

iAdministrator

Das Magazin für professionelle System- und Netzwerkadministration

**Im Test:
Dot Hill
AssuredSAN 3.000-Serie** 18

**Im Test:
sayFUSE Smart Server** 23

**Systeme:
Storage-Design für VMware** 44

**Systeme:
Datenwiederherstellung im Notfall** 49

**Workshop:
TByte-SAN im Eigenbau realisieren** 53

Storage



Wolken nicht immer schwarz malen

Liebe Leser,

wenn Sie diese Ausgabe in Händen halten, ist gerade die Storage Networking World (SNW) zu Ende gegangen und einige von Ihnen werden sicherlich vor Ort in Frankfurt gewesen sein. Bei Drucklegung des Magazins lag der Kongress noch in der Zukunft – wir wollen im Rahmen einer kleinen Vorausschau schon jetzt versuchen, ein Fazit der Veranstaltung zu ziehen.



Geht es um das meistgenutzte Schlagwort der SNW, dürften sich wohl "Virtualisierung" und "Cloud Computing" Platz 1 streitig machen. Für letztgenanntes Thema haben die Organisatoren sogar einen eigenen Vortragsstrang geschaffen. Virtualisierung führt bei den meisten IT-Leitern zu positiven Gedankenströmen, da es den Herstellern recht erfolgreich gelungen ist, mit der Technologie Konsolidierung und Kosteneinsparungen ins Haus zu bringen. Administratoren dürften da – die Zurufe lauten hier komplexes Management und mögliche Inkompatibilitäten in heterogenen Umgebungen – schon etwas kritischer hinsehen. Vollends ins Skeptische schlägt die Stimmung dann um, wenn es um die Datenhaltung in der Wolke geht. Unternehmenswissen in den Händen eines externen Storage-Providers? Was ist denn da mit der Sicherheit? Und dem Verbleib der Daten, sollte ein Anbieter Pleite machen?

Vorträge und Fachgespräche auf der SNW hatten die Chance, diese Bedenken zu zerstreuen oder wenigstens zu relativieren. Wir wagen zu prophezeien, dass die Parole "Daten nur in Unternehmenshand!" nicht auf ewig und zu 100 Prozent zu halten sein wird – zu groß sind die Vorteile, die eine Flexibilisierung des Datenbestandes mit sich bringt. Statt sich auf die Seite der ewigen Skeptiker zu schlagen, sollten Verantwortliche und Techniker lieber gemeinsam herausfinden, wo ihr Unternehmen auch im Storage-Bereich von der Wolke profitieren kann.

Wer nicht nur theoretisieren möchte, sondern Wert auf Praxis legt, ist außer auf der SNW auch mit diesem Heft gut bedient. Ab Seite 18 erfahren Sie, wie sich die Appliance AssuredSAN 3.000 in unserem Test geschlagen hat und auf was Sie bei der Auswahl von Solid State Storage achten sollten (Seite 36). Außerdem bringen wir Ihnen in unseren Workshops nahe, auf welche Art von Speicher Sie in VMware-Umgebungen setzen sollten (Seite 44) und wie Sie mit günstiger Hardware und etwas Know-how ein SAN im Eigenbau konstruieren (Seite 53).

Viel Spaß beim Lesen, Ihr

A handwritten signature in blue ink, appearing to read 'Lars Nitsch'.

Lars Nitsch
Redakteur

Das IT-Administrator Komplettprogramm!!!

Sichern Sie sich jetzt das **IT-Administrator Jahresabo All-Inclusive** mit allen Monatsausgaben, Sonderheften und der Jahres-CD.

Statt Euro 29,90 zahlen Sie dabei für jedes Sonderheft nur Euro 19,90 – und müssen keine zusätzliche Bestellung mehr tätigen.

Automatisch bekommen Sie im März und Oktober jeden Jahres das jeweilige IT-Administrator Sonderheft und mit Ihrer Dezemberausgabe die jeweilige Jahres-CD mit allen Monatsausgaben des Jahres im PDF-Format zugestellt.



Als bestehender Jahresabonnent können Sie hier upgraden:

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

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

INHALT

IT-Administrator – Ausgabe November 2010

Storage

Einkaufsführer: Solid State Storage



Solid State Storage, also Speicher auf Basis von Chips, die ihre Informationen auch ohne Strom nicht verlieren, wird immer beliebter. Diese Chips liefern hohe Zugriffsgeschwindigkeit, geringen Stromverbrauch bei wenig Abwärme und große Toleranz gegenüber Umwelteinflüssen. Dies macht die Technologie für unterschiedlichste Anwendungsszenarien interessant; entsprechend vielfältig sind die Formfaktoren und Gehäuse, in denen Nutzer SSDs kaufen können. Unser Einkaufsführer erklärt, welche Produktformen und Einsatzgebiete Solid State derzeit bietet.

Seite 36

Neue Features im SQL Server 2008 R2

Mit SQL Server 2008 R2 wartet Microsoft mit einigen Neuerungen in punkto Skalierbarkeit, Performance und Produktivität auf. Vor allem im Bereich Business Intelligence und Data Warehouses mit extrem großen Datenmengen gibt es interessante Veränderungen – nicht zuletzt bieten die Redmonder zwei komplett neue Editionen des SQL-Servers für große Rechenzentren an. Beim Thema Business Intelligence will Microsoft hingegen auch Anfänger ansprechen, die mit der Aufbereitung Ihrer Daten noch keine große Erfahrung haben. IT-Administrator hat sich die neue Version angesehen und stellt die Neuheiten und überarbeiteten Funktionen vor.

Seite 40



Server- und Systemmanagement



Clientmanagement



Storage



Sicherheit



Messaging

Themenübersicht



Virtualisierung



Netzwerkmanagement



Job/Weiterbildung



Recht

AKTUELL

- 06 **News**
- 13 **ITANet aktuell:** IT-Administrator-Workshop "Sicherheit für Windows-Clients" am 16. November 2010 in München Schotten dicht!
- 14 **IT-Administrator vor Ort:** IT Admin Tech Talk 2010, 27. und 28. September, Oberursel bei Frankfurt/M. Erfolgreiche Premiere
- 16 **IT-Administrator vor Ort:** VMworld 2010, 30. August bis 2. September, San Francisco Neue Wege, klare Ziele

PRODUKTE

- 18 **Im Test:** Dot Hill AssuredSAN 3.000-Serie Flinker Datensammler
- 23 **Im Test:** sayFUSE Smart Server Platte wechsle dich
- 28 **Im Test:** Citrix XenApp 6 Applikationszentrale für Terminalserver
- 36 **Einkaufsführer:** Solid State Storage Keine ordinäre Festplatte

PRAXIS

- 40 **Systeme:** Neue Features im SQL Server 2008 R2 Die intelligente Datenbank
- 44 **Systeme:** Wahl des richtigen Storage für VMware Schmuckes Heim für virtuelle Maschinen
- 49 **Systeme:** Datenwiederherstellung im Notfall Wider dem Datenverlust
- 53 **Workshop:** TByte-SAN im Eigenbau realisieren Unser neues Datenhäusle
- 56 **Workshop:** Citrix XenServer 5.6 über die PowerShell sichern Backup per Skript
- 61 **Workshopserie:** Stolperfallen bei der Umstellung auf IPv6 (1) Protokoll mit Tücken
- 66 **Workshopserie:** Drucken im Netzwerk (2) Drucker in Reih und Glied
- 72 **Tipps, Tricks & Tools**

WISSEN

- 76 **Know-how:** Accounting in virtuellen Umgebungen Virtuelle Maut
- 79 **Buchbesprechung** "Windows PowerShell 2.0 – Das Praxisbuch" und "Konzepte & Lösungen für Microsoft-Netzwerke"
- 80 **Website & Fachartikel online**

RUBRIKEN

- 03 **Editorial**
- 05 **Inhalt**
- 51 **Seminarmarkt**
- 81 **Das letzte Wort**
- 82 **Vorschau, Impressum, Inserentenverzeichnis**

Einheitliches Management für Netgear-Produkte

Mit der neuen **ProSafe-Managementkonsole NMS200** bietet **Netgear** ein Werkzeug für die einfache **Verwaltung von Netgear-Geräten** in einem Unternehmensnetz an. IT-Administratoren erhalten mit der Konsole eine zentrale Verwaltungsplattform, die ihnen Kontrolle über sämtliche eingebundenen Switching-, Wireless-, Storage- und Sicherheitslösungen von Netgear bietet. Das für bestehende Kunden kostenfreie neue Network Management-System liefert Überwachungs- und Konfigurations-Funktionen. Bei Inbetriebnahme entdeckt die Software automa-

tisch die unterstützten Netgear-Produkte und ermöglicht eine Überwachung und Verwaltung der Performance. Zum Start lassen sich mit der NMS200 ausschließlich Managed Switches verwalten – zukünftige Versionen sollen die Unterstützung für Smart Switches, Wireless-, Storage- und Security-Lösungen von Netgear mitbringen. Daneben bringt Netgear im Dezember einen neuen Ma-

naged Switch mit 10 GBit-Ethernet auf den Markt. Der ProSafe 24-Port 10 GE Managed L2+ Switch XSM7224S bietet eine Performance von 10 GBit/s sowie lokalen und Remote-Stacking-Support. An Anschlüssen stehen neben den 24 SFP+-Ports vier 10 GBit/s RJ45-Ports zur Verfügung. Das Gerät soll für 8.590 Euro auf den Markt kommen. (dr)

Netgear: www.netgear.de



Der neue Switch XSM7224S von Netgear bietet Layer 2- und Layer 3-Features

Zentrale Adressverwaltung

Infoblox bringt das **Microsoft Management Modul NIOS** auf den Markt – eine Agenten-freie und Appliance-basierte Lösung, die zentrale **Management-Funktionen für Microsoft DNS- und DHCP-Umgebungen** bietet. Dabei steht Administratoren eine einheitliche Verwaltungsoberfläche in Bezug auf DNC, DHCP sowie das IP-Adress-Management zur Verfügung. Dazu lässt sich die Appliance parallel zu existierenden DNS/DHCP-Infrastrukturen nutzen, die

entweder auf Infoblox oder Microsoft DNS/DHCP-Servern laufen. An Features bietet das Modul zentrales Management und Instandhaltung des Microsoft DNS/DHCP-Servers, unternehmensweite automatisierte Funktionen zur IP-Adressverwaltung, rollenbasierte Administration und detaillierte Audit-Logs sowie ein automatisiertes Disaster Recovery. Das Management-Modul synchronisiert zudem automatisch Microsoft DNS- und DHCP-Änderungen im Netzwerk. Dies

ermöglicht etwa die automatische DNS- und DHCP-Rekonfiguration der Microsoft-Server nach einem Ausfall. Das Web-Interface des Moduls erstellt daneben detaillierte grafische Reports zum Netzwerk sowie der Zuweisung und Nutzung der IP-Adressen. Dies soll die Planung und das Troubleshooting im Netzwerk erleichtern. Ab 8.990 US-Dollar ist die Appliance erhältlich. (dr)

Infoblox: www.infoblox.com/en/products/nios-for-microsoft-management.html

Augen fürs Netzwerk

LevelOne präsentiert zwei neue **PoE-Netzwerk-Kameras** für den Einsatz in sicherheitssensiblen Umgebungen. Die Modelle **FCS-1131** und **FCS-1141** richten sich in Sachen Funktionalität und Ausstattung speziell an Unternehmen und Einrichtungen, die beispielsweise ihr Gelände oder ihre Produktionsprozesse überwachen möchten. Die Variante FCS-1131 kommt mit einer Auflösung von 2 Megapixeln und ist PoE-fähig. Das Gerät liefert dabei HDTV-Qualität und unterstützt den SMPTE-Standard. Des Weiteren unterstützt die Netzwerkkamera das Format 16:9 sowie den Komprimierungsstandard H.264 zur Bandbreitenkontrolle innerhalb des Netzwerkes. Ein integrierter SD/SDHC-Karteneinschub ermöglicht die

lokale Speicherung der Videobilder im Falle eines Netzwerkausfalls. Dank BNC-Anschluss ist es zudem möglich, den analogen Videostream an einem separaten Monitor auszugeben. Beim Modell FCS-1141 handelt es sich um eine 1,3 Megapixel PoE-Netzwerk-Kamera, die ihre Qualitäten besonders an Orten mit schwierigen Lichtverhältnissen ausspielen soll. Das Aufzeichnungsgerät verfügt über einen Sony CCD-Sensor mit progressiver Abtastung. Die Komprimierungsverfahren H.264, MJPEG und MPEG-4 werden ebenfalls unterstützt und sollen eine gute Performance bei geringen Bandbreitenanforderungen an das Netzwerk gewährleisten. Wie bei der FCS-1131 gehören auch bei der FCS-1141 der integrierte SD/SDHC-Karten-

einschub, ein BNC-Anschluss sowie die Unterstützung der PoE-Technologie zur Ausstattung. Das Modell FCS-1131 ist für rund 730 Euro erhältlich, die Kamera FCS-1141 kostet rund 840 Euro. (dr)

LevelOne: www.level-one.de/levelone.php?page=prod&cat=7004



Die Netzwerkkamera FCS-1141 soll auch mit schwierigen Lichtverhältnissen gut klarkommen

Mehr Farbe für den Arbeitsplatz

LaCie ergänzt seine **Monitor-Reihe** um das Modell **324i** mit **10-Bit P-IPS LCD-Display**. Der Bildschirm bietet eine Auflösung von 1.920 x 1.200 dpi und eignet sich dank einer hohen Farbtreue laut Hersteller besonders für Grafik- sowie Webdesign und Fotobearbeitung. Das P-IPS-Display soll dabei eine realistische und farbgetreue Darstellung ohne Verzerrungen bieten. Das Modell verfügt über einen Farbraum von 102 Prozent NTSC und 98 Prozent Adobe RGB. Der Blickwinkel von 178 Grad erlaubt zudem aus verschiedenen Winkeln die gleiche visuelle Qualität ohne Bildverzerrung oder Farbverlust. Dank eines Blendschutzes gibt es keine Lichtspiegelungen, die bei glänzenden Displays sonst häufig auftreten. Durch Drehen des Monitors um 90 Grad erfolgt ein Wechsel vom Querformat ins Hochformat. Zusätzlich zu einem Kontrastverhältnis von 1.000:1 und der Stabilisierung der Hintergrundbeleuchtung kann der Nutzer den Bildschirm mit dem optionalen Ka-



Der Monitor 324i von LaCie soll eine besonders hohe Farbtreue bieten

librierungstool LaCie blue eye weiter optimieren. Die Software stellt beispielsweise bei der Druckvorstufe die Möglichkeit bereit, die Softproofing-Genauigkeit zu verbessern. Der Monitor verfügt über vier Display- sowie Video-Eingänge. Für Videoquellen wird der DisplayPort-, DVI-D-, HDMI- oder Component-Anschluss verwendet, um den Monitor zu verbinden. Zusätzlich hat das Modell drei USB 2.0-Anschlüsse für einen praktischen USB-Hub zum Computer. Ab 1.134 Euro ist der Bildschirm erhältlich. (dr)

LaCie: www.lacie.com/de/products/product.htm?pid=11570

Virtuelle Umgebungen im Griff

Veeam gibt **Version 5.0** von **Veeam Monitor** frei, einer Software zur **Überwachung von virtualisierten, auf VMware beruhenden Umgebungen**. Das neue Release bietet zahlreiche Informationen und Anleitungen zu Alarmmeldungen und Systemdaten sowie eine verbesserte Skalierbarkeit, die ein Monitoring von mehr als 200 ESX(i)-Hosts aus einer einzigen Installation heraus ermöglichen soll. Außerdem unterstützt die Lösung vSphere 4.1 mit über 100 neuen Leistungskennzahlen. Die Software Monitor 5.0 bringt nun außerdem ein eigenes Dashboard für jedes Objekt im Infrastrukturbaum der

virtualisierten Landschaft mit. So sind die wichtigsten Informationen zu jedem beliebigen Objekt auf einen Blick zu sehen. Ein Drill-down per Mausclick fördert auf Wunsch mehr Details zu Tage. Weitere neue Features sind das Monitoring logischen Festplatten-Speicherplatzes, die Überwachung von Snapshots und sogenannte "Infrastructure Overview Reports" – automatisch erstellte Berichte, die einen Überblick über die virtualisierte Infrastruktur geben sollen. Veeam Monitor 5.0 ist ab sofort verfügbar. Die Preise beginnen bei 220 Euro pro Socket. (In)

Veeam: www.veeam.com/vmware-esx-monitoring.html

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

Bacula Systems bringt seine Open Source Backup- und Restore-Lösung für den Unternehmenssatz, die **Bacula Enterprise Edition**, in Version 4.0 auf den Markt. Mit der neuen Version stehen erstmals Backup-Funktionen in einem Open Source-Produkt zur Verfügung. Zu den wichtigsten Funktionen der neuen Bacula Enterprise Edition 4.0 gehören das BWeb Enterprise Management Center zur Verwaltung mehrerer Rechenzentren, die Skalierbarkeit bis zu tausenden Servern und Clients und ein modulares multi-threaded Design. Die Einstiegspreise für den zugehörigen Support beginnen bei 3.900 Euro. (dr)

www.baculasystems.com

Version 5.0.2 des kostenlosen **BlackBerry Enterprise Server Express** ist nun auch in deutscher Sprache verfügbar. Die Software enthält zahlreiche Features, die im kürzlich präsentierten BlackBerry Enterprise Server 5.0.2 integriert sind. So bietet die neue Version Single Sign-On, das dem Nutzer eine Passwortabfrage für den Zugang zum Intranet sowie Daten hinter der Firewall, dem BlackBerry Web Desktop Manager und dem BlackBerry Administration Service für BlackBerry Enterprise Server Express erspart. (dr)

www.blackberry.com/besexpress

Brocade unterstützt den neuen **Fibre Channel-Standard FC-P15**, der Übertragungsgeschwindigkeiten von bis zu **16 GBit/s** ermöglicht. Der neue Standard ist laut Hersteller vor allem für Storage-Clouds und hoch skalierbare Virtualisierung geeignet. Die Durchsatzrate von maximal 16 GBit/s soll die Bandbreite und I/O-Performance erheblich steigern und die gewachsenen Anforderungen von Cloud-Architekturen adressieren. Brocade will die ersten 16 GBit/s-FC-Produkte voraussichtlich in der ersten Jahreshälfte 2011 auf den Markt bringen. (In)

www.brocade.com

Marathon Technologies bietet die Software **everRun MX** an, eine **fehlertolerante Lösung für symmetrisches Multiprocessing (SMP)** sowie Multicore-Server und -Anwendungen. Durch die Lösung lassen sich zwei hardwarebasierte Windows-Server zu einem virtuellen Server zusammenschalten, was zu einer 99,999 prozentigen Verfügbarkeit führen soll. Dabei ist keine besondere Hardware notwendig, vielmehr erkennt die Software Hardware-Änderungen automatisch. Ab 8.000 Euro ist everRun MX erhältlich. (dr)

www.marathontechnologies.com

Neues Zuhause für SOHO-Daten

Fujitsu erweitert sein Angebot für kleinere Unternehmen um den NAS-Server **CELVIN Q800**. Der Nutzer kann das **Storage-System** mit maximal vier SATA-Festplatten bestücken, die sich im laufenden Betrieb auswechseln lassen. Was die Kapazität der einzelnen Magnetspeicher betrifft, unterstützt das Gerät 1 / 2 TByte sowie in Zukunft auch 3 TByte. Die Platten lassen sich in den RAID-Leveln 0, 1, 5, 5+HS und 6 gruppieren – der Wechsel zwischen den verschiedenen Modi und die Erweiterung eines RAID sind online möglich. Ferner kann der NAS-Würfel als iSCSI-Zielserver und -initiator fungieren. Zu den weiteren Funktionen des Speichers

gehört das Management von maximal vier IP-Kameras. Unter der Haube sollen ein Intel Atom-Prozessor mit 1,8 GHz, 1 GByte RAM und ein schlankes, eingebettetes Linux für genügend Leistung sorgen und dabei trotzdem nur 37 Watt im normalen Betrieb verbrauchen. Zuständig für die Verbindung nach außen sind vier USB-Ports, zwei für Load Balancing geeignete GBit-LAN-Anschlüsse, zwei eSATA-Buchsen und ein VGA-Port für Wartungsarbeiten. Der NAS-Server ist ab Mitte November erhältlich. Mit zwei HDDs zu je 1 TByte ausgestattet, schlägt das Gerät mit rund 900 Euro zu Buche. (ln)

Fujitsu: <http://de.fujitsu.com>



Im Vergleich zu den bisher angebotenen NAS-Modellen hat Fujitsu die Variante CELVIN Q800 um einige Features ausgebaut

Business-Server von Lenovo

Lenovo bietet mit den Modellen **ThinkServer RD230, RD240** und **TD230** drei neue **Server im Tower- und Rack-Format** an. Die RD230 und RD240 Rack-Server richten sich an wachsende Unternehmen und deren geschäftskritischen Applikationen. Die Modelle verfügen über Web-basierte Remote-Management-Tools sowie im Fall des RD230 über ein serienmäßig integriertes RAID für erweiterte Datensicherheit. Durch die Remote-Tools kann ein Anbieter von Managed-Services etwa die IT-Systeme seines Kunden über-

wachen und verwalten. Hot-Swap-fähige Festplatten sollen daneben Ausfallzeiten minimieren. Die Server arbeiten mit Prozessoren der Intel Xeon 5500- und 5600-Serien. Dadurch können sie laut Hersteller bis zu 60 Prozent schneller arbeiten als Vorgängersysteme. Mit bis zu acht Festplatten, 8 TByte an Speicherkapazität und zwei Netzteilen versorgt der im Vergleich zum ThinkServer RD230 nur wenig größere RD240 Rack-Server Unternehmen mit allem, was notwendig ist, um Hochleistungsdatenbanken, Transaktionen und an-

dere Geschäftsanwendungen zu betreiben und auszuführen. Der Tower-Server TD230 ist für das Energiesparen optimiert und bietet beispielsweise ein Netzteil, das eine Effizienz von über 90 Prozent aufweisen soll. Der Rechner wurde als Dual-Prozessor-Server nach den EnergyStar Server 1.0-Spezifikationen entwickelt und arbeitet laut Anbieter zudem besonders leise. Die Preise für die ThinkServer TD230, RD230 und RD240 beginnen bei 935 Euro, 1.059 Euro beziehungsweise 1.165 Euro. (dr)

Lenovo: www.lenovo.de

Switch für virtuelle Netze

BLADE Network Technologies stellt den **Top-of-Rack Gigabit Ethernet Switch RackSwitch G8052** vor. Der Switch ist mit 48 Gigabit-Ethernet-Ports und vier 10 GBit-Ethernet SFP+ Uplink-Ports ausgestattet. Durch das ASIC-Design, geringe Latenzzeiten von 1,7 Mikrosekunden, optimiertem Luftstrom,

Line-Rate-Switching und zusätzlichen Paket-Puffer soll er eine gesteigerte Leistung und Effizienz für den Einsatz in virtualisierungsintensiven Umgebungen bieten. Die VMready-Zertifizierung stellt dabei sicher, dass die Einstellungen hinsichtlich Quality of Service (QoS) und VLAN sowie Access Control List (ACL) automa-

tisch übernommen werden, sobald virtualisierte Anwendungen von Server zu Server migrieren. Dadurch wird eine erweiterte Sicherheit für unternehmenskritische Anwendungen und Daten erreicht und das Management vereinfacht. Der RackSwitch ist zudem mit "Explicit Congestion Notification" (ECN) und "Weighted Random Early Detection" (WRED) ausgestattet. Damit erfolgt eine Kontrolle des Paketflusses der Server, um große Unterschiede im Netzwerkdurchsatz, die die Geschwindigkeit der Anwendungen drosseln, zu vermeiden. Ab 6.600 US-Dollar ist der Switch zu haben. (dr)

BLADE: www.bladenetwork.net/G8052.html



Der RackSwitch G8052 richtet sich an virtualisierte Infrastrukturen

Keine blinden Flecken beim Monitoring

Version 8 von **PRTG Network Monitor** ist ab sofort verfügbar. Die **Netzwerküberwachungssoftware von Paessler** wartet mit zahlreichen Neuerungen auf: Das Werkzeug ist mit neuen Sensor-Typen ausgestattet, so dass Nutzer eine höhere Anzahl an verschiedenen Geräten und Diensten überwachen können. Insgesamt verfügt das Tool über mehr als 80 Sensor-Typen für das Monitoring von VoIP-Anwendungen, Webseiten, E-Mailservern, Datenbanken, Applikationen und virtuellen Umgebungen. Zudem ist es dazu in der Lage, auch Linux- und UNIX-Umgebungen mit sieben neuen Sensoren in das zentrale Monitoring einzubeziehen. Ebenfalls neu ist ein echtes Clustering der Monitoring-Lösung. Alle Cluster-Nodes (maximal vier) überwachen permanent das Netzwerk. Jeder Knoten verfügt dabei über eine eigene Datenbank, was eine kontinuierliche Sicherung der PRTG-Konfiguration und der Monitoring-Daten gewährleisten soll. Zu den weiteren neuen Features zählt der im Web-Interface integrierte Google-Maps-Support, der die Anzeige geographischer Karten sowie die sofortige Verfügbarkeit historischer Daten erlaubt. Laut Hersteller vereint das Tool alle Features in einer Lizenz – lediglich die Anzahl der Sensoren bestimmt den Preis. 500 Sensoren etwa sind für 900 Euro zu haben. (In)

Paessler: www.de.paessler.com/prtg/



Der PRTG Network Monitor von Paessler nimmt nun auch Linux-Systeme in die überwachte Umgebung auf

Drucken per E-Mail

HP bietet die zwei neuen **Officejet-Modelle Pro 8500A e-All-in-One** sowie **8500A Plus e-All-in-One** an. Die beiden Geräte ermöglichen dank **ePrint-Technologie** das Ausdrucken von Dokumenten per E-Mailversand. Nach einer Sicherheitsprüfung werden Präsentationen, Dokumente oder Broschüren ohne PC automatisch ausgedruckt. Spam-Filter und eine hinterlegte User-Liste erlauben nur den Anwendern Zugriff, die dazu autorisiert sind. Daneben erlauben vorinstallierte Apps, Web-Inhalte direkt am Drucker zu nutzen und auszudrucken. Das zugehörige Display mit TouchSmart-Screen soll mit 6,1 Zentimetern beim 8500A beziehungsweise 10,9

Zentimetern beim Pro 8500A groß genug sein, um die Eingabe der benötigten Informationen problemlos zu ermöglichen. Die beiden e-All-in-Ones verfügen neben Druck-, Scan-, Kopier- und Faxfunktion auch über HP Easy Wi-Fi-Technologie und lassen sich so via WLAN anbinden. Die Geräte drucken bis zu 35 Seiten pro Minute in schwarz/weiß und bis zu 34 Seiten in Farbe und sind mit einer automatischen Duplexfunktion ausgestattet. Die 250-Blatt-Papierzuführung lässt sich um eine zweite Papierkassette für weitere 250 Blatt erweitern. Der HP Officejet Pro 8500A wartet außerdem mit einer 35 Blatt fassenden, automatischen Dokumentenzuführung auf; bei der Plus Version sind es 50 Blatt (Duplex). Der HP Officejet Pro 8500A e-All-in-One (CM775A) ist für 227 Euro erhältlich, der HP Officejet Pro 8500A Plus e-All-in-One (CM756A) für 294 Euro. (dr)

HP: www.hp.com/de/



Der HP Officejet Pro 8500A lässt sich auch per E-Mail über das Internet ansteuern

Access Points tanzen nach einer Pfeife

Funkwerk Enterprise Communications stellt mit dem **bintec WLAN Controller** eine Software vor, mit der sich bis zu 24 Access Points des Herstellers konfigurieren und überwachen lassen. Ihr besonderes Augenmerk wollen die Entwickler der Lösung auf deren schnelle Inbetriebnahme gelegt haben: Ein Wizard beschränkt die Schnellinstallation auf fünf Schritte und soll so die Konfiguration des WLAN-Netzes in weniger als 30 Minuten ermöglichen. Neue Access Points erkennt das Werkzeug automatisch und integriert diese per Plug&Play in das Funknetz. Das automatische Radio Frequency Management-System übernimmt

die Suche nach freien Kanälen und wählt die günstigsten für das Gesamtsystem aus. Die Administrations-Software ist in den Routern und Access Points der bintec R-Serie, W- und WI-Serie ab Release 7.9.6 enthalten und ist über eine Lizenz freischaltbar. In der kleinsten Ausbaustufe bis sechs Access Points wird keine zusätzliche Hardware benötigt, da sich die Software auf einem Master-Access Point betreiben lässt. Bei der Verwaltung von mehr als sechs Access Points ist ein Router der bintec R-Serie als Hardware nötig. Pro sechs Lizenzen kostet der Software-Controller rund 400 Euro. (In)

Funkwerk: <http://it-a.eu/aaa12>

Luchs im Schafspelz

Lynx baut sein Server-Portfolio um die Modelle **High-Performance Server 1440** und **2840** aus. Beide vereinigen in einem Chassis zwei beziehungsweise vier Boards – auf zwei Höheneinheiten lassen sich so bis zu vier vollwertige, individuell konfigurierbare Server betreiben. Jeder Rechner ist mit einem Intel 5520-Chipsatz bestückt und lässt sich mit bis zu zwei Intel Prozessoren der Serien 5500 oder 5600 aufrüsten. Maximal sind **48 Prozessorkerne mit 786 GByte Arbeitsspeicher** möglich. Im Einsatz sieht der Hersteller die neuen Systeme als **Infrastruktur Server für Cloud-Computing, Web 2.0-Umgebungen sowie für Cluster-Infrastrukturen**. Um Ausfallzeiten so gering



Zwei Server-Boards mit Intels 5520-Chipsatz finden sich in nur eine Höheneinheit messenden High-Performance Server 1440 von Lynx

wie möglich zu halten, lässt sich jeder Rechenknoten einzeln und per Fernwartung verwalten. Je nach Modell finden bis zu drei Hotswap-SATA-Festplatten pro Mainboard Platz. Beim Modell 2840 sichert ein redundant ausgelegtes Netzteil die Stromversorgung. Was den Energieverbrauch angeht, wirbt Lynx mit deutlich geringeren Werten als bei der gleichen Anzahl einzelner Server und spricht von einer Energieeffizienz von bis zu 94 Prozent. Die Variante 1440 ist je nach Konfiguration zu einem Preis ab 2.450 Euro zu haben. (In)

Lynx: www.lynx-pc.de

3 TByte in der schwarzen Rüstung

Seagate erweitert die Funktionalität der NAS-Modelle **BlackArmor 440** und **220** um die **Unterstützung für 3 TByte-Festplatten**. Somit beträgt die maximale Nettokapazität der vier respektive zwei Magnetspeicher fassenden Netzwerkspeicher 12 beziehungsweise 6 TByte. Die beiden Storage-Server wurden für Unternehmen mit bis zu 50 Angestellten entwickelt, um Daten zentral und sicher abzulegen. Für ein Plus an Sicherheit soll neben den gängigen RAID-Modi eine hardwarebasierte Verschlüsselung sorgen. Zu den weiteren Funktionen zählt eine E-Mailbenachrichtigung, um Nutzer über den Status oder Änderungen am Server zu informieren, sowie die Möglichkeit, die Speicher-Komponente als FTP-Server zu betreiben. Das BlackArmor NAS 440 ist als RAID 5 voreingestellt und wird mit zehn Backup-Lizenzen ausgeliefert. Modell 220 ist in einer RAID 1-Konfiguration für automatische Datenspiegelung und mit fünf Backup-Lizenzen erhältlich. Der Preis für Variante 440 in der Maximalausstattung mit 12 TByte beträgt rund 1.175 Euro. (In)

Seagate: <http://it-a.eu/aaa13>



Auch die Variante BlackArmor NAS 220 von Seagate mit zwei Laufwerkeinschüben unterstützt nun 3 TByte-Platten

Eaton schickt Server schlafen

Eaton bringt die neue **Shutdown-Lösung Intelligent Power Protector (IPP)** auf den Markt. Die Software ermöglicht bei länger andauernden Stromausfällen das **geordnete Herunterfahren von Computern und Servern**, die an ein USV-System angeschlossen sind. Sie ist eine Erweiterung von Eatons Intelligent Power Software-Produktlinie, die im Sommer 2009 mit dem Launch der Monitoring-Software Intelligent Power Manager (IPM) eingeführt wurde. Durch das geordnete Herunterfahren von IT-Systemen können begonnene Arbeiten gespeichert und Daten gesichert werden; dadurch entstehen bei einem Stromausfall keine Datenverluste oder Fehler im Dateisystem. Die Software IPP nutzt die gleiche einfach bedienbare, web-

basierende Oberfläche wie der IPM. Zusätzlich zum USV-Monitoring im Netzwerk ist es möglich, direkt angeschlossene Unterbrechungsfreie Stromversorgungen lokal über eine serielle oder eine USB-Schnittstelle zu überwachen. IPP verschickt Warn-E-Mails an Administratoren und Nutzer, falls Alarmer wie ein Netzausfall am USV-Eingang oder das Ende der Autonomiezeit anstehen, und sorgt für einen kontrollierten Shutdown, bevor die Batterie-Laufzeit endet. Dies trägt dazu bei, drohende Schäden zu minimieren, und ermöglicht zudem eine kürzere Reaktionszeit bei Störungen. Die Software ist ab sofort kostenlos auf der Hersteller-Webseite verfügbar. (dr)

Eaton: www.eaton.com

Download: <http://it-a.eu/aaa11>



USB Sicherheit Das braucht man wirklich!

Thorsten Scharmatin, Key Account Manager itWatch GmbH

Die Sicherheitsdefizite durch die generische Plug & Play-Pforte für Peripheriegeräte wie USB Memory-Sticks, Flash Pens, digitale Kameras, Scanner, Modems etc., sind seit langem bekannt: unerwünschte Inhalte sowie gefährliche Programme bedrohen die Integrität der Netze und entscheidendes Know-how des Unternehmens kann unerkannt abgezogen und vervielfältigt werden (*Data Loss oder Data Leakage*).

Die IT-Abteilungen der Unternehmen können das Problem mit Bordmitteln nicht in den Griff bekommen. Viele Lösungen sind am Markt, diese decken aber häufig nur einen Teil der Problematik ab. Zu den Interessen aus der IT-Sicherheit kommen noch die Anforderungen des Betriebes nach Effizienz und Kostensenkung - sowie die Notwendigkeit den Benutzer bei komplexeren Einsatzszenarien mit der nötigen Information in Echtzeit zu unterstützen.

Das Thema USB-Sicherheit ist damit breiter als nur das An- und Abschalten von USB-Sticks. In der Folge zeigen wir, was eine zukunftssichere Lösung beinhalten muss:

► Device- und Port-Kontrolle

Wer darf welche Funktion von welchem Device (Peripheriegerät und fest verbaute Hardware) wann und wo in welcher Situation nutzen? Die Nutzung von WLAN oder UMTS ist beispielsweise nicht an bestimmte Nutzer gebunden, sondern abhängig von den erreichbaren Netzen und verboten, solange eine LAN-Verbindung zum hausinternen Netz besteht.

► Content Kontrolle

Das Lesen von Word- oder PDF-Dokumenten von CD/ DVD mag freigegeben sein, aber es muss sichergestellt sein, dass diese Dokumente keine eingebetteten Schadprogramme enthalten (embedded executables). Die inhaltliche Analyse muss natürlich auf Archiven (ZIP etc.) und auf verschlüsselten Dokumenten oder Archiven mit den gleichen Mechanismen durchgeführt werden.

► Protokollierung und Alerting

Blockieren und Freigeben alleine genügt nicht, vielmehr ist bei den freigegebenen, sicherheitskritischen Aktionen auch die Protokollierung gefordert. Die Beweisbarkeit verschiedener sicherheitskritischer Aktionen ist heute in vielen Umgebungen ein notwendiger Teil der Compliance geworden. Um die Datenflut zu begrenzen, ist ein ausgeklügeltes Filterverfahren mit einfacher Administration notwendig. Bestimmte Ereignisse erfordern eine Echtzeitreaktion, wie etwa ein Alerting per Email oder SMS an einen vordefinierten Verteilerkreis. Sicherheitskritische Aktionen können u.a. sein:

- Datenbewegungen sensibler Daten,
- Nutzung kritischer Hardware (*Devices*) oder Anwendungen (*Applications*),
- der Zugriff von Anwendungen auf sensible Dateien,
- die Trennung der sicherheitsrelevanten Information (z.B. Vergabe eines neuen Schlüssels) von Systemmanagement-Information (z.B. Nichtverwendbarkeit eines USB-Gerätes wegen zu geringer Stromversorgung),
- Sonderfreigaben über Challenge Response oder Selbstfreigabe für den Notfall.

Alle Aktionen sind nach dem jeweiligen Nutzungskontext, etwa Uhrzeit, Wochentag etc., zu beurteilen, um die richtige Einschätzung in Echtzeit treffen zu können.



► **Benchmark des Risikos**

Die Protokollierung gibt die richtige Auskunft über die aktuelle Risikosituation und ermöglicht es, die Risiken anonym oder pseudonym in Qualität und Quantität direkt in das Risiko-Management zu übergeben. So kann immer auf Basis der realen Situation gehandelt werden.

► **Verschlüsselung sensibler Information**

Die Angriffe im ersten Quartal 2010 haben die Unsicherheit vieler selbstverschlüsselnder Memory-Sticks gezeigt. Die häufig verwendete Partitionsverschlüsselung hat wesentliche Nachteile, da ein einziger Schlüssel große Datenbereiche unwiderruflich „transparent“ frei gibt und die Daten für sogenannte USB-Dumper vollständig offen liegen. Deshalb sind moderne Verfahren mit Unternehmensschlüsseln und privaten Schlüsseln ausgestattet, die je nach Berechtigung des Anwenders und der Sensitivität der Daten zu einer optionalen oder zwangsweisen Verschlüsselung der Inhalte mit den richtigen Schlüsseln führen. Die zwangsweise Verschlüsselung mit einem Firmenschlüssel reduziert das Risiko des Datendiebstahls (Data Loss) auf null Prozent.

► **Kontrolle der Anwendungen**

Das Monitoring aller Anwendungen, deren Start überhaupt versucht wurde, mit den authentischen Merkmalen der Anwendung und weiteren Attributen, gibt den permanenten Überblick. Die Unterscheidung zwischen erlaubten und nicht erlaubten Anwendungen erfordert aus praktischen Gründen den Einsatz von Whitelists UND Blacklists, je Benutzer, PC oder Netzwerk. So kann z.B. Skype im Hausnetz verhindert, aber im Hotel über WLAN freigegeben werden. Alle Anwendungen – auch portable Apps – können mit ApplicationWatch inventarisiert, kontrolliert, und die Zugriffsrechte der Anwendungen unabhängig vom Recht der Anwender definiert werden, um z.B. unerwünschte Uploads ins Internet sicher zu verhindern.

► **Kontrolle der verwendeten Netze**

Die Netzwerk-, UMTS-Karten, WLAN-Geräte oder andere Zugangsmöglichkeiten zu weiteren Netzen, wie etwa Modems in PDAs, verbinden den Rechner mit potentiell gefährdeten Netzen. Durch die Unterscheidung zwischen erlaubten und nicht erlaubten Netzen kontrolliert die IT-Abteilung diese Kontakte. Entsprechend des erkannten Netzes wird die gültige Security Policy in Echtzeit eingestellt – (Heim Arbeitsplatz, Firmenzentrale, Standort Produktion, Schulung, etc.), so dass der PC netzbasiert die richtige Sicherheitseinstellung durchsetzt und die Rechte nicht mehr am Anwender hängen.

► **Personalisierung von Datenträgern**

Günstige Datenträger verfügen über keine eigenen Merkmale wie Seriennummern. Die Personalisierung von Datenträgern für Nutzer oder Projektgruppen ist hier Voraussetzung für eine kosteneffiziente individuelle Administration. Den „unternehmenseigenen Datenträger“ erstellt man am besten durch Personalisierung auf die Gruppe der Domänenbenutzer und vermeidet dadurch aufwändige Verfahren der Pflege von Seriennummern und den Einkauf teurer Hardware.

► **Security Awareness in Echtzeit**

Die Belange des Datenschutzes und der lokal gültigen Datenschutzgesetze sowie anderer branchentypischer Auflagen sind für den Endanwender nicht immer einfach zu verstehen. Zentrale Schulungen verpuffen oft, weil zu viele Inhalte, die nicht täglich angewendet werden, den Anwender überfordern.

E-Learning-Systeme werden häufig nicht geeignet wahrgenommen. Die beste Lösung ist alle Vorteile miteinander zu kombinieren und die Lerninhalte oder bestimmte elektronische Willenserklärungen (z.B. Zustimmung zur Protokollierung für Compliance) direkt an die kritische Aktion zu koppeln und die Zeitspanne bis zur Wiederholung des Anwenderdialogs in der Security Policy zu verankern um eine Häufung zu vermeiden.

► **Reports und Management Information**

Beweisbare Compliance auf Knopfdruck reduziert die Zeit der Prüfung, spart Geld und erlaubt es, die Kernfrage „Wie sicher sind wir?“ spontan und präzise zu beantworten. Revision, Auditoren, Risiko-Management und die Manager des Unternehmens haben mit historischer und Echtzeit-Auskunft über alle Ereignisse, nach Standorten, Abteilungen oder anderen Kriterien sortiert, echte Mehrwerte im Betrieb und können die Unternehmensressourcen zielsicher steuern.

► **Lokale Schleusenfunktion**

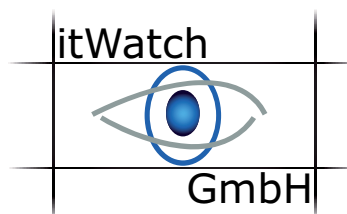
Entschlüsselung und Dekomprimierung in einer lokalen Quarantäne – erst dann können die Inhalte im Klartext geprüft werden. Je nach Ergebnis, werden die Dateien geblockt und sicher gelöscht, zur Prüfung an Dritte weitergeleitet oder freigegeben – zusätzliche Hardware und lange Wege sind unnötig.

Diese und viele weitere Herausforderungen löst die Endpoint Security Suite der itWatch auf mehreren Millionen PCs täglich mit Freigaben für NATO-restricted, Verschlussache NfD und GEHEIM. Sie skaliert nicht nur technisch für jede Unternehmensgröße, sondern auch für jedes Budget.

.....
Informieren Sie sich über umfassende DLP und Endgerätesicherheit bei unserem Vortrag am 16.11.2010 beim ITANet-Workshop „Sicherheit für Windows-Clients“.

Weitere Informationen erhalten Sie unter:

www.itWatch.de/events



Tel.: +49 (0) 89 620 30 100
Email: Info@itWatch.de
► www.itWatch.de

IT-Administrator-Workshop "Sicherheit für Windows-Clients" am 16. November 2010 in München **Schotten dicht!**

von John Pardey

Schwachstellen in Applikationen sind heute einer der breitesten Einfallswegen für Schadsoftware ins Unternehmen. Daher kann ein Patchen des Betriebssystems allein – etwa mit WSUS – nur circa 35 Prozent aller Sicherheitslücken schließen. Welche Wege bereitstehen, um umfassender zu patchen und Windows-Clients im Netz mit anderen Mitteln abzusichern, zeigt unser Workshop am 16. November in München.

Da unser Workshop-Thema "Client-Security" so facettenreich ist, haben wir uns für den November-Termin in München dazu entschlossen, das Programm auszudehnen und einen ganzen Tag mit spannenden Vorträgen zu bestücken. So beginnt diese Veranstaltung ausnahmsweise schon um 10 Uhr mit dem Vortrag "Aktuelle Schwachstellen in Windows XP/7" von Martin Dombrowski, der als Ethical Hacker für die entrada GmbH Windows-Systeme auf ihre Sicherheit untersucht.


Im Rahmen unseres Workshops zeigt Dombrowski zur Einführung in die Thematik aktuelle Sicherheitslücken der weit verbreiteten Clients Windows XP und 7. Die Teilnehmer können sich auf einen tiefen Einblick in die Windows-Sicherheitsarchitektur, begleitet von zahlreichen Live-Demos, freuen. Ist dem IT-Verantwortlichen erst einmal bewusst, welche starken wirtschaftlichen Interessen die Gegenseite verfolgt, sollten Dombrowskis abschließende Ausführungen zu sinnvollen Gegenmaßnahmen mehr als willkommen sein.

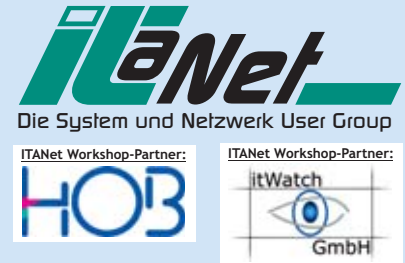
Eine dieser Gegenmaßnahmen ist zweifellos das regelmäßige Patchen der Windows-Clients. Und so setzt sich im zwei-

ten Vortrag des Tages Thomas Gronenwald, Berater bei adMERITia GmbH, mit dem Thema auseinander, wie Unternehmen ein erfolgreiches Patchmanagement für Windows betreiben können.

Zwei weitere Vorträge des Workshops am 16. November beschäftigen sich mit speziellen Problemen, mit denen sich Administratoren konfrontiert sehen. Zum einen erläutert Joachim Gietl von HOB, wie sich externe Zugriffe auf das Unternehmensnetzwerk über ein VPN sicher realisieren lassen.

Eine weitere Quelle möglicher Unsicherheiten sind die Applikationen der Windows-Clients, deren Daten häufig das Ziel von Angriffen darstellen. So beschäftigt sich Ramon Mörl von it-watch denn auch mit Wegen, den Datenabfluss aus dem Client und seinen Anwendungen zu verhindern.

Zudem zeigt Giebelhausen praktische Methoden zur Härtung und Absicherung, die die Workshopteilnehmer für die von Ihnen betreuten Systeme nutzen können. Wenn Sie also die Sicherheit Ihrer Clients verbessern wollen, freuen wir uns, Sie am 16. November in München zu begrüßen. 



Die Agenda des Workshops

10.00 Uhr: Begrüßung

10.15 Uhr: Aktuelle Schwachstellen in Windows XP/7
- Aktuelle Exploits in Windows
- Motivation und Ziele der Malwareentwickler
- Gegenmaßnahmen

Dozent: Martin Dombrowski, entrada Kommunikations GmbH

11.15 Uhr: Partnervortrag
Unterschiede herkömmlicher IPsec-VPNs zu SSL-VPNs, dargestellt an HOB RD VPN

Dozent: Joachim Gietl, Vertriebsleiter Software Central Europe, HOB

12.00 Uhr: Pause

13.00 Uhr: Patchmanagement für Windows
- Bedeutung des Patchmanagements
- Aufgeräumt mit Vorurteilen: Mythos Patchmanagement – Nichts geht mehr
- Warum es ohne einen geeigneten Sicherheits-Updateprozess schwierig wird
- Die Qual der Lösungs-Wahl

Dozent: Thomas Gronenwald, adMERITia GmbH

14.15 Uhr: Pause

14.30 Uhr: Partnervortrag:
Data Loss Prevention, Endpoint Security, Wirtschaftsspionage, Datenschutznovelle – Anforderungen und Best Practice / Lösungen

Dozent: Ramon Mörl, Geschäftsführer itWatch GmbH

15.30 Uhr: Härtung von Windows-Clients
- Gute Gründe für das Hardening
- Top 10 der ausgenutzten Schwachstellen und Funktionen
- Methoden zur Härtung eines Clientsystems

Dozent: Sascha Giebelhausen, adMERITia GmbH

17.00 Uhr: Ende der Veranstaltung

Ort: Expertech Training Center
Wredestr. 11, 80335 München

Teilnahmegebühren:

Für IT-Administrator Abonnenten kostenlos

Anmeldung bis zum 9. November unter
www.it-administrator.de/workshops/

Workshop "Sicherheit für Windows-Clients" am 16. November



IT Admin Tech Talk 2010, 27. und 28. September, Oberursel bei Frankfurt/M.

Erfolgreiche Premiere

von John Pardey

Erstmalig fand Ende September der IT Admin Tech Talk – die neue Veranstaltung für Netzwerk- und Systemadministratoren – als Kooperation des IT-Administrator und der IIR Technology statt. Rund 60 Administratoren mittelständischer und großer Unternehmen aller Branchen reisten nach Oberursel bei Frankfurt am Main, um sich über neueste technologische Trends, praxisbewährte How-Tos und sich wandelnde organisatorische Rahmenbedingungen ihres Berufsfelds zu informieren. Dabei gaben sich zahlreiche Autoren des IT-Administrator sowie weitere führende Industrieexperten ein Stelldichein und referierten über Virtualisierung, Servermanagement, Storage und vieles mehr. IT-Administrator war für Sie vor Ort.

Den Auftakt der zwei prall mit Vorträgen gefüllten Tage bildete die Keynote von Julien Ardisson, Strato AG. Ardisson skizzierte in seinem Beitrag "Admin 2020" Änderungen und Neuerungen im Berufsbild des Administrators. Dabei zeigte er in seiner Präsentation Parallelen zwischen der IT und der Automobilindustrie auf, um den interessierten Zuhörern darzustellen, in welche Richtung diese Änderungen erfolgen werden. Es sei eine zunehmende "Industrialisierung" des IT-Betriebs festzustellen, so Ardisson, deren Bedarf an Automatisierung von Abläufen und der damit verbundenen Fokussierung auf die Prozessebene bestimmend sei für die zukünftigen Aufgaben des IT-Verantwortlichen.

Mit der Fokussierung auf IT-Prozesse werde der Admin zukünftig eher zu einem "Manager", zu einem Gestalter im Unternehmen, während typische aktuelle Aufgaben des IT-Betriebs in den Hintergrund treten werden. Natürlich ist ein Blick auf die nächsten zehn Jahre in so einer schnelllebigen Branche wie der IT schwierig und die Änderungen im Berufsbild werden sich unterschiedlich gestalten, doch Ardissons positive Botschaft als Fazit: "IT-Jobs werden nicht weniger – sie ändern sich nur."



Unternehmensberater Lars Gerschau wirft einen Blick auf zukünftige Prozessor-Architekturen

Zukunft der IT

Als roter Faden zog sich eine Reihe von drei Vorträgen mit dem Zusatz "2020" im Titel durch den IT Admin Tech Talk. Nach der eben erwähnten Keynote stellte Lars Gerschau, Unternehmensberater, die "Hardware 2020" vor. Sein Streifzug durch zukünftige IT-Landschaften widmete sich Prozessoren und deren Architektur ebenso wie Schnittstellen und der strategischen Ausrichtung der wichtigs-

ten Anbieter im Prozessormarkt. Neben der kurz- und mittelfristigen Entwicklung der Chips wagte Gerschau die Prognose, dass bereits 2016 damit zu rechnen sei, dass 128 Bit-Prozessoren zum Standard werden.

