. Auf diese Weise können Administratoren zum Beispiel Aufgaben für DPM erstellen. Die Software enthält vorgefertigte Workflows und Automatisierungsansätze sowie Beispiele für die

wichtigsten Aufgaben in der Verwaltung von Rechenzentren.

Bestandteil der Lösung sind auch Anleitungen und Lösungen für Virtual Machine Lifecycle Management, Incident-Ticket-Management, Migration von virtuellen Maschinen und Cloud Computing. Die Workflows können sich aber nicht nur über die Tools in System Center erstrecken, sondern nutzen auch HP, CA, BMC, EMC und VMware. Orchestrator bietet, zusammen mit dem Service Manager, eine Plattform zur Automatisierung der IT-Prozesse auf Basis von MOF und ITIL.

Anwendungen im Griff mit App Controller 2012

App Controller ist das neueste Tool in System Center. Es soll Anwendern im Netzwerk ermöglichen, die eigenen Anwendungen in der Cloud besser zu verwalten. Das Tool trägt der klaren Cloud-Ausrichtung von System Center Rechnung. Der App Controller bietet ein Self Service-Portal, mit dem Anwender Aufträge und Service-Anforderungen für Apps stellen können. Es besteht die Möglichkeit, Remotedesktop-Verbindungen zu verwalten oder auch virtuelle Maschinen zu starten und herunterzufahren.

Vor allem in Virtual Desktop-Infrastrukturen kann der Einsatz sinnvoll sein, wenn Anwender zusätzlich noch mit Remote-

desktopdiensten und Heimarbeitsplätzen arbeiten. Der Einsatz von App Controllern macht vor allem in großen Unternehmen Sinn, bei denen Anwendungen über Kostenstellen abgerechnet werden.

Fazit

Die Produkte in System Center 2012 schaffen durch das Zusammenspiel der einzelnen Programme einen echten Mehrwert gegenüber anderen Herstellern. Allerdings macht der Einsatz auch nur dann Sinn, wenn mehrheitlich Microsoft-Server im Einsatz sind. Zwar lassen sich auch Linux/Unix-Server verwalten, allerdings spielt das System Center hier nicht seine wahre Stärke aus.

Da bisher vor allem Configuration/Operations Manager und der Virtual Machine Manager häufig im Einsatz sind, fasste Microsoft die bisher getrennten Bestandteile zu einem festen Paket zusammen, damit auch die anderen Produkte, die Microsoft teilweise teuer dazugekauft hat, endlich einigermaßen häufig eingesetzt werden. Dabei schauen vor allem Unternehmen in die Röhre, die bisher nur ein einzelnes Produkt im Einsatz hatten.

Was sicherlich Sinn ergibt, ist der Einsatz von Data Protection Manager und Forefront Endpoint Protection. Beide Produkte stehen Anwendungen von Mitbewerbern in nichts nach. Unternehmen, die schon einen Virenschutz und eine Datensicherungslösung einsetzen, werden natürlich ebenfalls nicht wechseln, können das aber zumindest in Erwägung ziehen. Der große Vorteil von Endpoint Protection ist die direkte Integration in System Center Configuration Manager. So entfällt die Verwaltung einer weiteren Server-Infrastruktur und Bedienung einer Konsole.

Produkte wie Orchestrator, Service Manager und App Controller sind sicherlich eher für sehr große Unternehmen geeignet. Ob der Mittelstand von diesen eher komplexen Tools profitiert, ist schwer abzuschätzen. Dennoch ist System Center 2012 eine Sammlung wertvoller Programme, die Administratoren entlastet und die Verfügbarkeit von Microsoft-Server-Produkten im Netzwerk sicherstellt. (jp)

[1] System Center 2012 plus optionaler Windows Server 2008 R2 SP1-Download
CBP41

[2] Informationen zum Microsoft System Center 2012
CBP42

Link-Codes





Windows PowerShell 3.0

PowerShell Web Access über Windows Server 2012

von Rolf Masuch

Mit der Version 3.0 der PowerShell wird neben vielen andern Funktionserweiterungen auch der PowerShell Web Access zur Verfügung gestellt – eine Funktion, die es ermöglicht, über ein Browserfenster ihre Serververwaltung von jedem beliebigen Ort aus durchzuführen. Aber vor dem Servermanagement vom Strand aus sind noch ein paar wenige Konfigurationen durchzuführen. PowerShell Web Access ist dabei keine Rolle, sondern ein Feature. Über den Servermanager ihres Windows Server 2012 können Sie den Server auswählen, der diese Aufgabe ganz im Sinne einer klassischen Gatewayserver-Installation übernehmen soll. Dabei kommt es sehr gelegen, dass Sie sich dazu nicht per Remote Desktop auf den Server direkt aufschalten müssen. Der Servermanager des Windows Server 2012 unterstützt das Hinzufügen von Rollen und Features auch zu einem entfernten Server, der in die Liste der verwalteten Server aufgenommen wurde.

Den Einstieg für das Hinzufügen einer Rolle oder eines Features finden Sie im oberen rechten Bereich des Servermanagers mit der Schaltfläche "Manage". Ein Wizard führt dann durch die einzelnen Schritte. Vermeiden Sie es dabei, die Rolle des Webservers manuell hinzuzufügen. Diese wird nämlich bei der Auswahl des Features "PowerShell Web Access" als fehlend festgestellt und die Nachinstallation automatisch angeboten. Dies ist die empfohlene Vorgehensweise, um alle notwendigen Komponenten zu installieren. Nach der erfolgreichen Installation steht bei einer Standardkonfiguration der Unterordner "pwsa" über die Management-Konsole des Webservers zur Verfügung. Es empfiehlt sich, hier die ersten Tests zur

Erreichbarkeit durchzuführen. Die Links dazu befinden sich auf der rechten Seite der Management-Konsole. Der Zugriff über Port 80 sollte zu einer Fehlermeldung führen, da die Installation automatisch ein Eigenzertifikat für den Webserver generiert und den Zugriff ausschließlich über HTTPS ermöglicht. In einer produktiven Umgebung empfiehlt sich deshalb das Einbinden eines Server-Zertifikats über eine vertraute PKI.

Die Session-Konfiguration

Leider ist aber selbst nach der erfolgreichen Installation die Nutzung des Web Access noch nicht möglich, denn es fehlt noch die Konfiguration der Zielsever. Die hierfür notwendigen Cmdlets ermitteln Sie leicht mit der PowerShell:

```
Get-Command *pssessionconfig*
```

Für den ersten Schritt benötigen Sie das Cmdlet "New-PSSessionConfigurationFile". Die Syntax zur Erzeugung einer Session-Konfigurationsdatei lautet

```
New-PSSessionConfigurationFile -Path .\PSWA.pssc
```


Dabei wird die Datei *PSWA.pssc* im aktuellen Verzeichnis erzeugt und kann mit dem nächsten Cmdlet "Test-PSSessionConfigurationFile" überprüft werden. Den nächsten und entscheidenden Konfigurationsschritt nehmen Sie über das Cmdlet "Register-PSSessionConfiguration" vor. Dieses fügt dem lokalen System einen Webservice "Endpunkt" hinzu, der – wie die Endpunkte des Remoting – nur für dieses Mal als namentlich konfigurierter Endpunkt genutzt werden kann. Im einfachsten Fall registriert der folgen-

de PowerShell-Befehl ihre Konfigurationsdatei *PSWA.pssc*:

```
Register-PSSessionConfiguration -Path .\PSWA.pssc -Name PSWA
```

Achten Sie dabei darauf, diesen Befehl in einer administrativen Shell auszuführen und die danach folgenden Fragen mit "Y(es)" zu beantworten. Nach der erfolgreichen Konfiguration des Zielsevers kann nun auf der Webseite des Windows PowerShell Web Access Servers unter Angabe des (Ziel-)Servernamens, der entsprechenden Benutzerkennung sowie des richtigen Endpunkts das Formular des Web Access Servers gefüllt werden. Hilfe zur detaillierten Konfiguration bietet übrigens die gegebenenfalls über *Update-Help* aktualisierte lokale Hilfe oder die Online-Version der Hilfe zur Session-Konfiguration [1] und ihrer Dateien [2].

Fazit

Die Funktionalität des Windows PowerShell Web Access ermöglicht die gesicherte Nutzung der PowerShell über die Grenzen Ihres Netzwerks hinweg. Die Konfiguration der Endpunkte ermöglicht es, die zur Verfügung stehenden Befehle für den jeweiligen Verwendungszweck einzuschränken. Die in der Hilfe beschriebenen Beispiele stellen erst den Anfang der Möglichkeiten dar. (dr) 

[1] Microsoft-Infos zu "about_Session_Configurations" CBPF1

[2] Microsoft-Infos zu "about_Session_Configuration_Files" CBPF2

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.



Wie allgemein empfohlen, existiert in unserem Netzwerk eine **Namenskonvention für sämtliche Bestandteile des Netzwerks**. Entsprechend diesem Konzept haben wir die Server dann auch installiert. Durch einen **Firmenzusammenschluss kam es jedoch zu einer Änderung** der Namenskonventionen und eine Umbenennung der einzelnen Komponenten steht an. Windows-Server sollten hier ja eigentlich recht schmerzfrei sein, aber wie steht es mit einer **Umbenennung des Failover Clusters**?

Auch die Neutaufe eines Failover Clusters ist möglich – ein Cluster Name Object (CNO) lässt sich ohne Probleme umbe-

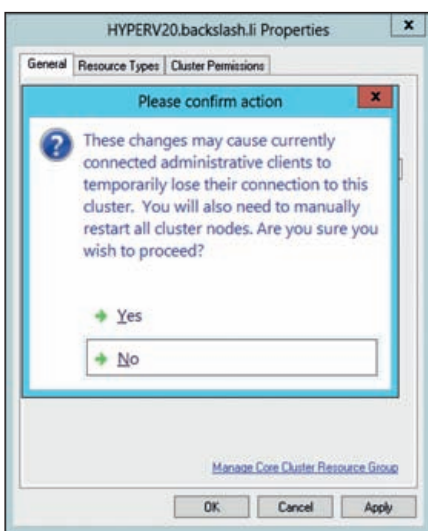
nennen. Am einfachsten führen Sie diese Änderung im "Failover Cluster Manager" unter "Properties" durch. Beachten Sie jedoch, dass diese Umkonfiguration eine kurze Unterbrechung der Verbindung zur Folge hat. Dies betrifft jedoch nicht die Cluster-Ressourcen selbst, sondern lediglich die Verbindungen zur Management-Konsole. Allerdings müssen Sie die Cluster Nodes nach der Änderung neu starten, damit die Änderungen aktiv werden. Über "Pause / Drain Roles" räumen Sie den Node einfach und schnell leer und setzen ihn in den Wartungsmodus. Seit Windows Server 2008 R2 können Sie eine derartige Aufgabe auch mit der PowerShell durchführen. Tippen Sie dazu folgenden Befehl ein:
`Import-Module FailoverClusters`
`$MyCluster = Get-Cluster -Name "Alter Name des Clusters"`
`$MyCluster.Name = "Neuer Name des Clusters"`

Weiter Informationen zum Umbenennen eines Failover Clusters finden Sie im Technet [Link-Code CBPE4]. Auch die dortige Auflistung der Failover Cluster-Cmdlets [Link-Code CBPE5] erweist sich in der Regel als äußerst hilfreich. (Michel Lüscher/ln)

SERVER TALK Weitere Informationen zu Server 2008 R2 und Hyper-V finden Sie auf www.server-talk.eu

Ansicht überleiten. Funktioniert eine derartige Umleitung auch mit Bordmitteln?

