

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

**Im Test:
McAfee Total Protection
for Virtualization**

14

**Im Test:
Protected Networks 8MAN 2.0**

22

**Workshop:
Sichere Netzwerk-
Konfiguration unter vSphere**

38

**Workshop:
Load Balancing für Exchange**

54

**Know-how:
Virtuelle Welten sicher gestalten**

72

Sicherheit für virtuelle Infrastrukturen



LANCOM



... connecting your business

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.



LANCOM OAP-310agn



LANCOM
Systems

www.lancom.de

Rückkehr des Löwenbändigers

Liebe Leser,

in unserer August-Ausgabe skizzierte das Editorial in einer kleinen Fabel die Herausforderungen des Admins als Dompteur einer wildgewordenen Herde von Löwen – virtualisierten Servern. Doch wie viele Geschichten fand auch diese Erzählung ein Happy End in modernen Managementtools für die Virtualisierung. Was folgt, ist die unvermeidliche Fortsetzung: "Die Rückkehr des Löwenbändigers: Sicherheit für virtualisierte Infrastrukturen". Aus Hollywood kommend ist ein Sequel oft nur ein fader Abklatsch, doch in unserem Fall wird die Geschichte eher noch dramatischer.



Denn unser tapferer Löwendresseur, kaum hat er seine virtuellen Maschinen im Griff, sieht sich nun mit ganz neuen Gefahren konfrontiert. Einer seiner Löwen verhält sich an manchen Tagen irgendwie merkwürdig. Er scheint ganz normal seinen Dienst in der Manege zu verrichten, doch hin und wieder hat der Admin das Gefühl, seinen Befehlen werde nicht zu einhundert Prozent Folge geleistet. Und in der Tat: Dieser Löwe hat eine "Blaue Pille" geschluckt, ein perfider Angriff auf den Server, bei dem der Hypervisor so geschickt manipuliert wird, dass dieser selbst Reboots vortäuschen kann. In seinem Beitrag ab Seite 43 zeigt unser Experte Nils Kaczinski auf, was es mit der Blue Pill-Attacke auf sich hat und wie Sie sich davor schützen.

Zum Glück lässt sich dieser Angriff (noch) in der Rubrik "Exotisches" einordnen. Gravierender ist da schon ein anderes Phänomen, das mit virtuellen Maschinen Einzug in die IT gehalten hat: der Wildwuchs von VMs. Leicht per Klick erstellt, finden sich in Unternehmensnetzen immer öfter virtuelle Maschinen, die dort eigentlich nichts mehr zu suchen haben. Ein prominentes Beispiel hierfür lieferte auf der TechEd letzten Jahres Microsoft: Der Compliance-Beauftragte für die Microsoft Cloud-Dienste wie Hotmail berichtete dort, er habe in einem nächtlichen Scan über seine Infrastruktur 20.000 Server gefunden, von denen niemand wusste. Ein Management- wie natürlich auch Sicherheitsfiasko. Und wenn, wie in unserer Vorabveröffentlichung aus dem Sonderheft "Active Directory" ab Seite 49 dargestellt, ein solcher Server ein virtualisierter Windows-Domänencontroller ist, dürfte sich jeder Hacker oder Wirtschaftsspion die Hände reiben ob der Tatsache, dass ihm der Generalschlüssel fürs Netzwerk sozusagen auf dem goldenen Tablett serviert wird.

Bleiben Sie also wachsam, Ihr

John Pardey
Chefredakteur

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

Oder Sie sind Neukunde? Hier können Sie bestellen:

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

www.it-administrator.de



Heinemann Verlag
Im Dialog mit Spezialisten.

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München

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

Vertrieb, Abo- und Leserservice IT-Administrator

vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville

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

INHALT

IT-Administrator – Ausgabe Oktober 2010

Sicherheit für virtuelle Infrastrukturen

Sicherheitsfunktionen in Microsoft App-V

Das Streamen von Anwendungen mit Microsofts App-V vereinfacht den Administrationsaufwand deutlich. Applikationen müssen nicht mehr lokal installiert werden, kommen nicht in Konflikt mit anderer Software und lassen sich zudem zentral konfigurieren. Doch auch bei dieser Art von Virtualisierung sollten Sie die Sicherheit nicht außer Acht lassen. Microsoft stellt eine Reihe von Schutzmechanismen zur Absicherung von App-V zur Verfügung, die wir im Workshop näher beleuchten.

Seite 34

Drucken im Netzwerk (1)

Das einst proklamierte papierfreie Büro ist ferner denn je und spätestens bei dem Szenario einer Betriebssystem-Migration taucht eine Frage auf, die mittlerweile fast gänzlich in Vergessenheit geriet: Gibt es denn dafür auch die passenden Treiber? Wie auch immer es gedreht wird: Drucken ist in unserer Zeit wichtiger denn je – PDF hin und XPS her. In der Workshopserie betrachten wir das Drucken aus zahlreichen Perspektiven und geben Tipps zur richtigen Druckerzuordnung, den passenden Zusatzprogrammen und nicht zuletzt gegen Papierstau.

Seite 60



Server- und Systemmanagement



Clientmanagement



Storage



Sicherheit



Messaging

Themenübersicht



Virtualisierung



Netzwerkmanagement



Job/Weiterbildung



Recht

AKTUELL

06

News

10

ITANet aktuell:

IT-Administrator-Workshop "Sicherheit für Windows-Clients" am 16. November 2010 in München
Das Böse ist immer und überall

12

IT-Administrator vor Ort:

"ice:lingen 2010", 13. und 14. August, Lingen an der Ems
Heiter bis wolkig

PRODUKTE

14



Im Test: McAfee Total Protection for Virtualization
Schotten dicht im virtuellen Raum

18



Im Test: Itelio Docusnap 5.0
Die Übersicht behalten

22



Im Test: Protected Networks 8MAN 2.0
Pfiffiger Verzeichnisplaner

30



Im Test: StorageCraft ShadowProtect Server 4
Backup am laufenden Band

PRAXIS

34



Workshop: Sicherheitsfunktionen in Microsoft App-V
Gefahrlose Wege im Applikations-Strom

38



Workshop: Sichere Netzwerk-Konfiguration unter vSphere
Virtuelle Schlupflöcher zumauern

43



Systeme: Sicherheit bei der Servervirtualisierung
Vorsicht: Blaue Pille

49



Workshopserie: Virtualisierung von Windows-Domänencontrollern (2)
Wege zurück

53



Workshop: Microsoft Exchange
Datenbank-Wartung steuern

54



Workshop: Load Balancing für Exchange
Lasten sicher verteilen

60



Workshopserie: Drucken im Netzwerk (1)
Die Qual der Wahl

64



Systeme: Grundlagen der Storage-Sicherheit
Speichern, aber sicher

68

Tipps, Tricks & Tools

WISSEN

72



Know-how: Virtuelle Welten sicher gestalten
Feste Schutzzäune für flexible Umgebungen

75



Know-how: Planen und Implementieren von IP-Kommunikationsnetzen
Reibungslose Migration

79

Buchbesprechung

"Network Maintenance and Troubleshooting" und
"Praxishandbuch VMware vSphere 4"

80

Website & Fachartikel online

RUBRIKEN

03

Editorial

05

Inhalt

47

Seminarmarkt

81

Das letzte Wort

82

Vorschau, Impressum, Inserentenverzeichnis

Drahtlose Redundanz

Mit dem **UMTS/DSL/WLAN-Router TL-MR3420** bietet **TP-LINK** einen 300 MBit/s WLAN-Router mit UMTS-Failover an. Der 17 x 11 x 3 Zentimeter große TL-MR3420 erfüllt die Standards IEEE 802.11n/g/b, IEEE 802.3/3u sowie USB 2.0. Dabei werden auf WAN-Seite PPPoE, dynamische und statische IP-Adressen, PPTP, L2TP und Kabel unterstützt. Clear Channel Assessment (CCA) soll Kanal-Konflikte vermeiden und so die WLAN-Stabilität erhöhen. Das Gerät verfügt über zwei abnehmbare Antennen mit 3 dBi und eine maximale Übertragungsstärke von 20 dBm. Drückt der Benutzer den QSS-Knopf, baut der Router automatisch eine verschlüsselte

Verbindung auf, ohne dass die Eingabe eines Passworts nötig ist. Per WDS-Bridge lässt sich das Funknetzwerk zudem erweitern. Daneben kann der Administrator mit einer IP-basierten Bandbreiten-Zuordnung definieren, welcher der angeschlossenen Rechner welche Übertragungskapazität beanspruchen darf. Für eine ununterbrochene Internetanbindung ist ein automatisches Failover integriert. Dabei kann der Nutzer zwischen UMTS und WAN (DSL/Kabel) als primäre oder sekundäre Verbindungsart wählen. Ist der Primärzugang nicht mehr verfügbar, schaltet das Gerät automatisch auf den Sekundär-Modus um. Wird dann die primäre Verbindung wiederhergestellt, er-



Der Router TL-MR3420 von TP-LINK lässt sich redundant ans Internet anbinden

folgt wiederum automatisch ein Fallback auf den bevorzugten Übertragungsweg. Der Router ist ab sofort auf dem Markt und kostet 42 Euro. (dr)

TP-LINK: www.tp-link.com/de/

Komplettpaket zum E-Mailmanagement

Mit **REDDOXX 2.0** bietet der gleichnamige Hersteller eine neue Version seiner **virtuellen Appliance zur E-Mail-Archivierung, -Verschlüsselung und -Signatur** an. Die für VMware-Umgebungen erhältliche Software soll Unternehmen ein sicheres und gesetzeskonformes Management von elektronischer Post ermöglichen und zudem Spam abwehren. Reddoxx will im aktuellen Release unter anderem die Funktionen zur E-Mail-Archivierung optimiert haben. Dazu integrierten die Entwickler den Archivcontainer RDX-ASC, der die Langzeitaufbewahrung und -lesbarkeit der Daten sicherstellen soll. Jeder dieser Container beinhaltet neben den E-Mails auch einen Volltext-Index und Meta-Informationen. Eine weitere Neuerung ist die vollautomatische Archivklassifizierung. Dabei kann der Anwender seine Mails beliebig vielen Kategorien zuordnen. Zudem ist es möglich, für jeden Ordner Workflows zu hinterlegen, um beispielsweise personenbezogene Daten entsprechend den gesetzlichen Bestimmungen rechtzeitig aus dem Archiv zu löschen. Die virtuelle Appliance ist ab sofort zu einem Preis ab 1.850 Euro erhältlich. (In)

REDDOXX: www.reddoxx.com

Eine USB-Docking-Station für alle

Als Alternative zu den Modell-spezifischen Docking-Stationen der jeweiligen Notebook-Hersteller bringt **LINDY** die **Notebook Docking Station DVI** auf den Markt, die jedes Notebook schnell und komfortabel lediglich über ein USB-Kabel mit der erforderlichen Peripherie einschließlich Monitor verbinden soll. Auch das Netzwerk, ein hochauflösender Monitor und Audio-Geräte werden über den USB-Anschluss mit dem Notebook verbunden. Als besonderes Feature besitzt die Docking-Station eine eingebaute DVI-I-Grafikkarte mit einem Chipsatz, der sowohl die höchste DVI-D Single Link-Auflösung von 1.920 x 1.200 als auch HDTV-Auflösungen bis 1.080 Pixel in voller Farbtiefe unterstützt. Im normalen Office-Betrieb funktioniert diese Lösung laut Hersteller mit Netbooks und älteren Notebooks problemlos. Eine flüssige Videowiedergabe von bewegten Bildern in HDTV verlangt dem Notebook allerdings sehr viel Rechenleistung ab, so dass es zumindest über einen Dual Core Prozessor der 2 GHz-Klasse verfügen sollte. Über den Monitor-Anschluss hinaus finden die Benutzer eine RJ45-Netzwerkbuchse und vier USB 2.0-Anschlüsse, die mit zusätzlichen USB-Hubs erweiterbar sind. Die Docking-Station läuft unter Windows- und Mac-Betriebssystemen.

Auf der Microsoft-Seite werden Windows 7 sowohl in der 32 Bit- als auch der 64 Bit-Version unterstützt sowie die älteren Windows-Betriebssysteme zurück bis Windows 2000 mit Service Pack 4. Nutzer von Intel-basierten Macs ab OS Tiger

10.4.11 können Treiber samt Installationsanleitung von der Hersteller-Website herunterladen. Für rund 120 Euro ist die Docking-Station erhältlich. (dr)

LINDY:
www.lindy.de



Die Notebook Docking Station DVI von LINDY bindet Notebooks über ein USB-Kabel an

Datenhaltung für die Großen

Mit der neuen **Deduplizierungs- und Replikationslösung DXi6700** mit VTL-Schnittstelle will **Quantum** Mid-range- und Enterprise-Kunden eine passende Kombination aus Performance, einfacher Nutzung und Preis-/Leistungsverhältnis für Fibre Channel SAN-Umgebungen bieten. Die Appliance schafft eine Backup-Performance von bis zu 3,5 TByte pro Stunde und bietet bis zu 56 TByte nutzbare Kapazität. Die VTL-Schnittstelle der DXi6700 lässt sich direkt in die bestehende SAN Fibre Channel-Umgebung integrieren. Die Remote Replikation und die integrierte Funktion zur direkten Tape-Erstellung unterstützen automatisiert sowohl schnelles Disaster Recovery als auch langfristige Datenvorhaltung. Die direkte Tape-Erstellung von Quantum schreibt die Daten dabei von den DXi-

Systemen ohne Umweg über den Backup-Server direkt auf Tape. Durch die Integration der Software Quantum Vision 4.0 lassen sich die Disk- und Tape-Systeme zentral von einer Konsole aus steuern. Standardmäßig für jedes Gerät der DXi-Serie zeigen die erweiterten Reporting-Tools der Appliance ein detailliertes Bild der internen Systemprozesse samt Backup- und Replikationsdaten für Trendanalysen. Das soll eine effektivere Planung und geringere Langzeitkosten ermöglichen. Daneben bieten die Tools Einblicke in CPU, Disk Input/Output und den Netzwerk-Traffic pro Port, überwachen Kapazitätsauslastung, Freigabe von Speicherplatz und den Replikationsstatus. Ab 113.575 Euro ist die Lösung erhältlich. (dr)

Quantum: www.quantum.com/Products/Disk-BasedBackup/DXi6700/Index.aspx

Die Ritter des Ni

SonicWALL kündigt mit den Modellen **SonicPoint-Ni und SonicPoint-Ne** zwei neue **Access Points** an. Beide Dual-Band-Single-Radio-Geräte unterstützen den WLAN-Standard 802.11n. Während die Ni-Variante lediglich über interne Antennen verfügt und sich ausschließlich über PoE mit Strom versorgen lässt, weist Modell Ne drei externe Antennen sowie zusätzlich zur PoE-Funktionalität einen herkömmlichen Stromanschluss auf. Die Netzwerkkomponenten unterstützen "Clean Wireless", ein System des Herstellers, das möglichst einfach und sicher drahtlose Access Points und PoE-Adapter in bestehenden Firewall- und VPN-Schutz integrieren soll. Die Access Points verschlüsseln den Datenverkehr nach den Standards WEP, WPA, WPA2 und greifen dabei auf die Protokolle TKIP und AES zurück. Die drahtlose Authentifizierung erfolgt offen, per PSK oder EAP. In entsprechende Umgebungen eingebunden, stellen die Kommunikationshelfer bis zu acht Virtual Access Points bereit. Die beiden Geräte sind ab sofort zu einem Preis von 295 beziehungsweise 425 Euro im Handel. (ln)

SonicWALL:

www.sonicwall.com/us/products/Secure_Wireless_Networking.html



Der Access Point SonicPoint-Ne von SonicWALL lässt sich wahlweise per PoE oder Netzkabel mit Strom versorgen

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

UTAX erweitert sein Angebot im Schwarzweißdruck um den **Laserdrucker LP 3130** im DIN A4-Einstiegsbereich. Zur Standardausstattung des LP 3130 gehören eine 250 Blatt-Papierkassette und eine Bypasszufuhr mit einer Kapazität von 50 Blatt. Die Duplexeinheit für den automatischen, beidseitigen Druck ist Standard. So können 30 DIN A4-Seiten im Simplexbetrieb und produktive 17 DIN A4-Seiten im Duplexbetrieb erstellt werden. Der LP 3130 druckt mit einer Auflösung von 600 x 600 dpi. Das Gerät ist ab sofort für 164 Euro erhältlich. (dr)

www.utax.de

CMS IT-Consulting bietet mit **PROCABS 3.0** eine grafikorientierte Dokumentationssoftware für strukturierte Verkabelungssysteme an. Das Tool lässt sich Browser-basiert bedienen und stellt Verkabelung sowie aktive Komponenten wie Switches, Router und Konverter, Endgeräte, Patchungen und VLAN-Zuordnungen dar. Dank Mandantenfähigkeit und Multi-Site-Tauglichkeit skaliert PROCABS 3.0 laut Hersteller auf bis zu 100.000 Ports. Für 995 Euro ist die Software auf dem Markt. (dr)

www.procabs.de

Amazon stellt in seiner Elastic Compute Cloud (EC2) nun auch **SUSE Linux Enterprise Server 10 und 11** als On-demand-Service zur Verfügung. Die Abrechnung erfolgt dabei auf Stundenbasis, Support kostet extra. Der Anbieter will die Plattform potentiellen Nutzern mit zertifizierten Linux-Anwendungen sowie SUSE Studio, einer Lösung zum Erstellen von Cloud-basierten Workloads, schmackhaft machen. Die Preise orientieren sich an den bereits erhältlichen Windows-Instanzen und beginnen je nach genutztem Umfang bei 12 US-Cent pro Stunde. (ln)

<http://aws.amazon.com/de/ec2/>

Riverbed veröffentlicht mit **Steelhead Mobile 3.1** eine neue Version seiner für Remote-Mitarbeiter gedachten Software zur WAN-Beschleunigung. Neu sind unter anderem ein Client für Rechner unter Mac OS X sowie eine Anpassung an aktuelle Microsoft-Anwendungen wie Exchange 2010. Außerdem will der Hersteller den Datenverkehr mit Citrix-Servern optimiert haben und spricht von im Vergleich zum ICA-Protokoll deutlich verbesserten Kompressionsraten. Weiterhin findet bei diesem Übertragungsweg eine Priorisierung von wichtigen Datenpaketen mittels QoS statt. (ln)

www.riverbed.com/products/steelhead_mobile/



Mit einem Preis von rund 2.350 Euro macht das Speichersystem AccuVault Deduplizierungs-Funktionen auch für den kleinen Geldbeutel erschwinglich

Deduplizierung für jedermann

Tandberg Data erweitert sein **Portfolio zur Datensicherung** um die Geräte-Serie **AccuVault**. Die Appliances sind als Desktop-Version und als Rackmount-Modelle erhältlich und basieren auf Windows Storage Server 2008. Die Anbindung erfolgt über GBit-Ethernet. Kern der Speichersysteme ist die Datensicherungssoftware AccuGuard Enterprise. Das Werkzeug verdichtet die Daten durch Aussortieren redundanter Informationen und sorgt damit laut Hersteller für eine Deduplizierungsrate von bis zu 20:1. Die Desktop-Variante für die Sicherung von bis zu fünf Rech-

nern lässt sich über ein Touch-Screen-LED-Display, das sich je nach vertikaler oder horizontaler Aufstellung ausrichtet, im Netzwerk installieren. Die Daten legt die Storage-Komponente auf einem mitgelieferten 1 TByte-RDX-Wechselspeicher ab. Die beiden Modelle zur Montage im Rack beherbergen hingegen jeweils vier 3,5-Zoll-Festplatten und kommen so auf 4 beziehungsweise 8 TByte Bruttokapazität auf einer Höheneinheit. Die Rack-Versionen bieten zudem Hochverfügbarkeitsmerkmale wie RAID-5-Konfiguration, Hot-Swap-Laufwerke, redundante Stromversorgung und duale GbE-Anschlüsse. Das Desktop-Gerät mit RDX-Laufwerk kostet rund 2.350 Euro, während die Rack-Speicher mit mindestens 6.650 Euro zu Buche schlagen. (ln)

Tandberg Data:
www.tandbergdata.com

Konverterlose Replikation

Infortrend stellt sein erstes Hybrid-Modell, das **ESVA (Enterprise Scalable Virtualized Architecture) F70**, vor. Es verfügt sowohl über Fibre Channel (FC) als auch iSCSI als Anschlussmöglichkeiten. Dadurch können Nutzer im High-End-Bereich geschäftskritische Anwendungen über FC SAN ausführen und gleichzeitig die Remote Replication über iSCSI-basierte Datenübermittlung via Ethernet nutzen. Traditionell sind Konverter notwendig, wenn Anwender Datensets von einem FC Host-Speichersystem auf ein anderes über Ethernet übertragen möchten. Durch das neue ESVA F70 sind Konverter zur Remote Replication überflüssig, da sich

integrierte iSCSI-Ports direkt an das IP-Netzwerk anschließen lassen. Das ESVA F70 verfügt über acht 8 GBit/s FC- und vier GBit/s iSCSI-Ports und unterstützt Solid State- (SSD), SAS- und SATA-Laufwerke. Für Anwender, die Remote Replication nicht nutzen, kann der Hybrid-Anschluss für konsolidierte tiered SANs verwendet werden. Ein einziger Speicherpool der ESVA F70 erfüllt die Service Level-Anforderungen von Tier 1-Anwendungen auf FC SAN und Tier 2-Anwendungen auf IP SAN. Der Einstiegspreis beträgt 35.049 Euro inklusive 16 SAS-Festplatten mit 600 GByte Kapazität. (dr)

Infortrend: <http://esva.infortrend.com/>

Virtueller Desktop verschlüsselt Unternehmensdaten

Citrix gibt die Verfügbarkeit von **XenDesktop 4** bekannt. Die Virtualisierungs-Software besteht aus dem Hypervisor XenClient und XenVault. Letztgenannte Technologie speichert Nutzerdaten von Unternehmensanwendungen automatisch in einem verschlüsselten Ordner – die Inhalte von geschäftlich relevanten Applikationen sind so laut Hersteller jederzeit vor unautorisiertem Zugriff geschützt. Dabei unterstützt die Lösung auch über XenApp und App-V ausgeführte Programme. XenClient beinhaltet mehrere neue Features. Dazu gehören Erweiterungen in puncto Benutzbarkeit und Sicherheit, neue Synchronisationsfunktionen und mehr unterstützte Hardware-Komponenten und USB-Geräte wie Webcams, iPads, iPhones, Androids, BlackBerrys und Windows Mobile-Smartphones. Gemäß Citrix eignet sich das Virtualisierungs-Modell besonders für mobile Mitarbeiter: Wird XenClient vom Netzwerk getrennt, arbeitet er genau wie ein traditioneller, physischer Desktop. Sobald sich der Anwender wieder verbindet, findet eine Synchronisation aller Änderungen mit dem Datacenter statt. Die Lizenzierung von XenDesktop 4 erfolgt pro Benutzer oder pro Device, was je nach Edition mindestens 95 US-Dollar pro Lizenz kostet. (ln)

Citrix: www.citrix.de/produkte/schnellsuche/xendesktop/



Mit der Komponente XenVault legt Citrix bei XenDesktop 4.0 besonders viel Wert auf die Verschlüsselung von Unternehmensdaten



Über den Dongleserver myUTN-80 lassen sich USB-Dongles über das Netzwerk verwenden

Dongles aus dem Netz

SEH bringt mit dem **Dongleserver myUTN-80** eine neue Netzwerklösung zum Dongle-Management auf den Markt. Das Gerät wird ins Netz eingebunden und stellt mittels acht USB-Schnittstellen **USB-Dongles** über das Netzwerk zur Verfügung. Anwender nutzen damit wie gewohnt ihre mit einem Kopierschutz-Dongle gesicherte Software, ohne die Dongles direkt lokal an ihren PC anstecken zu müssen. Außerdem ermöglicht die Lösung die Zuweisung jedes Dongles an verschiedene Nutzer, Kunden oder Abteilungen. Ein umfangreiches Sicherheitspaket soll dabei vor unberechtigtem Zugriff auf die Dongles schützen. Die Verwaltungssoftware SEH UTN Manager kommt an allen PC-Ar-

beitsplätzen zum Einsatz, von denen aus Anwender auf die Dongles zugreifen. Wie bei einem lokal angeschlossenen Dongle kann nur jeweils ein Anwender über eine Punkt-zu-Punkt-Verbindung den jeweiligen Dongle nutzen. Der Dongleserver ermöglicht überdies den Einsatz von Kopierschutz-Dongles in Server-based Computing-Infrastrukturen und virtualisierten Umgebungen mit VMware, Citrix XEN und Microsoft Hyper-V. Der Dongleserver für Ethernet-Netze ist kompatibel mit den Windows 32 / 64 Bit-Versionen Windows 7, Server 2008, Vista, Server 2003 und XP. Für rund 800 Euro ist der Dongleserver erhältlich. (dr)

SEH: www.seh.de

Nebelscheinwerfer erhellt Speicherumgebung

Quest Software erweitert sein Portfolio an Monitoring-Lösungen um **vFoglight Storage 1.0**. Die für Infrastrukturen unter VMware geeignete Software gibt mit ihrem Explorer-basierten Interface einen Überblick sowohl über die physische als auch die virtuelle Schicht eines Speichersystems. Sie soll so dem Administrator dabei helfen, Pfade zu optimieren, den physischen Speicher zu reorganisieren und wenn nötig, die Kapazität zu erhöhen. Zu den Funktionen des Werkzeugs zählen eine Performance-Überwachung sowie ein Kapazität-Monitoring, das Aufschluss gibt über den tatsächlich genutzten Speicherplatz, beispielsweise

innerhalb eines VMware-Datastore. Topologie- und grafische Ansichten zeigen die Beziehungen zwischen der virtuellen und physischen Storage-Infrastruktur als Momentaufnahmen. Vordefinierte Alarmer weisen auf Abweichungen von branchenüblichen Best Practices hin, während diverse Report-Funktionalitäten dem Nutzer erlauben, Informationen zur Storage-Performance anderen Verantwortlichen zur Verfügung zu stellen. vFoglight Storage 1.0 ist ab sofort für Windows Server 2003 und 2008 (jeweils SP2) erhältlich und kostet pro CPU inklusive einem Jahr Support 419 Euro. (ln)

Quest Software: www.quest.com/vfoglight-storage/

Intelligenter Datenräumer

O&O stellt **Version 14** seiner **Defragmentierungssoftware Defrag** vor. Die Benutzerführung wurde laut Hersteller an die häufigsten Anwendungsfälle angepasst, so dass die wichtigsten Aufgaben intuitiv lösbar sind. Alle grundlegenden Steuerungsmöglichkeiten sowie Funktionen von O&O Defrag sind über einen einzigen Klick erreichbar. Die Software ermöglicht es außerdem erstmalig, SSD-Laufwerke herstellerunabhängig zu optimieren. Mit Hilfe von regelmäßig ausgeführten ATA-TRIM-Befehlen wird einem SSD-Laufwerk mitgeteilt, welche Festplattenbereiche wieder für neue Daten zur Verfügung stehen. Anstatt die nicht mehr benötigten Inhalte gelöschter Dateien weiterhin zu speichern, kann die SSD die frei gewordenen Bereiche für eine laufwerksinterne Optimierung des Datenmanagements verwenden und somit Schreibzugriffe auf das SSD-Laufwerk beschleunigen und darüber hinaus vorzeitige Verschleißeffekte verhindern. Durch die Einteilung von Laufwerken in Geschwindigkeitszonen erfolgt daneben auf Festplatten eine logische Trennung des Datenbestandes in performancekritische und unkritische Dateien. Dateien werden dabei abhängig von ihrem Verwendungszweck und Zugriffshäufigkeit sortiert und in Zonen verschoben. Beispielsweise separiert die Software System- und Programmdateien, die einen besonders schnellen Zugriff erfordern, von anderen Daten, wie Dokumenten und Downloads. Eine zusätzliche Trennung von selten und häufig geschriebenen Dateien soll einer Fragmentierung intelligent vorbeugen. Die O&O Defrag 14 Server Edition soll 249 Euro kosten. Bestehende Kunden zahlen 149 Euro für das Upgrade auf die neue Version. (dr)

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

IT-Administrator-Workshop
“Sicherheit für Windows-Clients”
am 16. November 2010 in München

Das Böse ist immer und überall

von John Pardey

Windows-Clients, auch in Unternehmen, sind nach wie vor das Ziel eines großen Teils der Angriffe aus dem Internet. Neben altbekannten Phishing- oder Malware-Angriffen kommen in letzter Zeit aber immer raffiniertere Angriffsmethoden zum Einsatz. Zuletzt sorgte der LNK-Exploit unter Windows durch seinen neuartigen Verbreitungsweg für Aufsehen. In unserem Workshop am 16. November in München widmen wir uns daher einen ganzen Tag lang der Sicherheit von Windows-Clients.

sich das ursprüngliche Rootkit nur gegen sehr spezielle, industrielle Systeme, lehrt Experten jedoch mit einigen innovativen Angriffsmethoden das Fürchten.

Im Rahmen unseres Workshops zeigt Dembrowski 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. Was IT-Verantwortlichen jedoch weniger bekannt ist, ist die “Industrie” hinter den Schädlingen. Auch in diese führt Dembrowski die Teilnehmer ein, indem er Motivation und Ziele der Malware-Entwickler aufzeigt. Hinter den bekannten Botnetzen verbergen sich nicht selten gut geführte Marktplätze für Windows-Exploits. Ist dem IT-Verantwortlichen erst einmal bewusst, welche starken wirtschaftlichen Interessen die Gegenseite verfolgt, dann sollten Dembrowskis abschließenden Ausführungen zu sinnvollen Gegenmaßnahmen mehr als willkommen sein.

Patchen ist Sicherheit

Eine dieser Gegenmaßnahmen ist zweifellos das regelmäßige Patchen der Windows-Clients. Und so setzt sich im zweiten Vortrag des Tages Thomas Gronenwald, Berater bei adMERITia GmbH, mit dem Thema auseinander, wie Unternehmen ein erfolgreiches Patchmanagement für Windows betreiben können. Vielen Administratoren ist zwar bewusst, dass dies ein essentieller Baustein jedes Security-Konzepts sein muss, doch in der Praxis sehen sie sich hier mit vielfältigen Problemen konfrontiert, zu denen Gronenwald Stellung nimmt.

So zeigt dieser Vortrag unter anderem, wie Unternehmen das Patchmanagement in die Security-Prozesse integrieren sollten. Gronenwald räumt aber gleichzeitig auch mit zahlreichen Mythen rund um das Thema auf und diskutiert anschließend mit den Teilnehmern, welchen Ansprüchen ein Produkt für das Patchmanagement gerecht werden muss, um die Sicherheit tatsächlich zu erhöhen.

Da unser Workshop-Thema “Client-Security” so facettenreich ist, haben wir uns für unseren 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 Dembrowski, der als Ethical Hacker für die entrada GmbH Windows-Systeme auf ihre Sicherheit untersucht.

Windows als Zielscheibe

So war es denn auch Dembrowski, der auf unserer Website als einer der Ersten im deutschsprachigen Raum den “Windows-Link-Exploit” [1] beschrieb und Gegenmaßnahmen aufzeigte. Zwar wendet



Quelle: Photon75 - Fotolia.com

Sicherheit für Applikationen und Zugriff von außen

Zwei weitere Vorträge des Workshops am 16. November beschäftigen sich mit ganz 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. Denn immer häufiger sehen sich Sicherheitsverantwortliche der Anforderung gegenüber, einen sicheren Zugriff für Außendienstler, Home Offices oder auch externe Dienstleister zu gewährleisten. In seinem Vortrag fokussiert Gietl die sicherheitsrelevanten Unterschiede zwischen IPSec- und SSL-VPNs. Eine weitere Quelle möglicher Unsicherheiten sind die Ap-

plikationen 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 vom Client und seinen Anwendungen zu verhindern. Welche technischen, aber auch gesetzlichen Anforderungen Administratoren hierbei beachten sollten, vermittelt Mörl in seinem Vortrag.



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 Dembrowski,
entrata 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

Dozenten: 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 09. November unter

www.it-administrator.de/workshops/

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



Windows-Systeme härten

Zum Abschluss des Workshoptages geht es dann noch mal in die Bits und Bytes von Windows: Sascha Giebelhausen, Berater bei der adMERITia GmbH, härtet Windows-Clients. So erfahren die Zuhörer, warum sie den nicht geringen Aufwand betreiben sollten, Windows-Clients ebenso wie Server zu härten. Giebelhausen schließt den Kreis zum Eröffnungsvortrag unseres Workshops, indem er die zehn am häufigsten ausgenutzten Windows-Schwachstellen aufzeigt und Methoden erläutert, wie Administratoren ihre Clients dagegen wappnen können.

So 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.



Der Windows-Link-Exploit

www.it-administrator.de/themen/sicherheit/fachartikel/86501.html

Links



Bringt abends Arbeit mit nach Hause.

Und morgens Viren in die Firma.

Mitarbeiter sind auch nur Menschen. Da kann es passieren, dass ein privater USB-Stick Ihr ganzes Netzwerk lahmlegt. Oder dass wichtige Daten verloren gehen. Oder in falsche Hände geraten. Oder manipuliert werden. Schützen Sie sich davor!

- Kontrolle sämtlicher PC-Schnittstellen
- 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

Informieren Sie sich jetzt!
www.deviceclock.de oder wählen Sie die Nummer sicher: +49.2102.89211-0

DeviceLock
Proactive Endpoint Security





Für John Craddock weist die Cloud den Weg in die Zukunft, doch Kleingedrucktes gibt es auch in der Wolke

ice:lingen 2010, 13. und 14. August, Lingen an der Ems *Heiter bis wolkig*

von Daniel Richey

“You get what you pay for”, so lautet das Sprichwort, das vor allzu hohen Erwartungen an günstige oder gar kostenlose Errungenschaften warnt. Doch die ice in Lingen ist definitiv eine Ausnahme von dieser Regel. Zum siebten Mal in Folge konnten sich die rund 300 Teilnehmer einen ganzen Tag lang kostenlos über wichtige Trends und Themen rund um die Unternehmens-IT informieren. Das Gleiche galt für den IT-Administrator Workshop am Vortag der ice.

Bereits zum siebten Mal fand am 14. August die ice:lingen statt. Komplette ausgebucht war die Veranstaltung schon rund 28 Tage nach Freischalten der zugehörigen Anmeldeseite. Doch trotz des regen Interesses wollen die Veranstalter die ice bewusst im kleinen, aber feinen Rahmen halten. Dieses Jahr stand der Kongress unter dem Schwerpunkt Cloud Computing. So widmeten Nick Wruck und sein fünfköpfiges Team diesem aktuellen Trendthema denn auch einen eigenen der insgesamt vier Tracks.

Für John Craddock, IT-Infrastructure- und Security-Architekt bei XTseminars in Großbritannien, ist das Prinzip Cloud-Computing an sich nichts Neues. Bereits in den 1960er-Jahren hätten Unternehmer Rechenzentren zur Berechnung von Daten genutzt und den Dienst individuell bezahlt. Dennoch habe sich das Prinzip technologisch weiterentwickelt mit mehr mobilen Devices und mehr Flexibilität. So stellte der IT-Experte in seiner Keynote heraus, wie er sich Cloud Computing eigentlich vorstellt: Einfach und flexibel wie Strom aus der Steckdose. Für Unternehmen würde es denn auch immer schwieriger, die passende IT-Performance passgenau über eigene Re-

chenzentren zur Verfügung zu stellen. So sei die IT entweder nicht leistungsfähig genug oder überdimensioniert. Nichtsdestotrotz gebe es natürlich auch Stolperfallen beim Cloud Computing. Besonders auf die SLAs und das Kleingedruckte sollten Unternehmen achten, bevor sie ihre Daten munter in die Wolke schieben. Hier ließen sich mit dem richtigen Verhandlungsgeschick durch Verbesserungen erzielen.

Verbessern lässt sich mit den richtigen Handgriffen und Tools auch die Migration auf Windows 7. Im Vorfeld der ice fand wieder der IT-Administrator Workshop statt, der sich dieses Mal mit dem Umzug auf das neue Microsoft-Betriebssystem befasste. Rund 25 Abonnenten folgten den Ausführungen der Berater Thorsten Christoffers und Thomas Wegener des Beratungsunternehmens und IT-Dienstleisters sepago. Zunächst erläuterten die praxiserprobten Referenten, welche Vorüberlegungen stattfinden sollten: Passt die Hardware? Sind die richtigen Treiber vorhanden? Muss es unbedingt 64 Bit sein? Was ist mit den alten Applikationen? Anschließend demonstrierten Christoffers und Wegener, wie die Migration von Benutzerprofilen und -Da-

teien mit Hilfe von Microsoft- und Drittanbieter-Tools möglichst reibungslos über die Bühne geht – darunter auch der haus-eigene “Profile Migrator” von sepago. Den direkten Vergleich konnten die Teilnehmer dann zur Baramundi-Management-Suite ziehen. Der IT-Administrator Workshop-Partner baramundi software AG zeigte dem interessierten Publikum seine Lösung im Live-Betrieb und welche Vorteile sie gegenüber einer händischen Migration sowie Life-Cycle-Management bietet. Wie groß das Interesse an diesem Thema derzeit ist, zeigten die detaillierten Rückfragen während der Vorträge.