Als dritten Beitrag dieser Reihe präsentierte am zweiten Veranstaltungstag Nicholas Dille, sepago GmbH, in seinem Vortrag "Software 2020" einen intensi-

ven Blick auf das Cloud Computing und dessen Ausprägungen als IaaS, SaaS oder PaaS. Letztendlich, so Dille, bieten alle diese Dienste interessante Ansatzpunkte zukünftiger IT-Infrastrukturen, doch das Herz der IT – die Unternehmensdaten – in die Cloud zu stellen, sei in Deutschland auf Grund der rechtlichen Rahmenbedingungen sehr genau zu überlegen. Eine sehr pragmatische Einschätzung zukünftiger Dienste aus der Cloud bot Eckard Klockhaus, Conciety AG, in seinem Vortrag zu “Infrastructure as a Service”. Seiner Meinung nach wird “der erste Server, den Ihr Unternehmen in die Cloud stellt, einer sein, der Dienste bereitstellt, die Sie bis dahin noch nicht hatten.”

Aktueller Betrieb

Neben diesen unterschiedlichen Blickwinkeln auf zukünftig Bedeutsames stand selbstverständlich der aktuelle IT-Betrieb und dessen Optimierung im Fokus der zwei Tage in Oberursel. Ein zentrales Thema dabei: die Virtualisierung, beleuchtet in einer ganzen Reihe von Fachvorträgen und einer Podiumsdiskussion. So gab etwa IT-Administrator-Autor Dennis Zimmer, icomasoft AG, wertvolle Hinweise zur Kapazitätsplanung für virtuelle Infrastrukturen unter VMware sowie zur Vermeidung und Behebung von Performanceengpässen. Christian Knermann, Frauenhofer-Institut UMSICHT, stellte dar, wie sich virtualisierte Desktops in die bestehende Terminal Server-Landschaft integrieren lassen und Nils Kaczinski, WIT-store GmbH, erklärte der gespannten Zuhörerschaft, worauf es bei der Virtualisierung von Windows-Domänencontrollern ankommt.

Bedeutend für den aktuellen IT-Betrieb ist aber auch die Sicherheit. Hier stellte unter anderem Thomas Gronenwald, adMERITia GmbH, aktuelle Anforderungen an das Patchmanagement dar. So sei das Patchen unter der ausschließlichen Verwendung von WSUS nur in der Lage, etwa 35 Prozent aktueller

Schwachstellen zu schließen. Denn die steigende Sicherheit bei den Betriebssystemen lenke die Angriffslust der “Schwarzen Hüte” zunehmend auf die Applikationen, insbesondere das PDF-Dateiformat. Für die restlichen 65 Prozent seien durchschnittlich – je nach Struktur der Applikationen im Unternehmen – 13 weitere Updatemechanismen notwendig. Gronenwald betonte ausdrücklich, dass das Patchmanagement unbedingt als Prozess im Unternehmen zu betrachten sei. Dies erfordere zwar den Einsatz von Budget und Zeit, sei aber bei guter Umsetzung in der Lage, die Netzwerke vor etwa 95 Prozent aller Schwachstellen zu schützen.

Neben den Themen Virtualisierung und Sicherheit bot der IT Admin Tech Talk zahlreiche weitere tiefgehende technische Sessions, die sich etwa mit MS Exchange, Storage, Windows Server 2008 R2, dem Active Directory und der PowerShell beschäftigten. Spannend auch die Erfahrungen, die Arved Schierding, Karl Storz GmbH, in Sachen Migration und Produktivbetrieb von Windows 7 mit den Zuhörern teilte.

Auf Wiedersehen im nächsten Jahr!

Alles in allem bescherte der IT Admin Tech Talk 2010 den anwesenden Administratoren einen großen Strauß an wertvollen Informationen für den aktuellen und zukünftigen Betrieb der IT. Oft hatten die Teilnehmer in Angesicht der beiden parallelen Vortragsreihen die Qual der Wahl. Doch gerade dadurch war jeder Teilnehmer in der Lage, sich aus dem umfassenden Vortragsangebot seine Rosinen zu picken.

Falls Sie den IT Admin Tech Talk 2010 verpasst haben sollten, bleibt der Trost, dass IIR Technology und IT-Administrator schon bald mit der Planung der Veranstaltung für 2011 beginnen werden und gewiss auch im kommenden Jahr wieder eine praxisnahe, herstellerunabhängige Konferenz mit Top-Experten auf die Beine stellen.

VMware ESX 4



- Vollständige Kommando-referenz mit Schritt-für-Schritt-Anleitungen
- ESX-Aufbau, Fehlersuche, Umgang mit Festplatten-dateien und Snapshots
- PowerShell, PowerCLI, vCLI und vMA

687 S., 3. Auflage 2010, 69,90 €
» www.galileocomputing.de/2427



OpenVPN



- Installation, Konfiguration, Administration
- Authentisierung und Verschlüsselung
- Tipps, Praxisbeispiele, Troubleshooting

294 S., 2. Auflage 2010, 39,90 €
» www.galileocomputing.de/2466



Shell-Programmierung



- Einführung, Praxis, Referenz
- Bourne-, Korn- und Bourne-Again-Shell
- Inkl. grep, sed und awk, GUIs mit Tcl/Tk

808 S., 3. Auflage 2010, mit CD, 39,90 €
» www.galileocomputing.de/2440



Microsoft Project Server 2010



- Konfiguration, Anpassung, Erweiterung
- Grundlagen des Projektmanagements
- Einsatzszenarien für eine Project Server-Implementierung

869 S., 2010, 49,90 €
» www.galileocomputing.de/2306



www.GalileoComputing.de



booksonline
Ihre persönliche IT-Bibliothek

VMworld 2010, 30. August bis 2. September, San Francisco

Neue Wege, klare Ziele

von Dennis Zimmer

VMware meint es ernst – 190.000 Kunden, 50.000 Partner und 25.000 Certified Professionals sprechen eine klare Sprache. Dies wurde auch auf der VMworld 2010 in San Francisco deutlich, als der Virtualisierungsmarktführer zum Angriff auf das Betriebssystem-Establishment blies. So sieht VMware-Boss Maritz die Zukunft klar bei virtuellen Online-Applikationen. IT-Administrator war für Sie auf der US-Veranstaltung vor Ort.

Bereits einen Tag vor dem offiziellen Start begann die VMworld 2010 mit dem Technology Exchange Day, der sich an Technologiepartner von VMware richtete. Die zugehörigen Hands-on-Labs waren durchaus beeindruckend. So wurden insgesamt mehr als 100.000 VMs ausgerollt. Zudem standen Virtualisierungssessions für Anfänger zur Verfügung. Offizieller Start der VMworld war dann am Dienstag, den 31. August.

Zum ersten Mal wurden die beiden VMworld-Veranstaltungen in den USA und Europa mit einer zeitlichen Distanz von gerade einem Monat durchgeführt. Daher war auch die Beteiligung aus Europa wesentlich geringer als in den letzten Jahren – etwa ein Fünftel des letzten Jahres. Trotzdem gelang es VMware, in den USA mehr Teilnehmer anzulocken als im Rekordjahr 2009, mit einem Anstieg von 12.500 auf 17.000. Die weiteren Zahlen waren nicht weniger beeindruckend, da VMware mittlerweile 190.000 Kunden, 50.000 Partner und 25.000 VMware Certified Professionals (VCPs) aufweisen kann.

Angriff auf das Establishment

Paul Maritz erläuterte als CEO im Anschluss die Vision von VMware und wie sich die IT in den nächsten Jahren verändern könnte. Eine seiner wichtigsten Aussagen war allerdings, dass sich die IT verändern müsse, egal ob mit oder ohne VMwares Zutun. Die Unternehmer verlangen demzufolge nach neuen Lösungen,



Für VMware-CEO Paul Maritz sind SaaS-Applikationen die Zukunft

wie die benötigten Dienste und Anwendungen bereitgestellt, betrieben und verrechnet werden können, ohne stetig von der Infrastruktur abhängig zu sein. Mehrere Schlagwörter nannte Maritz dabei, darunter die vielleicht zukünftig dominierende Infrastruktur der Hybrid Cloud, einer Mischform von internen und externen Ressourcen, die über VPN oder Programmierschnittstellen verbunden sind. Dass ihm die herkömmlichen Betriebssysteme und deren Rolle ein Dorn im Auge sind, daraus machte der VMware-Geschäftsführer keinen Hehl. Das Betriebssystem sei zur Orchestrierung der Hardware und als Framework für die Applikationen zuständig. Die Orchestrierung übernehme die Vir-

tualisierungsschicht, das Framework würde in der virtuellen Appliance geladen (.NET, Java) und damit der Boden für die Applikation geschaffen. Damit griff er indirekt eine der Haupteinnahmequellen seines früheren Arbeitgebers Microsoft an.

Ziel des VMware CEOs war aber weniger die Hetze gegen die „alten“ Größen der IT, sondern viel eher die Wegbereitung für den Auftritt von CTO Steve Herrod. Der Technikchef stellte eine neue Produktreihe von VMware vor, um damit die zukünftige Strategie zu verdeutlichen. Herrod ging zunächst zwar auf die neuen Funktionen von vSphere 4.1 ein, die vMotion beschleunigen, I/O und Netzwerkverkehr deutlich

besser kontrollieren und mit den Storage-Systemen über die VAAI-Schnittstelle (vStorage APIs for Array Integration) kommunizieren. VAAI ist eine wesentliche Neuerung, die neben Storage vMotion-Vorgängen auch das Klonen der VMs nicht mehr über den ESX-Host, sondern das Storage Array selbst steuert, was deutlich ESX-Hostleistung einspart.

Um den Bogen zu den Anwendern zu schlagen, wurden anschließend die Anforderungen eines Geschäftsführers (respektive Anwenders) und die des IT-Leiters theoretisch dargestellt und wie diese sich verändern könnten. Im Endeffekt handelte es sich dabei um das gleiche Thema, das seit Jahren mit SaaS oder ASP gepredigt wird: Der Anwender möchte schlichtweg mit seinen Applikationen arbeiten, immer und überall, ohne sich Gedanken über die Infrastruktur, Performance oder Datenhaltung machen zu müssen. Hier zeigt sich natürlich der deutliche Weg in die Cloud und, dass VMware mithelfen möchte, die IT in die Richtung des Applikationsdenkens anstatt des Infrastrukturdenkens zu bewegen. Damit war die Zeit für die Ankündigung des VMware vCloud Director gekommen, der während der umfangreichen Beta-Phase den Namen "Project Redwood" trug. Dieser ist in der Lage, als zentrale Verwaltungsplattform die Infrastruktur für Kunden (virtuelle Rechenzentren) aus der verfügbaren Cloud Hardware-Masse zurechtzuschneiden und Applikationen samt virtuellem System zu verteilen. Automa-

tische SLA-Regeln (Resource Pools) und automatische Sicherheitskomponenten (VMware vShield Endpoint, VMware vShield App, VMware vShield Edge) zur Absicherung des virtuellen Rechenzentrums sowie VPN-Verbindung zwischen unterschiedlichen Clouds sollen den Endkunden dabei eine möglichst umfangreiche und einfache Lösung an die Hand geben.

Doch nicht nur die Eigenentwicklungen zeigten die Stoßrichtung von VMware. Auch neue Akquisitionen wie Integrien (Proaktive Systemanalyse), GemStone (Caching), Springsource (Application Framework, Überwachung et cetera), TriCipher (Sicherheit) verdeutlichten, dass VMware künftig auch Applikationen anbieten möchte, anstatt wie bisher nur die Infrastruktur. Genauer gesagt soll neben der traditionellen Anwendung auch die nächste Generation von Online-Applikationen adressiert werden als reine Software as a Service-Anwendungen.

Überbuchte Sessions, zahlreiche Hands-on Labs

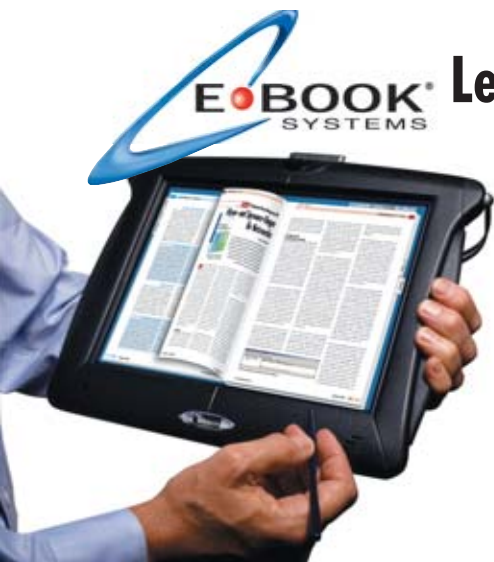
Nach den Keynotes begannen eine Vielzahl an Sessions und Supersessions, die sich natürlich auch zum großen Teil mit Automatisierung und Cloud Computing befassten. Leider waren viele sehr interessante Sessions komplett überbucht und es gab nicht selten keine Chance mehr, an ihnen teilzunehmen. Daran änderten auch die Wiederholungen der Sessions nichts. Dort zeigten sich wie schon in der Ver-

gangenheit die Organisationsschwierigkeiten bei zu vielen Session-Besuchern.

Die Solutions Exchange – sozusagen der Marktplatz, auf dem hunderte VMware Partner ihre Produkte vorstellten – war wie immer gut gefüllt. Wer etwas Zeit und Interesse mitbrachte, konnte auch viele sehr interessante Lösungen kleinerer Hersteller finden. Auch hier war der Schwerpunkt Cloud-Computing, außerdem fielen viele VDI-Anbieter auf. Richtig überwältigend waren die vor ein paar Jahren gestarteten Hands-on Labs, die mittlerweile fester Bestandteil der VMworld sind. Auf etwa 480 Lab-Plätzen konnten die Teilnehmer zahlreiche Anwendungen und Produkte austesten. Während der VMworld 2010 USA standen über 15.000 Labs mit rund 145.000 VMs zur Verfügung, die vollautomatisch auf einer Hybrid Cloud-Infrastruktur (VMware SFO, Verizon, Terremark) liefen. Gegenüber 2009 mit etwa 4.500 Labs hatte sich die Anzahl mehr als verdreifacht.

Fazit

Es sind immer neue Rekorde, die die VMworld aufstellt, getreu dem Motto: schneller, höher, weiter. VMware nimmt den Sprung in Richtung Cloud und neue Anwendungen sehr ernst und unterstreicht dies durch seine finanziellen Investments. Wie immer war auch 2010 der Besuch der Messe die Reise wert – nicht zuletzt dank der sozialen Kontakte auf den zahlreichen Partys und dem "CTO Office" für vExperts. (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



**Im Test: Dot Hill AssuredSAN 3.000-Serie**

Flinker Datensammler

von Jürgen Heyer



Mit der AssuredSAN 3.000-Serie hat Dot Hill seine Produktpalette um schnelle, flexibel einsetzbare Speichereinheiten für SAS, Fibre Channel und iSCSI erweitert. Preislich im Einstiegs- und Midrange-Bereich positioniert, finden sich bei diesen Modellen sehr interessante Funktionen wie Volume Copy und Remote Replication, die bisher eher der Highend-Klasse vorbehalten waren. Im Testlabor konnte sich IT-Administrator im Detail von den Features überzeugen.

Als Storage-Hersteller dürfte Dot Hill hierzulande weniger bekannt sein, obwohl mit Sicherheit so manches Unternehmen dessen Speichersysteme unter anderen Brandings in größerer Menge im Einsatz hat. So wirbt Dot Hill mit über 300.000 weltweit im Einsatz befindlichen Systemen und produziert unter anderem als OEM-Partner für Hewlett Packard, wo sich die AssuredSAN 3.000-Systeme in der MSA2000-Serie als die neuen G2-Modelle wiederfinden. Die augenscheinlichsten Vorteile sind der kompakte Aufbau und die modulare Bauweise. Mit bis zu 24 2,5-Zoll-Festplatten bestückt, wird die zwei Höheneinheiten messende Front im 19-Zoll-Rack optimal genutzt. An ein Basisgerät lassen sich bis zu sieben Erweiterungseinheiten anschließen, wobei sich maximal 144 Festplatten adressieren lassen. Bevor Sie sich wundern, dass acht mal 24 doch mehr als 144 ergibt, sei erwähnt, dass es auch ein Chassis mit bis zu zwölf 3,5-Zoll-Festplatten gibt und sich beide Typen mischen lassen.

Die SAS-Backplane besitzt eine Bandbreite von 6 GBit/s und es können wahlweise SAS-, SATA- und SSD-Laufwerke, auch gemischt und mit unterschiedlicher Kapazität, eingesteckt werden. Durch die

Verfügbarkeit verschiedener Controller ist die 3.000er-Serie erfreulich flexibel einsetzbar. Dabei kann ein Chassis mit einem oder für einen redundanten Betrieb mit zwei Controllern bestückt werden. Als Controller-Schnittstellen sind 6 GBit-SAS, 8 GBit-Fibre Channel sowie als Hybrid- beziehungsweise Multiprotokoll-Variante 8 GBit-FC mit 1 GBit-iSCSI verfügbar. Im dritten Quartal dieses Jahres soll noch ein Controller für 10 GBit-iSCSI/FCoE auf den Markt kommen. Das Produkt dürfte bei Erscheinen dieses Artikels bereits verfügbar sein.

Für unseren Test stand uns das Modell AssuredSAN 3920 mit Multiprotokoll-Controllern zur Verfügung, auf dem wir sämtliche Funktionen inklusive der lizenz- und kostenpflichtigen Features AssuredSnap, AssuredCopy und AssuredRemote Snapshot Replication (Beschreibungen siehe weiter unten) nutzen konnten. Die Performance der Speichersysteme liegt laut Datenblatt beim Anschluss mit 6 GBit-SAS oder 8 GBit-FC bei 264.000 IOPS beziehungsweise 1.750 MBit/s beim Lesen und 1.350 MBit/s beim Schreiben.

Einfache Inbetriebnahme

Unser Testgerät war komplett redundant ausgestattet, also mit zwei Netzteilen so-

wie zwei Controllern, und mit 24 146-GByte-SAS-Festplatten bestückt. Alle Komponenten sind bei einem Defekt im laufenden Betrieb austauschbar, Rändelschrauben sorgen dafür, dass sich kein Einschub aus Versehen lösen kann.

Die beiden Multiprotokoll-Controller verfügen über je zwei 8 GBit-Fibre-Channel-Anschlüsse und zweimal dediziertes LAN für GBit-iSCSI. Ein weiterer 100-MBit-LAN-Anschluss dient als Management-Port. Der Nutzer sollte darauf achten, dass die Management-Ports beider Controller mit dem Netzwerk verbunden sind, damit das Plattensystem nicht ständig eine Degraded-Warnung anzeigt. Für den Betrieb würde aber auch ein Anschluss reichen, da die Controller über die Backplane des Chassis verbunden sind und alle Einstellungen untereinander abgleichen. Neben dem Management-Port besitzt jeder Controller noch einen seriellen und einen USB-Port zum Zugriff auf die CLI-Schnittstelle (Command Line Interface), ein zweiter USB-Port ist für eine zukünftige Verwendung reserviert.

Zugriff per Browser oder CLI

Im Normalfall erfolgt der Zugriff per LAN mittels Browser auf die integrierte Web-GUI namens RAIDar, so dass für

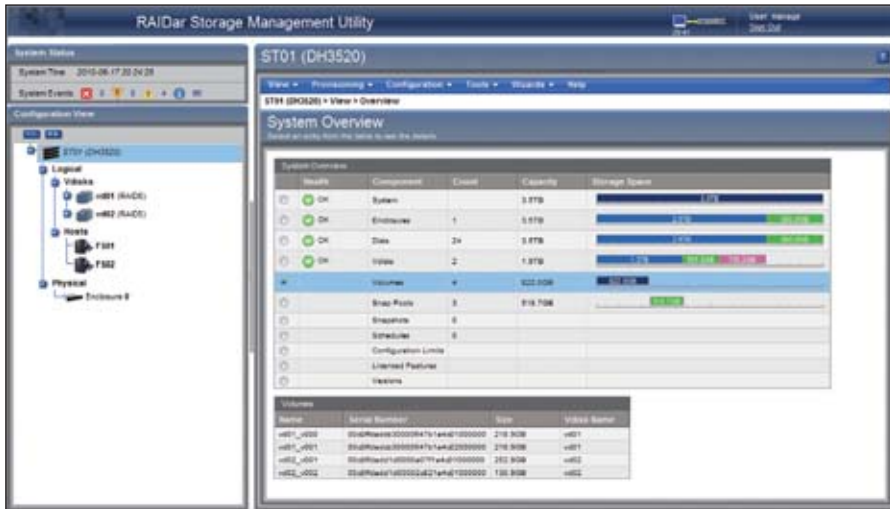


Bild 1: In der Systemübersicht sind alle Funktionen der GUI über umfangreiche, teilweise verschachtelte Pull-Down-Menüs erreichbar

die Bedienung keine weitere Software benötigt wird. Die CLI lässt sich auf diesem Wege auch erreichen, um beispielsweise bestimmte Aktionen per Skripting zu automatisieren. Ein SAS-Anschluss pro Controller dient zum Anschluss der schon erwähnten Erweiterungseinheiten, wobei diese wie auf einer Perlenschnur hintereinander angereiht werden.

Diverse LEDs an jeder Festplatte, am Chassis sowie auf den Controllern und den Netzteilen zeigen den technischen Zustand auf einen Blick an. Die intuitiv zu bedienende und recht übersichtliche GUI von RAIDar stellt Meldungen abgestuft in vier Kategorien (Kritisch, Fehler, Warnung, Information) mit unterschiedlichen Farben dar. In einem Fenster links oben ist der Systemstatus mit einer Auflistung der System-Meldungen abzulesen, ab dem Status "Warnung" ist in der darunter befindlichen Konfigurationssicht die betroffene Komponente durch ein entsprechendes Symbol markiert. Vorteilhaft ist, dass sich in die GUI einer Storage-Einheit weitere, entfernte Systeme einbinden lassen. Hierzu sind nur einmal IP-Adresse und Anmeldedaten anzugeben. Ursprünglich war diese Funktion für das Ergänzen eines Replizierungspartners gedacht, aber dies funktioniert prinzipiell auch mit jeder anderen Einheit.

Schnelle Erstkonfiguration

Im Test haben wir uns für die Erstkonfiguration mit einem Notebook über eine der ab Werk eingestellten IP-Adressen mit einem Controller verbunden und die LAN-Daten aller Ports passend für unser Netz geändert. Dies funktionierte über einen Konfigurationsassistenten sehr gut, der über mehrere Fenster hinweg alle Basisparameter (Neues Passwort, Management-Ports, aktivierte Dienste für das Management, Systeminformationen, SNMP-Konfiguration, SMTP-Benachrichtigung sowie FC- und iSCSI-Port-Einstellungen) abfragte. Ungewöhnlich ist, dass beim allerersten Aufruf des Assistenten alle IP-Adressen zwingend mit führenden Nullen auf drei Stellen aufzufüllen sind, also beispielsweise 010.000.000.005. Bei einem späteren Aufruf oder bei direkter Eingabe ohne Assistent sind dann die führenden Nullen nicht mehr erforderlich.

Für das Anlegen der Laufwerke sowie das Herstellen der Host-Mappings ist ebenfalls ein Assistent implementiert, diese Konfiguration klappte im Test dank einer guten Visualisierung aber auch ohne diesen ähnlich einfach. So bildet die GUI die Front mit den eingesteckten Platten ab und wir mussten nur die gewünschten anklicken, um ein Array zu bauen. Genauso stellt das Werkzeug für das Default-

Host-Mapping die Rückseite des Chassis mit den Controller-Ports dar.

Redundante Controller durch Multipathing

Für die Array-Konfiguration unterstützt die 3.000er-Serie die RAID-Level 0, 1, 3, 5, 6, 10, 50 und NRAID. In einem ersten Schritt sind über mehrere Platten hinweg eine oder auch mehrere Vdisks (virtual disk) mit dem gewünschten RAID-Level anzulegen. Maximal 16 Vdisks pro Controller sind möglich, da jede Vdisk stets einem Controller zugeordnet ist (Ownership). Sind zwei Controller vorhanden, sorgt das System bei der Vdisk-Erstellung automatisch für eine gleichmäßige Verteilung. Die Controller arbeiten Active-Active, so dass jede Vdisk jederzeit über beide Controller erreicht werden kann. Für eine optimale Performance sollte der Administrator aber dafür sorgen, dass der primäre Zugriff auf eine Vdisk über den Controller erfolgt, der auch die Ownership besitzt. Über entsprechende Einstellungen des bevorzugten Pfades (Preferred Path) in den verschiedenen Betriebssystemen lässt sich dies passend konfigurieren.

Beim Ausfall eines Controllers übernimmt der verbleibende temporär die Ownership und stellt dann alle Vdisks nach außen bereit. Das setzt natürlich auf Serverseite eine mehrpfadige Anbindung mit entsprechender Multipath-Konfiguration (beispielsweise unter Windows mit MPIO) voraus. Seit Windows 2008 ist MPIO im Betriebssystem integriert, für Windows 2003 stellt Dot Hill einen entsprechenden Treiber bereit.

Automatische Zuweisung von Ersatzlaufwerken

Neben den Vdisks kann der Administrator bis zu vier Hot-Spare-Platten definieren, jede entweder fest einem Array zugewiesen oder als Global Spare, die überall einspringt, sobald eine produktive Platte ausfällt. Darüber hinaus gibt es noch eine Einstellung namens Dynamic Spare, die bewirkt, dass eine neu eingesteckte Platte automatisch als Hot Spare zum Einsatz kommt. Andernfalls muss der Administrator dies manuell zuweisen.

Nachdem wir auf dem Testsystem zwei Vdisks mit RAID 5 und 6 definiert hatten, konnten wir darauf die benötigten Volumes anlegen, die letzten Endes auf Serverseite als SCSI-LUNs sichtbar wurden. Pro Vdisk kann der Nutzer automatisch ein oder mehrere Volumes erstellen. Benötigt er auf einem Speichersystem viele Volumes, empfiehlt Dot Hill die Anlage weniger Vdisks, möglichst gleichmäßig auf beide Controller verteilt, und auf jeder Vdisk die Anlage von mehreren Volumes.

Da das System auf alle Platten Metadaten bezüglich der Konfiguration schreibt, ist es problemlos möglich, die Platten innerhalb der Einheit beliebig zu vertauschen oder einen ganzen zu einer Vdisk gehörenden Plattensatz von einem System auf ein anderes zu portieren. Das bedeutet aber, dass auf bereits genutzten Platten vor einer neuen Verwendung eventuell vorhandene Metadaten gelöscht werden müssen. Dies ist innerhalb von RAIDar möglich.

Flexibles Volume-Mapping

Für manchen Administrator, der in der Vergangenheit bereits andere Plattensysteme betreut hat, mag das von Dot Hill ver-

wendete Mapping-Konzept neu sein. Anfangs vielleicht etwas gewöhnungsbedürftig, erweist es sich letztendlich als recht flexibel, wenn es darum geht, nicht nur einzelne Server einpfädig zu betreiben, sondern auch Cluster und Farmen für virtuelle Umgebungen zu realisieren, in denen mehrpfadige Anbindungen und wechselseitige sowie gleichzeitige Zugriffe auf gemeinsame Volumes zum Standard gehören. So beherrschen die Systeme ein so genanntes Default Mapping in Form eines Port-Zonings sowie ein Explicit Mapping als Bezeichnung für eine WWN-bezogene Zuweisung (WWN-Zoning).

Legt ein Administrator ein Volume an, so bietet das System gleich ein Default-Mapping an. Hierzu muss er die LUN-Nummer angeben, außerdem die Zugriffsart (no-access, read-only, read-write) und die Controller-Ports, auf denen das Volume sichtbar sein soll. Alle Hosts, die mit einem dieser Ports verbunden sind, können die LUN dann entsprechend der eingestellten Zugriffsart nutzen. Um nun ein einzelnes Volume gezielt bestimmten Hosts zuzuweisen, muss der Administrator ein Explicit-Mapping definieren und das Default-Mapping zu den anderen Hosts entfernen.

Zu erwähnen ist, dass innerhalb von RAIDar natürlich auch die Hosts anzulegen sind. Hierzu sind die Host-IDs anzugeben, also entweder bei Fibre Channel die WWN oder bei iSCSI die IQN, und weiterhin ein sinnvoller Host-Name für die Anzeige in der GUI. Im Falle von iSCSI lässt sich die Verbindung über CHAP mit Passwort sichern. In der Praxis ist es möglich, mit den beschriebenen Mapping-Arten mit wenig Aufwand ein passendes Zoning für die benötigten Zugriffe zu definieren und besondere Zugriffsvarianten zu implementieren: Greifen auf ein Plattensystem viele eigenständige Server zu, so nutzt der Administrator am besten primär das explizite Mapping. Werden aber alle Platten von einem großen Cluster oder einer VMware-Farm genutzt, so reicht es eventuell aus, alle Server per Default-Mapping zu berechtigen.

Unterschiedliche Zugriffsarten sind beispielsweise dann sinnvoll, wenn in der Medizintechnik nur der Server eines MRT die Bilddaten auf ein Volume schreiben können soll (Zugriff read-write), die Ärzte aber parallel über einen anderen Server bereits fertige Bilder ansehen wollen (Zugriff read-only). Wären beide Server schreibberechtigt, würden sie sich ständig gegenseitig die Metadaten überschreiben, so dass am Schluss ein korruptes Laufwerk übrig bliebe.

Zusatzfunktionen gegen Aufpreis

Die 3.000er-Modelle gibt es hinsichtlich des Funktionsumfangs als C-, S- und R-Serie. Die C-Serie beinhaltet die Speichereinheit ohne weitere Lizenz, die S-Serie bringt die Features AssuredSnap und AssuredCopy mit, die R-Serie enthält zusätzlich noch eine Lizenz für AssuredRemote Snapshot Replication. Dot Hill bezeichnet diese Ergänzungen als Data Management Software Suite (DMS). Statt die Geräte entsprechend im Bundle zu kaufen, können die Lizenzen auch später erworben werden. Um dieses schmackhaft zu machen, liegt der C-Serie die DMS als zeitlich begrenzte Try&Buy-Version bei.

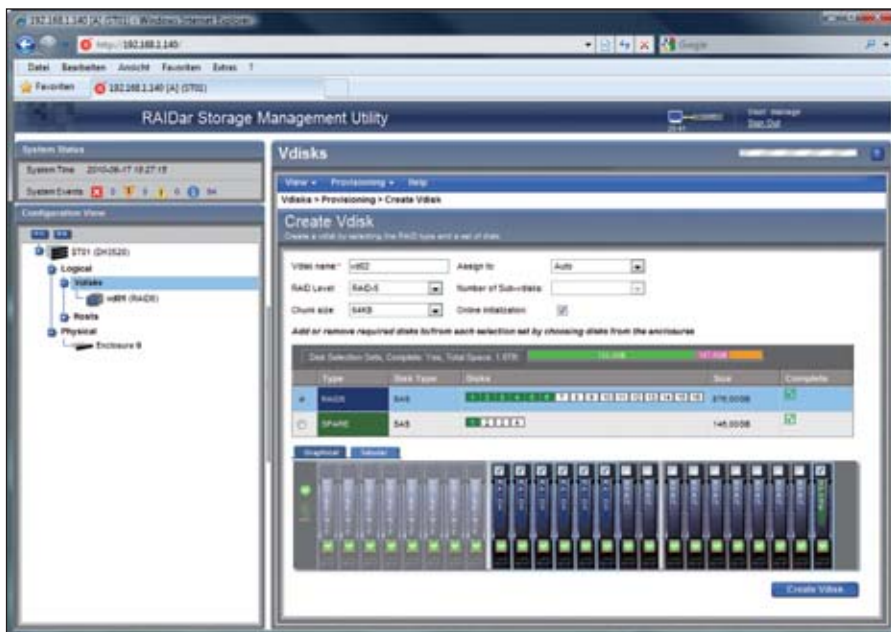


Bild 2: Bereits angelegte Arrays werden halbtransparent dargestellt, so dass der bereits konfigurierte Bereich leicht erkennbar ist

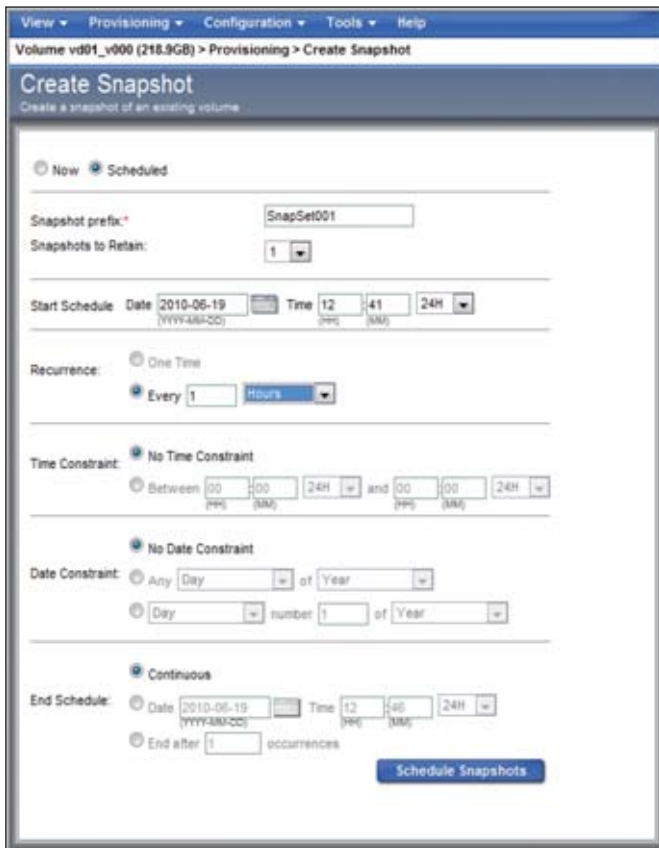


Bild 3: Snapshots lassen sich über einen komfortablen Scheduler individuell an die Erfordernisse anpassen

Snapshots gewähren mehr Freiraum

AssureSnap ermöglicht, wie der Name schon vermuten lässt, Snapshots. Sobald von einem Volume ein Snapshot erstellt wird, legt das System für dieses Volume einen so genannten Snap-Pool an. AssuredSnap

nutzt das copy-on-write-Verfahren, was bedeutet, dass bei der Änderung eines Blocks die alten Daten in den Snap-Pool kopiert werden und die neuen auf das eigentliche Volume. Wird später ein Snapshot gelöscht, müssen nur die entsprechenden Blöcke im Snap-Pool freigegeben werden. Snapshots lassen sich per Zeitplaner in festen Abständen automatisch erzeugen, der Administrator gibt dabei an, wie viele Versionen er halten will, so dass sich quasi ein umlaufender Pool ergibt.

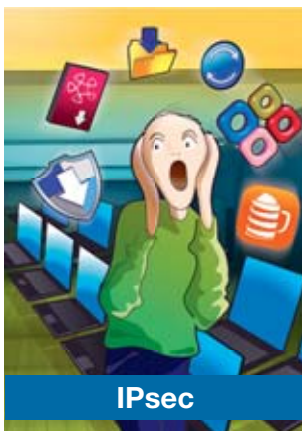
Ein Snapshot lässt sich auf verschiedene Arten verwenden. Wie üblich kann ein Snapshot dazu dienen, das Quellvolume wieder auf den Stand des Snapshots zurückzusetzen. Weiterhin kann ein Administrator einen Snapshot im Schreib-/Lesemodus als Laufwerk mappen, um bei-

spielsweise darauf eine neue Software zu installieren. War die Installation nicht erfolgreich, so kann er den Snapshot wieder auf den ursprünglichen Stand bringen. Er hat aber zudem die Möglichkeit, ein Quellvolume auf den Stand eines Snapshots inklusive der darauf gemachten Änderungen zu bringen.

Volume-Replizierung über Standorte hinweg

Im Gegensatz zum Snapshot erzeugt die AssuredCopy-Funktion eine komplette Kopie eines Volumes, um es anschließend als neues Standard-Volume zu nutzen. Dies schafft im Gegensatz zum Snapshot eine völlige Unabhängigkeit von der Quelle, so dass sich jegliche Performanceeinbußen vermeiden lassen. Es ist wahlweise möglich, ein Volume zu kopieren oder aus einem existierenden Snapshot eine eigenständige Kopie zu erzeugen.

Das AssuredRemote Replication Feature letztendlich ist eine Funktion, die in erster Linie als Disaster-Recovery-Maßnahme gedacht ist. Es repliziert den Inhalt eines Volumes asynchron auf Blockebene auf ein identisches Volume, das sich auf der gleichen Storage-Einheit, aber auch auf einer zweiten befinden darf. Kommt die zweite Einheit an einem anderen Firmenstandort zum Einsatz, so lassen sich Replizierungen über



Verzweifeln Sie nicht, steigen Sie auf HOB RD VPN um

Secure-Remote-Access ohne Installation

Die browserbasierte Remote-Access Lösung HOB RD VPN ist weder mit herkömmlichen SSL VPNs noch mit IPsec VPNs zu vergleichen. Der Administrator kann dank HOB RD VPN auf zeitraubende Installationen von Treibern oder Software auf den Client-Systemen verzichten. Der User kann orts- und plattformunabhängig auf einen virtuellen Desktop zugreifen – die Daten bleiben im Rechenzentrum.

HOB PPP Tunnel (IPsec Rest in Peace Juni 2010)

Möchte der User mit seinem MS Windows Vista-, Windows 7-, Apple Mac OS X- oder Linux-System einen vollständigen Netzwerkzugriff, kann er die treiberlose Technologie des HOB PPP Tunnels einsetzen. Zwei-Faktor-Authentifizierung, SSL-Verschlüsselung bis AES 256 Bit, Client Integrity Check – kein Sicherheitsverlust gegenüber IPsec – bei Performance und Einfachheit ist der PPP Tunnel meilenweit überlegen.

Die Security-Suite von HOB RD VPN ist vom BSI (Bundesamt für Sicherheit in der Informationstechnik) nach Common Criteria zertifiziert (HOBLink Secure BSI-DSZ-CC-0260-2004). Dadurch beweist HOB, dass der Zugriff wirklich sicher ist!



eine größere Entfernung realisieren. Der Datentransfer erfolgt wahlweise via Fibre Channel oder iSCSI. Eine anstehende Replizierung erzeugt zuerst einen Snapshot, der dann mit den Daten auf dem Ziel verglichen wird, um nur die unterschiedlichen Blöcke übertragen zu müssen. Eine Replizierung kann manuell oder mittels Zeitplaner automatisiert erfolgen.

Hinsichtlich der Nutzung von Snapshots ist uns aufgefallen, dass Dot Hill nur für Windows einen VDS-/VSS-Treiber bereitstellt, um mittels dieser Mechanismen dafür zu sorgen, dass die Snapshot-Daten konsistent sind. Für andere Betriebssysteme hat der Hersteller dazu nichts im Angebot, vielmehr müssen entsprechende Abläufe mit Zugriff über die CLI geskriptet werden. Der Support von Dot Hill unterstützt bei Bedarf bei einer Implementierung.

Umweltschonende Green IT sinnvoll umgesetzt

Dot Hill hat in seine 3.000er-Serie einige Stromsparmaßnahmen integriert. So haben die beiden Netzteile lastunabhängig einen Wirkungsgrad von mindestens 80 Prozent (80-PLUS-Zertifizierung). Weiterhin kann der Administrator das System so konfigurieren, dass es inaktive Platten und Global Spares herunterfährt (Drive Spin Down = DSD). Hierzu legt er die Zeitdauer in Minuten fest, nach der inaktive Platten heruntergefahren werden, und definiert außerdem einen Zeitraum wie beispielsweise die reguläre Arbeitszeit, in der das nicht passieren soll. Zu beachten ist, dass heruntergefahrne Platten nicht auf Defekte durchsucht und SMART-Meldungen nicht abgefragt werden, und dass es etwas länger dauert, wenn ein Plattenzugriff erfolgt, da die Disk erst wieder starten muss.


Als sehr gute Lösung bewerten wir den patentierten, batterielosen, aber dennoch gepufferten Cache der Controller. Statt eines Akkus, der in der Regel nur etwa

zwei Jahre hält, verwendet Dot Hill einen großen Kondensator mit rund zehn Jahren Lebensdauer, dessen Ladung ausreicht, um bei einem Stromausfall oder einer Abschaltung den Cacheinhalt in einen Flashspeicher zu schreiben. Neben der besseren Umweltverträglichkeit durch den Verzicht auf den Akku ergibt sich zudem der Vorteil, dass der Flashinhalt unbegrenzt hält, während die Akkus den Cacheinhalt in der Regel nur 72 Stunden puffern. Wer mehrere hundert Server betreibt, weiß, wie lästig es ist, wenn nach einiger Zeit die Pufferbatterien am laufenden Band den Geist aufgeben. Das kann hier nicht passieren. Nach einem Abschalten der Einheit konnten wir genau beobachten, dass eine LED auf den Controllern noch mehrere Sekunden lang blinkt, bis sie ausgeht.

Fazit

Die neue AssuredSAN 3.000-Serie von Dot Hill erweist sich in jeder Hinsicht als sehr breitbandig einsetzbare und individuell skalierbare Speicherlösung, die technisch auf dem neuesten Stand ist. Die Skalierbarkeit ist zum einen durch die Ausbaufähigkeit auf bis zu 144 Festplatten gegeben, mit verschiedenen Controllern für SAS, Fibre Channel und GBit-iSCSI deckt der Hersteller zudem alle praktikablen Anschlussmöglichkeiten ab. Eine 6 GBit-SAS-Backplane sowie 6 GBit-SAS-Controller und 8 GBit-FC sorgen für eine bestmögliche Performance. Allenfalls bei iSCSI muss der Administrator noch ein wenig auf höchste Leistung warten. Ein Controller für 10Gbit-iSCSI/FCoE sollte aber schon beim Erscheinen dieser Ausgabe verfügbar sein.

Funktional skalierbar ist die Serie durch zwei Lizenzen für Snapshots/Volume-Copy sowie Remote Replication, so dass sich die Speichereinheiten für einen wirkungsvollen Disaster-Schutz konfigurieren lassen. Vorteilhaft ist weiterhin die Active-Active-Arbeitsweise, so dass auf ein Volume jederzeit über beide Controller zugegriffen werden kann. Für ei-

ne optimale Performance sollte aber in erster Linie der Controller genutzt werden, der der Eigentümer der unter den Volumes liegenden virtuellen Disks ist. Erfreulich intuitiv zu bedienen ist die Web-GUI für die Administration, auch wenn der Umgang letztendlich etwas Einarbeitung erfordert, vor allem, um Mappings zu den angeschlossenen Hosts korrekt umzusetzen. (In) 

Produkt

Modular konfigurierbare Plattenspeichereinheiten für SAN-Umgebungen.

Hersteller

Dot Hill
www.dothill.com

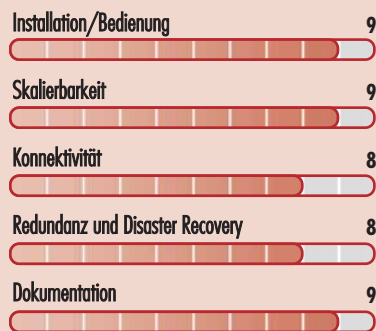
Preis

Die Modelle der AssuredSAN 3.000-Serie sind ab etwa 8.000 Euro erhältlich.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für Speicheranforderungen ab etwa 3 TByte in einer SAN-Infrastruktur sowie bei Bedarf für Snapshots und asynchrone Replizierung zwischen Betriebsstätten.

bedingt bei geringeren Kapazitätsanforderungen, da sich die Investition dann nicht rechnen dürfte, außer es werden die speziellen Features wie die Kopierfunktion oder die Replizierung benötigt.

nicht, wenn sich der Bedarf hinsichtlich Kapazität und Verfügbarkeit mit lokalen Festplatten in einem Server abdecken lässt.

Dot Hill AssuredSAN 3.000-Serie



Im Test: sayFUSE Smart Server

Platte wechsle dich

von Jürgen Heyer

Die Idee klingt sehr verlockend: Ein professioneller Server mit mehreren Wechselplatten als Sicherungsmedien dient als schnelle Backup-Lösung. Eine dafür geeignete, modular aufgebaute Hardware sollen die sayFUSE-Komponenten von sayTEC bieten. Wir haben dem Gerät in unserem Test genau auf die Finger geschaut und ein leistungsfähiges Backupkonzept vorgefunden. Als kleine Herausforderung erweist sich allenfalls die Automatisierung und Kombination mit einer geeigneten Sicherungssoftware.

Dem allgemeinen Trend der Zeit, die Datensicherung nicht auf Bänder, sondern auf Festplatten zu realisieren (Backup-to-Disk), folgt sayFUSE (Fast Universal Storage Engine) von sayTEC. Die Basis ist eine geeignete Hardware mit SATA-II- oder SAS-Festplatten in Wechselrahmen, vergleichbar mit Hot-Plug-Platten in professionellen Servern. Hinzu kommt allerdings eine spezielle Laufwerkssteuerung, um die einzelnen Wechselplatten gezielt ein- und ausschalten zu können. Das spart Energie und schont die Platten, da sie so nicht im laufenden Betrieb herausgezogen werden müssen. Letztendlich kann der Administrator die Wechselplatten ähnlich wie Bänder behandeln, vor allem hinsichtlich des Aufbewahrungskonzepts. So ist es kein Problem, zumindest einen Teil der Platten zum Schutz vor einem Brand oder einer sonstigen Katastrophe an einem anderen Ort beziehungsweise im Tresor aufzubewahren. Auch können weit mehr Datenträger in einem Sicherungskonzept verwendet werden, als Platteneinschübe am Sicherungsserver vorhanden sind. Die Platten ersetzen also letztendlich die Bänder und statt einer Band-Bibliothek hat der Administrator quasi eine Platten-Bibliothek vor sich.

Mehrwert durch modularen Aufbau

Mit dem sayFUSE-Konzept hat sayTEC ein innovatives, modulares System ent-

wickelt, das in der einfachsten Variante "sayFUSE Backup" die reine Datensicherungslösung beinhaltet. Als Betriebssystem kommt dann standardmäßig Windows XP Tablet zum Einsatz. Weiterhin gibt es den so genannten sayFUSE Smart Server, den wir in diesem Test eingehender betrachtet haben. Er verfügt über eine integrierte Server-Funktionalität in unterschiedlichen Ausbaustufen. Die dritte Variante ist ein mit VMware bestücktes Modell, um neben dem Backup zusätzlich mehrere virtuelle Maschinen betreiben zu können. Hier ist eine 16 GByte Solid State Disk für das Betriebssystem eingebaut, der Hauptspeicher beginnt bei 16 GByte und ist bis 128 GByte aufrüstbar. Ein zweiter Prozessor (Intel Xeon) lässt sich auch einbauen.

Die Hardware

Für den Test hat uns sayTEC einen "Smart Server SA" komplett vorkonfiguriert zur Verfügung gestellt. Hierbei handelt es sich um ein 19-Zoll-Gehäuse mit 4 HE Bauhöhe. Das Mainboard von Tyan ist mit einem Intel Core-2-Quad-Prozessor (2,66 GHz) und 8 GByte Hauptspeicher bestückt, eine Speicheraufrüstung ist aufgrund von zwei freien Steckplätzen noch möglich. Die Front wird von 12 Slots für Wechselrahmen mit SATA-II- oder SAS-Festplatten (3,5 Zoll) dominiert, die es in Kapazitäten bis 2 TByte gibt.

Die Wechselrahmen bestehen aus speziellen Aluminium-Profilen mit einer Kunststoffblende. Die Profile laufen sehr leichtgängig und machen den Eindruck, dass sie auch für viele Wechselzyklen durchaus geeignet sind. Die Arretierung erfolgt über einen Bügel in der Frontblende, wobei der Bügel durch einen kleinen Drehknopf zusätzlich gegen ein Öffnen gesichert werden kann. Etwas unglücklich erschien uns, dass der Bügel beim Drehen des Knopfes leicht unbeabsichtigt entriegelt werden kann.

Innenleben und Bedienung

Unser Testsystem war mit Windows 2008 Server in der Standard-Edition bestückt, für den Einsatz in kleineren Unternehmen bietet sich aber in erster Linie der Small Business Server an. Die Intension ist, dass das System zur Datensicherung dient, aber damit natürlich nicht ausgelastet ist, und in Verbindung mit einem geeigneten Betriebssystem auch als Applikationsserver genutzt werden kann. Kleinere Firmen können somit beide Anforderungen in einem Gerät vereinen.

Da die von vorne erreichbaren Wechselplatten ausschließlich für das Backup gedacht sind, ist das Betriebssystem der Einheit selbst auf zusätzlichen Disks untergebracht, die ebenfalls mit Hot-Plug-Rahmen (2,5 Zoll) von hinten in das Gerät eingeschoben werden. Hier gibt es



insgesamt vier Steckplätze, die je nach Wunsch mit SAS- oder SATA-Platten genutzt werden können.

Die Smart Server-Modelle verfügen standardmäßig über zwei redundante Hot-Plug-Netzteile. Die LAN-Anbindung erfolgt über zwei GBit-Anschlüsse, optionale Netzwerkkarten mit viermal GBit, 10 GBit Kupfer oder 10 GBit LWL sind auch erhältlich. Für einen autarken Betrieb ist der Smart Server mit einem Touchscreen (Auflösung 800 x 600 Punkte) ausgestattet, der hochgeklappt werden kann, um die dahinter befindlichen Festplatten zu erreichen. Wer die etwas umständliche Bedienung per Touchscreen nicht mag, kann auch Tastatur und Maus anschließen. Nur der VGA-Anschluss ist nicht nach hinten herausgeführt, sondern intern mit dem Touchscreen verbunden. Alternativ besteht natürlich die Möglichkeit, sich via Netz per RDP zu verbinden, was wir im Test überwiegend so gemacht haben.

Bei einem Blick ins Innere sahen wir trotz der vielen Festplattenanschlüsse eine sehr ordentliche Verkabelung, wobei sich sayTEC einiger Kabelkanäle bedient. Auffällig ist die Technik zur Mediensteuerung: Jeder Wechselplattenslot ist über ein Flachbandkabel mit einer zentralen Platine verbunden, die die Steuerelektronik enthält. Diese wiederum wird über USB angesprochen. Die Wechselplatten sind zu je drei Stück in einer Aufnahmeeinheit zusammengefasst, die über einen Lüfter gekühlt wird.

Optionen für Ausstattung und Support

Die Geräte sind bei sayTEC vorkonfiguriert erhältlich, sie können aber auch ohne Festplatten und ohne Betriebssystem bezogen werden. Dies hängt letztendlich davon ab, wie viel Arbeit das Systemhaus oder auch der Endkunde noch investieren will. Ebenso bietet sayTEC unterschiedliche Servicelevel bis hin zu einem Ersatzgerät innerhalb von 24 Stunden an. Ein Austausch gestaltet sich als einfach, da letztendlich nur die System- und Wech-

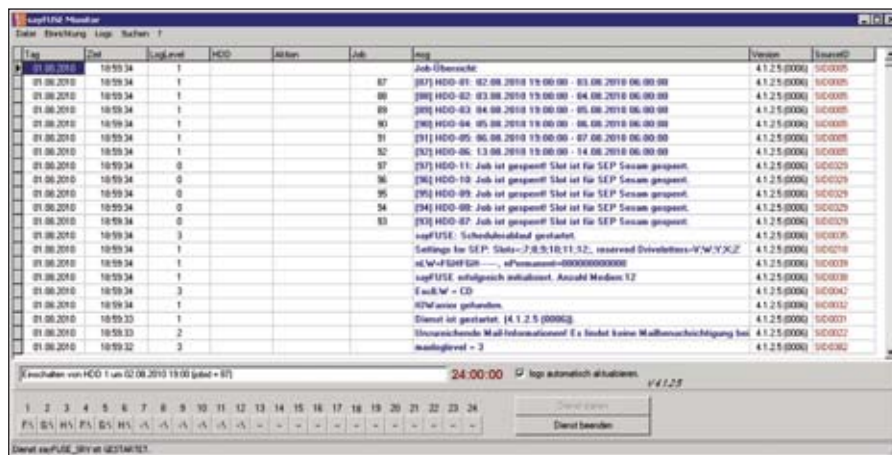


Bild 1: Der sayFUSE-Monitor zeigt alle Systemmeldungen an, die nächste geplante Aktion und den Status der Wechselmedien

selplatten umgesteckt werden müssen. Neben den Zentraleinheiten gibt es noch ein so genanntes Capacity Extension Module (CEM) für weitere zwölf Wechselplatten. Über einen entsprechend vorbereiteten Anschluss kann ein solches Modul angeschlossen werden, um die Anzahl der Steckplätze zu verdoppeln.