Schon seit Erscheinen der Preview-Versionen zu Windows 8 kursierten diverse Tweaks im Netz, wie sich der offiziell "Windows 8 style UI" getaufte Kachel-Look umgehen lässt. Die meisten dieser Wege funktionieren jedoch in der finalen Version des neuen Windows nicht mehr. Über eine bestimmte Registry-Änderung können Sie jedoch nach wie vor das direkte Schalten auf den Desktop bewirken. Drücken Sie dazu zunächst die Windows-Taste plus R und tippen Sie im Ausführen-Diaog *regedit* ein, um den Registry-Editor zu öffnen. Anschließend navigieren Sie links zu "HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Winlogon". Dort suchen Sie im rechten Fenster den Wert "Shell" und klicken doppelt darauf. Der per Default gesetzte Wert lautet "explorer.exe". Tragen Sie hier stattdessen die Zeichenfolge "explorer.exe /select,explorer.exe" ein. Beim Booten von Windows startet dann direkt der Desktop – allerdings mit einer kleinen Nebenwirkung: der Windows Explorer öffnet sich ebenso und zeigt den Benutzerordner an. Wurde die Änderung gespeichert, so wird der PC neu gestartet. Danach sollte Windows 8 direkt zum Desktop booten. Ein ganz spurloses Umschalten auf den Desktop ist mit Bordmitteln leider nicht möglich. Vielleicht ist es dann doch einfacher, mit einem simplen Drücken der Eingabetaste nach dem Start des Kachel-UI zum klassischen Arbeitsplatz zu wechseln. (ln)



Vor der Umbenennung eines Failover Clusters weist Windows auf die bevorstehende kurze Unterbrechung administrativer Zugriffe auf die Management-Konsole hin

Windows 8 ist ja mittlerweile im Handel und auch wir haben das neue Betriebssystem zu Testzwecken auf einem Rechner installiert. Bei der Steuerung mit Maus und Tastatur ist der Startbildschirm im Kachel-Look ja nicht wirklich hilfreich. Es gibt ja schon diverse Tools, die direkt auf die klassische Desktop-

Was mich bei der Nutzung von Windows 8 mit Maus und Tastatur manchmal stört, sind die aktiven Ecken am linken und rechten oberen Bildschirmrand. Links oben erscheint bei einer Mausbewegung ja die zuletzt geöffnete App und über die rechte Seite wird das Charms-Menü aufgerufen. Zu oft ist es mir aber schon passiert, dass ich beim Klicken in das obere Menü einer Anwendung versehentlich die aktiven Ecken ausgelöst habe. Gibt es irgendeinen Weg, um das Aufpoppen der Shortcuts im Eck zu verhindern?

Um die aktiven Ecken zu modifizieren beziehungsweise abzuschalten, führt der Weg auch hier wieder über die Registry. Unter "HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion" klicken Sie mit der rechten Maustaste auf den Eintrag "Immersive-Shell" und legen einen neuen Schlüssel mit dem Namen "EdgeUI" an. Auf diesen klicken Sie nun wieder mit rechts und schaffen einen neuen DWORD-Wert (32-Bit), den Sie "DisableCharmsHint" nennen und dessen Wert Sie per Rechtsklick von "0" auf "1" ändern. Dieser Eintrag deaktiviert das Aufklappen des Charms-Menüs, wenn sich die Maus in eine der rechten Ecken bewegt. Ebenfalls in "EdgeUI" können Sie mit dem DWORD-Wert (32-Bit) "DisableLTcorner" und einem Wert von "1" bewirken, dass die zuletzt geöffnete App in der linken oberen Ecke aufpoppt, wenn Sie den Mauszeiger dorthin bewegen. Übrigens können Sie die Charms-Leiste an der rechten Seite des Desktops jederzeit durch gleichzeitiges Drücken der Windows-Taste und C hervorzaubern. (ln)



Wir betreiben seit Kurzem eine SharePoint-Farm. Allerdings habe ich mich noch nicht so richtig in die Funktionen zur Erstellung von Berichten und Protokollen eingearbeitet beziehungsweise weiß nicht einmal, wie ich diese aufrufe. Können Sie mir hier weiterhelfen und kurz die Möglichkeiten und Settings zur Verwendung der Berichte erklären? Um über den Betrieb einer SharePoint-Installation stets auf dem Laufenden zu sein,

kommen die vordefinierten Administratorberichte in Frage. Um sich diese anzuzeigen, klicken Sie in der Zentraladministration auf "Überwachung" und anschließend im Bereich "Berichte" auf "Administratorberichte anzeigen". Wählen Sie dann auf der Seite "Administratorberichtbibliothek" den gewünschten Berichtsordner aus. Dort wählen Sie den gewünschten Bericht durch Klicken auf den entsprechenden Namen. Die meisten Berichte verfügen über Einstellungen und Filter, die Sie anpassen können, um die Ansicht anzupassen. Mit den Web Analytics-Berichten, die Sie im Bereich "Überwachung / Berichte" der Zentraladministration starten, lassen Sie sich das Nutzungsverhalten Ihrer SharePoint-Anwender anzeigen und sehen Nutzungsanalysen der verschiedenen Webseiten. Sie erhalten die Anzahl der Zugriffe sowie Details, wie zum Beispiel die Gesamtzahl der Nutzer und die verwendeten Browser. Integritätsberichte enthalten Verwendungsdaten von Websites und Websitesammlungen für einen Überblick über die Nutzung und Geschwindigkeit. Integritätsberichte stehen in der Zentraladministration nach einem Klick auf "Überwachung" zur Verfügung. Wählen Sie auf dieser Seite im Bereich "Berichte" den Link "Integritätsberichte anzeigen". Klicken Sie auf der Berichtsseite auf der Schnellstartleiste auf den Namen des Berichts, um den Bericht auf den Schirm zu bringen. Ihnen stehen verschiedene Filterkriterien zur Verfügung und Sie können einzelne Server oder Webanwendungen auswählen. (Thomas Joos/ln)

Ein Kollege hat mir bei Problemen in der SharePoint-Farm dazu geraten, doch einmal einen Blick auf die ULS-Protokolle zu werfen. Wie kann ich diese Protokolle anzeigen und verwalten? Auch eine Möglichkeit etwa zum Export zu Excel wäre sehr praktisch. Wie kriege ich das hin?

Mit den Daten aus den ULS-Protokollen (Universal Logging System) steht Ihnen ein hilfreicher Weg offen, um Probleme in der Farm zu erkennen und zu beheben. Sie können die protokollierten Einträge in der SharePoint 2010-Verwaltungshell filtern, auf unterschiedliche Weise anzeigen, sortieren, gruppieren und zu Excel 2010 exportieren. Verwenden Sie dazu das Cmdlet "Get-SPLogEvent". Die Syntax zur Filterung lautet:

```
Get-SPLogEvent | where-Object
{$_ .Level -eq [Information |
Warning | Error | Critical |
Verbose | Unexpected |
Monitorable | High | Medium]} | fl
```

Suchen Sie nach einer bestimmten Meldung, verwenden Sie:

```
Get-SPLogEvent | where-Object
{$_ .Message -like "*Zeichenfolge
der Ereignismeldung*"} | fl
```

So zeigt zum Beispiel

```
Get-SPLogEvent | where-Object
{$_ .Area -eq "SharePoint
Foundation"} | Out-GridView
```

eine Tabelle an. "Get-SPLogEvent | Out-GridView" ist der einfachste Weg, um alle Einträge in einer Tabelle anzuzeigen. Kopieren Sie die Spalten, die Sie in Excel verwenden wollen, und fügen Sie diese in Excel ein. (Thomas Joos/ln)

In der Regel überwachen wir in unserer SharePoint-Installation den Status von verschiedenen Workflows direkt im Browser. Auf diese Weise können wir schnell erkennen, welche Workflows aktuell in einer bestimmten Bibliothek oder Liste aktiv sind: Dazu navigieren wir zu der Liste oder Dokumentbibliothek mit dem Workflow, dessen Status wir überprüfen wollen, und suchen nach dem Element, für das wir den Status überprüfen wollen – die Workflowstatusspalte hat als Bezeichnung den Namen des Workflows. Gibt es denn noch eine andere, eventuell zielführendere Methode, um Workflows im Blick zu behalten?