Fazit

Mit der ice ist die Stadt Lingen an der Ems zum Zuhause für ein ganz besonderes IT-Event geworden. Den Veranstaltern ist es auch im siebten Jahr gelungen, zahlreiche IT-Profis – sowohl auf Teilnehmer- als auch auf Referenten-Seite – für sich zu gewinnen. Und das völlig kostenlos, ebenfalls auf beiden Seiten. Neben all der Expertise kam auch der soziale Aspekt nicht zu kurz: Rund 2.000 Euro spendeten die Teilnehmer für das Kinderhilfsprojekt “com for children” von Nicki Wruck und seiner Frau Christine. 



IT-Service-Management in der Praxis: Windows 7 Migration und Office 2010 Rollout

Automatisierte Windows 7 Migration

Der Umstieg von Windows XP oder Vista auf Windows 7 lockt mit einigen Vorteilen. Aber Migrationen haben auch ihre Tücken. Wir zeigen Ihnen live, wie Sie von Windows XP auf Windows 7 sicher und problemlos migrieren. Von der Planung über Hard- und Softwarescan bis zur erfolgreichen Migration.

Plus Praxisbericht unseres Kunden: Herr Küster von CMS Hasche Sigle, einer der größten deutschen Rechtsanwaltssozialitäten, wird Ihnen von seinen Erfahrungen bei der Umstellung von 1.200 Clients auf Windows 7 berichten.

Was ist bei einem Rolloutkonzept zu beachten: Hardwareauswahl, Treiberkompatibilität, Lizenzbeschaffung, Kosten. Wie sollten Sie am besten umstellen: Big Bang oder Stufenweise? Welche Installationstechnik am besten verwenden: Cloning oder Unattended-Installation? Außerdem erhalten Sie nützliche Tipps & Tricks, zum Beispiel wie Sie am besten Anwendungen portieren und Benutzerprofile migrieren. Und Herr Küster berichtet, warum Anwenderschulungen so notwendig sind und wie Sie in der Planung am besten vorgehen sollten, wie Sie Ihren internen Support aufstellen sollten und zum Schluss die Akzeptanzanalyse durchführen.

Office 2010 Rollout

Nach der Live-Installation von Windows 7 erleben Sie auch gleich den Rollout von MS Office 2010. Sie erfahren, wie die baramundi Management Suite Sie bei Skripterstellung, Softwarelizenzmanagement und Datenweiterverarbeitung unterstützt. Denn die baramundi Management Suite übernimmt nicht nur viele administrative Aufgaben, sie wird auch zur Schnittstelle zu anderen Anwendungen. Wir zeigen Ihnen, wie baramundi Connect mit dem OMNITRACKER Helpdesk der Firma OMNINET nahtlos zusammenarbeitet.

Client Management und Helpdesk-Integration

Begleiten Sie einen Helpdesk Agent live bei der schnellen Lösung von Anwenderproblemen. Über baramundi Connect erhält er Zugang zu allen nötigen Hardware- und Softwaredaten, sieht, welche Anwendungen wann und wie installiert oder modifiziert wurden. Eine Mail mit einem Problem wird so zum Startpunkt einer Fährtsuche, die zur gezielten Lösung führt und auch hilft, künftig ähnliche Probleme zu vermeiden.

Ihr IT-Praxistag

Was kann die baramundi Management Suite für Ihre IT-Praxis tun?
Antworten erhalten Sie schon bald in diesen sieben Städten:

- 11.10.2010 - **München**, Golden Tulip & Tulip Inn Munich City
- 12.10.2010 - **Stuttgart**, Meilenwerk Region Stuttgart
- 20.10.2010 - **Nürnberg**, Rödl & Partner
- 26.10.2010 - **Berlin**, Pullmann Berlin Schweizerhof
- 27.10.2010 - **Hamburg**, east Hotel & Restaurant GmbH
- 09.11.2010 - **Frankfurt**, 25hours Hotel Frankfurt by Levi's
- 10.11.2010 - **Essen**, Atlantic Congress Hotel Essen



Die Teilnahme ist für Sie kostenlos.



baramundi software AG
Beim Glaspalast 1
86153 Augsburg

Fon: +49 (821) 5 67 08 - 300
Fax: +49 (821) 5 67 08 - 19
E-Mail: focustour@baramundi.de

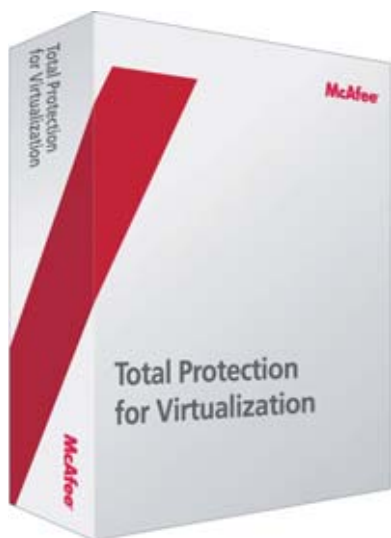
Weitere Informationen und
die detaillierte Agenda finden Sie online unter:
www.baramundi.de/focustour

IT einfach clever managen

**Im Test: McAfee Total Protection for Virtualization**

Schotten dicht im virtuellen Raum

von Thomas Bär



So virtuell die Rechenzentren auch geworden sind, so real sind die Gefahren, die für die betriebenen Systeme zu beinahe jedem Zeitpunkt herrschen. Denn so gut wie jeder Server steht in einer Verbindung, die schlussendlich ihren Weg ins Internet oder in weniger sichere Bereiche des Unternehmens findet. Die Frage, ob virtuelle Systeme anders geschützt werden müssen als ihre physikalischen Pendanten, beantwortet McAfee mit einem klaren Ja und hat einen speziellen Virtualisierungs-Schutz im Portfolio. In unserem Test haben wir uns die einzelnen Komponenten dieses Sicherheitskonzepts angesehen und verraten Ihnen, ob dem Hersteller ein stimmiges und gut zu verwaltendes Gesamtprodukt gelungen ist.

Vor gut zwei Jahren hat McAfee erstmalig eine Sicherheits-Suite auf dem deutschen Markt vorgestellt, die speziell auf Kunden zugeschnitten ist, die in professionellem Stil Virtualisierung betreiben. Da es sich bei "McAfee Total Protection for Virtualization" um ein Bündel aus Einzelprodukten handelt, hat der Hersteller dafür keine separate Versionsnummer definiert – in erster Linie ist es der Preis, der im Paket für die Gesamtheit der Einzelprodukte niedriger ausfällt. Was auf den ersten Blick wie ein Bauchladen an Sicherheitselementen für virtuelle Umgebungen wirken mag, präsentiert McAfee als stimmiges Sicherheitskonzept für große oder technologisch hoch entwickelte Unternehmen.

Die Suite besteht zum einen aus dem ePolicy Orchestrator, einer Plattform, über die sich die Schutzsysteme des Herstellers zentral im Unternehmensnetz steuern lassen. Außerdem mit dabei sind der VirusScan Enterprise für Offline Virtual Images, die Host Intrusion Preven-

tion für Server und VirusScan Enterprise für Windows beziehungsweise Linux. Ähnliche Produkte bieten auch die Mitbewerber wie Symantec, Trend Micro oder Sophos an. McAfee hebt jedoch den Offline Virtual Images Scanner und den ePolicy Orchestrator als die entscheidenden Unterschiede zur Konkurrenz besonders hervor.

Umfangreiches Paket an Schutzfunktionen

Grundsätzlich unterscheidet sich die Anforderung in Bezug auf die Sicherheit kaum – egal ob es sich um virtuelle oder physikalische Geräte handelt. Ein Betriebssystem oder eine Applikation kann, sofern Sicherheitslücken bestehen, durch Schadsoftware infiziert oder gestört werden. Somit ist das Verteidigungs-Arsenal der Administratoren in virtuellen Umgebungen identisch gefüllt: mit den bewährten Mitteln zum Virenschutz und zur Spyware-Abwehr sowie mit Host Intrusion Prevention-Lösungen. Wie die meisten Hersteller von Sicherheitsprodukten

bezeichnet McAfee seine Technologie als proaktiv – sprich, die Lösung soll eingreifen, bevor etwas passiert.

Die Feature-Liste von McAfees Sicherheitslösung ist lang – egal ob die Maschinen nur virtuell oder physikalisch existieren. On-Access-Scanner hindern Malware, Rootkits, Spyware, Bots, Trojaner und andere unerwünschte Programme daran, sich

Für die Basisinstallation ist eine typische und aktuelle Windows-Umgebung ausreichend. Verschiedene Clients für unterschiedliche Betriebssysteme lassen sich zentral über ePolicy Orchestrator verwalten. VirusScan Enterprise für Offline Virtual Images verlangt nach einem x86-Prozessor, Intel Pentium IV oder höher mit mindestens 2 GHz und 1 GByte RAM und .NET-Framework 2.0. Die Software arbeitet auf den Betriebssystemen Windows XP (nur x86), Vista (x86 und x64), Server 2003 R2 (nur x86) und Server 2008 (x86 und x64) in den Editionen Standard, Enterprise und Datacenter. Server Core-Installationen werden nicht unterstützt.

Systemvoraussetzungen



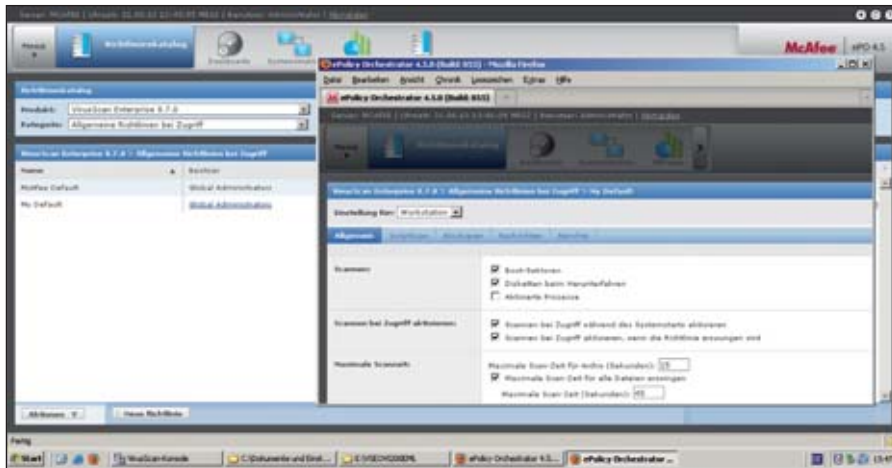


Bild 1: Mit "ePolicy Orchestrator 4.5" von McAfee kann der Nutzer beinahe alle administrativen Einstellungen der Sicherheitslösungen zentral aus einer übersichtlichen Intranet-Webseite heraus steuern

auf einem Computer zu installieren und weiter zu verbreiten. Zero-Day-Bedrohungen unterbindet der virtuelle Schutzwall durch das gezielte Blockieren von unerwünschten Aktivitäten – die Lösung kombiniert hierbei Signaturen und das verhaltensbasierte Intrusion Prevention System (IPS) mit einer Stateful-Firewall und Anwendungskontrolle.

Als Ergänzung oder Erweiterung zu den Fähigkeiten des Betriebssystems erlaubt McAfee weiterhin das Setzen von Regeln, die Änderungen an Dateien, der Registry oder Dienstprogrammen verhindern. Die verhaltensbasierte Technologie soll Hacker davon abhalten, bösartigen Code bei Buffer Overflow-Angriffen Rechnern einzuschleusen. Ebenfalls im Repertoire von McAfee findet sich eine Funktion zur Richtlinienüberprüfung. Schwachstellen, fehlerhafte Servicekonfigurationen und Richtlinienverstöße auf Client- oder Serversystemen werden so erkannt und dem Administrator gemeldet.

Speziell für virtuelle Umgebungen gedacht ist der Schutz für virtuelle Images im Offline-Modus namens VirusScan Enterprise for Offline Virtual Images. Die Laufwerksdateien virtueller Maschinen unterlaufen mit Hilfe dieser Software eine Prüfung auf maligne Inhalte, ohne dass die VM dazu in Betrieb sein müsste. So ist sichergestellt, dass nur virtuelle Ma-

schinen ohne eine Sicherheitsbedrohung in Betrieb gehen.

Installation verlangt nach richtiger Reihenfolge

Unseren Test führten wir auf einem typischen Windows Server 2003 in einer Active Directory-Umgebung durch. Der Testmaschine haben wir gemäß den Empfehlungen in der Produktdokumentation 1,5 GByte Arbeitsspeicher zugewiesen. Da sich keine Information zur Anzahl von CPU-Cores fand, haben wir dem virtualisierten Server auch nur einen einzigen Prozessorkern zugeordnet. In dieser Konfiguration reagierte die Software subjektiv stets zügig und das Arbeiten war jederzeit flüssig möglich.

Die Installation beginnt mit der zentralen Verwaltungssoftware, dem ePolicy Orchestrator. Da sich keine Microsoft SQL-Datenbankinstallation auf dem Testserver befand, richtete der Assistent diese in Rücksprache mit dem Administrator vollautomatisch ein. Das gesamte Setup dauerte nur einige Minuten und endete mit der Möglichkeit, sich auf der frisch eingerichteten Intranet-Seite auf den Server zu verbinden. Dieser Vorgang scheiterte jedoch zunächst an einem nicht mehr aktuellen Internet Explorer 6. Ein nachträglich installierter Firefox löste das Zugriffsproblem nicht – der Link auf dem Desktop ist fest mit dem Internet Explo-

rer verknüpft und passt sich nicht einem Wechsel des Standardbrowsers an. Das Anmelden auf der anfangs noch leeren Infrastruktur zeigte dann eine moderne Webseite, die an Funktionalität einer lokalen Konsole in nichts nachsteht.

Im nächsten Schritt versuchten wir, VirusScan Enterprise for Offline Virtual Images auf unserem Testserver einzurichten. Ohne das vorherige Einspielen der Basisinstallation von VirusScan Enterprise 8.7i war dies jedoch nicht möglich. Das Programm ist in der Windows-Ausprägung mit knapp über 25 MByte ein äußerst kleines Installationspaket. Entsprechend lang dauerte die Aktualisierung der Signaturdaten nach dem Neustart. Ebenfalls einige Zeit muss der Sicherheitsverantwortliche für die Komplettuntersuchung des Servers einplanen. Der McAfee-Scanner nimmt es sehr genau, lässt sich auf Wunsch des Administrators aber jederzeit abbrechen. Ein Blick in das deutschsprachige Readme brachte eine echte Überraschung. Die Testversion, die Interessierte 90 Tage kostenlos ausprobieren können, ist anscheinend schon etwas länger auf den Servern von McAfee, lauten doch die ersten Sätze im Dokument: "Die Betaversion dieses Produkts steht bis zum Ablauf der Betaproduktlizenz am 30. November 2008 zur Verfügung" und "Diese Version unterstützt Windows Server 2008 (Longhorn)".

Danach klappte dann das Aufspielen von "VirusScan Enterprise for Offline Virtual Images" – in der deutschen Übersetzung als "McAfee VirusScan Enterprise für virtuelle Laufwerke im Offline-Zustand" bezeichnet. Die Einrichtung dauerte nur einige Augenblicke und nach einem Neustart der Software stand die Oberfläche in der lokalen Konsole von "VirusScan" zur Verfügung. Alternativ lässt sich das Programm auch über ePolicy Orchestrator (EPO) verwalten.

Spezieller Schutz für Offline-VMs

Auf den ersten Blick wirkt VirusScan Enterprise for Offline Virtual Images 2.0 sehr

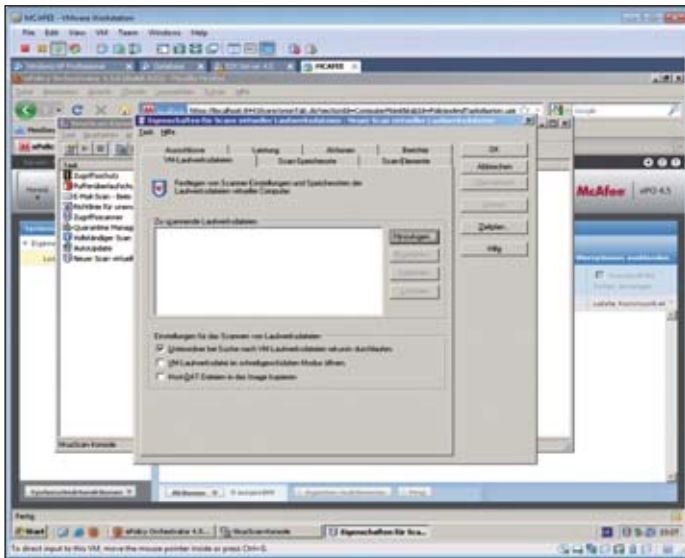


Bild 2: "VirusScan Enterprise für Offline Virtual Images" lässt sich über die lokale VirusScan-Konsole konfigurieren oder über die ePolicy Orchestrator-Versionen 4.0 und 4.5 verwalten

unscheinbar, besteht es doch aus gerade einmal sieben Registern und einem Zeitplaner. Die erste Testaufgabe für die Software bestand in der Überprüfung einer virtuellen Festplatte, die wir unter Windows 7 erzeugt haben. Die Vorgehensweise hierzu erklärt sich nahezu von allein: Ein neues VM-Laufwerk zur Prüfung mit dem Button "Hinzufügen" über einen kleinen Assistenten einhängen und den Scanvorgang starten.

Überzeugender Regelbetrieb

Bei der Typ-Auswahl unterscheidet McAfee zwei Arten von virtuellen Servern beziehungsweise Laufwerkdateien: Die Herkunft aus VMware ESX Server / VMware vCenter Server oder VMware Workstation/Server, Virtual PC, Hyper-V oder ISO-Laufwerksdateien. Die für den ersten Test er-

Intel schluckte Ende August unerwartet den Antiviren-Spezialisten McAfee. Mit einem Aufschlag von 60 Prozent auf den Aktienkurs des Vortags und einem Gesamtvolumen von rund 7,7 Milliarden US-Dollar ist das Angebot von Intel für McAfee üppig ausgefallen – für den Chiphersteller ist es die größte Übernahme der Firmengeschichte. Intel erhofft sich nach eigenen Angaben, durch die Kombination von Software und Hardware einen besseren Schutz der Kundensysteme verwirklichen zu können.

McAfee als Teil von Intel



zeugte VHD-Datei stand somit nicht direkt in der Typenauswahl zur Verfügung. Da es sich bei der Datei jedoch um das im Virtual-PC-System gebräuchliche Format handelt, ließ sich die Prüfung ohne Probleme starten. Das Ergebnis veränderte sich auch dann nicht, wenn wir anstelle des verbreiteten Master Boot Record

(MBR) die modernere GUID Partition Table (GPT) nutzten.

Die Erkennungsrate der Virenabwehr haben wir für diesen Test nicht überprüft. Statt verschiedene Schadprogramme einzusetzen, beließen wir es beim Einspielen des EICAR-Teststrings. Dieser untersucht, ob die Antiviren-Engine generell auf mögliche Bedrohungen anspringt – was in unserem Fall problemlos klappte.

Üppige Storage-Unterstützung

VirusScan Enterprise für Offline Virtual Images ist nicht auf die Zuordnung einzelner virtueller Maschinen beziehungsweise deren virtuellen Festplatten-Laufwerke beschränkt. Statt jedes einzelne System zu selektieren, ist es möglich, ganze Ordner auszuwählen, in denen die Software dann rekursiv nach untersuchbaren Images fahndet. Was Storage betrifft, unterstützt VirusScan Enterprise sowohl direkt angeschlossene Laufwerke als auch SAN- oder NAS-Laufwerksdateien. Der Zugriff auf CIFS-Laufwerke mit Netzwerkfreigaben funktioniert ebenso wie der direkte Zugriff. Zu den unterstützten VMDK-Speichertypen gehören Fibre Channel, iSCSI und NFS.

In der Fortschrittsanzeige ist zwar jederzeit zu sehen, welche Datei und welcher

Ordner aktuell im Image untersucht werden, nicht jedoch, welches Image derzeit bearbeitet wird. Eine zeitliche Schätzung, bis wann eine Untersuchung voraussichtlich dauern wird, vermisst der Administrator ebenso. Einziger Anhaltspunkt in dieser Richtung ist der Hinweis, die wievielte Imagedatei in Bezug auf die Gesamtzahl sich gerade unter der Lupe befindet.

Umfangreiche Steuerungsparameter

Der Administrator kann Einstellungen im laufenden Betrieb vornehmen, sprich während eine Untersuchung in Gang ist. Dann wirken sich die Änderungen in der Konfiguration allerdings erst beim nächsten Scandurchlauf aus. Will der Nutzer beispielsweise die Systemauslastung beim Scan auf einen definierten maximalen Prozentwert festlegen, arbeitet eine aktuelle Untersuchung mit dem Vorgängereintrag weiter. Die Parametrierungs-Möglichkeiten für VirusScan Enterprise für Offline Virtual Images sind umfangreich. Der Scheduler gestattet eine feine zeitliche Steuerung und das Hinterlegen von Zugangsinformationen.

Wie der Wächter auf einen Virusfund im Abbild einer virtuellen Maschine reagieren soll, legt der Nutzer separat fest – unabhängig davon, was allgemein für VirusScan Enterprise definiert ist. Zur Auswahl stehen die typischen Einstellungen wie "Säubern", "Löschen", "auf Benutzerauswahl reagieren" oder "den Scan fortsetzen". In der Standardeinstellung versucht das Programm zunächst, die betroffene Datei vom Schädling zu säubern. Ist dies nicht möglich, so wird sie gelöscht.

Über die Registerkarte "Ausschlüsse" ist der Administrator dazu in der Lage, bestimmte Elemente vom Scan auszuschließen. Zur Auswahl stehen hier Dateinamenerweiterungen, Ordner oder vollständig benannte Dateien – hierbei sind auch Textmuster erlaubt. Eine weitere Handhabe ist die Auswahl der Option "Geschützt durch Windows-Dateischutz", sprich Dateien, auf die Windows den Systemdateischutz anwendet, werden keinem Scan unterzogen.

Wackelige Ausnahmeregel für VMs im laufenden Betrieb

Eine Untersuchung von laufenden virtuellen Maschinen ist mit der Software weder möglich noch erforderlich. Da eine aktive VM typischerweise durch einen aktiven Online-Scanner geschützt ist, besteht an dieser Stelle kein Handlungsbedarf. Befindet sich eine VM in Betrieb, so sind die entsprechenden Dateien durch Lock-Mechanismen markiert. Diesen Hinweis erkennt Virus-Scan Enterprise for Offline Virtual Images und greift nicht auf die Datei zu. Leider hat der Lock-Mechanismus jedoch seine Tücken: Wird eine VM unsauber beendet, beispielsweise durch ein Ausfall der Virtualisierungsplattform, so bleibt der Lock-Hinweis bestehen, obwohl die VM eigentlich ausgeschaltet und prüfbar wäre. Dann überspringt der Scheduler bei der Überprüfung diese Dateien genauso wie VMs und setzt die Untersuchung mit dem nächsten Kandidaten fort. Selbiges gilt für pausierte VMs, die ja eigentlich aktiv sind – nur eben gerade jetzt nicht.

Schwierigkeiten hatte die Software außerdem mit der Erkennung von freien Betriebssystemen auf der virtuellen Festplatte: Während alle Windows-Versionen

ab 2000 SP4 für den Scanner kein Problem darstellten, so reagierte das Programm bei Linux/Unix-Betriebssystemen mit dem lapidaren Hinweis "Fehler beim Mounten des virtuellen Laufwerks 0. Laufwerk ist möglicherweise in Benutzung". Anhand der Konfiguration der VM hätte VirusScan Enterprise für Offline Virtual Images eigentlich erkennen sollen, dass es sich bei der Testdatei um ein FreeBSD-basiertes System handelt.

Bedrohungs-Top 10

Die Reports der VirusScan Enterprise for Offline Virtual Images gibt die Suite im ePolicy Orchestrator aus. Eine Abfrage listet die am häufigsten erkannten Bedrohungen als Übersichtstabelle auf, darunter die Top 10 der letzten drei Monate. Die im Laufe der letzten beiden Quartale entdeckten Bedrohungen werden als Balkendiagramm angezeigt, entdeckte Cookies sind jedoch nicht in der Aufstellung enthalten.

Fazit

Wird eine Image-basierte Suche nach Schadprogrammen in Offline-VMs oder Festplattencontainerdateien benötigt, so ist McAfee Total Protection for Virtualization dazu gut geeignet und funktionsfähig. Zu beachten ist allerdings stets, dass

Sicherheitslösungen von Haus aus komplexe Programme sind. Wichtig für deren korrekten Einsatz ist das entsprechende Wissen auf Seiten der Administratoren. Der Hersteller bietet daher Workshops für Unternehmen an, die die Virtualisierungs-Produkte einsetzen wollen. Bis die Software reibungslos läuft, sind laut McAfee rund zwei Arbeitstage für die Implementierung einzuplanen. Handbücher sind ausschließlich online vorhanden – jedoch auch auf Deutsch. (In) 

Produkt

Virenschutz für virtualisierte Umgebungen.

Hersteller

McAfee
www.mcafee.com/de/

Preis

Die Lösung kostet 2.876 Euro pro physikalischen Server oder Hypervisor. Die Lizenz gilt für ein Jahr und beinhaltet in diesem Zeitraum Gold-Support von Seiten des Herstellers.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Systemanforderung **8**

Flexibilität der Lösung **9**

Administrierbarkeit **8**

Sicherheitsfunktionen **9**

Automatisierbarkeit **8**

Dieses Produkt eignet sich

optimal für große und technisch hochentwickelte Unternehmen, die in den virtuellen Umgebungen ein Maximum an Sicherheit einfordern.

bedingt für Unternehmen, die über eher geringes Know-how im Bereich Virtualisierung verfügen.

nicht für Unternehmen, die keine virtuellen Systeme betreiben.

**McAfee Total Protection
for Virtualization**

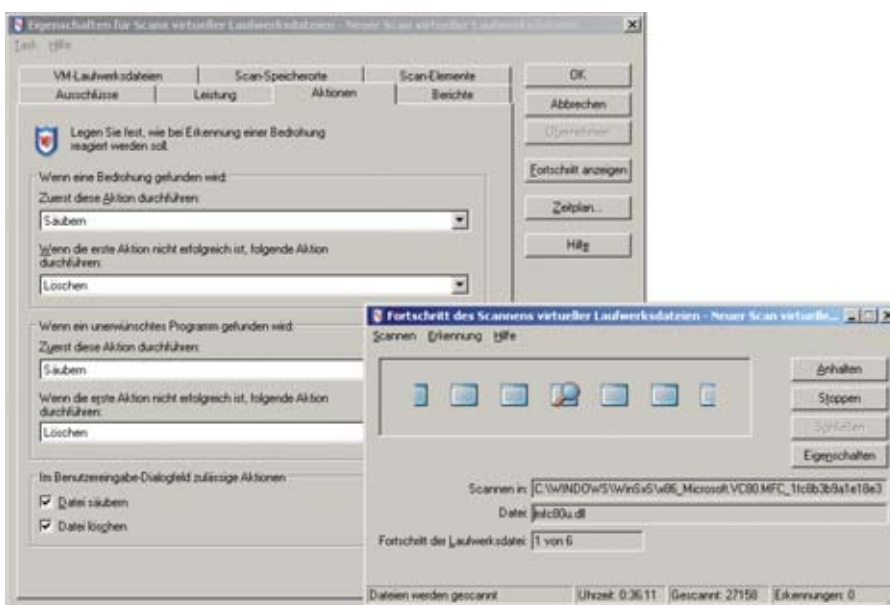


Bild 3: Wie lang ein Untersuchungsvorgang dauern wird, muss der Administrator erraten – die Software gibt hierzu keine Hinweise



Im Test: *Itelio Docusnap 5.0* **Die Übersicht behalten**

von *Sandro Lucifora*

Um den Überblick in einem Netzwerk zu behalten, bietet der Softwaremarkt diverse Tools zur Dokumentation der Infrastruktur an. Docusnap 5.0 will jedoch mehr, als nur die vorhandene Hard- und Software zu visualisieren. Es erweitert die Übersicht auch durch Rechte- und Lizenzanalysen. IT-Administrator hat sich die Fähigkeiten des aktuellen Release im Praxistest angeschaut.

Der modulare Aufbau von Docusnap 5 ermöglicht es dem Administrator, den Umfang des Tools nach den individuellen Bedürfnissen des Unternehmens anzupassen. So lassen sich auch die Erfassungsmaske und Berichte auf die persönlichen Wünsche einstellen. Im ersten Schritt wird der Ist-Zustand des Netzwerkes erfasst. Dazu müssen auf den zu inventarisierenden Zielgeräten keinerlei

Installation, keine Treiber oder Agenten eingerichtet werden – das ist schon mal ein großer Pluspunkt. Die ermittelten Daten werden zentral in der zuvor eingerichteten Datenbank gespeichert und jederzeit abgerufen. Im nächsten Schritt findet die Dokumentation der erfassten Daten in verschiedenen Formaten und Berichten statt. Dabei ist es den Nutzern überlassen, welche Teile des Netz-

werkes in welcher Form übersichtlich dargestellt werden. Beide Prozesse werden nach der erstmaligen Konfiguration auch durch den optional installierbaren Docusnap-Server automatisch angestoßen und benötigen keine weiteren Eingriffe unsererseits. So lagen uns jederzeit tagesaktuelle Netzwerkdokumentationen vor.

Setup mit Starthilfe

Die Installation erfolgt mittels einer 180 MByte großen Installationsdatei. Beim benutzerdefinierten Setup kann ausgewählt werden, ob der Docusnap Client und/oder der Docusnap Server installiert werden soll. Sowohl Server als auch Client lassen sich auf separaten Rechnern betreiben. Beim ersten Start öffnete sich "Docusnap Start", ein Assistent für die erste Konfiguration im Netzwerk. Nach der Überprüfung der Systemvoraussetzungen erfolgt die Lizenzierung. Anhand der Lizenz werden die lizenzierten Module freigeschaltet. Im nächsten Schritt legten wir die verwendete Datenbank fest. Es werden sowohl MS SQL Server als auch Access-Datenbanken unterstützt. Docusnap liefert zwar eine MDB-Datei mit, empfiehlt jedoch vorrangig den Einsatz eines MS SQL-Servers. Dabei reicht auch die Expressversion, um die Daten zentral zu speichern. Im Test nutzten wir einen zentralen MS SQL-Server mit einer neu angelegten Instanz. Es kann jedoch auch eine bestehende Datenbank verwendet werden. Im Bereich "Einstellungen" definierten wir nun die Pfade, unter denen Dokumentationen, Einstellungen und Anlagen abgelegt werden sollen. Hier gibt es lokale- und Team-Einstellungen. Weiterhin konnten wir feste Anlagen, wie Bilder oder Grundrisspläne, hinzufügen. Diese werden in der Datenbank gespeichert, stehen damit allen Docusnap Clients zur Verfügung und können später zum Beispiel Berichten hinzugefügt werden.

Um das Modul "Passwörter" zu aktivieren, mussten wir noch eine Verschlüsselungsdatei anlegen. Diese bildet die Grundlage, um die im System abgeleg-

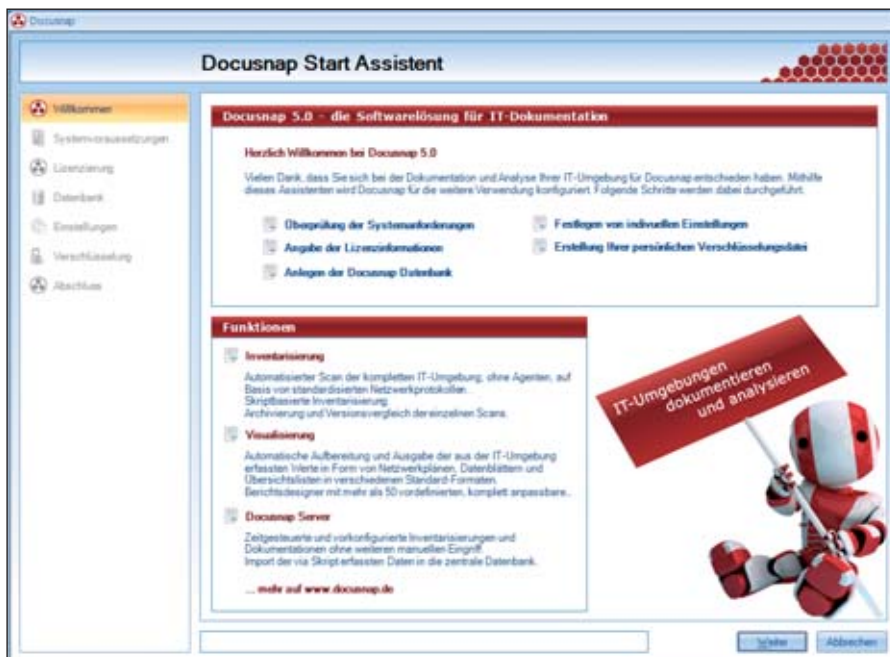


Bild 1: Beim ersten Start von Docusnap öffnet sich der Assistent, mit Hilfe dessen Docusnap für den Betrieb konfiguriert wird



ten Passwörter verschlüsselt in der Datenbank zu speichern. Diese Kennwörter können dann nur von Benutzern ausgelesen werden, die die gleiche Verschlüsselungsdatei verwenden. Im Test haben wir festgestellt, dass mit der Verschlüsselungsdatei sorgsam umgegangen werden muss, da es keine Möglichkeit gibt, diese bei Verlust zu rekonstruieren.

Inventarisierung mit Extra-Einladung

Sind die Installation und Konfiguration abgeschlossen, kann die erste Inventarisierung erfolgen. Hierzu starteten wir Docusnap und wechselten in die Multifunktionsleiste "Inventarisierung". Dort finden sich die Funktionen "Netzwerk scannen" und "Rechte scannen", die auch nacheinander ausgeführt werden sollten. Als "Netzwerk" kann der Administrator auch nur Teile des Netzwerkes oder einzelne Geräte festlegen. Wir

wählten für das erste Mal für einen Scan die komplette Netzwerk-Erfassung aus.

Der übersichtliche Assistent fragte uns anschließend nach Details zu der Inventarisierung der einzelnen Geräte und Komponenten, bevor er den Scan startete. Die Bedienung des Assistenten ist beim ersten Mal gewöhnungsbedürftig, doch fanden wir uns einmal zurecht, brachte uns die durchgängig gleiche Benutzerführung schnell ans Ziel. Im Test haben wir für die initiale Datensammlung einige Geräte vom Netz getrennt, um zu testen, ob diese später problemlos nachinventarisiert werden. So viel vorweg: Das hat reibungslos funktioniert. Bei der Sammlung der Geräteinformationen war das Desktop-Gerät mit Windows 7 angeblich nicht erreichbar, trotz deaktivierter Firewall. Es hat sich herausgestellt, dass Windows 7 einen Neustart nach dem Ausschalten der Firewall benötigte, um die Anfragen von Docusnap zu beantworten. Im Regelfall werden in Unternehmens-Netzwerken jedoch durch die Policy alle Firewall-Regeln gesteuert. Daher ist es empfehlenswert, nur die benötigten Ports für die Anfrage von Docusnap-Diensten auf diesem Wege und nur für den Rechner, über den die Anfragen laufen, zu öffnen.

Nach jeder Inventarisierung legt Docusnap einen Snapshot der Daten an – maximal fünf Stück. Damit ist es möglich auch eine Entwicklung des Netzwerk-Inventars nachzuvollziehen. Ist ein Snapshot besonders interessant, kann dieser unabhängig von den fünf Snapshots "eingefroren" und später zum Vergleichszwecken herangezogen werden.

Gelungene Rechteanalyse

Die vollständige Übersicht, welcher User und welche Gruppe auf welche Verzeichnisse und Daten zugreifen dürfen, ermit-

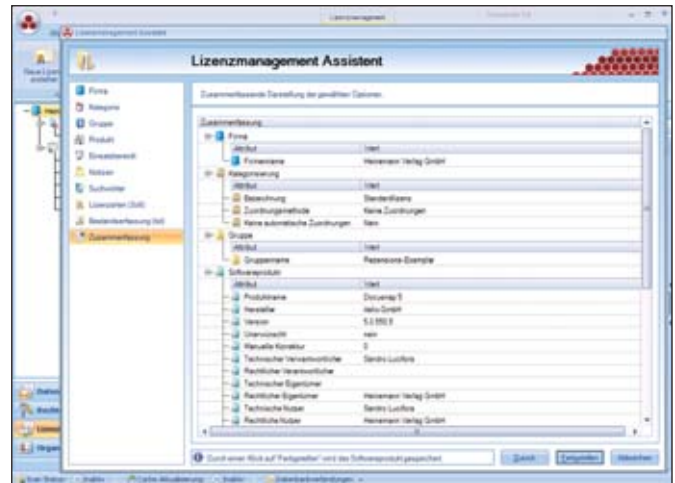


Bild 2: Das Lizenzmanagement gibt eine Übersicht der vorhandenen Lizenzen

telt die Rechteanalyse in Docusnap 5. Sie scannt alle Zugriffsberechtigungen freigegebener Verzeichnisse und Dateien. Der erste Scan, der problemlos ohne Aufsicht lief, dauerte in unserem Test gut eineinhalb Stunden und fand dabei rund 20.000 Freigaben. Danach erhielten wir eine komplette Übersicht, auf welche Verzeichnisse und Daten im Netzwerk überhaupt zugegriffen werden darf. Weiterhin erfuhren wir detailliert, welche Gruppen und User mit welchen Rechten zugreifen durften. Die Filter-Funktion in der Anzeige der Rechteanalyse kann zum Beispiel gezielt und aufschlussreich zeigen, auf welche Daten ein bestimmter User zugreifen darf. Das ist ein sehr sinnvolles Tool, um Sicherheitslücken aufzuspüren oder um im Gegenteil zu prüfen, ob ein Mitarbeiter auch auf das Zugriff hat, wozu er berechtigt sein soll.