Komplexe Mediensteuerung

Die standardmäßig mit sayFUSE gelieferte Software sayCONTROL zur Mediensteuerung erweist sich als recht mächtig, aber auch komplex. Sie besteht aus mehreren Modulen, die miteinander arbeiten und unterschiedliche Funktionen erfüllen. Das Herzstück ist der sayFUSE Server, ein Dienst, der eine vorhandene Jobliste automatisch abarbeitet und gegebenenfalls permanent einzuschaltende Medien nach der Inbetriebnahme ebenfalls automatisch startet. Zu beachten ist, dass dieser Dienst nicht laufen darf, wenn entweder über das Modul sayFUSE_SET Einstellungen geändert oder über sayFUSE_CTR die Mediensteuerung manuell bedient werden soll. Andernfalls könnte es zu Schaltkonflikten kommen. Ist der Serverdienst aktiv, wird der Aufruf eines der anderen beiden Module mit einem entsprechenden Hinweis verweigert. Jederzeit starten lässt sich nur der Monitor sayFUSE_MON, der den Status und die Rückmeldungen des Serverdienstes ausgibt. Der Monitor zeigt die bisherigen Meldungen an, den nächsten Schaltbefehl

inklusive der verbleibenden Zeit und auch den Status der sayFUSE-Ports, also der Wechselplatten. Weiterhin gibt es eine Ansicht der bisherigen Schaltzeiten sowie eine Übersicht der bereits getätigten Jobs.

Recht übersichtlich ist das Tool sayFUSE_CTR zur manuellen Steuerung, was für Test- und Restore-Zwecke gedacht ist. Hier gibt es einmal eine Ansteuerung über die Plattenlogik, was bedeutet, dass die Kriterien durch die Einstellungen zur Laufwerksvergabe berücksichtigt werden. Das ist anfangs verwirrend, aber durchaus sinnvoll. Sind beispielsweise in einem Pool drei Festplatten zusammengefasst, die (wechselweise) als Laufwerk "F:" sichtbar sind, so lässt sich die zweite Platte nicht einschalten, wenn auf der ersten noch ausreichend Platz ist, wobei sich der Füllgrad in der Mediensteuerung vorgeben lässt. Damit ist sichergestellt, dass innerhalb eines Medienpools immer die richtige Platte gestartet wird. Die zweite Möglichkeit, die direkte Ansteuerung, schaltet eine Platte auf jeden Fall ein, was aber bedeuten kann, dass sie unter einem anderen Laufwerksbuchstaben sichtbar wird, wenn eine andere Platte aus dem Pool bereits läuft. Die direkte Ansteuerung wird beispielsweise bei einem manuellen Restore benötigt, um gezielt auf ein Laufwerk zugreifen zu können.

Das umfangreichste Tool ist sayFUSE_SET, das den Zugriff auf die Einstellungen er-



laubt und den integrierten Zeitplaner enthält. So muss der Administrator hier die benötigten Medienpools festlegen, also einen oder mehrere Wechselplattenslots gruppieren, indem er ihnen einen gemeinsamen Laufwerksbuchstaben zuweist. Die Medienpools haben der Einfachheit halber stets den Namen des zugeordneten Laufwerksbuchstabens. Wird nun auf einen Pool zugegriffen, so schaltet die Mediensteuerung zuerst das Medium mit der niedrigsten Slot-Nummer ein, wodurch es als Laufwerk mit dem zugewiesenen Buchstaben sichtbar wird. Ist dieses voll beziehungsweise bis zu einem bestimmten, festgelegten Prozentsatz gefüllt, so schaltet das Tool auf das nächste Medium um. Wird sayFUSE in Verbindung mit der Sicherungssoftware Sesam von SEP betrieben, muss der Administrator die hiermit zu nutzenden Slots, wahlweise einen Teil oder alle, innerhalb von sayFUSE_SET reservieren. Sie sind dann von der Medienpoolkonfiguration und der Mediensteuerung ausgenommen, da Sesam das Ein- und Ausschalten selbst übernimmt.

Funktional sehr umfangreich ist der Scheduler gestaltet, der es nicht nur ermöglicht, regelmäßig wiederkehrende Sicherungen zu steuern. Vielmehr ist er auch dazu geeignet, die bei Bandlaufwerken beliebte GFS-Sicherung (Großvater, Vater, Sohn) mit Wochentags-, Wochen-, Monats- und auch Jahresbändern abzubilden. Um auf Wunsch Sicherungen an Sonn- und Feiertagen auszuschließen, werden diese Tage in einer Datenbank verwaltet. Der Scheduler berechnet nun für jeden Slot den nächsten Schaltzeitpunkt und trägt diesen in die Jobliste ein. Der Scheduler startet auf Wunsch auch Batchdateien, wobei sich eine Abhängigkeit zur Medienoperation angeben lässt (nach dem Einschalten, vor dem Ausschalten et cetera). Sofern der Administrator SMTP-Informationen hinterlegt hat, wird er vor fälligen Bandwechseln benachrichtigt.

Backup mit verteilten Aufgaben

Hinsichtlich des Schedulers ist zu beachten, dass dieser zwar das Ein- und Ausschalten der Medien steuert sowie Batch-

dateien startet, aber letztendlich keine eigenständige Backupsoftware darstellt. Vielmehr muss der Administrator für die Datensicherung ein Produkt wählen, welches auch auf Platten schreiben kann (Backup-to-Disk). Das ist mittlerweile kein Problem mehr und weitverbreitete Produkte wie CA Arcserve oder Symantec Backup Exec unterstützen dies. Umständlich ist dabei, dass der Administrator in zwei Oberflächen administrieren und den zeitlichen Ablauf selbst koordinieren muss. In der Praxis bedeutet dies, dass der Scheduler in sayCONTROL zuerst die gewünschte Wechselplatte einschalten muss und anschließend der eigentliche Sicherungsjob starten darf. Einfacher wird der Ablauf insofern, dass beispielsweise die komplizierteren Bandwechsel bei einer GFS-Sicherung nur innerhalb von sayCONTROL einzustellen sind, die Backupsoftware sichert einfach immer auf den gleichen Laufwerksbuchstaben. Bei einem Restore muss der Administrator dann natürlich genau wissen, auf welcher Wechselplatte sich welcher Tag befindet, die Backupsoftware kann ihm das nicht abnehmen.

Neben dem Einschalten der Medien muss der Administrator auch die Abschaltung nach der Sicherung festlegen. Hier kann er natürlich die Platte deutlich länger laufen lassen, als das Backup normalerweise dauert. Darüber hinaus prüft auch sayCONTROL vor einer Abschaltung auf eine Plattenaktivität hin und wartet, bis keine Daten mehr über-

tragen werden. sayCONTROL kann also das Sicherungsende selbständig erkennen. Da sich die Wechselplatten unabhängig voneinander ein- und ausschalten lassen, ist es möglich, bis zu zwölf Sicherungsaufträge parallel laufen zu lassen, in Verbindung mit dem oben genannten CEM sogar bis zu 24 Aufträge. Denkbar ist auch eine Sicherung mit unterschiedlicher Backupsoftware, sofern sich die Installationen auf dem Server untereinander vertragen. Indem der sayFUSE Smart Server optional mit einer 10 GBit-Netzwerkkarte ausgestattet werden kann, dürfte auch die Netzbandbreite ausreichen, wobei sich durch eine entsprechende Verschaltung der Sicherungsdatenverkehr von den Benutzerzugriffen trennen ließe. Laut Hersteller wird die Lösung häufig auch dazu genutzt, Systeme aus verschiedenen Netzwerksegmenten zu sichern, indem in den Smart Server mehrere Netzwerkkarten eingesteckt werden.

Damit eine defekte Festplatte nicht gleich zum Ausfall einer Sicherung führt, kann der Administrator einem Job ein Ersatzmedium zuordnen. Kommt es dann beim Einschalten der Platte zu einer Störung, so weicht sayControl auf das Ersatzmedium aus. Tritt ein Fehler während einer Sicherung auf, hilft das natürlich nicht. Weiterhin gibt es die Möglichkeit, von der für einen Job verwendeten Wechselplatte vor deren Abschaltung zusätzlich eine 1:1-Kopie auf ein anderes Laufwerk oder in ein Verzeichnis zu erstellen.

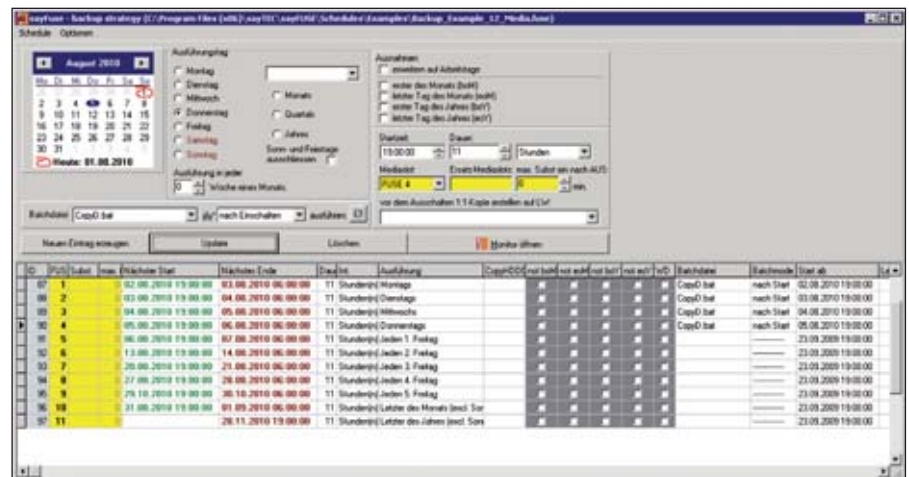


Bild 2: Der Zeitplaner ermöglicht das Anlegen umfangreicher Sicherungspläne, ist aber recht komplex in der Bedienung



Angesichts der nicht ganz einfachen Einrichtung empfehlen wir, am besten die Dienstleistung des Systemhauses in Anspruch zu nehmen, über das sayFUSE erworben wurde. Anhand der Einrichtung der ersten Jobs lernt ein Administrator schnell, wie bei späteren Änderungen vorzugehen ist. Ein Systemhaus dürfte zudem übliche, häufig verwendete Sicherungsjobs bereithalten, die sich problemlos im- und exportieren lassen. Das beschleunigt die Einrichtung enorm.

Laut sayTEC ist es geplant, nach und nach für die verschiedenen verbreiteten Backup-Produkte Schnittstellen zu schreiben, so dass die Bedienung aus einer Konsole heraus erfolgen kann und die Sicherungssoftware auch die komplette Mediensteuerung übernimmt. Genau diese direkte Unterstützung für sayFUSE existiert aktuell nur für die Sicherungssoftware Sesam von SEP. Wird Sesam genutzt, sind die entsprechenden Slots zu reservieren, damit sie vom Scheduler nicht mehr gesteuert werden. Aufgrund der direkten Mediensteuerung bietet Sesam einige funktionale Features wie das gleichzeitige Schreiben mehrerer Streams auf eine Platte sowie die Möglichkeit, mehrere Wechselplatten logisch zu einem großen Medium zusammenzufassen. Nichtsdestotrotz ist es deswegen nicht unbedingt notwendig, auf Sesam umzusteigen, die Kombination mit anderen Backup-Produkten ist ebenso möglich, wenn auch umständlicher und mit mehr Konfigurationsarbeit verbunden.

Leider verriet die uns vorliegende Dokumentation von sayFUSE abgesehen von einer einseitigen globalen Beschreibung noch sehr wenig über die Kombinationsmöglichkeiten. Insofern mussten wir die oben beschriebene Vorgehensweise beim Hersteller erfragen. Da die getestete Version 4 von sayCONTROL zum Testzeitpunkt noch sehr neu war, schien die Dokumentation noch nicht abschließend durchredigiert und wies noch kleinere Fehler auf, die aber nach und nach ausgebessert werden sollten. Wir haben den Hersteller darauf hingewiesen und auch empfohlen, die prinzipielle Vorgehensweise bei der

Kombination mit einem beliebigen Backup-Produkt genauer zu beschreiben.

Fazit

Das sayFUSE-Konzept hinterlässt mit der Idee, für die Datensicherung Wechselplatten quasi wie Sicherungsbänder zu behandeln und für diesen Zweck leistungsfähige Hardware bereitzustellen, einen ordentlichen Eindruck, auch wenn uns kleinere Schönheitsfehler aufgefallen sind. Überzeugen konnten der professionelle Aufbau der aufwändigen Hardware und die leichtgängigen, robusten Wechselplattenrahmen, die auch viele Wechselzyklen übertragen sollten. Gefallen hat uns weiterhin die intelligente Wechselsteuerung, die dafür sorgt, dass die Platten nur dann laufen müssen, wenn sie tatsächlich benötigt werden. Interessant ist zudem der Ansatz, das Sicherungssystem in Verbindung mit einem geeigneten Betriebssystem gleichzeitig als Applikationsserver zu verwenden, was diese Variante für kleinere Firmen prädestiniert.

Einen Optimierungsbedarf sehen wir hinsichtlich einer besseren Zusammenarbeit mit beliebiger Backupsoftware. So ist es prinzipiell schon möglich, sayFUSE mit diversen verbreiteten Sicherungsprogrammen zu kombinieren. Voraussetzung ist nur, dass das Sicherungsprogramm eine Gerätekonfiguration für Backupmedien zur Verfügung stellt beziehungsweise ein Backup-to-Disk unterstützt. Nachteilig ist aber, dass in diesem Fall die Mediensteuerung getrennt über sayControl erfolgen muss, der Administrator also zwei Konsolen bedienen und die Aktionen zeitlich abstimmen muss. Das erfordert auf jeden Fall einen Mehraufwand. Laut sayTEC sollen in Zukunft nach und nach Schnittstellen für verbreitete Backup-Produkte erscheinen.

Allein zu SEP Sesam gibt es diese Schnittstelle zur Mediensteuerung bereits jetzt, so dass hier die komplette Bedienung aus Sesam heraus erfolgt. Allerdings möchte verständlicherweise nicht jeder, der sayFUSE einsetzt, auch unbedingt auf diese Sicherungssoftware umsteigen. Die Do-

kumentation könnte umfangreicher sein, wobei allerdings zu berücksichtigen ist, dass die Lösung überwiegend über Systemhäuser vertrieben wird, die entsprechendes Know-how mitbringen. Abschließend empfehlen wir jedem Interessenten, im Vorfeld ein Konzept zu erstellen, dieses auf eine reibungslose Zusammenarbeit von Hard- und Software zu prüfen und auch einen eventuellen Mehraufwand abzuschätzen. (jp)



Produkt
Integrierte Backup-Lösung auf Wechselplatten mit gleichzeitiger Nutzung als Applikationsserver.

Hersteller
sayTEC
www.saytec.eu

Preis
Der sayFUSE Smart Server SA ist inklusive Software zur Mediensteuerung, aber ohne RAID- und Backup-Medien ab 6.490 Euro erhältlich.

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

So urteilt IT-Administrator (max. 10 Punkte)

Installation und Bedienung	8
<div style="border: 1px solid red; height: 10px; width: 80%; margin: 2px 0;"></div>	
Verarbeitung der Hardware	9
<div style="border: 1px solid red; height: 10px; width: 85%; margin: 2px 0;"></div>	
Unterstützung von Backupsoftware	7
<div style="border: 1px solid red; height: 10px; width: 70%; margin: 2px 0;"></div>	
Mediensteuerung	8
<div style="border: 1px solid red; height: 10px; width: 80%; margin: 2px 0;"></div>	
Dokumentation	6
<div style="border: 1px solid red; height: 10px; width: 60%; margin: 2px 0;"></div>	

Dieses Produkt eignet sich

- optimal** als Ergänzung für kleinere und mittlere Unternehmen, die bei der Sicherung bereits auf die Software SEP Sesam setzen.
- bedingt** dort, wo bereits eine andere Sicherungssoftware eingesetzt wird. Hier ist mehr Aufwand für die Konfiguration einzuplanen.
- nicht** für Firmen, bei denen sich sayFUSE nicht mit der vorhandenen Sicherungssoftware kombinieren lässt, diese aber beibehalten werden soll.

sayTEC sayFUSE Smart Server

Teilt ihre Gedanken
mit der ganzen Welt

genau wie ihre
Passwörter.



Mitarbeiter sind auch nur Menschen.

Da kann es passieren, dass Ihre Firmendaten in sozialen Netzwerken landen. Oder verloren gehen. Oder manipuliert werden. Schützen Sie sich davor!

- Kontrolle sämtlicher PC-Schnittstellen, inkl. Webmail, FTP, Facebook & Co.
- Schutz vor Datenbeschädigung und -verlust durch Unachtsamkeit oder Vorsatz
- Individuelle Justierbarkeit
- Für kleine, große und größte Netzwerke
- Über 4 Mio. Installationen
- Referenzen in hochsensiblen Branchen
- Neu! Jetzt mit vollständiger Content- und Kontext-Prüfung

Informieren Sie sich jetzt!

www.devicelock.de oder wählen Sie die Nummer sicher: +49.2102.89211-0

[www.devicelock.de]

DeviceLock®
Proactive Endpoint Security



Applikationszentrale für Terminalserver

von Christian Knermann

Microsoft-Terminalserver erlauben es Administratoren, ohne zusätzliche Software eine Remotedesktop-Umgebung aufzusetzen. Doch fehlt in derartigen Umgebungen so manches hilfreiches Admin-Feature. Hier setzt XenApp von Citrix an und bietet zahlreiche Zusatzfunktionen. Die derzeit aktuelle Version 6 unterstützt dabei erstmals und ausschließlich das 64 Bit-Betriebssystem Server 2008 R2. IT-Administrator hat die neuen Funktionen wie etwa Workergruppen und HDX getestet.

Die Citrix-Software XenApp fasst Terminalserver zu einer Server-Farm zusammen, in der die Systeme gemeinsam verwaltet werden. Die Konfiguration liegt in einem zentralen Datenspeicher. XenApp 6 möchte dazu den SQL Server Express auf dem ersten Server einer Farm installieren, spricht aber alternativ auch mit einem separaten SQL Server. Das Citrix Webinterface (WI) bezieht Informationen zur Konfiguration der Farm, zum Beispiel welcher Benutzer welche Applikationen starten darf, im XML-Format von den Terminalservern und veröffentlicht diese auf zwei Wegen (siehe Bild 1).

Eine XenApp-Website ermöglicht die interaktive Anmeldung über einen Browser. In diesem Fall kann die Web-Variante des Citrix Online Plug-Ins als Client zum Einsatz kommen. Die XenApp Servicesite liefert dagegen die Konfiguration für das Online Plug-In im XML-Format aus. Hierzu ist die vollständige Installation des Clients erforderlich. Das Plug-In verankert sich auf dem Client im Systemtray und integriert die Icons der freigegebenen Applikationen in Startmenü und Desktop. Für beide Varianten gilt, dass beim eigentlichen Start einer veröffentlichten Applikation eine direkte Verbindung zwischen Client und einem der Ter-

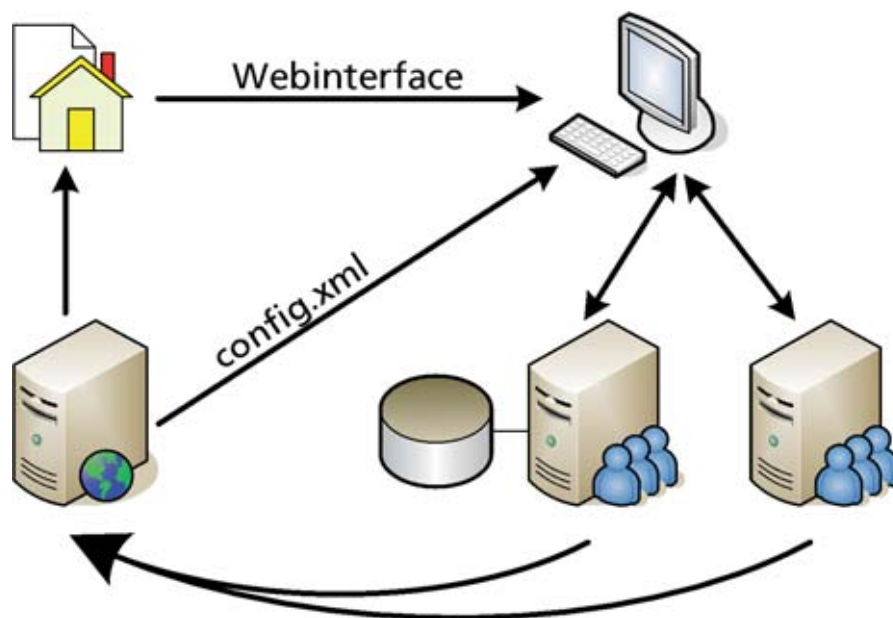


Bild 1: XenApp integriert mehrere Terminalserver zu einer Farm mit gemeinsamem Datenspeicher

minalserver über das Protokoll Independent Computing Architecture (ICA) etabliert wird.

Vier Editionen

Das Produkt ist in vier verschiedenen Editionen verfügbar mit Clients für diverse Windows-Versionen, Linux-Derivate, Mac OS X wie auch iOS-Geräte und weitere Smartphones. Alle Varianten können einzelne Anwendungen veröf-

fentlichen und nutzen die unter dem Kürzel HDX (High Definition User Experience) zusammengefassten Erweiterungen des ICA-Protokolls. Diese ermöglichen insbesondere für multimediale Inhalte eine signifikant verbesserte Wiedergabe auf kompatiblen Clients (siehe Tabelle "Features der verschiedenen Editionen"). Bei den XenApp Fundamentals handelt es sich um ein Einsteigerpaket für kleinere Umgebungen mit



Bild 2: Die Installation erfolgt ähnlich zum Windows Server 2008 rollenbasiert

maximal 75 Benutzern. Als einzige Variante werden die Fundamentals pro Named User lizenziert, während die übrigen Editionen pro Concurrent User, also nur nach Anzahl gleichzeitig aktiver Verbindungen, zu lizenzieren sind. Die Mindestmenge für eine initiale Beschaffung ist jeweils ein Fünf-User-Paket. Bereits die Advanced Edition unterstützt beliebig viele Anwender. Mit der Enterprise Edition kommen weitere Funktionen wie das Abfangen von Lastspitzen der CPU hinzu. Die Platinum Edition integriert zusätzliche Benutzerlizenzen für weitere Citrix Produkte wie das Access Gateway oder den Repeater zur Optimierung von WAN-Verbindungen.

Virtuelle Testumgebung

Für unseren Test installierten wir die Enterprise Edition in einer Active Directory-Domäne mit vier virtuellen Maschinen unter Windows Server 2008 R2. Von diesen sollte eine als Lizenz- und Webinterface-Server (WI-Server) fungieren, die übrigen Systeme waren als Terminalserver vorgesehen. Neben zwei Windows Server 2008 R2 Domain Controllern konnten wir auf einen bereits vorhandenen SQL Server 2005-Cluster zurückgreifen. Die XenApp 6-Installationsressourcen luden wir im Download-Bereich des MyCitrix-Portals als circa

4,5 GByte großes ISO-Image herunter und stellten dieses anschließend unseren VMs zur Verfügung.

Anschließend begannen wir mit der Installation von WI- und Lizenzserver. Per Autorun-Funktion begrüßte uns ein Dialog, wie er Administratoren der Vorgänger-Version vertraut ist. Sobald wir aber die Aktion "XenApp-Server installieren" aufrufen, wurde deutlich, dass wir es offensichtlich mit einer neuen Version zu tun hatten. Die Setup-Routine installierte zunächst automatisch das fehlende .NET Framework 3.5 SP1 nach und startete den Server Role Manager. Anschließend erfolgte die Installation ähnlich zu Windows Server 2008 rollenbasiert über die Option "Serverrollen hinzufügen". Es standen die unterschiedlichen Editionen des Produkts zur Auswahl. Nach dem obligatorischen Abnicken der Lizenzbestimmungen wurden uns die eigentliche Terminalserver-Rolle "XenApp" sowie weitere Komponenten angeboten.

Wir entschieden uns zunächst nur für den "Lizenzserver" und das "Webinterface". Im weiteren Verlauf zeigte sich nun eine wesentliche Verbesserung gegenüber früheren XenApp-Versionen. War es in der Vergangenheit oftmals nötig, den Installationsvorgang zu unterbrechen, um fehlende Voraussetzungen manuell zu erfüllen, übernimmt dies nun das XenApp-Setup. Nötige Windows-Komponenten wie Visual J# 2.0 und der IIS wurden automatisch ergänzt.

Es folgte eine Zusammenfassung der anstehenden Aktionen, die wir mit einem Klick auf die Schaltfläche "Installieren" bestätigten. Zurück im Server Role Manager wartete anschließend die Konfiguration der soeben installierten Komponenten auf uns. Zur Einrichtung des Webinterfaces startete die aus früheren Versionen bekannte Citrix Webinterface-Verwaltung. An dieser Stelle bestand nun ein Henne-Ei-Problem: Da zu diesem Zeitpunkt noch kein XenApp-Server verfügbar war, um mittels XML-Dienst ei-

ne Liste veröffentlichter Anwendungen zu liefern, ließen wir das Webinterface zunächst unkonfiguriert.

Damit blieb noch das Setup des Lizenzservers. Dieser trägt die gleiche Versionsnummer 11.6.1 wie unter XenApp 5, aber die höhere Build-Nummer 10007 und präsentiert sich mit komplett neuer Oberfläche. Die Konfiguration beschränkt sich auf die Ports für die Lizenzdienste und Management-Oberfläche. Neu ist das zusätzlich erforderliche Passwort. Beim zugehörigen Account "admin" handelt es sich um einen internen Benutzer des Lizenzservers. Dieses Konto diente uns anschließend zur Anmeldung an der web-basierten License Administration Console, die per HTTP auf Port 8082 erreichbar ist.

Der Administrations-Bereich gliedert sich in fünf Bereiche. Unter "System" finden sich allgemeine Informationen wie Versionsnummer, Hostname oder IP-Adresse des Servers. Innerhalb von "Benutzer" können weitere Accounts ergänzt werden. Diese Konten existieren nur im Kontext des Lizenzservers, eine Verbindung mit lokalen oder Domänen-Benutzern ist offenbar nicht vorgesehen. Grundsätzlich werden die Rollen "Benutzer" und "Administrator" unterschieden. Nur Letztere dürfen die Konfiguration ändern. Der Bereich "Warnungen" definiert Ereignisse und Schwellenwerte zur Anzeige von Meldungen im Dashboard, also auf der Startseite der Lizenz-Konsole. So kann der Server darauf hinweisen, dass ein bestimmter Prozentsatz eines Lizenzpakets ausgeschöpft ist oder dass das Ablaufende von Lizenzen bevorsteht. Eine Möglichkeit, Warnungen per E-Mail oder SNMP-Trap zu versenden, findet sich nicht. Citrix bietet jedoch die Möglichkeit, den Lizenz-Server mit der hauseigenen Monitoring-Lösung EdgeSight 5.3 zu überwachen.

Neben der Konfiguration der Ports bietet der Punkt "Server" die Möglichkeit, den Zugriff auf die Konsole mittels HTTPS zu aktivieren und passend dazu auch ein eigenes Server-Zertifikat zu installieren.



Hinter dem Punkt "Vendor Daemon" verbirgt sich zu guter Letzt die eigentliche Lizenzverwaltung. Dort importierten wir eine Eval-Lizenz für XenApp 6. Von deren Verfügbarkeit konnten wir uns anschließend im Dashboard überzeugen.

Terminalserver einfach aufgesetzt

Nachdem die Vorbereitungen abgeschlossen waren, konnten wir an die Installation der eigentlichen XenApp-Rolle auf dem ersten Terminalserver gehen. Es handelte sich um eine frische Installation des Windows Server 2008 R2, die noch nicht als Remotedesktopdienste-Sitzungshost konfiguriert war. Im Server Role Manager wählten wir die Rolle "XenApp" und beließen es im nächsten Dialogschritt bei der Standardauswahl. Das "XenApp-Management" wurde somit auch installiert. Die optionalen Komponenten installierten wir dagegen zunächst nicht. So ist die XML-Dienst-IIS-Integration nur dann von Interesse, wenn auf dem Terminalserver zusätzlich auch der Webserver IIS läuft. In diesem Fall kann wahlweise der Citrix XML-Dienst auf einen alternativen TCP-Port konfiguriert oder aber besagte Komponente hinzugefügt werden. Die IIS-Integration ergänzt den IIS um einen ISA-PI-Filter, so dass die Citrix XML-Informationen gemeinsam mit den Webseiten des IIS auf einem Port veröffentlicht werden können. Sofern der IIS zu einem späteren Zeitpunkt installiert wird, lässt sich die Integration auch nachträglich noch einrichten. Dann ist aber unter Umständen manuelles Eingreifen erforderlich [1].

Die Setup-Routine löste sämtliche Abhängigkeiten auf, auch die fehlenden Remotedesktop-Dienste. Sind diese eingerichtet, ist zunächst ein Neustart erforderlich. Anschließend konnten wir die Installation über den Server Role Manager fortsetzen. Die Setup-Routine installierte die fehlenden Microsoft-Komponenten sowie die XenApp-Rolle. Waren in früheren Versionen die Installation und Konfiguration in einem Arbeitsgang vorzunehmen, endete das Setup zunächst. Die Konfiguration ließ sich anschließend

als separater Prozess über den Server Role Manager aufrufen. Diese Änderung passt zur gestiegenen Bedeutung von Virtualisierung und Provisioning. So ist es auf diese Weise nicht mehr zwingend erforderlich, einen XenApp-Server im Zuge der Installation sofort zu konfigurieren. Der Server kann stattdessen als unkonfiguriertes Template verwendet und zu einem späteren Zeitpunkt automatisiert konfiguriert werden.

Wir entschieden uns an dieser Stelle zunächst für eine manuelle Konfiguration. Zuvor war zu bedenken, dass die Remotedesktopdienste ebenfalls zu konfigurieren sind. In diesem ersten Beispiel haben wir deren Installation vom XenApp-Setup erledigen lassen. Dabei handelte es sich aber um eine unbeaufsichtigte Installation. Entsprechend sind Lizenzierungsmodus sowie Lizenzserver über den Windows Server-Manager einzustellen. Ebenso ist das Feature "Desktopdarstellung" zu installieren und der Dienst "Designs" zu starten, sofern Windows 7-Optik für den Terminalserver-Desktop gewünscht ist.

So gerüstet konnten wir mit der Konfiguration von XenApp beginnen – ein Prozess, der Administratoren früherer Versio-

nen sehr vertraut sein dürfte. Wir wählten die Option "Neue Serverfarm erstellen" und konfigurierten den Farm-Namen "XenApp6-Farm". Als Lizenzserver verwendeten wir das zuvor installierte System und entschieden uns im nächsten Dialogschritt, statt der lokalen SQL Server Express-Datenbank eine "Bestehende Microsoft SQL Server-Datenbank" zu verwenden. Diese Datenbank hatten wir zuvor auf dem SQL Server-Cluster angelegt und einen Domänen-Benutzeraccount mit dbowner-Rechten versehen. Die Namen von SQL Server, Datenbank und Benutzer konnten wir entsprechend in den folgenden Dialogen eingeben und anschließend die Verbindung testen.

Im weiteren Verlauf waren das Spiegeln von Sitzungen, der TCP-Port für den XML-Dienst sowie unser WI-Server zu konfigurieren. Letzteren konnten wir zuvor mangels XenApp-Server mit laufendem Citrix XML-Dienst noch nicht einrichten. Dies holten wir nun nach und konfigurierten dort eine XenApp Webseite sowie eine XenApp Service-Site, die die Liste veröffentlichter Applikationen wiederum vom XML-Dienst des ersten Terminalservers beziehen. Für die Service-Site definierten wir die "Passthrough-

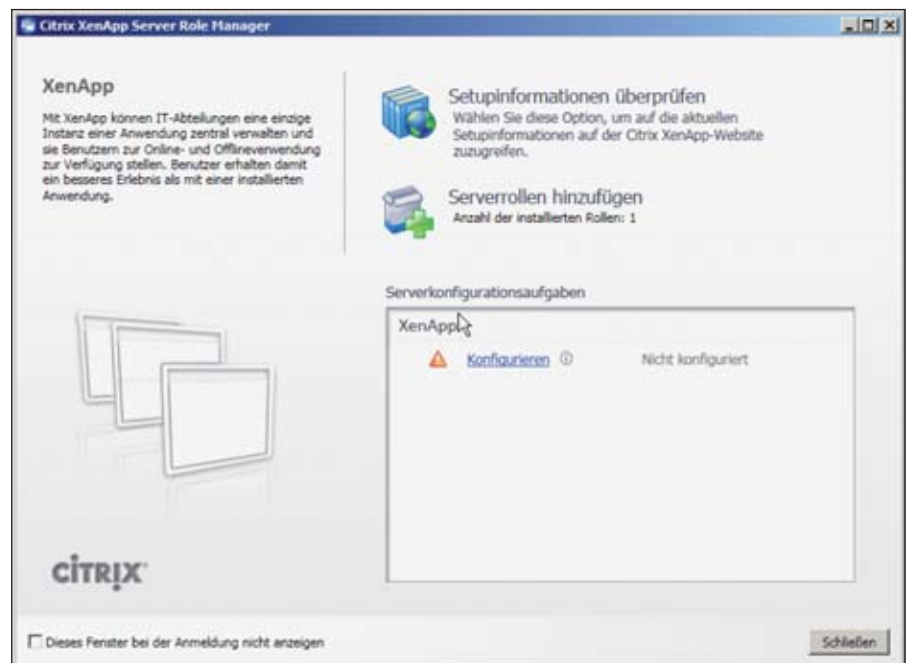


Bild 3: Die Konfiguration erfolgt als separater Prozess erst nach der Installation

Authentifizierung" als Standard, so dass Benutzer veröffentlichte Desktops und Anwendungen starten können, ohne erneut ihre Anmeldeinformationen eingeben zu müssen.

Damit war die Installation abgeschlossen und die XenApp-Dienste sowie das Citrix Online Plug-In starteten ohne Probleme. Nun konnten wir XenApp auf den übrigen beiden Terminalservern installieren. Wir entschieden uns dabei, einer bereits bestehenden Farm beizutreten. Das Setup verlief weitestgehend analog zum ersten Server, lediglich die Einstellungen für den Lizenzserver fanden sich nun im abschließenden Dialog bei den erweiterten Servereinstellungen. Die Basisinstallation war somit erledigt und wir konnten uns der weiteren Konfiguration der Farm widmen.

Management ohne Java-Konsole

Positiv fällt auf, dass die alte Java-Konsole – bekannt als "Erweiterte XenApp Konfiguration", davor als "Presentation Server Console" – endlich ausgedient hat. XenApp 6 vereint die Farm-Administration inklusive der Citrix-Richtlinien nun auf der MMC 3.0-basierten "Delivery Services Console". Diese hält für altgediente Citrix-Administratoren eine Überraschung bereit: Der Eigenschaften-Dialog des Farm-Objekts enthält bis auf die Konfigurationsprotokollierung keinerlei Optionen mehr. Aus dem Kontextmenü einzelner Server-Objekte ist der Punkt "Eigenschaften" gänzlich verschwunden. Einstellungen, die in früheren Versionen dort vorgenommen werden konnten, fanden wir im vollständig überarbeiteten Komplex der Citrix eigenen Richtlinien wieder.

Citrix integriert die XenApp-Richtlinien nun erstmals in die Gruppenrichtlinien des Active Directory. Hierzu wurde während des XenApp-Setups automatisch das Feature "Gruppenrichtlinienverwaltung" zu Windows hinzugefügt. XenApp bringt zudem die "Citrix Group Policy Engine" mit, die den neuen Ordner "Citrix Policies" in den Gruppenrichtlinienverwaltungs-Editor integriert. Wer aus organisatorischen oder technischen Gründen – etwa weil AD und XenApp-Farm von verschiedenen Teams administriert werden oder weil statt AD die Novell Directory Services für Windows zum Einsatz kommen – die Citrix-Richtlinien getrennt verwalten möchte, hat dazu weiterhin die Möglichkeit. In der "Delivery Services Console" findet sich dazu ebenfalls der Punkt "Richtlinien".

An dieser Stelle werden Einstellungen aber nicht im Active Directory, sondern weiterhin im Datenspeicher der Farm abgelegt [2]. Sind auf beiden Ebenen Richtlinien definiert, erhalten im Konfliktfall die Active Directory-Einstellungen den Vorrang vor denen der Farm. Wie von den Microsoft-Gruppenrichtlinien bekannt, sind die Citrix-Richtlinien nun gruppiert in Einstellungen pro Computer und pro Benutzer. Erstere beinhalten die Punkte, welche sich früher in den Farm-Ei-



Grenzenlose Remote Administration mit Support für Terminal Server und virtualisierte IT

GoToDevice unterstützt

Windows® 7
Windows Server® 2003 / 2008
Windows Vista®
Windows® XP
Windows® CE und Pocket PC
Linux®



Crossplattform-Fernwartung

- Betriebssystemunterstützung für 32- und 64-bit
- konfliktfreier Einsatz mit RDP und anderen Remote Control Tools
- Fast-User-Switching: Arbeiten Sie immer in Ihrem Rechte-Kontext
- Ad-hoc Support über Internet ohne Installation (optional)

Alle Funktionen, die Sie benötigen

- Zugriff auf Taskmanager, Registry, Dienste, Geräte, Ereignisprotokolle
- hierarchisches Telefonbuch (Node-Verwaltung)
- direkter Dateitransfer von Node zu Manager und von Node zu Node
- Protokollierung, Recording und optionales Session-Auditing
- Anwenderbenachrichtigung und Zugriffsbestätigung
- zentrales Lizenzmanagement

Perfekt für mobilen, installationsfreien Einsatz

- Fernwartung ohne Installation auf dem Ziel-PC
- mobile Nutzung auf Flash-Datenträgern



Jetzt gratis testen!

Probieren Sie GoToDevice **kostenlos** mit allen Funktionen in Ihrer IT-Umgebung aus.

Downloads, Lizenzkeys und mehr auf:
www.gotodevice.de

Exklusivdistribution Deutschland · Österreich · Schweiz

SBS Ges. für Systemlösungen Beratung und Service mbH
Mariabrunnstrasse 123 · 88097 Eriskirch
Tel. +49 (0) 75 41 97 00-0 · Fax +49 (0) 75 41 97 00-99
info@gotodevice.de · www.gotodevice.de





genschaften fanden, unter anderem CPU-Management und Speicheroptimierung. Auch der Neustartzeitplan ist aus der alten Java-Konsole hierhin umgezogen. Benutzerspezifische Einstellungen betreffen beispielsweise die diversen Möglichkeiten zur Optimierung der Desktop-Sitzungen sowie den Umgang mit Druckern und deren Treibern.

Die Einstellungen der Richtlinien wirken entweder pauschal auf die gesamte Farm oder eingeschränkt nur gemäß der in den Filtern definierten Regeln. So lassen sich benutzerspezifische Regeln auf bestimmte Benutzergruppen, Clientnamen oder IP-Adressen, die Art des Zugriffs (direkt oder über das Citrix Access Gateway) sowie eine neue Verwaltungseinheit namens Workergruppe eingrenzen. Die Einstellungen im Computerkontext wirken entweder global oder ebenfalls bezogen auf eine Workergruppe. Doch worum handelt es sich bei dieser neuen Funktion?

Vereinfachte Administration dank Workergruppen

In der Vergangenheit ließen sich veröffentlichte Applikationen und Einstellungen zum Load Balancing nur pro Terminalserver pflegen. Dies erforderte umfangreichere manuelle Eingriffe, Scripting oder den Einsatz von Drittanbieter-Tools, sobald einer existierenden Farm mit zahlreichen veröffentlichten Anwendungen weitere Server hinzugefügt werden sollen. Hier versprechen die neuen "Workergruppen" [3] Erleichterung bei der Farm-Administration. An Stelle einzelner Server können im Assistenten zur Veröffentlichung von Anwendungen und Desktops nun auch die Workergruppen ausgewählt werden. Werden neue Server der Farm hinzugefügt, genügt es, diese in eine oder mehrere Workergruppen aufzunehmen, um automatisch die veröffentlichten Applikationen und Load Balancing-Einstellungen der Workergruppe auf die Server anzuwenden. Natürlich müssen die entsprechenden Anwendungen zuvor auf dem Server installiert werden. Alternativ dazu empfiehlt es sich,

mehrere gleichartige Server mittels Provisioning Server aus einem gemeinsamen Image zu starten.

Provisioning ohne AppPrep-Tool

Das XenAppPrep Tool, das nötig war, um XenApp 5 für Provisioning oder Imaging vorzubereiten, gibt es in der aktuellen Version nicht mehr. Die entsprechenden Funktionen sind nun fester Bestandteil der XenApp-Installation. Das im XenApp 6 ISO-Image enthaltene XenApp Server Configuration Tool ist allerdings bereits veraltet. Eine neuere Version ist separat verfügbar [4]. Die Option, einen Server für die Bereitstellung via Provisioning vorzubereiten, steht damit im GUI der XenApp-Konfiguration zur Verfügung. Der Assistent bietet als Standard an, den Server aus der Farm zu entfernen. Wird der nachfolgende Dialog mit der Schaltfläche "Übernehmen" bestätigt, wird der Server generalisiert und tritt aus der Farm aus. Der Prozess der Generalisierung lässt sich auch über die Kommandozeile initiieren. Im Pfad `C:\Program Files (x86)\Citrix\XenApp\ServerConfig` kann dazu der Befehl

```
XenAppConfigConsole.exe /Execution-Mode:ImagePrep
```

aufgerufen werden. Hier ist zu beachten, dass im Gegensatz zum Weg über das GUI keine Sicherheitsabfrage zu bestätigen ist und der Server sofort aus der Farm austritt. Das System kann anschließend heruntergefahren und als Image verwendet

werden. Wird dieses anschließend mittels Provisioning Server gestartet, tritt der entsprechende Server mit seiner neuen Identität der Farm wieder bei und kann durch Zuordnung zu passenden Workergruppen konfiguriert werden.

Flüssige Videos durch HDX

Im Rahmen unserer Tests beließen wir es bei unseren drei manuell installierten Servern, für die wir zwei Workergruppen definierten: eine Standardgruppe mit zwei Servern, die einen vollständigen Desktop veröffentlichen soll, sowie eine zweite Gruppe mit einem Server für zusätzliche Applikationen. Als "Spezial-Anwendung" diente im Test ein veröffentlichtes Notepad. Wir benutzten das WI, um mit mehreren Test-Benutzern zunächst Verbindung zum veröffentlichten Desktop aufzunehmen und von dort das veröffentlichte Notepad zusätzlich zu starten. Mittels Password-Authentifizierung gelang dies ohne Probleme. Besonderes Augenmerk legten wir weiterhin auf die Benutzererfahrung und die Möglichkeiten von HDX. Es handelt sich dabei um eine Technik, die auch unter XenApp 5 FP3 sowie für den XenDesktop 4 verfügbar ist.

Um die Wiedergabe kontinuierlicher Medien zu optimieren, können Inhalte abhängig von Bandbreite und den benötigten Codecs zum Client umgeleitet werden. Integriert beispielsweise eine Webseite ein Flash-Video, so werden die statischen Elemente der Seite auf dem Terminalserver

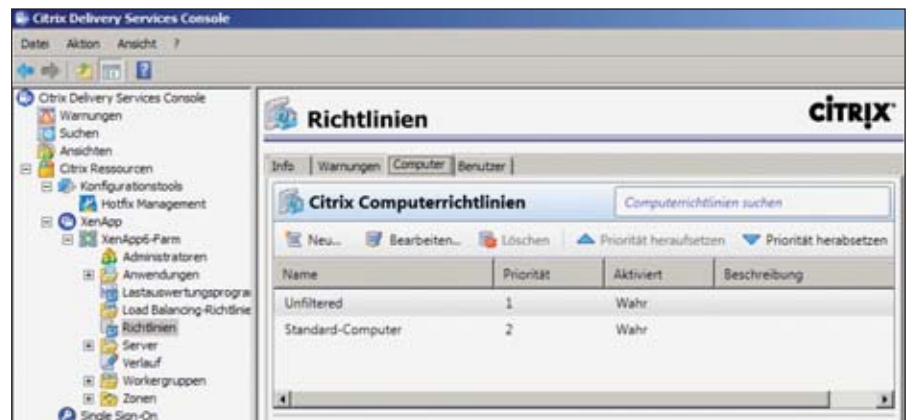


Bild 4: Analog zu den Microsoft-Gruppenrichtlinien unterscheiden die Citrix-Richtlinien nun Einstellungen pro Benutzer und pro Computer



Features der verschiedenen Editionen				
Funktionen	Fundamentals	Advanced	Enterprise	Platinum
Anwendungsbereitstellung				
Anwendungs-Hosting (Online-Zugriff)	Ja	Ja	Ja	Ja
Unterstützung lokaler Peripherie (Drucker, USB, et cetera)	Ja	Ja	Ja	Ja
Selbstbedienungs-Anwendungsladen (Dazzle)	–	Ja	Ja	Ja
Anwendungs-Streaming (Offline-Zugriff)	–	Ja	Ja	Ja
Benutzerfunktionalität				
High Definition User Experience (HDX)	Ja	Ja	Ja	Ja
Profil-Management	–	–	Ja	Ja
Optimierung von WAN-Verbindungen (Software Client-Lizenzen)	–	–	–	Ja
Sicherheit				
Zentrale Datenhaltung und Datensicherung	Ja	Ja	Ja	Ja
SSL-verschlüsselter Zugriff auf gehostete Anwendungen	Ja	Ja	Ja	Ja
Kompletter SSL-VPN-Tunnel und SmartAccess (Access Gateway Universal Licenses)	–	–	–	Ja
Single Sign-On und Passwort-Management	–	–	–	Ja
Richtlinienbasiertes Recording von Benutzersitzungen	–	–	–	Ja
Enterprise Class Infrastructure				
High Availability und Failover	Ja	Ja	Ja	Ja
XenServer Virtualisierungs-Plattform	Ja	Ja	Ja	Ja
CPU- und Speicheroptimierung	–	–	Ja	Ja
Server-Monitoring und automatisierte Alerts	–	–	Ja	Ja
Anwendungs-Performance-Monitoring	–	–	–	Ja
Provisioning Services (Workload Streaming für XenApp Server)	–	–	–	Ja
Preferential Load Management	–	–	–	Ja

gerendert und als Bitmap an den Client geschickt. Das Video wird stattdessen zum Client gestreamt und erst dort mit dem lokalen Codec dekodiert. Die positiven Erfahrungen aus unserem XenDesktop-Test [5] fanden wir auch unter XenApp bestätigt. Beim Aufruf einer Flash-Webseite fragte der Client bei der ersten Verwendung an, ob die entsprechende HDX-Funktion aktiviert werden soll. Die Inhalte wurden einschließlich YouTube-Videos ohne Probleme ausgegeben. Dies funktionierte auch von einem entfernten Client aus, der per VPN über eine DSL-Verbindung mit 3 MBit/s angebunden war.

In einem Punkt hat das Microsoft eigene Remote Desktop Protocol (RDP)

derzeit allerdings noch die Nase vorn, sofern Windows 7 auf dem Client zum Einsatz kommt. Auch mit den HDX-Erweiterungen und 32 Bit-Farbtiefe unterstützt das ICA-Protokoll noch keine Aero-Effekte in Terminalserver-Desktops. Es ist zwar möglich, Aero-Desktop-Themes zu laden, dies hat aber in ICA-Sitzungen keinen Einfluss auf die Farbe und Transparenz der Fenster. Diese Funktion soll Einzug halten, sobald Microsoft mit dem Service Pack 1 für den Windows Server 2008 R2 eine neue Technik namens RemoteFX einführt. Diese will Citrix wiederum zukünftig mit HDX integrieren, um die Darstellung grafikintensiver Anwendungen weiter zu verbessern [6].

XenApp 5 und dessen Ahnen boten die Möglichkeit, über die Java-Konsole Printserver zu importieren und deren Druckertreiber über die Server der Farm zu replizieren. Mit XenApp 6 ist diese Funktion nun nicht mehr im GUI vorhanden. Stattdessen kann eine manuelle oder automatische Replikation von Treibern mittels PowerShell-Cmdlets realisiert werden [7]. Alternativ verweist Citrix auf die Bordmittel des Windows Server 2008 R2 und empfiehlt, die Rolle "Druck- und Dokumentdienste" mit dem Rollendienst "Druckerserver" zu installieren, um dessen Import-/Export-Funktionen zu nutzen [8].

Zu guter Letzt stellte sich noch die Frage, wie wir uns einzelner Server unserer Farm



wieder entledigen können. Sollte ein Server nicht mehr in der Lage sein zu booten, besteht grundsätzlich immer die Möglichkeit, das System über die Delivery Services Console aus der Farm zu entfernen. Mittels Rechtsklick gelangen Sie zu der Aktion "Andere Aufgaben / Aus Farm entfernen". Sofern das System aber noch lauffähig und am Netz ist, empfiehlt der Hersteller, das System ordnungsgemäß aus der Farm austreten zu lassen. In früheren Versionen diente dazu der Kommandozeilen-Befehl `Chfarm`, den man im aktuellen Release aber vergeblich sucht [9]. Die Funktionalität findet sich im GUI der XenApp-Konfiguration als separater Punkt neben der Vorbereitung für das Provisioning.

Migration auf Version 6


Und wie gelangen Administratoren einer XenApp 5 Farm nun möglichst schnell zu einer XenApp 6 Umgebung? Beim neuen Wurf handelt es sich um ein komplett eigenständiges Release, das ausschließlich

für Windows Server 2008 R2 verfügbar ist. Eine Upgrade-Installation älterer Farmen oder ein gemischter Betrieb von XenApp 5- und 6-Servern innerhalb einer Farm wird nicht unterstützt. Angesichts der umfassenden Änderungen im Bereich der Policies und Management-Tools ist dies verständlich und bietet, positiv betrachtet, die Chance für einen Neuanfang ohne Altlasten. Gerade für größere Farmen mit komplexen Richtlinien und zahlreichen Anwendungen würde dies aber einen erheblichen manuellen Aufwand bedeuten. Mit dem XenApp 6 Migration Tool [10] bietet Citrix eine Sammlung von PowerShell 2.0-Cmdlets, die bei der Migration von Richtlinien und Anwendungen helfen soll.