Eine weitere Möglichkeit der Überwachung sind Workflowberichte. Es ist möglich, sich eine Liste aller verfügbaren Workflows für die Websitesammlung anzuzeigen, inklusive einer Zusammenfassung der Verwendung, wie oft diese Workflows jeweils zugeordnet wurden und wie viele Instanzen ausgeführt wer-

Viele weitere Tipps & Tricks sowie konkrete Hilfe bei akuten Problemen bekommen Sie auch im Internet bei unserem exklusiven Foren-Partner administrator.de. Über 60.000 registrierte Benutzer tauschen dort in über 100 Kategorien ihre Erfahrungen aus und leisten Hilfestellung. So wie der IT-Administrator das praxisnahe Fachmagazin für Administratoren ist administrator.de die Internetplattform für alle System- und Netzwerkadministratoren. www.administrator.de



den. Dazu wechseln Sie zur Website auf oberster Ebene der Websitesammlung und klicken im Menü "Websiteaktionen" auf "Websiteinstellungen". Dort navigieren Sie im Bereich "Websiteverwaltung" auf "Workflows". SharePoint Server 2010 bietet zwei vordefinierte Microsoft Excel-Berichte, die eine Analyse des Workflowverlaufs für jede Workflowinstanz ermöglichen. Der Aktivitätsdauerbericht zeigt, wie lange die Ausführung der einzelnen Aktivitäten in einem Workflow und wie lange die Ausführung aller Aufgaben in dem Workflow dauert. Der Abbruch- und Fehlerbericht zeigt, welche Workflows abgebrochen wurden oder wo Fehler aufgetreten sind. Um in SharePoint diese Berichte als Excel-Tabellen zu erhalten, navigieren Sie zu der Liste oder Dokumentbibliothek, die den Workflow enthält, für den Sie Berichte anzeigen wollen. Zeigen Sie auf ein in den Workflow eingebundenes Element, klicken Sie auf den angezeigten Pfeil und dann auf "Workflows". Dort klicken Sie im Bereich "Workflows ausführen" auf den Namen des Workflows. Befindet sich in diesem Bereich kein Workflow, ist aktuell auch keiner aktiv. Anschließend lassen Sie sich im Bereich "Workflowverlauf" unter "Workflowberichte anzeigen" den Bericht erstellen. Der Workflowverlauf enthält Informationen zu jedem Ereignis eines Workflows. Innerhalb von SharePoint 2010 findet als täglicher Auftrag "Automatischer Workflowcleanup" statt, um Workflowinstanzen und verbundene Aufgabeneingaben 60 Tage nach Beendigung oder Abbruch eines Workflows zu entfernen. Benötigen Sie diese Daten jedoch für die Fehlersuche und Protokollierung, können Sie den Auftrag "Automatischer Workflowcleanup" deaktivieren, indem Sie zunächst auf der Website für die Zentraladministration "Überwachung" wählen und dort im Bereich "Zeitgeberaufträge" auf "Auftragsdefinitionen überprüfen" klicken. Auf der nun angezeigten Seite finden Sie in der Spalte "Titel" den Link "Automatischer Workflowcleanup" für die Webanwendung, in der Sie die Funktion deaktivieren wollen. Klicken Sie auf der Seite "Zeitgeberauftrag bearbeiten" auf "Deaktivieren". Auf die gleiche Weise aktivieren Sie den Auftrag wieder.

(Thomas Joos/ln)



Wir nutzen den Citrix Receiver für HTML5 in Version 1.0 zum Ausrollen des nativen Citrix Receiver immer dann, wenn wir keine Möglichkeit haben, das Endgerät direkt zu managen – beispielsweise bei BYOD-Szenarien. Dies funktioniert für uns mit allen Grundfunktionen in der Regel auch sehr gut, jedoch kommt es beim Versuch, Anwendungen per HTTPS-URL aufzurufen, im Firefox-Browser mitunter zu folgender Fehlermeldung: "Exception: ... 'The operation is insecure.' Code: 18, nsresult: 0x80530012 (SecurityError) Location: ..." Wie lässt sich dieses Problem beheben?

Um das Starten von Anwendungen über eine HTTPS-Verbindung zuzulassen, müssen Sie lediglich eine kleine Änderung in der Konfiguration vornehmen. Führen Sie dazu folgende Schritte durch: Öffnen Sie einen neuen Tab in Firefox und geben Sie dort den Befehl `about:config` in die Adresszeile ein, um die erweiterten Konfigurations-Einstellungen aufzurufen. Suchen Sie in der Spalte "Preference Name" nach der Bezeichnung "network.websocket.allowInsecureFromHTTPS". Setzen Sie dann deren Wert auf "True", indem Sie auf die Zeile doppelklicken. Die Anwendungen lassen sich nun über HTTPS wie gewohnt ausführen. (Citrix/ln)

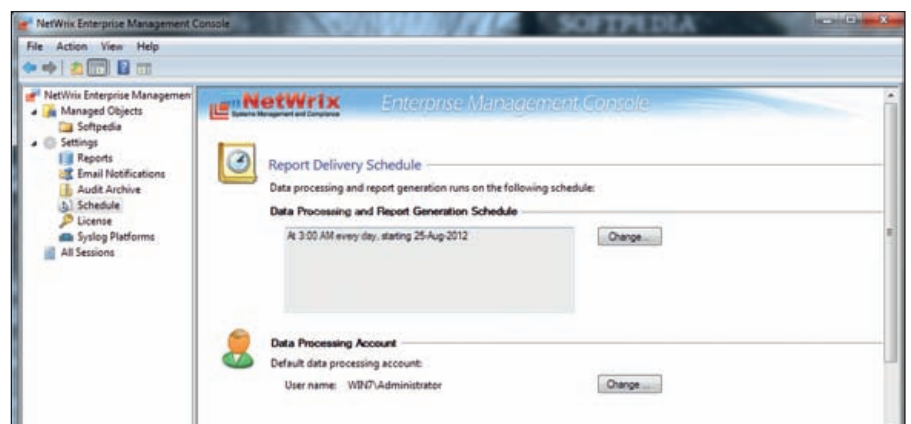


Tools

Ein nach wie vor oft unterschätztes Problem beim Monitoring der IT-Infrastruktur ist die Tatsache, dass die Überwachung von Servern, Clients oder Netzwerkgeräten zunächst meist lokal erfolgt und auch entsprechend aufgezeich-

net wird. Die Konsequenz bei einem IT-Notfall ist naheliegend: Der Administrator benötigt unter Umständen sehr viel Zeit, um an die für das Troubleshooting notwendigen Systemdaten zu gelangen, sofern er überhaupt Zugriff hat. Aber auch im störungsfreien Betrieb bietet eine zentrale Verfügbarkeit von Log-Daten zahlreiche Vorteile für IT-Abteilungen.

Wer für einen solchen Log-Daten-Sammeldienst kein IT-Budget einsetzen möchte, der sollte sich die Freeware-Edition von NetWrix Event Log Manager ansehen. Dieses Eventlog-Managementwerkzeug sammelt unternehmensweit gesammelte Daten, archiviert diese und erlaubt es zudem, IT-Verantwortliche zu alarmieren, sollten zuvor definierte Schwellenwerte überschritten werden. Der NetWrix Event Log Manager bietet dem IT-Verantwortlichen einen zentralen Sammelort für alle Log-Daten, die der Administrator dauerhaft im Blick behalten möchte. Dabei sammelt die Software die Daten nicht nur selbständig an den definierten Knoten ein, sie komprimiert und archiviert die Daten darüber hinaus. Für die Alarmierung gegen Grenzwerte definiert der Administrator für ein oder mehrere in der NetWrix Event Log Manager-Datensammlung berücksichtigten Geräte Werte, bei deren Über- oder Unterschreitung eine E-Mail an zuvor definierte Empfänger versandt wird. Unabhängig von solchen Alarmen lässt sich in dem Tool auch konfigurieren, dass eine bestimmte Personengruppe alle 24 Stunden eine Event-Übersicht per E-Mail erhält. Dabei setzt der Hersteller übrigens auf eine sehr einfache Bedienung: Die Einrichtung und Verwaltung aller Parameter erfolgt in einem einzigen Fenster.



Der NetWrix Event Log Manager sammelt Event-Informationen aus dem Netzwerk und versendet täglich einen Bericht der Ereignisse

Die freie Software ist auf die Überwachung von maximal 10 Servern/Domänencontrollern und 100 Clients beschränkt. (jp)
 Link-Code: CBPE1

Für den schnellen **Netzwerkcheck** ist das gute alte Pingen nach wie vor erste Wahl bei Administratoren. Ein kurzer Einsatz der Kommandozeile reicht dabei aus, um im Problemfall eine erste Diagnose zu erhalten und mit dieser Information dann gezielt auf die Suche nach der Ursache zu gehen. Und doch stammt der **Ping-Befehl** aus einer Zeit, in der WAN-Strecken nicht sonderlich verbreitet waren. Daraus resultierend erhält der IT-Verantwortliche von Ping keinerlei **Informationen über die immer wichtiger werdende Latenz**. Dies schränkt die Fehlersuche mit dem Standard-Ping erheblich ein.

Das hat sich wohl auch Windows-Guru Mark Russinovich gedacht und das kostenlose **PsPing** ins Netz gestellt. Genau wie beim bekannten Ping handelt es sich hierbei um ein Werkzeug für die Kommandozeile. Nach dem Download muss der Administrator die ausführbare Datei nur wie gewohnt aus der Kommandozeile starten, um **Latenz- und Bandbreitenwerte** der untersuchten Verbindung ebenso zu erhalten wie die gewohnten Ping-Informationen. Grundsätzlich stellt das Tool **vier Netzwerktests zur Verfügung**, deren Handhabung sich der Nutzer jeweils anzeigen lassen kann, in dem er den entsprechenden Parameter mit `psping -? [I|T|L|B]` übergibt:

- I: Verwendung für ICMP-Ping
- T: TCP-Ping-Optionen
- L: Parameter für Latenztests
- B: Einsatz als Bandbreitentest

Entscheidet sich der IT-Verantwortliche für einen **Test der Netzwerklatenz** mit PsPing, so stehen dafür Parameter bereit. Die Syntax des entsprechenden Befehls lautet für Server

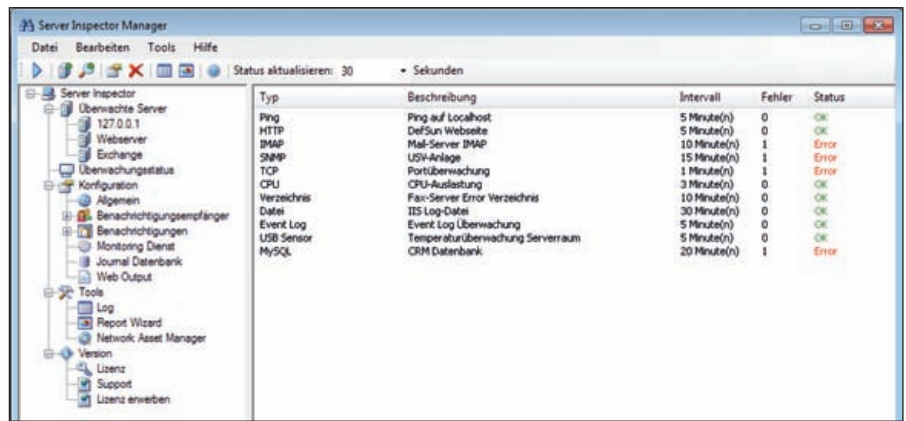
```
psping [[-6][[-4]] <-s source:
sourceport>
```

Und für den Client

```
psping [[-6][[-4]] [-h [buckets]]
[-r] <-l requestsize> <-n count>
[-w <count>] <destination:dest-
port>
```

Die zur Verfügung stehenden Parameter steuern dabei den Vorgang im Detail:

- "-h": Gibt ein Histogramm aus
- "-l": Größe des Requests



Die kostenlose Version des Server Inspector 3.3 kann dauerhaft einen Server überwachen

- "-n": Anzahl der Sende-/Empfangsver-suche
- "-r": Empfängt vom Server anstatt zu Senden
- "-w": Spezifiziert die Anzahl der Iterationen
- "-4": Erzwingt IPv4
- "-6": Erzwingt IPv6

Dabei läuft der Latenztest (wie auch der Bandbreitentest) solange, bis der Administrator diesen mit CTRL+C beendet. Der Einsatz von PsPing setzt Clients ab Windows Vista und/oder Server ab Windows 2008 voraus. (jp)

Link-Code: CBPE2

Einerseits ist der IT-Verantwortliche in kleinen Unternehmen immer irgendwie Mädchen für alles und schaut unter Umständen neidisch auf die Enterprise-Kollegen, die sich als Spezialisten nur um eine Technologie kümmern müssen. Andererseits sind im Kleinunternehmen die Anforderungen an beispielsweise das **Server-Monitoring** nicht so hoch und so speziell, dass der IT-Verantwortliche dies nicht mit einer kostengünstigen Lösung bewältigen könnte.