Lizenzen im Griff

Ein großer Risikofaktor in der Infrastruktur von Netzwerken ist die falsche Lizenzierung von Software. Während die unnötige Überlizenzierung zusätzliches Kapital bindet, steht die Geschäftsleitung eines Unternehmens durch unlizenzierte Software quasi mit einem Bein im Gefängnis. All diese Szenarien erkennt Docusnap 5. Um über die vorhandenen und installierten Softwarelizenzen den Überblick zu erhalten, ist das integrierte Lizenzmanagement die passende Lösung. Bei der normalen Inventarisierung ermit-

Folgende Netzwerksysteme können mit Docusnap 5.0 erfasst und dokumentiert werden:

- Microsoft Server & Workstations (ab NT)
- Linux 32/64 Bit (SuSe, Red Hat, Kubuntu)
- Macintosh-Rechner
- Virtuelle Rechner und VMware-Hosts
- Active Directory
- SNMP-fähige Systeme wie Router, Switches, Firewalls, Netzwerkdrucker
- MS Exchange & SQL Server Applikationen
- MS DHCP/DNS Serverdienste

Systemanforderungen für die Installation:

- Betriebssystem: Windows XP SP2, Vista, Windows 7, Server 2003, Server 2008
- RAM: mindestens 512 MByte
- .NET-Framework ab 3.5
- Datenbank: Wahlweise SQL 2005 Express/Standard/Enterprise; SQL 2008 Express/Standard/Enterprise
- Microsoft Visio 2007 SP1 (zur Erstellung von Plänen)

Systemanforderungen





telt Docusnap auch die Software, die im Netzwerk installiert ist. Dabei findet es jedoch keine Lizenznummern. Das liegt zwar in der Natur der Sache, da es keine Regel für das Speichern von Lizenznummern gibt, doch könnten zumindest bei den Lösungen von Microsoft, Adobe und anderen "großen" Anbietern entsprechende Funktionen zum Auslesen durchaus eingebunden werden. Damit würde sich ein Großteil der eingesetzten Software bereits erkennen lassen.

Um einen aussagekräftigen Ist-Soll-Vergleich zu bekommen, muss Docusnap nun noch wissen, welche Lizenzen ein Unternehmen gekauft hat. Komfortabel über den Import oder etwas aufwändiger mit der manuellen Anlage werden diese Angaben im Lizenzmanagement eingepflegt. Während dieses Prozesses zeigte uns Docusnap 5 an, auf welchen Geräten die jeweilige Software zum Ein-

satz kam. Im Assistenten haben wir dann die gefundenen Geräte den tatsächlich vorhandenen Lizenzen zugewiesen. In der Gesamtübersicht ließ sich so schnell erkennen, ob die Lizenzierung im Unternehmen ausreichend war.

Überzeugende Visualisierung

Bisher haben wir uns mit dem Erfassen von Daten befasst. Interessant wird es, wenn die Sammlung an Informationen über Berichte visualisiert wird. Dazu greift Itelio auf die Engine von Microsoft Visio zurück. Schon mit der Standardversion von Visio 2007 und 2010 lassen sich Netzwerkpläne, Exchange-Pläne, DNS- und DHCP-Server-Pläne und viele andere Informationen visualisieren. Die so erstellten Darstellungen können dann weiterverarbeitet werden. Insgesamt bekommt der Anwender 30 verschiedene Ausgabeformate und Reports mitgeliefert.

Während Docusnap von jeder Workstation im Netzwerk aus Daten sammeln kann, werden mit dem Docusnap-Server die Funktionen angestoßen, ohne dass ein manueller Eingriff seitens des Anwenders notwendig ist. Daher sollte dieser Dienst auch auf einem Netzwerkservers installiert sein. So kann die komplette Inventarisierung über eine Zeitsteuerung und mit anschließender Dokumentationserstellung erfolgen.

Fazit

Docusnap bietet mit dem aktuellen Release 5.0 umfangreiche Funktionen für einen strukturierten, detaillierten und automatisierten Dokumentationsprozess. Neben der eigentlichen Dokumentation, die auch von anderen Lösungen bekannt ist, stellt das Werkzeug sinnvolle Module zur Erweiterung bereit. Hervorzuheben sind die Rechteanalyse und Lizenzverwaltung. Durch den Einsatz von Visio ist das Erstellen der Berichte sehr umfangreich ausgefallen, doch gleichzeitig wird auch eine zusätzliche, kostenpflichtige Lizenz für Visio benötigt. Für IT-Dienstleister interessant ist die

Mandantenfähigkeit, die es ermöglicht, Netzwerkdaten ihrer Kunden in derselben Datenquelle zu verwalten.

Insgesamt hat Docusnap 5 zuverlässig und vor allem ohne Eingriff in den internen Arbeitsablauf Daten gesammelt und dargestellt. Um das System inklusive Lizenzmanagement sinnvoll einzusetzen, muss sich der Administrator zuvor Zeit nehmen, um alle notwendigen und nicht automatisch zu ermittelnden Angaben manuell zu erfassen. Danach erhält der Anwender ein mächtiges Tool, mit dem er die Dokumentationswünsche jeder Geschäftsleitung erfüllen kann. (dr) 

Durch zusätzliche Module lässt sich der Funktionsumfang von Docusnap 5.0 den individuellen Bedürfnissen anpassen:

- **Rechteanalyse:** Erfassung und Analyse der effektiven Verzeichnisberechtigungen
- **Lizenzverwaltung:** Soll-/Ist-Abgleich von installierten und gekauften Lizenzen inklusive Vertragsverwaltung
- **VMware:** Inventarisierung von VMware Infrastrukturen und virtualisierten Rechnern
- **Exchange Server:** Dokumentation von Microsoft Exchange Server Komponenten und Exchange Infrastruktur
- **SQL Server:** Erfassung von Datenstrukturen bis Tabellen-Level
- **DHCP/DNS:** Server Dokumentation der Applikationen im Bereich DHCP/DNS
- **Linux:** Inventarisierung von Linux-basierten Rechnern
- **Macintosh:** Inventarisierung von Mac OS X-basierten Rechnern
- **Customizing:** Anpassung von Datenstrukturen und Docusnap 5.0 Oberfläche

Optionale Module



Produkt

Software zur Dokumentation der Netzwerkinfrastruktur.

Hersteller

Itelio GmbH
www.docusnap.de

Preis

Basis-Software ab 200 Euro (bis 24 Systeme),
Erweiterungen ab 400 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Konfiguration / Einrichtung 8

Zuverlässigkeit 10

Analysefunktionen 8

Berichterstellung 8

Usability 8

Dieses Produkt eignet sich

gut für Unternehmen mit einer umfangreichen Netzwerk-Infrastruktur inklusive virtueller Server.

bedingt für Unternehmen ohne zentralen Server.

nicht für Peer-to-Peer-Netzwerke.

Itelio Docusnap 5.0

Konstant überzeugende Druckergebnisse sind Pflicht für Unternehmen

Original HP Tonerkassetten sorgen für störungsfreien Betrieb der HP LaserJet Drucker und Multifunktionsgeräte

Unternehmen wollen sich jederzeit auf hervorragende Druckergebnisse verlassen können. Präsentationen, Geschäftsdokumente oder andere Papiere sind zu wichtig, um sie mit Streifen oder verblassenden Farben dem Geschäftspartner oder Kollegen zu präsentieren – denn einen ersten Eindruck kann man nur einmal machen. Laserdrucker und Multifunktionsgeräte sollen bei Papierunterlagen diesen guten Eindruck vermitteln, denn die Ausdrücke symbolisieren gleichzeitig das Qualitätsverständnis der Firma. Neben hochwertigen Ergebnissen gefragt: einfache Bedienung der Laserdrucker, problemloser Tonerwechsel und der Druck mehrerer Tausend Seiten pro Kassette.

HP steht seit Jahren für Premium-Qualität bei Laser-Ausdrucken, aber auch für ein gutes Preis-/Leistungsverhältnis, das der Druckspezialist kontinuierlich optimiert – beispielsweise mit höheren Seitenreichweiten pro Tonerkartusche, HP LaserJet Hochleistungskassetten speziell für Vieldrucker, einer einfachen Handhabung sowie einem eigenen Recyclingprogramm. Doch warum original Tonerkassetten von HP? Das Marktforschungsinstitut Millward Brown fand in seiner aktuellen Studie heraus, dass knapp die Hälfte der Anwender, die keine Originalkassetten in ihren HP LaserJet Druckern nutzten, bereits schlechte Erfahrungen damit gemacht hatten¹ – ein guter Grund, auf das mit ISO-Standard 9001 zertifizierte Originalprodukt von HP zu setzen.

Konstant gute Ergebnisse sind ein Muss

Auch wenn undichte Tonerkartuschen, verschmierte Ausdrücke oder häufige Ausfälle oftmals nicht in die tatsächlichen Druckkosten eingerechnet, sondern als Ausrutscher vernachlässigt werden: Gerade durch das Nachdrucken unakzeptabler Seiten und durch einen erhöhten Serviceaufwand entstehen Kosten, die sich kein Unternehmen leisten kann. Die original HP Tonerkassetten sind speziell für den jeweiligen HP LaserJet entwickelt und können damit beste Ausdrücke, eine konstant hohe Zuverlässigkeit und vor allem auch einen störungsfreien Betrieb des LaserJet garantieren.



Dank Smart Printing Technologie erhalten Anwender immer die neuesten Statusinformationen ihres Toners. Dazu gehören die Anzahl der Seiten, die noch gedruckt werden können, Warnhinweise, wenn der Toner zur Neige geht, leer ist oder die Kassette nicht korrekt eingesetzt wurde. Neben diesen Qualitätsmerkmalen bietet HP aber auch speziell auf die Anforderungen unterschiedlicher Druckverhalten abgestimmte Tonerkartuschen an. Anwender sparen mit den HP LaserJet Hochleistungs-Druckkassetten bares Geld – und verringern die Kosten um bis zu 25 Prozent pro Seite im Vergleich zu HP LaserJet Standardtonern. Mit den HP LaserJet Doppelpack-Druckkassetten behalten Vieldrucker ihr Budget im Griff: Verglichen mit dem Einzelprodukt sparen sie bis zu zehn Prozent.

Auch die Umwelt profitiert

Aber HP investiert nicht nur Forschungsgelder und Entwicklungszeit in neue Toner, sondern auch in deren Recycling. Das HP Planet Partners Programm gewährleistet die einfache und kostenlose Rückgabe verbrauchter Tonerkassetten. Als eines der ersten Unternehmen ist HP darüber hinaus ISO 14001 zertifiziert – dies ist der freiwillige internationale Standard für Umweltmanagement. Auch beim Thema Energieeffizienz liegt HP vorne: Die neueste Generation der monochromen HP LaserJet Druckkassetten mit energiesparendem Toner spart bei jeder gedruckten Seite bis zu 35 Prozent Energie ein.²



Die original HP Tonerkassetten sind perfekt auf die jeweiligen HP Drucker abgestimmt

1) Millward Brown Befragung von 273 klein- und mittelständischen Kunden in Deutschland im Auftrag von HP (November 2009 – März 2010).

2) Für die Berechnung der Energieeinsparungen wurde ein Vergleich zwischen einem herkömmlichen HP Toner und dem neuen energieeffizienten HP Toner herangezogen. Der angegebene Energieverbrauch für das Drucken einer Standardtestseite wird durch die Anzahl der gedruckten Seiten geteilt. Die tatsächlichen Einsparungen können hiervon abweichen.

Im Test: Protected Networks 8MAN 2.0

Pfiffiger Verzeichnisplaner

von Jürgen Heyer



“Lizenz zum Aufpassen” ist der Slogan der protected-networks.com GmbH für ihre Software 8MAN zur Verwaltung der Datei- und Verzeichnisrechte in einer Active Directory-Umgebung. Statt mit Windows-Bordmitteln allein in größeren Umgebungen irgendwann die Übersicht zu verlieren, hilft dieses Tool dem Administrator durch eine gute Visualisierung sowie eine umfassende Analyse. Notwendig ist allerdings die Bereitschaft zur Einarbeitung in eine neuartige Benutzeroberfläche, wie unser Test zeigte.

Wer eine komplexe Active Directory-Domänenstruktur mit großen Fileservern betreibt, auf die viele Benutzer mit unterschiedlichen Rechten zugreifen, weiß, wie schwer es ist, allein mit den Windows-Bordmitteln auf Dauer einen genauen Überblick über die Zugriffsrechte zu behalten. Vor allem fällt es nicht leicht, schnell die effektiven Rechte zu erkennen und Verschachtelungen zu vermeiden. Um sich nicht irgendwann im selbstgeschaffenen Dschungel zu verlieren, gehen viele Administratoren beispielsweise dazu über, die Rechte im Dateisystem nur auf den ersten beiden Verzeichnisebenen zu vergeben, so dass weiter unten nur die normale Vererbung greift. Über eigene Regeln wie diese steht dann fest, wie weit die Verzeichnisstruktur durchforstet werden muss, wenn es darum geht, Berechtigungen nachzuvollziehen. Nicht unüblich ist auch deren händische Dokumentation in Listen oder Tabellen, beispielsweise mit Excel.

Verschärft wird die Situation in vielen Unternehmen durch regelmäßige organisatorische Umstrukturierungen, die es erforderlich machen, die Verzeichniss-

strukturen und die damit verknüpften Rechte anzupassen, wobei dann die Gefahr besteht, dass die Berechtigungen im Laufe der Zeit stark aufweichen. So mancher Administrator dürfte sich schon einmal gefragt haben, ob es nicht einfacher und besser wäre, allen Anwendern die gleichen Zugriffsrechte zu geben. Das aber widerspricht dem allgemeinen Grundsatz, dass jeder nur auf die Daten Zugriff haben sollte, die er für die Arbeit auch benötigt.

Den Mangel der Windows-eigenen Werkzeuge hat sich die protected-networks.com GmbH zu eigen gemacht und mit 8MAN eine Software geschaffen, die auf einfache Weise Transparenz in die Rechtestruktur bringen soll. Während die Version 1.0 nur eine Visualisierung der Berechtigungen erlaubte, ermöglicht die neu vorgestellte Version 2.0 jetzt auch deren Administration.

Am Anfang steht die Planung

Die Dimensionierung der 8MAN-Plattform hängt von der Anzahl der Benutzer- und Gruppenobjekte im Active Directory (AD) sowie der Anzahl der Verzeichnisse

auf den Dateiservern ab. Dabei arbeiten drei Komponenten eng miteinander:

- Der 8MAN-Server als zentrale Komponente,
- 8MAN-Kollektoren zum Auslesen des AD und der ACLs in den Dateisystemen sowie
- ein SQL-Server zur Speicherung der gesammelten Informationen.

Hinzu kommt noch eine Benutzerkonsole für die Bedienung.

Vorteilhaft ist, dass nicht auf jedem Fileserver ein Agent installiert werden muss, sondern nur gegebenenfalls mehrere Kollektoren, wenn das Auslesen der ACLs zu lange dauert. Hier spielt es eine große Rolle, wie oft überhaupt Scanläufe notwendig sind, was wiederum davon abhängt, ob die Verzeichnis- und Rechtestruktur eher statisch ist oder ständige Änderungen erforderlich sind. Der Einsatz mehrerer Kollektoren ist auch in durch Firewalls oder langsamere WAN-Strecken segmentierten Netzen sinnvoll. Dann übernimmt pro Segment ein Kollektor die Scanläufe, wobei dieser zur



Kommunikation mit dem 8MAN-Server nur einen Port benötigt. Ein weiterer Port ist für die Verbindung zwischen 8MAN-Server und Konsole erforderlich.

Für die Dimensionierung eines geeigneten 8MAN-Servers gibt der Hersteller grobe Richtwerte an (siehe Kasten "Systemvoraussetzungen"). Auf aktueller Hardware dauert das Auslesen von 100.000 Verzeichnissen etwa 15 Minuten. Für bis etwa 2.500 Benutzer kann laut Hersteller als Datenbankbasis noch SQL Express reichen, darüber hinaus ist auf jeden Fall aufgrund der Datenbankgrößen MS SQL erforderlich. Zu beachten ist, dass bei der Express-Version die Datenbank maximal 4 GByte groß werden kann.

Einfache Installation

Ist die Planung abgeschlossen, stellt die Installation von 8MAN kein Problem dar. Allerdings wird vorausgesetzt, dass der benötigte SQL-Server oder SQL Express bereits vorhanden ist. Dieser ist nicht in das Setup integriert. Mit der Installation erfolgt auch die Einrichtung der Konso-

500 Benutzerobjekte und ein Fileserver mit maximal 20.000 Verzeichnissen:

SQL-Server mit 15 GByte freier Plattenkapazität, Windows 2003/2008 (R2) Server, SQL Server 2005/2008 SQL, für kleine Umgebungen und Demozwecke SQL 2005/2008 Express (maximal 4 GByte DB-Größe)

8MAN-Server mit 4 GByte Arbeitsspeicher, Windows 2003/2008 (R2) Server, .NET 3.5 SP1

8MAN-Kollektor mit 3 GByte Arbeitsspeicher, Windows 2003/2008 (R2) Server, Windows XP Pro SP3, Windows 7 Pro, .NET 3.5 SP1

8MAN-Konsole mit 2 GByte Arbeitsspeicher, Windows 2003/2008 (R2) Server, Windows XP Pro SP3, Windows 7 Pro

5.000 Benutzerobjekte und zwei Fileserver mit maximal 100.000 Verzeichnissen:

Wie oben, aber SQL-Server mit 200 GByte Plattenkapazität, 8MAN-Server mit 8 GByte Arbeitsspeicher, Kollektor mit 4 GByte Arbeitsspeicher

Systemvoraussetzungen



Bild 1: Das Hauptmenü von 8MAN erlaubt den Einstieg über typische Szenarien oder über die sechs Icons direkt in die einzelnen Funktionsbereiche

le und eines Konfigurationstools, wobei Letzteres zuerst benötigt wird, um im nächsten Schritt über den Punkt "Basis-konfiguration" noch einige notwendige Einstellungen vorzunehmen, wie die Angabe der SQL-Datenbank inklusive Anmeldeverfahren. Außerdem wird ein Transferverzeichnis benötigt, in das die Kollektoren ihre Scandaten in Form temporärer Dateien ablegen, damit der 8MAN-Server die Informationen von dort in die Datenbank schreiben kann.

Beim ersten Aufruf des Konfigurationstools dürfte das Design der Oberfläche Erstauen hervorrufen, denn der Administrator blickt auf eine nachgebildete Kork-Pinnwand, auf der die einzelnen Punkte wie Notizzettel etwas schräg hindrapiert sind. Auf diesen "Zetteln" findet der Administrator wiederum Schaltflächen, um entsprechend zugeordnete Einstellungen zu ändern.

Ein weiterer Punkt beschäftigt sich mit dem Benutzermanagement, wobei der Administrator dies nicht unbedingt aktivieren muss. Allerdings kann sich dann jeder Benutzer bei 8MAN anmelden und

das Werkzeug nutzen. Da uns das hinsichtlich der Sicherheit bedenklich erscheint, halten wir es für besser, das Benutzermanagement zu aktivieren und die Benutzer auszuwählen, die für die Nutzung von 8MAN berechtigt werden sollen. Dabei kann der Administrator festlegen, welche Benutzer oder Gruppen nur sehen oder auch administrieren dürfen.

Komfortables Auslesen der Daten

Dann muss der Administrator die Scanläufe festlegen, mit Hilfe derer 8MAN seine Datenbank füllt. 8MAN kennt zwei Typen von Scanläufen, um die Benutzer- und Gruppenobjekte aus dem AD sowie die Rechte in den Dateisystemen zu erfassen. Gut ist, dass 8MAN auch das Auslesen mehrerer Domänen unterstützt, indem der Administrator mehrere Jobs aufsetzt und die unterschiedlichen Domänen inklusive entsprechender Anmeldeinformationen angibt. Weiterhin kann der Administrator festlegen, welche OUs in einer Domäne gescannt werden sollen, der Lauf kann also auch auf einen Teil der Domänenstruktur beschränkt werden. Das Scannen erfolgt über einen Server mit installiertem Kollektor.



Ebenso muss der Administrator die Scanläufe für die Dateisystemrechte definieren. Schrittweise wählt er hierzu einen Server aus und gibt einen geeigneten Benutzer mit Passwort an. Diese Informationen werden nun gleich genutzt, um alle Freigaben aufzulisten, damit der Administrator hier wieder eine Auswahl treffen kann. Zu beachten ist, dass pro Server nur ein Scanjob aufgesetzt werden kann, was bedeutet, dass es nicht möglich ist, einzelne Freigaben unterschiedlich oft auszulesen. Sehr wohl aber lassen sich verschiedene Server unterschiedlich oft scannen. Neben dem Auslesen von Windows 2003/2008-Servern unterstützt 8MAN auch die Filer von Netapp und EMC (Celerra).

Besonders gefallen hat uns, dass sich erstellte Scanjobs noch zusätzlich aktivieren und deaktivieren lassen. Ein Administrator kann also alle notwendigen Jobs vordefinieren, auch wenn einzelne nur sporadisch laufen sollen. Der Scheduler unterstützt stündliche, tägliche und wöchentliche Jobs zu einer vorgegebenen Zeit. Zu beachten ist, dass während eines laufenden Dateisystem-Scans dort über 8MAN keine Rechte administriert werden können.

Der verbleibende Konfigurationspunkt in Form des Gruppenassistenten ist optional und weiter unten in Zusammenhang mit der späteren Verwendung dieser Funktion beschrieben.

Eigenwillige, aber durchdachte Benutzeroberfläche

Wie schon das Konfigurationstool kommt auch die eigentliche 8MAN-Konsole mit eigener und letztendlich etwas eigenwilliger Optik daher. Dabei werden sogar für die Standard-Schaltflächen zum Verkleinern und Vergrößern des Fensters eigene Symbole verwendet. Das erfordert anfangs eine gewisse Eingewöhnung, mit der Zeit mussten wir aber feststellen, dass die Konsole für den gegebenen Zweck erfreulich überlegt gestaltet ist. Hinsichtlich der Performance ist die Konsole flott bedienbar,

ein trüges Verhalten konnten wir nirgendwo feststellen.

Über alle Ansichten hinweg ist die Kopfzeile mit der Angabe von Domäne und Datenstand sowie einer Suchfunktion einheitlich gestaltet. Die Startseite der Konsole ermöglicht wahlweise den Einstieg über vorbereitete, typische Szenarien (Verzeichnisrechte bearbeiten, Reporte erzeugen), bei denen die benötigten Informationen schrittweise abgefragt werden, oder über sechs Icons (Dashboard, Active Directory, Mehrfachauswahl, Dateisystem, Verzeichnisrechte und Server Information), hinter denen sich die wesentlichen Funktionen von 8MAN verbergen.

Das "Dashboard" zeigt sehr informative Auswertungen des AD an. Neben den reinen Zahlen (Anzahl der Benutzer, der diversen Gruppen und Objekte) liefert es die Verschachtelungstiefe der Gruppen sowie eine sehr hilfreiche Analyse auf Fehler sowie optimierungsbedürftige und eventuell sicherheitskritische Konstellationen. Dies sind Rekursionen, leere Gruppen, Berechtigungen für "Jeder" und "Authentifizierte Benutzer", direkte Benutzerberechtigungen sowie unaufgelöste SIDs. Um Genaues über einen dieser Punkte zu erfahren, reicht es, auf ein zugeordnetes Icon zu klicken, worauf 8MAN einen CSV-Report erstellt oder die betroffenen Objekte in einer entsprechenden Ansicht auflistet. Letztendlich erweist sich das Dashboard als wertvolle Hilfe zur schnellen Basisanalyse.

Die Ansicht "Active Directory" ist ein grafischer Browser durch die Gruppen- und Benutzerstruktur des AD mit Angabe der Kinder und Eltern zum aktuell ausgewählten Objekt. In der normalerweise dreigeteilten Ansicht zeigt 8MAN in der Mitte die Strukturansicht mit dem gewählten Objekt und den direkten Eltern und Kindern an. Im linken Fenster sind zudem die Eltern und im rechten Fenster analog die Kinder in Listenform

aufgeführt. In der grafischen Strukturansicht kann der Administrator Eltern oder Kinder ein- und ausblenden. Zahlen über und unter jedem Objekt zeigen zudem an, wie viele Eltern und Kinder es jeweils gibt. Der Administrator kann sich nun in der Ansicht von Objekt zu Objekt weiterhangeln, durch einen Doppelklick auf eines der Objekte, egal in welchem der Fenster, erhält dieses den Fokus und 8MAN zeigt nun dessen Beziehungen an. Wichtig ist zu wissen, dass es sich hier um eine reine Ansichtsfunktion handelt. Ein Administrator kann also nichts verändern, keine Objekte löschen oder neu anlegen.

Die Funktion "Mehrfachauswahl" bietet mehrere Möglichkeiten zur Anzeige und zum Vergleich von AD-Objekten, ist aber gerade am Anfang vom Nutzen her nicht so leicht zu verstehen. Die Ansicht ist normalerweise zweigeteilt. Durch das gleichzeitige Markieren mehrerer Objekte in einer flachen AD-Ansicht im linken Fenster listet 8MAN nun im rechten Fenster alle zugeordneten Kinder auf mit der Angabe, wie oft sie enthalten sind. Dies erleichtert beispielsweise einen Vergleich der Mitglieder von zwei oder mehreren Gruppen.

Um gerade in großen Umgebungen die Ausgabe vorzufiltern, gibt es bei der AD-Ansicht und bei der Mehrfachauswahl die Möglichkeit, zu filtern, und zwar sowohl durch eine Texteingabe als auch durch einen vorbereiteten Filter nach Benutzern, Gruppen, Kontakten und Computern. Komfortabel ist, dass diese Filterung stets nur einen Mausklick erfordert und der aktuelle Stand auf einen Blick erkennbar ist.

Tiefgehende Analyse bestehender Rechte

Die Funktion "Dateisystem" ist das primäre Hilfsmittel von 8MAN zur Analyse des Dateisystems mit allen Pfaden und Berechtigungen. Eine zentrale Bedeutung haben hier kleine Symbole (unter anderem grüne Pfeile und Ausrufezeichen),

Welche Funktion hat die Vermittlungsschicht des OSI (Open System Interconnect) - Modells?

Wofür wird User Datagram Protocol (UDP) Port 67 verwendet?



Bodo Vander, Regionaldirektor Deutschland, Österreich und der Schweiz bei CompTIA

Netzwerkwissen ist gefragt

Verschiedene Studien von CompTIA beweisen: Das Fachwissen der IT-Mitarbeiter ist ein entscheidender Faktor für die Minimierung der Ausfallzeiten von IT-Netzwerken. Arbeitgeber greifen daher für die Betreuung dieses sensiblen Geschäftsbereiches bevorzugt auf zertifizierte Netzwerk-Fachkräfte zurück. Zu hoch sind die Risiken, die mit einem Ausfall der Netzwerke durch unsachgemäßes Verhalten der Mitarbeiter einhergehen würden. Zertifiziertes Fachwissen lohnt sich jedoch nicht nur für die Unternehmen: IT-Fachkräfte können damit gezielt Karrierechancen und Gehalt verbessern.

CompTIA Network+ ist die weltweit führende herstellere neutrale Zertifizierung für Netzwerkprofis. „Arbeitgeber auf der ganzen Welt achten bei der Einstellung neuer Netzwerk-Fachkräfte auf dieses international anerkannte Siegel“, erklärt Bodo Vander, CompTIA Regionaldirektor für Deutschland, Österreich und die Schweiz. „Denn CompTIA Network+ bestätigt von der Industrie anerkanntes praxisrelevantes Basiswissen zum Thema IT-Netzwerke. Darüberhinaus zeigt die Zertifizierung, dass der Bewerber motiviert ist, sich weiterzubilden und sich der Bedeutung seines Jobs für das Unternehmen bewusst ist.“

Ein Inhaber der herstellereutralen Zertifizierung CompTIA Network+ kann Netzwerke professionell planen, installieren, konfigurieren, bedienen und Fehler im Netzwerk beheben. Darüber hinaus ist er in der Lage, Netzwerktechnologien und wesentliche Design-Prinzipien zu beschreiben, Verkabelungsstandards einzuhalten und Prüfwerkzeuge einzusetzen.

Die Inhalte der Prüfung für CompTIA Network+ wurden aus mehreren Studien abgeleitet, die den Arbeitsalltag eines Netzwerkprofis genau analysiert haben. Die so erreichte hohe praktische Relevanz der Prüfung wird verstärkt durch das aktive Mitwirken von Branchengrößen wie Canon, Cisco, Hewlett-Packard, Microsoft, Novell oder Ricoh. Darüber hinaus ist CompTIA Network+ seinerseits nach dem internationalen Weiterbildungsstandard ISO 17024 zertifiziert.

CompTIA Network+: Sprungbrett für die Netzwerk-Karriere

Aufgrund des breiten und praxisrelevanten Anforderungskatalogs von CompTIA Network+ haben diverse Anbieter von produktspezifischen Zertifikaten die CompTIA-Zertifizierung in ihre Ausbildungsprogramme integriert. Microsoft beispielsweise hat CompTIA Network+ in sein Programm für den Microsoft Certified Systems Administrator (MCSA) aufgenommen. Auch Novell, Cisco, HP, Lotus und 3Com erkennen CompTIA Network+ im Rahmen ihrer produktspezifischen Ausbildungsprogramme an.

Sind Sie ein Netzwerk-Profi? Testen Sie Ihr Wissen online!

Bis Ende Oktober können Sie auf der Seite <http://www.it-administrator.de/comptia> ihr Netzwerk-Wissen online prüfen. Dort finden Sie einen Fragenkatalog, der an die Prüfungsfragen von CompTIA Network+ angelehnt ist. Prüfen Sie Ihr Wissen und gewinnen Sie ein iPad!

CompTIA (www.comptia.de):

Die Computing Technology Industry Association (CompTIA) ist das Sprachrohr der IT-Industrie. Zu den Mitgliedern des weltweit aktiven Verbandes zählen IT-Unternehmen und andere Branchenangehörige aus insgesamt 102 Nationen. Ziel von CompTIA ist die Förderung des weltweiten Wachstums der IT-Branche.

Zu den wichtigsten Aufgaben von CompTIA zählt die weltweit standardisierte Aus- und Weiterbildung von IT-Fachkräften. Hierfür hat CompTIA herstellere neutrale Zertifizierungen entwickelt. Diese bestätigen IT-Professionals nach international anerkannten Standards grundlegende IT-Kenntnisse zu Spezialgebieten wie PC-Support, IT-Sicherheit, Projektmanagement oder Netzwerk-Administration.

Die wichtigsten CompTIA-Zertifizierungen im Überblick:

- CompTIA A+ (PC-Support)
- CompTIA Network+
- CompTIA Security+
- CompTIA Server+
- CompTIA CTT+ (Certified Technical Trainer)
- CompTIA Project+ (Projektmanagement)
- CompTIA PDI+ (Druck- und Kopiersysteme)
- CompTIA CDIA+ (Dokumenten-Management)
- CompTIA Linux+ powered by LPI

CompTIA®

deren Bedeutung der Administrator auswendig kennen sollte, um die Ansicht lesen zu können. Darüber hinaus ist es anfangs sehr hilfreich, dass beim Überstreichen eines Symbols mit der Maus dessen Bedeutung eingeblendet wird. Die Symbole zeigen beispielsweise für ein Verzeichnis an, ob sich darunter noch Verzeichnisse mit abweichenden Berechtigungen befinden oder ob sich die Berechtigungen zum übergeordneten Verzeichnis geändert haben. Bei Bedarf lassen sich die Änderungen auch im Detail auflisten. Für einen Vergleich der Rechte auf unterschiedliche Verzeichnisse, für eine Weitergabe an Dritte oder auch zur Dokumentation lassen sich die Einstellungen in einer XPS-Datei speichern. Vorteilhaft ist, dass dazu alle Gruppen aufgeklappt werden, wobei die Darstellung wiederum in einem Baum- sowie im Listenformat erfolgen kann.

Hilfreich ist außerdem, dass beim Überfahren eines Verzeichnisses mit dem Mauscursor die Berechtigungslage zusätzlich als Pop-up-Fenster eingeblendet



Bild 2: Irgendwo zwischen ungewohnt und verspielt ist die Ansicht des Konfigurations-Tools einzuordnen, das dennoch seinen Job verrichtet

wird. Das Analysieren verschiedener Rechtekonstellationen im Test brachte übrigens auch für uns erstaunliche Resultate, die vorher noch nicht aufgefallen waren. So verwendeten wir 8MAN nicht nur, um die Rechte von eigens

zum Test eingerichteten Servern auszu-lesen, sondern wir starteten auch einen Scan auf einem von uns produktiv genutzten Server, auf dem die Rechte über Monate hinweg gewachsen waren. Das gestaltete sich insofern als problemlos, da wir dort dank der Arbeitsweise über einen Kollektor nichts installieren mussten. Dabei fiel uns auf, dass im Verzeichnisbaum an einer Stelle mit sicher 200 parallelen Unterverzeichnissen an vielen ein Symbol zu sehen war, welches auf eine Rechteänderung gegenüber dem darüber befindlichen Verzeichnis hindeutete. An in neuerer Zeit angelegten Verzeichnissen aber war kein Symbol zu sehen. Eine genaue Analyse zeigte nun, dass bei den Verzeichnissen mit dem Symbol neben der Vererbung das gleiche Recht zusätzlich nochmals explizit eingetragen war, was eigentlich nicht beabsichtigt und auch nicht sinnvoll war. Durch eine konsequente Durchvererbung konnten wir die Berechtigungen schließlich vereinheitlichen.

Letztendlich konnte 8MAN im Test als wertvolle Hilfe überzeugen. Nichtsdesto-trotz ist es ein Werkzeug, das die Erfahrung eines Administrators nicht ersetzen kann, sondern diesen vielmehr unterstützt.

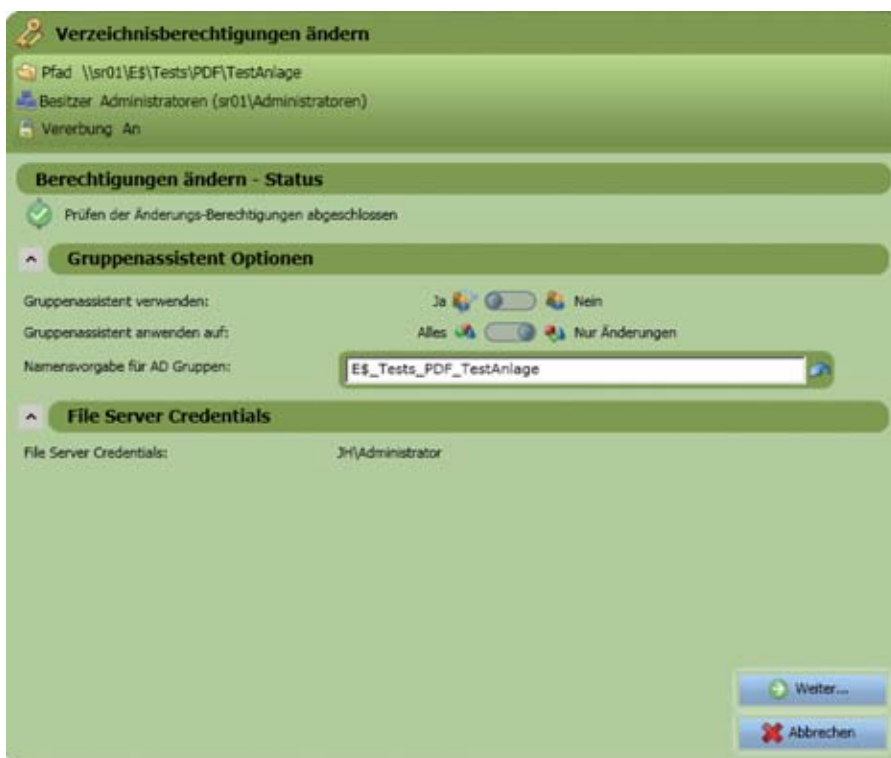


Bild 3: Beim Ändern von Berechtigungen prüft 8MAN diese in mehreren Schritten und gibt alle Einstellungen für eine nochmalige Kontrolle aus



Teilweise wirkt der Informationsumfang ein wenig erschlagend und der Nutzer muss schon genau hinsehen, um Auffälligkeiten zu erkennen. Hilfreich ist hier, dass es diverse Möglichkeiten gibt, die Informationen zu filtern. So kann sich der Administrator nur nicht vererbte Berechtigungen anzeigen lassen, wodurch er tatsächliche Änderungen besser erkennt.

Rechte mit Übersicht administrieren

Während die bisher beschriebenen Funktionen letztendlich übersichtlichere Darstellungen bieten, aber keine Änderungen ermöglichen, dient der Punkt

“Verzeichnisrechte” zur Änderung oder Neuvergabe von Rechten im Dateisystem, wobei sich auch neue Verzeichnisse anlegen lassen.