Fazit

Mit XenApp 6 unterstützt Citrix endlich den Windows Server 2008 R2 und stellt eine Reihe interessanter Verbesserungen des Produktes vor. Dass das Farm-Management nun über eine einheitliche Konsole erfolgt, darf als Meilenstein in der Entwicklung des Produkts betrachtet werden. Der Installationsprozess wurde signifikant vereinfacht und trägt durch die Trennung von Installation und Konfiguration der steigenden Bedeutung von Provisioning Rechnung. Die neuen Richtlinien bringen mehr Übersicht in die Konfiguration. Nicht zuletzt nehmen die Workergruppen dem Admin Arbeit ab, da nun veröffentlichte Anwendungen nicht mehr pro Server gepflegt werden müssen.

Leider hat mit der neuen Version neben den Konsolen auch der Citrix Resource Manager ausgedient. Wer bislang dessen Funktionen zur statistischen Auswertung der Farm-Nutzung verwendete, kommt nun nicht mehr daran vorbei, sich mit Citrix EdgeSight zu beschäftigen. Schade ist zudem, dass die neuen Funktionen bislang ausschließlich für Terminalserver unter Windows Server 2008 R2 verfügbar sind. Wer parallel dazu noch Applikationen unter Windows Server 2003/2008 oder virtuelle Desktops unter XenDesktop 4 betreiben möchte, hat weiterhin mit

den alten Konsolen und Richtlinien zu tun. Nichtsdestotrotz zeigt das neue Release sehr gute Ansätze zur Vereinfachung der Administration. So bleibt zu wünschen, dass XenDesktop hier nachzieht und beide Produkte identisch verwaltet werden können. Der Bereitstellung einheitlicher Arbeitsumgebungen mit Windows 7 Desktops und Windows Server 2008 R2 Terminalservern steht bereits jetzt nichts mehr im Wege. (dr) 

Produkt

Funktionserweiterung der Microsoft-Remotedesktopdienste.

Hersteller

Citrix Systems
www.citrix.de

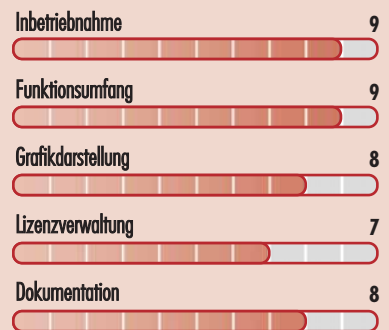
Preis

Advanced Edition rund 200 Euro pro User,
Enterprise Edition etwa 260 Euro pro User,
Platinum Edition etwa 345 Euro pro User.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für Umgebungen, in denen Windows-Applikationen unter Windows Server 2008 R2 von vielen verschiedenen Plattformen aus genutzt werden sollen.

gut für mittlere und größere Unternehmen, insbesondere auch zur Anbindung von Außenstellen und Heimarbeitsplätzen.

derzeit weniger für Unternehmen mit überwiegend oder ausschließlich mobilen Benutzern, die noch dazu meistens offline arbeiten.

Citrix XenApp 6

- [1] **Nachträgliche IIS-Integration**
<http://support.citrix.com/article/CTX125107/>
- [2] **Getrennte Verwaltung der Citrix-Richtlinien**
<http://support.citrix.com/article/CTX125152/>
- [3] **Workergruppen**
<http://support.citrix.com/article/CTX124481/>
- [4] **Aktuelles XenApp Server Configuration Tool**
<http://support.citrix.com/article/CTX124981/>
- [5] **XenDesktop-Test**
"Im Test: Citrix XenDesktop 4.0 – Arbeitsplatz im Netz" in IT-Administrator 04/2010
- [6] **Integration von RemoteFX und HDX**
<http://hdx.citrix.com/hdxrichgraphics/>
- [7] **Replikation von Treibern mittels PowerShell-Cmdlets**
<http://support.citrix.com/article/CTX126125/>
- [8] **Import- und Exportfunktion des Druckerservers nutzen**
<http://support.citrix.com/article/CTX125160/>
- [9] **Server ohne Chfarm-Befehl entfernen**
<http://support.citrix.com/article/CTX125130/>
- [10] **PowerShell 2.0-Cmdlets zur Migration von Richtlinien und Anwendungen**
<http://support.citrix.com/article/CTX125471/>

Links



Clustering-Feature in PRTG Network Monitor 8

Ausfallsichere Netzwerküberwachung

Version 8 der Netzwerküberwachungssoftware PRTG Network Monitor ist mit zahlreichen neuen Features ausgestattet. Beispielsweise ermöglicht die neu integrierte „Cluster“-Funktion ein ausfallsicheres Monitoring. So wird sichergestellt, dass auch bei einem Software-Update oder Crash des Hauptservers das Monitoring ganz normal weiterläuft. Dazu überwachen alle Cluster-Nodes (bis zu 5) permanent das Netzwerk – optional aus verschiedenen Perspektiven und falls erforderlich auch in verteilten Netzwerken. Jeder „Knotenpunkt“ verfügt dabei über die gesamte aktuelle Cluster-Konfiguration und eine eigene Datenbank, in der die Monitoring-Ergebnisse vorgehalten werden.

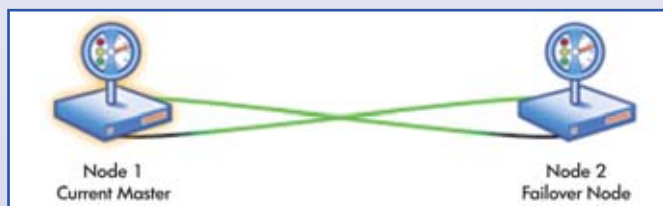
In einem PRTG Cluster bilden bis zu 5 PRTG-Server-Installationen als Knotenpunkte („Nodes“) ein ausfallsicheres Failover Monitoring System. Ziel ist es, eine nahezu 100-prozentige Verfügbarkeit bei der Netzwerküberwachung zu erreichen. Mit Hilfe des Clustering wird die Betriebszeit nicht mehr durch Verbindungsstörungen oder einen Ausfall der Internetanbindung am PRTG Server, fehlerhafte Hardware oder Software-Upgrades beeinträchtigt.

Funktionsweise

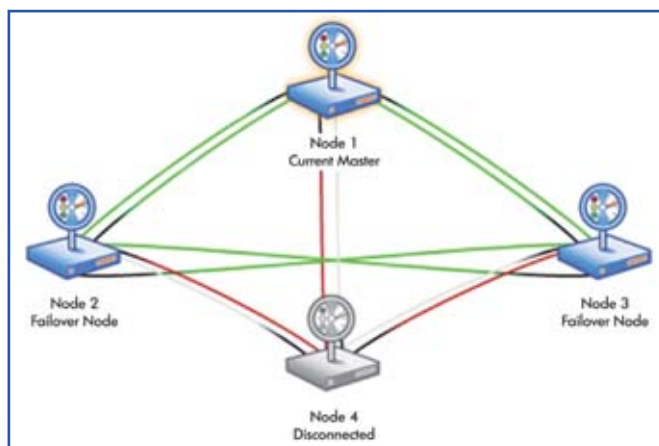
Ein PRTG-Cluster besteht aus einem „Master Node“ sowie einem oder mehreren „Failover Nodes“. Jeder dieser Knotenpunkte wiederum besteht aus einer vollständigen Installation des PRTG Network Monitors und führt selbstständig die komplette Überwachung des Netzwerks durch. Die Knoten sind über verschlüsselte TCP/IP-Verbindungen miteinander verbunden und kommunizieren bidirektional.

Konfiguration

Während des normalen Betriebs wird der „Master Node“ genutzt, um Geräte und Sensoren zu konfigurieren (per PRTG Web-Interface oder Windows GUI). Anschließend verbreitet dieser automatisch die Konfiguration an alle anderen Knoten. Auf Basis der Einstellungen überwachen die Nodes parallel das gesamte Netzwerk und speichern die Resultate jeweils in einer eigenen Datenbank ab. Dadurch stehen selbst bei einem kompletten Datenverlust auf einem Knoten immer noch die Monitoring-Ergebnisse auf den anderen Cluster-Nodes bereit. Der Administrator kann das Monitoring via Web-Interface auf dem „Master Node“ zentral managen und zusätzlich jederzeit alle Ergebnisse auf jedem Cluster-Knoten im Lesemodus einsehen. Fällt der „Master Node“ aus, übernimmt automatisch einer der „Failover Nodes“ dessen Rolle und sorgt dafür, dass Benachrichtigungen und Berichte unterbrechungsfrei zur Verfügung stehen. Durch ein intelligentes internes Management werden die Rollen wieder getauscht, sobald der „Master Node“ erneut zur Verfügung steht. Bricht der Server komplett zusammen – beispielsweise durch einen Hardwaredefekt – kann ein solcher temporärer „Master Node“ auch dauerhaft die Master-Rolle übernehmen.



Bereits eine „Single Failover“ Installation ermöglicht ausfallsicheres Monitoring und die Abfrage von Überwachungsdaten aus unterschiedlichen Perspektiven



In einem PRTG-Cluster führen alle „Knotenpunkte“ ein selbstständiges Monitoring durch. Dies ermöglicht eine lückenlose Datenaufzeichnung, selbst wenn ein Node ausfällt.

Benachrichtigung

Für den Fall, dass ein oder mehrere Knoten Ausfälle oder Schwellenwertüberschreitungen erkennen, erhält der Administrator eine zentrale Benachrichtigung durch den Master-Node (per E-Mail, SMS etc.). Zusätzlich bietet PRTG im Cluster einen neuen Sensor-Status namens „Down (Partial)“, der einen Ausfall indiziert, der nur von einigen Nodes im Cluster gemeldet wird. Damit kann der Administrator leicht feststellen, ob tatsächlich ein Dienst oder Gerät einen Fehler aufweist oder ob nur eine bestimmte Verbindung betroffen ist.

Alle PRTG Lizenzen ermöglichen mit nur einem Lizenzschlüssel die Einrichtung einer „Single Failover“ Installation, bei der zwei PRTG-Installationen zusammen ein Cluster bilden. PRTG Site und Corporate Lizenzen bieten zusätzlich die Möglichkeit Failover Cluster mit drei bis fünf Knoten aufzusetzen.

 **PAESSLER®**

Paessler AG

Burgschmietstraße 10
D-90419 Nürnberg
Tel.: +49 (911) 7 39 90 30
Fax: +49 (911) 7 39 90 31

E-Mail: info@paessler.com

URL: www.de.paessler.com



Einkaufsführer: Solid State Storage

Keine ordinäre Festplatte

von Marcus Schneider

Solid State Storage, also Speicher auf Basis von Chips, die ihre Informationen auch ohne Strom nicht verlieren, wird immer beliebter. Die Chips liefern hohe Zugriffsgeschwindigkeit, geringen Stromverbrauch bei wenig Abwärme und große Toleranz gegenüber Umwelteinflüssen. Dies macht die Technologie für unterschiedlichste Anwendungsszenarien interessant; entsprechend vielfältig sind die Formfaktoren und Gehäuse, in denen Anwender SSDs kaufen können. Unser Einkaufsführer erklärt, welche Produktformen und Einsatzgebiete Solid State derzeit bietet.

Am gängigsten sind Solid State Disks (SSD), also Flash-Chips, die in Form einer herkömmlichen Festplatte daherkommen. Der große Vorteil: Sie lassen sich in Servern oder RAID-Systemen anstatt einer Festplatte einbauen, wenn das vom jeweiligen Hersteller zertifiziert ist. Gerade bei den Speichersystemen kommen dann in der Praxis typischerweise nur die Festplatten vom Hersteller des jeweiligen Speichersystems in Frage. Natürlich ist es möglich, in einem Gehäuse SSD und herkömmliche Festplatten zu mischen und so Platz zu sparen.

Unterscheiden müssen wir zwischen SSD für den Einbau in herkömmlichen PCs und in Enterprise Speichersystemen. Letztere werden auch "Enterprise Class SSD" genannt und zeichnen sich durch eine deutlich bessere Haltbarkeit aus, sind allerdings auch deutlich teurer als die "Consumer SSD".

Flashspeicher auf PCI-Karten

In letzter Zeit haben Flash-Chips auf PCI-Karten für Furore gesorgt. Schon bei nur wenigen SSD lassen sich bei Speichersystemen manchmal keine Geschwindigkeitssteigerungen mehr erreichen, weil der Kommunikationsweg zum Flaschenhals wird, insbesondere bei Verwendung von SAS am Backend des Speichersystems. Im Gegensatz dazu erreichen PCI-

Karten durch den direkten Kontakt zum Serverbus sehr hohe Geschwindigkeiten. Allerdings sind sie einem Server fest zugeordnet. Somit sind sie für typische Speichernetzaufgaben nicht geeignet, also immer dann, wenn mehrere Server auf ein Speichersystem parallel zugreifen sollen.

Das hervorstechende Merkmal von PCIe-basierten Flash Karten ist die besonders hohe Geschwindigkeit. Um solche Karten zu vergleichen, ist es zunächst wichtig zwischen PCIe 1 und dem doppelt so schnellen PCIe 2 zu unterscheiden. Das zweite Kriterium ist die Anzahl sogenannter "Lanes". Wenn eine Karte zwei Lanes bietet, ist sie doppelt so schnell wie mit einer Lane und es findet sich die Bezeichnung "x2". Schnelle Karten unterstützen bis zu 32 Lanes.

Flash als Cache

Einen gänzlich anderen Weg gehen einige Hersteller, die ihre Speichersysteme mit Einschubkarten auf Basis von Flash-Chips bestücken. Anders als bei SSD entscheidet nicht der Nutzer, welche Daten er auf dem Flash-Chip speichert – die Chips sind hier kein Fest-



Bild 1: Eine Flash-basierte Caching-Karte zur schnelleren Datenbereitstellung

plattenersatz, Storage ist nicht ihre Primäraufgabe. Vielmehr nutzen die Storage-Systeme den Flashspeicher als Cache, also als klassischen Zwischenspeicher. Damit lassen sich bemerkenswerte Geschwindigkeitsverbesserungen erreichen, ohne dass sich Anwender vie-

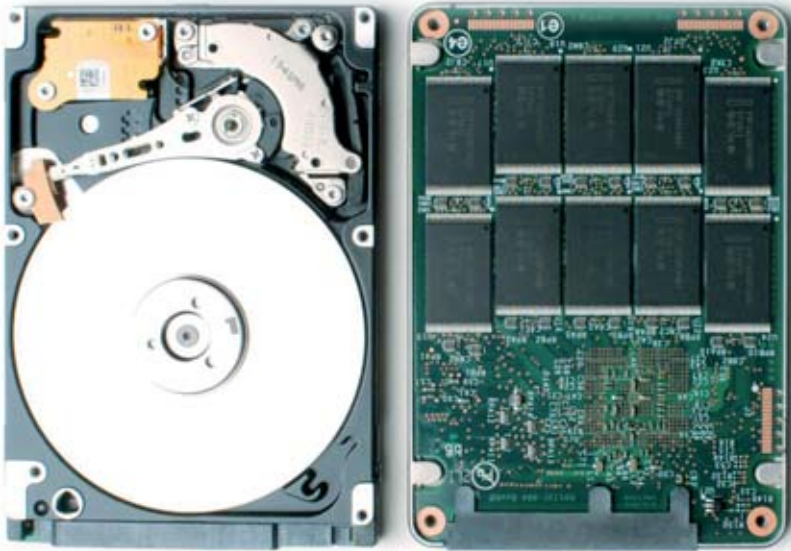


Bild 2: Ein Solid State Drive im Format einer herkömmlichen Festplatte

le Gedanken um das Datenkonzept machen müssen. Eine optimale Datenverteilung gemäß Servicelevels lässt sich aber auf diesem Weg nicht erreichen.

Reiner Flashspeicher und DRAM

Schließlich finden sich auch erste Speichersysteme am Markt, die konsequent nur auf Flashbausteine setzen. Ihre Funktionalitäten unterscheiden sich prinzipiell nicht von denen festplattenbasierter Storage-Systeme. Da sie aber von vorneherein für reinen Flash-Speicher neu entwickelt wurden, können sie deutlich platzsparender gebaut werden und auch die Kommunikation nach außen wurde für den enormen Durchsatz der Halbleiter optimiert. Solche Systeme haben allerdings ihren Preis; Anwender müssen sorgsam abwägen, ob die höhere Leistung die Ausgaben rechtfertigt, vor allem da Solid State Drives eine begrenzte Lebensdauer aufweisen. Hier gibt es von Industrieseite Applikationen, welche die Kalkulation erleichtern [1, 2].

Zu guter Letzt sind DRAM-basierte Systeme zu erwähnen. Sie sind schon etwas länger auf dem Markt. Anders als Flash Memory verliert ein DRAM-Chip seine Information, wenn ihm der Strom ausgeht. Dafür ist er allerdings noch schnell-

ler. Auch diese Systeme sind typischerweise in den oberen Preisregionen zu Hause und empfehlen sich nur für spezifische Anwendungsszenarien.

Auf den Einsatzzweck kommt es an

Vor einer Entscheidung für eine bestimmte Solid State-Storage-Technologie ist natürlich die Frage nach dem Einsatzzweck zu beantworten. Typischerweise steht der Wunsch nach einer größeren Geschwindigkeit einer Applikation am Anfang. Für Fileservices machen Flash-Speicher also eher weniger Sinn, spannend wird es bei Datenbankapplikationen. Nun lohnt sich der Blick ins Detail: Von Flash-Bausteinen kann sehr schnell gelesen werden, das Schreiben von Informationen muss aber nicht gravierend schneller sein als bei herkömmlichen Festplatten. RAID-Controller verfügen über umfangliche Caches, die insbesondere das Lesen von Daten beschleunigen. Wenn also große, zusammenhängende Datenmengen gelesen werden, kann es passieren, dass die durch den Controller Cache erreichte Geschwindigkeit kaum noch gesteigert werden kann. Beim Lesen von kleinen Informationsblöcken, auf die recht willkürlich zugegriffen wird, zeigt Flash seine wahre Stärke.

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



Übersicht einiger Einsatzszenarien und passender SSS-Produkte

Einsatzszenario	Geeignete Produkte
Bedarf an maximaler Geschwindigkeit, um zum Beispiel digitale Bild-/Videobearbeitung zu beschleunigen.	PCIe-Karte (Fokus auf Geschwindigkeit), SSD im Server
Flash für Notebook, um Energie zu sparen und den PC schneller starten zu können.	Einfache und günstige Consumer-SSD im Festplattenformat. Hier lassen sich auch MLC-Chips nutzen.
Networked Storage, um zum Beispiel von virtualisierten Servern auf einen gemeinsamen, möglicherweise gar redundanten Speicherpool zuzugreifen.	Netzwerkspeicher mit Flash-Beschleunigungskarte oder mit Enterprise Class SSD; hohe Anforderungen an Geschwindigkeit und Haltbarkeit; auf Flaschenhalse im Speichernetzwerk achten.

Obwohl es am schönsten wäre, die ganze Datenbank im Solid State-Speicher vorzuhalten, so ist das recht kostspielig und auch nicht unbedingt nötig. Nicht alle Tabellen einer Datenbank sind für die Geschwindigkeit des Zugriffs gleich wichtig. Wenn zum Beispiel nur die wichtigsten Index- und Logdateien auf dem Flashspeicher liegen, lassen sich mit relativ geringen Kapazitäten und kleinen Kosten erhebliche Leistungssteigerungen realisieren.

Ein gutes Indiz, wo Halbleiterspeicher helfen können, bietet der Einsatz von Festplatten, die im "Short Stroking"-Verfahren genutzt werden. Nutzen Sie also viele Festplatten und viele Spindeln, um hohe Geschwindigkeiten zu erreichen, bleibt der Großteil der Platten-Kapazität jedoch ungenutzt. In diesen Fällen steht offensichtlich die Geschwindigkeit im Vordergrund, ein klassischer Fall für die Vorzüge des Halbleiters. Auch im Kostenvergleich sieht SSS hier gut aus, da die (günstige) Kapazität der Festplatten ja gar nicht ganz genutzt wird.

Neben dem Einsatz für Datenbanken gibt es zahlreiche Branchen, in denen spezifische Anwendungen geradezu nach Flash verlangen. Kurz gesagt wird Flash immer dann interessant, wenn höchstmögliche Verarbeitungsgeschwindigkeit verlangt wird und die Festplatte bisher den Flaschenhals darstellte. Solche Szenarien finden sich zum Beispiel in der Bild- und Videobearbeitung, aber auch im Forschungsbereich.


Praxisnahe Auswahlkriterien

Das hervorstechende Merkmal von SSS ist die hohe Geschwindigkeit, sowohl im Durchsatz als auch in Hinblick auf die Latenzzeit beim Zugriff auf Daten. Und bei der Geschwindigkeit gibt es große Unterschiede. Die SNIA (Storage Networking Industry Association) Europe hat vor kurzem Informationen veröffentlicht, welche die Geschwindigkeit von Halbleiterspeichern vergleichbarer machen [3]. Ein Hauptproblem bisher: SSS sind zu Beginn sehr schnell, werden aber in der ersten Zeit der Nutzung langsamer, bis sich ihre Leistung auf einem gewissen Pegel einpendelt. Die Testbeschreibung der SNIA hilft nun, diesen Effekt bei der Geschwindigkeitsmessung einzubeziehen und sowohl praxisnahe als auch vergleichbare Werte zu ermitteln. Weiterhin zu beachten: Flash-Speicher sind stets langsamer beim Schreiben als beim Lesen. Je nach Einsatzwunsch ist also explizit auf beide Werte zu achten.

Auch ein wichtiger Punkt ist, dass Flash-Speicher altern. Sie können nur für eine endliche Anzahl von Schreibvorgängen genutzt werden. Hersteller nutzen mannigfaltige Techniken, die Lebensdauer zu erhöhen. Beispielsweise Reservezellen, welche eine gewisse Zahl von Zellausfällen kompensieren. Leider gibt es keine verlässliche Standardisierung, um die Haltbarkeit von SSS zu beschreiben. Eine garantierte Anzahl Schreibvorgänge ist aber ein guter Wert, anhand dessen Sie einen Vergleich starten können.

Haltbarkeit und Geschwindigkeit von SSD haben auch mit den verwendeten Chips zu tun. SLC (Single Layer Cell) Flash-Chips sind typischerweise schneller, haltbarer und teurer als MLC (Multi Level Cell)-Chips. Um den Preis für SSS zu senken, arbeiten viele Hersteller daran, MLC-Chips fit für höhere Speicherweihen zu machen. Da die Anzahl der Levels in MLC steigt, wird der Preisabstand zwischen MLC und SLC größer. Bei allen preislichen Verlockungen gilt es aber insbesondere die Haltbarkeit im Auge zu behalten, sonst droht ein böses Erwachen.

Fazit


Gibt es Flash-Technologie-Empfehlungen für kleine, mittlere oder große Unternehmen? Nein. Die Entscheidung für eine bestimmte Technologie hängt davon ab, was Sie damit erreichen möchten. Auch für einen Freiberufler kann sich Flash rechnen, wenn es ihm hilft seine Effizienz deutlich zu steigern, während es für Großunternehmen sinnvoll sein kann, zumindest vorerst auf Flash zu verzichten, wenn die benötigten Service Levels mit günstigeren Festplatten erfüllt werden und sich durch höhere Geschwindigkeiten von relevanten Services keine Wettbewerbsvorteile erzielen lassen. (jp) 

Marcus Schneider ist Mitglied im SNIA Europe Board of Directors und Director Product Segment Data Protection bei Fujitsu.

[1] SNIA SSD TCO Calculator
<http://it-a.eu/aat61>

[2] SNIA SSD TCO Whitepaper
<http://it-a.eu/aat62>

[3] SNIA Solid State Storage Performance Test Specification Overview
<http://it-a.eu/aat63>

Links 



Bestellen Sie jetzt das IT-Administrator Sonderheft II/2010!

180 Seiten Praxis-Know-how
rund um das Thema

Active Directory

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

* IT-Administrator Abonnenten erhalten das Sonderheft II/2010 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/



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

Ja, ich bin IT-Administrator Abonnent mit der Abnummer (falls zur Hand) _____ und bestelle das IT-Administrator Sonderheft II/2010 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

Ja, ich bestelle das IT-Administrator Sonderheft II/2010 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 Eltville.

So erreichen Sie unseren Vertrieb, Abo- und Leserservice:

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



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 1110

Neue Features im SQL Server 2008 R2

Die intelligente Datenbank

von Thomas Joos

Mit SQL Server 2008 R2 wartet Microsoft mit einigen Neuerungen in punkto Skalierbarkeit, Performance und Produktivität auf. Vor allem im Bereich Business Intelligence und Data Warehouses mit extrem großen Datenmengen gibt es interessante Veränderungen – nicht zuletzt bieten die Redmonder zwei komplett neue Editionen des SQL-Servers für große Rechenzentren an. Beim Thema Business Intelligence will Microsoft hingegen auch Anfänger ansprechen, die mit der Aufbereitung ihrer Daten noch keine große Erfahrung haben. IT-Administrator hat sich die neue Version angesehen und stellt die Neuheiten und überarbeiteten Funktionen vor.

SQL Server 2008 R2 baut direkt auf SQL Server 2008 auf. Dies bedeutet, dass die neue Version bereits beim Release vom hohen Sicherheitsstandard, der Leistung sowie den Funktionen und Tools von SQL Server 2008 profitiert. In den beiden neuen Editionen sind intuitive Werkzeuge integriert, um Business Intelligence im Unternehmen zu erweitern oder frisch einzuführen. Diese neuen Varianten sollen die Leistung für stark beanspruchte Datenbanken vergrößern. Microsoft holte sich dafür Hardware-Partner an Bord, die die neuen Editionen als Appliance anbieten.

Gezielte Einbindung in die Produktpalette

Besonders im Zusammenspiel mit Office 2010 und SharePoint 2010 soll SQL Server 2008 R2 eine homogene und hochleistungsfähige Basis für Business Intelligence im Unternehmen bilden. Ein Beispiel dafür ist Office 2010, das über Client-Features wie Adhoc-Analysen oder Reporting verfügt, während SQL Server 2008 R2 die passende Serverlösung für die Verarbeitung und SharePoint 2010 das Enterprise-Portal bereitstellt. Die Verbindung lässt sich einfach realisieren und Microsoft stellt für die Verwaltung einige kostenlose Zusatztools zur Verfügung. Die Berechtigungen dazu lassen sich im Active Directory integrieren.



Passend dazu bietet Microsoft Downloads an wie das SQL Server 2008 R2 Reporting Services-Add-In für Microsoft SharePoint-Technologien 2010, das Sie unter [1] herunterladen können. Mit dem Werkzeug lassen sich die Berichte mit den Reporting Services aufbereiten und direkt über eine Webseite in SharePoint darstellen. Die Installation ist kostenlos und bietet ein Webfrontend auf den SharePoint-Servern. Dazu installieren Sie auf den SharePoint-Servern

einen Berichtsproxy und ein Webpart, das die Ansicht der Berichte aus den Reporting Services ermöglicht. Die Kommunikation zwischen SharePoint und Reporting Services erledigt ein Proxy, der auch die Authentifizierung steuert. Der Berichtsserver muss dazu mit SQL Server 2008 R2 im integrierten SharePoint-Modus installiert sein. Eine ausführliche Anleitung und Erklärung der technischen Hintergründe finden Sie unter [2].



Bild 1: Bereits während der Installation der Reporting Services wählen Sie die SharePoint-Integration aus

Neue Hochleistungsplattformen

Mit den beiden neuen Editionen "Datacenter" und "Parallel Data Warehouse" bietet Microsoft vor allem im Bereich der Business Intelligence neue Dimensionen in Leistung und Verfügbarkeit. Die Datacenter-Edition baut auf SQL Server 2008 Enterprise Edition auf, enthält also alle Funktionen dieser Variante und weitere Möglichkeiten wie die Unterstützung von mehr Arbeitsspeicher. Die neue Edition ist als Hochleistungsplattform vorgesehen, um große Anwendungs-Workloads zu meistern und Datenbanken zu konsolidieren. Sie ist dafür ausgelegt, eine extrem hohe Datenmenge zu verarbeiten und dabei deutlich leistungsfähiger zu sein als mehrere SQL-Server älterer Versionen. Auch für die Virtualisierung stellt die Edition die beste Lösung dar und ist für eine maximale Virtualisierung unter Hyper-V optimiert, zum Beispiel in virtuellen Rechenzentren mit leistungsfähigen Hosts. Bei der Verwendung des Arbeitsspeichers ist SQL Server 2008 R2 Datacenter nicht wie die anderen Editionen eingeschränkt, sondern unterstützt so viel RAM wie das zu Grund liegende Betriebssystem (siehe Kasten).

Die zweite neue Edition mit der Bezeichnung Parallel Data Warehouse ist vor allem für den Einsatz als Business Intelligence-Basis für extrem hohe Datenmengen ge-

dacht, die auf verschiedene Server verteilt sind und an die verschiedene Client-Anwendungen angebunden sind. Über die neue Massively Parallel Processing (MPP)-Technologie sowie die Unterstützung von zahlreichen Hardware-Partnern können Sie ein Data Warehouse auf den Petabyte-Bereich ausdehnen. Dazu skalieren Sie unter Verwendung von MPP mehrere hundert TByte auf 1 PByte. Der Vorteil der MPP-Technologie liegt darin, dass sich große Datentabellen auf mehrere Server in einem Cluster verteilen lassen. Auf jedem Knoten läuft dann eine eigene Datenbank-Instanz, was die Leistung extrem verbessert. Die Rechenleistung erledigt dann nicht nur ein einzelner sehr leistungsfähiger Server, sondern gleich mehrere im parallelen Einsatz. Die Kehrseite der Medaille: Da nicht nur ein einzelner, sondern mehrere Server die Berechnung ausführen, steigt natürlich auch der Administrations-Aufwand, um den Cluster zu verwalten.

Nahtlose Integration in passende Hardware

Microsoft hat im Zusammenhang mit dieser neuen Technologie das Unternehmen DATAlegro gekauft, das die entsprechenden Funktionen entwickelt hat. SQL Server 2008 R2 Parallel Data Warehousing unterstützt Hardware von HP, Dell, Bull, IBM und EMC und steht

als Appliance zur Verfügung. Die Hardwarepartner liefern also die Software und optimal angepasste Hardware, ähnlich zum Datacenter-Konzept in Windows Server 2008 (R2). Darüber hinaus unterstützt die Edition noch Star Join-Abfragen und Change Data Capture. Star Join-Abfragen optimieren die Abfragen im Data Warehouse, während Change Data Capture dafür sorgt, dass nur geänderte Daten in die Datenbank geschrieben werden. Dies soll die Verarbeitungen von Abfragen bei hohen Datenmengen beschleunigen. Da derartige Abfragen vor allem im Bereich Business Intelligence (BI) und in Data Warehouses auftreten, sind so leistungsfähigere BI-Lösungen mit größeren Datenmengen möglich. Zusätzlich lässt sich SQL Server 2008 R2 in die Integration Services, Reporting Services und Analysis Services von SQL Server 2008 integrieren.

Ebenfalls neu sind die Master Data Services. Diese ermöglichen die zentrale Pflege von Daten, die von unterschiedlichen Quellen verwendet werden. Auch die Hub-and-Spoke-Architektur nach Branchenstandards für das Data-Warehousing ist möglich. Die Datenbank verhält sich dabei so, dass die Daten auf einem Enter-

Zusammen mit Windows Server 2008 R2 unterstützt SQL Server 2008 R2 folgende Maximalwerte:

Server 2008 R2 Foundation x64:

1 CPU, maximal 8 GByte RAM

Server 2008 R2 Standard x64:

4 CPUs, maximal 32 GByte RAM

Server 2008 R2 Enterprise x64:

8 CPUs, maximal 2 TByte RAM

Server 2008 R2 Datacenter x64:

64 CPUs, maximal 2 TByte RAM

Web Server 2008 R2 x64:

4 CPUs, maximal 32 GByte RAM

Server 2008 R2 für Itanium-basierte Systeme:

64 CPUs, maximal 2 TByte RAM

**Diese Hardware unterstützt
SQL Server 2008 R2 in der
Datacenter Edition**



prise-Hub an die verschiedenen Empfänger (Spokes) verteilt werden. Dabei handelt es sich um Geschäftseinheiten oder Fachabteilungen. Die neuen Editionen verwalten bis zu 25 Instanzen, die über mehrere Server verteilt sein können. SQL Server 2008 R2 unterstützt bis zu acht Prozessoren und 256 Kerne. Was viele Unternehmen freuen wird, ist die Tatsache, dass Microsoft als einziger der großen Datenbankanbieter die Lizenzierung nicht an der Anzahl von Prozessorkernen ausrichtet, sondern an der Anzahl der tatsächlich vorhandenen Prozessoren. Beim Einsatz von vier Quad-Core-Prozessoren ist so nur eine Lizenzierung von vier Prozessoren notwendig.

Aufgebohrte Standard-Versionen

Neben den beiden neuen Editionen bietet SQL Server 2008 R2 aber auch für die Basis-Ausgaben Enterprise und Standard erweiterte Funktionalitäten. In der Enterprise-Edition können Sie mehrere Server zentral verwalten und bis zu 25 Instanzen einrichten, die über mehrere Server verteilt sein können. Die Master Data Services bieten dabei konsistente Daten über heterogene Systeme hinaus. Mit der Datenkomprimierung unterstützt die neue Version jetzt auch UCS-2-Unicode. In den Design-Tools für die Erzeugung von Business Intelligence-Lösungen helfen neue Assistenten dabei, Data Warehouses zu erstellen und weisen gleich zu Beginn auf eventuelle Performance-Probleme hin.

An gleicher Stelle unterbreiten die Assistenten Lösungsvorschläge, so dass auch weniger geübte Anwender leicht ans Ziel kommen. Microsoft hat dazu Best Practices in die Assistenten integriert und mit SQL Server 2008 R2 deutlich ausgebaut. Die Assistenten schlagen bereits bei der Erstellung eine optimale und leistungsoptimierte Struktur vor und warnen frühzeitig vor Leistungsproblemen, die auf einem fehlerhaften Design beruhen. Es erscheinen keine Popups, sondern lediglich blaue Wellenlinien beim Erstellen. Einzelne Warnungen wählen Sie pro Instanz oder global auf dem Server ab, wenn

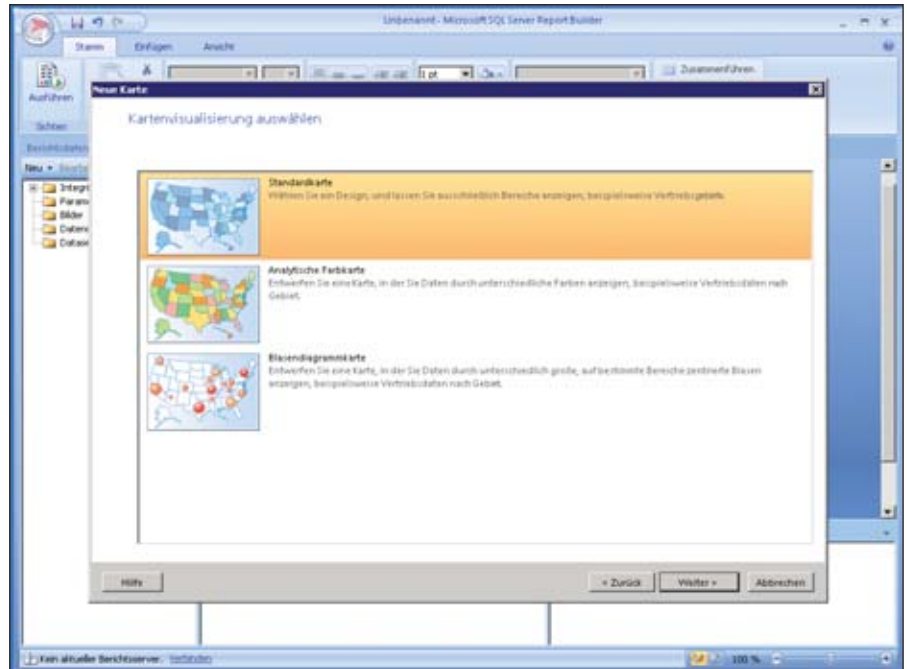


Bild 2: Auch geografischen Daten lassen sich nun übersichtlich in Berichten einbinden

zum Beispiel bestimmte Design-Richtlinien gewünscht sind, die den Best Practices widersprechen. Profis können bei der Erstellung von Cubes auf Wunsch auch arbeiten, ohne dass Assistenten durch Popups stören.

PowerPivot und verbesserte Berichte

Ebenfalls neu ist PowerPivot für SharePoint. Mitarbeiter in Fachabteilungen haben jetzt verbesserte Möglichkeiten, selbst professionelle Berichte mit dem Report Designer zu erstellen, ohne das Business Intelligence Development Studio verwenden zu müssen. Auf diesem Weg lassen sich Berichte im Word-Format erstellen. Mit PowerPivot können Unternehmen Self Service BI aufbauen, um Daten, die aktuell noch in Excel-Tabellen oder Access-Datenbanken gespeichert sind, anderen Anwendern im Unternehmen zur Verfügung zu stellen. Auf diese Weise können Unternehmen Daten, die aktuell von verschiedenen Mitarbeitern jeweils nur lokal gepflegt werden, in einer BI-Lösung leicht auch unternehmensweit zur Verfügung stellen.

Mit PowerPivot können Endbenutzer zum Beispiel mit Excel 2010 und SQL Server

2008 R2 sehr große Datenmengen einfach und schnell analysieren. Bei dieser Technik fassen Excel und SQL-Server Werte eines bestimmten Bereichs, die sehr nahe beieinander liegen, zu einem einzelnen Wert zusammen und beschleunigen dadurch die Verarbeitung der Daten. Mit PowerPivot können Sie ferner Feldsuchen basierend auf Namen, benannten Mengen und Beziehungen durchführen. Durch diese Funktion lassen sich PowerPivot-Anwendungen in SharePoint hosten und verwalten. Das Werkzeug steht als Add-in für Excel 2010 zum Download bereit, als Datenbank ist eine SQL Server 2008 R2 Enterprise-Lizenz vorgesehen. Mit der 64 Bit-Version von Excel 2010 lassen sich so leicht mehrere 100 Millionen Datensätze analysieren.

[1] Reporting Services-Add-In für SharePoint
<http://it-a.eu/aap11>

[2] TechNet-Workshop zur Verwendung der Reporting Services
<http://it-a.eu/aap12>

[3] SQL Server 2008 R2 Report Builder 3.0
<http://it-a.eu/aap13>

Links




Die Daten lassen sich anschließend in Excel-Datenblätter speichern und später weiter analysieren und aktualisieren.

Außerdem können Sie mit dieser Funktion auch Daten aus anderen Datenquellen, wie zum Beispiel Oracle oder Sybase importieren. Durch die Darstellung der aufbereiteten Daten in SharePoint lassen sich Dashboards auf Basis der Excel-Tabellen erzeugen. Für komplexere Aufgaben hilft die Data Analysis Expression Language (DAX). Diese baut auf der Syntax zur Erstellung von Formeln auf und unterstützt geübte Nutzer bei der Erstellung von Abfragen. DAX kann Analyseaufgaben in Excel durchführen, die auf dem Server so nicht vorhanden sind.

Schnellere Report-Erstellung

Eine weitere Neuerung in SQL Server 2008 R2 ist der neue Report Builder 3.0, den Sie unter [3] herunterladen können. Dieser verfügt über einen Server-Modus, der beim Erstellen von Berichten hilft. Nachträgliche Änderungen am Layout kann der Client so sehr schnell durchführen, da die Daten in einem Cache liegen. Berichte stellt SQL Server 2008 R2 mit der neuen Version wesentlich schneller dar, auch nach der Aktualisierung der Daten. Mit neuen Controls lassen sich Berichte zudem besser gestalten. Mit der Map Control in den Reporting Services können Sie zudem Landkarten und Geodaten in einer SQL-Datenbank speichern.

Mit den Reporting Services erstellte Berichte lassen sich in PowerPivot-Anwendungen integrieren. Datenfelder sind nicht einfach Listen, sondern die grafische Oberfläche stellt diese in Hierarchien grafisch dar. Daten integrieren Sie bequem per Drag&Drop in Berichte. Auch Gruppierungen von Daten erstellen Sie jetzt viel leichter. Berichte formatieren Sie direkt im Report Designer und zeigen diesen in einer Vorschau an. Einzelne Felder lassen sich nachträglich aufsplitten und Berichte anpassen. Es gibt statische und dynamische Felder, die Sie jederzeit ändern und erweitern können. Auch das nachträgliche Löschen ist möglich. Einzelne Felder im Bericht lassen sich nachträglich ein- und ausblenden.

Mit StreamInsight können Unternehmen Datenströme innerhalb einer fest definierten und garantierten Zeit verarbeiten. Dazu lassen sich verschiedene Antworten priorisieren. Mit einer SQL Server 2008 R2 Enterprise Lizenz dürfen Unternehmen bis zu vier virtuelle Server installieren. Die Enterprise-Edition unterstützt acht Prozessoren und bis zu 2 TByte Arbeitsspeicher. In der Standard-Edition sind durch Sicherungskomprimierung bis zu 60 Prozent kleinere Datenmengen und dadurch eine deutlich beschleunigte Sicherung möglich. Die Standard-Edition lässt sich außerdem als Verwaltungsinstanz in einer Multi-Server-Umgebung einsetzen. SQL Server 2008 R2 Standard Edition unterstützt 64 GByte Arbeitsspeicher und vier Prozessoren. Mit einer Standard-Lizenz von SQL Server 2008 R2 darf nur ein Server, physisch oder virtuell, installiert werden. (In) 

Kostenlos für
IT-Administrator-Abonnementen

iläNet

Workshop in München

Sicherheit für
Windows-Clients
am 16. November 2010

Die Agenda:

10.00 Uhr: Begrüßung

10.15 Uhr: Schwachstellen in Windows XP/7

- > Aktuelle Exploits in Windows
- > Motivation und Ziele der Malwareentwickler
- > Gegenmaßnahmen

Referent: Martin Dembrowski, entrada Kommunikations GmbH

11.30 Uhr – Partnernvortrag:

Unterschiede herkömmlicher IPsec-VPNs zu SSL-VPNs,
dargestellt an HOB RD VPN

Referent: Joachim Gietl, Vertriebsleiter Software Central Europe, HOB

ITANet Workshop-Partner:



12.15 Uhr: Pause

13.15 Uhr: Patchmanagement für Windows

- > Bedeutung des Patch Managements
- > Aufgeräumt mit Vorurteilen: Mythos Patch Management – Nichts geht mehr
- > Warum es ohne einen geeigneten Sicherheits-Updateprozess schwierig wird
- > Die Qual der Lösungs-Wahl

Referent: Thomas Gronenwald, adMERITia GmbH

14.30 Uhr: Pause

14.45 Uhr – Partnernvortrag:

Data Loss Prevention, Endpoint Security, Wirtschaftsspionage,
Datenschutznovelle – Anforderungen und Best Practice / Lösungen

Referent: Ramon Mörl, Geschäftsführer itWatch GmbH

ITANet Workshop-Partner:



15.30 Uhr: Härtung von Windows-Clients

- > Gute Gründe für das Hardening
- > Top 10 der ausgenutzten Schwachstellen und Funktionen
- > Methoden zur Härtung eines Clientsystems

Referent: Sascha Giebelhausen, adMERITia GmbH

17.00 Uhr: Ende der Veranstaltung

Termin: 16. November 2010

Ort: Experteach Training Center,
Wredestraße 11, 80335 München

Uhrzeit: 10.00 bis 17.00 Uhr

Teilnahmegebühren:

Für IT-Administrator-Abonnementen kostenlos.

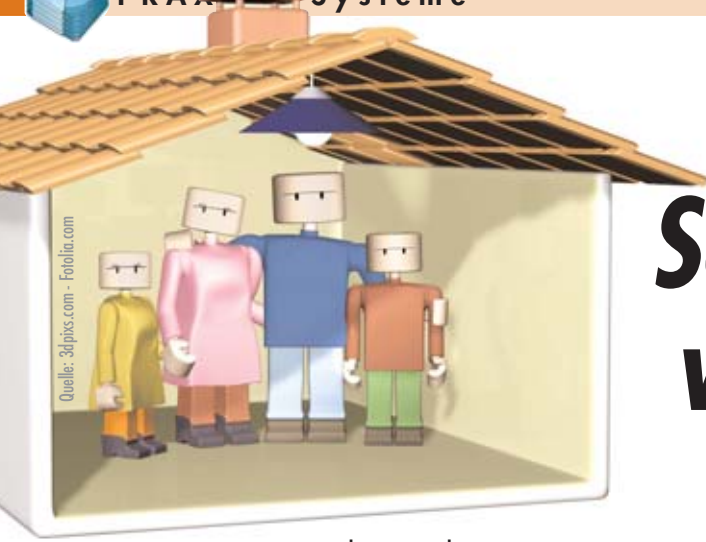
Anmeldeschluss: 10. November 2010

Trainings-Partner:



EXPERTeach

Mehr Infos und Anmeldeformulare unter
www.it-administrator.de/workshops/



Wahl des richtigen Storage für VMware Schmuckes Heim für virtuelle Maschinen

von Bertram Wöhrmann

Bei der Vorplanung zum Einsatz von Virtualisierungstechnologien sind viele Punkte zu beachten. In diesem Beitrag gehen wir darauf ein, mit welchen Storage-Technologien Sie beim Einsatz von VMware vSphere arbeiten können. Dabei ist stets zu bedenken, dass die zum Einsatz kommende Technologie immer stark von den Rahmenbedingungen des Projektes abhängig ist. Was im zentralen Rechenzentrum gute Dienste leistet, muss nicht zwangsläufig auch die passende Lösung für Außenstandorte sein.

Letzendlich landen alle Daten auf einer oder mehreren wie auch immer gearteten Festplatten. Unterschiedliche Plattentypen haben voneinander abweichende Datendurchsätze: Während eine Festplatte mit 10.000 Umdrehungen pro Minute auf einen Datendurchsatz von 120 MByte/s kommt, sind es bei einem mit 15.000 Umdrehungen arbeitenden Magnetspeicher schon 180 MByte. König in dieser Disziplin sind Solid State Drives (SSD), die maximale Datendurchsatzraten von bis zu 6.000 MByte/s erzielen.

Um ausreichend Platz auf den Plattenverbunden bereitzustellen, werden die Magnetspeicher auf unterschiedliche Art und Weise zusammengefasst. Das erfolgt durch RAID-Level. Außer der Zusammenfassung von Ressourcen lässt sich mittels eines RAID die Ausfallsicherheit erhöhen. Die Auswahl hat Auswirkungen auf die Schreib- und Leseschwindigkeit des Systems und ist somit auch für die Performance der einzelnen VM entscheidend. Wichtig sind zwei Faktoren: zum einen der Plattenplatz selbst und zum anderen die Anzahl der Festplattenspindeln. Letztere ist dann wichtig, wenn es um die Erhöhung des Durchsatzes geht.

Einsatz lokaler SAS-Platten

Die Tatsache, dass auf einer physikalischen Platte mehr als nur eine Datei einer virtuellen Festplatte liegt, führt dazu, dass eigentlich fast nur Random-Zugriffe erfolgen. Berücksichtigen Sie nun noch die unterschiedlichen Datendichten bei SAS- und SATA-Platten, wird schnell klar, dass ein Einsatz von lokalen SATA-Platten für virtuelle Maschinen keinen Sinn macht. Diese Platten sind eher für den sequenziellen Zugriff gebaut – die anderen Plattentypen sind beim Random-Zugriff einfach schneller.

Noch schneller als SAS-Festplatten sind Fibre Channel-Platten. Diese sind aber aufgrund der hohen Kosten für die Realisierung des Anschlusses selten in Servern zu finden. Sie sind allerdings im Storage-Sektor weit verbreitet. Die Zukunft gehört jedoch eindeutig der SSD. In diesem Festplattentyp sind keine mechanischen Teile mehr verbaut – die Daten werden auf sehr schnellen Speicherchips abgelegt. Dabei kommen entweder Flash-Speicher oder SDRAMs zum Einsatz. Diese Speichertypen unterscheiden sich in einigen Punkten (siehe Tabelle "Vergleich der SSD-Technologien"). Vergleichende Messwerte aus dem Praxiseinsatz finden Sie unter [1].

Ein Problem der SSD-Technologie ist derzeit noch der Preis und die Flüchtigkeit des Speichers.

Abschließend bleibt zu sagen, dass für den Fall der lokalen Nutzung einzig und allein SAS-Platten zu empfehlen sind. Wichtig sind dabei vor allem möglichst viel Cache und viele Spindeln, damit der Durchsatz stimmt und die VMs mit hoher Leistung laufen können.

So binden Sie externen Storage an

Bei der externen Storage-Anbindung sind zusätzliche Faktoren zu berücksichtigen. Zunächst ist es wichtig zu eruieren, mit welcher Anbindungstopologie gearbeitet werden soll. Auch wenn sich dahinter verschiedene technische Optionen verbergen, bleibt zunächst einmal nur die Wahl zwischen Block- und Datei-basiertem Zugriff. Dahinter verbirgt sich bei VMware die Möglichkeit, mit iSCSI, Fibre Channel oder per NFS auf den Datastore zuzugreifen. Bei dem Datastore handelt es sich um den Ablageort für die virtuellen Maschinen. Per Default legt das System für jede VM ein eigenes Unterverzeichnis an. Dort finden Sie alle Daten, die der VM zugehörig sind. Für die VM selbst ist es nicht



Vergleich der SSD-Technologien		
	SSD Flash	SSD SDRAM
Zugriffsgeschwindigkeit	gut	sehr gut
Datenflüchtigkeit	nicht flüchtig	flüchtig
Geschwindigkeit	mittel bis hoch	hoch
Preis	mittel bis hoch	sehr hoch

sichtbar, welche Art von Datastore ihr den Platz zur Verfügung stellt.

Halten Sie sich an Kompatibilitätslisten

Die unterschiedlichen Topologien verhalten sich auch unterschiedlich – siehe dazu die Tabelle “Protokolle für den Datastore-Zugriff im Vergleich”. Durch den Einsatz von 10 GBit-Netzwerken lässt sich die Geschwindigkeit bei den Zugriffsarten iSCSI und NFS noch erhöhen, auch im FC-Umfeld steigen dadurch aber die Durchsatzraten.

Bevor wir die nötigen Schritte beim Aufbau eines VM-Storage beschreiben, sei Ihnen ein Rat ans Herz gelegt: Berücksichtigen Sie die Hardware-Kompatibilitätsliste (HCL) von VMware und den Komponentenherstellern. Gehen Sie nie mit einer nicht freigegebenen Konfiguration an den Start, denn das kann eigentlich nur Probleme geben. Wichtig ist immer die Freigabe für den Servertyp, den Server-HBA, die FC-Switches und den Storage. Weiterhin müssen Sie die Firmware-Stände der einzelnen Elemente berücksichtigen.

Fibre Channel im Praxiseinsatz

Es existieren nur wenige Storage-Arrays mit Support, die sich per Fibre Channel direkt an den Server anschließen lassen. Die Standardkonfiguration ist auch hier die Switched Fabric. Es handelt sich dabei um eine Sternverkabelung der FC-Komponenten.

Durch den Aufbau von zwei Fabric's können Sie eine Redundanz erzeugen und haben die Option, die Wartung des Systems ohne Auszeiten vorzunehmen, wenn die Systeme redundant angebunden sind. Die Verkabelung erfolgt über Kreuz, damit Sie alle genannten Vorteile nutzen können. Dabei ist es kein Problem, ein SAN-Netzwerk mit unterschiedlichen Servergruppen zu nutzen. Im SAN werden sogenannte Zonen eingerichtet. Eine Zone beinhaltet alle Komponenten einer zusammengehörigen Landschaft, also die Server, die FC-Ports und die Storage-Processor-Ports des Storage.