Dies gilt etwa für die freie Version des **Server Inspector 3.3**. Die Vollversion der Software hatten wir erst in der Februar-Ausgabe diesen Jahres ausführlich getestet. Nun steht das Monitoring-Werkzeug auch in einer kostenlosen Version zur Verfügung, die 30 Tage lang alles leistet, was die Vollversion kann und nach Ablauf dieses Zeitraums lediglich die Anzahl zu überwachender Server einschränkt. Also vielleicht genau das, was der IT-Verantwortliche in einer kleinen Firma benötigt. Der Server Inspector bietet **Überwachungen für Betriebssysteme**, die Programme, Dienste,

CPU oder freien Festplattenspeicherplatz beinhalten. Auch das **Netzwerk und Mailserver** lassen sich mit der Software funktional testen. Gängige Datenbanken wie MS SQL, MySQL oder Oracle werden durch SQL-Abfragen auf Funktion überprüft, andere Datenbanksysteme per ODBC. Ergänzend ist es auch möglich, über einen USB-Sensor die Temperatur und Luftfeuchtigkeit in Serverräumen zu messen. Findet Server Inspector 3.3 dabei einen Wert, der von der Norm abweicht, so informiert das System den Zuständigen wahlweise per E-Mail oder SMS. Durchdacht ist dabei, dass das System bei der Auswahl zwischen E-Mail und SMS die Arbeitszeiten des Administrators berücksichtigen kann und entsprechend auswählt. Bei den Systemanforderungen sind hinsichtlich der Hardware mindestens eine 2 GHz-CPU, 512 MByte RAM und 100 MByte auf der Festplatte vonnöten. Lauf-fähig ist das Tool auf Systemen mit mindestens Windows Server 2000 und dem .NET Framework 3.5. (jp)

Link-Code: CBPE3

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



Application Performance Monitoring Leistungsnachweis

von Ales Zeman



Quelle: gradt – Fotofia.com

Die Architektur moderner Applikationen führt oft zu komplexen Umgebungen und macht es sehr aufwändig und zum Teil unmöglich, den Grund für Performance-Engpässe oder Ausfälle zeitnah zu ermitteln. Datenbanken, physische und virtuelle Infrastrukturen, Java oder .NET, Webserver, Netzwerkkomponenten und nicht zuletzt das Endbenutzer-Verhalten können der Grund für diese Probleme sein und erfordern die Aufmerksamkeit der Administratoren. Selbst dann ist es aber meist nicht möglich, die Applikation in ihrer Gesamtheit darzustellen. Worauf es beim Application Performance Monitoring ankommt, lesen Sie in diesem Beitrag.

Applikation Performance Monitoring (APM) ermöglicht es, die Performance und Verfügbarkeit einer Applikation vom Punkt der Interaktion des Benutzers, durch die Web-Schicht, den Applikationscode bis hin zur Datenbank zu überwachen und zu bewerten. Entscheidend dabei ist, dass aus allen Komponenten einer Applikation performance-relevante Daten gewonnen und in Beziehung gesetzt werden können.

Unabhängig davon, ob die Applikation im traditionellen Datenzentrum oder in einer Cloud-basierten Umgebung betrieben wird, bietet APM die Visualisierung und die Informationen, um optimale Performance zu liefern. Antworten auf folgende Fragen werden gegeben:

- Wieso wird eine Anwendung im Laufe des Tages immer langsamer?
- Welchen Anteil hat die Java-Anwendung an der Antwortzeit der Webseite?
- Die DB-Aufrufe sind langsam, obwohl die Datenbank sehr performant läuft.
- Der Application Server läuft mit 90 Prozent CPU-Last, aber es lässt sich in den Logfiles keine Ursache dafür finden.
- Wieso ist die neue Software langsamer als die alte?

Bei APM werden breite und tiefe Fähigkeiten für die Gewinnung der Daten benötigt. Im Folgenden beschreiben wir, welche Technologien benutzt werden, um Performance- und Verfügbarkeitsprobleme einer Applikation zu erkennen, zu bewerten und zu beheben.

Benutzer im Fokus

Bei der Einführung von APM hat es sich bewährt, zuerst die Benutzer-Erfahrung (User Experience Monitoring, UEM) auszuwerten, da die Benutzer die Performance und Servicequalität einer Anwendung definieren. Performance und Servicequalität sämtlicher Komponenten einer Anwendung müssen sich daran orientieren. Die User Experience umfasst das Erleben oder die Erfahrung, die ein Benutzer beim Aufruf einer Anwendung macht. Dazu gehören Bedienbarkeit, Intuitivität, Schnelligkeit beim Seitenaufbau, Fehlermeldungen, Irritationen, Weiterleitungen et cetera. Das User Experience Management beschäftigt sich damit, dieses "Erleben" zu überwachen und zu optimieren.

Um die entsprechenden Daten zu gewinnen, gibt es aktive und passive Ansätze, die auch in Kombination eingesetzt

werden können. Zum einen die aktive Messung mit synthetischen Transaktionen, bei der definierte Arbeitsabläufe über Roboter von beliebigen Standorten ausgeführt werden. Es werden also Benutzer simuliert und die Performance bestimmter Arbeitsschritte auf den Mausklick genau erfasst und dargestellt. Der zweite Ansatz ist eine passive Messung der End User-Performance. Hier werden die Performancedaten realer Benutzer durch den Zugriff auf das Netzwerk erfasst und der gesamte Datenfluß analysiert. Dadurch wird eine 100-prozentige Abtastung der Transaktionsperformance, der Fehler und Volumina erreicht. Dies geschieht über Appliances, die beispielsweise über einen Span Port oder Netzwerk-Tap Zugriff auf die Datenströme erhalten. Damit kann bei Web-Anwendungen der gesamte HTTP-Verkehr nach Inhalten, Antwortzeiten, technischer Qualität, Lokationen, Service Providern et cetera überwacht werden. Detaillierte Metriken über Sites, Seiten, Elemente, Datenmenge, Downloadzeit, Fehler und Sessions stehen so zur Verfügung. Diese Technologie ermöglicht neben der Gewinnung von Performancedaten durch Erfassung des Webcontents auch die



nachträgliche Analyse von einzelnen User Sessions sowie Speicherung und Replay der kompletten Session.

Bei neueren Applikationen, durch die der Web-Browser zu einem Fat-Client wird (Web 2.0), ist es zusätzlich notwendig, die Abläufe auf dem Client überwachen zu können. Dies kann über Kennzeichnung oder Code Insertion geschehen. Damit werden die Browser-basierten Events wie Mausklicks, -Bewegungen oder Eingaben gesammelt und für die Auswertung zur Verfügung gestellt. Die Verwendung des Client-seitigen Scriptings, um die Web 2.0 User Experience zu verstehen, dürfte sich dabei immer mehr durchsetzen – insbesondere, da Technologien wie AJAX, Adobe Flex und Microsoft Silverlight stärker in den Vordergrund rücken.

Zuletzt kann auch eine ressourcenintensivere Methode zur Fehlerverfolgung eingesetzt werden: die Auswertung der Web-Log-Dateien. In den letzten Jahren ist die Bedeutung der Web-Log-Analyse zurückgegangen, hauptsächlich wegen der Einführung neuer Technologien wie Web Content Delivery Networks (CDNs), Web-Beschleuniger und Proxys, womit der Datenbestand unvollständig wird. Individuelle Benutzersessions sind schwierig zu identifizieren. Durch die oben genannten Methoden werden wichtige Fragen beantwortet wie:

- Besteht das Problem im Front-End oder Back-End?
- Wie viele Anwender hatten das Problem?
- Ist es ein lokales oder globales Problem?
- Was haben die User gemacht, als Sie ein Performance-Problem hatten?
- Welche Teams sollten nach den Problemen schauen?
- Wie sieht die Verfügbarkeit der Applikation über die Zeit aus?

Performance-Analyse

Die im ersten Schritt gewonnenen Daten lassen sich jetzt mit den Metriken aus der Applikation und Infrastruktur in Verbindung setzen. Zuerst stellen wir uns die Frage, wie die Performance-Daten aus der Applikationsschicht gesammelt werden. Generell laufen Anwendungen als Prozesse oder Services auf einem oder mehreren Hosts. Daher werden Verfügbarkeitsdaten

The screenshot shows a web browser window with a performance monitoring dashboard. The dashboard is divided into several sections:

- User Information:** Alarm: Active User; IP: 10.1.40.105; Server IP: 10.1.34.12; User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.1; .NET CLR 1.1.4322); City: United States (US); ISP: AT&T WorldNet Services; Access Speed (kbps): 549.9; Duration (secs): 603.668; Start Time: 4/29/06 9:07:28; Stop Time: 4/29/06 9:17:32; Session Key: lqvctr1stlhznn8uslmanwsvrv0rbhgjzptqtku_
- Page Metrics:** Page Client Time (msecs): 268.070; Page Download Attempts: 170; Page Download Time (secs): 1.003; Page Processing Time (msecs): 734.850; Page Redirect Ratio (%): 0.00; Page Round-Trip Time (msecs): 0.170; Page Stop Count: 2; Page Stop Time (msecs): 114.790
- Request-Response Metrics:** Success Ratio (%): 100.00; Success Ratio (with client errors) (%): 100.00; Success Ratio (with server errors) (%): 100.00; Error Count (HTTP 4xx client errors): 0; Error Count (HTTP 5xx server errors): 0
- Command Performance Metrics:** Command Completion Time (msecs): 822.850; Command Client Time (msecs): 157.110; Command Round-Trip Time (msecs): 0.170; Command Processing Time (msecs): 665.740; Command Initial Response Time (msecs): 664.680; Element Download Time (msecs): 823.020; Element Redirect Ratio (%): 0.00
- Command Volume Metrics:** Command Count: 199; Command Byte Volume - Server (mb): 1.164; Command Byte Volume - User (kb): 188.659; Command Data Size - Server (kb): 5.877; Command Data Size - User (bytes): 948.040; Command Timeout Count: 0; Element Download Attempts: 198
- IP Metrics:** IP Packet Byte Volume - Server (mb): 1.226; IP Packet Byte Volume - User (kb): 240.655; IP Packet Count - Server: 1334; IP Packet Count - User: 1200; IP Packet Size - Server (bytes): 918.950; IP Packet Size - User (bytes): 188.010
- Request Codes:** POST: 131; GET: 68
- Response Codes:** Successful: OK: 198
- All Alarms:** 4/29/06 9:15:00 Active User 170.000 +127%
- Pages:** Table with columns: Start Time, Stop Time, Download Time (msecs), Processing Time (msecs), Client Time (msecs), Size (bytes), Server IP. Example row: /sales_enq/start_sve?SVEcd=Start&SVEH=YY 9:07:28 9:07:34 6235.260 5564.960 670.164 12846 10.1.34.12

Bild 1: Alarme helfen dabei, kritische Entwicklungen im Blick zu behalten

und Ressourcen-Verbrauch gesammelt und Workload-Abläufe aufgezeichnet, um Kapazitätsengpässe und Konfigurationsprobleme zu entdecken. Weiterhin werden Applikations-Logdateien ausgewertet und dort gefundene Events in Beziehung mit der Performance gebracht. Eine detaillierte Überwachung von Java oder .NET lässt sich durch die Bytecode-Instrumentierung der jeweiligen Applikationsserver erreichen. Neben dem Zustand des Applikationsservers selbst können so auch Performanceinformationen zu einzelnen Requests ermittelt werden.

Ein weiterer Schritt ist das Tracing der Requests, um bis auf Methoden- und SQL Statement-Ebene Performance-Engpässe erkennen zu können. Die Bytecode-Instrumentierung erfordert üblicherweise den Neustart des Applikationsservers. Sollte dies nicht möglich oder gewünscht sein, lassen sich Daten auch über

die JMX-Schnittstelle gewinnen. Viele Hersteller von Applikationsservern unterstützen JMX und liefern eine Reihe von Performance- und Verfügbarkeitsdaten über diese Schnittstelle, aber in weit geringerem Umfang, als es die Instrumentierung ermöglicht. Um die Sicht auf die Applikation abzurunden, ist es notwendig, auch die beteiligten Datenbanken und die physische, virtuelle oder hybride Infrastruktur zu überwachen. In einem heterogenen Umfeld ist es wichtig, alle Datenbanken und Systeme in vergleichbarer Art und Weise darstellen zu können.

Datensammlung lokal oder remote

Zu unterscheiden ist auch zwischen der lokalen und Remote-Sammlung der Performance-Daten. Die Möglichkeit, Datenbanken und die Infrastruktur remote überwachen zu können, bietet Vorteile beim Rollout und der Administration besonders

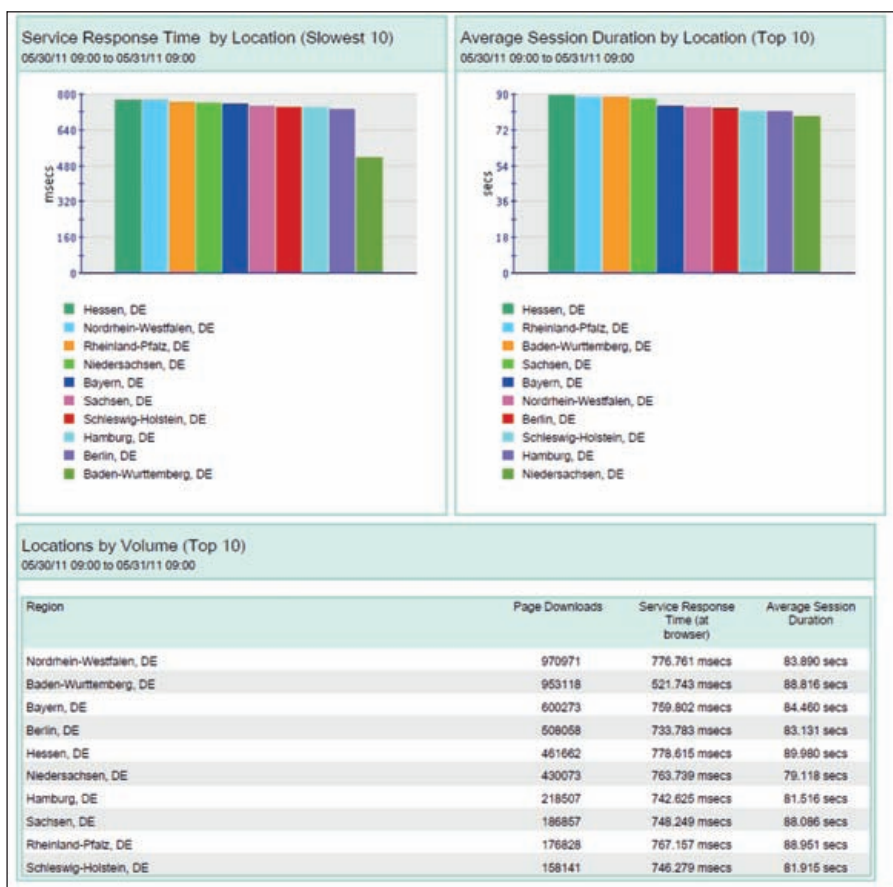


Bild 2: Die Antwortzeiten lassen sich idealerweise geografisch aufschlüsseln

in großen Umgebungen. Bei dieser Architektur werden aber höhere Ansprüche an die Kapazität der zentralen Komponenten gesetzt. In diesem Szenario sind Firewall-Freigaben erforderlich, da die Sammlungsmethoden meistens auf SSH, WMI und ähnlichen Protokollen aufsetzen. Bei komplexeren Umgebungen wird eine Art von Kaskadierung unvermeidlich.

Bei der Überwachung physikalischer Infrastrukturen werden neben den Daten über I/O, CPU-, Netzwerk- und Speicher-Auslastung auch Metriken der Hauptsystemprozesse gesammelt, um zu identifizieren, wann ein Problem begann und die Ursache zu isolieren. Bei virtuellen Infrastrukturen werden Metriken über den Hypervisor gesammelt, da die klassischen System-Monitoring-Daten keine relevante Aussage ergeben. Die 90-prozentige Auslastung einer virtuellen CPU etwa hat keine Aussagekraft über die tatsächliche Auslastung des virtuellen Hosts. Metriken wie "CPU Ready %", "Memory Ballooning" und "Prozessor Zyklen" sind für die Suche nach Performance-Engpässen nötig. Neben Informationen

über den Zustand der virtuellen Maschinen benötigen wir auch Daten aller Komponenten der virtuellen Umgebung wie Rechenzentren, Data Stores, Cluster oder Ressource Pools.

Bei der Überwachung von Datenbanken sind neben der Verfügbarkeit, Antwortzeiten und Füllgrad auch Sessiondaten, Auslastungen und Informationen zu den verwendeten SQL-Statements entscheidend für die Analyse der Performance. Diese Daten lassen sich über die angebotene API der jeweiligen Datenbank-Plattform remote oder lokal sammeln oder über eine Technik, die auf dem Sampling des Arbeitsspeichers im Datenbankserver beruht, bei dem keine Verbindung zur Datenbank notwendig ist. Diese Technik ist darauf ausgerichtet, kritische Datenbanken zu überwachen und eine tiefgreifende Analyse von Performance-Engpässen vorzunehmen, ohne das produktive System weiter zu belasten. Die Datensammlung erfolgt bis zu 400 Mal pro Sekunde. Damit ist gewährleistet, dass auch kurze Befehle, die durch ihre Anzahl kritisch sind, erfasst werden.

Alle durch die Überwachung gewonnenen Daten laufen in einem zentralen Repository zusammen. Dies bietet neben der historischen Analyse auch die Korrelation aller Daten, um aus den einzelnen Silos eine echte Applikationssicht zu entwickeln. Die Komponenten lassen sich so zu Services zusammenfassen und mit Definitionen möglicher Service Levels verknüpfen. Ein graphisches User Interface mit anpassbaren und benutzerbezogenen Dashboards hilft bei der Visualisierung und Analyse der Performance- und Verfügbarkeitsdaten.

Application Monitoring in der Praxis

Wie sieht Application Monitoring in der Praxis aus? Nehmen wir ein Beispiel, bei dem eine APM-Lösung für die Internet-Online-Banking-Anwendung bei einem deutschen Finanzdienstleister implementiert wurde. Die Infrastruktur wurde bereits mit Systemmonitoren überwacht, die aber weder Informationen über Benutzererfahrung noch Korrelation zu den Performancedaten der Applikation bieten. Die Problemsuche war langwierig, und es fehlten Informationen für die Priorisierung der Vorfälle, beispielsweise welche Auswirkung eine Störung auf die Performance der Applikation hat oder wie viele Benutzer davon betroffen sind.

Die Lösung sollte die Messung der Servicequalität für die Anwender erlauben und eine rollenbasierte Darstellung der gesamten Applikationskette für die Fach- und IT-Abteilung anbieten. Zielgerichtete Alarmierung, die Einbindung der Lösung in die bestehende IT-Umgebung (beidseitige Integration in ein Ticketing-System) und die geringe Belastung der Systeme durch das Monitoring waren weitere Parameter, die zu beachten waren.

Die Banking-Anwendung wird in zwei Rechenzentren in zwei weit entfernten Städten betrieben, um die Ausfallsicherheit zu garantieren. Die Benutzeranfragen fließen von dem Internetprovider über einen Hauptloadbalancer ein. Hier wird die SSL-Verbindung terminiert und die Sessions in die Rechenzentren weitergeleitet. In den Rechenzentren werden die Requests über weitere Loadbalancer an die




Apache Webserver verteilt. Die Webserver, platziert in der äußeren DMZ, kommunizieren eins zu eins mit vorgeschalteten Tomcat-Servern in der per Firewall getrennten inneren Zone. Schließlich werden die Requests von im Kernnetz platzierten Weblogic-Servern beantwortet und die Daten in einer Oracle-Datenbank hinterlegt. Aus dem Kernnetz werden Schnittstellen zu anderen Systemen wie SAP angesprochen.