Die Möglichkeiten zur Rechtevergabe hängen entscheidend davon ab, wie in der Konfiguration der oben bereits erwähnte Punkt “Gruppenassistent” eingestellt ist. Je nachdem, ob der Gruppenassistent aktiviert oder deaktiviert ist, werden die Rechte grundsätzlich über Gruppen oder direkt vergeben. Ist der Assistent aktiv, kann der Administrator einmalig bei der ersten Aktivierung vorgeben, ob die Vergabe nur über lokale oder über lokale und globale Gruppen er-

folgen soll. Diese Einstellung lässt sich später nicht mehr ändern. Microsoft empfiehlt, Ressourcen über lokale Domänengruppen und Benutzer über globale Gruppen zu verwalten, was sich bei entsprechender Einstellung des Assistenten auch realisieren lässt.

Bei aktiviertem Gruppenassistent erstellt dieser Gruppen mit einheitlichem Format, wobei dem Administrator flexible Möglichkeiten zur Vorgabe der Namensstruktur mit Gruppenkennung, festen Namensbestandteilen, Pfad und Rechtekennzeichen offenstehen. Das Resultat sind zwar recht kryptische Namen, die aber diverse Infos zu deren Bedeutung enthalten. So verrät zum Beispiel ein Gruppenname wie “lr_jh.local_E\$_Tests_md”, dass es sich um eine lokale Gruppe (=lr) in der Domäne “jh.local” für den Pfad “E\$\Tests” mit Rechten zum Ändern (=md) handelt.

Auf der Konfigurationsseite des Gruppenassistenten legt der Administrator auch fest, welche Rechtekategorien (Vollzugriff, Ändern, Lesen und Ändern, Ordnerinhalt auflisten, Lesen, Schreiben) überhaupt zur Rechtevergabe zur Verfügung stehen sollen. Dies geschieht unabhängig von der Aktivierung des Assistenten und greift auch bei einer direkten Rechtevergabe auf Benutzer. Damit der Gruppenassistent nicht zu tief in die Rechtestruktur vordefinierter Benutzer und Gruppen (etwa die Gruppen



Bild 4: Der Active Directory-Browser zeigt die Zusammenhänge zwischen den Objekten übersichtlich an und hilft auch bei der Analyse von Fehlern wie hier einer Rekursion

Enable Limitless Workplaces.

**Ein Tag.
Echte Experten.
Alle Themen.**

Run IT as a Business – nach diesem Motto bietet die Matrix42 Konferenz eine Kombination aus Information, Kommunikation und der Möglichkeit, hochkarätige Kontakte zu knüpfen. Erleben Sie den Arbeitsplatz der Zukunft und informieren Sie sich über erfolgreiche IT-Strategien u.a. zu den Themen wie Virtualisierung und Windows 7 Migration.



matrix42

Jetzt anmelden unter:
www.matrix42.de/konferenz



VORDEFINIERT und NT-AUTORITÄT oder der Benutzer JEDER) eingreifen kann, gibt es eine so genannte Schwarze Liste, in der diese Objekte bereits eingetragen sind und die sich vom Administrator noch erweitern lässt. Alle Objekte der Schwarzen Liste werden vom Gruppenassistenten ignoriert und jegliche Änderungen an den Rechten dieser Benutzer verhindert. Wichtig bei der Konfiguration des Gruppenassistenten erscheint uns wiederum eine wohlüberlegte Vorplanung. Zum einen gibt es die Einstellung zur Verwendung lokaler und globaler Gruppen, die einmalig festzulegen ist, zum anderen ist es ärgerlich, wenn man nach einiger Zeit erkennt, dass die gewählten Vorgaben für den automatischen Aufbau der Gruppennamen ungeeignet sind und geändert werden müssen, nachdem schon diverse Gruppen definiert worden sind.

Ist die Konfiguration abgeschlossen, sollte der Rechtevergabe über 8MAN nichts mehr im Wege stehen. Der Administrator kann nun durch die Verzeichnisstruktur browsen und ein vorhandenes Verzeichnis auswählen oder ein neues anlegen. Für jede in der Konfiguration frei gegebene Rechtekategorie sieht er eine Spalte, in die er Benutzer oder auch Gruppen aufnehmen beziehungsweise von dort entfernen kann. Etwas gewöhnungsbedürftig erscheint uns hierbei die Art, wie Benutzer und Gruppen auszuwählen sind. Hierzu gibt es in der Ansicht eine so genannte Ablage-Spalte, in die der Administrator in der obersten freien Zeile den Namen oder zumindest einen Teil eingeben muss. Ist das Pull-Down-Menü anfangs leer, so zeigt 8MAN die in Frage kommenden Objekte erst an, wenn mindestens ein Zeichen eingegeben ist.

Der Administrator kann nun das gewünschte Objekt wählen und dann in die gewünschte Rechtekategorie-Spalte ziehen. Um einem Objekt ein Recht zu nehmen, zieht er es einfach aus der Kategorie-Spalte in die Ablage. Um ein Recht zu ändern, kann er es von einer Spalte in eine andere verschieben. Kleine Symbole vor den Objekten zeigen an, ob hier ein Recht geändert

oder ganz neu vergeben wird. Wird die Rechtevergabe in einem Unternehmen genutzt, in dem viele Anforderungen beispielsweise per E-Mail an die Administratoren gesendet werden, ist die Übernahme daraus recht einfach zu realisieren. Gibt es nämlich eine Aufstellung von Benutzern oder Gruppen in Textform, in einer Liste oder im Mailtext, so kann der Administrator diesen Abschnitt über die Zwischenablage in die Ablage der Rechtevergabe kopieren. 8MAN analysiert nun alle Einträge anhand seiner Datenbank und ordnet über die Bezeichnung gefundene Objekte zu. Treffer sind dann mit einem grünen Punkt, nicht erkannte Einträge mit einem roten Punkt in der Zeile markiert. Nun kann der Administrator die Liste leicht bereinigen oder korrigieren und den Rechteeintrag ohne viel Tipperei umsetzen.

Sind für ein Verzeichnis alle Änderungswünsche eingetragen, muss der Administrator diese noch übernehmen. Dann führt 8MAN zuerst eine Prüfung im Dateisystem durch, da sich die in der Datenbank gespeicherten Informationen seit dem letzten Scan geändert haben könnten. Anschließend fragt 8MAN gegebenenfalls neue Credentials ab, sofern dem angemeldeten Benutzer die Rechte für die durchzuführenden Änderungen fehlen, verlangt noch zwingend einen Kommentar, der sich jederzeit später wieder abrufen lässt, listet die anstehenden Änderungen nochmals im Detail auf und führt dann die gewünschte Aktion aus. Das mag anfangs etwas umständlich erscheinen, dient aber letztendlich dazu, dass die Änderungen korrekt ausgeführt werden und dass der Administrator genügend Prüfmöglichkeiten hat, um möglichst nichts Falsches einzutragen. Insgesamt hat uns der Ablauf gut gefallen.

Nicht so übersichtlich ist allenfalls die Darstellung bereits vergebener Rechte innerhalb der Funktion zur Rechtevergabe. Hilfreich ist dabei aber, dass ein Administrator jederzeit zwischen den Ansichten Dateisystem und Verzeichnisrechte umschalten kann. Nur sollte er dabei berücksichtigen, dass eingetragene, aber noch nicht über-

nommene Rechteänderungen bei einer Umschaltung zwischen den Ansichten ohne vorherigen Hinweis verloren gehen und gegebenenfalls neu zu erfassen sind.

Insgesamt hat uns die Funktion zur Vergabe von Verzeichnisrechten überzeugt, auch wenn es kleinere Dinge zu verbessern gibt, wie ein Hinweis beim Umschalten zwischen den erwähnten Ansichten. Auch könnte die Administration vor allem in kleineren Umgebungen noch etwas komfortabler ablaufen, wenn die Pull-Down-

Produkt

Programm zur Verwaltung und Administration der Rechte in einem Microsoft Active Directory.

Hersteller

Protected networks GmbH
www.protected-networks.com

Preis

Die Lizenzierung erfolgt auf Basis der aktiven Benutzer, beginnend bei 35 Euro pro Endanwender bei 100-500 Usern, darüber hinaus gibt es eine Mengenstaffel.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Installation	9
Bedienung	7
Analyse der Rechte	9
Vergabe von Rechten	8
Dokumentation	7

Dieses Produkt eignet sich

optimal für mittlere und größere Umgebungen mit stark differenzierten Benutzerrechten.

bedingt bei einer einfachen und weitgehend einheitlichen Rechtestruktur. Hier sollte zuerst eine Kosten-/Nutzenanalyse erstellt werden.

nicht für die Verwendung in kleinen Umgebungen mit identischen Rechten für die meisten Mitarbeiter.

Protected Networks 8MAN 2.0



Liste in der Ablage bereits mit AD-Objekten gefüllt wäre, auch ohne dass vorher mindestens ein Zeichen für eine Filterung einzugeben ist.

Spezielle Features mit Pfiff

Eine besondere Funktion in 8MAN ist die Möglichkeit zur verzögerten Rechtevergabe. So können in bestimmten Situationen eingetragene Rechte erst nach erneuter Anmeldung eines Benutzers wirksam werden. Mit 8MAN ist es nun möglich, das Schreiben der ACLs auf einen Zeitpunkt zu verschieben, an dem wenige Benutzer angemeldet sind. Auch lassen sich damit beispielsweise Umstrukturierungen in einem Unternehmen vorbereiten, bei denen Anwender ab einem bestimmten Stichtag geänderte Rechte haben sollen. Der Administrator kann hierbei die Verzögerung in Tagen sowie die Uhrzeit zur Realisierung vorgeben.

Während der Testphase erfuhren wir noch von einer weiteren speziellen Funktion, der temporären Rechtevergabe, die gerade programmiert wurde. Es wird dann möglich sein, Berechtigungen für bestimmte Zeiträume einzutragen, was in der Praxis durchaus sinnvoll ist, um beispielsweise einem Mitarbeiter nur während der Dauer eines Projekts einen Zugriff zu geben. Die Scheduler-Funktion von 8MAN sorgt dann automatisch da-

für, dass die Änderung zeitlich passend rückgängig gemacht wird.

Gute Dokumentation

Recht umfassend ist die Dokumentation, auch wenn sie sich offensichtlich noch in der Bearbeitung befindet. Neben der reinen Funktionsbeschreibung findet der Leser Hinweise zu Szenarien und Vorgehensweisen bei typischen Aufgabenstellungen, was den Einstieg erleichtert. In diesem Zusammenhang finden auch häufig gestellte Fragen eine Antwort.

Als recht informativ erweist sich zudem die integrierte, kontextsensitive Hilfe. In der Konsole erscheint diese als Fenster nach Drücken der F1-Taste, innerhalb der Konfiguration sind die Hilfehinweise auf den jeweiligen Seiten mit integriert, da hier mehr Platz zur Verfügung steht. Hilfreich sind auch vielfach die kurzen Beschreibungen, die, wie schon erwähnt, beim Überstreichen eines der vielen Symbole eingeblendet werden.

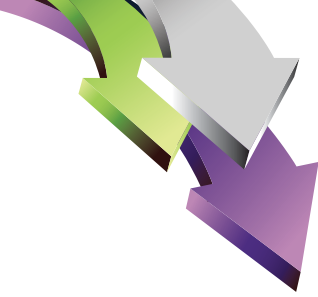
Fazit

Insgesamt ist 8MAN eine erfreulich gut gelungene Lösung zur Vereinfachung beziehungsweise zur Unterstützung bei der Administration der Berechtigungen in einer Microsoft Active Directory-Umgebung. Dabei kann ein Administrator sowohl durch die Dateisysteme als auch das

Active Directory browsen, Zusammenhänge und Verknüpfungen analysieren sowie die vergebenen Datei- und Verzeichnisberechtigungen ansehen.

Neu mit der Version 2.0 hinzugekommen ist die Möglichkeit zur Rechteadministration, wobei Rechte wahlweise direkt auf Benutzer oder über lokale und auch globale Gruppen, die 8MAN automatisch anlegt, vergeben werden können. Durch ein regelmäßiges Scannen des AD sowie der gewünschten Freigaben mit Übernahme in eine eigene Datenbank löst 8MAN das Problem, dass die benötigten Rechteinformationen für eine flüssige Bedienung schnell zur Verfügung stehen müssen, obwohl sie womöglich über mehrere Dateiserver hinweg weit verstreut eingetragen sind. Bei der Administration der Berechtigungen vermeiden entsprechende Prozesse und sorgfältige Prüfungen, dass durch Unterschiede zwischen den Einträgen in der Datenbank und im Dateisystem Inkonsistenzen entstehen.

8MAN erscheint uns als große Hilfe für eine konsistente Rechtevergabe in mittleren und auch größeren Unternehmen zwischen 100 und 5000 oder noch mehr Benutzern. So lässt sich vermeiden, dass die Rechte im Laufe der Zeit aufweichen oder beispielsweise in Form von Rekursionen fehlerhaft vergeben werden. (jp) 



**Sparen Sie 120€ Eintrittsgebühr bei
Verwendung des
Promo-Codes: M41S10 auf
www.snweurope.net
26 - 27 Oktober, Congress Frankfurt**



Platinum sponsors:



SNW Europe findet zusammen mit Datacenter Technologies und Virtualization World im Congress Frankfurt statt. Sie haben die Wahl zwischen über 120 Konferenz Sessions und einer Reihe an spezifischen Fallstudien. Treffen Sie über 55 führende IT-Anbieter. Networken Sie mit über 1500 Ihrer Kollegen aus ganz Europa. So melden Sie sich noch heute an für die zwei wichtigsten Tage im IT Kalender.

POWER OF 3 3 Events
2 Tage
1 Ort



Im Test: StorageCraft ShadowProtect Server 4 **Backup am laufenden Band**

von **Thomas Bär**

Backups zählen zum absoluten Pflichtprogramm von Administratoren. Fällt ein System aus oder sind Daten nicht aufzufinden, so gehen Benutzer stillschweigend und meist zu Recht davon aus, dass ihr Admin das Problem zu lösen weiß. Im Falle eines Desasters dauert die Reparatur und Wiederherstellung möglicherweise Stunden oder Tage – es sei denn, es kommt eine moderne Backupstrategie wie ShadowProtect 4 zum Einsatz. IT-Administrator wollte wissen, wie gut die Software funktioniert.

Bereits im Frühling dieses Jahres hat StorageCraft die aktuelle Version 4 von ShadowProtect in englischer Sprache auf den Markt gebracht. Im Sommer 2010 folgte die deutschsprachige Version der Software, die die Dauer zur Wiederherstellung von Windows-Computern drastisch reduzieren soll. Die Kerntechnologie in StorageCrafts Produkten ist ein zertifizierter VSS-Provider, den auch andere Backup-Anbieter einsetzen.

Schattenkopien und ihre Grenzen

Je nach Einstellung der Windows-Bordmittel sind Wiederherstellungen von Dateien und Ordnern mittels Schattenkopien über einen Zeitraum von mehreren Tagen oder sogar Wochen möglich. Welche Zeitpunkte für die Windows-Schattenkopien eingerichtet werden, ist einzig und allein vom Umfeld abhängig. Geht jedoch ein ganzer Server mit allen Daten aufgrund eines Hard- oder Softwarefehlers verloren, so ist die smarte und für Benutzer leicht zu erlernende Funktion keine Hilfe mehr. Angesichts der großen Masse an Daten, die in vielen Umgebungen schon die TByte-Größe geknackt hat, ist ein schnelles Wiedereinspielen eines Tape-Backups kaum möglich. Für einen hochverfügbaren Cluster oder das Vorhalten von gespiegelten Systemen fehlt in vielen kleineren und mittleren Unternehmen jedoch die finanzielle Grundlage. StorageCrafts ShadowProtect 4 ist für derlei Umgebungen möglicherweise eine pas-

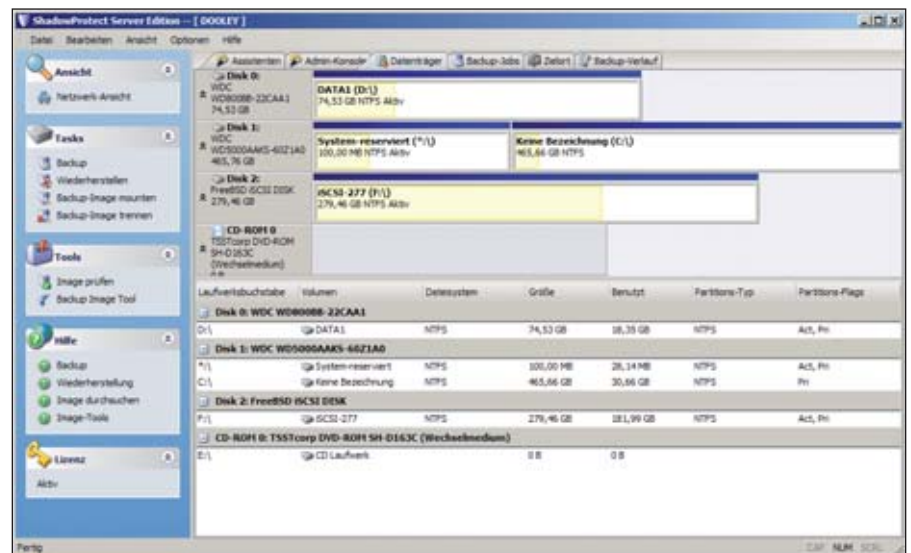


Bild 1: Die Oberfläche von ShadowProtect liefert alle benötigten Informationen für die Einrichtung und Durchführung von Backups. Insgesamt verläuft die Arbeit mit der Software sehr intuitiv.

sende Lösung. Neben vielen soliden und gebräuchlichen Möglichkeiten, die eine aktuelle Backup-Software bietet, hat ShadowProtect einige Zusatzfunktionen auf Lager. Besonders spannend ist die Fähigkeit der Software, ein ausgefallenes System in einer virtuellen Umgebung binnen kurzer Zeit wieder online zu bringen.

Neues in ShadowProtect Server Edition 4

Im Vergleich zur Vorgängerversion haben die Entwickler einige komplett neue Funktionen integriert. Die neue Management-Konsole ermöglicht es IT-Administratoren, die benötigte Client-Agent-Software auf verschiedene Computer per

“Push”-Befehl zu verteilen. Server lassen sich nun zur besseren Übersicht nach eigenen Wünschen gruppieren – was besonders für größere Installationen hilfreich sein dürfte. VirtualBoot ermöglicht es außerdem, Backup-Images mithilfe der kostenfreien Virtualisierungssoftware Virtual-Box von Sun/Oracle auf einem virtuellen Computer zu starten. ShadowProtect Backup-Imagedateien, auch inkrementell gesicherte, lassen sich so in kürzester Zeit online bringen. Mit der neuen Funktion “Resume on Interruption”, sprich Wiederaufnahme nach einer Unterbrechung, ist die Software in der Lage, eine Wiederherstellung auch dann fortzusetzen, wenn sie durch eine Störung, beispielsweise



durch einen Stromausfall, unterbrochen wurde. Bei allen ShadowProtect-Versionen wird das Programm "ImageManager" mitgeliefert. Diese Software ermöglicht die Überprüfung, Konsolidierung und lokale Replikation der erstellten Backup-Images. Mit Benachrichtigungsfunktionen, wie beispielsweise einer Meldung, die erstellt wird, sobald nur noch zehn Prozent freier Festplattenspeicher zur Verfügung steht, ist der Administrator gegen unangenehme Überraschungen gewappnet, ohne diese Funktionen über Skript-Jobs selbst erstellen zu müssen.

Erste Schritte

Für einen ersten Überblick über die Software bietet sich die 30-Tage-Testversion an, die der Hersteller über seine Homepage anbietet. Hintergrundinformationen über die Funktionsweise der Software und PDF-Handbücher in deutscher Sprache erleichtern den Einstieg. Die Installation selbst ist in wenigen Minuten und einen Neustart später erledigt. Bei der Übersetzung der Oberfläche musste es wohl schnell gehen – Windows 7 wird irrtümlich als Serversystem deklariert und da es sich um einen Server handelt, wird nur die Konsole installiert.

Die ShadowProtect Server Edition 4 ist eine reine Windows-Software. Die aktuellen Betriebssysteme Windows 7 und Server 2008 R2 werden sowohl in der x86-, als auch in der x64-Version unterstützt. Windows 2000 SP4, sowohl in der Professional- als auch Server-Variante, begrenzt die Unterstützung im Sinne einer "Minimalanforderung" nach unten. Ältere Windows-Versionen oder Windows auf Itanium-Basis werden nicht unterstützt.

Alle von Windows gebräuchlichen Filesysteme von FAT16, FAT16X, FAT32, FAT32X, NTFS, MBR Disks, GPT Disks bis hin zu Basis- oder dynamischen Datenträgern können mit ShadowProtect bearbeitet werden. Zur Speicherung der Backup-Images können beinahe beliebige Laufwerksarten wie DAS, Netzlaufwerke, SAN, NAS, iSCSI, SCSI, USB oder Firewire/IEEE1394, Solid State Disks (SSD) und auch optische Datenträger wie CD/DVD/Blu-Ray eingesetzt werden.

Systemvoraussetzungen

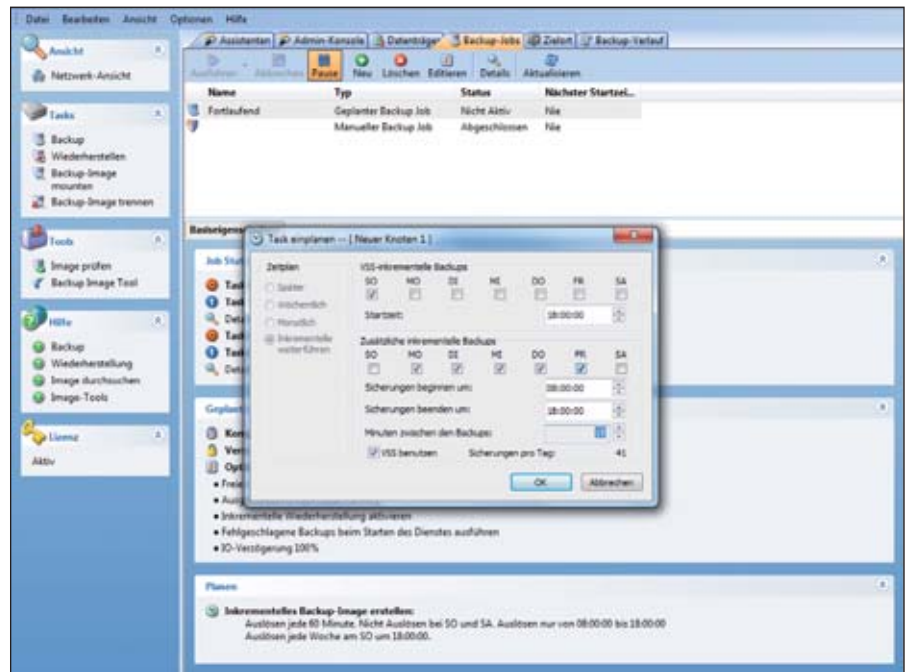


Bild 2: Backups in ShadowProtect basieren stets auf Schattenkopien. Diese sind sehr schnell angelegt und erlauben somit eine große Anzahl an Sicherungspunkten an einem Tag.

Die Oberfläche von ShadowProtect erklärt sich weitgehend von selbst – Assistenten unterstützen den Benutzer bei der Erstellung von Backup-Jobs. Alle klassischen Funktionen wie Kompression oder Verschlüsselung von Backups, Definition von Speicherorten oder Einrichtung von Backup-Jobs über einen Scheduler bietet die Software so, wie es auch von anderen Programmen her bekannt ist. Von der zentralen Installation aus lassen sich Agents auf andere Server/PCs verteilen. Ohne einen anschließenden Neustart sind die zu verwaltenden Maschinen jedoch nicht nutzbar. Die erste Aufgabe besteht darin die Backup-Jobs für die unterschiedlichen Maschinen einzurichten. In rund 20 Minuten sind alle Grundfunktionen eingerichtet und die ersten Sicherungen laufen bereits.

Die Backup-Geschwindigkeit hängt wie üblich in erster Linie von der verwendeten Hardware und der Schreibgeschwindigkeit der Sicherungsplatten ab. Während eine Vollsicherung eines Testservers auf lokal angeschlossenen Festplatten innerhalb weniger Minuten erledigt war, dauerte dieselbe Sicherung auf ein über

Fast Ethernet angebundenes iSCSI-Device entsprechend länger. Die Sicherungen selbst legt ShadowProtect als Images an. Je nach Einstellung durch den Administrator handelt es sich bei diesen Images entweder um einzelne große Dateien oder viele Dateien einer festen Größe, die beispielsweise auf optische Datenträger übertragen werden können.

Einfache Datenrettung

Sollen einzelne Dateien oder Ordner aus den Sicherungen wiederhergestellt werden, so wird das benötigte Image als "Backup-Image" geöffnet. Das Image steht anschließend als Read-Only-Datenträger unter Windows zur Verfügung und kann vom Administrator bearbeitet werden. Komplette Datenvolumen werden über den Wiederherstellungsassistenten wiederhergestellt.

Systempartitionen können bekanntlich nur dann wiederhergestellt werden, sofern das Betriebssystem nicht über sie gestartet wurde. Über eine Boot-CD, die so genannte ShadowProtect Recovery CD, lassen sich Windows-Computer wiederherstellen, die über das eigene Be-

triebssystem nicht mehr starten können. Die Boot-CD bietet zwei unterschiedliche Umgebungen zur Wiederherstellung – eine XP/2003-basierte und eine Vista/2008-basierte. Je nach Betriebssystem wird so die passende Umgebung über einen einzigen Datenträger bereitgestellt. Netzlaufwerke lassen sich bei Bedarf mappen und so Backup-Images auf anderen Servern öffnen. Insgesamt ist die Verwendung der Recovery-CD dank guter Dialogtexte selbsterklärend. Der Funktionsumfang ist beeindruckend: Ein eingebauter VNC-Dienst sorgt dafür, dass der Administrator nicht direkt vor dem Gerät sitzen muss, sondern sich, über ein Passwort vor unfreiwilligem Zugriff geschützt, bequem über das Netzwerk aufschalten kann. Backup-Images lassen sich zunächst prüfen, ehe sie als Grundlage für eine Wiederherstellung genutzt werden.

Virtuelle Wiederherstellung

Die Grundfunktionen der Software in Bezug auf die Sicherung von Daten, die Wiederherstellung von Dateien, mögliche Snapshots und aussagekräftige Reports sind solide und wichtig. Eine Besonderheit von ShadowProtect ist jedoch die schnelle Bereitstellung einer ausgefallenen Maschine durch das Mounten in einer virtuellen Umgebung.

In den Menüs und der Hauptoberfläche von ShadowProtect sucht der Administrator die Option zum Starten in einer virtuellen Maschine zunächst vergeblich. Die Onlinehilfe, die direkt auf die Webseiten des Herstellers verweist, ist alles andere als eine Hilfe. Die Links verwiesen uns im Test auf 404-Fehler, da die Webseite vom Hersteller nicht unter der URL betrieben wird. Insgesamt ist der Gedanke, die Hilfetexte ausschließlich online bereitzustellen, schon in Frage zu stellen: Was ist mit Servern, die über gar keine Verbindung mit dem Internet verfügen? Wenn jedoch ein Hersteller dem Kunden eine reinrassige Onlinehilfe aufbürdet, dann sollte er zumindest dafür Sorge tragen, dass diese erreichbar ist.

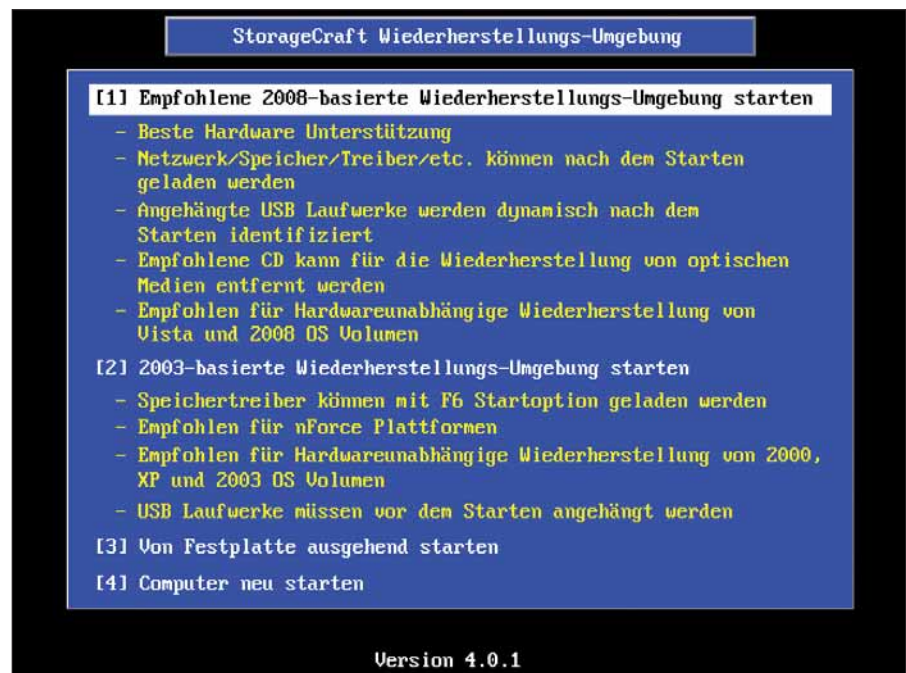


Bild 3: Das Boot-Medium von ShadowProtect bietet unterschiedliche Wiederherstellungsumgebungen. Über das Netzwerk ist ein Zugriff auf entfernte Backup-Images möglich.

Das Programm "VirtualBoot" findet sich schlussendlich im Startmenü und der Administrator wird von einem längeren Dialogtext begrüßt, der die Funktion des Programms erklärt: Die Aktivierung einer virtuellen Maschine auf Basis einer Sicherung. Handelt es sich bei der ursprünglich gesicherten Maschine um ein x64-System, so hat der Administrator sicherzustellen, dass die entsprechenden Fähigkeiten in Form einer passenden CPU auf Intel/AMD-Basis vorgehalten werden. Es folgt ein simples Dialogfenster zur Auswahl der Backup-Dateien, die angenehmerweise den Namen des Servers/PCs direkt anzeigen – sind erst einmal hunderte von Sicherungsdateien angehäuft, so ist ein Administrator für alle Hinweise dankbar, die im Notfall wichtige Zeit einsparen.

Ein Doppelklick auf die gewünschte Datei startet den Vorgang – zumindest, wenn alles korrekt eingerichtet wurde. Wird das Programm erstmalig gestartet und keine VirtualBox-Umgebung von Sun/Oracle auf dem Server vorgefunden, so gilt es zunächst, eine kompatible Version herunterzuladen und zu in-

stallieren. Mit dem Download-Link und der passenden Versionsinformation, die eingeblendet werden, ist dies glücklicherweise eine äußerst leichte Übung. Da die Installation von Oracle VM VirtualBox 3.2.6 oder höher für einige Augenblicke die Netzwerkverbindungen trennt, um die virtuellen Netzwerkkarten einzubinden, sollte diese Installation in einem ordentlichen Wartungsfenster stattfinden. Auf unserem Testserver, einem Intel Xeon X3220-System mit 2,4 GHz Taktfrequenz, 4 GByte Arbeitsspeicher und Windows Server 2008 R2 als Betriebssystem, dauerte die Einrichtung keine Minute.

Zum Abschluss der Installation wird VirtualBox noch einmal gestartet. Dabei haben wir im Test der Verlockung des Updates auf die aktuellste Version 3.2.8 widerstanden – in der Produktunterstützung von ShadowProtect ist bislang nur von Version 3.2.6 die Rede. Das Dialogfenster zur Auswahl der Dateien muss erneut mit Inhalt gefüllt werden, da die gewählten Imagedateien offensichtlich nicht zwischengespeichert werden. Ein Assistent unterstützt den Ad-

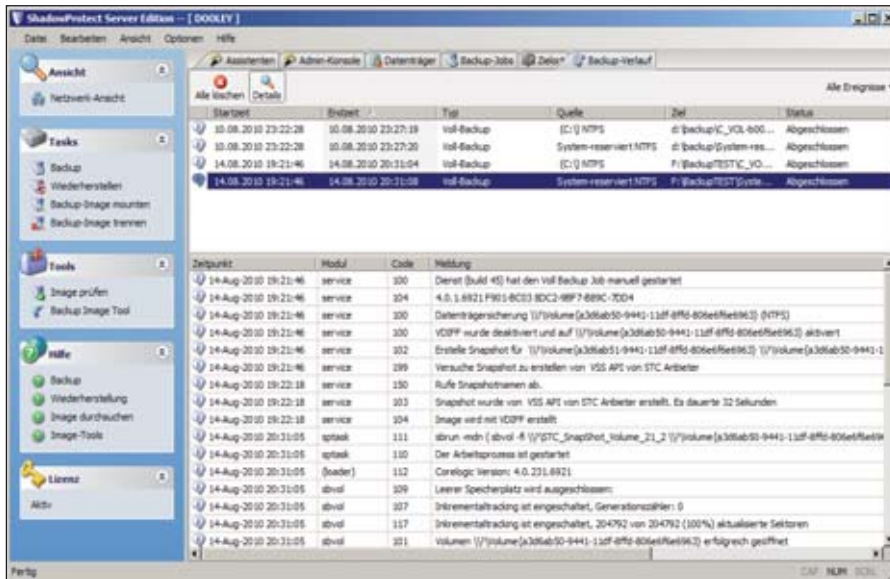


Bild 4: Sehr genau protokolliert ShadowProtect jeden Schritt bei der Erstellung eines Backups

ministrator bei der Erstellung einer virtuellen Maschine – lediglich Netzwerkarten, Arbeitsspeichergröße und das zu erwartende Betriebssystem müssen eingetragen beziehungsweise die Vorausswahl des Assistenten geprüft werden. Ehe die Wiederherstellung in der VM beginnt, erscheint ein weiteres Dialogfeld, das zur Einrichtung weiterer Treiberkomponenten auffordert, ohne die VirtualBox im Zusammenspiel mit ShadowProtect nicht funktioniert. Die Software richtet diese speziellen Gerätetreiber automatisch ein und es dauert wieder nur ein paar Sekunden. Dennoch bleibt die Frage im Hinterkopf: Weshalb richtet der Installer nicht gleich alles so ein, dass es funktioniert?

Das Wiederherstellen eines gesicherten Servers mit einer Oracle XE 10g-Installation, ursprünglich als virtuelle Maschine unter VMware betrieben, zog sich in der Teststellung zunächst über einige Zeit hin. Sehr schnell konnte jedoch der Schuldige ausgemacht werden: VirtualBox läuft auf dem Testserver extrem zäh. In einer anderen Umgebung auf einer anderen Maschine funktionierte die Wiederherstellung des Servers in VirtualBox absolut problemlos und sehr schnell. Durch die Neueinbindung der virtuel-

len Hardware gehen erwartungsgemäß einige Einstellungen zur Bildschirmauflösung oder zum Netzwerk verloren. Insgesamt ist die schnelle Notwiederherstellung über dieses Verfahren in wenigen Minuten gut möglich.

Zusatzmodule nur gegen Aufpreis

Je nach Bedarf lässt sich die Basissoftware ShadowProtect mit optionalen und kostenpflichtigen Zusatzmodulen erweitern. Eines dieser Module ist die neueste Version von "HeadStart Restore". Hier werden Backups und Wiederherstellungen quasi simultan erstellt. Mit jedem inkrementellen Backup wird auch der Wiederherstellungsauftrag in einer Hyper-V- oder VMware-Umgebung aktualisiert. Im Falle eines Desasters kann der Auftrag abgeschlossen, die Treiber für die "hardwareunabhängige Wiederherstellung" angepasst und das fertige System neu gestartet werden.

Fazit

ShadowProtect eignet sich gut für reine Windows-Umgebungen, in denen schnelle Wiederherstellungen aus Snapshots heraus interessant sind. Die Übertragung der Sicherung auf Bänder bleibt dem Administrator selbst überlassen. Ge-

fallen hat uns die Möglichkeit, ein ausgefallenes System in einer VM schnell wieder verfügbar zu machen. Für relativ wenig Geld ist so eine hohe Ausfallsicherheit auch in kleineren Umgebungen realisierbar. (dr)



Produkt

Software zur Erstellung von Schattenkopien.

Hersteller

StorageCraft,
www.storagecraft.eu

Preis

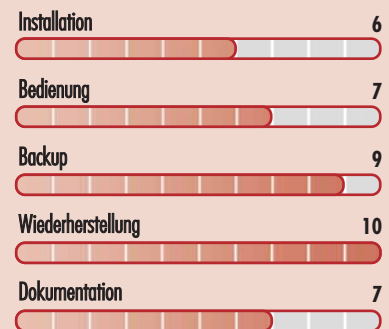
ShadowProtect 4, SBS Edition
(Small Business Server): 432 Euro
ShadowProtect 4, Server Edition: 869 Euro
ShadowProtect 4, ImageManager Enterprise:
261 Euro.