Die Mitglieder einer Zone werden über ihre WWPN identifiziert. Die WWPN

(World Wide Port Number) ist eine eindeutige Gerätenummer von Fibre Channel-Komponenten. Bedenken Sie, dass Sie bei jedem Tausch einer Komponente auch das Zoning anpassen müssen, denn durch den Tausch ändert sich die WWPN. Zur Vereinfachung der Arbeiten lassen sich Gruppen definieren. Ein neuer VMware-Host wird dann der vorhandenen Gruppe hinzugefügt und erkennt damit sofort alle notwendigen FC-Geräte.

iSCSI beschleunigt vSphere

Das iSCSI-Netzwerk unterscheidet sich nur geringfügig von einem FC-Netzwerk. Auch hier können wir nur den Einsatz von dedizierten Switchen empfehlen, um den normalen Netzwerk-Traffic vom Storage-Datenverkehr zu trennen. Die Isolation der einzelnen Komponenten erfolgt durch VLANs, die Identifikation durch sogenannte iNAMEs. Dem Sicherheitsaspekt tragen Sie durch die Nutzung der CHAP-Authentifizierung Rechnung.

Lassen Sie sich durch die Verwendung von Standard-Netzwerkkomponenten nicht den Blick verschleiern – auch bei der Anbindung über iSCSI müssen die Komponenten in der HCL stehen. Es lohnt sich aber die Kompatibilität sicherzustellen: Im Vergleich zu ESX 3.5 hat sich der Datendurchsatz im iSCSI-Umfeld bei VMware vSphere um den Faktor 10 beschleunigt.

Protokolle für den Datastore-Zugriff im Vergleich			
	Fibre Channel	iSCSI	NFS
Durchsatz	Hoch (100%)	Mittel (92%)	Mittel (95%)
Latenz	Sehr niedrig	Mittel	Mittel
Redundanz	Einfach und gut.	Abhängig von der LAN-Struktur, aber gut realisierbar.	Ist möglich, die Konfiguration aber recht komplex.
Skalierbarkeit	Gut, das VMFS setzt aber Beschränkungen.	Mittel, das VMFS setzt aber Beschränkungen.	Sehr gut, keine VMFS-Limitierungen.
Komplexität	Hoch	Mittel	Niedrig
Management	Aufwändig	Mittel	Niedrig
Speicherverbrauch	Normal, mit Thin Provisioning niedriger.	Normal, mit Thin Provisioning niedriger.	Niedrig, Thin Provisioning per default.
Kosten	Hoch, Einführung neuer Technologie.	Nutzung ist mit kostenloser Software möglich.	Niedrig, Know-how ist meistens vorhanden.

Kaum Limits unter NFS

Der Aufbau der Netzinfrastruktur bei der Nutzung von NFS unterscheidet sich zum Einsatz von iSCSI nur unwesentlich. Auch hier ist eine Trennung vom eigentlichen Netzwerk für die Anbindung der VMs sehr empfehlenswert. Im Gegensatz zu FC und iSCSI erfolgt der Zugriff bei NFS auf den Storage jedoch nicht blockorientiert. Die VMs liegen also nicht auf einem VMFS-Datenspeicher. Das File-System der freigegebenen Netzwerkressource bleibt dabei der Hardware überlassen, die den Platz zur Verfügung stellt. Ein großer Vorteil der Storage-Anbindung über NFS liegt darin, dass es keine SCSI-Reservations gibt. SCSI-Reservations sind kurzzeitige Blockierungszustände, die bei bestimmten Aktionen in einem VMFS-Filesystem erfolgen.

Die Anzahl der VMs, die auf dem Speichermedium gehostet werden können, ist hier im Gegensatz zur blockorientierten Variante nicht begrenzt. Bei der blockbasierten Speicherung sollten Sie maximal acht bis zehn VMs pro LUN ablegen. Die Kommunikation erfolgt bei NFS mit dem DNS-Namen und Sicherheit gewährleisten Sie durch eine Authentifizierung am Storage. Wie auch bei der Nutzung von iSCSI sollten Sie über den Einsatz von Jumboframes nachdenken (MTU-Size 9.000). Zu berücksichtigen ist ferner, dass RAW-Device-Mappings nicht möglich sind und dass der Sicherheitsstandard nicht besonders hoch ist. Ein Vorteil ist aber das standardmäßig aktivierte Thin Provisioning. Durch die nicht vorhandene Beschränkung bei der Anzahl der VMs pro Storage bietet es sich besonders in VDI-Umgebungen an, auf NFS-Storage abzubilden.

Setzen Sie auf dedizierte Switches

Der Vollständigkeit halber möchten wir hier noch das Protokoll Fibre Channel over Ethernet (FCoE) auflisten. Bei FCoE wird der Netzwerk- und der Storage-Traffic über ein und dieselbe Ethernet-Verbindung geleitet. Das spart Kos-

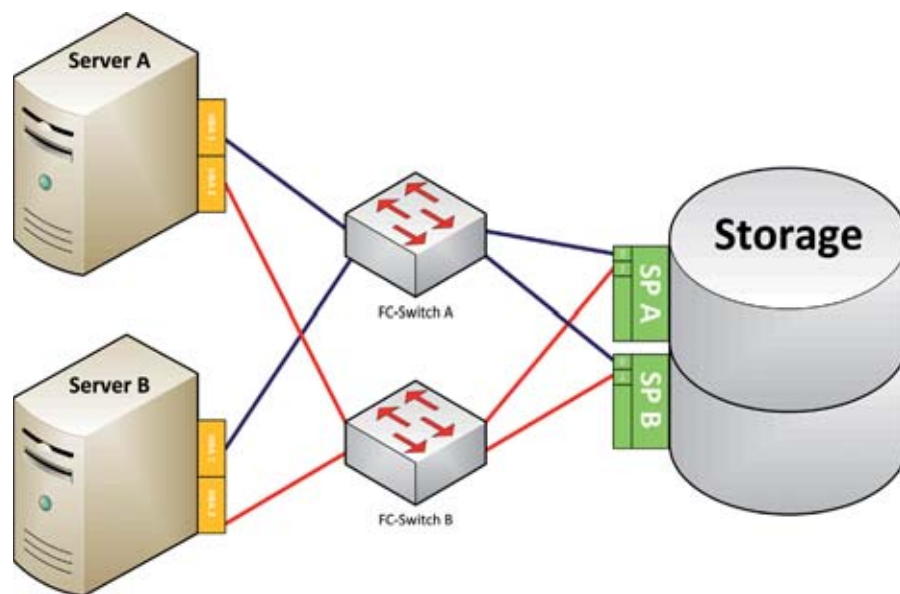


Bild 1: So sieht eine typische Fibre Channel-Umgebung aus

ten in vielerlei Hinsicht. Es gibt aber derzeit nur wenige Implementierungen dieser Technologie.

Letztendlich müssen Sie selbst entscheiden, mit welcher Technologie Sie arbeiten möchten. Seien Sie aber vorsichtig, was die Bewertung der Kosten angeht. Beim Einsatz von Fibre Channel heißt es immer, dass die Kosten durch die dedizierten Switches sehr hoch sind. Bedenken Sie aber, dass beim Einsatz von iSCSI beziehungsweise NFS auch dedizierte Switches zum Einsatz kommen sollten. Denn ein überprovisioniertes Netzwerk ist keine gute Basis für Storage-Zugriff über diese Protokolle.

Bevorzugen Sie Hardware-HBAs

Auf die physikalische Ebene reduziert, findet die Kommunikation über einen Hardware- oder Software-basierten Host-Bus-Adapter (HBA) im Server über das Netzwerk zum angeschlossenen Storage statt. Der Unterschied zwischen den HBA-Lösungen besteht darin, dass die Hardware-Variante die CPU des Servers nicht so stark belastet. Die HBAs besitzen eine eigene CPU, die das Paket-Handling für die Storage-Anbindung übernimmt. Im Gegensatz dazu erfolgt das Handling beim Software-iSCSI-Initiator zu Lasten der Server-CPU.

Durch die Tatsache, dass viele Serverhersteller sogenannte Multifunktionsadapter in den Systemen verbauen, benötigen Sie keine extra Karten mehr für den Zugriff auf den Storage und Sie können die Vorteile der Hardwarelösung nutzen. Über ein im Idealfall dediziertes Netzwerk erfolgt der Zugriff dann auf den Storage.

Am anderen Ende des Netzwerks für den Storage-Zugriff steht der externe Festplattenstapel. Er wird als Target bezeichnet. Dabei greift der einzelne Server nicht direkt auf die Festplatten zu, sondern er wird zu dem sogenannten Storage-Prozessor (SP) geleitet. Die Anzahl der Ports eines SPs kann durchaus variieren. Selbst wenn manche Hersteller andere Bezeichnungen für den SP haben, wie etwa Slammer oder Kopf, so ist die Funktion doch identisch. Sie können aber nicht nur Serversysteme an diese Ports anschließen, auch weitere Storage-Systeme lassen sich über diese Ports konnektieren. Der SP ist das Bindeglied für den Zugriff auf das Plattensubsystem. Er verwaltet sowohl den Zugriff auf die unterliegenden Plattensysteme als auch das Caching der Anfragen für eine Erhöhung der Schreib- und Lesezugriffe. Für die Zugriffsart auf den Storage sind die in diesem verbauten HBAs verantwortlich.



Klassenprimus Active/ Active-Pfadmanagement

Technisch gesehen gibt es drei Anbin-
dungsarten auf den Storage. Ist der Zu-
griff parallel auf allen Ports in voller
Geschwindigkeit möglich, liegt ein
Active/Active-Pfadmanagement vor.
Damit erreichen Sie einen hohen Daten-
durchsatz und Ausfallsicherheit der Pfa-
de. Zudem gibt es die Active/Passive-An-
bindung. Bei dieser Konfiguration können
die verschiedenen Storage-Prozessoren
nicht gleichzeitig auf eine RAID-Gruppe
zugreifen. Dabei ist der aktive SP der Be-
sitzer der RAID-Gruppe, der passive über-
nimmt den Job des aktiven bei dessen
Ausfall. Das Umschalten von einem ak-
tiven SP auf den passiven kann einige Se-
kunden in Anspruch nehmen. Deshalb
sollten Sie bei einer solchen Konfigura-
tion von einem automatischen Loadba-
lancing absehen.

Last but not least existiert die Zugriffs-
weise Active/Active Asymmetric bezie-

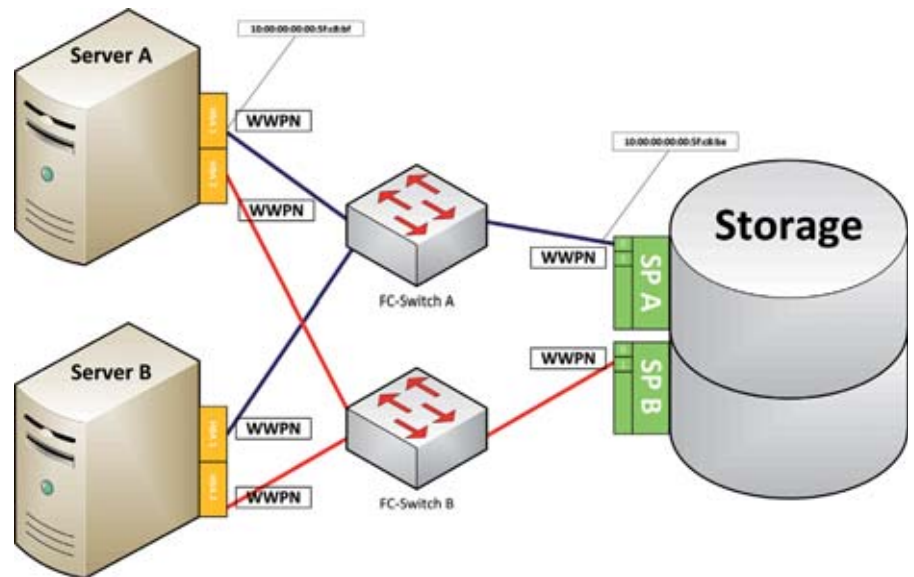


Bild 2: Das Zoning fasst in Fibre Channel-Umgebungen mittels WWPN mehrere Storage-Komponenten zusammen

ungsweise Pseudo Active/Active. Es
handelt sich dabei um eine Mischform
aus den beiden zuvor beschriebenen Va-
rianten. Zwar kann der Host parallel
über beide SPs auf die einzelne RAID-
Gruppe zugreifen, aber die Geschwin-

digkeit der Ports ist nicht identisch.
Auch hier gibt es nämlich einen Besit-
zer der RAID-Gruppe. Soll nun aber
über den zweiten SP Zugriff erfolgen,
geschieht dies über diesen zweiten SP
via den Owner-SPs auf die LUN. Dies

NETGEAR® FÜR KLEINERE UND MITTLERE UNTERNEHMEN

Die einfache Antwort auf Komplexität.

Infos und Katalog:
Tel. 089 45242-9400
vertrieb@netgear.com

NETGEAR® entwickelt passgenaue Lösungen für kleinere und mittlere Unternehmen – und bietet deshalb Enterprise-Class-Qualität mit erheblichen Kostenvorteilen. NETGEAR® ReadyNAS™ Netzwerkspeicher sind die perfekte Antwort auf immer größeres und komplexeres Datenaufkommen im Unternehmensnetzwerk. Bezahlbar, besonders einfach implementierbar, mit minimalem Administrationsaufwand und plattformübergreifend arbeitend.

www.netgear.de/readynas



NETGEAR®
Connect with Innovation™



ist sehr abträglich für die Zugriffsgeschwindigkeit. Achten Sie zudem darauf, dass verschiedene Hersteller Mischvarianten von Zugriffsmöglichkeiten anbieten. Schnell wird dann aus niederwertigeren Systemen eine Active/Active-Konfiguration.

Flaschenhalse vermeiden durch ein optimales RAID-System

Ein weiterer wichtiger Punkt ist die Leistungsfähigkeit der RAID-Systeme. Hier sind mehrere Faktoren ausschlaggebend. Zum einen die Anzahl der Backend-I/O-Operationen beim lesenden beziehungsweise schreibenden Zugriff und zum anderen die Geschwindigkeit der Festplatten. So benötigt RAID 5 im Backend vier I/Os für das Schreiben von Daten (Block lesen, Parität lesen, Block schreiben, Parität schreiben). Haben Sie nun ein RAID mit drei FC-Platten, dann ergibt sich eine Lesegeschwindigkeit von 450 I/Os (150 x 3) und eine schreibende Geschwindigkeit von 112,5 I/Os ($[150 \times 3] / 4$). Schnell ist etwas anderes. Befinden sich die Daten auf externem Storage, wird es noch schwieriger, die Zugriffsgeschwindigkeiten festzustellen. Durch verschiedene Beschleunigungsmaßnahmen der Hersteller wie etwa Caching erhalten Sie nur aussagekräftige Zahlen, wenn sie die Leistung des Gesamtsystems messen.

Die Festlegung, mit wie vielen Platten Sie eine RAID-Gruppe aufbauen wollen, ist nicht ganz so trivial, wie es auf den ersten Blick aussieht. Zu berücksichtigen sind die benötigte Kapazität und die Ausfallsicherheit. Die Berechnung der Parität eines RAIDs ist letztendlich auch von der Anzahl der beteiligten Platten abhängig. Je mehr Platten ein RAID enthält, desto länger dauert die Berechnung der Parität. Der Hersteller Ihrer Storage-Lösung kann Sie bei der richtigen Wahl der Konfiguration unterstützen, um die für Sie optimalen Einstellungen zu ermitteln.

Der Zusammenhang zwischen Kapazität und Geschwindigkeit wird gerne ver-

nachlässigt, spielt aber ebenfalls eine wichtige Rolle. Lassen Sie uns einmal einen Vergleich anführen mit der Situation, bevor Systeme virtualisiert worden sind, um an diesem Punkt Klarheit zu schaffen. Der Einfachheit vergleichen wir 50 Serversysteme. Gehen wir davon aus, dass in jedem Server zwei Festplatten à 72 GByte verbaut waren, ergibt sich eine Gesamtkapazität von 3,6 TByte netto bei der Nutzung von RAID 1. Die Leistungsfähigkeit beträgt dabei 15.000 IOPS bei SAS-Platten und 7.000 IOPS bei SATA-Platten.

Stellen Sie sich nun vor, dass ja nur 4 TByte Kapazität benötigt werden, dann könnten Sie die 50 ehemals physischen Systeme auf einem RAID 5 mit fünf Festplatten abbilden. Dass eine solche Umgebung nicht sehr leistungsfähig ist, springt sofort ins Auge. Somit wird deutlich, dass die Kapazität zwar wichtig, die Anzahl der IOPS aber wesentlich entscheidender für die Leistungsfähigkeit einer Storage-Lösung ist.

Auch bei der Wahl der LUN-Größe spielen derartige Überlegungen eine nicht unerhebliche Rolle. Zunächst sollten Sie wissen, wie es um die durchschnittliche Größe der VMs beschaffen ist und welchen Durchsatz der Storage benötigt. Sie sollten nie zu viele virtuelle Maschinen auf eine LUN legen – erinnern Sie sich an die maximale Anzahl pro VMFS-Datatore von acht bis zehn VMs.

Hersteller wollen mit Spezial-Features punkten


Verschiedene Hersteller versuchen, mit ganz speziellem Design das Maximale an Geschwindigkeit herauszuholen. Schauen wir uns beispielsweise die Firma 3PAR an. Deren Systeme haben eine automatische Lastverteilung über alle Controller und Ports. Die LUNs werden dabei über alle vorhandenen Festplatten verteilt. Ist der 3PAR-Storage mit 100 Festplatten ausgestattet und legen Sie dort eine LUN von 500 GByte an, dann befinden sich auf jeder Festplatte 5 GByte der LUN – un-

abhängig davon, welchen RAID-Level die einzelnen RAID-Gruppen haben.

Hitachi bietet ebenfalls sehr interessante Lösungen an. Neben einer Active/Active-Anbindung bietet der Hersteller die Option, sogenannte Mega-LUNs anzulegen. So können Sie LUNs erzeugen, die über RAID-Gruppengrenzen hinweg liegen können. Die LUN-Größe ist somit nicht durch die Größe der RAID-Gruppe limitiert. Dies bedeutet nicht nur mehr Platz, sondern auch bessere I/O-Durchsätze.

Fazit

Es gibt eine ganze Reihe von Storage-Herstellern und deren Produkte. Berücksichtigen Sie dabei stets die HCL und vergleichen Sie die unterschiedlichen Konfigurationen. Es findet sich für jeden Einsatzzweck das Richtige. Vergessen Sie aber nicht das Wachstum der Landschaft. Ist die Basis zu klein gewählt, wird eine Aufrüstung extrem teuer. Es kann sinnvoll sein, mit einer größeren Basis zu beginnen, wenn das Wachstum dies später fordern könnte. Auch bei der Anbindung der Platteneinheiten können Sie wie beschrieben unterschiedliche Wege gehen. Bachten Sie dabei die Isoliertheit der Storage-Anbindung und vermischen Sie keine Dinge, die nicht zusammengehören.

Abschließend können wir nur empfehlen, sich vor der Entscheidung für einen Anbieter immer Referenzen nennen zu lassen. Sprechen Sie mit den Personen, die solche Systeme bereits konfigurierten. Denn was nutzt etwa preiswertere Storage, wenn die Administration des Systems Unmengen von Zeit in Anspruch nimmt. In der Gesamtrechnung ist es dann doch teurer als manch andere Lösung. (ln) 

[1] Datendurchsatz von verschiedenen SSD-Produkten
<http://it-a.eu/aap71>

Links





Datenwiederherstellung im Notfall Wider dem Datenverlust

von Thomas Bär

Kaum etwas dürfte für Administratoren unangenehmer sein als verloren gegangene Daten. Ausgefallene Serverkomponenten können Daten mit sich reißen, gelöschte Dateien und Ordner belasten den IT-Support. Was Sie unternehmen können, wenn Datenträger verloren scheinen, und mit welchen technischen Möglichkeiten sich das Unheil am besten abwehren lässt, zeigt dieser Beitrag.

Die einfachste und glücklicherweise häufigste Form des Datenverlusts betrifft einen einzelnen Benutzer. Ursache ist in den seltensten Fällen ein technisches Problem. Häufig sind es Anwenderfehler, in deren Folge einzelne Dateien oder Ordner nicht mehr an ihrem ursprünglichen Ort zu finden sind. Das Löschen von Dateien auf einem Netzlaufwerk in Windows befördert diese nicht, wie vom lokalen PC gewohnt, in den Papierkorb. Die betreffenden Dateien werden sofort gelöscht und lassen sich aus Sicht des Benutzers nicht mehr zurückholen. Ebenfalls ein in der Praxis sehr häufig auftretendes Problem ist nicht das Löschen von Ordnern und Dateien, sondern deren irrtümliches Verschieben in eine andere Ordnerstruktur. Da die gewünschten Elemente nicht mehr am ursprünglichen Speicherort zu entdecken sind, geht der Benutzer von einem Löschvorgang aus – den er nicht durchgeführt hat. Handelt es sich dabei um Benutzer der Kategorie “einfach alles mit Winword öffnen”, so sind deren Möglichkeiten zur Problemlösung in der Tat so begrenzt, dass nur ein findiger Kollege oder der IT-Support behilflich sein kann.

Anwenderschulung vermeidet Datenverluste

Der wichtigste Problemlösungsansatz in diesem Fall ist das Vermitteln der entsprechenden Kenntnisse bei der Verwendung von Windows. Was für den IT-Professional vollkommen einleuchtend ist, beispielsweise die Hierarchie von Dateien und Ordnern im Filesystem, ist für viele Anwender kaum nachvollziehbar. Die Fähigkeit, sich mit Web 2.0 und E-Mail gut auszukennen, überschattet bei vielen Mitarbeitern die Basiskenntnisse über die Funktionsweise des Computers und Betriebssystems. Die zunehmende Abstraktion durch “Eigene Dateien” und “Dateibibliotheken” mag der Produktivität der Anwender dienlich sein, vermindert aber das Gefühl dafür, wo sich die Informationen tatsächlich befinden.

Neben dieser Vermittlung von Kenntnissen sind die “Vorherigen Versionen” in Microsoft Windows das geeignete Mittel, um tatsächlich verlorene Dateien schnell wiederherzustellen oder sich als IT-Support-Mitarbeiter zumindest ein Bild davon zu machen, wie die Ordnerstruktur eigentlich hätte aussehen sollen. Dank der Tatsache, dass Microsoft die Variante der Volumenschattenkopien mit Windows Vis-

ta und Windows 7 auch auf den Client-Betriebssystemen anbietet, kann in der nächsten Zeit davon ausgegangen werden, dass sich das Wissen um die Verwendung der Funktion auch ohne aktives Benutzertraining verbreitet. Windows Server sind schon seit Version 2003 dazu in der Lage, Volumenschattenkopien (VSS) zu erzeugen und mehrere Zeitpunkte als “kleine Sicherung” vorzuhalten.

Die Begrifflichkeit “Versionen” ist in diesem Zusammenhang von Microsoft allerdings etwas unglücklich gewählt. Microsoft SharePoint beispielsweise versteht unter einer Version jeden Speicherzeitpunkt des Dokuments. Ähnlich verhält sich ein Urvater dieser Technik: Novell Salvage Files. Bei Novell wurde jede gelöschte Datei solange vorgehalten, bis der Speicherplatz auf dem Volume tatsächlich benötigt wurde. Office-Programme legen beim Öffnen einer Datei eine neue Datei an und benennen die ursprüngliche Version um. Die Kombination aus dem Verhalten des Umbenennens und der Methode des Löschens von Novell sorgte dafür, dass eine nicht exakt definierbare Zeit lang die Möglichkeit bestand, faktisch jede Version eines Dokuments wiederherzustellen.



Die Versionierung in Microsoft Windows arbeitet anders. Es wird zu einem exakten Zeitpunkt eine gedachte Kopie der Dateien, ein so genannter "Snapshot", erstellt. Dieser Snapshot wird über den Scheduler automatisch zu vom Administrator vorgegebenen Zeitpunkten wiederholt. Der Vorteil des Snapshots liegt in seinem universellen Einsatzgebiet. Ob Programme Dateien einfach überschreiben oder umbenennen, spielt dabei keine Rolle. VSS arbeitet so mit allen Programmen zusammen. Die Funktion auf Seiten des Desktop-Computers ist nicht auf aktuellere Windows-Versionen beschränkt. Windows XP und höher besitzt von Haus aus die entsprechenden Komponenten, um "Vorherige Versionen" auf einem Windows-Server anzuzeigen. Für Windows 98, 98SE und Windows 2000 ist hierfür der "Shadow Copy Client", den Microsoft kostenlos im Internet anbietet, erforderlich. Für Windows 95, ME und NT4 ist eine Nutzung indes unmöglich.

Schnappschuss zur richtigen Zeit

Schattenkopien erlauben es Administratoren und Benutzern sehr einfach und ohne zusätzliche Kosten, auf frühere Varianten von Dateien und Ordnern zugreifen zu können. Die Schattenkopie bietet aber nicht nur die Möglichkeit, eine frühere Version wiederherzustellen, in vielen Fällen wird auch der Rückgriff auf die Datensicherung unnötig. Das funktioniert jedoch nur dann, sofern die VSS von Windows ordentlich und bedacht geplant wurden. Die Mischung aus zwei verschiedenen Zeitplänen ist für den Unternehmenseinsatz besonders effektiv: "Mehrfach am Tag" und "Mehrere Tage".

Typischerweise werden Serversysteme in der Nacht gesichert, da in dieser Zeit die Belastung der Server durch Benutzeraktionen am geringsten ist. Dies bedeutet, dass eine Datei, die am Tag verändert oder gelöscht wird, möglicherweise überhaupt nicht wiederhergestellt werden kann. Durch tägliche Schattenkopien am Vormittag, Mit-

tag, frühen Nachmittag und späten Nachmittag lässt sich dieses lange Zeitfenster durch VSS-Zwischenkopien verkürzen. Möglicherweise ist es für das Unternehmen auch interessant, über mehrere Tage Schattenkopien zu erstellen, um so möglichst viele Kopien vorhalten zu können. Da Festplattenspeicher im Vergleich zum Bandspeicher günstig ist, sind die Kosten für dieses Vorgehen überschaubar, auch wenn viele Schattenkopien erstellt werden sollen. Zwar ist Windows in der Lage, bis zu 512 Snapshots pro Volume zu verwalten, jedoch können über

die Funktion "Vorherige Versionen" auf maximal 64 Snapshots zugegriffen werden.

Die Frage nach dem Platzbedarf von Schattenkopien lässt sich nicht einfach in der Angabe von MByte oder GByte beantworten. Wird eine Datei auf einem Volume mit VSS gelöscht, so wird lediglich der Verzeichniseintrag verändert, was kaum Speicherplatz erfordert. Ändert sich eine Datei, so wird eine neue Datei in einem freien Speicherbereich abgelegt und ein neuer Verweis im Verzeichnis erstellt. Für Volumenschattenkopien lässt sich eine Obergrenze pro Volume festlegen. Bei Überschreiten des reservierten Speicherplatzes beginnt VSS, die jeweils ältesten Dateien zu löschen. Dabei verschlechtern die VSS zwar im geringen Maße die Schreibleistungen auf Festplatten. Die Vorteile des Verfahrens wiegen die Nachteile jedoch um ein Vielfaches auf. Neben der richtigen Einstellung auf Serverseite beziehungsweise auf aktuellen Windows-Client-Computern sind die Benutzer im Unternehmen auf diese Technik hin zu informieren. Kaum jemand kommt von allein auf die Idee, mit der rechten Maustaste das Kontextmenü eines Ordners oder Netzlaufwerks zu öffnen und in den Eigenschaften nach "Vorherigen Versionen" zu suchen. Eine kurze Erklärung per E-Mail entlastet den IT-Support.

Wirklich sicher nur mit Backup

Es versteht sich von selbst, sei aber dennoch erwähnt: Volumenschattenkopien sind kein Ersatz für die Sicherung auf externe Medien, wie beispielsweise Bandlaufwerke. VSS funktionieren nämlich nur, solange das Betriebssystem und die Festplatten des Servers einwandfrei arbeiten und deckt somit in erster Linie "Benutzungsfehler" der Anwender ab. Es gibt eine schier unüberschaubare Anzahl von guten Backup-Programmen am Markt und eine nicht minder unübersichtliche Anzahl von guten und sehr guten Bandlaufwerken. Bandlaufwerke oder sonstige Wechseldatenträger für die Massenspeicherung sind in der Backup-Konzeption unersetzlich. Jedoch haben sie auch Nachteile: Bandlaufwerke und deren Medien sind üblicherweise teuer, sofern

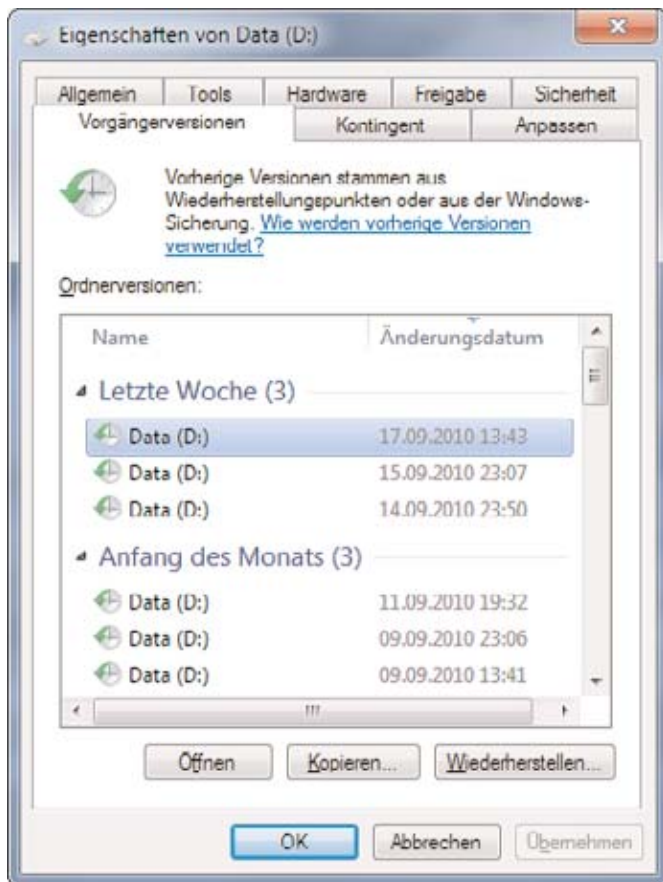


Bild 1: Die einfachste Form der Datenwiederherstellung ist die Verwendung der "Vorherigen Versionen" in Windows



sie eine gute Performance bieten sollen. Die Wiederherstellungszeit einer Applikation oder Servers von einem Bandlaufwerk kann mitunter Stunden dauern, was in vielen Anwendungsfällen inakzeptabel ist.

Für Applikationen im Microsoft-Umfeld bietet das Unternehmen aus Redmond seit einigen Jahren eine Kombinationslösung aus Backupsoftware und professionellem VSS-System an. Geschäftsanwendungen wie Microsoft SQL Server, Exchange oder SharePoint lassen sich mit "System Center Data Protection Manager" (DPM) 2007 und höher möglicherweise effektiver sichern als mit Produkten der Marktbegleiter. DPM ist ein Teil der Microsoft System Center-Produktfamilie zur professionellen Verwaltung der Windows Server-Infrastruktur und geht weit über die Fähigkeit der Windows-Sicherung und -Wiederherstellungen hinaus. Zwar bietet jedes Windows-Betriebssystem eine eigene Backup-Lösung, NT-Backup oder die "Windows Sicherung", doch handelt es sich bei diesen Programmen um einfachere Basisprogramme, die zwar ihre Aufgabe befriedigend erledigen, jedoch ohne jeglichen Komfort. Doch selbst das "alte" NT-Backup verwendet im Hintergrund Schattenkopien, um das Problem der geöffneten Dateien oder der noch nicht abgeschlossenen Transaktionen bei Datenbanken zu umgehen.

DPM ermöglicht zudem eine permanente Sicherung der Daten von Microsoft-Anwendungen und -Dateiservern. Es verbindet die permanente Datensicherung (Continuous Data Protection, CDP) mit der traditionellen Bandsicherung. DPM sichert in erster Linie die wichtigsten Microsoft-Serverprodukte, wie Exchange, SQL Server, SharePoint und Windows-Dateidienste, fortwährend auf einen dafür eingerichteten DPM-Server. Über diesen stehen dann eine festplattenbasierte Wiederherstellung und eine Langzeitsicherung auf Bandlaufwerken zur Verfügung.

Virtualisierung, DFS und RAID

Serversysteme werden in der klassischen Ausprägung mit mindestens zwei Festplatten

im RAID 1-Modus betrieben. Somit kann eine Festplatte ausfallen, ohne dass der Server seinen Betrieb einstellt. Über lautstarke Warntöne, SNMP-Nachrichten und Einträge in der Ereignisanzeige macht der RAID-Adapter einen möglichen Missstand deutlich. Leuchtet dann noch die betroffene Festplatte mit einer roten LED am Chassis, so wird der Festplattentausch am Server zu einem Kinderspiel.

Erfahrene Administratoren wissen, dass die Wiederherstellung eines RAID-Verbunds – auch bei RAID 1 – mitunter sehr viel Leistung des Servers in Anspruch nimmt. In der Hauptbetriebszeit empfiehlt sich der Start eines "RAID-Rebuilds" kaum. Preisgünstigere RAID-Adapter fallen während der Wiederherstellungsphase des Festplattenverbunds üblicherweise durch eine besonders hohe Systemlast auf. Da macht das Software-RAID von Windows keine Ausnahme. Fällt ein Volume aus, so sorgt der Rebuild des Array für eine recht hohe Auslastung der CPU. Insgesamt bietet sich das Software-RAID von Windows nur für wenige Einsatzgebiete an, beispielsweise um die Datenpartition auf zwei Festplatten im Mirror-Betrieb abzulegen. Die Platten lassen sich übrigens in einem anderen Computer problemlos einhängen – auch ohne dass sie weiterhin als RAID-Member betrachtet werden. Leider bietet Windows nicht die direkte Möglichkeit, ein externes Laufwerk, beispielsweise eine externe

USB-Festplatte, als Teil eines RAID-Verbunds zu akzeptieren.

Virtuelle Maschinen sind in Ausfallsszenarien deutlich einfacher zu handhaben als physikalische Server. Lassen sich VMs doch sehr leicht transportieren, kopieren und auf anderen Host-Systemen starten. Natürlich hängt auch eine virtuelle Maschine davon ab, dass die Technik im Host-System funktioniert, doch die Unabhängigkeit von virtueller und physikalischer Hardware machen den Weiterbetrieb auf einer anderen Maschine möglich, ohne dass mit größeren Schwierigkeiten zu rechnen ist. Eine weitere Möglichkeit, sich größeren Ärger zu sparen, ist die Verwendung des "Distributed File Systems" (DFS), anstelle auf Freigaben auf Maschinennamen zu setzen. Ändert sich der Maschinename, so ist es erforderlich, Client-Computern einen veränderten Freigabennamen mitzuteilen. Wird die komplette Dateifreigabe über DFS abgewickelt, können sich die Servernamen problemlos ändern, da Client-Computer auf die "logischen Freigabennamen" zugreifen. Ein defekter Fileserver kann durch DFS viel einfacher durch ein Ersatzgerät ausgetauscht werden.

Defekte Festplatten zum Spezialisten

Gibt eine Festplatte nur noch seltsame Klack-Geräusche von sich, ohne dass ein RAID-Adapter den Austausch im laufen-

SEMINARMARKT

**Den IT-Administrator
Seminarmarkt
mit News zu IT-Trainings
finden Sie auch online auf:**

www.it-administrator.de/seminarmarkt

Log.in
consultants

**Von Profis entwickelte
High-Level-Trainings!**

- ✓ Server-Based Computing
- ✓ Virtualisierung
- ✓ Softwaremanagement
- ✓ Herstellerunabhängig
- ✓ Praxisorientiert

Jetzt buchen!

www.loginconsultants.de

den Betrieb ermöglicht, oder wird die Platte gar vom Betriebssystem überhaupt nicht mehr erkannt, so ist der Wirkungsbereich der IT-Mitarbeiter bereits überschritten. Mechanische Schäden erfordern eine Reparatur in einem staubfreien Reinraum. Alle weiteren Versuche, die Daten der Festplatten selbst auszulesen, bergen die Gefahr, dass zusätzliche Schäden auf dem Datenträger entstehen. Verschiedene Dienstleister und Speziallabore bieten bei der Datenwiederherstellung von defekten Datenträgern ihre Hilfe an. Mit Kosten von über 1.000 Euro pro Datenträger kann gerechnet werden – ohne die Gewissheit, ob wirklich alle Daten zu retten sind. Knapp über achtzig Prozent aller Datenschieden, die zu einem auf Datenwiederherstellung spezialisierten Labor eingeschickt werden, betreffen Festplatten. Dabei können die Schäden sehr unterschiedliche Ursachen haben. Neben dem allgemeinen Verlust der magnetischen Eigenschaften mit der Zeit sind vor allem mechanische und elektrische Defekte zu nennen. Üblicherweise sorgt der Bernoulli-Effekt für ein Schweben der Köpfe über der sich drehenden Platte. Bei einem Headcrash fehlt dieser Effekt und die Beschichtung der Trägerplatte wird unwiderruflich beschädigt oder zerstört. Schäden dieser Art machen eine komplette Wiederherstellung einer Festplatte in der Regel unmöglich, denn wo keine datentragende Beschichtung mehr vorhanden ist, da können auch keine Daten mehr ausgelesen werden. Häufig lassen sich aus den noch verbleibenden intakten Beschichtungsbereichen Datenbestände wiederherstellen.

Ein für die Festplatte besonders fataler Defekt ist der Ausfall der 12 Volt-Stromversorgung, die für den Betrieb des Spindelmotors mit den Datenscheiben benötigt wird. Fällt die Spannung aus, bewegen sich die Lese/Schreib-Köpfe automatisch in die vorgesehene Parkposition. Bewegt sich das so genannte Head Assy unkontrolliert in die Ruheposition, kann bei gleichzeitig anliegender Schreibspannung auf den Köpfen eine spiralförmige Spur magnetisiert werden. Die Zerstörung der Daten ist dann

ebenfalls sehr nachhaltig. Bei Defekten an den Lagern kann sich der Plattenturm verklemmen und die Platte “frisst” sich wörtlich fest. Kommt es zu einer Bewegungshemmung des Head Arm Assy, also der Kopfvorrichtung, kann diese nicht mehr richtig positioniert werden und die Festplatte wird nicht mehr vom System erkannt. Besonders in der warmen Jahreszeit treten immer wieder Anlaufstörungen auf, die darin begründet liegen, dass die Schreib-/Leseköpfe an der Datenoberfläche “festkleben” – eine so genannte Stiktion. Dies ist Folge einer chemischen Veränderung in der Beschichtung der Datenoberflächen durch übermäßige Wärmeeinwirkung.


Daten von einer Festplatte eines durch einen Brandschaden verschmolzenen PCs zu retten ist sicherlich werbewirksam. Doch bei einem Brandschaden sind vor allem die zeitliche Dauer der Hitzeentwicklung und die Höhe der Temperatur von Bedeutung. Das Plastik-Chassis des Rechners schmilzt bereits bei geringen Temperaturen und verwandelt den PC in ein schwarz-verkohlt Wrack. Erst wenn die Hitze so hoch wird, dass sich Metall zu verformen beginnt, wird das Innenleben einer Festplatte nachhaltig zerstört. Oft ist erst die Arbeit der Feuerwehr für die Datenträger das Todesurteil. Keine Festplatte ist zu 100 Prozent luftdicht verschlossen – durch die Druckausgleichlöcher kann beim Löschen Wasser in das Innenleben der Festplatte eindringen, neben gasförmigen Belastungen, die bei einer Brandlöschung entstehen.

Alles, was sich innerhalb einer Festplatte befindet, ist für das Einwirken von Wasser besonders empfindlich. Neben Rost kann sich sogar Schimmel bilden, der die magnetische Beschichtung auflösen vermag. Wird eine mit Flüssigkeit gefüllte Festplatte auf Betriebsumdrehung gebracht, ist eine erfolgreiche Wiederherstellung von Daten immer unwahrscheinlicher. Kommt es zu einem Brandschaden mit Löschwassereinwirkung, sollten die Datenträger innerhalb kürzester Zeit zu einem professionellen Datenretter gebracht werden. Neben der eigentlichen

Sanierung ist eine intensive Prüfung der Datenträger durch Profis erforderlich, die feststellen können, was wirklich bis in den Innenraum der Festplatte durchgedrungen ist. Wenn sich herausstellt, dass eine Festplatte überhaupt als wiederherstellbar gilt, so lassen sich in aller Regel über neunzig Prozent der Daten zurückholen.

Kompressionsverfahren und Verschlüsselungsmethoden sind im Falle eines Datenträgerausfalls ein extrem großes Hindernis. Der Verlust eines Datenbereichs wirkt sich durch fehlende Informationen innerhalb der Dateien aus. Da bei beiden Verfahren die Konsistenz von Daten von entscheidender Bedeutung ist, wird die Dechiffrierung komplizierter oder unmöglich. Auch der Ausfall einer zweiten Platte innerhalb eines RAID 5-Verbunds ist ein Szenario, das eintreten kann. Dann hilft es nicht mehr, ein oder zwei Hot-Spare-Platten einzusetzen – das System kann sich bei Versagen von mehr als einer Festplatte in der Regel nicht mehr selbst regenerieren. In diesem Fall ist die Wiederherstellung einer Festplatte außerhalb des Verbunds zweckvoll. Sobald eine der ausgefallenen Platten wiederhergestellt wurde, kann der RAID-Adapter mit dem Rebuild des Verbunds fortfahren.

Fazit

Grundsätzlich sollte das Motto lauten: sichern, sichern und noch mal sichern. Bei der Datensicherung jedoch ist es mit dem Wegklicken der Meldung “Alles fehlerfrei gesichert” nicht getan. Der komplette Sicherungsbericht muss von der IT-Abteilung geprüft werden, da auch in der Zusammenfassung nicht gesicherte Dateien oft nicht genannt werden. Das Einschalten der Prüffunktion des Bandlaufwerks sollte eine Selbstverständlichkeit sein, auch wenn das den gesamten Sicherungslauf verlängert. Auch ein leistungsfähiges SAN mit doppeltem Redundanzkopf kann schließlich einmal in eine Fehlersituation kommen – dann nämlich, wenn eine Festplatte nicht einfach ausfällt, sondern fehlerhafte Daten an den Controller zurückgibt. (dr) 



TByte-SAN im Eigenbau realisieren

Unser neues Datenhäusle

von Dr. Michael Schwartzkopff



Viele Administratoren kennen das Problem "Plattenplatz" aus eigener, leidvoller Erfahrung: Die Anwender und Applikationen können nie genug bekommen. Zwar sinkt der Preis pro GByte kontinuierlich; im selben Maße wachsen aber auch die Ansprüche, so dass unter dem Strich der Speicherbedarf immer eine kostspielige Angelegenheit bleibt. Dies umso mehr, da mit steigendem Volumen die Ansprüche an die Zuverlässigkeit und damit an die Verwaltung wachsen. Was liegt da näher, als den Bedarf in einem Storage Area Network mit zentraler Administration zu bündeln. Mit ein wenig Hintergrundwissen ist es ein Leichtes, ein solches SAN kostengünstig im Eigenbau zu realisieren. In diesem Workshop bauen wir ein SAN auf, das neben hoher Kapazität und Zuverlässigkeit auch eine hohe Verfügbarkeit bei Ausfall einer Komponente bietet.

Unsere Workshop konstruiert ein SAN, das seine Daten per iSCSI zur Verfügung stellt. Dieses Protokoll hat den Vorteil, den Clients die Daten in Form eines Block-Gerätes zur Verfügung zu stellen und somit alle möglichen Dateisysteme zuzulassen. Ob der Server, der sich gerade den Plattenplatz importiert, diesen mit NTFS (Windows), ext3 (Linux) oder ZFS (Solaris) formatiert, ist aus Sicht des SAN egal. Es stellt seine Daten allen Betriebssystemen zur Verfügung.

Da der Ausfall einer einzelnen Komponente nicht den Ausfall des gesamten SAN bedeuten darf, sollten alle Einzelteile redundant vorhanden sein. Die Daten werden über die Festplatten zweier Server repliziert und eine Clustersoftware sorgt für einen reibungslosen Betrieb auch im Fehlerfall. Der Standby-Server übernimmt die Aufgaben des aktiven Systems, wenn dieses ein Problem hat. Da die Daten auf die Festplatten beider Systeme repliziert werden, funktioniert der Übergang auch ohne Datenverlust.

Die Säulen des SAN

Das Grundsystem soll aus zwei leistungsfähigen Servern bestehen. Unser Haupt-

augenmerk liegt natürlich auf dem Festplattensystem: SATA-Festplatten haben das günstigere Preis/Leistungsverhältnis und sind aktuell in Größen bis zu 2 TByte erhältlich; SAS-Festplatten sind teurer, bieten dafür aber wesentlich höhere Schreib- und Lesegeschwindigkeiten sowie Zuverlässigkeit. Je nach Applikation sollten Sie die passenden Festplatten aussuchen. Wichtig ist, dass Sie lokal ein RAID-System aufbauen, da Sie sich so später viel Ärger beim Ausfall einer einzelnen Platte ersparen. Ein zusätzlicher, batteriegepufferter Cache auf dem Controller beschleunigt den Datendurchsatz noch einmal.

Als Betriebssystem kommt für unser Projekt nur Linux in Frage, da alle Komponenten bei den gängigen Distributionen enthalten sind und deshalb keine Probleme bei der Integration zu erwarten sind. Im Folgenden zeigen wir den Aufbau anhand von Ubuntu 10.04.

Es ist eine kluge Entscheidung, das Betriebssystem auf einem separaten RAID 1-Verbund aufzusetzen und einen weiteren für die Daten einzurichten. Dieser kann RAID 5 sein, da der vorhandene

Plattenplatz so besser ausgenutzt wird. Das DRBD (siehe unten) sorgt für eine zusätzliche Redundanz.

Synchronisation der Daten einrichten

Da ein Rechner die Daten ausliefert und der andere für den Notfall bereitsteht, müssen alle Daten vom aktiven Rechner auf den passiven synchronisiert werden. Das Betriebssystem stellt hierfür sogenannte Distributed Redundant Block Devices (DRBDs) zur Verfügung. Dieser Gerätetreiber sorgt dafür, dass auf Geräteebene alle Blöcke, die auf den aktiven Knoten geschrieben werden, sofort auf die Festplatte des passiven Knotens repliziert werden. Das Dateisystem erhält die Rückmeldung "Ich habe geschrieben" erst dann, wenn der Block auf beiden Festplatten beziehungsweise im Cache der Controller angekommen ist. So ist dafür gesorgt, dass der passive Knoten auch im Fehlerfall ohne Datenverlust weiterarbeitet. Ab Version 8 können Sie DRBD auch im Aktiv/Aktiv-Modus betreiben, in dem auf beide Spiegelhälften geschrieben werden kann. Aber für unser SAN brauchen wir nur den einfachen

Modus (Aktiv/Passiv), da ja nur ein Server die Daten ausliefern soll.

In den meisten Distributionen ist das Kernelmodul für DRBD schon eingebaut. Ab Version 2.6.35 ist DRBD auch fester Bestandteil des Kernels, so dass Probleme beim Kernelupdate in Zukunft gänzlich entfallen. Bei Ubuntu findet sich die Software im Paket *drbd8-utils*. Die Konfiguration der DRBD erfolgt über die Datei */etc/drbd.conf* und wir halten – der Übersichtlichkeit halber – alle Dateien im Verzeichnis */etc/drbd.d*. In der dortigen globalen Konfiguration legen Sie Parameter fest, die für alle DRBD gelten. Eine Konfiguration von “r0” als */dev/drbd0* in *r0.res* sieht in der Kurzform (möglich ab Version 8.2.1) so aus:

```
resource r0 {
    device    /dev/drbd1;
    disk      /dev/sdb;
    meta-disk internal;
    on node1 {
        address 172.29.56.1:7789;
    }
    on node2 {
        address 172.29.56.2:7789;
    }
}
```

Die sehr ausführlichen Kommentare in der Konfigurationsdatei beantworten alle Fragen bezüglich der Einstellungen. Der erste Start der DRBD ist unter [1] dokumentiert.

Auf beiden Rechnern richten Sie die Metadaten von DRBD auf der physikalischen Platte ein:

```
# drbdadm create-md r0
```

und starten die DRBD auf beiden Rechnern gleichzeitig:

```
# drbdadm up r0
```

Jetzt müssen Sie nur noch einen Rechner auswählen, die Partition dort zum Master machen und per Synchronisation der Daten auf den anderen Rechner übertragen. Danach ist das DRBD einsatzbereit:

```
# drbdadm -- --overwrite-data-of-peer primary r0
```

Das iSCSI-Target und den Cluster einrichten

Der nächste Schritt ist, die einzelnen Partitionen per iSCSI freizugeben. Zuerst installieren wir die notwendige Software mit dem Paket *iscsitarget*. Der *ietd*-Daemon startet den Dienst im Hintergrund. Die Konfiguration erfolgt über die Datei */etc/iet.conf*, in der alle Informationen über verfügbare physikalische Partitionen und Freigaben hinterlegt sind. Die Clustersoftware kann diese Informationen allerdings selbstständig verwalten, so dass hier keine weitere Konfiguration notwendig ist.

Natürlich soll der Aufbau bei Versagen einer einzelnen Komponente weiterhin seinen Dienst verrichten. Deshalb muss eine Clustersoftware die Verwaltung der Ressourcen übernehmen. In den letzten zwei Jahren hat sich eine Kombination aus *corosync* für die Kommunikation im Cluster und *pacemaker* [2] als Cluster Resource Manager als zukunftsweisende Kombination herauskristallisiert. Bei Ubuntu ist die notwendige Software schon integriert, so dass ein

```
# apt-get install pacemaker
```

für die richtige Installation sorgt.

Die Konfiguration der Kommunikation im Cluster erfolgt in */etc/corosync/corosync.conf*. In dieser Datei müssen Sie le-

diglich die Netzwerkadresse (nicht die IP-Adresse) der Schnittstelle eintragen, über die die Kommunikation im Cluster erfolgen soll. Mit */etc/init.d/corosync start* starten Sie den Kommunikationsdienst, der wiederum für einen Start des Clustermanagers *pacemaker* sorgt.