Für die Implementierung kam Foglight, eine Application Performance Monitoring-Lösung von Quest Software, zum Einsatz. Nach der Analyse der Systemlandschaft entschieden sich die IT-Experten für die folgende Architektur: Als zentrale Instanz diente ein Foglight Management Server. Dieser fungierte als zentrales Repository für alle gesammelten Daten, zur Analyse, Visualisierung und als zentrale Alarmierungsinstanz. Die Messung der Servicequalität der Anwender erfolgte durch zwei Foglight Experience Monitor Appliances in den beiden Rechenzentren, und die gesammelten Daten wurden mittels eines FxM-Portals zusammengeführt.

Die Appliances wurden für die Datenflußanalyse über einen von der HW des Loadbalancers vorgesehenen Span Port eingebunden, auf den der Datenstrom der Anwendung gespiegelt wurde. Die IP-Adressen der Endbenutzer werden durch den Loadbalancer in einem HTTP-Feld abgelegt und von den Appliances ausgelesen. Dies ist eine wichtige Funktion, um die geografische Lokation der Benutzer identifizieren zu können, da im Rechenzentrum nur die IP-Adresse des Loadbalancers sichtbar ist.

Die Analyse der gesammelten Daten erfolgte auf den Appliances, die Benutzer-Sessions wurden dabei zusammengeführt und die Metriken an den Foglight Management Server weitergeleitet. Foglight Java-Agenten überwachten die beteiligten Tomcat- und WebLogic-Server. Hierzu wurde eine Bytecode-Instrumentierung der Applikationsserver durchgeführt. Auch die Oracle-Datenbank wurde mit entsprechenden Agenten an Foglight angebunden. Da sich die Agenten in verschiedenen DMZ befanden und eine durchgängige Freischaltung der Firewalls

nicht zulässig ist, werden die Daten über Foglight Agent Manager-Konzentratoren durch verschiedene Ports kaskadiert.

Nach Verteilung der Agenten wurde Foglight auf die Maßgaben angepasst. Dazu gehörten Filter für den Datenstrom auf den Appliances, kundenspezifische Dashboards zur Visualisierung der Systeme, Schwellwertanpassungen, Definition der Baselines und abteilungsspezifische Alarmierungen. Somit stehen dem Application Support-Team nun aktuelle Informationen über die Verfügbarkeit und Performance der Transaktionen aus der Sicht des Anwenders auf einem Blick zur Verfügung. Bei Über- oder Unterschreitung der Baselines erhalten die zuständigen Mitarbeiter automatisch eine Benachrichtigung. Um eine weitergehende Analyse von Problemen durchführen zu können, stehen Dashboards zur Verfügung, durch die ein Drilldown oder Workflow vorgegeben wird, der den Weg zum Root-Cause des Problems erleichtert. (dr) 

Ales Zeman ist Senior Presales Consultant bei Quest Software.



Liefertermin:
März 2013

Bestellen Sie jetzt das IT-Administrator Sonderheft 1/2013!

180 Seiten Praxis-Know-how rund um das Thema

Windows Server 2012

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

* IT-Administrator Abonnenten erhalten das Sonderheft 1/2013 für € 24,90. Nichtabonnenten zahlen € 29,90. IT-Administrator All-Inclusive Abonnenten "zahlen" für Sonderhefte nur € 19,90 - diese sind im Abonnement dann automatisch enthalten. Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier 
www.it-administrator.de/kiosk/sonderhefte/

HP Discover 2012

Termin & Ort

4. bis 6. Dezember 2012
 Messe Frankfurt GmbH, Ludwig-Erhard-Anlage 1,
 60327 Frankfurt a. M.

Inhalt

Kongressmesse rund um HP-Technologien und -Produkte

Teilnahmegebühr

1.150 Euro zuzüglich Booking-Fee und Mehrwertsteuer

Weitere Informationen und Anmeldung

Link-Code: CAW43

JOBcon IT

Termin & Ort

6. Dezember 2012
 Hotel Novotel Karlsruhe, Festplatz 2,
 76137 Karlsruhe

Inhalt

Karriereplanung für IT-Fachpersonal in Einzelgesprächen mit Arbeitgebern und Personalentwicklern

Teilnahmegebühr

Kostenlos

Weitere Informationen und Anmeldung

Link-Code: CBW44

**Handelsblatt Jahrestagung
 Strategisches IT-Management**

Termin & Ort

28. bis 30. Januar 2013
 Sofitel Bayerpost, Bayerstraße 12,
 80335 München

Inhalt

Strategien für IT in Großunternehmen

Teilnahmegebühr

Ab 2.699 Euro

Weitere Informationen und Anmeldung

Link-Code: CBW41

**Embedded Software
 Engineering Kongress**

Termin & Ort

3. bis 7. Dezember 2012
 Congress Center Stadthalle Sindelfingen,
 Schillerstrasse 23, 71065 Sindelfingen

Inhalt

Entwicklung von Geräte- und Systemsoftware

Teilnahmegebühr

Ob Sie sich als Einzelperson anmelden oder eine Gruppenanmeldung vornehmen – der Preis richtet sich nach der Anzahl der insgesamt gebuchten Kongress-Tage und beginnt bei 300 Euro pro Tag.

Weitere Informationen und Anmeldung

Link-Code: CBW42

i+e 2013

Termin & Ort

24. bis 26. Januar 2013
 Messe Freiburg, Europaplatz 1, 79108 Freiburg

Inhalt

Regionale Industrie- und Elektronikmesse

Teilnahmegebühr

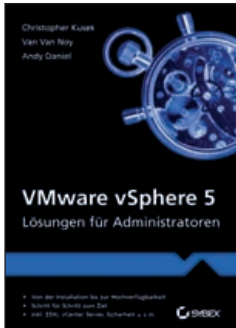
Tageskarte 5 Euro

Weitere Informationen und Anmeldung

Link-Code: CBW43



VMware vSphere 5 – Lösungen für Administratoren



vSphere5 ist das Flaggschiff von VMware, für dessen praktische Probleme beim Einsatz die Autoren in "VMware vSphere 5" Lösungen präsentieren. Zunächst zeigen sie die Installation von vSphere5 auf, um

dann ESXi, vCenter Server/Appliance und vSphere Client zu dokumentieren. Dies dürfte Administratoren freuen, die vSphere vor Version 5 kennen, da die Vorstellung der neuen Funktionen eventuelle Wissenslücken schließt. Das Zuweisen, Verwalten und Prüfen von Lizenzen ist Bestandteil des Folgekapitels, bevor die Aktualisierung von einer bereits bestehenden früheren vSphere4-Umgebung thematisiert wird. Auf notwendige Vorbe-

reitungen und Aufgaben, die ein erfolgreiches Upgrade sichern sollen, weisen die Autoren hin.

Die vielfältigen Konfigurationsmöglichkeiten im Bereich Netzwerk und Speicher leiten den zweiten Teil des Buches ein, der sich mit der Konfiguration der vSphere5-Umgebung detailliert befasst. Neben den grundlegenden virtuellen Netzwerkfunktionen finden sich auch vSphere Standard Switches beziehungsweise Distributed Switches wieder. Da die Einrichtung des Speichers ein wichtiges Element einer virtualisierten Umgebung ist, werden die Speicherkonzepte Fibre Channel SAN, iSCSI SAN und NFS-Speicher beschrieben. Die Möglichkeiten zum Schutz vor Ausfällen von Hosts und VMs, vSphere High Availability und Fault Tolerance, sind im Abschnitt "Hochverfügbarkeit" dargelegt. Die Verwaltung, der Im- und Export virtueller Maschinen sowie die Absicherung des vCenter-Servers und der ESX-/ESXi-Hosts bilden den Abschluss, bevor die Zusammenhänge und Steuerung von

Ressourcen und Performanceoptionen wiedergegeben werden. Ein Index hilft beim raschen Nachschlagen.

Fazit

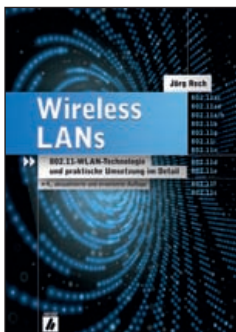
Mit dem vorliegenden Buch liefern die Autoren eine sinnvoll strukturierte Ansammlung von praktischen Lösungen für vSphere 5. Da sich das Buch den Themen über die Grundlagen und Installation nähert, ist es auch für unerfahrene Administratoren zu empfehlen. Als primäre Zielgruppe werden die Praktiker angesprochen, was auch der Intention des Untertitels gerecht wird. Die Inhalte zeichnen sich durch eine Mischung von theoretisch notwendigem Wissen, praktischen Hinweisen und How-To-Lösungen aus.

Frank Große

Autoren	Christopher Kusek, Van Van Noy, Andy Daniel
Verlag	Sybex
Preis	34,95 Euro
ISBN	978-3527760206

Bewertung (max. 10 Punkte) **9**

Wireless LANs, 4. Auflage



Seit der Verabschiedung des IEEE-802.11-Standards hat eine gewaltige Entwicklung im Bereich Drahtlosnetzwerke stattgefunden, die mit der Einführung der IEEE-802.11ac-Erweiterung im kommenden Jahr

eine Steigerung der Datenrate um knapp das 3.500-fache erreichen soll. In seinem Buch "Wireless LANs" beschreibt Jörg Rech nach einer Einführung in die Funknetzwerke verschiedene WLAN-Netzformen, bevor er sich sehr detailliert den diversen Spezifikationen des Physical und MAC Layer widmet. Mit FHSS, DSSS, OFDM, PBCC und den 802.11g-PHY-Erweiterungen wird keine Technologie ausgelassen.

Darauf aufbauend folgen die besonderen Eigenschaften der 802.11n-Erweiterung,

die für höhere Datendurchsätze verantwortlich ist. Dieses Kapitel ist gegenüber der Vorgängerversion überarbeitet worden, da der Standard mittlerweile verabschiedet wurde. VHT-Erweiterungen zeigen den Weg in die Zukunft und bilden den Abschluss des sehr detaillierten theoretischen Parts, der akademischen Ansprüchen gerecht wird und aufgrund seiner Strukturierung beste Voraussetzungen zum Nachschlagen mitbringt. Erfreulich ist, dass der Autor mit vielen Grafiken und Tabellen zur Veranschaulichung arbeitet, da die vermittelten Inhalte auf hohem theoretischem Niveau angesiedelt sind.