Bei allen Produkten ist die Funktion zur hardwareunabhängigen Wiederherstellung inbegriffen, eine Option, die bei einigen Mitbewerbern zusätzlich erworben werden muss. Staffelpreise nennt der Hersteller auf Anfrage.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

sehr gut für datenträgerbasierte Sicherungen in reinen Windows-Umgebungen mit Bedarf an hoher Verfügbarkeit.

bedingt in Umgebungen, in denen bereits Hochverfügbarkeitslösungen im Einsatz sind.

nicht für Umgebungen ohne Windows als Betriebssystem.

StorageCraft ShadowProtect Server 4



Quelle: Marko Cerovic - Fotolia.com

Sicherheitsfunktionen in Microsoft App-V

Gefahrlose Wege im Applikations-Strom

von Marc Grote

Das Streamen von Anwendungen mit Microsofts App-V vereinfacht den Administrationsaufwand deutlich. Applikationen müssen nicht mehr lokal installiert werden, kommen nicht in Konflikt mit anderer Software und lassen sich zudem zentral konfigurieren. Doch auch bei dieser Art von Virtualisierung sollten Sie die Sicherheit nicht außer Acht lassen. Microsoft stellt eine Reihe von Schutzmechanismen zur Absicherung von App-V zur Verfügung, die wir in diesem Workshop näher beleuchten.

Anwendungen werden bei App-V [1] von einem zentralen Server mittels eines Streams zum Rechner des Nutzers übertragen. Schon kurz nach Beginn des Transfers kann dieser die Applikation bereits verwenden, während im Hintergrund weitere Teile des Programms nachgeladen werden. Bis auf den App-V-Client muss dazu auf dem Rechner keine Software installiert sein. Die App-V-Systemarchitektur besteht aus folgenden Komponenten:

- Microsoft Systems Center Virtual Application Server: Dieser Server hostet das Softwarepaket und streamt es zur lokalen Ausführung auf den Client. Dabei konvertiert er Anwendungen mit dem SoftGrid Sequencer zu virtualisierten Paketen.
- Microsoft SoftGrid Application Virtualization for Desktops: Dieses Element wird auch als SoftGrid Client bezeichnet und ist zuständig für die clientseitige Ausführung der App-V-Pakete.
- App-V Management Console: Hierbei handelt es sich um das Verwaltungswerkzeug für den Application Server. Mit Hilfe dieser Konsole lassen sich virtualisierte Anwendungspakete erstellen, verwalten, aktualisieren und replizieren.

Microsoft bemüht sich um Vertrauen

Aufgrund der verteilten Architektur von App-V ist eine sichere Betriebsumgebung der Anwendungsvirtualisierung äußerst wichtig. Grundlage für eine sichere Infrastruktur sind die vom Hersteller herausgegebene Best Practice-Anleitung [2] und der App-V Security Operations Guide [3]. Die Redmonder Entwickler haben Version 4.6 nach folgenden Sicherheitsinitiativen programmiert:

- Trustworthy Computing (TwC)
- Secure Windows Initiative (SWI)
- Security Development Lifecycle (SDL)

Trustworthy Computing [4] ist eine langfristig angelegte, auf Kooperation basierende Initiative, deren Ziel mehr Sicherheit und Zuverlässigkeit im Umgang mit Computern ist und die auf vier Säulen fußt: Sicherheit, Datenschutz und Zuverlässigkeit von Software, Diensten und Produkten sowie Integrität im geschäftlichen Handeln von Microsoft. Die Secure Windows Initiative fokussiert sich auf die Entwicklung von sicheren Anwendungen, die gegen Vulnerabilities, Buffer Overruns und weitere Gefährdungen schützen soll. Das Security Development Lifecycle schließ-

lich beschäftigt sich mit der Entwicklung von sicheren Microsoft-Anwendungen und beinhaltet mehrere Schritte von der Entwicklungsphase bis zum Einsatz der Software und beschreibt einen ganzheitlichen Ansatz.

Sicherheit nur in einem abgesicherten Umfeld

Bevor wir uns mit den Möglichkeiten beschäftigen, wie Sie die unmittelbaren App-V-Komponenten absichern können, wenden wir uns zunächst dem Umfeld der Anwendungsvirtualisierung zu. Denn das Streamen von Applikationen kann selbst noch so sicher sein – es nützt alles nichts, wenn das zugrunde liegende Betriebssystem Lücken aufweist oder das Netzwerk nicht entsprechend abgesichert ist.

Sorgen Sie für ein gehärtetes Betriebssystem

Der erste Schritt zur Absicherung von App-V sollte die Absicherung des darunterliegenden Betriebssystems sein. Für dessen Härtung bietet sich der Windows Server 2008 Security Guide an, der sehr detailliert auf die notwendigen Konfigurationsschritte zur Absicherung der einzelnen Subsysteme eingeht und Maß-



Bild 1: Der Sicherheitskonfigurationsassistent überprüft unter anderem, über welche Ports es zum Austausch von Daten kommt

nahmen zur Umsetzung vorschlägt. Für einen erweiterten, rollenbasierten Schutz von Windows Server 2008 R2 können Sie zudem auf den Sicherheitskonfigurationsassistenten SCW (Security Configuration Wizard) zurückgreifen. Mit dessen Hilfe sichern Sie die als Basis für die Installation von Microsoft App-V dienende Windows-Umgebung mit einer Reihe von Best Practice-Empfehlungen ab. Der Assistent ist Bestandteil von Windows Server 2008 R2 und lässt sich mit Hilfe des Server Manager aufrufen.

Alles dicht im Netzwerk

Zur Absicherung der Kommunikationsverbindungen zwischen App-V-Client und -Server sowie zwischen Infrastrukturkomponenten wie Active Directory Domain Controller, DNS-Server und Microsoft SQL Server lässt sich der Datenverkehr mit SSL oder IPSec verschlüsseln. Empfehlenswert sind weiterhin wirkungsvolle Zugriffskontrollmechanismen wie Authentifizierung, Freigabe- und NTFS-Berechtigungen. Auch sollten Sie über den Einsatz einer Host-Firewall in Form der in Windows Server 2008 R2 integrierten Firewall nachdenken. Ferner ist die Verwendung einer zentralen Firewall wie Microsoft Forefront TMG zum Schutz der internen Netzwerksegmente vor externen Zugrif-

fen sehr sinnvoll, besonders wenn Sie Anwendungen mit Hilfe von App-V über das Internet zur Verfügung stellen – dazu später noch mehr.

SQL-Server nicht vergessen

App-V verwendet Microsoft SQL Server unter anderem zur Speicherung von Reports über die Verwendung der Anwendungsvirtualisierung. Um einen

einheitlichen Sicherheitsstandard zu gewährleisten, sollten Sie sich also auch um die notwendige Absicherung des Microsoft SQL Servers kümmern. Hierzu existiert ein Best Practice Guide, der alle notwendigen Maßnahmen beschreibt. Desweiteren können Sie auf das in Microsoft SQL Server enthaltene "SQL Server Surface Area Configuration Tool" zurückgreifen. Mit dessen Hilfe können Sie unter anderem die notwendigen SQL-Serverdienste konfigurieren und die verwendeten TCP-Ports festlegen.

Schutzmauern um App-V sinnvoll aufstocken

Ein Ergebnis der oben genannten Sicherheitsinitiativen ist, dass Microsoft mit App-V die integrierte Authentifizierung mit Hilfe von Kerberos unterstützt – neben dem ebenfalls bekannten NTLM-Authentifizierungsmechanismus. Außerdem bezeichnet der Hersteller die App-V-Konfiguration nach der Standardinstallation als "Secure by Default". Mit Hilfe von Benutzerberechtigungen können Sie steuern, welche Berechtigungen der App-V Desktop Client erhalten soll. Eine der weiteren Neuerungen ist die Möglichkeit, Dateisystem-ACLs (Access Control List) während des Sequencing-Prozesses aufzuzeichnen und der gestreamten Applikation zur Verfügung zu stellen.

Sichere Kommunikationswege mit IPSec

Bei der Kommunikation zwischen App-V Management Server / App-V Management Service und dem Microsoft SQL Server kommt standardmäßig Port 1433 zum Einsatz. Um den Datenaustausch des Management Servers und des Management Services zu sichern, ist die Verwendung von IPSec zu empfehlen. Mit Hilfe dieses Protokolls können Sie nur den Datentransfer auf Port 1433 verschlüsseln. Ein weiterer Kontakt, den es abzusichern gilt, ist der Zugriff des App-V Management Servers auf das App-V Content Directory. Dieses enthält alle Anwendungspakete, die für die App-V Clients zur Verfügung stehen. Für ein Plus an Sicherheit sollten Sie auch hier IPSec verwenden, um den Zugriff auf die Dateifreigaben einzuschränken.

Geschütztes Streaming mit RTSPS

Die Publishing-Daten einer Anwendung sendet der App-V Management Server als XML-Datei zum App-V Client. Die XML-Datei enthält den Pfad zum OSD-File, das für das Streamen der Anwendung zuständig ist. Die Bereitstellung der XML-Datei kann mit Hilfe von RTSP oder RTSPS geschehen. RTSP steht für Real Time Streaming Protokoll, dessen Erweiterung RTSPS die Sicherheit noch einmal erhöhen soll. Mit Hilfe von RTSPS richten Sie eine verschlüsselte Verbindung zwischen App-V Server und App-V Client ein: Dabei erfolgt allerdings keine Mutual Authentication, es wird lediglich die Server-Authentizität bestätigt. Um eine Verbindung über RTSPS herzustellen, müssen folgende Voraussetzungen erfüllt sein:

- Das Zertifikat muss gültig sein.
- Das Zertifikat ist für die korrekte EKU (Extended Key Usage)-Server Authentication (OID 1.3.6.1.5.5.7.3.1) ausgestellt.
- Der FQDN des Servers stimmt mit dem Common Name (CN) des Zertifikats überein.
- In NLB-Umgebungen ist ein SAN (Subject Alternate Name)-Zertifikat notwendig.



Bild 2: So sieht der Aufbau der Infrastruktur aus, wenn Sie Anwendungen mit App-V über das Internet streamen wollen

- Client und Server müssen der ausstellenden Zertifizierungsstelle (CA) vertrauen.
- Der private Schlüssel des Zertifikats ist für Änderungsrechte des App-V-Dienstes zugreifbar.

App-V Client mit begrenzten Rechten

Microsoft hat in der aktuellen Version des App-V Clients die Berechtigungen so eingeschränkt, dass der Endbenutzer lediglich einen Refresh der Anwendungsveröffentlichungen durchführen und Anwendungen auf den Client streamen darf. Zu den weiteren Sicherheitsmaßnahmen gehören:

- Der Client darf ein OSD Cache Update nur während des Veröffentlichungs-Refreshes durchführen.
- Nur Benutzer mit Admin-Rechten können die Datei `sfilog.txt` öffnen.
- Die Logdatei hat nun eine maximale Größe.
- Alle App-V-Clientvorgänge werden im System Log der Ereignisanzeige aufgezeichnet.

Eine gestreamte Anwendung lässt sich nur nach erfolgreicher Überprüfung der Anmeldeinformationen starten. Ist der App-V Server nicht verfügbar und die Anwendung wurde noch nicht gestartet, ist somit kein Aufruf der Anwendung möglich. Hat der Nutzer die Anwendung zuvor schon einmal geöffnet, lässt sich sel-

bige selbst dann ausführen, wenn keine Verbindung zum Server existiert. In diesem Fall arbeitet der Client mit lokal zwischengespeicherten Anmeldeinformationen. Dieses Verhalten lässt sich allerdings durch die Modifikation der Registry-Einstellung "RequireAuthorizationIfCached" ändern. Zur weiteren Erhöhung der Sicherheit des App-V Clients können Sie administrative Vorlagendateien, sogenannte ADM-Templates, einsetzen. Mit deren Hilfe legen Sie an zentraler Stelle Client-Settings fest. Ferner sollte auf Clientseite ein Virens Scanner im Gebrauch sein. Beim Scanvorgang ist jedoch die Datei `sfilog.txt` auszuschließen – diese enthält den App-V-Paketcache.

Anwendungen sicher über das Internet transportieren

Seit Version 4.5 von App-V ist es möglich, auch Clients im Internet, die nicht Mitglied des firmeninternen LANs sind, Applikationen über das Internet zur Verfügung zu stellen. Bei der Veröffentlichung von Anwendungen über das Internet ist die Verwendung von RTSPS oder HTTPS zwingend vorgeschrieben. Welcher Verbindungstechnik Sie den Vorrang geben wollen, ist abhängig von Ihren Anforderungen an die verfügbaren Funktionen. RTSPS erlaubt zum Beispiel ein aktives Upgrade, während HTTPS bessere Performance in großen Client-Umgebungen liefert.

Egal für welches Verfahren Sie sich entscheiden, für die Web-Bereitstellung eines App-V Servers bieten sich nur zwei Varianten an: Entweder Sie stellen die App-V-Dienste durch die Veröffentlichungsfunktionen von Microsoft Forefront TMG bereit oder Sie betreiben den App-V-Server in einer DMZ, um diesen vom internen Netzwerk zu trennen. In letzterem Szenario müssen Sie allerdings zusätzliche Ports zum internen Netzwerk öffnen für:

- SQL
- SMB/CIFS (wenn das App-V Inhaltsverzeichnis im internen Netzwerk liegt)
- Kerberos
- DNS
- LDAP

Fazit

Microsoft stellt für App-V eine Reihe von integrierten Sicherheitsmaßnahmen zur Verfügung. Auch wenn diese korrekt konfiguriert sind, sollten Sie nicht vergessen, durch weitere Sicherheitsfunktionen des darunterliegenden Betriebssystems für eine noch besser gehärtete Umgebung zu sorgen. (In)

Marc Grote ist MVP für Forefront.

Sie finden seinen Blog unter:

www.it-training-grote.de/blog/

[1] Microsoft App-V im Überblick

www.microsoft.com/systemcenter/appv/default.aspx

[2] Microsoft App-V Security Best Practice

http://download.microsoft.com/download/f/7/8/f784a197-73be-48ff-83da-4102c05a6d44/AppV_Security_Best_Practices.docx

[3] Microsoft App-V Security Operations Guide

http://download.microsoft.com/download/f/7/8/f784a197-73be-48ff-83da-4102c05a6d44/AppV_Security_Operations_Guide.docx

[4] Microsoft Trustworthy Computing

www.microsoft.com/about/twc/en/us/default.aspx

Links



Network Monitoring hilft bei der frühzeitigen Erkennung von Malware-Attacken

Studie zeigt: PRTG Network Monitor wichtiger Bestandteil von IT-Sicherheitskonzepten

Wie eine Anwenderumfrage der Paessler AG zum Einsatz ihrer Software PRTG Network Monitor zeigt, gewinnt der Sicherheitsaspekt bei der Verwendung einer Netzwerküberwachungslösung für Unternehmen zunehmend an Bedeutung. Rund 75 Prozent nutzen das Tool mittlerweile als strategische Komponente und sinnvolle Ergänzung zu Virenschannern, E-Mail-Sicherheitsprogrammen oder Firewalls. Ein Hauptgrund ist die Zeitersparnis beim frühzeitigen Erkennen von Malware-Attacken.

Netzwerksicherheit in Unternehmen setzt die Planung und Umsetzung eines ganzheitlichen Konzeptes voraus. Denn viele Firmen wännen ihre IT-Infrastruktur in Sicherheit, wenn die Firewall zuverlässig arbeitet und der Virenschanner aktuell ist. Jedoch entwickeln Cyberkriminelle immer professionellere Methoden sowie intelligenter und effektiver arbeitende Schad-Software. So hat beispielsweise die Zahl an Drive-by-Downloads und Denial-of-Service-Angriffen in den vergangenen Jahren stetig zugenommen. Als Angriffsziel immer häufiger im Fokus sind Social Media-Plattformen wie Facebook, Twitter, Xing & Co., die vermehrt von Unternehmen als strategisches Kommunikations-Tool genutzt werden.

Monitoring als Frühwarnsystem

Eindeutige Warnzeichen werden hier häufig übersehen. Vielmehr beklagen sich Unternehmen über langsame Antwortzeiten von Applikationen und Webseiten. Hohe, abrupt auftretende CPU-Laständerungen, unerwartet starker Traffic oder eine Überbeanspruchung der Festplattenkapazitäten sind dabei wichtige Hinweise auf unentdeckte Angriffe. Trotzdem werden Malware-Attacken oft erst zu spät entdeckt. Eine in das Sicherheitskonzept integrierte Network Monitoring-Lösung wie PRTG dient hier mit passend konfigurierten Schwellenwerten als Frühwarnsystem.

Wie die Paessler-Umfrage bestätigt, ist Netzwerküberwachung neben Sicherheits-Tools, wie beispielsweise Virenschannern und Firewalls ei-



Toplisten zeigen unter anderem, welche Art der Netzwerknutzung den meisten Traffic verursacht.

ne sinnvolle Ergänzung zur Erhöhung des Sicherheitsgrads. Unregelmäßigkeiten im Netzwerk können damit frühzeitig aufgedeckt werden. Eine entsprechende Monitoring-Software zeigt zudem Trends auf und hilft bei der strategischen Planung. PRTG alarmiert den Administrator sofort über alle Auffälligkeiten, die ein Hinweis auf Malware-Attacken sein können, und sendet umgehend Benachrichtigungen via E-Mail, ICQ, Pager, SMS etc. Dieses Feature stuften 77 Prozent der Befragten als „sehr wichtig“ ein.

Auf Basis der Paessler-Lösung ist es möglich, Daten zu Bandbreiten von Standleitungen, Netzwerkverbindungen oder -geräten (Routern, Switchen etc.) zu erfassen. Zudem stellt das Tool Auslastungstrends, drohende Engpässe und Verbindungsfehler fest. Die Ergebnisse präsentiert PRTG detailliert in Form von Tabellen und Graphen. Netzwerkadministratoren können so die Bandbreitennutzung überwachen und mittels Packet Sniffing oder NetFlow-Monitoring die aktivsten IP-Adressen und häufigsten Protokolle ermitteln. Mit Hilfe von Remote Probes hat die Software das gesamte – auch in räumliche Segmente getrennte – Unternehmensnetzwerk im Auge. Managed Service-Providern bietet sie zudem die Möglichkeit, Kundennetzwerke umfassend zu monitorieren.



Packet Sniffer-Sensoren analysieren den Traffic nach Protokollen und stellen die gesamte Bandbreitennutzung anschaulich dar.

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



Sichere Netzwerk-Konfiguration unter vSphere

Virtuelle Schlupflöcher zumauern

von Dennis Zimmer



Quelle: AKS - Fotolia.com

Konsolidierung und eine zentrale Verwaltung bringen beim virtualisierten Betrieb der IT-Infrastruktur zahlreiche Vorteile und sind für viele Administratoren eine Arbeitserleichterung. Allerdings stehen Komfort und Sicherheit in manchen Teilen leider konträr zueinander – umso komfortabler sich das Management der VMware-Umgebung gestaltet, desto offener sind nicht selten Einfallstore für unbefugte Eindringlinge. Wir zeigen Ihnen in unserem Workshop, wie Sie mit Bordmitteln die gängigen und oft vergessenen Schlupflöcher unter vSphere schließen und welche Besonderheiten es bei virtuellen Maschinen zu beachten gibt.

Sicherheit beginnt bereits beim Download von Software – selbst von vermeintlich vertrauenswürdigen Webseiten wie der von VMware oder Drittherstellern. Sie sollten die Integrität dieser Dateien stets mittels eines MD5- oder SHA-1-Schlüssels prüfen, der zumeist direkt beim Downloadlink zu finden ist. Auch den Zugriff mittels vSphere Client auf die ESX-Hosts oder vCenter Server sollten Sie mit gültigen eigenen Zertifikaten absichern, um eine größtmögliche Verbindungssicherheit zu gewährleisten.

Host-Sicherheit kommt zuerst

Der erste wichtige Schritt zum sicheren Betrieb einer vSphere Umgebung beginnt beim Infrastruktur-Zugriff und daher schon bei der Netzwerkplanung. Dazu gehört natürlich das Management-Netz (Service-Konsole bei ESX, VMkernel Management bei ESXi), über das jegliche

Verwaltung des ESX-Servers und damit der virtuellen Maschinen stattfindet. Daher sollten Sie an dieser Stelle zu verschiedenen Schutzmaßnahmen greifen.

Root-Zugang einschränken

Eine wichtige Maßnahme, um unberechtigte interne oder externe Zugriffe auf die Service-Konsole zu verhindern, besteht darin, die Netzwerkkarten (vSwitch Uplinks) so zu konfigurieren, dass sie sich in einem abgeschotteten Management-Netzwerk befinden. Dieses sollte komplett physikalisch oder durch die Nutzung von vLANs vom Produktiv-LAN und vor allem von halböffentlichen (DMZ) oder öffentlichen Netzwerken separiert sein.

Zu den weiteren Mitteln gehört es, den Root-Zugriff und damit den wichtigsten Benutzer Unix-orientierter Betriebssysteme möglichst restriktiv zu

handhaben, da dieser für die Verwaltung aller Dienste und Dateien autorisiert ist. Empfehlenswert ist hier eine Anmeldung per Benutzer-Account mit Standardberechtigung und "Switch" zu Root (su- und sudo-Befehle). Auch die Wahl eines komplexen, in regelmäßigen Abständen geänderten Kennworts sollte selbstverständlich sein. Zur Definition der Passwort-Regeln verwenden Sie den Befehl `esxcfg-auth usepamqc`. ESXi bietet zudem den "Lockdown Mode" als Sicherheitsmaßnahme an, wodurch alle Zugriffe des Root-Benutzers durch die API und damit vSphere Client, vCLI und PowerCLI gesperrt werden. Nicht-Root-Benutzer sind davon nicht betroffen. Der sogenannte Tech Support Mode, der den Konsolenzugriff auf den ESXi-Server erlaubt, lässt sich mit der erweiterten Einstellung `VMkernel.Boot.techSupportMode` abschalten. Grundsätzlich gar nicht



erst aktivieren sollten Sie den nicht offiziell unterstützten SSH-Zugriff auf den ESXi-Server.

Firewall schließen, Webzugriff deaktivieren

Nach der Installation von VMware ESX 4 ist die Durchlässigkeit der Firewall auf ein Minimum beschränkt und es sind nur wenige VMware-Dienste sowie (anders als beim ESXi-Server) SSH-Zugriff erlaubt. Wollen Sie zusätzliche Dienste betreiben, etwa Hardwaremanagement-Agenten oder Backup-Agenten, müssen Sie dies explizit erlauben. Sie sollten immer prüfen, ob zusätzliche Programme in der Service-Konsole wirklich notwendig sind. Bei der Verwendung von ESXi erübrigt sich die Frage, da sich keine Tools installieren lassen. Eine Auflistung des derzeit gültigen Regelwerks bringt das Kommando `esxcfg-firewall -q` auf den Bildschirm.

Benötigen Sie keinen Zugriff über das Web, sollten Sie diesen abschalten. Verbinden Sie sich dazu mit dem vSphere Client auf den ESX-Host und klicken Sie dort unter "Configuration / Security Profile" auf "Web Access deaktivieren". Gleiches gilt für den Managed Object Browser. Dies lässt sich durch Anpassung der Datei `proxy.xml` (Löschen oder Auskommentieren der Zeile "`<serverNamespace>/mob</serverNamespace>`") realisieren.

Patches und Protokolldateien im Blick behalten

Weiterhin sind natürlich die typischen administrativen Tätigkeiten wie das Überprüfen auf die Verfügbarkeit neuer Patches und deren Installation auf den ESX-Servern Pflicht. Dazu bietet sich natürlich der Update Manager sehr gut an. Aber auch diesen sollten Sie im Auge behalten. Beachten Sie, dass die Service-Konsole zwar auf Red Hat basiert, Sie im Netzwerk allerdings keine Red Hat-Updatemechanismen (etwa RedHat Network Satellite) nutzen sollten. Denn kommen andere Patch-Methoden als `esxupdate`

```
isolation.tools.diskwiper.disable=TRUE
isolation.tools.diskshrink.disable=TRUE
remotedisplay.maxConnections=1
isolation.tools.copy.disable=TRUE
isolation.tools.paste.disable=TRUE
isolation.tools.setGUIOptions.enable=FALSE
isolation.device.connectable.disable=TRUE
isolation.device.edit.disable=TRUE
vmci0.unrestricted=FALSE
tools.setInfo.sizeLimit=1048576
guest.command.enabled=FALSE
tools.guestlib.enableHostInfo=FALSE
```

**Listing: Absicherung von VMs
gemäß VMware Hardening Guide**



oder der VMware Update Manager zum Einsatz, können schwerwiegende Probleme die Folge sein.

Die Protokolldateien sollten Sie ebenfalls regelmäßig überwachen. Sie können den Syslog-Agenten auf den ESX-Hosts so konfigurieren, dass die Protokolleinträge zusätzlich an einen zentralen Syslog-Server versendet werden. Nicht nur den Zeitstempeln der Protokolldateien zuliebe, sondern auch um eine korrekte Systemzeit sicherzustellen, ist in jedem Fall NTP auf den Hosts zu konfigurieren. Zusätzlich sollten Sie alle Überwachungsmöglichkeiten von VMware nutzen, was unter anderem das Alerting des vCenter (Mail, SNMP Traps) und die SNMP-Überwachung beinhaltet. Wollen Sie die Konfigurationen zentral konfigurieren und auf die ESX-Hosts verteilen beziehungsweise deren Integrität testen, empfehlen sich Host Profiles, die ab der Enterprise Plus Lizenz verfügbar sind.

Virtuelle Maschinen absichern

Sicherheit im Virtualisierungsumfeld bedeutet natürlich auch Sicherheit auf den virtuellen Maschinen (VM) selbst beziehungsweise bei deren Betrieb. Das Thema Ausfallsicherheit einmal ausgeklammert, sollten Sie, was die Zugriffssicherheit betrifft, einige wichtige Einstellungen vornehmen.

VMware hat im vSphere Hardening Guide [1] einige Zeilen zur Absicherung virtueller Maschinen verfasst. Neben den gängigen Standards, Netzwerke sicher auf-

zubauen und die Änderung der Netzwerkzuordnung in den VMs zu überwachen, stehen vor allem VMware-eigene Funktionen im Fokus. Im Kasten "Absicherung von VMs gemäß VMware Hardening Guide" sind die wichtigsten Grundeinstellungen aufgeführt. Eine genaue Beschreibung dieser Settings finden Sie unter [2]. Außerdem steht unter [3] zudem ein Skript zur Verfügung, das für die Automatisierung des Härtungs-Prozesses sorgt.

Wollen Sie VMs in der DMZ einsetzen, so sollten Sie folgende Punkte zur zusätzlichen Absicherung nicht vergessen:

- Verwenden Sie ESX-Hosts mit eigenen LUNs für die DMZ.
- Trennen Sie ESX-Hosts in der DMZ von ESX-Hosts im normalen LAN.
- Mischen Sie keine DMZ-VMs mit LAN-VMs auf dem gleichen ESX Host oder der gleichen LUN.
- Bei der Nutzung von DRS Cluster müssen entsprechende Regeln zum Schutz vor automatischer Migration geschaffen werden, um Mischumgebungen zu vermeiden.
- Storage VMotion und VMotion wird im Klartext durchgeführt, daher sollten Sie diese Netze vom Netzwerk der virtuellen Maschinen trennen.

Switching mit doppeltem Boden

Wer über ESX hinaus einen Blick in Richtung Netzwerke wirft, dem wird spätestens beim zweiten Gedankengang klar, dass die virtuellen Portgruppen administrativ zwar ein Segen sind, Fehlkonfigu-

Was die System-Architektur betrifft, ist die normale ESX-Version als weniger sicher anzusehen als die ESXi-Variante. Dies liegt vor allem an deren reduzierten Angriffsfläche aufgrund der abgespeckten und gehärteten Verwaltungskonsolle, die auf einem Busybox-Linux basiert. Da diese Konsolle wesentlich weniger zusätzliche Komponenten als die Nicht-ESXi-Version besitzt, fällt die Anzahl der Patches über die gesamte Laufzeit gesehen deutlich geringer aus.

**ESXi gilt als
schlanker und sicherer**



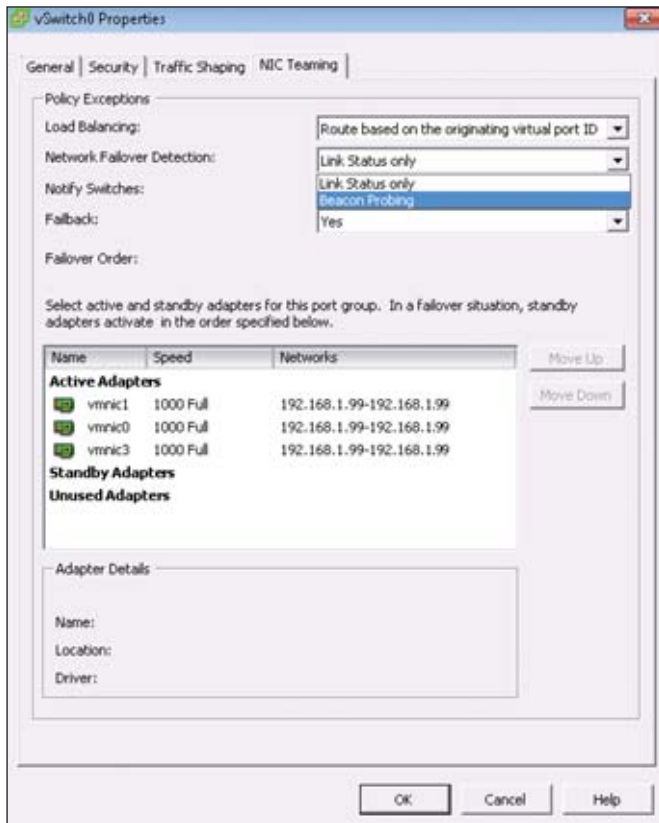


Bild 1: Das Aktivieren von "Beacon Probing" in den Eigenschaften eines virtuellen Switch sorgt für zusätzliche Sicherheit

rationen allerdings oft im Verborgenen bleiben. Haben Sie etwa einen virtuellen Switch mit mehreren Uplinks angelegt, auf dem wiederum drei Dutzend VLANs konfiguriert sind, so legen Sie im Regelfall für jedes VLAN eine entsprechende Portgruppe an. Es lässt sich allerdings nur schwer verhindern, dass ein Administrator einmal eine falsche Portgruppe der VM konfiguriert – urplötzlich steht das System dann in einem ungeschützten Netz, etwa der DMZ. Kommen dann noch DHCP-Server oder erreichbare IP-Adressen mit ins Spiel, entsteht eine äußerst riskante Sicherheitslücke.

Konfigurationschaos bei VLANs vermeiden

Ein weiteres Manko betrifft die Ausfallsicherheit: Vor allem bei häufiger VLAN-Nutzung sind Konfigurationsfehler nichts Ungewöhnliches. So kommt durchaus vor, dass eine VM dank HA, DRS oder einer manuellen VMotion-Migration nicht mehr über das Netzwerk erreichbar ist,

da auf dem Ziel-ESX-System zwar die richtige Portgruppe existiert, den Uplinks aber nicht alle VLANs zugeordnet wurden. Daher empfiehlt es sich, die Uplinks stets genau zu prüfen und gegebenenfalls "Beaconing" zu aktivieren. Dies ist ein verbessertes Prüfverfahren, um Uplinks auf korrekte Kommunikationsmöglichkeiten zu überwachen. Allerdings müssen dazu mindestens drei Uplinks entsprechend konfiguriert sein, damit "Beacon Probing" korrekt funktioniert.

Weiterhin sollten

Sie bei den vSwitches wie auch bei den Portgruppen vermeiden, die Sicherheits-Einstellungen herabzusetzen. Wenn dies aufgrund eines Netzwerk-Sniffers oder anderer Anwendungen notwendig ist, so sollten Sie an dieser Stelle eine Ausnahmeregelung nur für die Netzwerkadapter dieser einen VM mit reduzierter Sicherheit konfigurieren.

Virtuelle Brandschutzmauern mit vShield Zones

Im Prinzip lässt sich VMware vShield Zones einfach als Firewall-Lösung in Form einer oder mehrerer virtueller Appliances beschreiben, die den Netzwerkverkehr zwischen den virtuellen Maschinen beziehungsweise den VMs und der Außenwelt protokollieren und regulieren. Somit können Sie auf Protokoll- und Port-Ebene Firewall-Regeln über eine zentrale Weboberfläche definieren.

Technisch gesehen wird dabei den virtuellen Maschinen ein neuer virtueller

vSwitch ohne Uplinks zugewiesen. Die vShield Zone, die das entsprechende Netz überwachen soll, ist mit einem Netzwerkinterface auf dem vSwitch verbunden und das gesamte Netzwerk wird über diese Zone geleitet. Als zweites Interface arbeitet die vShield Zone in dem ursprünglichen vSwitch mit den physikalischen Uplinks und leitet den Netzwerkverkehr je nach Regelentsprechung um oder blockiert diesen. Bevor Sie vShield Zones einsetzen, sollten Sie sich einige Gedanken zur Implementierung und den Ausfallszenarien (wenn eine Zone ausfällt) machen.

Sicherheit bei physikalischen Switches

Wollen Sie Sicherheit physikalisch realisieren und nicht nur in Form einer virtuellen Appliance, sollten Sie sich die Sicherheits-Features der Switch-Hersteller genauer ansehen. Cisco bietet zum Beispiel in Verbindung mit den

VMware hat mit vSphere die VMsafe-API ins Leben gerufen, die dafür sorgen soll, dass Hersteller von Sicherheits-Software die Kernel-Mitteilungen und damit auch die Informationen über alle virtuellen Maschinen miteilen können. Damit würde sich ein Agent in jedem Gastbetriebssystem erübrigen, was deutliche Last von den VMware-Systemen nehmen würde.

So etwa ist Antivirensoftware durch VMsafe in der Lage, direkt vom VMkernel Daten zu erhalten und diese auf Viren und andere Schadsoftware zu durchsuchen. Dazu muss lediglich eine Antivirus-Instanz als virtuelle Appliance vorhanden sein, um den Datenverkehr, die Hauptspeicherzugriffe, ablaufende Prozesse oder den Netzwerktransit zu überwachen und gegebenenfalls einzugreifen.

Die VMsafe-API lässt sich vom Endanwender nicht konfigurieren oder manipulieren und muss seitens VMware natürlich so sicher aufgestellt werden, dass keine Entwickler von Schadsoftware in deren Genuss kommen können. VMware arbeitet aus diesem Grund sehr eng mit Unternehmen wie McAfee, Symantec oder Trend Micro zusammen. Bis zur Drucklegung des Artikels wurde aber noch keine freigegebene, VMsafe nutzende Antivirenlösung veröffentlicht. Allerdings sind bereits Betaversionen verfügbar.

Zukunft VMsafe?





*Das Ziel für
IT-Sicherheits-
Verantwortliche:*

it·sa Nürnberg,
19.-21.Okt. 2010

it-sa 2010: Der Treffpunkt der IT-Security Branche

- 300 Aussteller mit Lösungen zu Informations-Sicherheit, Datenschutz, Hardware-Sicherung und Security-Awareness
 - Non-Stop-Vortragsprogramm auf 3 großen Foren mit 170 Kurzreferaten, Podiumsdiskussionen, Live-Demos und Best-Practice-Beiträgen
 - Guided Tours und Topic-Routen
 - 20 Kongresse, Tagungen, Workshops, z.B.:
 - Workshop: Forensic Extreme
 - Hacking-Lab: Web Security Hand-on Training
 - Web 2.0 - Web Applications: Advanced
- Mehr Infos: www.it-sa.de/veranstaltungen**



Die IT-Security-Messe

**Nürnberg,
19.-21.Okt. 2010**

Veranstalter: SecuMedia Verlags-GmbH
Postfach 12 34, D-55205 Ingelheim,
Telefon +49 6725 9304-0, Fax +49 6725 5994



Gastkarte anfordern

**[www.it-sa.de/
e-ticket](http://www.it-sa.de/e-ticket)**

Code: 9ADM9682N2

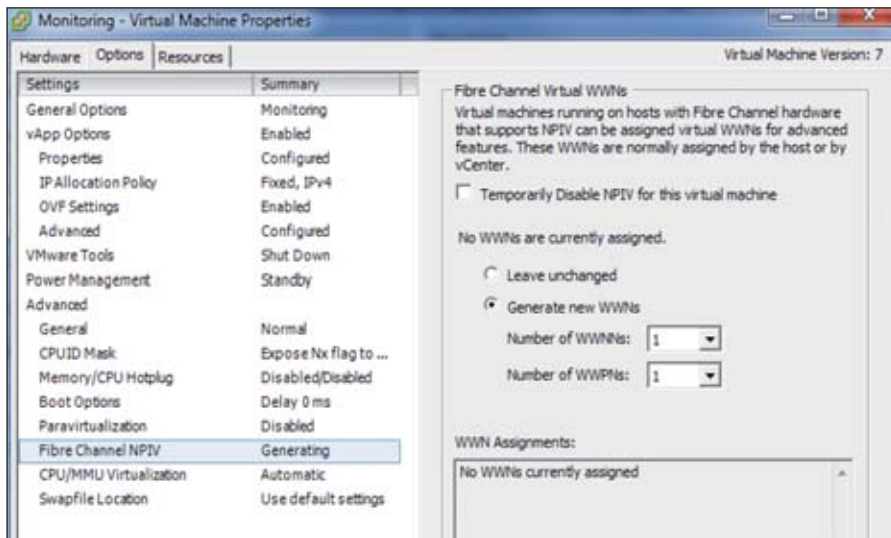


Bild 2: Die NPIV-Konfiguration erfolgt direkt in den Eigenschaften der virtuellen Maschine

Distributed vSwitches die Möglichkeit einer Nutzung von PVLANs (Private VLANs), welche die Kommunikation zwischen virtuellen Systemen physikalisch verbieten können. Ein weiterer Hersteller ist Enterasys, der es bei seinen Geräten erlaubt, einer VM Profile auf dem Switch zuzuordnen, in denen genau definiert wird, welche Ports und Netzwerke für diese nutzbar sind. Die Profiltzuordnung realisiert der Switch aufgrund der MAC-Adressen der virtuellen Maschinen.