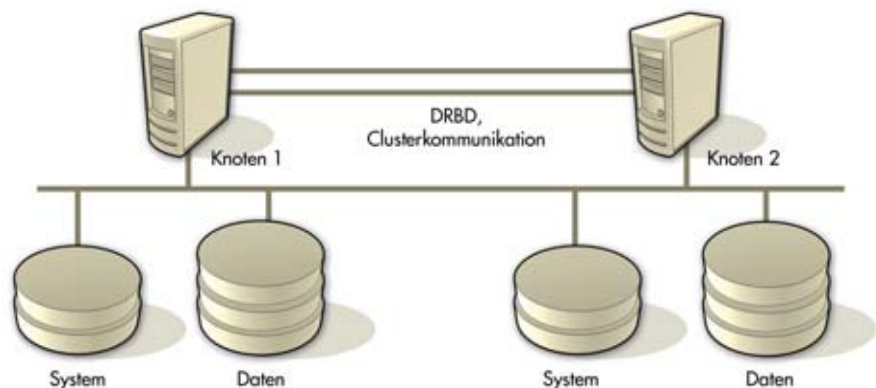
Es versteht sich von selbst, dass ein Pfad, über den sich die beiden Rechner unterhalten können, nicht genug ist – besser ist eine redundante Anbindung. Wenn Sie zwei Schnittstellen zu einem *bond*-Interface zusammenfassen, hat das auch den Vorteil, dass die Last auf die zwei Leitungen verteilt werden kann und DRBD eine Synchronisation doppelt so schnell erledigt.

Konfiguration der Dienste im Cluster

Nachdem wir alle Komponenten getestet haben, folgt nun die Konfiguration des iSCSI-Portals und aller Dienste, die dafür notwendig sind, im Cluster. In *pacemaker* geben Sie die Konfigurationen sehr bequem über die eingebaute Subshell ein. Grundsätzlich sind in einem Cluster auf zwei Knoten ohne *STONITH*-System (siehe unten) folgende Befehle notwendig, um die Voreinstellungen anzupassen:

```
# crm configure property
no-quorum-policy=ignore
# crm configure property
stonith-enabled=false
```

Nachdem wir das *init*-System angewiesen haben (*update-rc.d*), sich nicht mehr



Der schematische Aufbau unseres SAN



um den DRBD-Dienst zu kümmern, können wir die DRBDs durch den Cluster verwalten lassen:

```
# crm configure
crm(live) configure# primitive
  resDRBD ocf:linbit:drbd \
  params drbd_resource=r0
crm(live) configure# ms msDRBD
  resDRBD meta_notify=true
crm(live) configure# commit
```

Die Konfiguration von iSCSI teilt sich in drei Teile: Erst wird der ietd-Dienst gestartet, dann das iSCSI-Portal eingerichtet und abschließend die Partition veröffentlicht. Der Dienst wird über das zugehörige LSB-Script verwaltet und für die beiden anderen Ressourcen gibt es eigene Resource Agents des Clusters, die die API der Open Cluster Foundation (OCF) nutzen.

Zusätzlich sorgen wir mit einer Gruppe dafür, dass die drei Ressourcen in der richtigen Reihenfolge und auf demselben Knoten starten. Mit den Bedingungen (Co-Lokation und Anordnung) stellen wir sicher, dass die Gruppe nur dort gestartet

wird, wo das DRBD sich im Zustand "Master" befindet:

```
crm(live) configure# primitive
  resIETD lsb:iscsitarget
crm(live) configure# primitive
  resTarget \
  ocf:heartbeat:iscsitarget \
  params iqn="iqn.2010-08.de.it-administrator.san:drbd0" tid="1"
crm(live) configure# primitive
  resLUN \
  ocf:heartbeat:iscsiLogicalUnit \
  params path="/dev/drbd0" \
  target_iqn="iqn.2010-08.de.it-administrator.san:drbd0" lun="0"
crm(live) configure# group groupSAN
  resIETD resTarget resLUN
crm(live) configure# colocation
  colSANDRBD inf: \
  groupSAN:Started msDRBD:Master
crm(live) configure# order
  ordDRBDSAN inf: \
  msDRBD:promote groupSAN:start
crm(live) configure# commit
```

Natürlich muss der Cluster unter einer einheitlichen IP-Adresse erreichbar sein. Es wäre fatal, wenn das Portal nach einem Failover unter einer anderen Adresse liefe. Deshalb definieren wir mit

```
crm(live) configure# primitive
  resIP ocf:heartbeat:IPaddr2 \
  params ip="{ip}"
```

eine entsprechende Ressource und fügen sie mit *edit groupSAN* ans Ende der Liste der Ressourcen ein. Sieht die Ausgabe von *crm_mon -lf* wie folgt aus, dann haben Sie alles richtig gemacht:


```
Online: [ node1 node2 ]
```

```
Master/Slave Set: msDRBD
Masters: [ node1 ]
Slaves: [ node2 ]
Resource Group: groupSAN
resIETD (lsb:iscsitarget): Started node1
resTarget (ocf::heartbeat:iscsi-Target): Started node1
```

```
resLUN (ocf::heartbeat:iscsiLogicalUnit): Started node1
resIP (ocf::heartbeat:IPaddr2): Started node1
```

Abschließende Arbeiten

Dieser Workshop kann aus Platzgründen nur zur ersten Orientierung dienen und bietet keine komplette Anleitung für die Einrichtung des Netzwerkspeichers. Jede einzelne Ressource muss zum Beispiel noch von einer monitor-Operation überwacht werden und die Knoten des Clusters sollten überprüfen, ob sie ein paar Gegenstellen im Netzwerk erreichen können (ping-Ressource). Somit ist sichergestellt, dass ein Fehler entdeckt wird und die Verwaltung des Clusters auch darauf reagieren kann. Cluster mit gemeinsam genutztem Speicher (DRBD) brauchen auch unbedingt einen Mechanismus, der katastrophale Auswirkungen verhindert, wenn die Kommunikation zwischen den beiden Knoten einmal gestört sein sollte (Split Brain). Pacemaker bietet für diese Fälle das STONITH-System, mit dem unbotmäßige Knoten von der Stromzufuhr abgeschnitten werden können.

Im Beispiel von oben ist auch keinerlei Absicherung (Authentifizierung, Autorisierung) für die Nutzung des Portals eingebaut. Eine produktives SAN sorgt natürlich dafür, dass nur autorisierte Server Plattenplatz in Anspruch nehmen dürfen. Deshalb wird üblicherweise in der Konfiguration einer LUN noch ein Benutzername mit Passwort hinterlegt. Wenn all diese zusätzlichen Sicherheitsmaßnahmen eingebaut sind, steht einem hoch verfügbaren SAN mit Kapazitäten im TByte-Bereich nichts im Wege. So kann jeder Server seine eigene Partition vom zentralen SAN beziehen und die Verwaltung des Speichers liegt in einer Hand. (jp) 

Mit dem Logical Volume Manager (LVM) bietet der Linux-Kernel noch eine interessante Möglichkeit, die Verwaltung des Speicherplatzes dynamisch zu gestalten. Je nach Bedarf lassen sich Partitionen im laufenden Betrieb vergrößern oder verkleinern. Natürlich muss auch das Dateisystem so eine Operation verkraften. In der Praxis kennt der Bedarf an Speicher nur eine Richtung und die Online-Vergrößerung schaffen die meisten Dateisysteme inzwischen.

Die Anordnung von DRBD und LVM ist frei wählbar. Hier kann der Administrator seine eigenen Vorstellungen umsetzen, egal, ob zwei große Partitionen mit DRBD synchronisiert werden, aus denen dann kleine Stücke per LVM herausgeschnitten werden, oder auf Basis eines großen LVs viele DRBDs repliziert werden.

Anstelle des */dev/drbd0* im Beispiel von oben wird einfach */dev/lv01* per iSCSI exportiert. LVs bieten neben der Dynamik noch den Vorteil, einfache Snapshots für ein späteres Backup nutzen zu können. Aber ebenso wie sich die LVs einbauen lassen, bleibt jedem Administrator genügend Raum für eigene Erweiterungen.

Dynamik im SAN



[1] Konfiguration von DRBD

www.drbd.org

[2] Pacemaker

www.clusterlabs.org

Links





Mit den richtigen PowerShell-Befehlen sichern Sie Ihren XenServer

Citrix XenServer 5.6 über die PowerShell sichern **Backup per Skript**

von Martin Pajonk

Citrix XenServer erfreut sich immer größerer Beliebtheit. Das liegt zum einen am kostenlosen Einstieg in die Virtualisierungswelt und zum anderen am durchaus überzeugenden Funktionsumfang. Doch gibt es derzeit noch zu wenige Alternativen im Backupbereich. Hier lassen sich die Hersteller ihre Lösungen teuer bezahlen – der geldwerte Vorteil von XenServer ist so schnell wieder aufgebraucht. Genau hier setzt eine Kombination aus Microsoft PowerShell und den kommandozeilenbasierten XenCenter-Tools an. Wie Sie damit virtuelle Systeme sichern und wiederherstellen, zeigt Ihnen dieser Workshop.

Die Sicherung und Wiederherstellung von XenServer-Snapshots ist mit ein wenig Handarbeit und ohne eine weitere Softwarelösung möglich. Hierzu wird lediglich die PowerShell, das Citrix XenCenter und das “XenServerPSSnapIn” benötigt. Dem zu Grunde liegt natürlich ein installierter Citrix XenServer inklusive der virtuellen Maschinen, die er beheimatet. Nachfolgend eine kurze Übersicht zu den verwendeten Komponenten.

Auf den aktuellen Microsoft Betriebssystemen, Windows Server 2008 R2 oder Windows 7, findet sich bereits die aktuelle Version der Windows PowerShell. Diese lässt sich aber auch für ältere Semester der OS-Familie problemlos von der Microsoft Website in der Version 2.0 herunterladen und nachinstallieren [1]. Die PowerShell stellt eine Reihe von nützlichen Commandlets (kurz Cmdlets) zur Verfügung und bietet die Möglichkeit, diese auch in Form von PowerShell Snap-Ins zu erweitern. Ein Cmdlet besteht aus einem Verb, einem

Substantiv und einer optionalen Parameterliste wie *Get-ChildItem*. Hilfe zu Cmdlets erhalten Sie entweder durch das Ausführen des Cmdlets *Get-Help {cmdlet} [-params]* oder auf der TechNet Seite von Microsoft [2].

Citrix XenServer und XenCenter installieren

Für die Erstellung der Skripte haben wir in unserem Workshop-Szenario zunächst einen Citrix XenServer in der Version 5.6 eingerichtet. Weiterhin wurden zu Testzwecken mehrere virtuelle Maschinen eingespielt. Das XenCenter läuft in Version 5.6 auf einer Windows 7-Maschine. Die dazugehörige grafische Benutzeroberfläche ermöglicht es, die eingetragenen XenServer und die dort beheimateten virtuellen Maschinen auf einfache Art und Weise zu überwachen und zu administrieren. Sowohl den XenServer als auch das XenCenter können Sie über die Citrix-Seite [3] beziehen. Sollte Hilfe bei der Installation vonnöten sein, ist diese ebenfalls auf der Citrix Seite zu finden [4].

Bei der Installation des XenServers wird auf dem Host automatisch ein Kommandozeilen-basiertes Tool namens “xe” mit installiert. Dieses gibt es auch als eigenständiges Remote-Tool für Windows. Für Windows-Clients wird es bei der Installation von XenCenter aufgespielt und befindet sich im üblichen Installationspfad des XenCenters “C:\Programme\Citrix\XenCenter”. Unter Linux ist der Installer als rpm-Paket verfügbar. Darüber hinaus ist “xe” Bestandteil der Serverinstallations-CD und kann von dieser installiert werden. Zur Vereinfachung der Benutzung sollten Sie den Installationspfad von “xe” in die globale PATH-Variablen eintragen. Eine umfangreiche Dokumentation zum Command Line Interface finden Sie unter [5].

Das PowerShell Snap-In für XenServer wird uns im weiteren Verlauf bei der Auswahl der zu sichernden virtuellen Maschinen behilflich sein. Es steht auf der Citrix Community-Seite zum Download bereit [6].



XenServer PowerShell-Snap-In

Das "XenServerPSSnapIn" besteht aus einer umfangreichen Sammlung von Cmdlets, die für die einfache Administration von XenServern mit Hilfe der PowerShell gedacht sind. In der Kombination mit dem CLI-Tool "xe" können Sie damit praktisch alle denkbaren Aufgaben automatisieren. Vor der Installation sollten Sie jedoch die Rechte innerhalb der PowerShell anpassen – weitere Informationen hierzu erhalten Sie durch die Eingabe von *Get-Help about_execution_policies*. Für unser Beispiel setzen wir die Rechte zur Ausführung von Skripten durch *Set-ExecutionPolicies RemoteSigned*. Die hier bereitgestellten Cmdlets halten sich leider nicht an den vorgeschriebenen Standard für die Benennung. Als Grund werden potenzielle Konflikte mit Konkurrenzprodukten angeführt. Falls Sie keine derartigen Konflikte befürchten, finden Sie im Installationspfad das Skript *Initialize-Aliases.ps1*, das die inkorrekte Namensgebung wieder geradebiegt. Im weiteren Verlauf verwenden wir die nicht standardkonformen Bezeichnungen, da sie in beiden Fällen immer funktionieren sollten. Nach der Installation des XenServerPSSnapIn ist es erforderlich, das Snap-In in der Konsole bekannt zu machen:

```
PS H:\>Get-PSSnapIn -Registered
```

```
Name: PowerGUI
```

```
PSVersion: 1.0
```

```
Description:
```

```
Name: XenServerPSSnapIn
```

```
PSVersion: 2.0
```

```
Description: Citrix XenServer  
PowerShell SnapIn
```

Verließ die Installation erfolgreich, erscheint nach der Eingabe von *Get-PSSnapIn -Registered* das XenServerPSSnapIn auf der Konsole. Nun muss es nur noch in der PowerShell angemeldet werden. Das erfolgt durch die Eingabe von *Add-PSSnapIn XenServerPSSnapIn*. Eine erneute Kontrolle durch die Eingabe von *Get-PSSnapIn* zeigt eine Liste

der in der aktuellen PowerShell angemeldeten Snap-Ins. Das XenServerPSSnapIn kommt mit vielen Cmdlets daher. Sie können sie sich alle durch die Eingabe von *Get-Command -Module XenServerPSSnapIn* anzeigen lassen. Nachfolgend eine kurze Beschreibung der drei Cmdlets, die in den Backup- und Restore-Skripten Verwendung finden.

- Connect-XenServer: Wie der Name erahnen lässt, dient dieses Cmdlet dazu, eine Verbindung mit dem XenServer aufzubauen. Als Parameter werden die URL, der Benutzer und das Passwort benötigt. Weitere Parameter und Informationen zu diesem Cmdlet erhalten Sie durch die Eingabe von *Get-Help Connect-XenServer*. Eine erfolgreiche Verbindung hat die Rückgabe eines Xen-API.XenObject-Objekts zur Folge. Die genaue Syntax finden Sie sowohl im weiteren Verlauf des Artikels als auch in der Hilfe zu Connect-XenServer.
- Get-XenServer:VM: Mit Hilfe dieses Cmdlets werden alle auf dem XenServer sich befindenden virtuellen Maschinen ausgegeben, inklusive Templates, Snapshots und Controll Domains. Zu beachten ist hierbei, dass zuvor eine Verbindung mit dem XenServer mittels Connect-XenServer aufgebaut wurde. Wie später zu sehen ist, kann mit Hilfe des "Where-Object"-Cmdlets und einer Pipe auf simple Art und Weise die Ausgabe, der Output des Get-XenServer:VM Cmdlets gefiltert werden. Auch hier liefert das Cmdlet ein Objekt zurück, diesmal vom Typ "System.Array".
- Disconnect-XenServer: Über das dritte Cmdlet müssen nicht viele Worte verloren werden. Es schließt eine bestehende Verbindung mit einem XenServer, der über den URL-Parameter spezifiziert werden kann.

Entwicklungsumgebung und Aufbau der Skripte

Für das Erstellen der Skripte können Sie jeden beliebigen Texteditor verwenden. Trotzdem ist zu erwähnen, dass Microsoft der PowerShell eine recht nützliche Entwicklungsumgebung – das "Windows

PowerShell Integrated Scripting Environment" oder kurz ISE – spendiert hat. Dieses verfügt sogar über rudimentäre Debuggingfunktionen, womit das Auffinden von Fehlern um einiges vereinfacht wird. Als eine Alternative bietet sich zudem die PowerGUI an, die mit Code-Vervollständigung und einer Anzeige der aktuellen Variablen daherkommt. Doch nun zu den Skripten selbst. Diese sind auf vier Dateien verteilt worden.

```
1. config.ps1
```

```
2. xen.ps1
```

```
3. backup.ps1
```

```
4. restore.ps1
```

Die Namensgebung der einzelnen Dateien verrät bereits, wofür die einzelnen Skripte gut sind. In der Datei *config.ps1* sind alle benötigten Informationen hinterlegt, um mit einem speziellen Server Kontakt aufzunehmen oder wo die zu speichernden Dateien abgelegt werden sollen. Die Pfade beziehen sich auf den Host, auf dem auch die Skripte aufgerufen werden. Die Zeile "Set-PSDebug -Strict" dient dazu, nicht initialisierte Variablen zu melden, so dass leicht zu übersehende Tippfehler bei der Benennung von Variablen von vorneherein vermieden werden.

Die Datei *xen.ps1* bündelt alle benötigten Funktionen für die Sicherung und den Export von Snapshots und für die

```
# Variablen müssen vor Benutzung
# initialisiert werden
Set-PSDebug -strict

# citrix server
$_ip = '192.168.23.42'
$_url = 'http://' + $_ip
$_user = 'root'
$_pw = 'geheim'

# Sicherungspfad für Backupdateien
$_storePath = 'C:\STORE\PATH'

# Beinhaltet wiederherzustellende
# Snapshots
$_restorePath = 'C:\PATH\TO\FILES'

# Logging Pfad und Dateiname
$_logPath = 'C:\PATH\TO\LOG\STORAGE'
$_logFileName = 'my.log'
```

Listing 1: config.ps1





```

$_scriptRoot = "C:\PATH\TO\SCRIPTS\"

# externe Skripte includieren
. ($scriptRoot + "config.ps1" )
. ($scriptRoot + "xen.ps1" )

trap
{
    "Hier ist etwas furchtbar schief gegangen: " + $_
}

# Eine Liste zu sichernden VMs holen
$vmList = GetVmList "vm"

if ($vmList -ne "") {
    foreach ($vm in $vmList) {
        DoSnapshot $vm | Out-Null
    }
} else {
    throw "Leere VM Liste übergeben"
}

# Eine Liste zu exportierender Snapshots holen
$snapshotList = GetVmList "snapshot"

if ($snapshotList -ne "") {
    foreach ($snapshot in $snapshotList){
        ExportSnapshot $snapshot
    }
} else {
    throw "Leere Snapshotliste übergeben"
}

```

Listing 2: backup.ps1



Wiederherstellung von Templates und ist somit die zentrale Datei bei diesem Unterfangen. Die Skripte *backup.ps1* und *restore.ps1* bedienen sich der anderen beiden Skripte, um die ihnen angedachten Aufgaben zu erfüllen. In beiden wird einleitend zunächst der Skriptpfad gesetzt und anschließend die benötigten Dateien *config.ps1* und *xen.ps1* eingebunden.

Snapshot erstellen

Um Snapshots erstellen zu können, müssen Sie zunächst in Erfahrung bringen, wovon Snapshots gemacht werden sollen. Hierzu dient die Funktion "GetVmList" in der Datei *xen.ps1*. Innerhalb der Funktion legen Sie anhand des übergebenen Parameters fest, wonach gefiltert werden soll. Wie Sie dem Quellcode entnehmen können, sorgt der Parameter "vm" nach dem Verbindungsaufbau dafür, dass eine Liste jener Ressourcen zurückgegeben wird, die kein Snapshot, Template oder Kontrolldomäne sind. Im Detail geschieht dies durch das Anwenden des Cmdlets "Where-Object", das mit Hilfe des Pipeoperators an das "Get-XenServer:VM"-Cmdlet angehängt wird. Das Ergebnis des

Cmdlets "Get-XenServer:VM" wird dann an ein "Where-Object" übergeben, das anhand der an ihn weitergereichten Filterregeln die gewünschten Ergebnisse liefert. Beim "\$_"-Konstrukt handelt es sich um eine in PowerShell vordefinierte Variable, die auf das zuletzt übergebene Objekt zugreift. Durch den Punktoperator "." wird auf Eigenschaften des Objekts zugegriffen. Mit wenig Aufwand ist es auch problemlos möglich, die Auswahl der zu sichernden virtuellen Maschinen den eigenen Bedürfnissen anzupassen. Nach dem Zugriff auf den XenServer wird die Verbindung wieder geschlossen und das Ergebnis von der Funktion wieder zurückgegeben.

In der Signatur der Funktion werden nun die benötigten Parameter mit den Defaultwerten aus der Konfigurationsdatei besetzt. Durch die Angabe von konkreten Werten lassen sich über eine foreach-Schleife auch mehrere XenServer mit dieser Funktion nach potentiellen Snapshot-Kandidaten durchforsten. Die von "GetVmList" zurückgegebene Liste wird iteriert und von jedem Kandidaten nun mit Hilfe der Funktion "DoSnapshot" ein Snapshot auf dem Server angefertigt. In der Funktion "DoSnapshot" passieren zwei Dinge: Es wird der Name des Snapshots generiert und durch den Aufruf von

```

xe -s $ip -u $user -pw $pw vm-
snapshot vm=$uuid new-name-
label=$snapshotNameLabel

```

der Snapshot erzeugt. Als Ergebnis erhalten Sie eine uuid, die den erstellten Snapshot eindeutig identifiziert.

Snapshot exportieren

Ebenso wie beim Erzeugen der Snapshots muss dem Skript bekannt sein, welche Snapshots es exportieren soll. Hierzu nutzen Sie die Funktion "GetVmList". Dieses Backup-Skript gibt alle auf dem XenServer vorhandenen Snapshots zurück. Die so erhaltene Liste wird abermals durchlaufen und der Export der zu-

vor erstellten Snapshots beginnt mit Hilfe der Funktion "ExportSnapshot". Der eigentliche Export der Snapshots findet in der Zeile

```

$exportResult = xe -s $ip -u $user
-pw $pw snapshot-export-to-template
snapshot-uuid=$uuid
filename=$fileName

```

statt. Dadurch wird ein Template des angelegten Snapshots erzeugt und als XVA-Image unter dem in "\$filename" angegebenen Dateinamen gespeichert.

```

function ExportSnapshot([XenAPI.XenObject] $snapshot,
[string] $ip = $ip, [string] $user = $user, [string]
$password = $pw, [string] $storePath = $storePath)
{
    if (!$snapshot) {
        throw "kein Snapshot für Export übergeben"
    }
    $uuid = $snapshot.uuid
    $fileName = $storePath + $snapshot.name_label + ".xva"
    $exportResult = xe -s $ip -u $user -pw $pw
    snapshot-export-to-template snapshot-
    uuid=$uuid filename=$fileName

    if ($exportResult -eq "Export succeeded") {
        Out-File -FilePath ($_logPath + $_logFileName)
        -InputObject ("$(Get-Date -Format yyyyMMddHHmmss)
        - " + $uuid + " - export - [ OK ]") -Encoding
        utf8 -Append
        RemoveSnapshot $snapshot $ip $user $pw
    } else {
        Out-File -FilePath ($_logPath + $_logFileName)
        -InputObject ("$(Get-Date -Format yyyyMMddHHmmss)
        - " + $uuid + " - export - [ FAIL ]") -Encoding
        utf8 -Append
        Out-File -FilePath ($_logPath + $_logFileName)
        -InputObject ("$(Get-Date -Format yyyyMMddHHmmss)
        - " + $uuid + " - export - " + $exportResult)
        -Encoding utf8 -Append
    }
}

function RemoveSnapshot([XenAPI.XenObject] $snapshot,
[string] $ip = $ip, [string] $user = $user, [string]
$password = $pw)
{
    if ($snapshot.is_a_snapshot) {
        $uuid = $snapshot.uuid
        $removeResult = xe -s $ip -u $user -pw $pw
        snapshot-uninstall snapshot-uuid=$uuid force=$true
        Out-File -FilePath ($_logPath + $_logFileName)
        -InputObject ("$(Get-Date -Format yyyyMMddHHmmss)
        - " + $uuid + " - remove - [ OK ]") -Encoding
        utf8 -Append
        Out-File -FilePath ($_logPath + $_logFileName)
        -InputObject ("$(Get-Date -Format yyyyMMddHHmmss)
        - " + $uuid + " - remove - " + $removeResult)
        -Encoding utf8
        -Append
    } else {
        Out-File -FilePath ($_logPath + $_logFileName)
        -InputObject ("$(Get-Date -Format yyyyMMddHHmmss)
        - " + $snapshot.uuid + " - remove - [ FAIL ]")
        -Encoding utf8
        -Append
    }
}
}

```

Listing 3: xen.ps1 (Teil 1)



```

function GetVmList([string] $trigger = "vm", [string] $url = $_url, [string] $user = $_user, [string] $pw = $_pw)
{
    Connect-XenServer -Url $url -UserName $user -Password $pw | Out-Null

    switch ($trigger.ToLower())
    {
        "vm" { $vmList = Get-XenServer:VM | Where-Object {!$_is_a_snapshot -and !$_is_a_template -and !$_is_control_domain} }
        "snapshot" { $vmList = Get-XenServer:VM | Where-Object {$_is_a_snapshot -eq $true} }
        default { throw "Trigger [$trigger] in Funktionssignatur nicht definiert" }
    }

    Disconnect-XenServer -Url $url

    return $vmList
}

function DoSnapshot([XenAPI.XenObject] $vm, [string] $ip = $_ip, [string] $user = $_user, [string] $pw = $_pw)
{
    if (!$vm) {
        throw "keine VM übergeben"
    }

    # Snapshotnamen mit Zeitstempel generieren
    [string]$snapshotNameLabel = "$(Get-Date -Format yyyyMMddHHmmss)_" + $vm.name_label

    $uuid = $vm.uuid
    # gib die erzeugte Uuid zurück
    return xe -s $ip -u $user -pw $pw vm-snapshot vm=$uuid new-name-label=$snapshotNameLabel
}

function ImportSnapshot([string] $fileName, [string] $ip = $_ip, [string] $user = $_user, [string] $pw = $_pw)
{
    if ($fileName -ne '') {
        $filePath = $_restorePath + $fileName

        $msg = "$(Get-Date -Format yyyyMMddHHmmss) - " + $filePath + " - import -"

        $uuid = xe -s $ip -u $user -pw $pw vm-import filename=$filePath
        if ($uuid -ne '') {
            out-File -FilePath ($_logPath + $_logFileName) -InputObject ($msg + " [ OK ]") -Encoding utf8 -Append
            CreateVm $uuid $fileName
        } else {
            out-File -FilePath ($_logPath + $_logFileName) -InputObject ($msg + " [ FAIL ]") -Encoding utf8 -Append
        }
    }
    else {
        throw "Kein Dateiname für Import eingegeben"
    }
}

function CreateVm([string] $uuid, [string] $fileName, [string] $ip = $_ip, [string] $user = $_user, [string] $pw = $_pw)
{
    if ($uuid -eq "") {
        throw "keine uuid angegeben"
    }

    if ($fileName -eq "") {
        throw "kein Dateinamen übergeben"
    }

    # Namen für neue VM erstellen
    $newNameLabel = $fileName.TrimEnd('.xva')

    $newUuid = xe.exe -s $ip -u $user -pw $pw vm-install new-name-label=$newNameLabel template-uuid=$uuid

    # erstellte VM starten
    xe.exe -s $ip -u $user -pw $pw vm-start vm=$newUuid
}

```

Listing 4: xen.ps1 (Teil 2 ab function GetVmList)



Nach dem erfolgreichen Export können Sie den Snapshot vom XenServer entfernen. Dies geschieht durch die Funktion "RemoveSnapshot". Das Löschen der Snapshots auf dem XenServer initiieren Sie durch den Aufruf der Zeile

```
xe -s $ip -u $user -pw $pw snapshot-uninstall snapshot-uuid=$uuid force=$true
```

Diese Zeile ist allerdings mit Vorsicht zu genießen. Normalerweise ist eine Bestätigung des Benutzers beim Ausführen dieses Kommandos vonnöten, um den Löschvorgang anzustoßen. Diese Sicherheitsabfrage schalten Sie im Skript durch den Zusatz "force=true" aus. Als nächster Punkt sei erwähnt, dass jede an das Kommando übergebene uuid vom Server entfernt wird, unabhängig davon, ob es sich dabei um einen Snapshot handelt oder nicht. So sollten Sie sich durch die Formulierungen innerhalb des abgesetzten Befehls *snapshot-uninstall snapshot-uuid* nicht auf der sicheren Seite wähnen – schließlich ist nicht davon auszugehen, dass etwas anderes als ein Snapshot gelöscht werden könnte. Nach Beendigung des Skriptes lohnt noch ein prüfender Blick in das angefertigte Logfile. In der *config.ps1* wurde es unter dem Namen *my.log* angelegt und befindet sich im Verzeichnis der exportierten Templates.

Snapshot wiederherstellen

Das Wiederherstellen der Snapshots aus den gesicherten Templates geht in zwei Schritten vor sich.

1. Die wiederherzustellenden Templates importieren.
2. Das Erstellen von virtuellen Maschinen aus den importierten Templates.

Im Skript *restore.ps1* werden zunächst alle Dateien mit Hilfe des Cmdlets "Get-ChildItem" in der Variable "\$backupFiles" abgelegt, die in *config.ps1* über "\$_restorePath" definiert sind. Dank des Cmdlets können Sie sich das aktuelle Verzeichnis anzeigen lassen, ganz im Stil des klassischen dir-Befehls. Nebenbei erwähnt



ist *dir* der Alias für *Get-ChildItem* in der PowerShell. Da für unsere Zwecke die Namen der vorhandenen Dateien völlig ausreichen, teilen wir dies dem Cmdlet über den Parameter “-Name” mit. Weiterhin sind nur die Dateien mit der Endung *.xva* interessant, was Sie durch ein *-Include *.xva* an das Cmdlet weitergeben. Für jede der von “Get-ChildItem” zurückgelieferten Dateien wird die Funktion “ImportSnapshot” aufgerufen. Durch den CLI-Aufruf *xe -s \$ip -u \$user -pw \$pw vm-import filename=\$filePath* werden die Templatedateien auf den XenServer hochgeladen und stehen ab dann bereit, um installiert zu werden.

Ist das Template hochgeladen, geht die Wiederherstellung einer virtuellen Maschine recht schnell vonstatten. Der CLI-Aufruf

```
xe.exe -s $ip -u $user -pw $pw
vm-install new-name-label=$newName
Label template-uuid=$uuid
```

stellt die virtuelle Maschine aus dem bereits hochgeladenen Template wieder her. Ist die virtuelle Maschine installiert, können Sie diese per CLI direkt starten. Dies geschieht durch den Aufruf

```
xe.exe -s $ip -u $user -pw $pw
vm-start vm=$newUuid
```

Welche virtuelle Maschine gestartet wird, lässt sich entweder durch die Angabe des Namens oder der *uuid* bestimmen.

Automatisierung der Snapshotlösung

Um das regelmäßige Ausführen von Backups zu automatisieren, bietet sich in der Microsoft-Welt der Aufgabenplaner an. Sie finden ihn unter “Start / Alle Programme / Zubehör / Systemprogramme”. Das Hinzufügen einer neuen Aufgabe sollte kein Problem darstellen. Hierbei ist zu beachten, dass bei der Erstellung der Aufgabe die Aktion “Programm/Skript starten” ausgewählt ist. Als das auszuführende Programm geben Sie die PowerShell an: *C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe*. Sie wird mit den Argumenten *-command “Add-PSSnapin XenServer PSSnapIn; & C:\PATH\TO\SCRIPT\backup.ps1”* gestartet, die Sie in dem dafür vorgesehenen Feld “Argumente hinzufügen (optional)” eintragen. Mit dem Parameter “-command” sorgen Sie dafür, dass die folgenden Instruktionen wie in einem geöffneten PowerShell-Fenster interpretiert werden. Als Erstes stellen Sie damit sicher, dass das *XenServerPSSnapIn* geladen ist. Anschließend wird das Backupskript ausgeführt und Sie müssen nur noch die Frequenz angeben, mit der die Backups ausgeführt werden sollen. Bestätigen Sie diese Aktion nun zweimal mit “OK”.

Fazit

Die hier vorgestellten Skripte sind ein Anfang und sollten an die eigenen Bedürfnisse angepasst beziehungsweise erweitert werden [7]. Im Zusammenspiel mit dem Windows-Aufgabenplaner ist es ohne weiteres möglich, gezielt und regelmäßig Backups von virtuellen Maschinen anzufertigen. Der Einsatz des *XenServerPSSnapIns* erlaubt eine unkomplizierte Auswahl und Export der zu sichernden virtuellen Maschinen. Da Backupskripte den Großteil ihrer Zeit ohne Aufsicht ablaufen, ist es sicher von Vorteil, wenn Ausnahmebehandlung implementiert ist. Abhängig von der vorhandenen Infrastruktur kann es erforderlich sein, dass nicht zu-

erst alle Abbilder erstellt und anschließend nacheinander exportiert werden, vielmehr kann die Sicherung auch so gestaltet werden, dass jede virtuelle Maschine komplett abgebildet und exportiert wird, bevor weitere Sicherungen vorgenommen werden.

Anstatt alle gesicherten Templates aus einem Verzeichnis wiederherzustellen, kann es komfortabler sein, die betroffenen Templates in einer Textdatei zusammenzufassen und über diese importieren zu lassen. Nach der Wiederherstellung dürften die importierten Templates in den meisten Fällen nicht mehr vonnöten sein. Sie können diese nach der erfolgreichen Erstellung automatisch vom System entfernen. Hierdurch halten Sie auch die Redundanz der vorhandenen Templates auf dem XenServer in Grenzen. Abhängig von der Anzahl und Größe der zu sichernden virtuellen Maschinen sowie dem möglichen Maximaldurchsatz des vorhandenen Netzwerks kann es nötig werden, die Sicherung auf mehrere Slots zu verteilen. Es kann durchaus vorkommen, dass eine Sicherungskopie einer 75 GByte großen virtuellen Maschine zwischen 90 und 120 Minuten oder noch länger in Anspruch nimmt. Bei einer Handvoll virtueller Maschinen bieten sich Backups von Hand über das XenCenter an. Wesentlich sicherer und komfortabler ist es allerdings, diese Aufgabe zu automatisieren. (dr)

```
$_scriptRoot = "C:\PATH\TO\SCRIPTS\"

# externe Skripte includieren
. ($_scriptRoot + "config.ps1" )
. ($_scriptRoot + "xen.ps1" )

trap
{
    "Hier ist etwas furchtbar schief gegangen: " + $_
}

$backupFiles = Get-Childitem $_restorePath -Name -Include
*.xva

if ($backupFiles -ne '') {
    foreach ($backupFileName in $backupFiles) {
        ImportSnapshot $backupFileName
    }
}
```

Listing 5: restore.ps1



- [1] Download der PowerShell 2.0
<http://support.microsoft.com/kb/968929>
- [2] Hilfe zu Cmdlets
<http://it-a.eu/aap32>
- [3] XenServer und XenCenter-Download
<http://it-a.eu/aap33>
- [4] Installationshilfe zu XenServer und XenCenter
<http://it-a.eu/aap34>
- [5] Dokumentation zum Command Line Interface
<http://it-a.eu/aap35>
- [6] PowerShell Snap-In für XenServer
<http://community.citrix.com/cdn/xs/sdks>
- [7] Citrix XenServer Administrators Guide
<http://it-a.eu/aap37>

Links



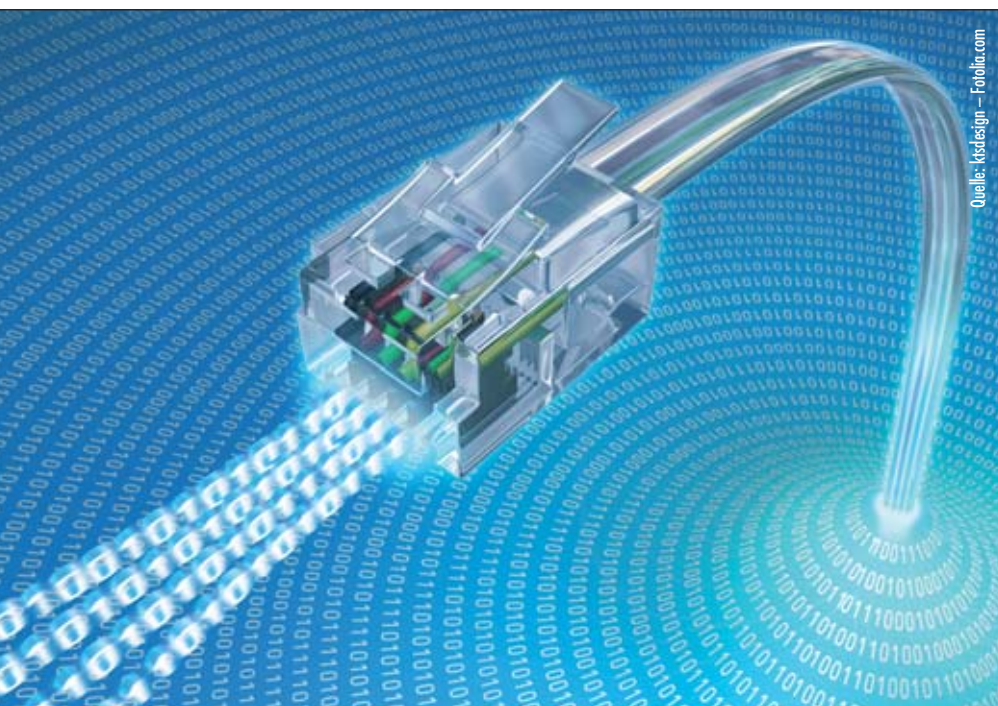


Stolperfallen bei der Umstellung auf IPv6 (1)

Protokoll mit Tücken

von Christian Rusch und Alexander von Gernler

Seit Jahren heraufbeschworen, steckt das neue Internet-Protokoll IPv6 noch immer in den Startlöchern fest. Nur zögerlich trauen sich Provider und Unternehmen an die Umstellung. Nicht ganz ohne Grund, denn neben den Vorteilen des größeren Adressraums und flexibleren IP-Adressen birgt IPv6 auch so manche Stolperfallen. Doch lassen sich diese angesichts der tatsächlich knapp werdenden IPv4-Ressourcen nicht mehr lange ignorieren, wie unsere neue Workshopserie zeigt.



Mehr als 90 Prozent des Adressraumes von IPv4 seien vergeben, gab Anfang des Jahres die ICANN in einer Pressemitteilung bekannt [1]. Nur noch 24 Adressblöcke zu je 16,7 Millionen Adressen wären noch nicht zugeteilt.

Das war im Januar 2010. Mittlerweile gibt es nur noch 14 freie Adressblöcke [2]. Hochgerechnet wird demnach Mitte April 2011 der letzte noch freie Adressblock an eine Regionale Internet Registry (RIR) zugewiesen [3]. Mit der Zuteilung des letzten Adressblocks hört das Internet aber nicht plötzlich auf zu funktionieren. Vielmehr sollte kurzfristig nichts

davon zu spüren sein. Erst nach ein paar Monaten wird eine nach der anderen RIR nicht mehr in der Lage sein, ihren Kunden neue IP-Adressen zuzuteilen. Zugang zum Internet zu bekommen wird ab dann schwieriger – oder teurer. Beschränkt ist die Größe eines Adressraumes primär durch die Zahl der eindeutigen Adressen, die sich mit dem verwendeten Schema darstellen lassen. Im Schema für IPv4 besteht eine Adresse aus 32 Bit. Mehr als vier Milliarden eindeutige Adressen stehen dadurch theoretisch zur Verfügung. Davon sind allerdings knapp 600 Millionen für protokollspezifische Details und Erweiterungen wie

Loopback, Broadcast oder Multicast reserviert und daher nicht verwendbar.

Auf der Annahme beruhend, Zugang zum Internet sei ausschließlich für ein paar global agierende Organisationen von Bedeutung, wurden Internet-Adressen gemäß EIN 48 ursprünglich als eine Kombination einer 8 Bit langen Netzwerknummer und einer 24 Bit langen Host-ID definiert. Obwohl diese Annahme sehr bald als unzutreffend erkannt und die Definition mehrfach angepasst wurde, sind die Folgen davon heute noch klar erkennbar [4]. So ist ungefähr 60 Prozent des verfügbaren Adressraumes durch Organisationen und Regierungsstellen der USA belegt; einem Land, das mit 344 Millionen Einwohnern gerade einmal fünf Prozent der Weltbevölkerung stellt [5].

IPv6 vergrößert Adressraum

Prinzipiell lässt sich das Problem der immer knapper werdenden Adressen auf zwei Arten lösen. Der vorhandene Adressraum wird erweitert oder er wird effizienter genutzt. Letzteres ist wegen der in keinem Vergleich zum Nutzen stehenden Risiken und nicht abschätzbaren Kosten nicht realisierbar. Riesige Adressblöcke müssten jeweils auf einen Schlag und ohne Möglichkeit eines Rollbacks unnummeriert werden. Zugewiesene, aber dennoch komplett unbenutzte Adressblöcke wird es seit dem Aufruf, diese zurückzugeben (RFC 1917), wohl auch keine mehr geben.

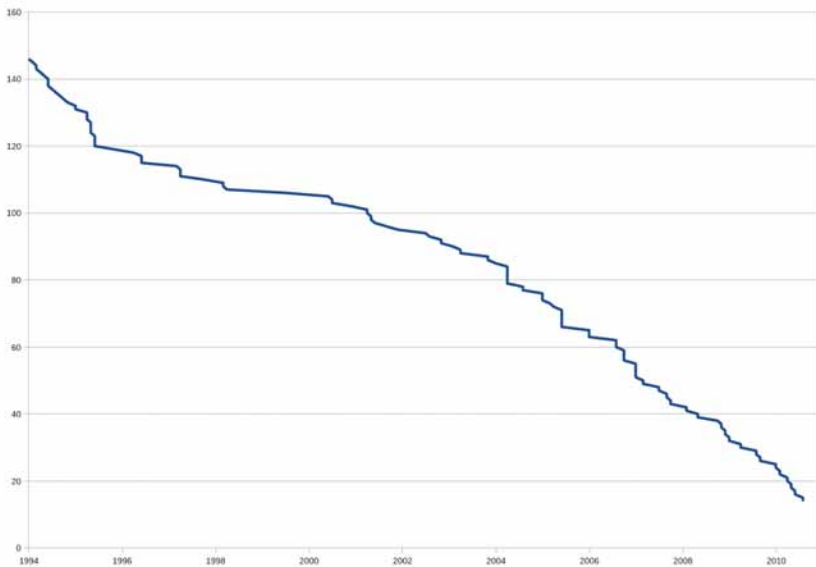


Bild 1: Es geht bergab mit den verfügbaren IPv4-Adressen...

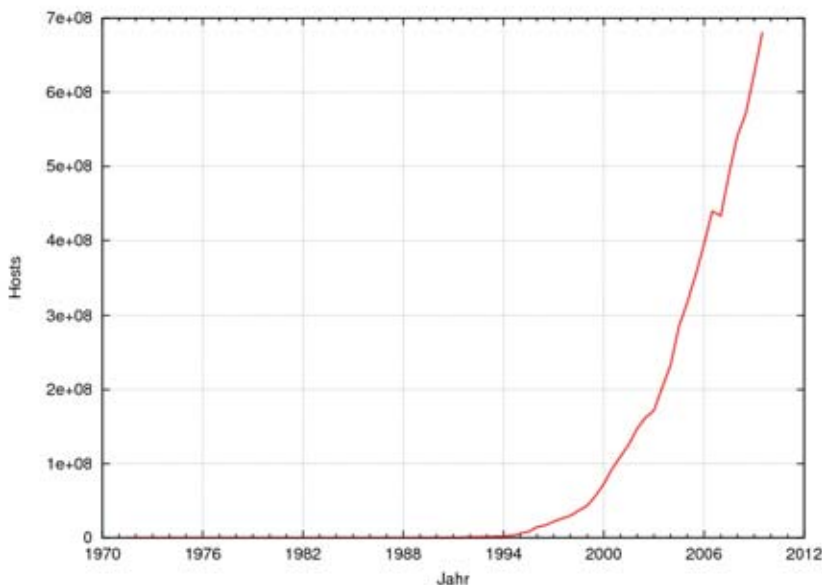


Bild 2: ... dafür steigt die Anzahl an Hosts sprunghaft an

Vergrößern lässt sich der Adressraum beispielsweise über ein geändertes Adressierungsschema. Da dies zum Verlust der Kompatibilität mit dem bisherigen Schema führt, entspricht es dem Wechsel zu einem neuen Protokoll. Mit IPv6 steht ein Protokoll zur Verfügung, das nicht nur in Bezug auf den Adressraum die heutigen Erwartungen übererfüllt, sondern das auch noch weitere interessante Leis-

tungsmerkmale mitbringt. Darüber hinaus adressiert es auch viele Probleme, unter denen IPv4 zu leiden hatte. Besonders hervorzuheben ist, dass IPv6 so viele Adressen mitbringt, dass sich nicht nur theoretisch jeder Toaster und jede Waschmaschine auf dem Planeten mit einer Internetadresse ausstatten ließe, sondern auch, dass sich endgültig das eigentlich als Notlösung für die Adress-

knappheit gedachte Verfahren der Network Address Translation (NAT) erledigt hat. Das bedeutet, es müssen nicht länger Arbeitszeit und Technik eingesetzt werden, nur um die Folgen eines Adressmangels zu umgehen. Eine Welt ohne NAT sähe auch deshalb besser aus, weil Nutzer sich nicht mehr um Workarounds für die beim NAT verwendeten privaten IP-Adressen kümmern müssten. Hier wäre beispielsweise STUN (RFC 3489) zu nennen. Das gesamte RFC beschäftigt sich nur damit, von NAT verursachte Probleme bei UDP-basierten Protokollen zu lösen.

Hochkomplexe Kopfgeburt

Ein oft geäußerter Kritikpunkt am neuen Internet-Protokoll ist die im Vergleich zu IPv4 stark gewachsene Komplexität. Eine Unzahl neuer Leistungsmerkmale verhindert effektiv die Wiederverwendbarkeit von Teilen der bestehenden und über lange Zeit gereiften Implementierung für IPv4. Fehler, darunter sehr wahrscheinlich auch sicherheitsrelevante, sind daher in den Implementierungen von IPv6 zu erwarten.

Um das Jahr 1991 begann die IETF damit, einen Nachfolger für das bestehende Internet-Protokoll IPv4 zu suchen. Der Hauptgrund war die Befürchtung, der verfügbare IP-Adressraum werde in absehbarer Zeit erschöpft sein. Viele Projekte wurden mit der Absicht ins Leben gerufen, Vorschläge zu finden, wie das Problem mit dem begrenzten Adressraum zu lösen ist. Einige dieser Projekte nahmen sich darüber hinaus auch weiteren bekannten Problemen von IPv4 an, wie der automatischen IP-Adresskonfiguration von Hosts ohne fremde Hilfe oder der nachträglichen Erweiterbarkeit des Protokolls. 1994 wurde schließlich aus den Ideen der vier besten eingereichten Vorschläge IPv6 in einem Normvorschlag (RFC 1752) spezifiziert. Eine vorab ins Leben gerufene Arbeitsgruppe hatte hochgerechnet, dass der bestehende IP-Adressraum frühestens im Jahr 2005 aufgebraucht sei. Die daraus resultierende Erkenntnis, dass gut zehn Jahre



für die Implementierung zur Verfügung stehen würden, hatte dazu bewogen, weitere, neue Funktionalität aus den Vorschlägen mit in die Spezifikation aufzunehmen.

So ist beispielsweise die Unterstützung für das Unterbringen von Optionen und Erweiterungen im Protokoll-Header im Gegensatz zu IPv4 modular aufgebaut. Ergänzungen verschiedener Typen können optional an den eigentlichen Paket-Header gehängt werden und diesen so erweitern. Für die Implementierung von Routern ist dies ein Segen. Der Haupt-Paket-Header ist immer gleich lang und die zur Weiterleitung des Pakets notwendigen Adressfelder sind immer an derselben Stelle zu finden und auf 64 Bit ausgerichtet ("64 bit aligned"). Darüber hinaus gibt es keine Prüfsumme mehr, die ausgewertet und modifiziert werden müsste. Pakete, die für das Routing relevante Zusatzinformationen mitführen, sind als solche einfach zu erkennen und können – sofern vom Router unterstützt und vom Betreiber gewollt – einer separaten Behandlung zugeführt werden. Für alle übrigen Pakete ist aber weder Speicherplatz dynamisch bereitzustellen, noch muss der bestehende Header aufwändigen Berechnungen unterzogen werden.

Weniger erfreulich ist das neue Konzept für Firewall-Hersteller, deren Produkte jedes Paket sehr genau unter die Lupe nehmen müssen. Hier stellt die Möglichkeit, Paket-Header mit theoretisch beliebigen Erweiterungen zu versehen, einen Graus dar. Alle Ergänzungen zum Protokoll-Header müssen zunächst analysiert werden, um an der Firewall die Entscheidung treffen zu können, was mit dem vorliegenden Daten-Paket passieren soll. Das Interpretieren dieser Header-Listen ist bei Weitem komplizierter, als Bits oder Felder im (dafür größeren) IPv4-Protokoll-Header zu prüfen. Mehrere Entwickler aus dem Umfeld des OpenBSD-Betriebssystems sind der Meinung, dass IPv6 durch den Verzicht auf neue Funktionalität zwar nur das Adressraum-Problem gelöst, aber aufgrund seiner Einfachheit schneller Akzeptanz gefunden

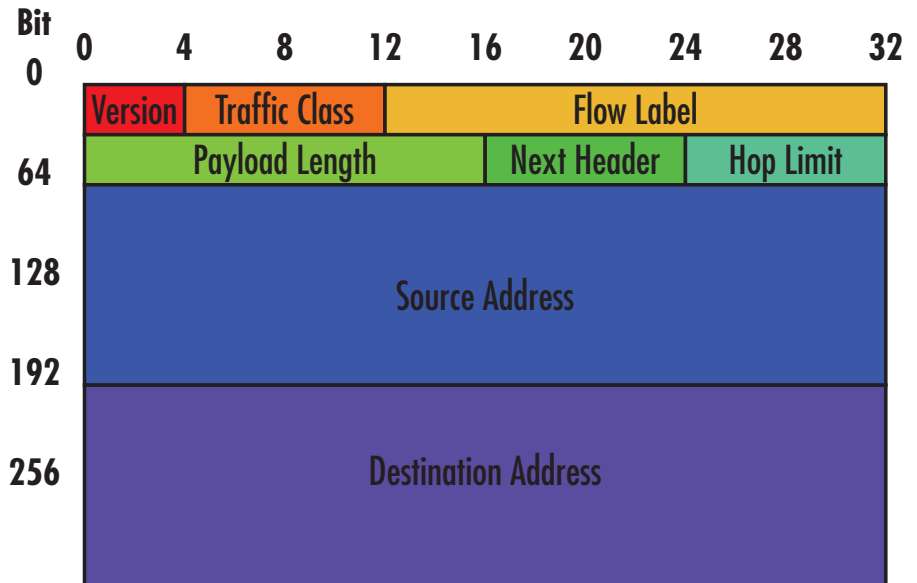


Bild 3: Der Aufbau eines IPv6-Pakets

hätte [6]. Stattdessen ist mehr als ein Jahrzehnt nach den ersten Schritten IPv6 noch immer nicht flächendeckend im Einsatz.