Im Hardware-Abschnitt des Buches beschreibt Rech die passende Antennentechnik. Die Kapitel zu Antennentypen und Antennenstecker bereiten auf das Folgekapitel WLAN-Produkte vor, sodass in Bezug auf die zu erwerbenden Komponenten keine Frage offenbleibt. Die Kapitel über die praktische Umsetzung bauen idealerweise auf den Vorkapiteln auf und helfen dabei, die richtigen Entscheidungen zur Realisierung zu treffen.

WLAN-Sicherheit und Fehleranalyse werden ebenso ausführlich behandelt.

Fazit

Mit der vierten Auflage führt Jörg Rech sein WLAN-Buch auf den aktuellen Stand der Technik. Der Leser lernt in Detailtiefe verschiedene drahtlose Netzwerkformen, WLAN-Komponenten und Antennen kennen. Nach wie vor ist kein vergleichbares Werk bekannt, das die verschiedenen WLAN-Standards in dieser Detailtiefe beleuchtet. Doch auch die Praktiker dürften profitieren, wenn diese den Aufbau eines Hochleistungs-WLANs planen, ohne Themen wie Performance, Sicherheit oder Spektrumanalyse zu vernachlässigen. Ein umfangreicher Abschnitt zur Fehleranalyse rundet den Inhalt ab.

Frank Große

Autor	Jörg Rech
Verlag	Heise Zeitschriften Verlag
Preis	49,90 Euro
ISBN	978-3936931754

Bewertung (max. 10 Punkte) **10**


<http://clouduser.de/>
Cloud für echte Kerle

Ist aktuell von "Cloud" die Rede, muss der interessierte IT-Verantwortliche durch geschicktes Nachfragen erst einmal privat genutzte Online-Speicherdienste, proprietäre Shop-Angebote mit Cloud-Label und Methoden der Virtualisierung der Unternehmens-IT auseinanderdividieren. Doch wird dies recht mühsam, wenn die Suche nach Cloud-Informationen im Internet erfolgt, schließlich bringt Google zum Suchwort "Cloud Computing" kaum weniger als eine viertel Milliarde Fundstellen. Eine fundierte Know-how-Quelle, die sich in Sachen Cloud zudem auf die Belange der Administratoren fokussiert, ist unsere diesmonatige Website clouduser.de.

Seit 2009 führt Rene Büst den ehemaligen Blog, der sich mittlerweile zu einem waschechten Cloud-Magazin gemausert hat mit der Mission, Cloud Computing im deutschsprachigen Raum populärer zu machen. Es lässt sich sicher trefflich streiten, ob Letzteres angesichts des allgegenwärtigen Hypes überhaupt notwendig ist. Büsts Methoden der Popularitätssteigerung sind jedoch hervorragend. Die Seite bietet eine Vielzahl unterschiedlicher Informationen rund um die IT-Wolke: Analysen betrachten und bewerten aktuelle Virtualisierungskonzepte und

-technologien, der Besucher hat Zugriff auf eine Übersicht der Marktteilnehmer und kann sich über relevante Branchenevents informieren.

Aber das ist nur der Einstieg. Überhaupt sollte der Besucher von clouduser.de etwas Zeit mitbringen, den Büst und sein Team gehen mitunter in die Tiefe. So etwa mit dem frei zugänglichen 80-Seiter, der sich mit der Frage beschäftigt, wie die Cloud Unternehmen und deren IT verändert. Ergänzend bietet der Bereich "Grundlagen" Dutzende von sehr gut auf den Bedarf von IT-Verantwortlichen zugeschnittene Texte wie etwa "Was bei der Nutzung von EC2-Instanzen zu beachten ist". Ähnlich passgenau und bedarfsgerecht sind die Beiträge in den Bereichen "Interviews", "Management" und "Meinungen".

Noch recht spärlich befüllt ist aktuell der Bereich "Tests", ausführliche Infos zu Cloud-Diensten und -Werkzeugen findet der IT-Verantwortliche aktuell daher eher im Bereich "Services". Hier stellt Büst allerlei mehr oder weniger bekannte Angebote vor, ohne den Artikeln einen Test-Charakter zu verleihen. Spannend sind auch die "Tutorials" der Website, die Cloud-Anfängern, aber auch Fortgeschrittenen den Weg durch die Cloud-Welt Schritt für Schritt darlegen. Und wem das noch zu viel zum Lesen ist, der findet sicher in einem der Filme in "Videos" seinen professionellen Zeitvertreib. (jp) 



Clouduser.de bringt IT-Profis alles zum Cloud Computing für IT-Abteilungen



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

**Wege einer umfassenden
Zweigstellen-Konsolidierung**

Obwohl viele Unternehmen durch Virtualisierung und WAN-Optimierung einen hohen Grad an Konsolidierung erreicht haben, halten nicht wenige noch immer Server und Storage in Zweigstellen vor. Dies wird meist mit den hohen Kapazitätsanforderungen vieler Anwendungen begründet, die jeder WAN-Beschleunigung trotzen. Auch die Sorge um die Produktivität ist groß, sollte das WAN nicht verfügbar sein. Unser Online-Fachartikel nennt Herausforderungen, die eine komplette Konsolidierung oft behindern, zeigt aber auch Lösungsmöglichkeiten auf, die sich an der Virtual Desktop Infrastruktur orientieren.

Link-Code: CBW51

Anwenderbericht: Eigene IT versus Cloud

Nach Meinung vieler Marktbeobachter steht der Zukunft, in der die IT "aus der Steckdose" kommt, nichts mehr im Wege. Die IT-Abteilungen mittelständischer Unternehmen stehen somit im Wettbewerb mit Cloud-Anbietern wie Microsoft, Google und Amazon. Die IT-Verantwortlichen beim WEKA-Fachverlag in Kissing sind jedoch der Überzeugung, dass eine gut aufgestellte IT-Abteilung den Cloud-Anbietern in puncto Kosten mindestens ebenbürtig und bei der Servicequalität überlegen ist. In unserem Anwenderbericht im Web erfahren Sie, warum die eigene IT kein Auslaufmodell sein muss.

Link-Code: CBW52

RZ in der Cloud:

Umkonfigurieren im laufenden Betrieb

Cloud-Lösungen werden oft als simpler Weg beschrieben, um vorhandene Kapazitäten in Rechenzentren schnell aufstocken zu können. Wirklich komfortabel und kosteneffizient sind aber nur Modelle, die vertikal skalieren. Mit Live Vertical Scaling können IT-Verantwortliche die Anzahl Ihrer CPUs und Arbeitsspeicher erhöhen, ohne Ihren virtuellen Server neu starten zu müssen. Das Erweitern eines virtuellen Rechenzentrums bei Lastspitzen ist so bei laufendem Server möglich. Lesen Sie in unserem Fachbeitrag im Web, wie Sie sogar einzelne CPU-Kerne ohne Serverneustart zu VMs hinzufügen können.

Link-Code: CBW53

Worauf Sie bei Colocation achten sollten

Outsourcing und Outtasking sind in wirtschaftlich schwierigen Zeiten, aber auch in Phasen des Aufschwungs willkommene Instrumente, um die Schlagkräftigkeit des Unternehmens zu optimieren. Colocation – also die Unterbringung und Netzanbindung eigener Server im Rechenzentrum eines Service Providers – als separat betrachteter Outsourcing-Faktor dürfte in den kommenden Jahren wesentliches Wachstum erzielen. Unser Online-Beitrag beschreibt, wie sich gerade unternehmenskritische Anwendungen und Prozesse erfolgreich an Carrier-neutrale Rechenzentren auslagern lassen.

Link-Code: CBW54

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

»Die Verwaltung von SBC-Arbeitsplätzen ist wesentlich effektiver«

Die Steinwender EDV-Beratung GbR ist ein Systemhaus in Hamburg und bietet seinen maritimen Kunden eine Rundum-Betreuung in allen Belangen der Informations- und Kommunikationstechnologie. Das Unternehmen berät Reedereien hinsichtlich der IT und rüstet Schiffe mit IT-Infrastrukturen aus. David Dammeier (24) ist dafür verantwortlich, dass modernste IT auf Schiffen läuft und die Vorteile von Server-based Computing auch auf den Weltmeeren effizient eingesetzt wird.

Warum sind Sie IT-Administrator geworden?

Wegen meiner persönlichen Affinität zu Einsen und Nullen.

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

Die Aufgabe ist spannend, abwechslungsreich und nahezu krisensicher. Zudem ist das gesammelte Know-how im privaten Umfeld unbezahlbar.

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

Wenn Kunden sich freuen, mich wieder zu sehen. Konkrete Erfolgserlebnisse bringen natürlich auch viel Spaß. Durch die weltweiten Aufträge komme ich mit Menschen unterschiedlichster Herkunft zusammen und ich sehe Ecken der Welt, die andere niemals sehen werden. Support-Cases bei Herstellern dagegen, die sagen: 'Sie sind der Einzige, bei dem dieses Problem auftritt', sind durchaus frustrierend. Es gibt Tage, an denen Herr Murphy stets neben mir zu stehen scheint.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

An der Implementierung der neuen Infrastrukturen auf Schiffen, der Einrichtung von Dokumentenscannern in Terminalserverumgebungen sowie an P2V-Migrationen. Am spannendsten ist derzeit die Einführung eines neuen Systems auf Schiffen, das mich vermutlich wieder viel in der Welt herumkommen lässt. Wir haben das System zwei Jahre entwickelt und sind stolz darauf, wie gut es am Markt ankommt.

Nutzen Sie Server-based Computing und wenn ja, mit welchen Werkzeugen?

Seit ich mich im Unternehmen mit IT beschäftige, arbeite ich mit Windows RDS, Citrix und Co.

Was waren die Gründe für diese Entscheidung?

Die Verwaltung von SBC-Arbeitsplätzen ist wesentlich effektiver, denn irgend-

wann nervt es nur noch, ein Update auf 17 PCs installieren zu müssen. Ein weiteres Argument, das wir auch gegenüber dem Kunden anbringen, sind Kosteneinsparungen.

Welches war die größte Herausforderung bei der Einführung? Welche sind es aktuell?

Die Umstellungen von PC-Applikationen auf SBC ist eine Herausforderung. Die Anwender zufriedenzustellen und ihnen das Gefühl zu geben, dass alles genauso oder besser läuft wie vorher, gehört dazu. Jetzt und zukünftig wird es immer eine Herausforderung sein, Entscheider davon zu überzeugen, dass die Konzentration auf einen oder wenige Server der richtige Weg ist.

Welche Art von Nutzer versorgen Sie so mit Applikationen?