Storage wirkungsvoll abschirmen

Was die Sicherheit des Storage anbetrifft, sind in erster Linie die IP-basierten Storage-Systeme beziehungsweise die Kommunikation zwischen den Komponenten betroffen. Setzen Sie Fibre Channel ein, gibt es nicht ganz so viele Optionen, die Sie beachten müssen. Als wichtigste Maßnahme ist hier "Single Initiator Zoning" zu nennen. Dies bedeutet die Bildung von Zonen, die einen einzelnen Initiator mit Storage-Targets verbinden und niemals zwei.

Zur Erhöhung der Zugriffssicherheit trägt außerdem das Zoning auf dem FC-Switch bei. Ein weiterer Punkt ist die Nutzung von NPIV (N-Port ID Virtualisierung), bei der Sie dediziert FC-

WWPNs einer virtuellen Maschine zuordnen und so nur dieser den Schreibzugriff gestatten.

Wichtig bei IP-basierten Storage-Systemen ist der Schutz vor Man-in-the-middle Attacks – niemand soll sich zwischen Target und Initiator klemmen können. Am besten regeln Sie dies mit einer Mischung aus physikalischer Switch-Sicherheit und logischer Kommunikationssicherheit. Die physikalische Sicherheit realisieren Sie entweder über eigene Switches für den Storage oder über eigene VLANs am Switch, an dem das Storage-Netzwerk beheimatet ist. Damit verhindern Sie wirkungsvoll die Kommunikation des Standard-LAN mit der Storage-Umgebung.

Bei der Verwendung von NFS sollten Sie unbedingt von der Option Gebrauch machen, zusätzliche erlaubte IP-Adressen anzugeben, die Zugriff auf die NFS Exports haben. iSCSI bietet die Möglichkeit, CHAP (Challenge Handshake Authentication Protocol) zu nutzen. Dieses Protokoll erlaubt eine Kommunikation nur dann, wenn sowohl Initiator als auch Target den gleichen geheimen Schlüssel verwenden. Die Verschlüsselung der iSCSI-Pakete mit IPsec wird von VMware aktuell nicht unterstützt.

Fazit

Es gibt viele einfache Möglichkeiten, um unter vSphere die virtuelle Infrastruktur abzusichern und für Eindringlinge nur äußerst schwer zugänglich zu machen. Reduzieren Sie die Möglichkeiten der Netzwerkkommunikation mit dem ESX-Host so weit wie möglich und arbeiten Sie mit komplexen Passwörtern sowie definierten Berechtigungsrollen. Außerdem sollten Sie immer die Aktualisierungen im Auge behalten und bei Sicherheitslücken einer Version die verfügbaren Patches nachpflegen.

Zusätzlich ermöglichen weitere, kostenlos im Internet erhältliche Skripte [4] eine recht bequeme Überwachung und Prüfung der virtuellen Infrastruktur in einer VMware-Umgebung. Diese Här-tung sollten Sie allerdings sehr ernst nehmen, da Sicherheitslücken auf einem Hostsystem Probleme für alle virtuellen Maschinen bedeuten können – schließlich stehen diese in einer 1:n-Beziehung zueinander. (In)

- [1] vSphere 4.0 Security Hardening Guide
<http://communities.vmware.com/docs/DOC-12306/>
- [2] VMware Hardening Guide Certification
<http://communities.vmware.com/docs/DOC-12535/>
- [3] Skript zur Härtung virtueller Maschinen unter vSphere
www.lucd.info/2010/02/16/security-hardening-part-1-virtual-machines/#more-1773
- [4] vSphere Security Hardening Report Check
<http://communities.vmware.com/docs/DOC-11901/>

Dennis Zimmer: VMware vSphere 4 – Das umfassende Handbuch.
Galileo Computing, 1.052 Seiten,
ISBN 978-3-8362-1450-6, 89,90 Euro

Dennis Zimmer: VMware ESX 4 – Automatisierung, Befehle, Scripting.
Galileo Computing, 687 Seiten,
ISBN 978-3-8362-1644-9, 69,90 Euro

Links





Sicherheit bei der Servervirtualisierung

Vorsicht: Blaue Pille

von Nils Kaczenski

Die "Blaue Pille" ist ausnahmsweise kein neuer Viagra-Spam, sondern ein äußerst subtiler Angriff auf virtualisierte Server. Neben ihren überzeugenden Vorteilen wie weniger Hardwarebedarf, höhere Effizienz und neue Möglichkeiten in Administration und Betrieb warten auf virtuelle Server auch immense Gefahren. Gartner geht in einer aktuellen Studie davon aus, dass in den nächsten zwei Jahren 60 Prozent der Server weniger sicher sind als heute. Zentrale Themen dieser Betrachtung sind die Security der Systeme und die Ausfallsicherheit. In diesem Beitrag gehen wir daher Fragen nach potentiellen Bedrohungen von virtuellen Maschinen ebenso auf den Grund wie der Aufgabenstellung, eine höhere Ausfallsicherheit zu gewährleisten.



Quelle: Tortenboxer - Fotolia.com

Virtualisierung im Serverraum ist beileibe kein neues Thema mehr: Bereits 2001 veröffentlichte VMware die ersten Serverversionen seiner Virtualisierungssoftware und zwei Jahre später mit Version 2.0 des ESX Servers begann die Technik, sich im Mittelstand zu etablieren. Im selben Jahr übernahm Microsoft das Produkt "Virtual PC" von Connectix mit dem erklärten Ziel, die Technik in den Serverraum zu bringen. Und doch bleibt Servervirtualisierung ein Aufreger, der Hype scheint ungebrochen.

Viele IT-Verantwortliche haben jedoch eher unscharfe Vorstellungen davon, wozu virtuelle Server in ihrem Netzwerk gut sein könnten. Trotzdem fragen sie mit Nachdruck nach solchen Lösungen und äußern vage Ideen von Kostensenkung, Energiesparen und Ausfallsicherheit. Der Verantwortliche tut gut daran zunächst einen Schritt zurückzutun und zu fragen: Virtualisierung – wozu eigentlich? Denn die Erfahrung zeigt, dass ein Projekt ohne klares Ziel nur scheitern kann. Ohne trennscharfe Kriterien, die ein neues System erfüllen muss, wird niemand die Frage beantworten können, ob das Projekt

erfolgreich war. Grund genug, sich die Versprechen der Marketingfolien genauer anzusehen und sie daraufhin zu untersuchen, ob sie für das eigene Vorhaben überhaupt relevant sind. Führt dies nicht zu einem überwiegend positiven Ergebnis, dann wird der Ansatz nicht zur Betriebssicherheit der IT beitragen.

Ziele der Virtualisierung genau definieren

Die oben angerissenen Schlagworte wie Kostensenkung, Energiesparen oder Ausfallsicherheit sind für sich genommen nicht abwegig, wenn Unternehmen ein Netzwerk auf Virtualisierung umstellen. Doch Differenzierung tut not: Ein hochgradig ausfallsicheres VM-System wird dem Controller Tränen in die Augen treiben, denn die Kosten der nötigen technischen Redundanz summieren sich schnell sechs- oder gar siebenstellig (vom Strom ganz zu schweigen). Was die Hersteller nämlich gern im Kleingedruckten verbergen, sind Investitionen in teure SAN-Technik (Netzwerkspeicher und Fibre Channel-Komponenten) oder in die LAN-Infrastruktur, die zum Beispiel getrennte Rechenzentren redundant ver-

binden kann. Auch die Server selbst schonen nicht unbedingt den Geldbeutel: Wer 60 physische Server durch virtuelle ersetzen will, kann zwar durchaus mit vier bis sechs neuen Maschinen arbeiten, aber die spielen in einer anderen Güteklasse als die "Pizzaboxen", die sie vielleicht ablösen.

Damit ist die Frage nach der Ausfallsicherheit selbst aber noch nicht beantwortet. In der Praxis teilen sich die Anforderungen der IT-Verantwortlichen in zwei Kategorien. Die einen sagen "Wir können uns eigentlich gar keinen Ausfall erlauben" und die anderen geben an: "Bei uns ist das nicht so wild, 95 oder 98 Prozent Verfügbarkeit reichen völlig". Während im ersten Fall eine Skizze des nötigen Budgets für ein komplett ausfallsicheres Netzwerk die Realität zurück ins Blickfeld holt, reicht im zweiten Fall eine einfache Prozentrechnung: Eine Verfügbarkeit von 95 Prozent bedeutet aufs Jahr gerechnet, dass in fünf Prozent der Zeit, also über 18 Tage, die IT nicht bereitsteht. Um allerdings zu einer brauchbaren Betrachtung zu gelangen, ist das keine reine EDV-Frage mehr, denn die



Unternehmensleitung muss definieren, welche Prozesse so geschäftskritisch sind, dass sie höhere Ausgaben rechtfertigen. Am Ende steht idealerweise eine Matrix, wie sie die Tabelle "Tolerierbare Ausfallzeit" vereinfacht darstellt. Eine Matrix der Anforderungen an die Verfügbarkeit sollte sich an einzelnen Komponenten oder Prozessen orientieren. Neben der tolerierbaren Ausfallzeit sind Fragen nach verkraftbaren Datenverlusten und Archivierungszwängen zu beantworten.

Hinter der Fassade: Komplexe IT

Nicht nur hinter der Virtualisierung verbirgt sich einiges an Komplexität, sondern auch die Technik selbst hat ihre Eigenarten, die Sie im Blick haben sollten. Möchten Sie ein vorhandenes Netzwerk in ein virtuelles überführen, wird dies – anders als oft erwartet – den administrativen Aufwand in aller Regel nicht reduzieren, sondern erhöhen. Die vorhandenen Maschinen erfordern weiterhin Updates, Benutzerverwaltung oder Konfiguration, egal ob sie als VMs laufen oder "auf Blech". Hinzu kommt jedoch noch die Virtualisierungs-Infrastruktur selbst: Die Hostserver, die Virtualisierungssoftware, das Speichersystem und eine anspruchsvolle Netzwerkanbindung. Das tägliche Operating benötigt Know-how, und an kritischen Stellen brauchen Sie vielleicht externe Unterstützung. Der Ausfall eines VM-Hostservers ist viel kritischer als der eines herkömmlichen Rechners, denn an ihm hängen gleich mehrere wichtige Applikationen.

Daraus erwachsen gleichzeitig Herausforderungen für die IT-Sicherheit. Zweifellos sind viele Mechanismen der

VM-Welt sehr praktisch und zeitsparend. Es fällt etwa sehr leicht, neue Server auf der Basis vordefinierter "Templates" zu erzeugen – mit wenigen Mausklicks und innerhalb weniger Minuten steht neue Rechnerkraft zur Verfügung. Genauso leicht ist es, vorhandene produktive Server zu klonen, um beispielsweise ein lebensnahes Testsystem zu erzeugen oder eine Kopie für den Notfall vorzuhalten.

Was Administratoren hierbei leicht übersehen: Derart vervielfältigte Installationen bergen hohe Sicherheitsrisiken. Der Klon eines Produktivsystems etwa ist genauso sicherheitskritisch wie das Original: Er enthält dieselben Konten und Kennwörter und den sensiblen Datenbestand des Vorbilds. Ein solches Testsystem darf keinesfalls in einem leicht zugänglichen Labor laufen. Ähnliches gilt für VM-Templates, die oft als Installationsgrundlage dienen. Viele Kunden vergessen, dass sie dort etwa administrative Zugangsdaten hinterlegt haben. Gesellt sich dazu die Hektik des Alltags, in der solche VM-Images "mal eben" auf irgendeiner Freigabe im Netz abgelegt werden, wird es Angreifern leichtgemacht. Einfach ausgedrückt: Warum soll ein Angreifer in einen Live-Datenbankserver einbrechen, wenn er ihn einfach und bequem als Datei mit nach Hause nehmen kann?

Sandboxes sind keineswegs immer sicher

Solcherlei administrative Sünden, die schon in einer herkömmlichen Umgebung heikel sind, erzeugen in VM-Landschaften hohes Gefahrenpotenzial. Allzu

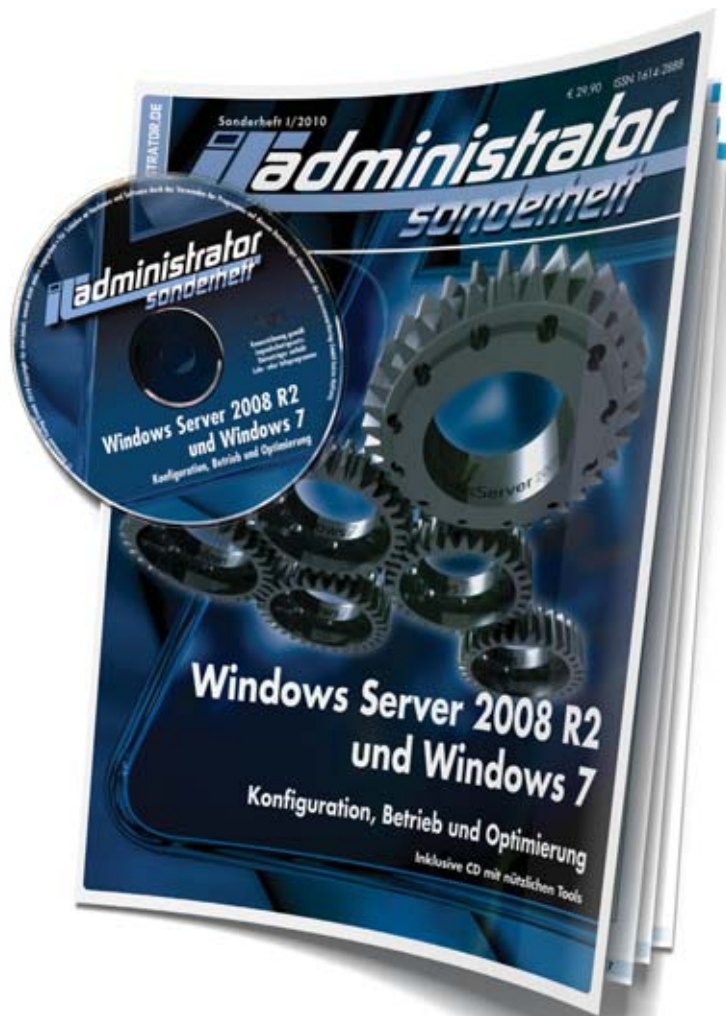
leicht ist es dort, sich auf den Komfort der eingebauten Werkzeuge zu verlassen. So breiten sich leicht knackbare Standard-Kennwörter und unpassend konfigurierte Systeme aus und vergrößern die Angriffsfläche. Wer denkt schon daran, die neue VM, die in der DMZ laufen soll, zu härten und abzusichern, wenn sie per Mausklick eingerichtet wurde?

Das Thema DMZ birgt weitere Risiken. Eine solche demilitarisierte Zone dient meist als Puffer zwischen dem Internet und dem LAN. Applikationen, die dort laufen, stehen unter Beschuss, daher trennt man sie vom internen Netzwerk. Zahlreiche Kunden betreiben ihre DMZ-Server aber auf denselben physischen VM-Hosts wie ihre internen Systeme. Sie nutzen dabei die Netzwerkkonfiguration des Virtualisierungssystems, um die virtuellen Gäste voneinander zu trennen. Glauben wir den Virtualisierungs-Herstellern, so ist das auch sicher, denn angeblich bildet das VM-System "Sandkästen" um die darauf laufenden Server, so dass der Übergriff von einer VM auf eine andere oder gar auf den Host ausgeschlossen sei.

Die Vergangenheit hat aber gezeigt, dass derartige Ausbrüche aus der "Sandbox" keineswegs unmöglich sind. Wie bei jeder Software lassen sich auch hier Schwachstellen ausnutzen. Ein besonders interessanter Angriff nutzte erfolgreich eine Lücke in VMwares VGA-Treiber, um von einer gekaperten VM auf die anderen und letztlich auf den Host zu gelangen – schnell ist so das gesamte Netzwerk kompromittiert. Zwar ist diese Lücke mittlerweile geschlossen, doch sie zeigte deutlich, dass an physischer Netzwerktrennung auch weiterhin kein Weg vorbeiführt.

Der Königsweg kann also nur sein, Systeme aus unterschiedlichen Netzwerkzonen auf separierten physischen Hostservern zu betreiben. Das steigert den Aufwand und die Kosten, ist aber unumgänglich, wollen Sie ein akzeptables

Tolerierbare Ausfallzeit (Beispiel)			
	Klasse 1: < 1 Stunde	Klasse 2: < 4 Stunden	Klasse 3: < 8 Stunden
Exchange		✓	
Dateien	✓		
Data Warehouse			✓
ERP	✓		



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

180 Seiten Praxis-Know-how

rund um das Thema

Windows Server 2008 R2 und Windows 7 + Tools-CD zum Abonnenten-Vorzugspreis* von

nur € 24,90!

*IT-Administrator Abonnenten erhalten das Sonderheft I/2010 für € 24,90.
Nichtabonnenten zahlen € 29,90.

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 Abonummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft I/2010 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft I/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

Geldinstitut: _____

Kto.: _____

BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

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 1010



Sicherheitsniveau erreichen. Ganz nebenbei ermöglicht nur diese Trennung eine wirkungsvolle Netzwerk-Analyse. Die virtuellen Switches moderner VM-Systeme sind zwar sehr leistungsfähig, doch sie lassen sich meist nicht vollständig in Netzwerk-Managementsysteme einbinden. Liefere nun noch der nur virtuell getrennte Traffic verschiedener LAN-Segmente über dieselben physischen Schnittstellen, wären Intrusion Detection oder andere Sicherheitsmechanismen schnell wirkungslos.

Die Verbindung unterschiedlicher Systeme auf demselben Host hat in größeren Unternehmen noch andere Auswirkungen. Oft sind dort unterschiedliche Teams der IT-Abteilung für bestimmte Serverkategorien zuständig, etwa ein Datenbank-Team, ein Mail-Team und eines für den Verzeichnisdienst. Laufen deren Server auf denselben physischen Hosts, ist der administrative Zugriff kaum noch zu trennen: Welche Rolle nimmt hier etwa der Admin des VM-Systems ein?

Live-Migration ist keine Ausfallsicherheit

Gerade beim Aspekt der Ausfallsicherheit bestehen in der Virtualisierung viele Fehleinschätzungen, die im Ergebnis nicht zu einer höheren, sondern zu einer geringeren Betriebssicherheit führen. Das betrifft in erster Linie die Funktion der "Live-Migration", die alle führenden Virtualisierungsanbieter unter verschiedenen Namen (vMotion, XenMotion und so weiter) feilhalten. Sie ermöglicht eine virtuelle Maschine im laufenden Betrieb von einem physischen Hostserver auf einen anderen zu verschieben, ohne dass Benutzerverbindungen abreißen oder die VM pausiert. Anders als viele Administratoren denken, dient dieser Mechanismus praktisch überhaupt nicht der Ausfallsicherheit.

Diese Technik ist nämlich machtlos, wenn einer der Hostserver oder die VM ausgefallen sind. Ganz im Gegenteil funktioniert das Verfahren nur dann, wenn die ge-

samte Umgebung "gesund" ist, denn hinter der Kulisse laufen sehr komplizierte Prozesse ab. Es kann etwa durchaus passieren, dass die Live-Migration fehlschlägt, wenn eine VM stark unter Dampf steht oder wenn das Netzwerk ausgelastet ist. Zur Migration ist es erforderlich, den Arbeitsspeicher der VM in Echtzeit über das LAN von einem auf den anderen Host zu synchronisieren, bis nur noch eine minimale Differenz bleibt. Unter ungünstigen Bedingungen kommt es nie so weit, bevor das Timeout für den Vorgang einsetzt.

Live-Migration kann hingegen bestimmte geplante Downtimes vermeiden, und zwar solche, die durch die Host-Wartung entstehen. Muss der Admin den physischen Server nach einem Update neu starten, so verschiebt er die laufenden VMs auf eine andere Maschine und es

gibt keine Unterbrechung für die Benutzer. Bei Updates der VM-Gäste selbst hilft das nicht, denn ein Reboot des virtuellen Betriebssystems lässt sich per Migration nicht vermeiden. Eigentlich hat das Verschieben auch einen anderen Sinn, nämlich die automatische Lastverteilung. Gehen einem Hostserver die Ressourcen aus, während ein anderer noch Kapazitäten frei hat, ist Live-Migration sehr hilfreich, um jedem virtuellen Server ausreichend Leistung zu verschaffen. Der Pferdefuß: Dieser Grad an Automatisierung erzeugt meist zusätzliche Lizenzkosten, denn Komfort lassen sich alle Hersteller extra bezahlen.

Wer geplante und ungeplante Unterbrechungen seiner Applikationen vermeiden oder zumindest deren Dauer minimieren möchte, wird daher auch

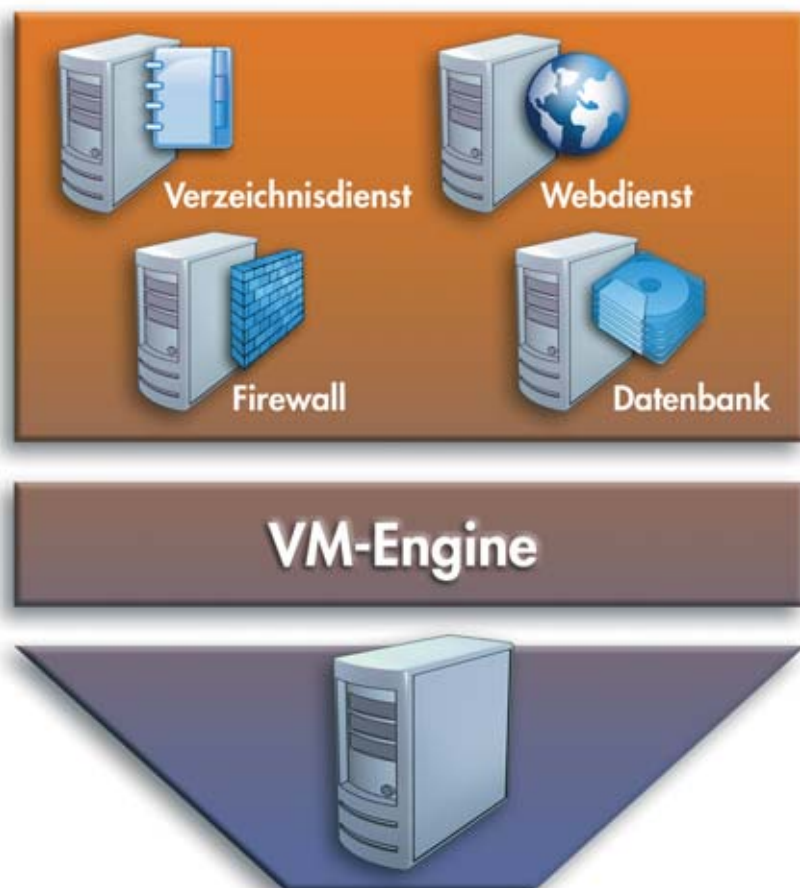


Bild 1: Der Betrieb virtueller Server verschiedener Netzwerkzonen auf demselben VM-Host hebt die Netzwerktrennung auf und macht es Angreifern leicht, von der DMZ ins LAN überzugreifen

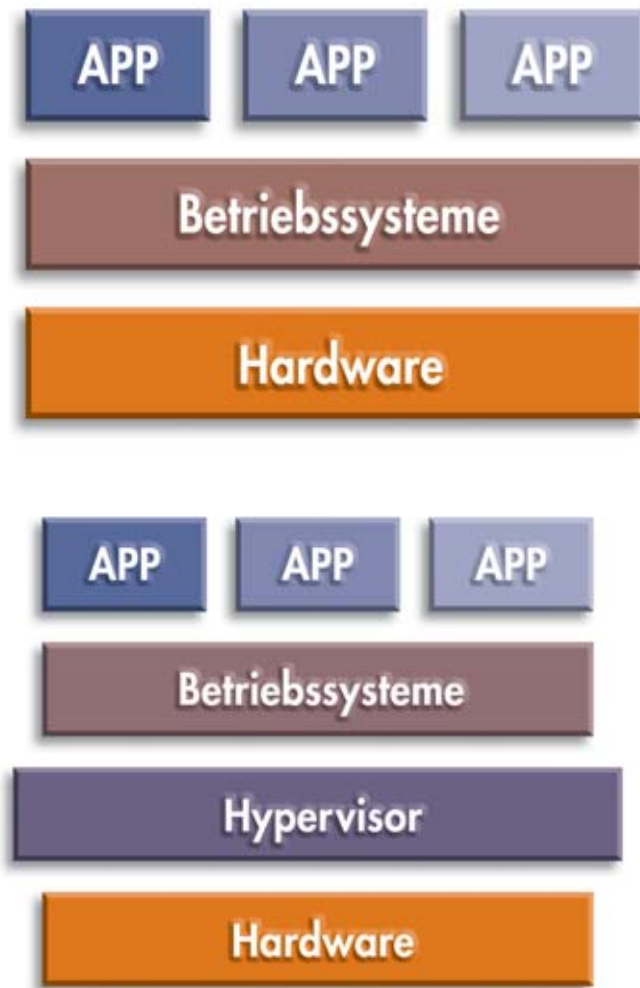


Bild 2: Ein unbemerkt platzierter Hypervisor zwischen Hardware und Betriebssystem erlaubt die volle Kontrolle über alle Vorgänge

weiterhin auf klassische High-Availability-Methoden wie das Clustering setzen. Hierzu lassen sich zwei (oder mehr) VMs zu einem Cluster zusammenfügen, der unabhängig von der Virtualisierung den Zustand der Applikation beobachtet und nötigenfalls einen Neustart auf einer der beteiligten VMs ausführt.

Auf dieser Ebene bieten VMware und Citrix eine interessante, noch recht neue Funktion an: Die Live-Spiegelung einer virtuellen Maschine von einem Host auf einen anderen. Das Versprechen lautet, dass alle Instruktionen, die die "aktive" VM ausführt, zeitgleich auf einer Kopie der VM ebenfalls ablaufen, welche im Netz nicht sichtbar ist. Auf diese Weise sind beide virtuellen Server stets im selben Zu-

stand. Sollte das aktive System ausfallen, so kann der "Spiegel" nahtlos übernehmen und steht mit genau derselben Identität und exakt demselben Datenbestand zur Verfügung.

Leider hat auch dieser Ansatz seine Einschränkungen. Prinzipbedingt eignet sich das Verfahren nur für virtuelle Server mit einer einzigen virtuellen CPU. In Multiprozessorsystemen sorgen nämlich aufwändige Mechanismen für eine Verteilung der Aufgaben auf die Rechenkern. Dies auf einen anderen Host zu synchronisieren, würde derart erhebliche Eingriffe

erfordern, dass die Performance in den Keller ginge. Gerade solche Server,

für die hohe Ausfallsicherheit relevant ist, stehen aber oft unter hoher Last, die von Single-CPU-Servern nicht zu stemmen ist. Solche Systeme eignen sich für diese Technik also nicht. Hinzu kommt, dass auch der VM-Spiegel keine Null-Unterbrechung ermöglicht, denn nicht zuletzt muss die Netzwerk-Infrastruktur darauf reagieren, dass das System plötzlich auf ganz anderen LAN-Ports aktiv ist.

Nicht umsonst positionieren VMware und Citrix ihre Spiegel-Features auch eher für kleinere, aber gleichwohl unternehmenswichtige Applikationen, für die es herstellerseitig keine anderen Verfügbarkeitsmechanismen gibt. Schon aus Supportgründen sind jedoch die Methoden zu bevorzugen, die ein Applikationshersteller selbst vorsieht.

Risiko Snapshots

Die wohl gefährlichste Fallgrube lauert unter einer sehr beliebten VM-Funktion: den Snapshots. Alle Hersteller erlauben es, den momentanen Zustand einer virtuellen Maschine einzufrieren und quasi als Sofort-Image abzulegen. Der Administrator kann damit jederzeit auf diesen historischen Zustand zurückspringen. Viele IT-Abteilungen nutzen dies als Element ihrer Recovery-Strategie, um etwa einen Patchfehler ungeschehen zu machen.

SEMINAR MARKT

**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



Allerdings kommen längst nicht alle Applikationen damit klar, wenn sie sich plötzlich in der Vergangenheit wiederfinden. Das betrifft vor allem komplexe verteilte Systeme wie Active Directory (AD) und Exchange, aber auch viele andere Anwendungen. So sind etwa die AD-Domänencontroller jederzeit informiert, auf welchem Stand sich ihre Partner gerade befinden. Meldet sich ein solcher Server nach der Wiederherstellung eines VM-Snapshots plötzlich mit einem veralteten Datenbestand, so kann AD dies nicht ausgleichen. In der Folge schaltet der betroffene Server seine AD-Dienste ab und verschwindet aus der Replikation. Ein scheinbares Recovery würde so also erst zu einem gravierenden Ausfall führen.

Angriffe gegen virtualisierte Server

Risiken entstehen nicht nur aus allzu sorglosem Umgang mit den Funktionen des Virtualisierungssystems. Auch die Virtualisierung selbst erzeugt Bedrohungen, die in klassisch-physischen Umgebungen unbekannt sind. Zwei Beispiele machen dies deutlich, die zumindest bislang glücklicherweise keine kriminelle Anwendung gefunden haben – oder wenigstens ist nichts darüber bekannt.

Die Angriffe machen sich den Umstand zunutze, dass ein virtualisiertes System vollständig der Kontrolle durch den Hypervisor unterliegt. Er liegt als Softwareschicht zwischen der physischen Hardware und den virtuellen Betriebssystemen. Jeden Zugriffsversuch einer VM auf Hardwarekomponenten fängt der Hypervisor ab und ersetzt ihn durch seine Emulations- und Abstraktionsfunktionen. Das geht so lange gut, wie der Hypervisor dem Betriebssystem nichts vorgaukelt, was gar nicht der Fall ist, oder ihm etwas verbirgt. Vereinfacht gesagt, setzt Virtualisierung blindes Vertrauen in den Hypervisor voraus.

Der SubVirt-Angriff

Einen Angriff auf dieses Vertrauen hat Microsoft Research als Proof of Concept bereits 2005 durchgeführt. Wo der Hypervisor normalerweise absichtlich zwischen Hardware und Betriebssystem geschoben wird, um eben bewusst eine VM-Umgebung aufzubauen, führt der "SubVirt" genannte Angriff dies in einem laufenden System ohne Wissen des Anwenders durch. SubVirt installiert einen Hypervisor und biegt die Startfunktionen des Systems so um, dass beim nächsten Bootvorgang nicht das legitime Betriebssystem die Steuerung übernimmt, sondern der Hypervisor selbst. Damit hat er alle Vorgänge des nun virtuell laufenden Systems unter Kontrolle und kann beispielsweise von diesem unbemerkt Daten kopieren oder Kennwörter an Kriminelle schicken.

SubVirt verändert dazu den Datenbestand auf der Festplatte, weil es seine eigenen Komponenten installiert. Das ehemals physische Betriebssystem kann diese Daten nicht sehen, weil SubVirt sie wie ein Rootkit vor ihm verbirgt. Eine Offline-Analyse der Festplatte könnte die Manipulation allerdings sichtbar machen – ob das aber rechtzeitig vor einem Schaden geschieht, ist letztendlich Zufall.

Der Blue Pill-Angriff – Datenklau per Zusatzschicht

Einen Schritt weiter geht "Blue Pill" von der Sicherheitsspezialistin Joanna Rutkowska, vorgestellt Ende 2006. Blue Pill nutzt die Virtualisierungsfunktionen moderner Prozessoren, die AMD damals gerade in den Markt gebracht hatte. Vereinfacht gesagt haben solche Prozessoren einen Hypervisor-Modus, der eine Kontrollschicht unterhalb der klassischen Betriebssysteme erzeugt und so den besonders effizienten Betrieb von Virtualisierungssystemen ermöglicht. Rutkowska aktiviert auf einem angegriffenen System diesen Modus und schleust einen "ultradünnen" Hypervisor ins System ein, der im laufenden Betrieb die

Kontrolle übernimmt. Anders als SubVirt muss Blue Pill dazu nichts auf der Festplatte installieren, sondern läuft ausschließlich im Speicher.

Das so angegriffene Betriebssystem hat keine verlässliche Möglichkeit, diesen Wechsel der Betriebsart festzustellen, denn der Prozessor sieht keine Funktion vor, die darüber Auskunft gibt. Aus Sicht des ehemals legitimen Systems gibt es keine Veränderung zu früher, denn alle Systemzugriffe scheinen zu funktionieren. Tatsächlich aber hat Blue Pill nun die Kontrolle über alle Vorgänge übernommen und kann unbemerkt seine Schadfunktionen ausüben. Im Unterschied zu SubVirt überlebt Blue Pill keinen Reboot der physischen Maschine. Es hat aber Methoden, um solch einen Neustart zu vermeiden: Fordert der Admin innerhalb des Betriebssystems einen Neustart an, so simuliert Blue Pill diesen einfach – ganz so, wie man eine "normale" VM neu startet. Nur der Hardware-Netzschalter kann dem Treiben ein Ende setzen.

Fazit

Mit der Virtualisierung ist es wie mit jedem anderen komplexen System: Den vielen Vorteilen stehen große Gefahren gegenüber. Noch mehr als in der klassischen IT ist es in virtuellen Umgebungen notwendig, dass die IT-Verantwortlichen gut planen und mit großer Sorgfalt arbeiten. Neben der erhöhten Umsicht beim Betrieb virtueller Server gilt es aber auch, die neuartigen Risiken solcher Umgebungen im Blick zu behalten und einzudämmen.

Mit der zunehmenden Verbreitung der Technik werden Angriffe, die bislang meist eher akademischen Charakter haben, aus den Showrooms der Security-Konferenzen schnell in die "freie Wildbahn" übertreten und IT-Abteilungen vor enorme Herausforderungen stellen. (jp)

Nils Kaczinski ist Microsoft-MVP und leitet das Consulting bei der WITstor in Hannover.



Virtualisierung von Windows-Domänencontrollern (2)

Wege zurück

von Florian Frommherz und Ulf B. Simon-Weidner

Durch Virtualisierung ist der Administrator heutzutage unabhängiger von der Hardware, kann die Infrastruktur verfügbarer gestalten und ist für einen Recovery-Fall bestens gerüstet. Soll jedoch ein Windows-Domänencontroller virtuell betrieben werden, benötigt der Administrator tiefgehendes Know-how des Systems und des Active Directory. Im zweiten Teil unserer Workshopserie zur Virtualisierung von Domänencontrollern erfahren Sie, wie Sie Ihre Änderungen wieder rückgängig machen können. Dabei gehen wir auf USN-Rollbacks und Snapshots ein.

Damit unterschiedliche Domänencontroller feststellen können, welche Änderungen sie von anderen Domänencontrollern replizieren müssen, kommen sogenannte "Update Sequence Numbers" (USN) zum Einsatz. Diese werden bei jeder Änderung, die ein Domänencontroller in sein lokales Active Directory schreibt, erhöht. Die USN ist also lokal an jedem Domänencontroller unterschiedlich.

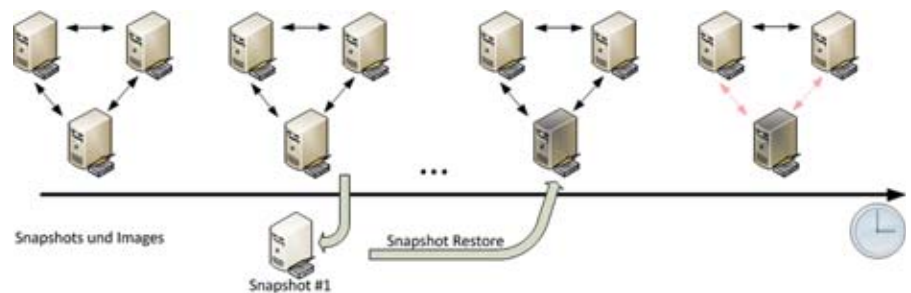


Bild 1: Schema einer möglichen Ursache eines USN-Rollbacks

USN-Rollbacks vermeiden

Wenn ein DC repliziert, merkt er sich die zuletzt replizierte USN seines Replikationspartners (im sogenannten High Watermark Table). Bei dem nächsten Replikationszyklus fragt der Domänencontroller dann seinen Replikationspartner nach allen Änderungen, die nach derjenigen USN erfolgt sind, die er zuletzt repliziert hatte. Erhält er nun diese Änderungen, prüft der DC anhand einer Versionsnummer und gegebenenfalls des Zeitstempels (AD erlaubt ja auch Änderungen auf verschiedenen DCs, wobei unter Umständen Konflikte entstehen), ob er die Änderung annimmt und schreibt diese in seine Datenbank. Dabei erzeugt er eine eigene, lokale USN, die wiederum seinen Replikationspartnern hilft, die letzten Änderungen anzufordern.