IPv6 wird kommen

Der Internet Engineering Task Force war bereits bei der Ausschreibung für den Nachfolger von IPv4 klar, dass ein Umstieg auf ein neues Internet-Protokoll ein schwieriger und komplexer Prozess sein würde. Im Anforderungskatalog für das neue Protokoll ist deshalb auch die Forderung nach einem Plan für die Übergangsphase enthalten.

Anders als beim Wechsel des Internetprotokolls von NCP nach TCP/IP in grauer Vorzeit wurde für den Wechsel zu IPv6 eine ganze Reihe an Übersetzungsverfahren spezifiziert, die den Datenaustausch zwischen den beiden Netzwerkprotokollen ermöglichen sollten. Für die Migration von NCP zu TCP/IP wurde geplant, am 1. Januar 1983 NCP endgültig zu deaktivieren (RFC 801). Wie aus den Fortschrittsberichten (RFC 832 bis RFC 839, RFC 842 bis RFC 848 und RFC 876) ersichtlich ist, war das Internet aber erst ungefähr neun Monate später vollständig umgestellt. Auch deshalb hat die IETF davon abgesehen, ein Datum festzulegen, bis wann die Umstellung auf IPv6 abgeschlossen sein muss. Angesichts des zwischenzeitlich fast aufge-

brauchten Adressraumes von IPv4 und den zur Verfügung stehenden Mitteln für eine sanfte Migration müsste das neue Protokoll eigentlich weit verbreitet sein. Die Wirklichkeit sieht anders aus: Wenn auch in den letzten Monaten endlich etwas Bewegung in die Verbreitung von IPv6 gekommen ist, so ist noch immer viel zu wenig davon spürbar.

Die Ursache für die schleppende Verbreitung ist die Wechselwirkung zwischen Anbietern von Inhalten und den Zugangsprovidern. Inhalteanbieter erreichen durch die Aufschaltung ihrer Angebote auf IPv6 keinen größeren Kundenkreis. Es besteht sogar ein – wenn auch verschwindend kleines – Risiko, dass ihre Angebote danach weniger gut erreichbar sein werden. Zuganganbieter andererseits sehen keine Notwendigkeit, ihren Kunden Zugang über IPv6 zum Internet anzubieten, solange darüber keine Inhalte abrufbar sind. Diese Situation wird sich nun aber sehr bald ändern. Voraussichtlich ab Oktober 2011 wird eine der fünf Regionalen Internet Registries (RIR) anfangen müssen, Anträge auf neue IP-Adressen abzuweisen. Spätestens ein Jahr darauf werden alle RIRs in dieser Lage sein. Hochrechnungen zufolge soll dann nämlich der letzte jetzt noch freie Adressblock aufgebraucht sein.

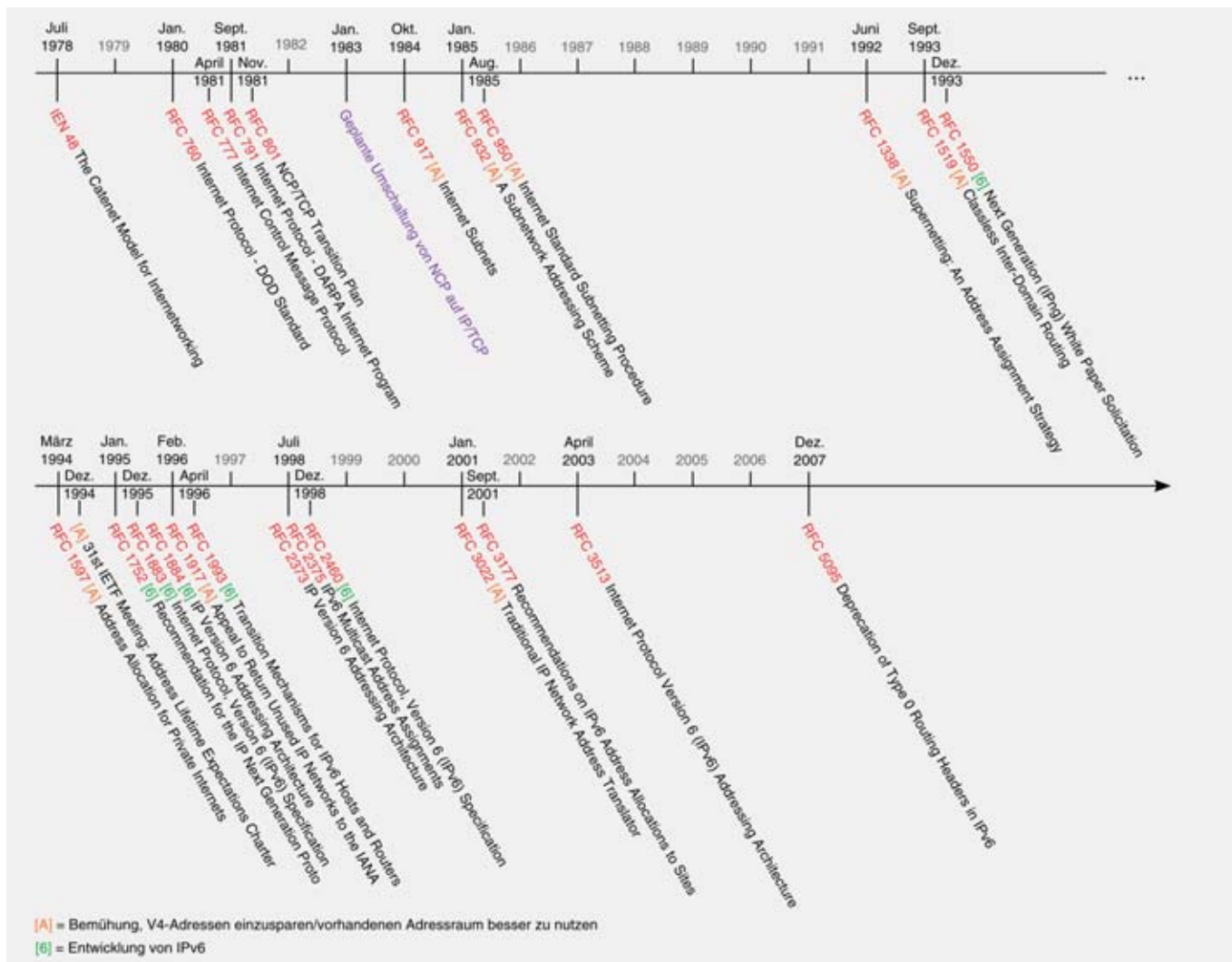


Bild 4: Die Entwicklungsstufen von IPv4 und IPv6. 1993 begann die IPv6-Entwicklung.

Diese Tatsache scheint jetzt auch bei den Zugangsanbietern ins Bewusstsein gerückt zu sein. Was für dramatische Folgen sie darin für sich erkennen, hat sich auf dem 78. Treffen der Internet Engineering Task Force (IETF) gezeigt. Der Internetanbieter COX Communications stellte dort mit der Veröffentlichung eines Internet-Drafts auch im Namen von AT&T und Warner Cable den Antrag, die IANA solle verpflichtet werden, einen der noch freien Adressblöcke für die private Nutzung zuzuteilen. Die Zugangsanbieter haben geplant, über diesen Block diejenigen Kunden mit Internet zu versorgen, die noch im Besitz von nicht-IPv6-fähigen Heimroutern sind. Diese Zugangsanbieter haben also offensichtlich noch bis vor Kurzem über die Existenz von IPv6 vollkommen hinweggesehen und Router

an ihre Kunden abgegeben, bei denen sich nicht einmal per Firmware-Update Unterstützung für IPv6 nachrüsten lässt.

Ein steiniger Weg

An IPv6 führt also kein Weg vorbei. Dennoch ist das Unterfangen, die Infrastruktur auf IPv6 umzustellen, sehr anspruchsvoll. Es sind nicht nur die Endbenutzer, deren Betriebssysteme v6-fähig gemacht werden müssen (eine eher leichte Übung), sondern vielmehr deren umfangreiche Client-Anwendungssoftware sowie die gesamte Infrastruktur auf Provider- und Backbone-Seite. Hier sind nicht nur die Einwahlknoten, Router und Server zu nennen, sondern auch vitale Komponenten wie Firewalls oder für den Geschäftsbetrieb unerlässliche Erfassungsmaßnahmen wie Traffic-Accounting

sind von der Umstellung betroffen. Im kleineren Maßstab betrachtet fallen die Millionen von SOHO-DSL-Routern (Small Office/Home Office) ins Auge, die die Provider ihren Kunden zuschicken – auch diese Geräte müssen in Zukunft IPv6 unterstützen. Neben den reinen Kosten, die die Wirtschaft als Grundinvestition in eine neue Netzinfrastruktur zu tragen hat, stellen sich auch einige (teilweise bereits gelöste) Probleme auf der Software-Seite, von denen hier exemplarisch einige besprochen werden sollen.

Spezialsoftware und Branchenlösungen

Besonders betroffen werden bei der Umstellung auf IPv6 diejenigen Softwarepakete sein, die ohne große Berücksichti-




gung modularer Programmierkonzepte gestrickt wurden oder die über viele Jahre gewachsen sind. Hier wurde meist wenig Wert auf Abstraktion bei der Behandlung von Netzwerkadressen gelegt. Verantwortlich dafür ist unter anderem die Tatsache, dass die IP-Adress-Arithmetik auf 32 Bit-Hardware eher noch an Komplexität gewinnt, wenn sie abstrahiert wird. Da IPv4-Adressen 32 Bit groß sind, lassen sich ohne Probleme Berechnungen an und mit ihnen durchführen. Auch die Übergabe von IP-Adressen an Unterprogramme erfolgt als 32 Bit-Integer und könnte aus Programmierersicht nicht einfacher sein.

Soll ein solches Programm mit Unterstützung für IPv6 versehen werden, kann es allerdings sehr schnell zu einem Minenfeld mutieren. Zur Verarbeitung von IP-Adressen reicht ein einfacher Integer-Datentyp nicht mehr aus. Stattdessen kommt eine Datenstruktur zur Anwendung. Als Folge davon muss für IP-Adres-

sen also Speicherplatz explizit zugewiesen und irgendwann auch wieder freigegeben werden. Letzteres wird sogar bei neuen Implementierungen hin und wieder vergessen und führt zu den gefürchteten sogenannten Memory Leaks, also zu Programmen, die während ihrer Laufzeit immer mehr und mehr Speicher belegen und nie wieder schrumpfen.

An jeder Stelle im Code, wo eine Parameterübergabe erfolgt, muss abgeklärt werden, ob sich durch das aufgerufene Unterprogramm im Zuge von Berechnungen die Adresse verändert. Dann muss nämlich an der richtigen Stelle eine Kopie der Adresse angefertigt werden. Bei der Übergabe einer IPv4-Adresse in Form eines Integer-Wertes sind Überlegungen dieser Art nicht notwendig, da als Folge der Übergabeart automatisch immer eine Kopie angefertigt wird und kein Speicher extra angefordert werden muss. Nachträglich um IPv6 erweiterte und damit also derartig verbesserte Software funktioniert dann meist und der

Benutzer bekommt davon nichts mit. In punkto Fehleranfälligkeit und Wartbarkeit ist allerdings mit derartiger Software kein Blumentopf zu gewinnen.

Im zweiten Teil unserer Serie lesen Sie, welche Neuerungen IPv6-Adressen mitbringen und wie sich Adresskollisionen vermeiden lassen. (dr) 

- [1] ICANN-Pressmitteilung
<http://it-a.eu/aap91>
- [2] Freie IPv4-Adressblöcke
<http://it-a.eu/aap92>
- [3] Hochrechnung zur IPv4-Vergabe
<http://it-a.eu/aap93>
- [4] Wikipedia-Liste der zugeteilten IPv4-Adressen
<http://it-a.eu/aap94>
- [5] Adresszuteilung nach Regionen
www.internetworldstats.com/stats.htm
- [6] Präsentation zur reibungslosen Migration auf IPv6
<http://it-a.eu/aap96>

Links 

VMgoes2010

berlin · düsseldorf · wien · münchen · frankfurt

02.11 04.11 09.11 17.11 23.11

VIRTUALISIERUNG • CLOUD COMPUTING • TRENDS 2011

Virtualisierung ist eine bewährte Technologie, die unsere heutige IT-Landschaft mit zunehmender Geschwindigkeit verwandelt und grundlegend die Art und Weise von IT-Organisationen und deren Nutzung von Ressourcen verändert.

VMgoes2010 ermöglicht Ihnen direkten Zugriff auf qualitativ hochwertige Inhalte zum Thema Cloud-Infrastruktur und Cloud Computing sowie Zugang zu den führenden Anbietern aus den Bereichen Virtualisierung und Cloud Computing. Das Angebot der Vorträge umfasst Themen wie die Lösung von Virtualisierungsherausforderungen vom Desktop über das Rechenzentrum bis hin zum Cloud Computing und 'IT as a Service.' Die Veranstaltungsreihe richtet sich an mittelständische sowie größere Unternehmen und Organisationen des öffentlichen Dienstes.

VMgoes2010 integriert VMware Vorträge und Beiträge führender Anwender virtualisierter IT-Lösungen. Weiterhin erwarten Sie Breakout Sessions unserer Sponsoren, eine offene Diskussionsrunde sowie eine Live-Demonstration zum Abschluss des Tages.

Melden Sie sich noch heute mit Promocode: V9M10 an, um sich Ihren Platz zu sichern.

www.vmgoes2010.com

Platin Sponsor: 

Sponsorship Kontakt:
VMgoes2010@angelbcl.co.uk

Gold+ Sponsoren*



Gold Sponsoren*



Silber Sponsoren*



*Bitte beachten Sie, dass pro Veranstaltung unterschiedliche Sponsoren vor Ort sein werden. Detaillierte Informationen zu den einzelnen Standorten finden Sie auf unserer Webseite



Drucken im Netzwerk (2)

Drucker in Reih und Glied

von Thomas Bär

Im zweiten Teil unserer Workshopserie zum Thema Drucken werfen wir einen genaueren Blick auf das Druckermanagement mit Bordmitteln von Microsoft Windows. Wir erklären, wie Sie dabei auf Gruppenrichtlinien zurückgreifen und dem Anwender durch eine sinnvolle Benennung der Ausgabegeräte das Leben einfacher machen. Außerdem verdeutlichen wir anhand von Beispielen, wie Sie sich mittels WMI und VBS-Skripten die Arbeit beim Druckermanagement erleichtern.

Ein lokal installierter Drucker unter Microsoft Windows steht automatisch allen Benutzern des Computers zur Verfügung. Sollen Drucker an anderen Rechnern, etwa an Windows-Printservern, zum Einsatz kommen, so wird eine benutzerbezogene Verbindung eingerichtet. Dazu verwendet der Benutzer entweder den Dialog "Drucker suchen" von Windows oder spricht den Drucker über den UNC-Pfad in der Form `\\{SERVERNAME}\{FREIGABENAME}` an. Windows sorgt dann selbstständig dafür, dass die entsprechenden Treiber installiert werden. Sind auf dem Windows-Printserver die Druckdienste für Unix (LPD) aktiviert und installiert, so ist möglicherweise auch deren Verwendung auf dem Client-Computer eine Option. Die Verwendung des "neuen" LPR-Anschlusses steht, wie ein lokal installierter Drucker, allen Benutzern auf dem Computer zur Verfügung. Der Befehl `con2prt` aus dem Windows Resource Kit eignet sich für das Verbinden oder Trennen von Netzwerkdruckern in Skripten, beispielsweise dem Anmeldeskript.

Drucker per Gruppenrichtlinie verteilen

Das Drucksystem von Windows lässt sich insgesamt mit den Eigenschaften robust, leistungsfähig und wenig attraktiv beschreiben. Erst seit Server 2008 verfügt das Betriebssystem über eine zentrale Konsole, mit der sich alle Drucker von einer Stelle aus verwalten, hinzufügen oder entfernen lassen. Sogar die seit Jahren geforderte Möglichkeit, die Anzeige von Druckern mit Filtern zu begrenzen, haben die Entwickler umgesetzt. Das interessanteste Feature des Druckerservers ist jedoch die Weiterentwicklung der Fähigkeit, Drucker über Gruppenrichtlinien bereitzustellen. Bevor jedoch die Neuerungen überhaupt nutzbar sind, müssen Sie diese durch die Installation der Serverrolle "Druck- und Dokumentendienste" erst installieren.

Die Druckverwaltung des Servers listet alle Drucker in der Fenstermitte auf. Im Kontextmenü des Druckers ist der Befehl "Mit Gruppenrichtlinie verteilen..." zu finden. Alle Benutzer und alle Computer, für die eine ausgewählte Richtlinie angewendet wird, werden automa-

tisch mit dem gewählten Drucker verbunden. In einer Umgebung mit Windows XP-Clients sei auf das Tool `PushPrinterConnections.exe` hingewiesen, das zum Lieferumfang des Servers gehört. Eine detaillierte To-Do-Anleitung bietet Microsoft im TechNet unter [1].

Die Zuordnung von Druckern, unabhängig davon, an welcher Arbeitsstation sich ein Benutzer anmeldet, ist auch ohne Active Directory (AD) oder Anmelde-Skripte realisierbar. Üblicherweise verwenden Administratoren in Windows-Umgebungen das Active Directory für beinahe alle Verwaltungsaufgaben. Es gibt jedoch Szenarien, in denen Administratoren auf die Nutzung des AD für die Zuordnung von Druckern verzichten müssen – beispielsweise in Umgebungen, in denen sie schlicht nicht über das Recht zur Modifikation und Anlage von Gruppenrichtlinien-Objekte (GPOs) verfügen. Grundsätzlich ist eine Vielzahl von Druckerinformationen, beispielsweise Treiber und Anschlüsse, maschinenweit gespeichert. Diese Informationen stehen also allen angemeldeten Benutzern auf der Maschine gleichermaßen zur Verfügung. Netzwerkdrucker-Informationen

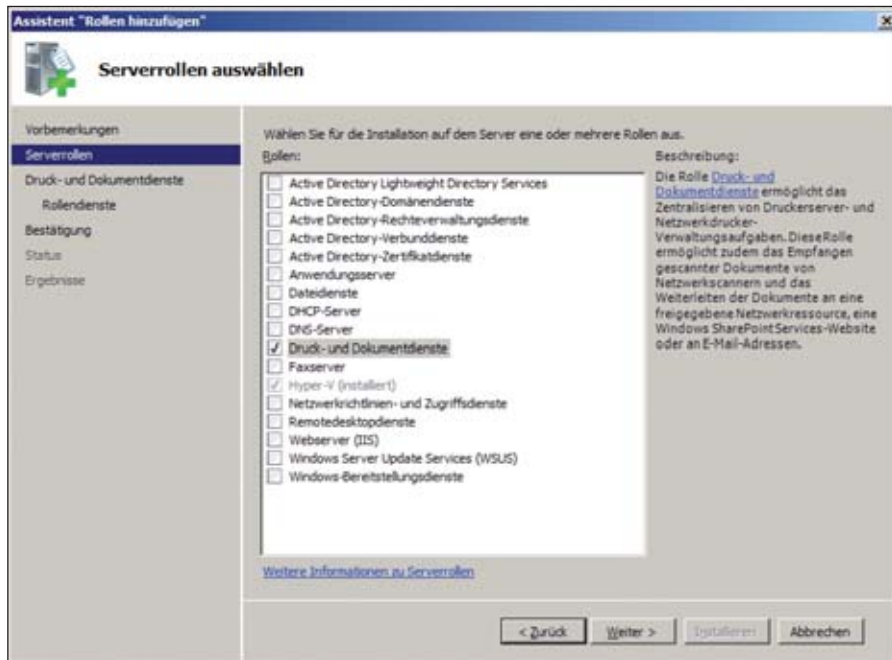


Bild 1: Windows Server 2008 bietet die seit Jahren von Administratoren geforderte zentrale Verwaltungsoberfläche für Drucker. Soll sie verwendet werden, so ist sie zunächst als Rolle zu installieren.

werden jedoch im Benutzerkontext gespeichert. Dies hat zur Folge, dass Netzwerkdrucker durch jeden Benutzer individuell ausgewählt und verbunden werden können und müssen.

Sinnvolle Druckerbenennungen wählen

Ein für den Anwender nützlich Benennungsschema zu erstellen, ist ein sehr wichtiger Schritt – kryptische Bezeichnungen, wie sie von Administratoren manchmal vergeben werden, haben den Nachteil, dass es dem Benutzer schwerfällt, sich eigenständig einen Drucker zuzuordnen. Eine Möglichkeit der Kennzeichnung besteht darin, die Drucker schlicht mit Hilfe eines Aufklebers zu beschriften. Beispielsweise “Personalabteilung – vertraulicher Drucker” oder “Drucker Raum 5”. Sinnvollerweise arbeiten Sie spezifische Merkmale wie “Farbdrucker” oder “Gesicherter Drucker” in die Namenskonvention ein. Besteht diese Möglichkeit nicht mehr, so empfiehlt es sich die Attributfelder “Standort” und “Kommentar” zu nutzen, um dem Anwender die Identifikation eines Druckers so einfach wie möglich zu gestalten. Da beide Attributfelder in den Dialogfenstern von Windows angezeigt werden, sind die dort hinterlegten

Informationen meist sehr hilfreich. Ein gutes Benennungsschema vereinigt alle benötigten Informationen wie Ort, Funktion und Abteilung bereits im Namen. Beispiele für sinnvolle Bezeichnungen sind “Haus50-Raum100-Farbdrucker” oder “Raum300-KundenService”.

Selbst wenn ein Benennungsschema eher kryptischer Natur ist, so empfiehlt es sich, den Benutzer mit an Bord zu holen und aus der Logik der Bezeichnung kein Geheimnis zu machen. Ist das Schema in sich stimmig durchgehalten worden, so ist es ein Leichtes, den Benutzer darüber in Kenntnis zu setzen.

Den richtigen Drucker finden

Nach dem Benennungsschema folgt der Blick auf die zur Verfügung stehenden Möglichkeiten der Druckerverbindung. Die am weitesten verbreitete Methode der Druckerverbindung ist der Assistent “Drucker hinzufügen”. Der Aufruf geschieht bei Windows XP / 2003 über den Dialog “Drucker und Faxgeräte” und bei Vista / 7 im Dialogfeld “Drucker und Geräte”. Die drei Methoden zur Auswahl eines Netzwerkdruckers sind die Suche im Verzeichnis, die Eingabe eines UNC-Pfa-

des und die Eingabe einer Drucker-URL. Welche der drei Möglichkeiten sich für Benutzer am besten eignet, hängt davon ab, inwieweit das Schema bekannt und wie viel Grundlagenwissen über Windows im Allgemeinen vorhanden ist.

In größeren AD-Strukturen werden Anwender zunächst das Verzeichnis nach Druckern durchsuchen, sofern sie anhand des Namens Rückschlüsse auf dessen Position ziehen können. Wird der Suchdialog gestartet, so erscheinen, in Abhängigkeit zu den gewählten Suchkriterien und der Anzahl vorhandener Drucker im Unternehmen, womöglich tausend oder mehr Drucker im Ergebnisfenster. Sinnvollerweise wird das Ergebnis durch die Eingabe von Teilen der Druckerbezeichnungen, beispielsweise “Farb”, von vornherein reduziert. Durch einen Doppelklick auf den gewünschten Drucker oder durch die Bestätigung der Schaltfläche “OK” kommt die eigentliche Druckereinrichtung auf der Workstation ins Rollen.

Ist den Anwendern der Name des gewünschten Printservers bekannt, so ist die einfachste Vorgehensweise bei der Druckzuordnung die Auswahl über die Eingabe der UNC-Bezeichnung. In diesem Fall ist im Dialogfenster “Drucker angeben” die zweite Option zu wählen. Jedoch ist die Eingabe der vollen Bezeichnung des Printservers vonnöten. Das UNC-Format benennt Druckerschlangen gemäß dem Schema `\\{PRINTSERVERNAME}\{FREIGABENAME}`. Somit würde ein Drucker aus dem obigen Beispiel wie folgt benannt: `\\MeinPrintServer\Raum100-Farbdrucker`. Wurden im Vorfeld bereits Drucker über UNC mit der Workstation verbunden, so schlägt Windows die bereits bekannten Printserver vor, sobald der Nutzer einen Backslash eingibt. Nach der Eingabe des Namens des Printservers vergeht nur ein kurzer Augenblick, ehe Windows alle an dieser Maschine freigegebenen Drucker in einer Auswahl anzeigt. Die genaue Bezeichnung des Druckers ist für diese Methode somit zweitrangig. Durch einen Mausklick auf



“Weiter” und die Beantwortung der Frage, ob es sich bei diesem Drucker nun um den unter Windows zu verwendenden Standarddrucker handelt, ist das Drucker-Mapping über UNC abgeschlossen.

Die dritte Methode der Netzwerkdrucker-Verbindung setzt voraus, dass “Internet Printing” generell aktiviert wurde. In diesem Fall besteht die Möglichkeit, das Drucker-Mapping über die Eingabe einer URL, beispielsweise `http://MeinPrintServer/Printers/Raum100`, durchzuführen. Um die URL-Variante zu wählen, ist im Dialogfenster “Drucker angeben” die dritte Option auszuwählen. “Internet Printing” unter Windows funktioniert nur dann, sofern auf dem Printserver ein Microsoft IIS (Internet Information Server) installiert und aktiviert ist.

Abkürzung über öffentliche Verknüpfungen

Ob die hier genannten Basismöglichkeiten von Windows für die Druckerzuordnung wirklich nutzbar sind, hängt davon ab, ob Benutzer in der Lage sind, die Dialogfenster zu bedienen. Aber es geht auch einfacher: über das typischerweise existierende Gruppenlaufwerk zur Ablage gemeinsamer Dateien. In diesen Ordnern finden sich gemeinsam benötigte Dokumente oder Vorlagen, die beinahe von jedem Mitarbeiter der Abteilung geöffnet werden dürfen. Unabhängig von den sonstigen EDV-Kenntnissen der Benutzer finden diesen Ordner meist doch alle. Es liegt also nahe, die Freigaben der Drucker in eben diesem Ordner abzulegen.

Um eine Verknüpfung in dem Ordner zu erzeugen, bedarf es lediglich ein paar Klicks im Windows Explorer. In einem Fenster öffnen Sie den allgemeinen Ordner selbst, ein weiteres Fenster zeigt das Dialogfenster “Drucker und Faxgeräte” mit den Freigaben auf dem gewünschten Printserver. Wird ein Icon aus dem Fenster mit den Freigaben in das Ordnerfenster gezogen, so ist nach dem Loslassen der Maustaste lediglich der Eintrag “Verknüpfung hier erstellen” auszuwählen. Die

Berechtigungen der Freigabe sind im Kontextmenü “Eigenschaften” zu prüfen. Wie gewöhnlich benötigen Benutzer die Berechtigungen “Lesen” und “Ausführen”.

Je nachdem, wie viele Printserver sich in einem Unternehmen finden, ist dieser Vorgang einige Male zu wiederholen. Verwenden die Drucker spezifische Treiber, so folgt möglicherweise der entsprechende Dialog zur Installation dieser Komponenten. Es empfiehlt sich, dieses Verfahren unter Verwendung der generischen Microsoft-Treiber durchzuführen, da diese in beinahe allen Windows-Varianten zur Verfügung stehen. Anschließend gilt es, die Benutzer über diese neue Bereitstellung von Druckern zu informieren. Wird der Ordner durch den Anwender geöffnet, so ist der gewünschte Drucker mit einem Rechtsklick anzuklicken und im Kontextmenü der Eintrag “Verbinden” zu wählen. Fehlt das Kommando “Verbinden” im Kontextmenü, so ist der Drucker bereits mit der Maschine verbunden.

Druckerparametrierung mit WMI und VBS

Mit Hilfe von Visual Basic Scripts (VBS) und Windows Management Instrumentation (WMI) lässt sich die Steuerung von Druckern unter Microsoft Windows elegant gestalten. Insgesamt drei WMI-Klassen kommen für das Management von Druckern und Druckaufträgen zum Einsatz. Druckaufträge werden in der Klasse “Win32_PrintJob” abgebildet, “Win32_Printer” symbolisiert den installierten Drucker und die Klasse “Win32_PrinterConfiguration” repräsentiert die Konfigurationseinstellungen eines Druckers, auch auf x64-Windows Computern. Allein die als Alias “Printer” bezeichnete Klasse “Win32_Printer” liefert mehr als fünfzig lesbare und rund dreißig änderbare Eigenschaften. Windows-Versionen vor XP / 2003 sind nur bedingt in der Lage, die WMI-Funktionen korrekt umzusetzen. Da Microsoft den Support für NT4 / 2000 und 9x bereits eingestellt hat, berücksichtigen wir diese Versionen hier nicht mehr.

Auf WMI lässt sich per Visual Basic Script oder mit dem Kommandozeilenbefehl `WMIC.EXE` zugreifen. Das Werkzeug bietet auch in Zeiten der PowerShell den Vorteil, dass es sich selbst in einfachste Batch-Jobs einbinden lässt und faktisch auf allen Systemen zur Verfügung steht. WMIC lässt sich sowohl als Standard-Befehl als auch interaktiv verwenden. Die hier gezeigten Kommandos sind stets in sich abgeschlossen und lassen sich so sehr einfach in Batch-Jobs integrieren. Sollen alle Drucker des Computers ausgegeben werden, so verwenden Sie in der Eingabeaufforderung den Befehl

```
WMIC Printer GET Name
```

WMIC erlaubt eine Eingrenzung mit einer SQL-ähnlichen Syntax, dem so genannten WQL. Sollen beispielsweise nur die Drucker angezeigt werden, deren Namen mit L beginnt, so greifen Sie auf folgendes Kommando

```
WMIC Printer WHERE "Name like 'L%'"
GET Name
```

zurück. Um alle Eigenschaften eines Druckers auszugeben, wenden Sie den Get-Befehl nicht auf eine spezielle Eigenschaft wie “Name” an, sondern setzen den Schalter “/VALUE” ein:

```
WMIC Printer "{DRUCKERNAME}" GET
/VALUE
```

Das Ergebnis ist die Ausgabe aller Eigenschaften zu einem spezifizierten Drucker. Mit Hilfe des Konsolenbefehls WMIC lassen sich auch entfernte Drucker ansprechen. Der Schalter “/NODE:” bezeichnet den Computernamen des Zielsystems. Mehrere Computernamen lassen sich mit Komma getrennt angeben oder mit “@filepath” eine Datei bezeichnen, aus der die Zielrechnerbezeichnungen ausgelesen werden sollen. Die Schalter “/USER” und “/PASSWORD” verwenden Sie dabei im Format “Domäne\Konto” oder “Computer\Konto”, um in eine andere Rolle für den Zugriff zu schlüpfen:



```
WMIC /NODE:{NAME}
  /USER:{DOMÄNE\USER}
  /PASSWORD:{Passwort} Printer GET
  Name
```

Die Verwendung von Benutzer und Passwort öffnet jedoch eine nur wenig bekannte Sicherheitslücke von Windows XP und Server 2003: Fehlgeschlagene WMIC-Befehle werden standardmäßig in einem Logfile namens %SYSTEMROOT%\SYSTEM32\WBEM\LOGS\WMIC.LOG protokolliert. Unterläuft ein Fehler beim Ablauf, so wird das Passwort des administrativ berechtigten Benutzers in der Protokolldatei gespeichert. Um dies zu umgehen, empfiehlt sich die Deaktivierung des Protokolls. In der Computerverwaltung ist dazu das Kontextmenü der WMI-Steuerung zu öffnen und im Register "Protokollierung" die Protokollierungsstufe auf "Deaktiviert" zu setzen. Der Befehl

```
WMIC /node:{Rechnername} Printer GET
  Drivename, Name
```

zeigt alle Drucker mit den Treiberinformationen eines entfernten Rechners an. Das Umbenennen eines Druckers realisieren Sie mit folgendem Kommando:

```
WMIC Printer "{alter Druckername}"
  RenamePrinter "{neuer Drucker-
  name}"
```

Wird der "ReturnValue" als "0" zurückgegeben, so war die Durchführung des

Befehls erfolgreich. Sollen alle auf dem Server verfügbaren Drucker auf einen Schlag in den Pause-Modus versetzt werden, so lässt sich dies mit

```
WMIC Printer Where Name!=NULL Pause
```

bewerkstelligen. Mit "Resume" anstelle von "Pause" aktivieren Sie alle Drucker wieder. Mit "CancelAllJobs" löschen Sie alle Druckaufträge der Maschine mit einem Befehl. Mit folgendem Kommando können Sie einen bestimmten Drucker komplett löschen:

```
WMIC Printer {Druckername} delete
```

WMI und VB-Script als perfektes Duo

Nicht nur mit Hilfe der PowerShell von Windows lassen sich viele Parameter verändern oder Informationen auslesen. Auch über VB-Skripts lässt sich WMI sehr elegant nutzen. Wird in der ersten Zeile des unten stehenden Skripts der Variable "strComputer" anstelle des Punktes, dem Zeichen für den lokalen Rechner, eine IP-Adresse oder der Na-

me eines entfernten Systems angegeben, so werden die Drucker mit der Bezeichnung der Freigabe für diesen Rechner angezeigt. Das Skript, abgespeichert mit der Dateinamenerweiterung .VBS, starten Sie entweder per Doppelklick oder über die Eingabeaufforderung mit `CSCRIPT {DATEINAME}.VBS`.

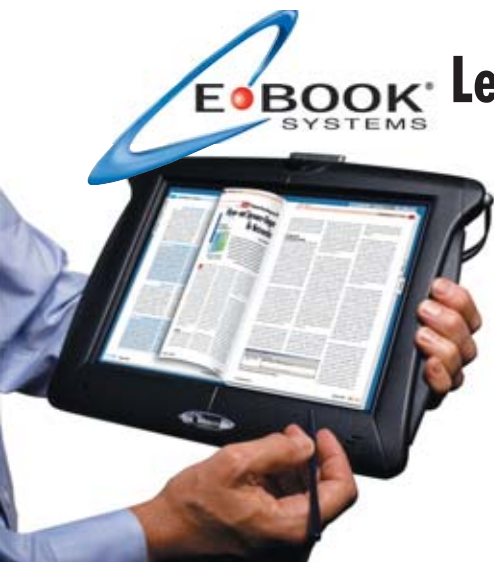
```
strComputer = "."
Set objWMIService = GetObject _
  ("winmgmts:\\." & strComputer &
  "\root\cimv2")
Set colPrinters =
  objWMIService.ExecQuery _
    ("select * From Win32_Printer")
For Each objPrinter in colPrinters
  wscript.Echo objPrinter.Name & "
  - " & objPrinter.ShareName
Next
```

Ausgabe aller fehlerhaften Drucker

Setzen Sie im Unternehmen Windows-Maschinen als Printserver ein, so verliert sich ab einer gewissen Größe schnell die Übersicht über die Drucker und deren Status. Folgendes Skript zeigt alle Drucker

```
C:\Windows\system32\cmd.exe
C:\>WMIC Printer "DELL1320C735F08" RenamePrinter "Laserdrucker"
(\\SERVERS\ROOT\CIMV2:Win32_Printer.DeviceID="DELL1320C735F08")->RenamePrinter() wird ausgeführt
Methode wurde ausgeführt.
Ausgabeparameter:
Instance of _PARAMETERS
{
    ReturnValue = 0;
};
C:\>
```

Bild 2: Mithilfe des Kommandozeilen-Programms WMIC lassen sich Drucker erstellen, umbenennen, konfigurieren oder löschen – auch auf entfernten Computern



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





cker an, bei denen der Status auf "Error" gesetzt wurde – sprich, die nicht einsatzbereiten Geräte.

```
strComputer = "."
Set objWMIService = GetObject _
    ("winmgmts:\\\" & strComputer &
    "\\root\cimv2")
Set colPrinters =
    objWMIService.ExecQuery _
        ("Select * From win32_
        Printer where Status=
        'Error'")
For Each objPrinter in colPrinters
    Wscript.Echo objPrinter.ShareName
    & "<p>"
Next
Wscript.Echo date & " " & time &
    "</font><html>"
```

Mehr Übersicht durch HTML

Das Ergebnis lässt sich mit einfachen Bordmitteln in ein Intranet als HTML-Datei einbinden – beispielsweise durch einen Scheduler-Eintrag, der das Skript regelmäßig startet. Dazu erweitern Sie lediglich den Quellcode ein wenig:

```
strComputer = "."
Wscript.Echo "<html><body
    bgcolor='#FF0000'>"
Wscript.Echo "<font face='Arial'
    size=6 color='#FFFFFF'>"
Wscript.Echo "Folgende Drucker sind
    im Fehlerstatus :<p>"
```

Die Einrichtung eines neuen Druckers übernimmt ein Visual Basic Script mit der Methode "SpawnInstance_". Unbedingt zu beachten ist der Umstand, dass der unter "DriverName" benannte Druckertreiber auf dem System bereits vorhanden sein muss.

```
strComputer = "."
set objWMI = GetObject("winmgmts:\\\"
    & strComputer)
set objPrinter = objWMI.Get("win32_Printer").
    SpawnInstance_
with objPrinter
    .DriverName = "HP LaserJet 2200 Series PCL 5"
    .PortName = "LPT1:"
    .DeviceID = "Testdrucker"
    .Network = True
    .Shared = True
    .ShareName = "Test"
    .Comment = "Kommentar"
    .Put_
end with
Wscript.Echo "Drucker installiert."
```

Druckerinstallation mit WMI



```
Set objWMIService = GetObject _
    ("winmgmts:\\\" & strComputer &
    "\\root\cimv2")
Set colPrinters =
    objWMIService.ExecQuery _
        ("Select * From win32_
        Printer where Status=
        'Error'")
For Each objPrinter in colPrinters
    Wscript.Echo objPrinter.ShareName
    & "<p>"
Next
Wscript.Echo date & " " & time &
    "</font><html>"
```

Das Skript starten Sie so, dass keine Copyright-Bezeichnungen ausgegeben werden und das Ergebnis direkt in eine Datei umgeleitet wird. Ist das Skript als *SHOW-PRINTERERROR.VBS* abgespeichert, so lässt es sich beispielsweise über *showprintererror //NOLOGO > TEST.HTM* starten. Eingearbeitet in den Task-Scheduler mit einer Nennung des Zielsystems in der Variable "strComputer" kann so ein Intranetserver regelmäßig den Printserver prüfen.

Mit Argumenten an das Skript

Wie Batch-Dateien lassen sich VB-Skripts mit Argumenten aufrufen. So ließe sich beispielsweise der Name eines zu analysierenden Rechners per Argument an das Skript übergeben. Leider reagiert VB-Skript nicht sonderlich hübsch auf fehlende Argumente, darum muss zunächst auf die Existenz eines Arguments hin geprüft werden. Das folgende Skript gibt alle Drucker auf einem Printserver aus, bei denen die Priorität gegenüber dem Standardwert "1" erhöht wurde. Der Aufruf geschieht über {Skriptname} {Rechnernamen};

```
Set objArgs = Wscript.Arguments
if objArgs.Count > 0 then
    strComputer = cstr(objArgs(0))
Set objWMIService = GetObject _
    ("winmgmts:\\\" & strComputer &
    "\\root\cimv2")
Set colPrinters =
    objWMIService.ExecQuery _
        ("Select * From win32_Printer
        where priority > 1")
```

```
Wscript.Echo "Erhöhte Priorität
    entdeckt:"
For Each objPrinter in colPrinters
    Wscript.Echo objPrinter.Share-
        Name & " Priorität : " &
        objPrinter.Priority
Next
else
Wscript.Echo "Kein Zielcomputer
    spezifiziert (IP/NetBIOS-Name) !"
end if
```

Natürlich lässt sich auch mit WMI eine Drucker Verbindung zu einer Freigabe auf einem Printserver einrichten:

```
strComputer = "."
Set objWMIService = GetObject( _
    "winmgmts:{impersonationLevel=
    Impersonate}!\" & _strComputer
    & "\\root\cimv2")
Set objPrinter =
    objWMIService.Get("win32_Printer")
errReturn = objPrinter.AddPrinter-
    Connection _
        ("\\{PRINTSERVER}\{FREIGABE}")
```

Den kompletten Leistungsumfang und die Methode von WMI in einem Artikel zu beschreiben, würde den Umfang bei Weitem sprengen. Zur schnellen Übersicht sei auf das Tool *%SYSTEMROOT%\SYSTEM32\WBEM\wbemtest.exe* und auf einen Microsoft-TechNet Artikel unter [2] hingewiesen. Im nächsten Teil unserer Druck-Serie betrachten wir die erweiterten Features von Drittherstellern und widmen uns dem treiberlosen Druck in Terminalserver-Umgebungen. Außerdem beantworten wir die Fragestellung, wie sich alle Ausdrücke im Unternehmen in Dateien protokollieren lassen. (In)

- [1] Microsoft TechNet – Bereitstellen von Druckern mithilfe der Gruppenrichtlinie <http://it-a.eu/aap01>
- [2] Microsoft TechNet – Scripting-Handbuch WMI <http://it-a.eu/aap02>

Links



Kompetentes Schnupperabo sucht neugierige Administratoren

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

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

Damit Sie sich Zeit,
Nerven und Kosten sparen.

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

6

**Monate
lesen**

3

**Monate
bezahlen**



www.it-administrator.de

 **Heinemann Verlag**
Im Dialog mit Spezialisten.

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München
Tel: 0049-89-4445408-0
Fax: 0049-89-4445408-99
info@heinemann-verlag.de

Vertrieb, Abo- und Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville
Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de



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.



Wir nutzen Windows 7-Rechner als **öffentliche Terminals** für Internet-Zugänge im Unternehmen. Hierfür würden wir gerne **bei der Anmeldemaske unser Firmenlogo hinterlegen**. Wie kann ich das machen?

Es lässt sich neben dem Hintergrundbildschirm auch der Anmeldebildschirm anpassen. Mit Windows 7 steht Ihnen hierfür von Haus aus eine einfache Möglichkeit zur Verfügung, ohne dass Sie auf Tools zurückgreifen müssen. Prüfen Sie zunächst, ob in der Registry der DWORD-Wert "OEMBackground" unter "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Background" vorhanden ist. Falls nicht, legen Sie ihn an und setzen ihn auf "1", um ihn zu aktivieren. Nun ermitteln Sie das Größenverhältnis Ihres Bildschirms, indem Sie die Werte für die horizontale und vertikale Auflösung teilen – also beispielsweise 1280:800 = 1,6:1. Grundsätzlich werden die Bilder für die eigenen Anmeldemasken im Verzeichnis `%windir%\System32\oobe\info\backgrounds` gespeichert. Falls dieser Ordner fehlt, legen Sie ihn einfach an. Der Befehl `withinwindows` stellt Ihnen

eine Liste zur Verfügung, welche Dateien in diesem Ordner unterstützt werden. Das Seitenverhältnis steht in Klammern. Außerdem dürfen die Dateien maximal 256 Kilobyte groß sein:

- backgroundDefault.jpg
- background768×1280.jpg (0.6)
- background900×1440.jpg (0.625)
- background960×1280.jpg (0.75)
- background1024×1280.jpg (0.8)
- background1280×1024.jpg (1.25)
- background1024×768.jpg (1.33)
- background1280×960.jpg (1.33)
- background1600×1200.jpg (1.33)
- background1440×900.jpg (1.6)
- background1920×1200.jpg (1.6)
- background1280×768.jpg (1.66)
- background1360×768.jpg (1.770833)

Die Datei `backgroundDefault.jpg` wird dabei ohne Angabe eines Seitenverhältnisses geladen und gegebenenfalls gestreckt angezeigt. Hinterlegen Sie also Ihr gewünschtes Hintergrundbild in der passenden JPG-Datei und starten Sie das System neu. Sollte es zu einem unbekanntem Fehler mit dem eigenen Hintergrundbild kommen, lädt das System von sich aus die Datei `images-res.dll`. Dort ist der Standard-Anmeldebildschirm vorhanden, auf den zurückgegriffen wird. Neben der Client-Version von Windows 7 steht die Funktion auch beim Windows Server 2008 R2 zur Verfügung. (dr)

Nachdem wir in unserem Unternehmen von Server 2008 auf 2008 R2 migriert sind, gingen aus unerfindlichen Gründen unsere selbst konfigurierten **Sicherheits-einstellungen für WMI Namespaces verloren**. Dies hatte unter anderem zur Folge, dass keine auf Hyper-V basierende Remote-Verbindung mehr möglich war. Woran liegt dieses ominöse Verschwinden der zusätzlichen Settings?

Leider ist es so, dass der Upgrade-Prozess von Server 2008 auf Server 2008 R2 in Bezug auf die Sicherheitseinstellungen für WMI Namespaces nur die Default-Parameter berücksichtigt. Selbst erstellte Sicherheitsregeln bleiben außen vor. Ihnen bleibt also nur, die entsprechende Konfiguration vor dem Upgrade auf R2 zu dokumentieren und dann neu aufzusetzen. Etwas leichter können Sie sich die Arbeit machen, wenn Sie die Security-Settings exportieren. Dies geht am besten über die Kommandozeile mit den Operatoren `GetSecurityDescriptor` und `SetSecurityDescriptor`. Wie Sie diese genau einsetzen, erfahren Sie im Internet unter <http://it-a-eu/aape1/> beziehungsweise <http://it-a-eu/aape2/>. (ln)

Nachdem wir für die **Migration auf Server 2008 R2** einen neuen Rechner in Betrieb genommen haben, habe ich durch ein Robocopy-Skript die Dateien und Ordner samt Freigaben und Rechten auf

den neuen Rechner kopiert. Dies hat im Prinzip auch alles gut geklappt – bis auf ein Problem, das anscheinend die **NTFS-Berechtigungen** betrifft. Was nicht funktioniert, ist, dass manche Anwender auf ihre gemappten Laufwerke zugreifen können, obwohl von den Einstellungen her eigentlich alles passen müsste. Stattdessen erscheint die Fehlermeldung "Access Denied". Was könnte ich hier falsch gemacht haben?

Da wir Ihre genaue Vorgehensweise nicht kennen, können wir Ihnen nur ein paar allgemeine Tipps geben. Zunächst einmal sollten Sie unbedingt den Systemdienst "LanmanServer" neu starten. Geben Sie dazu am besten unter "Ausführen" das Kommando `cmd /c net stop lanmanserver && net start lanmanserver` ein. Der Dienst steuert in Windows-Systemen die Datei- und Druckerfreigaben. Über die Registry können Sie auch die eingestellten Sicherheitseinstellungen dieses Systemdienstes genauer unter die Lupe nehmen. Navigieren Sie dazu nach der Eingabe von `regedit` in das Verzeichnis "HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ services \ LanmanServer". Hier können Sie im Ordner "Shares" kontrollieren, ob die Freigaben auch richtig gesetzt sind. (In)



Beim Zugriff mittels **Outlook Web Access** halte ich es für ziemlich unpraktisch, dass Anwender, deren Passwort abgelaufen ist, **keine Möglichkeit haben, selbständig ein neues Kennwort zu wählen**. Nun habe ich gehört, dass Exchange 2010 SP1 und 2007 SP3 genau dieses Feature implementiert hat. Ich weiß allerdings nicht wie. Können Sie mir sagen, wo ich die Option aktiviere?

In der Tat sehen die jüngsten Service Packs für Exchange 2007 und 2010 eine Funktion vor, die es Nutzern mit abge-

laufenem Passwort erlaubt, ein neues zu wählen. Diese Option müssen Sie in der Registry jedoch erst aktivieren. Öffnen Sie dazu auf dem Client Access Server mit `regedit` die Registrierungsdatenbank und navigieren Sie zum Eintrag "HKLM \ SYSTEM \ CurrentControlSet \ Services \ MExchange OWA". Klicken Sie hier mit der rechten Maustaste auf den Eintrag "MExchange OWA" und erstellen Sie einen neuen DWORD-Wert (32-Bit). Diesen Eintrag nennen Sie "ChangeExpiredPasswordEnabled" und geben ihm den Wert "1". Nun müsste bei abgelaufenem Passwort eine neue Wahl möglich sein. Mit dem Streichen des Eintrags oder dem Wert "0" machen Sie diese Option wieder rückgängig. Beachten Sie allerdings, dass Sie diese Modifikation der Registry auf jedem Ihrer Client Access-Server durchführen müssen und dass danach ein Neustart der IIS nötig ist. Am schnellsten veranlassen Sie diesen mit dem Kommando `IISReset /noforce`. (In)



Die neuesten Service Packs ermöglichen unter Outlook 2007 und 2010 beim Zugriff mit OWA auch das Neusetzen von abgelaufenen Passwörtern.

Microsoft bietet für Exchange 2010 ja mittlerweile das **Service Pack 1 in der endgültigen Version** an. Da sich dieses Update wie auch schon die Beta-Version davon nicht wieder entfernen lässt, würde ich bei der Installation auf einem System mit Server 2008 R2 gerne auf Antrieb alles richtig machen. Ich habe jedoch gehört, dass das Betriebssystem **bestimmter Voraussetzungen bedarf**. Welches sind diese?

Wollen Sie das SP1 von Exchange 2010 auf einem Server mit Windows Server 2008 R2 installieren, müssen Sie vorher zunächst einige Patches herunterladen und installieren. Ohne diese Patches bricht der Installationsassistent mit einem Fehler ab. Die genannten Patches sind vor allem auf Servern mit der Clientzugriffrolle notwendig. Folgende Aufstellung zählt die benötigten Aktualisierungen auf. Unter den angegebenen Links finden Sie auch Weiterleitungen zu entsprechenden Patches für Windows Server 2008 x64:

1. KB982867 – WCF: Enable WebHeader settings on the RST/SCT.
Link: <http://it-a.eu/aape3/>
2. KB979744 – Hotfix 1 für Visual Studio und .NET.
Link: <http://it-a.eu/aape4/>
3. KB977020 – Hotfix 2 für Visual Studio und .NET.
Link: <http://it-a.eu/aape5/>
4. KB983440 – Win7 Rollup Package.
Link: <http://it-a.eu/aape6/>
5. Update zum Entfernen des Anwendungsmanifestablauf-Features von AD RMS-Clients.
Link: <http://it-a.eu/aape7/>

Achten Sie darauf, neben der 64 Bit-Version auch die entsprechende Variante für Windows Server 2008 R2 oder Windows 7 herunterzuladen. Teilweise tragen die Patches für Windows Server 2008 R2 die Bezeichnung Windows 6.1. Bei einigen Aktualisierungen ist es notwendig, den Server danach neu zu starten. (Thomas Joos/In)

Viele weitere Tipps & Tricks sowie konkrete Hilfe bei akuten Problemen bekommen Sie auch im Internet bei unserem exklusiven Foren-Partner [administrator.de](http://www.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](http://www.administrator.de) die Internetplattform für alle System- und Netzwerkadministratoren.





Wir nutzen den **VMware Virtual Infrastructure Client 3** und möchten gerne **Single Sign-On** auf unseren Windows-Rechnern ermöglichen. Wie können wir dies einrichten?

Der Virtual Infrastructure Client unterstützt seit Version 3.5U2 das Single Sign-On unter Windows. Allerdings ist diese Option nicht so leicht zu finden und lässt sich unter dieser Version nur über die Kommandozeile aktivieren. Mit der Installation wird auf dem Desktop normalerweise eine Verknüpfung zum VI-Client angelegt. In dieser passen Sie nun das Ziel wie nachfolgend aufgeführt an:

```
"C:\Programme\VMware\Infrastructure\Virtual Infrastructure Client\Launcher\vpclient.exe" -passthroughAuth -s {VI-Centerserver Name}
```

Nach dem Abspeichern genügt ein Doppelklick, um den VI-Client ohne separate Anmeldung am Centerserver zu starten. (dr)



Linux

Die meisten Linux-Distributionen verwenden ja die **Bash als Standard-Shell**. Der Prompt der Shell lässt sich dabei über die Variable **PS1** beziehungsweise **PS2** nach Belieben anpassen. So ganz klar ist mir der **Unterschied zwischen den beiden Variablen** allerdings nicht. Können Sie mir hier weiterhelfen?