All jene, die halbwegs standardisierte PC-Arbeitsplätze haben und denen die einfachere Wartung einen Mehrwert für die Unternehmens-IT bringt. Da reicht die Palette vom Großunternehmen bis hin zum kleinen Handwerksbetrieb.

Wie sind die Erfahrungen in der IT und bei den Nutzern?

Durchweg positiv, speziell bei den Remote-Nutzern. Es macht einen Riesenschied in der Anwendererfahrung, ob eine Datei über VPN mit dem lokalen Word oder Excel geöffnet wird oder in einer RDP-Session.

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

Die Absicherung eines HA-Clusters unter VMware mit einer APC-USV wie auch die Automapping-Funktion im Exchange in Verbindung mit dem Exchange Cache-Modus haben mich einiges an Nerven gekostet. VPN-User mag diese Kombination nicht unbedingt freuen.

Wenn Sie sich ein beliebiges Tool wünschen könnten, was würde dieses leisten?



Geburstag: 19.08.1988
Admin seit: 2 Jahren
Hobbys: Musizieren, IT, anderen Menschen helfen (ASB)

David Dammeier, IT-Administrator

Ausbildung und Tätigkeit

- Ausbildung zum Fachinformatiker für Systemintegration
- Heute tätig in den Bereichen Technik & Support, Systemintegration

Betreute Umgebung

- Diverse Windows-Netzwerke, Terminalserver-Umgebungen, zumeist VMware oder Hyper-V virtualisiert.

Event-IDs lesen und selbstständig den Fehler beheben.


Wie finden Sie den nötigen Ausgleich zu Ihrer Arbeit?

Über ehrenamtliche Tätigkeiten, bei denen ich größeren körperlichen Einsatz zeige.

Inwieweit hat Ihr Beruf Ihre Hobbys geprägt?

Durch das breite Umfeld an IT-Produkten, die ich durch die Arbeit kennenlerne, empfinde ich manchmal Produkte für zu Hause als nützlich oder unverzichtbar, ohne die ich Jahre zuvor gut ausgekommen bin – zum Leidwesen meiner Freundin.

Wie denken Sie, arbeitet ein Administrator in zehn Jahren?

Leider immer weniger vor Ort mit Menschen und immer mehr an einer Support-Konsole. Zudem wird die GUI im Administratorumfeld wieder weitestgehend abgeschafft. Back to the roots! 

Das Interview führte Petra Adamik.

Möchten Sie auch einmal das letzte Wort im IT-Administrator haben? Dann melden Sie sich einfach unter redaktion@it-administrator.de (Betreff: "Das letzte Wort"). Wir freuen uns auf Sie!

Was haben Sie zu sagen?

Die Ausgabe 01/13 erscheint am 31. Dezember 2012

Schwerpunktthema:

Client-Security

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

Im Februar dreht sich im Heft alles um den Schwerpunkt **Desktop-Virtualisierung**. Im Testbereich nehmen wir unter anderem Immidio Flex+ und Unidesk unter die Lupe. In der Praxisrubrik erfahren Sie alles über Konfiguration und Betrieb von ownCloud. Außerdem beschäftigen wir uns damit, was der Client-Hypervisor von Windows 8 zu bieten hat.

Der Schwerpunkt im März liegt beim Thema **Monitoring & Verfügbarkeit**.

Im Test: Mobile Device Management mit Good for Enterprise

Im Test: Frontrange Desktop & Server-Management 7.0.1

Workshop: Client-Security mit Bordmitteln in Windows 8

Workshopserie: Best Practice für Gruppenrichtlinien (1)

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.



IMPRESSUM

Redaktion

John Pardey (ip), *Chefredakteur*
verantwortlich für den redaktionellen Inhalt
john.pardey@it-administrator.de

Daniel Richey (dr), *Stellv. Chefredakteur und Cvd*
daniel.richey@it-administrator.de

Lars Nitsch (ln), *Redakteur*
lars.nitsch@it-administrator.de

Markus Heinemann, *Schlussredakteur*
markus.heinemann@email.de

Autoren dieser Ausgabe

Petra Adamik, Thomas Bär, Jürgen Heyer, Frank Große,
Thomas Joos, Christian Knerrmann, Sandra Lucifora,
Rolf Masuch, Dr. Holger Reibold, Christian Schulenburg,
Marc Salimans, Ulf B. Simon-Weidner,
Markus Wittwer, Ales Zeman

Anzeigen

Anne Kathrin Heinemann, *Anzeigenleitung*
verantwortlich für den Anzeigenteil
kathrin@it-administrator.de
Tel.: 089/4445408-20

Es gilt die Anzeigenpreisliste
Nr. 9 vom 01.01.2012



Produktion / Anzeigendisposition

Lightrays: Andreas Skrzyplik, 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-Hohstadt

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

SI special interest Pressevertrieb GmbH,
www.special-interest.com

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,-
Jahres-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 85
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 / Anteilverhältnisse
Geschäftsführende Gesellschafter zu gleichen Teilen
sind Anne Kathrin und Matthias Heinemann.

ISSN

1614-2888

Urheberrecht

Alle in IT-Administrator erschienenen Beiträge sind
urheberrechtlich geschützt. Alle Rechte, einschließlich
Übersetzung, Zweitverwertung, Lizenzierung vorbe-
halten. Reproduktionen und Verbreitung, gleich wel-
cher Art, ob auf digitalen oder analogen Medien, nur
mit schriftlicher Genehmigung des Verlags. Aus der
Veröffentlichung kann nicht geschlossen werden, dass
die beschriebenen Lösungen oder verwendeten Be-
zeichnungen frei von gewerblichen Schutzrechten sind.

Haftung

Für den Fall, dass in IT-Administrator unzutreffende
Informationen oder in veröffentlichten Programmen,
Zeichnungen, Plänen oder Diagrammen Fehler ent-
halten sein sollten, kommt eine Haftung nur bei
grober Fahrlässigkeit des Verlags oder seiner Mit-
arbeiter in Betracht. Für unverlangt eingesandte
Manuskripte, Produkte oder sonstige Waren über-
nimmt der Verlag keine Haftung.

Manuskripteinsendungen

Die Redaktion nimmt gerne Manuskripte an. Diese
müssen frei von Rechten Dritter sein. Mit der Ein-
sendung gibt der Verfasser die Zustimmung zur Ver-
wertung durch die Heinemann Verlag GmbH. Sollten
die Manuskripte Dritten ebenfalls zur Verwertung
angeboten worden sein, so ist dies anzugeben.
Die Redaktion behält sich vor, die Manuskripte
nach eigenem Ermessen zu bearbeiten. Honorare
nach Vereinbarung.

So erreichen Sie den Leserservice

Leserservice IT-Administrator
Stephan Orgel
65341 Eltville
Tel.: 06123/9238-251
Fax: 06123/9238-252
E-Mail: leserservice@it-administrator.de

Bankverbindung für Abonnenten

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. 85
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. 85
80802 München
Tel.: 089/4445408-20
Fax: 089/4445408-99
E-Mail: kathrin@it-administrator.de

T und I	S. 31	IBM	S. 84	Strato	S. 02, S. 13
ExperTeach	S. 29	IGEL	S. 49	Teldat	S. 05
Fast Lane	S. 67	Lancom	S. 25	webtopia (myLoc managed IT)	S. 19
Galileo	S. 41	Servermeile	S. 47		
HP	S. 35	Sicontact	S. 42, S. 43		

INSERENTENVERZEICHNIS

Das IT-Administrator Komplettprogramm!!!

NEU!

Jetzt auch inklusive
E-Paper!

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

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



Als bestehender Jahresabonnent
können Sie hier upgraden:

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

Oder Sie sind Neukunde? Hier können Sie bestellen:

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

www.it-administrator.de

 **Heinemann Verlag**
Im Dialog mit Spezialisten.

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München

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

Vertrieb, Abo- und Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville
Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de

Doppelte Virtualisierung. Geringere Betriebskosten. Keine Kompromisse.

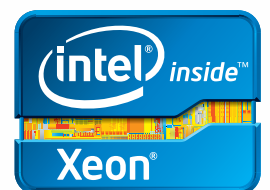


Sie suchen eine IT-Lösung, die den wachsenden Ansprüchen an Ihre Infrastruktur gerecht wird? IBM Flex System™ mit Intel® Xeon® Prozessoren verbindet Einfachheit, Flexibilität und Steuerbarkeit in einem System – ganz ohne Kompromisse.

Es unterstützt doppelt so viele virtuelle Maschinen wie die vorherige Generation Blade Server.¹ IBM Flex System Manager™ hilft Ihnen außerdem dabei, die Betriebskosten zu senken. Denn Transparenz und Kontrolle aller virtuellen und physischen Anwendungen wird so von einem einzigen Gerät aus möglich.²

Sie können zwischen verschiedenen Elementen wählen und sie selbst integrieren. Aber natürlich steht Ihnen auch Ihr IBM Geschäftspartner gerne zur Seite. Oder Sie entscheiden sich für IBM PureFlex™ System und nutzen das integrierte Expertenwissen von IBM für eine einfachere Bedienung. Erfahren Sie mehr unter ibm.com/systems/de/nocompromise/

Sehen Sie selbst, warum Clabby Analytics das IBM Flex System für das Beste auf dem Markt hält. Jetzt den Bericht herunterladen unter ibm.com/systems/de/nocompromise/



¹Basiert auf IBM Testverfahren und der Dokumentation zur IBM System x® Sizing-Methode für die Server-Virtualisierung und -Konsolidierung. IBM Flex System x240 unterstützt 2,7-fach mehr Peak Utilization Virtual Machines (VMs) als BladeCenter® HS22V der früheren Generation. ²Auf Grundlage des IDC-Whitepapers „The Economics of Virtualization: Moving Toward an Application-Based Cost Model“, Michelle Bailey, November 2009, <http://www.vmware.com/files/pdf/Virtualization-application-based-cost-model-WP-EN.pdf> Optionaler Storage Node für das IBM Flex System ist ab dem vierten Quartal 2012 verfügbar.

IBM, das IBM Logo, ibm.com, PureFlex, IBM Flex System Manager, IBM Flex System, BladeCenter und System x sind Marken oder eingetragene Marken der International Business Machines Corporation in den Vereinigten Staaten und/oder anderen Ländern. Die komplette Liste der IBM Marken siehe unter: <http://www.ibm.com/legal/us/en/copytrade.shtml>. Intel, das Intel Logo, Intel Inside, das Intel Inside Logo, Xeon und Xeon Inside sind Marken oder eingetragene Marken der Intel Corporation oder ihrer Tochtergesellschaften in den Vereinigten Staaten und/oder anderen Ländern. © 2012 IBM Corporation.