Das Zurücksichern von Domänencontrollern mit nicht supporteten Methoden

wie Imagebackups oder Snapshots führt genau an dieser Stelle zu massiven Problemen. Anhand eines Beispiels wird die Problematik deutlich: DC-A und DC-B sind in der gleichen Domäne und replizieren deren Inhalte. Der USN-Stand der letzten Änderung liegt für DC-A bei 1734, für DC-B bei 975. Die beiden Domänencontroller kennen ihren jeweilig eigenen Stand sowie den USN-Stand des Partners: DC-A {1734, 975}, DC-B {975, 1734}. Der aktuelle Stand des Betriebssystems und aller Daten auf DC-A wird mit einem Image oder Snapshot der Festplatte festgehalten. In den folgenden Tagen nimmt ein Administrator mehrere Änderungen an der von DC-A und DC-B geteilten Partition vor, so dass mehrere Erhöhungen der USNs auf beiden Domänencontrollern und daraus resultierend mehrere Replikationsvorgänge stattfinden. Die aktuellen USN-Stände sind nun DC-A {1809, 992}, DC-B {992, 1809}.

Aufgrund eines Defektes fährt das AD-Team DC-A herunter, tauscht die Hardware aus und setzt ihn mit dem festgehaltenen Image neu auf (oder schlimmer, jemand hat eine Änderung gemacht und will sie über einen Snapshot wieder rückgängig machen). Die beiden DCs haben nun folgende USN-Stände: DC-A {1734, 975} und DC-B {992, 1809}. DC-A besitzt offensichtlich den per Image gesicherten, alten Stand seines High Watermark Tables sowie der lokalen USNs. Dies ist der Zeitpunkt des sogenannten "USN-Rollback". Die zuvor unter den DCs bekannte USN von DC-A wurde durch eine nicht supportete Backuplösung wiederhergestellt – und die USN illegal auf einen alten Stand zurückgerollt. Änderungen an der Partition führen zur Erhöhung der USN auf DC-A.

Wenn jetzt DC-B bei der nächsten Replikation nach den Änderungen fragt,

möchte er alle Änderungen seit USN 1809 von DC-A. Da dieser aber erst bei USN 1734 ist, gibt es keine Änderungen zu replizieren. DC-B wird somit die vorgenommenen Anpassungen von DC-A nicht aktualisieren, sodass das Verzeichnis in einem inkonsistenten Zustand fährt. DCs sind per Voreinstellung so konfiguriert, dass sie die Durchführung der Replikation mit potentiellen Opfern von USN-Rollbacks verweigern. Wäre dies nicht der Fall, würde DC-A verschiedene Änderungen schreiben, bis er den Stand erreicht, den DC-B erwartet, um wieder zu replizieren. DC-A hat hiermit Änderungen den anderen DCs vorenthalten, nähme aber dann plötzlich wieder an der Replikation für weitere Objekte teil. Daher ist es auch wichtig, dass die Replikation ausgesetzt ist, bis ein Administrator den Fehler behoben hat.

Eine weitere Folge ist eine Meldung in der Ereignisanzeige des Quelldomänencontrollers mit der ID 2095 und dem Typ "NTDS Replication". Je schneller USN-Rollbacks erkannt werden, desto einfacher ist es, inkonsistente "lingering objects", die nicht repliziert werden, zu minimieren und beheben.

Das Zurückspielen von Images ist nicht die einzige Methode, sein Verzeichnis mit einem USN-Rollback in Gefahr zu bringen. Virtualisierungstechnologien wie das Erstellen und spätere Zurückrollen von Snapshots sind eine ähnlich sichere Methode, das Active Directory aus dem Tritt zu bringen. Verwirft ein Administrator den aktuellen Stand des Domänencontrollers und reaktiviert einen veralteten Stand, ist der alte USN-Stand des DCs wieder aktiv.

Ebenfalls mit Vorsicht zu genießen sind Undo-Disks für virtuelle Maschinen. Undo-Disks finden Verwendung, wenn Daten von virtuellen Festplatten ab einem gewünschten Zeitpunkt in eine gesonderte virtuelle Festplatte geschrieben werden sollen. Das ermöglicht Administratoren ebenso die Möglichkeit, zu einem früheren Datenzustand zurückzuspringen. Images, Snapshots und Undo-Disks sollten nur dann eingesetzt werden, wenn der Forest aus einer Domäne mit nur einem Domänencontroller besteht. Da dies, wenn sich Administratoren an Best Practices halten, nur selten auftritt, ist auch die Verwendung solcher Sicherungen nicht notwendig.



Dieser Beitrag ist eine Vorabveröffentlichung aus dem im Oktober 2010 erscheinenden IT-Administrator-Sonderheft "Active Directory". Als ausgewiesene, langjährige Experten für den Windows-Verzeichnisdienst stellen die Autoren Ulf B. Simon-Weidner und Florian Frommherz ihr Wissen den Lesern zur Verfügung. Neben der Erläuterung entscheidender Me-

chanismen im Verzeich-

dienst, die zum grundlegenden Verständnis der Funktionsweise beitragen, bietet das Sonderheft zahlreiche praxisnahe Anleitungen für Administratoren kleiner und großer Active Directory-Infrastrukturen.

So zeigen die Autoren etwa auf, wie Administratoren die Sicherheit im Active Directory gewährleisten, widmen sich mit Beiträgen zur Schemaerweiterung, dem AD-Scripting, Backup & Recovery und vielen weiteren Themen der täglichen Administration und bieten in der Rubrik "Optimierung und Troubleshooting" echtes Insider-Know-how.



Ulf B. Simon-Weidner



Florian Frommherz

Als Abonnent können Sie das Sonderheft schon jetzt zum Vorzugspreis von 24,90 Euro bestellen (Nicht-Abonnenten erhalten das Sonderheft zum Preis von 29,90 Euro. Die Preise verstehen sich jeweils inklusive Versand und 7 Prozent MwSt.).

**Jetzt Vorbestellen:
Sonderheft "Active Directory"**

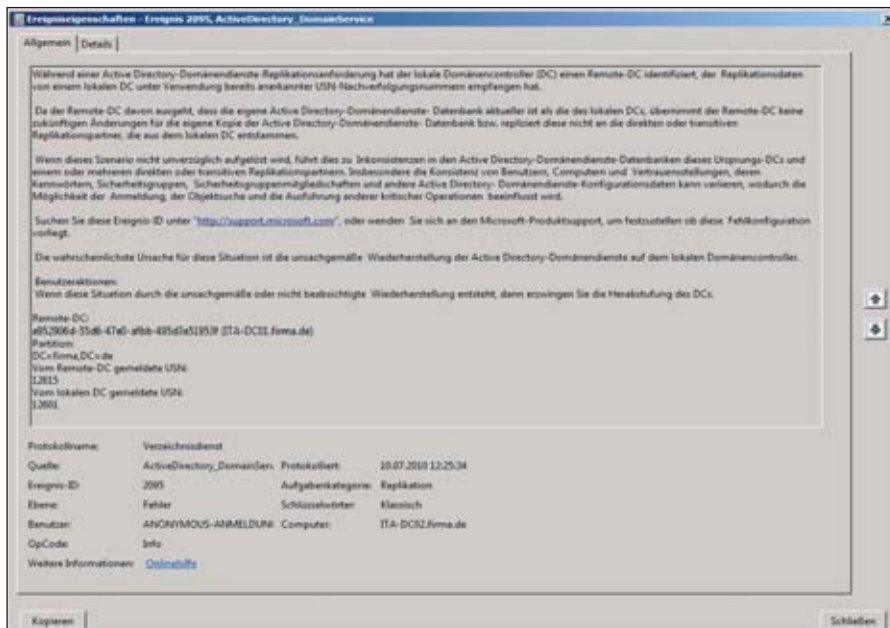


Bild 2: Das Event 2095 zeigt an, dass ein USN-Rollback stattgefunden hat, weil ein Domänencontroller unsachgemäß rückgesichert wurde. Jetzt hilft nur noch ein Herabstufen und Re-Promoten des DCs.

Der Schlüssel für eine sichere- virtuelle Infrastruktur für Domänencontroller liegt darin, diese Technologien auszuschließen oder sicherzustellen, dass nur Administratoren entsprechende Möglichkeiten haben, denen das Problem bekannt ist. Ein häufig genannter Weg, um Snapshots zu vermeiden, ist es sogenannte "linked Volumes" zu verwenden, also keine virtuellen Festplatten, sondern tatsächliche Vo-

lumes auf dem Virtualisierungshost, die an den Gast-DC durchgereicht werden. Hier stehen die Snapshot-Möglichkeiten nicht zur Verfügung.

Da nun die nicht unterstützten Sicherungsmethoden und die damit verbundenen Gefahren bekannt sind, drängt sich die Frage nach einer Liste unterstützter Backupslösungen auf. Microsoft selbst führt keine Aufstellung, nennt aber das Kriterium, das eine Backupslösung zu einer "unterstützten" macht. Das Geheimnis liegt in der "InvocationID", die jeder Domänencontroller trägt. Die InvocationID ist ein sogenannter Global Unique Identifier (GUID), die den Domänencontroller eindeutig identifiziert (auch nach der Umbenennung). Unterstützte Backupslösungen markieren nach einer erfolgreichen Wiederherstellung der AD-Datenbank den DC, so dass er die InvocationID beim nächsten Start ändert. Damit verhält sich der DC dann wie ein "Neuer" und handelt die Replikation mit USN und geänderter InvocationID neu aus. Sollte es notwendig sein, einen Snapshot zurückzuspielen, muss auch der Mechanismus zur Änderung der InvocationID angewandt werden.

Snapshots ohne Probleme zurückspielen

Um einen Domänencontroller über eine imagebasierte Sicherung oder einen Snapshot zurückzuspielen, können Sie die InvocationID auch "manuell" ändern. Um festzustellen, welche USNs von welchem DC zuletzt repliziert wurden (High Watermark Table oder Up-To-Date-Vector), verwenden Sie den Befehl `Repadmin /showutdvec`. Besonders interessant dabei ist, dass Sie mit dem zusätzlichen Parameter `/nocache` auch die eigene InvocationID sowie die der Replikationspartner erhalten:

`Repadmin /showutdvec localhost dc=firma,dc=de /nocache`

Der folgende Prozess sollte nur im absoluten Notfall angewendet werden, im Normalfall sollten Domänencontroller lieber durch Neuinstallation und Replikation der letzten Daten von benachbarten Domänencontrollern der gleichen Domäne hergestellt werden. Wenn aber ein Snapshot zurückgespielt wurde (oder eine imagebasierte Sicherung), gehen Sie wie folgt vor:

1. Deaktivieren Sie die Netzwerkverbindung unmittelbar vor, während oder nach der Rücksicherung, aber auf alle Fälle bevor der rückgesicherte DC das erste Mal startet.
2. Booten Sie in den Verzeichnisdienstwiederherstellungsmodus (Directory Services Restore Mode oder DSRM)
3. Wenn Sie den Dateireplikationsdienst NTFRS für Sysvol verwenden (standardmäßig vor Windows Server 2008 R2), halten Sie den Dienst an. Dann navigieren Sie in den Registrierungsschlüssel "HKLM \ System \ CurrentControlSet \ Services \ NtFrs \ Parameters \ Backup/Restore \ Process names". Dort ändern oder erstellen Sie den Wert "BurFlags" (Format DWORD) und setzen ihn auf "D2" (das ist für die

Kostenlos für
IT-Administrator-Abonnenten

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 – Partnervortrag:

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 – Partnervortrag:

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: Expertech Training Center,
Wredestraße 11, 80335 München

Uhrzeit: 10.00 bis 17.00 Uhr

Teilnahmegebühren:

Für IT-Administrator-Abonnenten kostenlos.

Trainings-Partner:



EXPERTech

Anmeldeschluss: 10. November 2010

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

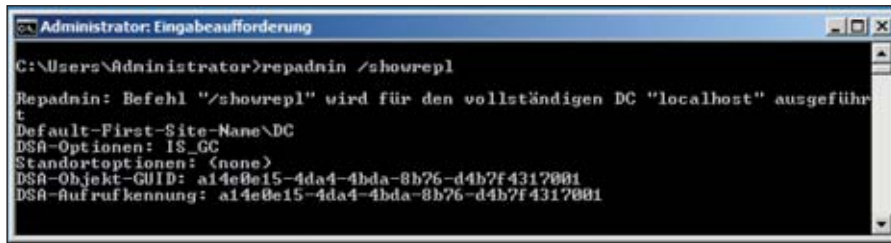


Bild 3: Die InvocationID identifiziert den Domänencontroller eindeutig

Wiederherstellung der Sysvol-Replikation notwendig).

4. In der Registry setzen Sie nun unter "HKLM \ System \ CurrentControlSet \ Services \ NTDS \ Parameters" den Schlüssel "Database restored from backup" auf "1" (sollte er nicht vorhanden sein, erstellen Sie ihn als DWORD). Dies sagt dem DC, dass er nach dem nächsten Start eine neue InvocationID erzeugen soll.
5. Wenn an dieser Stelle auch der Schlüssel "DSA Previous Restore Count" existiert, merken Sie sich den Wert. Er sollte sich nach dem Reboot um 1 erhöhen.
6. Hängen Sie jetzt den Server wieder an das Netzwerk und starten ihn (im normalen Modus) neu.
7. Verifizieren Sie anschließend, dass eine neue InvocationID erzeugt wurde und der Registrierungsschlüssel "DSA Previous Restore Count" um 1 erhöht ist. In der Ereignisanzeige sehen Sie jetzt auch das Event 1109, das anzeigt, dass das AD von einer Datensicherung wiederhergestellt wurde.

Durch diesen Prozess erhält der DC eine neue InvocationID und verhält sich wie ein frisch installierter DC, das heißt, er versucht alle Daten im Verzeichnis erneut abzugleichen und verlässt sich nicht auf die Daten, die er bereits hat.

Sollten Sie Snapshots oder imagebasiertes Backup der virtuellen Festplatten verwenden (müssen), so ist es empfehlenswert, den Registrierungsschlüssel vor der Datensicherung zu setzen und nach der Sicherung wieder zu entfernen. Damit wird sichergestellt, dass eine Rücksicherung niemals zu einem USN-Rollback führt. Den Registrierungsschlüssel immer

gesetzt zu lassen, wird jedoch nicht empfohlen, da dann die Invocation ID bei jedem Neustart geändert wird, was zu Netzwerkproblemen und langfristigen Problemen im AD führen kann.

Einsatzmöglichkeiten virtualisierter DCs

Eingangs nannten wir einige Vorteile der Virtualisierung bei Domänencontrollern. Aber wenn Sie sich tiefergehend mit dem Thema beschäftigen, dann sind virtualisierte DCs auch optimal für die folgenden, beispielhaften Einsatzzwecke:

- Klonen der virtuellen Maschinen durch einfaches Kopieren erlaubt dem Administrator, eine produktionsnahe Testumgebung zu realisieren (Achtung: darauf achten, dass das Netzwerk abgeschottet ist).
- Für kritische Updates, wie Schema-Updates, können zusätzliche virtualisierte DCs eingesetzt werden (etwa ein bis zwei DCs pro Domäne), die sich vorübergehend abschotten lassen. Die Schema-Updates können dann dort einge spielt und überprüft werden. Und die Replikation mit dem restlichen Netz-

werk wird erst wieder erlaubt, wenn das Update erfolgreich war.

- Dedizierte Domänencontroller in Außenstellen könnten auf einem virtualisierten Server laufen. Im Allgemeinen, vor allem in größeren Umgebungen, sollten Sie Infrastrukturdienste wie AD, DNS und so weiter von Anwendungs- oder Dateiservern trennen (da diese auch häufig von verschiedenen Personen administriert werden und damit man beim Wiederherstellen von DCs nicht Rücksicht auf "fremde Daten" nehmen muss). Die Virtualisierung vereinfacht auch dies.

Es gibt unzählige Einsatzzwecke für virtuelle Domänencontroller. Wenn damit verantwortlich umgegangen wird, Single Points of Failure vermieden werden, die USN-Rollback-Problematik bekannt ist und die Zeit-Infrastruktur entsprechend aufgebaut ist, gibt es keinen Grund, diese Vorteile nicht zu nutzen. (jp) 

Florian Frommherz ist MVP für Gruppenrichtlinien und arbeitet als Systems Engineer. Sie können seinen Blog unter <http://frickelsoft.net/blog> besuchen.

Ulf B. Simon-Weidner ist MVP für Windows Server Directory Services und arbeitet als Consultant und Trainer. Sein Weblog finden Sie unter <http://msmvps.com/ulfbjsimonweidner>.

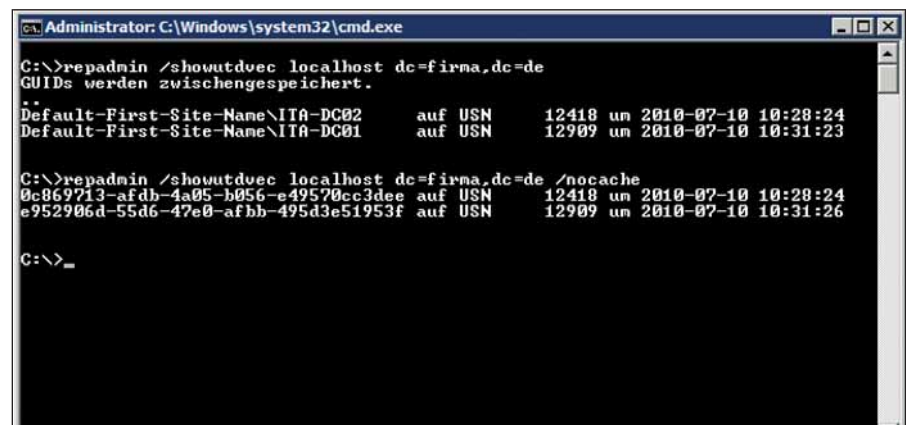


Bild 4: Vor dem Ändern der InvocationID sollte der Administrator diese notieren, was auch von einem Replikationspartner aus erfolgen kann



Microsoft Exchange

Datenbankwartung steuern

von Robert Lindermeier

Exchange-Datenbanken müssen regelmäßig einer Wartung unterzogen werden, damit beispielsweise die abgelaufenen Elemente aus der Datenbank verschwinden und die aktiven Inhalte für einen schnelleren Zugriff in eine sinnvolle Reihenfolge gebracht werden. Dieser Vorgang ist den meisten Administratoren als Online-Defragmentierung bekannt. Die gelöschten Datenbankseiten werden dann als freier Bereich gekennzeichnet, da eine Freigabe des übrigen Speicherplatzes innerhalb der Datenbank zurück an das Betriebssystem nur im Rahmen einer Offline-Defragmentierung mittels ESEUTIL – wir berichteten in einem früheren Workshop – möglich wird. In diesem Zusammenhang werden desweiteren noch folgende Prozesse an der Datenbank abgearbeitet. Die wichtigsten sind:

- Säuberung der Indizes
- Wartung der Tombstones (Dauerhaftes Entfernen sämtlicher Nachrichten oder Postfächer, die die konfigurierte Aufbewahrungsdauer überschritten haben)
- Säuberung des Dumpster, Second Level Trash
- Verfallszeiten von Einträgen in Öffentlichen Ordnern abarbeiten.
- Verfallszeiten von gelöschten Öffentlichen Ordnern bearbeiten.
- Überprüfen des Active Directory, um zu ermitteln, ob gelöschte Postfächer vorhanden sind und deren Aufräumen.

Ohne weitere Eingriffe läuft dieser Maintenance-Prozess zwischen 01:00 und 05:00 Uhr ab. Sollte jedoch das Backup in dieser Zeit greifen, so ist es ratsam, die Termine entsprechend anzupassen. Der Grund: Das Online-Defrag wird unmittelbar gestoppt beziehungsweise beendet, wenn auf einer Datenbank ein Backup

gestartet wird oder noch läuft. Startet an einer Exchange Server 2003-Datenbank die Sicherung, unterbricht diese die Wartung aller anderen Datenbanken der Speichergruppe. Ist die Sicherung dabei vor Ablauf des Zeitfensters abgeschlossen, wird die Wartung neu gestartet.

Wartungszeiten festlegen

Befinden sich zwei oder mehr Datenbanken in einer einzigen Speichergruppe, wird im Fall einer Sicherung einer der Datenbanken die Onlinedefragmentierung dieser aktuell zu sichernden Datenbank abgebrochen, während die Wartung auf den anderen weiterläuft. Deshalb sollten Sie als Administrator entsprechend die Zeiten anpassen, um nicht permanent den Abbruch des Online-Defrag zu bewirken – was sich letztlich auch auf die Performance auswirken könnte. Hier ist es hilfreich, sich einen Plan aufzustellen, wann welche Datenbank gesichert wird und wann die Online-Wartung anzusetzen ist. Das Ergebnis des Online-Defrag können Sie mittels der Event-Ids 700 bis 704 nachverfolgen:

- 700 == Online defragmentation is beginning a full pass on database: Die Online-Defragmentierung wird gestartet.
- 701 == Online defragmentation has completed a full pass on database: Die Online-Defragmentierung wurde erfolgreich innerhalb des Zeitfensters abgeschlossen.
- 702 == Online defragmentation is resuming its pass on database: Die vorherige Online-Defragmentierung wurde unterbrochen, bevor sie vollständig beendet werden konnte.
- 703 == Online defragmentation has completed the resumed pass on database: Die unterbrochene Online-Defragmentierung wurde fortgesetzt und erfolgreich beendet.

- 704 == Online defragmentation of database 'XX' was interrupted and terminated: Die Online-Defragmentierung wurde abgebrochen, da sie aus dem Zeitfenster gelaufen ist oder ein Backup gestartet wurde.

Angepasst wird der Zeitplan beim Exchange Server 2003 über die Eigenschaften des jeweiligen Mailbox Stores beziehungsweise Public Stores, er kann aber auch über eine zentrale System-Richtlinie einheitlich für alle Stores definiert werden. Um die Online-Datenbankwartung für Exchange Server 2000/2003 einzustellen, öffnen Sie Exchange System Manager und erweitern Sie die Punkte "Serverobjekt / Speichergruppe". Klicken Sie hier auf die Eigenschaften des gewünschten Informationsspeichers und aktivieren Sie den Punkt "Register Datenbank". Wählen Sie nun das Wartungsintervall aus der Dropdown-Liste aus oder definieren Sie es nach Ihren Wünschen.

Die Online-Datenbankwartung für Exchange Server 2007 stellen Sie dagegen ein, indem Sie die Exchange-Verwaltungskonsole öffnen, den Punkt "Serverkonfiguration" erweitern und den zu konfigurierenden Server auswählen. Erweitern Sie die gewünschte Speichergruppe und öffnen Sie die Eigenschaften des Informationsspeichers. Aktivieren Sie hier das Register "Allgemein" und wählen Sie das Wartungsintervall aus der Dropdown-Liste aus. Bei Exchange Server 2010 wird der Zeitplan schließlich über "Organisationskonfiguration / Postfach / Datenbankverwaltung" bei den Eigenschaften der Postfachspeicher definiert. Hier stellen Sie im Register "Wartung" den Wartungszeitplan ein. Damit wartet auch der Exchange Server 2010 nach Ihren zeitlichen Vorgaben. (dr)





Load Balancing für Exchange Lasten sicher verteilen

von Thomas Joos



Quelle: Orlando Fiorin Resu - Fotolia.com

Unternehmen, die auf Exchange setzen und eine hochverfügbare Server-Umgebung betreiben wollen, erhalten mit den Cluster-Möglichkeiten der Postfachserver-Rolle eine optimale Handhabe, um die Groupware im Bereich des Postfachzugriffs ausfallsicher zu konfigurieren.

Wie sieht es aber auf Seite des Client-Zugriffs für Clientzugriffserver in Exchange Server 2007/2010 oder Front-End-Server in Exchange Server 2003 aus? IT-Administrator hat sich die Möglichkeiten genauer angesehen, die sich mit den Bordmitteln von Exchange Server 2003 bis 2010 für die Ausfallsicherheit von Clientzugriffservern umsetzen lassen.

Sobald Sie einen Serverdienst auf mehrere Server verteilen können, zum Beispiel bei Clientzugriffservern, macht ein NLB-Cluster mehr Sinn als ein Failover-Cluster. Windows Server 2003, 2008 sowie Windows Server 2008 R2 bringen alles zur Erstellung von Load Balancing-Clustern mit. Im Gegensatz zur Failover-Cluster-Funktionalität steht Network Load Balancing (NLB) in Windows Server auch in den Standard-Editionen zur Verfügung. Das Feature lässt sich dabei leicht mit Exchange nutzen. Generell ist dabei unerheblich, ob sich Anwender über den ersten oder zweiten Clientzugriffserver verbinden. Wichtig ist nur, dass sie Zugang zu ihrem Postfach erhalten.

Cluster versus Load Balancing

Während die Aufgabe eines Clusters darin besteht, eine Serverlösung – etwa einen Datenbankserver oder einen Exchange-Postfachserver – vor dem Ausfall zu sichern, ist ein Loadbalance-Verbund grundsätzlich etwas anderes: Load Balancing kann mehrere Server miteinander verbinden, ohne dass ein gemeinsamer Datenträger vorhanden sein muss. Da sol-

che Server meistens für die Verbindung von Benutzern dienen, nicht aber der Speicherung von Daten, können Unternehmen mehrere solche Clientzugriffspunkte zusammenfassen und unter einem zentralen Namen zur Verfügung stellen. Ein solcher Verbund nimmt Anfragen der Nutzer entgegen und teilt den Anwendern einen der Server im Verbund zu. Auf diese Weise teilt sich die Last auf und der Ausfall eines einzelnen Servers lässt sich leichter kompensieren.

Bei NLB bauen die Clients eine Verbindung zum NLB-Cluster auf, der wie ein Failover-Cluster einen eigenen Namen und eine eigene IP-Adresse besitzt. Anschließend lenkt der Cluster die entsprechende Anforderung der Anwender an einen Server im Verbund. Dabei lassen sich bis zu 32 Server zu einem Load Balancing-Cluster zusammenfügen, der von außen über eine gemeinsame virtuelle IP-Adresse zur Verfügung steht und somit wie ein einzelner Computer erscheint. Sie können dabei das Lastenausgleichsgewicht der einzelnen Hosts im Cluster für jeden einzelnen Server konfigurieren. Fällt ein Host des Clusters aus, übernehmen

die anderen Server im Cluster die Zugriffe der Anwender. Daten werden allerdings nicht ausgetauscht oder über einen gemeinsamen Datenträger zur Verfügung gestellt. Dies ist Sache eines Failover-Clus-

Sie können auch Clientzugriffserver über Hyper-V und NLB clustern, müssen bei der Konfiguration jedoch einiges beachten. Erstellen Sie einen NLB-Cluster, verwenden Sie eine MAC-Adresse. In einigen Fällen ändert Windows diese MAC-Adresse in Hyper-V ab. Bei der Erstellung des Clusters bieten sich daher Unicast oder Multicast an. Bei **Unicast** erhält jeder Server im NLB-Cluster die gleiche MAC-Adresse. Die vorhandene MAC-Adresse der Netzwerkkarten entfernt der Assistent dabei. Setzen Sie **Multicast** ein, fügt der Assistent den MAC-Adressen der Netzwerkkarten eine zusätzliche MAC-Adresse hinzu. Die Clients können dann über ihre alte MAC-Adresse kommunizieren und über die neue des NLB-Clusters. In diesem Fall funktioniert der virtuelle NLB-Cluster oft nicht mehr. Sie können diesen Fehler aber leicht umgehen: Rufen Sie die Einstellungen der Clientzugriffserver im Hyper-V-Manager auf und klicken Sie auf "Netzwerkkarte" und aktivieren Sie die statische Zuordnung der MAC-Adressen. Aktivieren Sie außerdem noch "Spoofing von MAC-Adressen für die Clientzugriffserver". Microsoft beschreibt dieses Szenario auf der Webseite [1] genauer. Die Einstellungen gelten auch für Exchange Server 2010.

Clientzugriffserver und Hyper-V



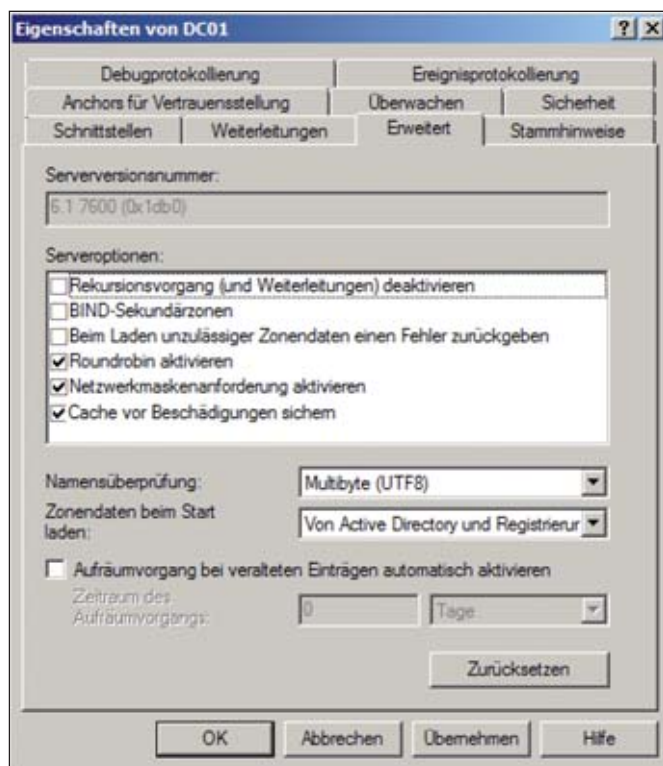


Bild 1: So aktivieren Sie Round Robin für DNS-Server unter Windows Server 2008 R2

ters. Serverdienste wie Clientzugriffserver lassen sich mit dem NLB-Dienst zuverlässig vor Ausfall schützen, da diese keine Daten speichern, sondern nur einen Zugriffspunkt darstellen.

Alternative Round Robin

Neben NLB können Sie auch über DNS-Round Robin eine gewisse Ausfallsicherheit und Lastverteilung in Exchange erreichen. Die Konfiguration ist zwar sehr einfach, aber bei weitem nicht so effizient wie ein NLB-Cluster. Round Robin ist ein einfacher Mechanismus, mit dem DNS-Server die Last auf Netzwerkressourcen, also auch verschiedene Clusterzugriffserver, verteilen können. Sie verwenden diese Funktion, um die Reihenfolge der zurückgegebenen Ressourcen-Einträge bei DNS-Abfragen in der Antwort auf eine Abfrage zyklisch zu ändern, wenn für den verlangten DNS-Domännennamen mehrere Einträge desselben Typs existieren. Einfach gesagt, erstellen Sie für jeden Clientzugriffserver einen DNS-Eintrag mit demselben Namen und der jeweiligen IP-Adresse. Auf

jeweils um eins verschiebt. Damit steht im Mittel jeder Eintrag gleich häufig an erster Stelle. Um dem Client möglichst einen Server direkt in seiner Nähe zu nennen – bei TCP/IP bedeutet das innerhalb desselben IP-Subnetzes –, ermittelt Round Robin bei Hostnamen mit mehreren zugeordneten IP-Adressen vor der Umsortierung, ob es einen Eintrag gibt, der dem Subnetz des Clients entspricht. Diesen setzt das DNS-System dann anschließend an die erste Stelle der zurückgegebenen Liste. Nur wenn kein passender eindeutiger Eintrag vorhanden ist, kommt Round Robin zur Lastverteilung zum Einsatz. Um einen Round Robin-Eintrag zu erstellen, gehen Sie folgendermaßen vor:

1. Öffnen Sie die Verwaltung Ihres DNS-Servers.
2. Erstellen Sie in der Zone des Active Directorys einen neuen Forward-Lookup-Eintrag mit der Bezeichnung des Round-Robin-Verbundes. Verwenden Sie als Namen keinesfalls den Namen eines Servers innerhalb des Verbunds, sondern einen eigenständigen Namen.

diese Weise können Sie im DNS konfigurieren, dass Clients bei der Namensabfrage eines Clientzugriffsservers immer eine andere IP-Adresse erhalten und diese dann weiter verwenden.

Dabei tragen Sie einen Hostnamen mehrfach, mit jeweils einer anderen IP-Adresse, in der DNS-Zone ein. Erreicht den DNS-Server nun eine Anfrage des Clients, liefert er die Liste aller gefundenen IP-Adressen zurück, wobei er die Reihenfolge der Einträge

3. Tragen Sie als IP-Adresse die Adresse eines Servers ein und bestätigen Sie die Erstellung des Eintrags.
4. Erstellen Sie jetzt für jeden weiteren Server der Farm einen identischen Eintrag, der jeweils zur IP-Adresse eines anderen Servers zeigt.
5. Abschließend haben Sie für jeden Server in der Farm einen Eintrag mit gleichem Namen und jeweils einer IP-Adresse.

Damit ein DNS-Server Round Robin unterstützt, müssen Sie in der DNS-Verwaltung die Funktion "Roundrobin aktivieren" in den Eigenschaften des Servers setzen. Antwortet ein Server auf eine Clientanfrage nicht, erhält der Client eine Fehlermeldung und muss die Anfrage wiederholen. Im Beispiel von Outlook äußert sich das in einem Fehler und der Anwender muss Outlook neu starten und hoffen, dass der nächste Server verfügbar ist. Aus diesem Grund ist NLB ein wesentlich effizienteres Mittel, um Lasten zu verteilen und für Ausfallsicherheit zu sorgen.

NLB für fast alle Exchange-Versionen

Am besten geeignet für die Erstellung eines NLB-Verbunds ist Exchange Server 2007. Da ab dieser Version eine rollenbasierte Installation möglich ist, lassen sich Clientzugriffserver optimal mit NLB absichern. Sie können auf dem gleichen Weg zudem Front-End-Server in Exchange Server 2003 schützen, die Konfiguration dabei ist identisch. Die Möglichkeiten hat Microsoft in Exchange Server 2010 ausgebaut. Wir zeigen Ihnen in den folgenden Abschnitten, wie Sie das Load Balancing für die aktuellen Exchange-Versionen ab 2003 einrichten. Ein Vorteil von NLB ist, dass Sie keine eigene Hardware oder dedizierte Server benötigen. Sie müssen lediglich die Server im Netzwerk, die bereits den abzusichernden Dienst ausführen, zu einem NLB-Cluster zusammenfassen.

Notwendige Vorbereitungen für Clientzugriff-NLB-Cluster

Setzen Sie mehrere Netzwerkkarten in den Clientzugriffsservern ein, sollten Sie ent-

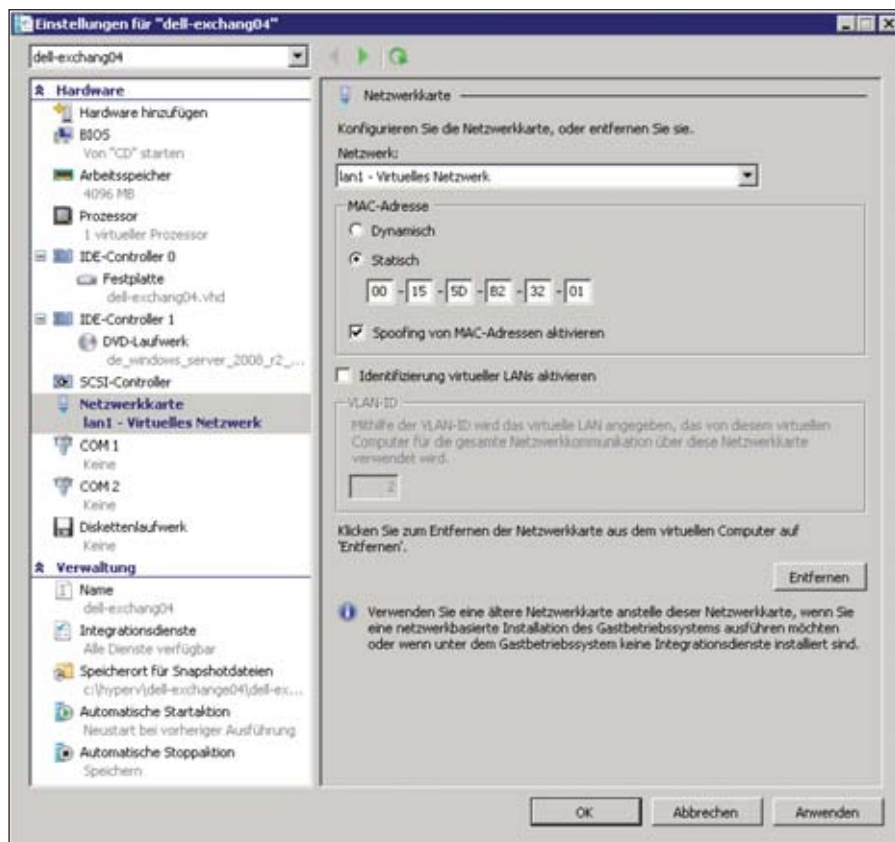


Bild 2: Bei virtuellen Servern sollte die MAC-Adresse angepasst werden

weder für eine der Karten ein Standardgateway eintragen oder IP-Forwarding aktivieren. Diese Funktion ist in Windows Server 2008 und 2008 R2 allerdings standardmäßig deaktiviert. Um sie zu aktivieren, geben Sie in der Befehlszeile das folgende Kommando ein:

```
Netsh interface ipv4 set int {Name  
der LAN-Verbindung} forwarding=  
enabled
```

Durch diese Option erlauben Sie dem Rechner, IP-Pakete, die nicht zum lokalen Server gehören, an andere Server weiterzuleiten. Da die Server in einem Cluster laufen, ist diese Funktion unbedingt notwendig. Im Server ist der Einsatz von mindestens zwei Netzwerkadaptern empfehlenswert, um optimale Leistung und Ausfallsicherheit zu gewährleisten. Eine Karte dient der Kommunikation mit den Anwendern im produktiven Netzwerk, während die andere der Verbindung der Server im Cluster dient. Außerdem sollten

Sie sicherstellen, dass die Namen dieser Verbindungen im Netzwerk- und Freigabecenter entsprechend gesetzt sind.