PS1 steht für den Prompt, der erscheint, wenn die Shell bereit ist, ein Kommando auszuführen. PS2 tritt dann in Erscheinung, wenn die Shell auf weitere Eingaben des Benutzers wartet. Möchten Sie die aktuellen Einstellungen abfragen, so gelingt dies mit folgendem Kommando:

```
# echo $PS1
[\u@\h \w]$
```

beziehungsweise

```
# echo $PS2
>
Üblicherweise ist stets der PS1-Prompt sichtbar. PS2 kommt immer dann zum Tragen, wenn Sie beispielsweise ein Skript zeilenweise eingeben und nach jeder Zeile "Enter" drücken, ohne dass die Shell das Skript bereits erfolgreich ausführen kann. Ein Beispiel ist die bekannte for-Schleife:
for n in `seq 1 3`
> do
> echo $n
> done
1
2
3
```

Hier erscheint solange der PS2-Prompt, bis die Shell in der Lage ist, die Eingaben erfolgreich auszuführen. In der man-Page der Bash-Shell befindet sich im Abschnitt "PROMPTING" eine genaue Beschreibung der zur Verfügung stehenden "escaped Character", mit denen sich der Prompt anpassen lässt. Das obige Beispiel von PS1 würde das folgende Ergebnis liefern:

```
[tscherf@tiffany ~]$ (Thorsten Scherf/ln)
```



Tools

Die Netzwerkschicht (OSI-Schicht 3) ist die Heimat von **Routern und Layer-3-Switchen** beziehungsweise deren Protokollen. Der auch als Vermittlungsschicht bekannte Layer sorgt für das Schalten von Verbindungen und bei paketorientierten Diensten für die Weitervermittlung von Datenpaketen. Er leistet somit für die IT unverzichtbare Dienste, ist allerdings oft ein weißer Fleck auf der Security-Landkarte der Unternehmen. Selbst für versierte Netzwerker ist das **Testen auf mögliche Schwachstellen in Layer 3** äußerst komplex.

Das kostenlose Werkzeug **Loki** ist ein fortgeschrittenes **Tool zum Test der Layer 3-Sicherheit**, das vom Systemhaus ERNW anlässlich der Konferenz "Black Hat USA 2010" veröffentlicht wurde. Loki ist ein Python-Framework,

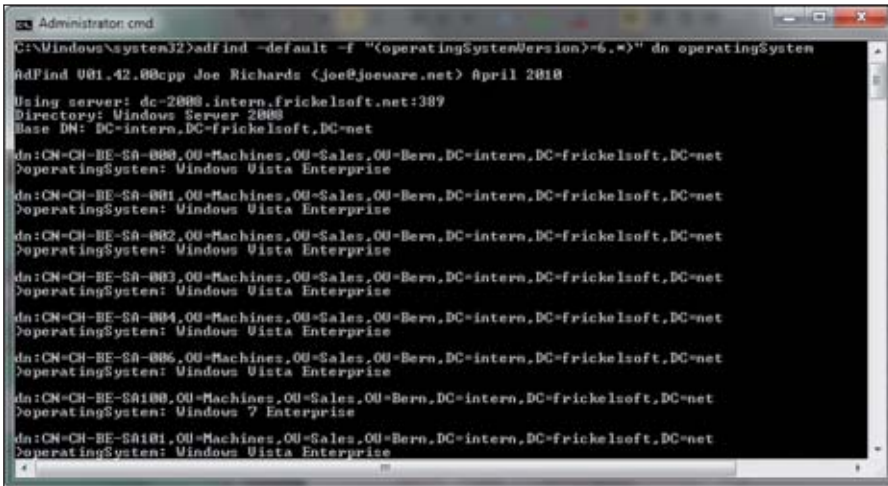
das Module zum Erzeugen von Paketen und Simulation von Angriffen auf Layer-3-Protokolle bereitstellt. Loki hilft so beim Finden von Schwachstellen, selbst solche, die bisher als eher theoretisch betrachtet wurden. Doch auch hier können heutzutage tatsächliche Gefahren lauern. Die Liste bereits unterstützter Protokolle und möglicher Sicherheitslücken beziehungsweise Angriffsmethoden ist lang:

- ARP (Address Resolution Protocol): ARP-Spoofing, -Scanning, -Flooding
- BFD (Bidirectional Forwarding Detection): DoS-Angriffe auf laufende Sessions
- BGP (Border Gateway Protocol): NLRI-Injection (Network Layer Reachability Information)
- HSRP, HSRPv2 (Hot Standby Router Protocol): Übernahme von IP-Adressen
- LDP (Label Distribution Protocol): Einschleusen von Label-Mapping-Nachrichten
- MPLS (Multiprotocol Label Switching): Überschreiben von MPLS-Labels, MPLS-VPN-fähiger Netzwerkstack
- OSPF (Open Shortest Path First): Einschleusen von LSA-Paketen (Link State Acknowledgement), Brechen der MD5-Authentifizierung
- RIP (Routing Information Protocol): Einschleusen von Routen
- VRRP, VRRPv3 (Virtual Router Redundancy Protocol): Übernahme von IP-Adressen

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



ADFind durchsucht das Verzeichnis und gibt die gewünschten Attribute zu jedem Objekt aus

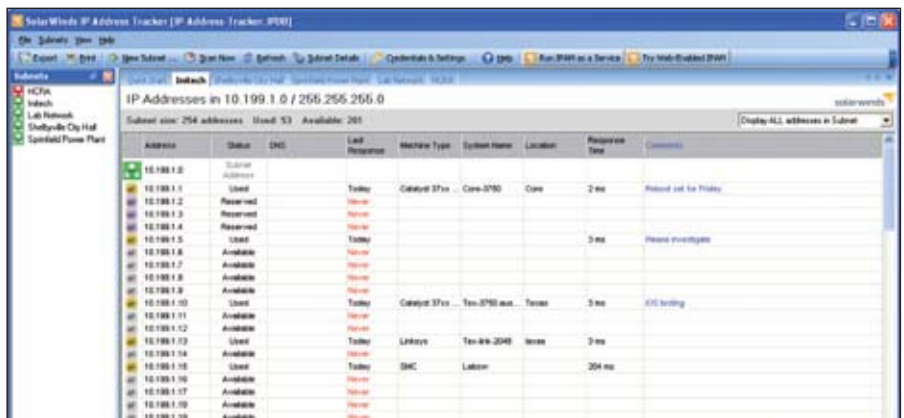
Dieses wirklich sehr fortgeschrittene Tool sollten nur erfahrene Netzwerk-Admins zu Testzwecken einsetzen und im Zweifelsfall mit dem Hersteller in Kontakt treten. (jp)
 Quelle: http://ermw.de/content/e6/e180/index_eng.html

Für die Administration des **Active Directory** stellt Microsoft neben der GUI auch Kommandozeilenprogramme bereit. Für Massenoperationen am Active Directory sind dabei die DS-Tools erste Wahl. Doch diese Tools erwarten gewisse Voraussetzungen der AD-Infrastruktur und stoßen bei manchen Aufgaben auch an Ihre Grenzen. Zwei kostenlose Werkzeuge überwinden diese Hürden.

Hier ist von den beiden Tools **ADfind** und **ADmod** die Rede. ADFind gibt Netzwerkadministratoren ein kommandozeilenbasiertes Werkzeug in die Hand, das die Stärken bekannter AD-Tools wie ldapsearch und DSquery in einem schlanken Programm vereint. Es bietet darüber hinaus viele Zusatzfunktionen, die sich alternativ nur durch aufwändige Skripte realisieren ließen. Grundsätzlich dient **ADfind zum Suchen im Active Directory**. Auch eigene LDAP-Aufrufe lassen sich so anstoßen. Durch Piping ist es einzelnen AdFind-Instanzen möglich, untereinander zu kommunizieren. Das Filtern von Netzwerkteilnehmern nach bestimmten Kriterien, das Suchen nach einem bestimmten Rechner oder alle-

meine Statusabfragen werden so stark vereinfacht. Wohingegen **ADmod das Ändern von AD-Objekten** erheblich erleichtert. Die mit ADfind zuvor identifizierten Objekte lassen sich mit dem Tool als Massenoperation ändern. Ein dynamisches Duo also, das in keiner Active Directory-Toolsammlung fehlen sollte. (jp)
 Quelle: <http://joeware.net/freetools/index.htm>

Ein IP-Subnetz der C-Klasse umfasst 253 IP-Adressen, bei einem B-Klasse-Netz sind es dann 65.534 IP-Adressen. Eine **Dokumentation der IP-Adressen** im Unternehmen kann also leicht ausufern, was Zeit und Aufwand betrifft. Zum einen, was die eigentliche Pflege der Dokumentation (etwa in MS Excel) angeht, zum anderen auch, weil der Administrator sehr diszipliniert die Änderungen der IP-Adressen beobachten und erfassen muss.



Mit dem IP Adress Tracker lassen sich Subnetze komfortabel dokumentieren

Das freie Tool **IP Address Tracker** von Solarwinds **scannt IP-Subnetze** nach verwendeten Adressen und erleichtert dem Administrator die Arbeit deutlich. Das Werkzeug durchsucht vorgegebene Subnetze nach belegten beziehungsweise freien IP-Adressen. Außerdem ist das Tool in der Lage, über SNMP weitere Informationen (Maschinentyp, Systemname und Ort) zum Gerät abzufragen. Um ein Subnetz zum ersten Mal zu scannen, trägt der Administrator lediglich die IP-Adresse des Subnetzes und die zugehörige Maske ein. Nun muss nur noch ein Name für den Scan vergeben werden und schon tritt das Solarwinds-Tool seinen Dienst an. Hilfreich ist, dass sich die Anzahl der IP-Pings ebenso einstellen lässt wie der Abstand pro Adresse zwischen diesen Pings. Daneben gibt es noch einen Parameter für den Timeout der Pakete. Bei B-Klassen-Netzen mit vielen IP-Adressen hilft ein Filter, der nur solche IP-Adressen anzeigt, die auch tatsächlich im Gebrauch sind. Weiter kann sich der Administrator reservierte oder freie IP-Adressen anzeigen lassen. Der Klick auf eine einzelne IP-Adresse erlaubt, einen Ping, Telnet oder den Web-Browser mit der IP-Adresse zu starten. Dies ist praktisch, um beispielsweise per Browser das Administrations-Interface eines Netzwerk-Druckers aufzurufen. Wie immer bei Solarwinds erfordert der Download des kostenlosen Werkzeugs eine kurze Registrierung. (jp)
 Quelle: www.solarwinds.com



Quelle: Pixello.de

Accounting in virtuellen Umgebungen

Virtuelle Maut

von Patrick Schwanke

Virtuelle Umgebungen bieten zahlreiche Vorteile und halten daher in immer mehr Unternehmen Einzug, führen aber immer öfter auch zu einem "Wildwuchs" virtueller Maschinen. Solche VMs bergen zahlreiche Risiken in Sachen Sicherheit, aber auch Wirtschaftlichkeit der IT. Diesen Risiken der Virtualisierung können IT-Organisationen durch eine stringente Abrechnung der Leistungen begegnen, die sich flexibel den jeweiligen Umgebungen anpassen lässt. Dieser Beitrag zeigt auf, welche Kosten bei der Abrechnung in Betracht gezogen werden müssen und auf welche Abrechnungsmodelle IT-Verantwortliche dabei zurückgreifen können.

Virtualisierung bietet die Möglichkeit, durch das Zusammenlegen mehrerer ehemals physischer Server auf eine einzige physische Maschine erhebliche Einsparungen bei den Betriebskosten zu realisieren. Außerdem sind Aufgaben wie Server-Provisionierung und Ressourcenzuteilung in virtuellen Umgebungen ungleich einfacher und zeitsparender zu realisieren.

Virtualisierung bildet zudem die Grundlage für zwei sehr wünschenswerte Eigenschaften einer heutigen IT-Infrastruktur:

- Agilität: VMs lassen sich in Minuten schnelle und für die Benutzer transparent zwischen physischen Rechnern verschieben, um schnell oder sogar proaktiv auf Lastspitzen zu reagieren und somit eine gleichbleibende Service-Qualität gegenüber den Endbenutzern sicherstellen zu können.
- Elastizität: Die zur Verfügung stehenden Ressourcen passen sich dynamisch und sehr kurzfristig den Business-Anforderungen an, beispielsweise erhält ei-

ne VM bei Bedarf weitere Ressourcen oder wird auf eine andere, leistungsfähigere physische Maschine verschoben. Oder aber es werden Server beziehungsweise Cluster-Knoten als VMs dynamisch aus einer Ressourcen-Wolke alloziert und wieder freigegeben. In Amazons EC2 (Elastic Compute Cloud) ist dieses Konzept auch in den Namen eingeflossen, ein weiteres Beispiel ist die Windows Azure-Plattform sowie natürlich die sogenannten "Private Clouds".

Gefahr des Wildwuchses

Angesichts dieser Vorteile und neuen Möglichkeiten lässt sich bereits erahnen, wo die Herausforderungen beim Betrieb einer solchen Infrastruktur liegen: Zum einen ist die Verlockung groß, mal schnell einen Server aufzusetzen, was kurzfristig sehr pragmatisch aussieht, langfristig aber auch zu einem Wildwuchs, dem sogenannten VM Sprawl, führen kann. Für eine IT-Abteilung ist es in aller Regel nicht möglich, den Überblick darüber zu behalten, welche VMs tatsächlich gebraucht werden und mit welchen Ressourcen diese ausgestattet sein müssen. Und eine einfache Deprovisionierung, zum Beispiel per Verfallsdatum, ist zu riskant.

Die Frage, ob eine gegebene VM überhaupt noch gebraucht wird und ob sie die zugewiesenen Ressourcen wirklich benötigt, sollten Sie besser dezentral von den Nutzern beziehungsweise Ownern der VM beantworten lassen. Jedoch gehen auch die Nutzer allzu oft recht großzügig mit den bereitgestellten Ressourcen um. Dies lässt sich lösen, indem Sie dem Besitzer der VM die Ressourcen in Rechnung stellen. Die Services der IT-Abteilung erhalten so einen definierten Wert, lassen sich besser messen und beurteilen.

Diese Situation ist nicht erst mit der Virtualisierung entstanden, gewinnt aber in deren Kontext an Intensität, denn Server-Kosten können nicht mehr einfach eins zu eins auf die Kunden umgelegt werden. Zudem steigt die Komplexität, da die oben genannten Aspekte wie dynamische Ressourcenzuteilung, Agilität und Elastizität eine faire Kostenberechnung sehr anspruchsvoll machen.

IT-Kosten ermitteln

Die entscheidende Frage lautet also, wie viel die von der IT bereitgestellten Ressourcen tatsächlich kosten. Ähnlich wie bei einem Mehrparteienhaus müssen Sie



dafür die Gesamtkosten der physischen Hardware nach einem zuvor vereinbarten Verteilerschlüssel auf die VMs umlegen und den VM-Ownern in Rechnung stellen. Letzteres gilt streng genommen nur, wenn die IT als Profit-Center oder eigenständiges Unternehmen agiert. Aber auch bei einer Aufstellung als Cost-Center ist es erfahrungsgemäß sinnvoll, die Zahlen rein informativ an die "Kunden" weiterzuleiten, wie wir weiter unten im Abschnitt "Good Practices" noch beschreiben. Dieser Vorgang lässt sich in drei Schritten abbilden:

1. Alle Beteiligten müssen sich zunächst auf ein Abrechnungsmodell, sprich auf einen Verteilerschlüssel, einigen.
2. Anschließend messen Sie Daten über den tatsächlichen Ressourcenverbrauch pro VM. Hier oder im folgenden Schritt sollten Sie möglichst auch eine Zuordnung der VMs auf Kostenstellen, Applikationen, Business-User, Service-Manager, VM-Owner oder ähnliches durchführen.
3. Mit den gesammelten Verbrauchsdaten sowie den angefallenen Kosten aus der physischen Welt (Hardware-, Strom-, Stellplatz-, Lizenz-, Support-Kosten et cetera) erstellen Sie entsprechende Abrechnungen.

Bisweilen ist es sinnvoll, mehrere Abrechnungsmodelle parallel zu benutzen. Diese können Sie entweder bei der Gesamt-Abrechnung kombinieren, beispielsweise um fixe Grundkosten für die Bereitstellung und variable Verbrauchskosten für den tatsächlichen Ressourcenverbrauch zu addieren. Oder aber Sie nutzen mehrere alternative Modelle ausschließlich für interne Zwecke, um bei eventuell aufkommenden Diskussionen über das verwendete Modell oder die berechneten Kosten Vergleichsrechnungen in der Hinterhand zu haben.

Unternehmen, die bereits vor Einführung von Virtualisierung ein Accounting betrieben haben, erleben dennoch meistens neue Herausforderungen bei den ersten beiden Schritten, da zum einen die Kos-

ten eben nicht mehr an physischen, sondern an virtuellen Maschinen aufgehängt werden müssen, zum anderen VMs jederzeit auf eine andere physische Maschine umziehen können.

Abrechnungsmodelle

Drei Abrechnungsmodelle stellen wir im Folgenden genauer vor:

- Tiered Flat Rates (TFR): Hierbei handelt sich um im Voraus festgelegte, von der jeweils angebotenen Ressourcenausstattung abhängige Kosten pro VM. Die tatsächliche Ressourcennutzung spielt bei der Abrechnung keine Rolle.
- Measured Resource Utilization (MRU): Hier wird der tatsächliche Ressourcenverbrauch berücksichtigt und es muss weiter unterschieden werden nach "Full Cost Recovery", das die Gesamtkosten auf alle Nutzer umlegt, die somit auch für bereitgestellte, aber nicht genutzte Ressourcen aufkommen müssen. Maßgeblich ist also der Anteil jeder VM am Gesamt-Ressourcenverbrauch.
- "Partial Cost Recovery" legt die Gesamtkosten auf alle Nutzer sowie die IT-Organisation um, wobei Letztere für nicht genutzte Ressourcen aufkommt. Maßgeblich ist hier der Anteil jeder VM am Gesamt-Ressourcenangebot.

Die oben erwähnte Agilität, also Funktionen wie VMwares vMotion beziehungsweise HA- und DRS-Cluster, führt dazu, dass es keine statische Zuordnung von VMs zu physischen Servern gibt. Für die Praxis heißt dies, dass Sie beim TFR-Modell nicht einfach die Server-Kosten als Gesamtkosten benutzen können. Stattdessen sollten Sie bei CPU- und Memory-Kosten auf den Cluster (HA- und/oder DRS-Cluster) abstellen, in dem sich die VM befindet. Hinsichtlich Storage-Kosten bieten sich dagegen die SAN-Kosten für das von der VM benutzte Datastore an.

Beim MRU-Modell können Sie weiterhin mit Server-Gesamtkosten arbeiten, benötigen aber ein Werkzeug, das neben den reinen Verbrauchsdaten regelmäßig den "momentanen Aufenthalts-

ort" der VM aufzeichnet und bei der Abrechnung berücksichtigt.

Tiered Flat Rates

Bei einer Abrechnung nach Tiered Flat Rates (TFR) werden VMs mit einer bestimmten, zuvor festgelegten Ressourcenausstattung zu einem fixen Preis angeboten. Vom Standpunkt des Ressourcenverbrauchs liefert dieser Abrechnungsmodus zwar keine "fairen" Preise, für Kunden und VM-Owner ist aber ein Höchstmaß an Kosten-Vorhersehbarkeit gegeben, und zwar über den gesamten Lebenszyklus der VM hinweg. Beispielsweise könnte die IT folgende vier Flat Rates anbieten:

- Tier A: 1 CPU, 1 GByte Hauptspeicher, 10 GByte Plattenspeicher für 250 Euro
- Tier B: 1 CPU, 2 GByte Hauptspeicher, 10 GByte Plattenspeicher für 350 Euro
- Tier C: 2 CPUs, 2 GByte Hauptspeicher, 20 GByte Plattenspeicher für 600 Euro
- Tier D: 4 CPUs, 4 GByte Hauptspeicher, 40 GByte Plattenspeicher für 1.500 Euro

In der Praxis ist ein reines TFR-Modell meistens noch zu unflexibel und sollte daher um "Add-Ons" erweiterbar sein. Wie bei einer Fahrzeug-Konfiguration können Sie beziehungsweise die Kunden Extras ergänzen, beispielsweise Hauptspeicher für 100 Euro pro GByte oder Plattenspeicher für zehn Euro pro GByte. Ein Kunde kann auf diese Weise beispielsweise Folgendes konfigurieren: Eine CPU mit 2 GByte Hauptspeicher und 25 GByte Plattenspeicher entspricht "Tier B" plus 15 GByte Plattenspeicher zum Preis von 500 Euro.

Eine zusätzliche Möglichkeit ist, TFR als Grundpreis zu nutzen und um Verbrauchspreise aus einem MRU-Modell zu ergänzen. Hier ist natürlich ein gewisser kalkulatorischer Aufwand nötig, um Preisstaffeln zu finden, die mindestens kostendeckend sind. Außerdem entstehen bei diesem Modell regelmäßig Diskussionen mit den Kunden, inwieweit die Preise gerechtfertigt sind. Die Tatsache, dass ausschließlich die angebotenen



Ressourcen zählen und somit auch ausgeschaltete VMs verrechnet werden, kann diese Diskussionen noch verschärfen.

Measured Resource Utilization (MRU)

Die MRU-Methode sieht eine Abrechnung nach dem tatsächlichen Ressourcenverbrauch vor. In dieser Hinsicht liefert die Methode also faire Preise. Andererseits sind die Kosten somit nicht mehr vollständig planbar. Ein wichtiger Unterschied im Hinblick auf die organisatorische Aufstellung der IT (Profit-Center oder Cost-Center) besteht zwischen den beiden Varianten "Full Cost Recovery" (volle Kostendeckung) und "Partial Cost Recovery" (teilweise Kostendeckung).

Darf sich die IT nicht als Cost-Center verhalten, bleibt eigentlich nur eine volle Kostendeckung: Alle Kosten müssen den Endkunden in Rechnung gestellt werden, insbesondere – und das ist der entscheidende Unterschied zur teilweisen Kostendeckung – solche für bereitgestellte, aber nicht genutzte Ressourcen. Die Auslastung der physischen Hardware mit VMs spielt somit eine entscheidende Rolle. Das folgende, sehr einfach gehaltene Beispiel verdeutlicht dies: Die monatlichen Gesamtkosten für einen physischen Server betragen 5.000 Euro. Im ersten Monat laufen auf diesem Server fünf VMs mit identischem Ressourcenverbrauch. Den Endkunden werden somit 1.000 Euro pro VM in Rechnung gestellt. Da der Server noch freie Kapazitäten hat, werden im nächsten Monat fünf weitere VMs darauf untergebracht, insgesamt also zehn VMs. Obwohl sich an deren Ressourcennutzung nichts verändert hat, betragen die Kosten pro VM jetzt nur noch 500 Euro.

Solche Sprünge finden aber hauptsächlich in der Einführungsphase statt. Nachdem die virtuelle Infrastruktur sich bei einer typischen Auslastung eingependelt hat (beispielsweise 70 bis 80 Prozent Auslastung der physischen Server) und lediglich kleinere, iterative Anpassungen erfolgen, pendeln sich auch die Preise

entsprechend ein. Zu den Vorteilen dieses Ansatzes zählt insbesondere, dass Sie automatisch einen vernünftigen Kompromiss zwischen Performance und Kosten der virtuellen Infrastruktur erreichen und das IT-Management in die Lage versetzt wird, sowohl eine Unter- als auch Überauslastung der Hardware zu vermeiden. Für das Reporting bietet sich hier die Benutzung eines sogenannten "Profit Multipliers" an, um durch einen prozentualen Aufschlag auf die reinen Kosten auch Margen zu realisieren, beispielsweise ein Aufschlag zwischen einem und zehn Prozent.

Soll die IT-Abteilung die Kosten für ungenutzte Ressourcen selbst tragen, ist alternativ eine teilweise Kostendeckung ("Partial Cost Recovery") möglich. Analog zum obigen Beispiel bedeutet dies für einen Server mit 5.000 Euro monatlichen Gesamtkosten: Laufen auf dem Server fünf VMs mit jeweils fünf Prozent Ressourcenverbrauch, dann werden für jede VM 250 Euro abgerechnet, die restlichen Kosten in Höhe von 3.750 Euro trägt die IT-Organisation. Kommen im nächsten Monat fünf weitere VMs mit derselben Last dazu, ändert sich für die bestehenden VMs nichts und auch den neuen VMs werden je 250 Euro berechnet. Lediglich der von der IT zu tragende Restbetrag schrumpft auf 2.500 Euro. Eine Unterauslastung der virtuellen Infrastruktur geht in diesem Fall also ausschließlich zu Lasten der IT-Organisation. Aus IT-Sicht sind die Ziele Kostenminimierung und Auslastungsmaximierung der virtuellen Infrastruktur daher deckungsgleich.

Beim TFR-Modell wiesen wir bereits auf die Möglichkeit von Add-Ons, etwa zusätzlichem Hauptspeicher, hin. Aber auch für MRU-Modelle werden praktisch immer Add-Ons benötigt. Diese können Sie sich als "A la carte"-Leistungen vorstellen, die einer spezifischen VM oder einem physischen Server zugeordnet werden, beispielsweise Software-Lizenzen oder spezielle Sicherheits-Vorkehrungen für eine VM, eine USV oder ein besonderer Stand-


platz für einen physischen Server. Im Rahmen der Abrechnung werden die Kosten für solche Add-Ons auf die anderen Kosten (TFR und/oder MRU) aufaddiert.

Good Practices

Es bietet sich an, beim Thema Accounting überschaubar zu beginnen und anschließend das Accounting-Modell auszubauen und zu flexibilisieren. Die TFR-Methode bildet einen guten Einstieg. Parallel lässt sich im Hintergrund ein MRU-Modell mit Add-Ons aufbauen und iterativ verfeinern. Ansonsten besteht die Gefahr, dass Sie sich in Details und den entsprechenden Diskussionen verlieren. Werkzeuge wie Vizioncores vFoglight oder VMwares vCenter Chargeback unterstützen die beschriebenen Abrechnungsmodelle und bieten entsprechende Reports.

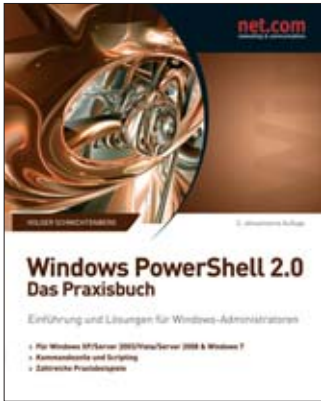
Von vornherein sollten Sie wirklich alle Kosten berücksichtigen. So entstehen beispielsweise für Plattenplatz eben nicht nur Anschaffungskosten, sondern auch zahlreiche weitere Kosten für Strom und Stellplatz, Materialkosten für Switches, Ports und Kabel, Personalkosten für die Administratoren, Wartungskosten bis hin zu Abschreibungen. Hier lohnt sich häufig eine Rücksprache nicht nur mit Beteiligten aus dem Datacenter-Bereich, sondern auch mit dem Financial- oder Accounting-Bereich des Unternehmens.

Fazit

Selbst wenn die Kosten nicht in Rechnung gestellt werden, lohnt es sich meistens, sie informativ an die Kunden zu kommunizieren. Auf diese Weise entsteht Transparenz und ein besseres Gefühl dafür, wo Ressourcen benutzt oder auch verschwendet werden. Im besten Falle erleichtert das eine Kooperation mit dem Ziel einer effizienteren Ressourcennutzung. Ansonsten kann bei Eskalationen zumindest niemand behaupten, er hätte von nichts gewusst. (jp) 

Patrick Schwanke ist Senior Systems Consultant / VCP bei Quest Software.

Windows PowerShell 2.0 Das Praxisbuch



Spätestens mit Windows Server 2003 war die Zeit reif für neue und mächtigere Scripting-Werkzeuge. Eines davon ist die PowerShell, die, wenngleich in Version 2.0 erschienen, noch eher ein Schatten-

dasein fristet. Aus diesem Unwissen will der auf diesem Gebiet anerkannte Autor Holger Schwichtenberg den Leser befreien und vollführt dabei noch eine weitere gute Tat: Er zeigt den aufgabenbeladenen Administratoren Wege zur Vereinfachung und Automatisierung. Das Buch ist klassisch aufgebaut und führt über eine Einführung zur Installation über die Architektur der Power-

Shell zu den Einsatzbefehlen und Hilfsfunktionen. Der richtige Einstieg wird im Kapitel "Objektorientiertes Pipelining" vollzogen, indem der Autor die Grundlagen der Arbeitsweise mit der PowerShell darlegt. Erfreulich ist dabei, dass der theoretische Teil nicht übermäßig ausufernd präsentiert wird. In den Folgekapiteln wird das Rüstzeug zur Erstellung der Skripte vermittelt.

Im zweiten Teil behandelt der Autor das umfangreiche Aufbauwissen. So kommen .NET-Klassen ebenso zur Sprache wie auch der Einsatz von Windows Management Instrumentation (WMI). In den Abschnitten Remoteausführung, Fehlersuche und Jobs werden fortgeschrittene Techniken erläutert, die bei Bedarf zum Einsatz kommen können. Auch das für die Auswertung notwendige Ereignissystem, Module wie Erweiterungen, wird erklärt. Der dritte Teil nimmt über 25 Prozent des Buchvolumens ein und ist für alle, die über Erfahrung in der PowerShell verfügen, eine Fundgrube: der Praxiseinsatz. Zahlreiche Skripte zu den vielseitigsten Themen wie Dateisystem,

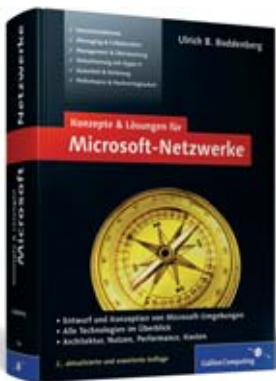
Computer-Hard- und Softwareverwaltung, Registry, Ereignisprotokolle, Active Directory und GPO bieten eine Grundlage für den ambitionierten Skriptprogrammierer. Profis werden im vierten und abschließenden Abschnitt Freude an der Entwicklung von Cmdlets (auch in C#) und Modulen finden.

Fazit: Auf über 800 Seiten Inhalt weiß der Autor seinen Leser für die Skriptsprache PowerShell und deren Möglichkeiten zu interessieren. Dabei endet das Material nicht beim Erklären von Strukturen und Anweisungen. Zahlreiche Beispiele aus der Alltagspraxis des Administrators wissen zu gefallen und regen zu Eigenentwicklungen an. Eine Begleit-CD rundet den Inhalt ab.

Frank Große

Autor:	Holger Schwichtenberg
Verlag:	Addison-Wesley
Preis:	49,80 Euro
ISBN:	978-3-8273-2926-4
Bewertung:	★★★★★

Konzepte & Lösungen für Microsoft-Netzwerke



Bereits die Erstausgabe des vorliegenden Werkes war ein Bauchladen voller administrativer Weisheiten im Windows-Arbeitsumfeld. Mittels detaillierter und umfangreich erläuteter Beschreibungen gab das Buch einen strukturierten

Leitfaden zur Arbeit in Windows Client-Server-Umgebungen. Genau an diesem Punkt knüpft die aktualisierte und erweiterte zweite Auflage an. In neun umfassenden Kapiteln werden ausgehend von den Fragen "Was lässt sich damit machen?" und "Wie wird es installiert?" die

derzeit wichtigsten Microsoft-Technologien und deren Einsatzmöglichkeiten vorgestellt. Der Leser darf aber hier keine schlichte Tutorial-Sammlung erwarten, sondern kann sich an gelungenen Erläuterungen erfreuen.

Ausgehend von Aufbau und Struktur erfährt der Leser Wissenswertes zu Planung und Design einer AD-Domäne, bevor die Gruppenrichtlinien, Zertifikatdienste und Rechteverwaltungsdienste ihren Platz erhalten. Unter dem Stichwort "Collaboration" findet der Neugierige ein Kapitel, das sich primär mit Sharepoint, Workflows und Groove sehr detailliert auseinandersetzt und damit für viele Administratoren grundlegende Fragen klärt. Ein Viertel des gesamten Buchumfangs nimmt der Abschnitt über Kommunikation ein. Hier kommen die Exchange-(2007)-Administratoren auf ihre Kosten. Aber nicht nur die, denn auch Themen wie Mail-Hygiene, Mobiler Zugriff, Office Communications Server, Telefonie

und Unified Communications finden ihren Platz. Kurz gehalten ist der Abschnitt über Virtualisierung (Hyper-V, Terminaldienste), indem sich der Autor auf die wichtigsten Schlüsselkonzepte konzentriert. Ebenso geht er beim Abschnitt "Sicherheit und Sicherung" vor.

Fazit: Das Aufgabenfeld des Administrators im Windowsumfeld erweitert sich ständig. Mit dem vorliegenden Buch werden moderne Konzepte der Vernetzung und Kommunikation vorgestellt und mit nachvollziehbaren praktischen Lösungen versehen. Dabei wird der Leser virtuell an die Hand genommen und der Fokus auf den praktischen Nutzen gelegt.

Frank Große

Autoren:	Ulrich B. Boddenberg
Verlag:	Galileo Computing
Preis:	69,90 Euro
ISBN:	978-3-8362-1356-1
Bewertung:	★★★★★

www.operating-system.org Museumsbesuch

Falls Sie sich schon einmal gefragt haben, wie viele Betriebssysteme es wohl gibt, könnte unsere Website des Monats etwas für Sie sein. Der aktuelle Zählstand dort: 582 (ohne die 605 Linux-Distributionen selbstverständlich). Und falls Sie – genau wie die Redaktion – noch nie etwas von Drywell OS, MRT1700 oder zeVenOS gehört haben, lohnt sich ein Besuch von operating-system.org. Die Website dokumentiert Betriebssysteme aller Art und ist wahrlich ein Museum für Bits und Bytes.

Die mit großem Aufwand von Stefan Berka zusammengestellte Website bietet nach eigenen Angaben viele Informationen über die Geschichte von Betriebssystemen und historische Fakten seit der ersten Veröffentlichung. Und "viele" ist dabei noch untertrieben: Selbst zu den exotischsten Systemen findet der Leser hier umfangreiche Informationen. Oder wussten Sie, dass "das MorphOS-Projekt 1999 ursprünglich gestartet wurde, um AmigaOS von der 68k CISC-Architektur auf die aktuellere PowerPC RISC Architektur zu portieren"? Sicher,

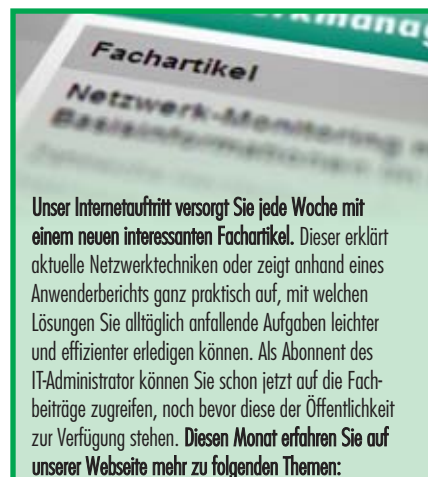
dies ist keine Information, die über das Wohl und Wehe Ihrer IT entscheiden wird und doch ist operating-system.org gespickt mit spannenden Hintergrundinformationen, Kuriosen, aber auch technischen Details.

Die Website besteht denn auch hauptsächlich aus den Artikeln zu den Betriebssystemen. Hier findet der Leser unterschiedlich ausführliche Beschreibung der Funktionalitäten, Entwicklung und Anwendungsgebiete. Wer hier hin und wieder stöbert, dem dürfte so mancher Zusammenhang klar werden oder erfahren, wann die Geburtsstunde bestimmter Features war. Ergänzend stellt Berka Artikel bereit, die Hintergründe beleuchten: Etwa die Entwicklung der Linux-Distributionen, eine Apple-Firmengeschichte oder auch die Unterschiede zwischen den Dateisystemen.

Der Besuch der Website verbreitet wirklich den Flair eines Museumsbesuchs. Wer sich für Zusammenhänge und Hintergründe der IT interessiert, kann hier leicht viele Stunden verweilen. Vorbildlich auch, dass die Site in drei Sprachen zur Verfügung steht. Allein die Navigation bedarf noch leichter Optimierung. Viel Spaß beim Rundgang. (jp)



Ein Fall fürs Museum: Windows 1.0 auf operating-system.org



Unser Internetauftritt versorgt Sie jede Woche mit einem neuen interessanten Fachartikel. Dieser erklärt aktuelle Netzwerktechniken oder zeigt anhand eines Anwenderberichts ganz praktisch auf, mit welchen Lösungen Sie alltäglich anfallende Aufgaben leichter und effizienter erledigen können. Als Abonnent des IT-Administrator können Sie schon jetzt auf die Fachbeiträge zugreifen, noch bevor diese der Öffentlichkeit zur Verfügung stehen. **Diesen Monat erfahren Sie auf unserer Webseite mehr zu folgenden Themen:**

Effizientes Storage-Resource-Management

In Zeiten rasanten Datenwachstums kann es wesentlich effizienter sein, statt eines Neukaufs von Hardware über den Einsatz einer zentralen Storage-Resource-Management-Lösung nachzudenken. Diese erlaubt es, den ungenutzten Speicher im Unternehmen zu entdecken, zu analysieren und darzustellen, ob er sinnvoll an anderer Stelle verwendet werden kann. Unser Online-Artikel informiert, in welchen Szenarien sich der Einsatz einer SRM-Software lohnt und was Sie bei der Umsetzung beachten sollten.

www.it-administrator.de/themen/storage/fachartikel/86829.html

Nachrüsten alter Clients mit SSDs

Die SSD-Technologie verlängert den Lebenszyklus von Desktop-PCs und Notebooks und steigert gleichzeitig die Performance der Clients. In unserem Fachbeitrag im Web beschreiben wir, wie IT-Verantwortliche durch Einsatz von Flash auch in Zeiten knapper Kassen und gekürzter IT-Budgets eine leistungsfähige Umgebung garantieren. SSDs haben dabei das Potenzial, selbst in schwachen ökonomischen Phasen bei gleichzeitigem Leistungszuwachs kostensparend zu wirken und verfügen – aller Unkenrufe zum Trotz – mittlerweile über ausgezeichnete ROI-Werte.

www.it-administrator.de/themen/storage/fachartikel/86830.html

Konvergenz von Daten- und Speichernetzwerken

Die IT-Branche befindet sich inmitten eines bedeutenden Innovationszyklus. Infrastrukturen im Rechenzentrum entwickeln sich ganz klar zu hoch virtualisierten Service-on-Demand-Strukturen, die von der Cloud getragen werden. Eine wichtige Grundvoraussetzung dafür ist die Konvergenz von Speicher- und Datennetzen. In unserem Online-Fachartikel zeigen wir, wie dieser Umbruch zu einer Vereinfachung der Infrastruktur, zur Reduzierung des Equipments und zur Steigerung der Performance führt.

www.it-administrator.de/themen/netzwerkinfrastruktur/fachartikel/86831.html

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

»Wechselnde Themen halten den Arbeitsalltag interessant«

Johannes Sieß (41) arbeitet in einem Team von Fachleuten bei TakeSAP als technischer Consultant sowie als Administrator für die bei Kunden installierten SAP-Lösungen. Zum Portfolio des Full-Service-Dienstleisters aus Würzburg gehört die Dimensionierung (Sizing) eines SAP-Systems sowie der gesamte Installations- und Implementierungsaufwand von Hard- und Software und der nachfolgende Regelbetrieb.

Welche Ausbildung haben Sie gemacht?

Ich habe an der Julius-Maximilian-Universität in Würzburg ein Studium als Diplom-Physiker abgeschlossen. Im Laufe meines Berufslebens habe ich dann noch Zertifizierungen als SAP Technology Consultant sowie SAP OS/DB Migrateur erworben.

Warum sind Sie IT-Administrator geworden?

Der Spaß an der Arbeit mit dem Computer und die damit verbundenen vielseitigen Aufgaben haben mich fast zwangsläufig in diese Richtung gebracht.

Welche IT-Umgebung betreuen Sie?

Für TakeSAP arbeite ich überwiegend im SAP-Umfeld. Das Unternehmen bietet rund um SAP ein ganzheitliches Dienstleistungsportfolio. Im Rahmen meiner Aufgaben bin ich unter anderem als Senior SAP Technology Consultant tätig, arbeite als SAP Basis-Berater und in Personalunion auch IT- und System-Administrator. Die Umgebungen, die ich gemeinsam mit Kollegen betreue, richten sich an den SAP-Projekten aus, die wir für Kunden realisieren und verwalten. Die Infrastruktur ist abhängig vom jeweiligen Auftrags- und Vertragsvolumen. Je nach Anforderung betreue ich, teilweise parallel, diverse SAP-Landschaften mit ERP, CRM und/oder Logistik. Zu meinem Aufgabengebiet zählt die Installation einer Lösung ebenso wie die Wartung, Migration, das Backup und die Verwaltung.

Welches Netzwerk- und Systemmanagement setzen Sie ein?

Wir nutzen Nagios sowie den SAP Solution Manager.

Was sind im Hinblick auf die IT-Administration die größten Herausforderungen Ihres Arbeitsalltags?

Durch die Vielzahl der betreuten Projekte bin ich fast täglich mit wechsel-



Geburtstag: 25.03.1969
Familienstand: verheiratet
Hobbys: Jogging (Marathon), Mountainbike, Kochen

Johannes Sieß, IT-Administrator

den Herausforderungen konfrontiert. Ich muss auch immer wieder neue Themen bearbeiten, aber das finde ich besonders spannend, denn es hält den Arbeitsalltag interessant.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Für diverse Kunden arbeite ich an der Installation und Betreuung von SAP-Systemen mit unterschiedlichen Ausmaßen. Hinzu kommen die Migrationen von bestehenden Systemen sowie diverse Upgrades.

Was macht Ihnen an Ihrem Job am meisten Spaß?

Ich mache fast alles gern. Der Beruf bietet so viele unterschiedliche Möglichkeiten, dass es nie langweilig wird.

Was mögen Sie nicht so sehr, muss aber gemacht werden?

Berechtigungen einzurichten finde ich nicht so spannend, aber auch das muss erledigt werden.

Was tun Sie für Ihre Fort- und Weiterbildung?

Wichtig finde ich den Austausch mit Kollegen sowie Experten aus meinem Fachgebiet. Dann lese ich selbstverständlich auch die einschlägige Fachliteratur und informiere mich im Internet.

Was war der größte persönliche Flop oder Fehler, den Sie gemacht haben?

Da fällt mir ad hoc nichts ein. Bisher habe ich mir noch keinen spektakulären Fehler geleistet. Ich hoffe, das bleibt so.


Was war Ihr größter Erfolg als IT-Administrator?

Eigentlich ist jedes installierte System, das gut läuft, eine besondere Leistung. Für mich persönlich ist es ein Erfolg, dass ich mein Wissen und Können in eine neue Firma einbringen konnte und hier meinen Platz gefunden habe.

Was war der dümmste Anwender oder Anwenderfehler, der Ihnen untergekommen ist?

Na ja – das ist einer der Klassiker, den sicher jeder Administrator in dieser oder ähnlicher Form kennt: Ein Anwender meldete aufgeregt, dass das SAP-System defekt sei. Dabei stellte sich heraus, dass der Druckauftrag nur deshalb nicht ausgeführt wurde, weil kein Papier im Drucker war.

Was sehen Sie als die größte Herausforderung der IT in den nächsten drei Jahren?

Für beratende Unternehmen wird es eine Herausforderung bleiben, die Qualität für Dienstleistungen trotz der Preiskämpfe zu halten. 

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 12/10 erscheint am 3. Dezember 2010

Schwerpunktthema:

WiFi, VoIP und WLAN-Management

Im Test: QoS-Messungen mit TraceSim VoIP

Im Test: Fluke AirCheck WiFi-Tester

Workshop: WLAN-Sicherheit mit Linux-Tools prüfen

Systeme: Priorisierung im Netz bei Echtzeitströmen

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

Unsere Ausgabe im Januar hat sich zum Schwerpunkt **Virtualisierung** gesetzt. In einem unserer Tests nehmen wir unter anderem XenClient Express unter die Lupe. In den Workshops befassen wir uns mit Sicherheitslösungen für KVM-basierte Maschinen sowie Virtualisierung mit dem Microsoft Systems Center.

Als Schwerpunkt im Februar folgt dann das Thema **Sicherheit von Unternehmensdaten**.

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*
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,
Alexander von Gemler, Frank Große, Thomas Joos,
Christian Kneemann, Martin Pajank, Christian Rusch,
Marcus Schneider, Patrick Schwanke, Dr. Michael
Schwartzkopf, Bertram Wöhmann, Dennis Zimmer

Anzeigen

Anne Kathrin Heinemann, *Anzeigenleitung*
verantwortlich für den Anzeigenteil
kathrin@it-administrator.de
Tel.: 089/4445408-20

Es gilt die Anzeigenpreisliste
Nr. 7 vom 01.11.2009

LAC/2008



Produktion / Anzeigendisposition

Lightrays: Andreas Skrzypnik
dispo@it-administrator.de
Tel.: 089/4445408-88
Fax: 089/4445408-99

Druck

Konrad Tritsch
Print und digitale Medien GmbH
Johannes-Gutenberg-Straße 1-3
97199 Ochsenfurt-Hohestadt

Vertrieb

Anne Kathrin Heinemann
Vertriebsleitung
kathrin@it-administrator.de
Tel.: 089/4445408-20

Abo- und Leserservice

Vertriebsunion Meynen GmbH & Co. KG
Stephan Orgel
Große Hub 10
65344 Eltville
leserservice@it-administrator.de
Tel.: 06123/9238-251
Fax: 06123/9238-252

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
(mit Sonderheften + 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: € 9,45
E-Paper-Jahresabonnement: € 99,-
E-Paper-Studentenabonnement: € 49,50
Jahresabonnement-Kombi mit E-Paper: € 168,-
(Studentenabonnements nur gegen Vorlage
einer gültigen Immatrikulationsbescheinigung)

Alle Preise verstehen sich inklusive der
gesetzlichen Mehrwertsteuer sowie
inklusive Versandkosten.

Verlag / Herausgeber

Heinemann Verlag GmbH
Leopoldstraße 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 / Anteilsverhältnisse

Geschäftsführende Gesellschafter zu gleichen Teilen
sind Anne Kathrin und Matthias Heinemann.

ISSN

1614-2888

Internet

www.it-administrator.de

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 zuzutreffende
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.

Manuskripteneinsendungen

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

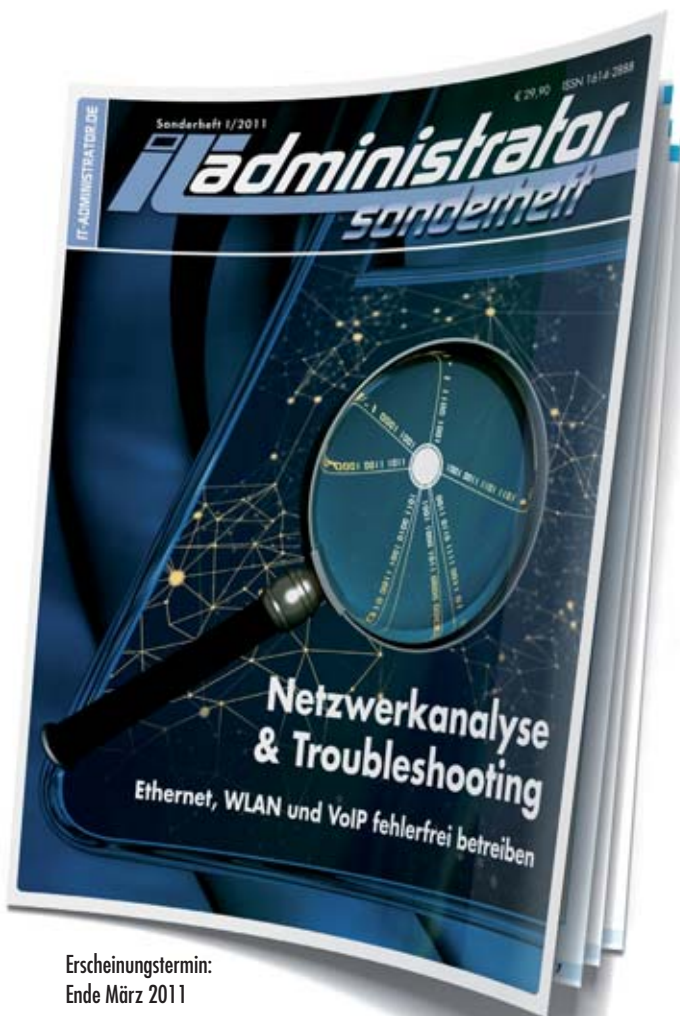
Redaktion IT-Administrator
Heinemann Verlag GmbH
Leopoldstr. 85
80802 München
Tel.: 089/4445408-10
Fax: 089/4445408-99
E-Mail: redaktion@it-administrator.de

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

DeviceLock	S. 27	IT-Watch	S.11, S.12	Paessler	S. 35
Galileo	S. 15	LANCOM	S. 84	SBS	S. 31
HOB	S. 22	Log.in Consultants	S. 51	VM goes 2010	S. 65
IBM	S. 02	NETGEAR	S. 47		

INSERENTENVERZEICHNIS



Erscheinungstermin:
Ende März 2011

Bestellen Sie jetzt das IT-Administrator Sonderheft 1/2011!

180 Seiten Praxis-Know-how rund um das Thema

Netzwerkanalyse & Troubleshooting

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

* IT-Administrator Abonnenten erhalten das Sonderheft 1/2011 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/



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 Abnummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft 1/2011 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

Ja, ich bestelle das IT-Administrator Sonderheft 1/2011 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 Eltville.

So erreichen Sie unseren
Vertrieb, Abo- und
Leserservice:

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

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

EBOOK
SYSTEMS

Abos und Einzelhefte
gibt es auch als E-Paper



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 1110

LANCOM



. . . c o n n e c t i n g y o u r b u s i n e s s . . .

Das beste WLAN aller Zeiten!

Die höchsten Datenraten aller Zeiten, die beste Funkfeldabdeckung, maximale Kompatibilität – 802.11n setzt neue Maßstäbe im Wireless LAN. Drinnen wie draußen.

Machen auch Sie Ihr Netz zukunftsfähig – und steigen Sie um auf die 802.11n Indoor & Outdoor Access Points, Clients und „11n-ready“ WLAN-Controller von LANCOM.

Ob im kleinen Netz mit wenigen Access Points, im Controller-basierten WLAN mit Tausenden von Geräten, für den Hotspot-Betrieb oder im Freien: 802.11n WLAN von LANCOM sorgt überall für ungekannte Leistungsfähigkeit – auf Wunsch sogar ganz dezent ohne sichtbare Antennen.

Kundenstimmen unter: www.lancom.de/referenzen



LANCOM OAP-310agn



LANCOM
Systems

www.lancom.de