Haben Sie mehrere Netzwerkkarten in Ihrem Computer verbaut, werden Netzwerkpakete nicht immer an alle Netzwerkkarten gleichzeitig verschickt, sondern stets in einer bestimmten Reihenfolge. Damit die Antwortzeiten im Netzwerk optimiert sind, sollten Sie die Reihenfolge so konfigurieren, dass Ihre produktive Netzwerkkarte in der Reihenfolge ganz oben steht. Dazu gehen Sie folgendermaßen vor:

1. Klicken Sie zunächst im Netzwerk- und Freigabecenter auf den Link "Adapter-einstellungen ändern".
2. Aktivieren Sie anschließend über "Organisieren/Layout" die Menüleiste. Alternativ können Sie temporär die Menüleiste über die Taste Alt einblenden.
3. Rufen Sie den Menübefehl "Erweitert/Erweiterte Einstellungen" auf.
4. Es öffnet sich ein neues Fenster, über das Sie unter anderem die Bindungs-

reihenfolge der Netzwerkkarten einstellen können. Klicken Sie dazu auf der Registerkarte "Adapter und Bindungen" im Bereich "Verbindungen" auf die ausgewählte LAN-Verbindung und dann auf die Schaltflächen mit den Pfeilen, damit die gewünschte Verbindung nach ganz oben gesetzt wird.

Netzwerklastenausgleich installieren

Als Nächstes müssen Sie auf allen Clientzugriffsservern, die Sie im NLB-Cluster aufnehmen wollen, den Netzwerklastenausgleich installieren. Dies geschieht bei Windows Server 2008 (R2) über den Server-Manager als Feature. Öffnen Sie zur Installation den Server-Manager und klicken Sie auf "Features/Features hinzufügen". Wählen Sie den Punkt "Netzwerklastenausgleich" aus und führen Sie die Installation durch. Während der Installation müssen Sie keinerlei Konfigurationen vornehmen. Die Einrichtung des NLB-Clusters findet erst im Nachhinein in der entsprechenden Verwaltungskonsole statt. Installieren Sie das Feature auf allen Clientzugriffsservern, die Sie dem NLB-Cluster hinzufügen wollen.

Wollen Sie im Unternehmen Exchange Server 2007 auf Servern mit Windows Server 2008 R2 betreiben, ist die Installation des Service Pack 3 für Exchange Server 2007 nötig. Erst mit SP3 ist Exchange Server 2007 kompatibel zu Windows Server 2008 R2. Für die Installation auf Windows Server 2008 benötigen Sie mindestens das SP2. Die RTM-Version von Exchange Server 2007 unterstützt lediglich Windows Server 2003. Aber auch hier ist NLB verfügbar, allerdings nicht gerade effizient zu verwalten. Sie finden die Einstellungen in den Eigenschaften der entsprechenden Netzwerkverbindung. Setzen Sie Exchange Server 2003 ein, müssen Sie auf Windows Server 2003 setzen und hier die entsprechenden Einstellungen vornehmen. Bei Exchange Server 2010 ist nichts Besonderes zu beachten, da die neue Version standardmäßig bereits Windows Server 2008 R2 unterstützt und Windows Server 2008 ab SP2.

Bleiben Sie in Verbindung!



Folgen Sie uns auf Twitter

twitter.com/ita_blog



Werden Sie ein Fan auf Facebook

www.facebook.de/itanet



Treten Sie unserer Xing-Gruppe bei

www.xing.com/net/itanet



Lesen Sie unseren RSS-Feed

www.it-administrator.de/rss.xml

Social Networks sind auch beim IT-Administrator angekommen!

Auf Facebook haben wir ein eigenes Profil. Neben ausgesuchten Informationen rund um das Magazin und Veranstaltungshinweisen finden Sie hier auch Gewinnspiele oder Wissenstests. Oder wollen Sie den IT-Administrator in 140 Zeichen täglich begleiten? Verfolgen Sie unser „Gezwitscher“ über die interessantesten Neuigkeiten, besten Downloads und Tipps auf Twitter. Wenn Sie aber den direkten Austausch suchen, sind Sie in unserer Xing-Gruppe genau richtig. Lernen Sie dort Ihre Kollegen aus der IT und die Heftmacher des IT-Administrators persönlich kennen und nehmen Sie Einfluss auf Ihr Praxismagazin. Immer gut informiert bleiben Sie auch über unseren RSS-Feed.

Treten Sie unserer Community bei. Wir freuen uns auf Sie.



Bild 3: Das Hinzufügen einer Portregel für das CAS-Array ist schnell geschehen

Korrekten DNS-Eintrag erstellen

Nach der Installation des Netzwerklastenausgleichs erstellen Sie den DNS-Eintrag, indem Sie den Namen und die IP-Adresse des Clientzugriffs-NLB-Clusters hinterlegen. Anwender nutzen dann diesen Namen. Microsoft bezeichnet NLB-Cluster für Exchange auch als "CAS-Array". Rufen Sie das NS-Verwaltungsprogramm auf und erstellen Sie einen neuen Host (A)-Eintrag mit Namen und IP-Adresse des NLB-Clusters. Im Anschluss erschaffen Sie in der Verwaltung des Netzwerklastenausgleichs einen neuen NLB-Cluster.

Starten Sie dazu das Verwaltungsprogramm "Netzwerklastenausgleich-Manager" in der Programmgruppe "Verwaltung" des ersten Servers im CAS-Array. Klicken Sie dann auf "Cluster" und anschließend auf "Neu". Geben Sie im neuen Fenster den Servernamen des ersten Clusterknotens ein und klicken Sie auf "Verbinden". Wählen Sie die Netzwerkverbindung aus, die Sie für

den NLB-Cluster verwenden wollen, und klicken Sie auf "Weiter". Belassen Sie auf der folgenden Seite "Hostparameter" alle Einstellungen, wie sie sind. In der nächsten Ansicht fügen Sie die IP-Adresse hinzu, die Sie dem NLB-Cluster als Ganzes zuweisen möchten. Hier tragen Sie die IP-Adresse ein, die Sie als Host-Eintrag auf dem DNS-Server hinterlegt haben. Im weiteren Verlauf setzen Sie bei "Vollständiger Internetname" den DNS-Eintrag als FQDN, den Sie zuvor in DNS hinterlegt haben. Belassen Sie den Clusteraus-

führungsmodus auf "Unicast". Stellen Sie Verbindungsprobleme fest, können Sie an dieser Stelle auch "Multicast" verwenden. Nutzen Sie Multicast-IP-Adressen mit IGMP, sind Class-D IP-Adressen erforderlich. Auf der nächsten Seite löschen Sie die angelegte Standardregel und erstellen mit "Hinzufügen" eine neue. Die Regeln dienen dem Zugriff der Clients über das Netzwerk. Standardmäßig wartet ein NLB-Cluster auf allen Ports seiner konfigurierten IP-Adressen auf Anfragen. Dies sollten Sie in sicheren Umgebungen aber einschränken. Erstellen Sie eine eigene Regel, deaktivieren Sie die Option "Alle" bei Cluster-IP-Adresse und wählen Sie die IP-Adresse des Clusters aus:

1. Als Portbereich verwenden Sie 135 als Anfangs- und als End-Wert.
2. Aktivieren Sie bei "Protokolle" TCP.
3. Bei "Filterungsmodus" aktivieren Sie "Mehrfachhost".
4. Belassen Sie die Einstellung für Affinität auf "Einfach" und klicken Sie abschließend auf "OK".

Ports korrekt zuweisen

Erstellen Sie anschließend eine weitere Regel. Hier hinterlegen Sie als Portbereich die Ports, die von Outlook und dem CAS-Array verwendet werden. Haben Sie einen statischen Port für die Kommunikation festgelegt, tragen Sie diesen ein. Wie das geht, lesen Sie weiter unten. Arbeiten Sie nicht mit dem statischen Port, sondern mit der Standardeinstellung von Exchange Server 2007/2010, müssen Sie den Portbereich auf TCP 1024 bis 65535 festlegen. Sollen sich über das CAS-Array auch andere Clients verbinden, ist es ratsam, noch weitere Regeln für den entsprechenden Portbereich zu hinterlegen. Verwenden Sie dazu die gleichen Einstellungen und setzen Sie die notwendigen Ports ein. Arbeiten Sie zudem mit IMAP oder POP3, setzen Sie die Affinität für diese Regeln auf "Keine". Folgende Ports sind notwendig:

- Outlook Anywhere, Exchange ActiveSync, Outlook Web App – TCP 443
- IMAP4-SSL – TCP 993
- POP3-SSL – TCP 995
- IIS-Umleitung von HTTP auf HTTPS – TCP 80

Diese Regeln müssen Sie nur hinterlegen, wenn Sie die entsprechenden Protokolle auch verwenden. Haben Sie alle Regeln erstellt oder verwenden Sie die vorgefertigte Standardregel, klicken Sie auf "Fertigstellen". Anschließend sehen Sie in der Verwaltung des Netzwerklastenausgleichs den Cluster, der aktuell nur ein Mitglied hat. Im nächsten Schritt fügen Sie weitere Clientzugriffserver zum NLB-Cluster hinzu. Achten Sie darauf, dass auf allen Mitgliedern das Feature für den Netzwerklastenausgleich installiert sein muss. Klicken Sie mit der rechten Maustaste auf den erstellten Cluster und wählen Sie die Option "Host dem Cluster hinzufügen" aus. Geben Sie den Namen des Servers ein, den Sie hinzufügen wollen und klicken Sie auf "Verbinden". Belassen Sie die Standardeinstellungen auf der Seite "Hostparameter". Die bereits erstellten Portregeln akzeptieren Sie und klicken auf "Fertigstellen". Fügen Sie auf diesem Weg sämtliche Server hinzu.

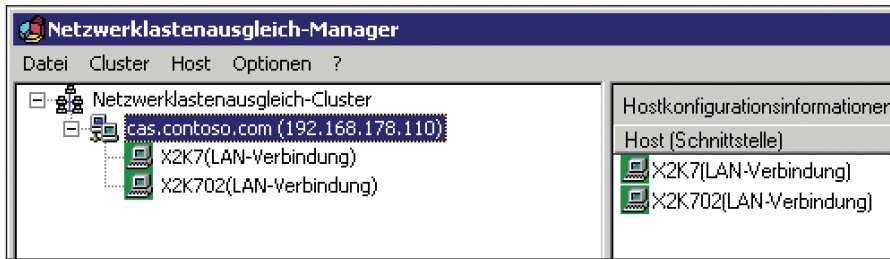


Bild 4: Im Netzwerklastenausgleich-Manager ist nach erfolgreicher Erstellung das CAS-Array sichtbar

Verbindungs Aufbau mit OWA testen

Nach der Erstellung sollten Sie zunächst den Zugriff testen, indem Sie eine Verbindung per OWA aufbauen und den Namen des erstellten CAS-Arrays verwenden. Achten Sie darauf, dass für den Test der Cluster erstellt sein und der entsprechende DNS-Eintrag vorhanden sein muss. Nach dem Verbindungsaufbau erscheint die Anmeldemaske von OWA, da der NLB-Cluster die Anfrage an einen Server im Cluster weitergeleitet hat. Erstellen Sie ein solches CAS-Array für Exchange Server 2010, müssen Sie vor der Verbindung noch in der Exchange-Verwaltungshell das Array hinterlegen. Verwenden Sie dazu das CMDlet `New-ClientAccessArray`, zum Beispiel mit der Syntax

```
New-ClientAccessArray -Name {Name
des Arrays} -Fqdn {FQDN des
Arrays} -Site {Active Directory-
Standort}
```

Exchange erstellt nun das Array und nimmt alle Clientzugriffserver am Standort automatisch mit in die Liste auf. Sie können bereits an dieser Stelle einen Ausfall testen, indem Sie den ersten Knoten im Cluster deaktivieren. Rufen Sie die OWA-Seite erneut auf, verbindet Sie der Cluster automatisch auf den zweiten Knoten. Achten Sie bei der Konfiguration bei der Zuweisung des Zertifikats zu den Servern auf den allgemeinen Zugriffsnamen des Zertifikats. Da die Clients nicht den Servernamen verwenden, sondern den Namen des NLB-Clusters, muss dieser Name als allgemeiner Name im Exchange-Zertifi-

kat hinterlegt sein. Alle NLB-Mitglieder sollten am besten das gleiche Zertifikat verwenden, mit identischem Namen, den Sie als Bezeichnung für den NLB-Cluster verwenden.

Häufig kommen dabei Subject Alternative Name (SAN) SSL-Zertifikate zum Einsatz. Mit diesen können Sie mehrere Domänen mit einer einzelnen IP-Adresse verbinden. Auf diesem Weg decken Sie mehrere Webseiten, Domänen und URLs mit einem einzigen Zertifikat ab. Verbindet sich ein Client per MAPI mit einem Clientzugriffserver, also mit Outlook im internen Netzwerk oder über Outlook Anywhere über das Internet, spielt das RPC-Protokoll mit seinen dazugehörigen Ports eine wichtige Rolle. Zwischen dem Clientzugriffserver findet eine Verbindung zwischen dem Port 135 und des dynamischen Portbereichs 6005-59530 statt. Vor allem beim externen Zugriff ist es sinnvoll, den dynamischen Bereich einzugrenzen, da Sie ansonsten zahlreiche Ports in Firewalls oder Routern öffnen müssen. Dazu sind allerdings Änderungen in der Registry auf den Clientzugriffservern und den Postfachservern nötig. Mehr zu diesem Thema finden Sie unter [2] und [3].

Sonderrolle Hub-Transport auf NLB-Clustern

Haben Sie die Hub-Transport-Rolle auf den gleichen Servern installiert wie die Clientzugriffsrolle, können Sie den NLB-Cluster nicht für Hub-Transport-Server verwenden. Exchange arbeitet intern mit bestimmten Mechanismen für den E-Mail-Versand und die Sicherheit zwischen Hub-Transport-Servern, so dass dieser Einsatz nicht empfohlen ist. Um

Hub-Transport-Server ausfallsicher zu gestalten, reicht es aus, pro Active Directory-Standort einfach mehrere Hub-Transport-Server zu installieren. In Exchange Server 2010 hat Microsoft zudem Techniken integriert, um den Ausfall von Hub-Transport-Servern abzufangen und den Versand von E-Mails sicherzustellen, indem der Quellserver diese erneut versendet. Bei Exchange Server 2010 wartet immer der sendende Server darauf, dass der empfangende Server die E-Mail entweder in ein Postfach oder einen weiteren Transportserver zugestellt hat.

Merkt der sendende Server, dass eine E-Mail auf dem Empfangsserver nicht zugestellt werden kann, versucht Exchange Server 2010 eine Zustellung auf einem alternativen Weg. Beispiel: Server A schickt eine Mail an Server B, der die E-Mail zwar entgegennimmt, aber aufgrund von Netzwerkproblemen nicht an Server C weiterleiten kann. Server A hat die E-Mail zwar erfolgreich an Server B zugestellt, diese aber noch nicht gelöscht. Stellt Server A fest, dass Server B die E-Mail nicht an Server C weitersenden kann, versucht Server A auf einem alternativen Weg, zum Beispiel Server D, die E-Mail an Server C zuzustellen. Auch hier behält Server A die E-Mail weiterhin auf dem Server, bis sichergestellt ist, dass Server D die E-Mail an Server C zugestellt hat. Die Kommunikation für diese Technik erfolgt mit den beiden SMTP-Befehlen `XSHADOW` und `XQDISCARD`. (In)



[1] **Hotfix bei Problemen im Zusammenspiel von Hyper-V und NLB**
<http://support.microsoft.com/kb/953828/en-us/>

[2] **Configuring Static RPC Ports on an Exchange 2010 Client Access Server**
<http://social.technet.microsoft.com/wiki/contents/articles/configuring-static-rpc-ports-on-an-exchange-2010-client-access-server.aspx>

[3] **Statische Portzuordnungen für Exchange Server**
<http://support.microsoft.com/kb/270836/de/>

Links



Drucken im Netzwerk (1)

Die Qual der Wahl

von Thomas Bär

Das einst proklamierte papierfreie Büro ist ferner denn je und spätestens bei dem Szenario einer Betriebssystem-Migration taucht eine Frage auf, die jüngst fast gänzlich in Vergessenheit geriet: Gibt es denn dafür auch die passenden Treiber? Wie es auch immer gedreht wird, Drucken ist in unserer Zeit wichtiger denn je – PDF und XPS hin oder her. In dieser Workshopserie betrachten wir das Drucken aus zahlreichen Perspektiven und geben Tipps zur richtigen Druckerzuordnung, den passenden Zusatzprogrammen und nicht zuletzt gegen Papierstau.

Es gibt eine schier unüberschaubare Anzahl von Druckern auf dem Markt. Für quasi jeden Zweck und für jeden Geldbeutel werden Geräte angeboten. Diese Vielfalt mag zwar Privatanwender erfreuen – im Unternehmensumfeld ist sie in erster Linie negativ zu betrachten. Verschiedenste Drucker haben verschiedenste Verbrauchsmaterialien, verschiedenste Eigenschaften beim Wechsel von Tinte oder Toner und häufig unterschiedliche Treiber. Verbrauchsmaterial, Know-how und Treiber für alle erdenklichen Geräte vorzuhalten, ist schlicht unwirtschaftlich. Eine generelle Empfehlung zu Herstellern und Geräten lässt sich objektiv kaum geben, da je nach Einsatzgebiet andere Eigenschaften gefragt sind. Die Vor- und Nachteile von Laserdruckern und Druckern auf Tintenstrahlbasis sind hinlänglich bekannt. Andere Druckerarten, beispielsweise Label-Drucker mit Thermodruck oder Festtintendrucker, sind für spezielle Bereiche interessant und im Büroalltag weniger häufig zu finden. Auch Matrixdrucker, die in den 1980er Jahren noch zur Standardausrüstung eines jeden Office-Terminals gehörten, sind in einigen Nischen immer noch sehr gefragt.

Farblaserdrucker befinden sich nach wie vor auf dem Vormarsch und sind in Bezug auf die Anschaffung kaum mehr teuer

als die Schwarz-Weiß-Drucker. Das Auffüllen aller Tonereinheiten in einem Farblaserdrucker ist jedoch mindestens viermal so teuer wie die Neuausstattung eines S/W-Druckers. Überhaupt spielen die Kosten der Verbrauchsmaterialien eine weitaus größere Rolle als die Anschaffungskosten. Durch den Vergleich der Reichweite von S/W-Tonern mit der von Vierfarb-Laserdruckern wird deutlich, dass ein Farbausdruck rund zehnmal so teuer ist wie ein einfacher S/W-Druck. Diese Preisunterschiede sollten Anwendern bewusst sein, ehe sie auf die Idee

kommen, selbst Probeausdrücke von Präsentationen in Farbe zu erstellen. Einige Druckertreiber erlauben daher, die Farbdruckoption bei der Installation gegenüber den Anwendern zu verbergen. Einstellungen, mit denen eine Abteilung wiederum nicht, sind so auch ohne Spezialsoftware realisierbar.

Viele Hersteller veröffentlichen auf ihrer Homepage Empfehlungen bezüglich des monatlich zu erwartenden Druckvolumens. Auch wenn sich diese Zahlen nicht

ID	Jobbezeichnung	Benutzer	Host-Bezeichnung	Ausgabegeräte	Drucknummer	Zahl der Blätter	Host IP	Jahresgehalt
1573	Microsoft Office Outlook - Memo	Thomas	CHALMERS	Abgeschlossen	4	4	LPD	2010/05/25 19:23:52
1574	Microsoft Office Outlook - Memo	Thomas	CHALMERS	Abgeschlossen	4	4	LPD	2010/05/26 10:58:47
1575	4p_Pflege-Thermometer_2009_Kurz	Thomas	CHALMERS	Abgeschlossen	8	8	LPD	2010/06/02 17:49:01
1576	WITZMAKING PDF	Christina	AGEDV,752	Abgeschlossen	3	3	PuS100	2010/06/03 13:47:33
1577	Microsoft Word - English Lessons	Christina	AGEDV,752	Abgeschlossen	1	1	PuS100	2010/06/07 14:00:51
1578	Microsoft Word - English Lessons	Christina	AGEDV,752	Abgeschlossen	1	1	PuS100	2010/06/07 14:13:45
1579	Microsoft Word - 1.doc	Thomas	CARL	Abgeschlossen	4	4	LPD	2010/06/08 20:33:32
1580	Microsoft Word - English Lessons	Christina	AGEDV,752	Abgeschlossen	1	1	PuS100	2010/06/08 09:09:38
1581	Microsoft Word - English Lessons	Christina	AGEDV,752	Abgeschlossen	1	1	PuS100	2010/06/08 09:44:15
1582	Microsoft Word - English Lessons	Christina	AGEDV,752	Abgeschlossen	1	1	PuS100	2010/06/08 09:47:08
1583	Microsoft Word - English Lessons	Christina	AGEDV,752	Abgeschlossen	1	1	PuS100	2010/06/11 11:51:36
1584	Microsoft Word - English Lessons	Christina	AGEDV,752	Abgeschlossen	1	1	PuS100	2010/06/11 12:01:00
1585	http://www.kidhouse.com/Panof	Christina	AGEDV,752	Abgeschlossen	1	1	PuS100	2010/06/11 12:11:32

Bild 1: Moderne Drucker verfügen über einen Netzwerkanschluss und eine Weboberfläche mit wichtigen Informationen zu Druckaufträgen, Druckvolumen oder Tonerständen

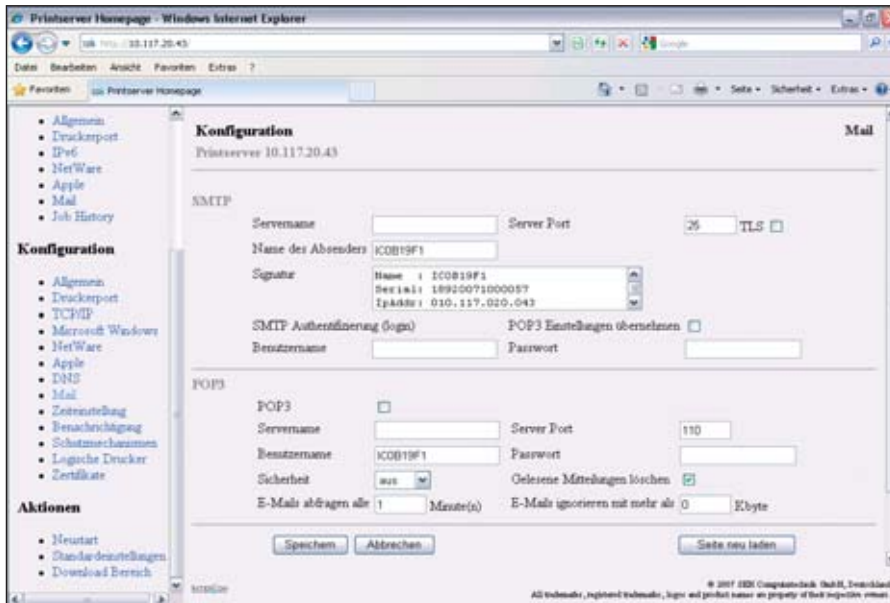


Bild 2: Auch ohne den Aufbau einer SNMP-Management-Umgebung ist dank der E-Mailfunktion von Printerboxen und Druckern der Administrator über Missstände bereits informiert, ehe Benutzer den Support anrufen

vollständig auf das eigene Unternehmen anwenden lassen, so geben sie doch darüber Auskunft, wie die Geräte eines Herstellers unter sich zu vergleichen sind. Ein kleiner Einzelplatz-Laserdrucker für knapp über 100 Euro wird sich kaum für den Massen-Rechnungsdruck in einem großen Unternehmen eignen – dafür ist das Gerät nicht gebaut worden. Ein Phänomen, das übrigens bei vielen dieser kleinen Einzelplatzdrucker zu beobachten ist und eine Ursache für das Symptom “Papierstau” darstellt. Einzelplatzdrucker sind dafür gebaut worden, kleinere Druckervolumen, in der Regel einige wenige Seiten am Stück, zu bedrucken. Wird auf diesen Druckern jedoch ein Druckauftrag mit 100 Seiten und mehr abgesetzt, so fällt spätestens nach der zwanzigsten Seite auf, dass sich das Papier beim Ausdruck wellt. Die Ursache für dieses Verhalten ist die fehlende Möglichkeit, die entstehende Wärme in den kleinen Geräten ausreichend abzuführen. Infolgedessen erwärmen sich die am Druck beteiligten mechanischen Bauteile und das Papier verzieht sich. Für größere Volumina entworfene Drucker haben diese Probleme nicht und dürften Anwendern und folglich dem IT-Support diesbezüglich mehr Freude bereiten.

Wenn also das Papierfach eines Druckers gerade einmal 50 Seiten fasst, sollte der IT-Profi bereits hellhörig werden.

Drei Standards: GDI, PCL und PostScript

Besonders beim Kauf günstiger Laserdrucker spielt ein Feature eine große Rolle: GDI. Dieses “Graphics Device Interface” ist in erster Linie eine Komponente des Betriebssystems Windows und dient als Programmierschnittstelle zu den logischen Grafikgeräten wie Grafikkarte oder Drucker. Bei Druckern erlaubt GDI den Einsatz relativ einfacher Hardware, da die Intelligenz der Druckaufbereitung nicht vom Drucker vorgehalten werden muss, sondern vom Betriebssystem. Der fehlende Bildprozessor, der die Rasterung des Ausdrucks vornimmt, mündet so in einen besonders günstigen Anschaffungspreis. Diesem niedrigen Preis steht jedoch ein Risiko gegenüber: die Treiberverfügbarkeit. Stellt der Hersteller für eine neue Windows-Version keinen Treiber bereit, so ist das Gerät nutzlos. Scheinbar ist das Interesse der Hersteller bei der Treiberbereitstellung gering, da sich beim Neuverkauf mehr Geld verdienen lässt. Für den Hewlett Packard LaserJet 1010 beispielsweise gibt es keine Treiber für Windows Vista oder höher,

wohl aber für den beinahe baugleichen LaserJet 1018. Der Einsatz von GDI-Druckern ist im Unternehmensumfeld kaum zu empfehlen – insbesondere dann, wenn Terminal-Services im Zusammenspiel mit Thin Clients verwendet werden. Interessanterweise sind GDI-Drucker bei kleineren Druckaufträgen in Bezug auf die Druckgeschwindigkeit größeren Druckern nicht unterlegen.

Anders als bei den GDI-Druckern handelt es sich bei PCL- und PostScript-Geräten um Drucker, die die Rasterung für den Ausdruck selbst berechnen. Das von Adobe entwickelte PostScript hat sich mit den Jahren immer mehr zu einem De-facto-Standard in der Druckindustrie entwickelt. PostScript ist weit mehr als eine Sprache, um einen Drucker anzusteuern – das heute sehr weit verbreitete PDF-Format basiert auf dem deutlich älteren PostScript. Nicht ganz so mächtig im Befehlsumfang, dafür ohne den Anspruch, ein Dateiformat zu sein, ist PCL. Die “Printer Command Language” ist eine von Hewlett-Packard entwickelte Befehlssprache zum Steuern von Laserdruckern, die aber auch bei vielen Tintenstrahldruckern zum Einsatz kommt. PCL wird von einer großen Anzahl von Herstellern verwendet und ist aktuell der Standard für Laserdrucker. Historisch betrachtet hat PCL den früheren Industriestandard für Drucker von Epson (den ESC/P) weitgehend abgelöst.

Detailfrage Druckprozessoren

Blicken Sie in die Tiefen der Optionen im Druckereigenschaften-Dialog, so finden Sie eine Auflistung unterschiedlicher Druckprozessoren. Seit Microsoft Windows NT 4.0 wird das “Enhanced Metafile” (EMF) für den Ausdruck als Standarddateityp verwendet. Im Gegensatz zu RAW-Druckern, bei denen die Daten über den Druckertreiber erzeugt werden, baut EMF auf das Graphical Device Interface (GDI) noch vor dem Spoolen des Auftrags auf. Nach dem Erzeugen der EMF-Informationen wird der Auftrag im Hintergrund durch das Spooler-Subsystem zum Druckertreiber

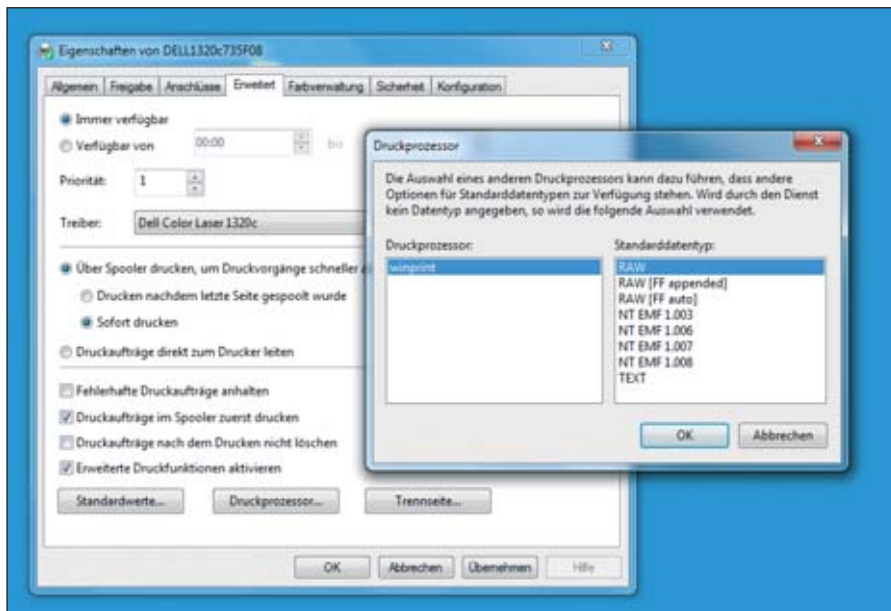


Bild 3: Verborgen in den Tiefen der Druckereinstellungen finden sich die Druckprozessoren

geschickt. EMF ist als Format flexibler als RAW. Eine EMF-Datei kann von verschiedenen Druckertypen gelesen werden. Zudem sind EMF-Dateien im Umfang kleiner als RAW-Druckaufträge. Der erste Teil des Render-Auftrags wird somit von dem Rechner übernommen, der den Druckauftrag erzeugt hat; den zweiten Teil übernimmt der ausführende Printserver. Dieses Verfahren stellt sicher, dass der Client-PC binnen kurzer Zeit wieder für Benutzereingaben zur Verfügung steht. Das EMF-Datenformat sorgt außerdem dafür, dass auf dem Client und auf dem Printserver die Schriften in der gleichen Ausprägung verwendet werden.

Das IMF-Format von Zenographics ZJ Incorporates stellt den Standard-Spooler-Datentyp für die so genannten "Super-Print 6"-Treiber dar, die von vielen namhaften Druckerherstellern wie Canon, Epson oder Xerox lizenziert wurden. Das Ziel von IMF ist es, mit einem kleineren Speicherausbau als bei EMF eine höhere Arbeitsgeschwindigkeit zu erzielen. Hierfür werden Kontrollinformationen wie StartDoc, EndDoc, StartPage oder EndPage übermittelt und grafische Elemente mit SuperRIP-Subobjekten, Zeichenteilen und einem Set von Basisinformationen zur Beschreibung eines Druckauf-

trags zur Beschleunigung verwendet. Die Unterstützung für übergeordnete Druckertreiber wie PCL-XL, PostScript oder PDF ist dabei gewährleistet. Das RAW-Format indes kommt zum Einsatz, um dem Spooler mitzuteilen, dass der Auftrag in keiner Form verändert werden darf. Der Auftrag muss dann vom Drucker so abgearbeitet werden, wie er ist. Ältere Applikationen und Windows 95/98-Clients verwenden dieses Format für die Bereitstellung von Druckaufträgen. In der Ausprägung "RAW [FF Appended]" wird jedem Druckauftrag ein so genannter "Form-Feed Character (0x0C)" angehängt, um den Auswurf der Seite beispielsweise auf einem PCL-kompatiblen Drucker zu erzielen. Ansonsten würde der Drucker die letzte Seite des Druckauftrags erst auf Knopfdruck auswerfen. "RAW [FF Auto]" prüft, ob ein 0x0C als letztes Zeichen im Druckauftrag gesendet wird. Falls nicht, wird es automatisch angefügt. Der Druckprozessor "TEXT" verwendet ausschließlich den ANSI-Zeichensatz, um den Druckauftrag abzuwickeln. Es werden automatisch die Grundeinstellungen für Schrift, Seitenausrichtung und Auflösung vom Drucker verwendet. Eine Vielzahl moderner Anwendungen können mit diesem Druckprozessor jedoch nicht mehr arbeiten.

Vielseitige Anbindung

Wird ein Drucker von mehr als einem Benutzer verwendet, stellt sich die Frage der Bereitstellung des Anschlusses: Eine eingebaute Netzwerkkarte, der lokale Anschluss am PC mit Freigabe oder die Nutzung einer kleinen Printerbox sind hier die Alternativen. Eine große Anzahl von Druckern ist bereits von Haus aus mit einem Ethernet-Anschluss ausgerüstet oder verfügt über eine eingebaute WLAN-Schnittstelle. Sicherlich gehört der integrierte Netzwerkanschluss zum guten Ton. Dank dieser Netzwerkanschlüsse sind Drucker relativ schnell in Netzwerke eingebunden. Mit einer zugewiesenen festen IP-Adresse oder einer Reservierung im DHCP-Bereich ist sogar eine von der DNS-Namensauflösung befreite Anbindung möglich. Je nach Hersteller wird deutlich mehr geboten als lediglich eine Einbindung in ein Netzwerk: Die Web-Oberflächen der Printer geben Auskunft über die bereits gedruckte Anzahl von Seiten, führen Buch über die letzten Druckaufträge oder visualisieren den Tonerstand. Wird der Drucker mit den passenden SNMP-Informationen ausgestattet, sen-

Alternative LPR/Unix-Druckdienste

LPR/Unix-Druckdienste stellen besonders in größeren Umgebungen eine interessante Alternative zu den Windows-eigenen Druckdiensten dar. Wir konnten jedoch in verschiedenen Tests feststellen, dass die Standard-Druckerfreigabe unter Windows einen kompletten Ausdruck schneller abarbeitet als ein LPR-Druck auf derselben Maschine.

Weniger Punkte, mehr Tempo

Je weniger Punkte für den Aufbau eines Druckrasters gebraucht werden, desto weniger Aufwand müsste der Drucker bei der Bearbeitung haben. In verschiedenen Tests konnte eine Verbesserung der Geschwindigkeit von maximal 47 Prozent durch die Reduktion von 600 DPI auf 300 DPI erzielt werden. Die Qualität des Ausdrucks leidet unter der Maßnahme jedoch besonders stark, wenn Fotos oder Zeichnungen im Ausdruck vorhanden sind. Beim Druck einfacher Textausgaben sind 300 DPI allerdings durchaus ausreichend.

Schneller drucken





den viele Geräte bei verschiedensten Zuständen, die vom Normalbetrieb abweichen, die dazu passende Nachricht aus. Ist in der Netzwerkumgebung keine SNMP-Überwachung aktiv, so bieten glücklicherweise viele Drucker die Nutzung von E-Mails zur Benachrichtigung.

Mini-Printserver

Die Freigabe des Druckers über eine Workstation ist immer dann problematisch, sobald nicht sichergestellt ist, dass der PC dauerhaft eingeschaltet ist. Kleine Hardware-Printserver, umgangssprachlich auch "Printerboxen" genannt, schaffen hier Abhilfe. Der Vorteil der Boxen gegenüber dem Standard-PC mit der Druckerfreigabe ist die einfachere Wartung und der geringere Stromverbrauch im Vergleich zu einem dauerhaft eingeschalteten PC. Zudem geben Printerboxen im Gegensatz zu den meisten Büro-Rechnern keinerlei Geräusche von sich, da sie oft ohne aktive Kühlung auskommen.

An die Qualität eines Ausdrucks werden heutzutage weitaus höhere Forderungen gestellt, als dies noch vor einigen Jahren der Fall war. Der Ausdruck von umfangreichen Dokumenten, die sich über mehrere Seiten erstrecken, mit Bildern und Grafiken aufgelockert und in einer hohen Druckqualität, ist eine Anforderung, die die kleinen Printerboxen erfüllen müssen. Die Mini-Server haben dabei eine äußerst lange Lebensdauer. Kommt es im

Zusammenspiel mit den Boxen zu Geschwindigkeitsproblemen, sollten Sie die technischen Eckdaten der Geräte genauer betrachten. Ältere Geräte bieten teilweise nur einen Pufferspeicher von 256 KByte – eine solch kleine Dimensionierung kann bei heutigen Druckaufträgen bereits der Grund für eine langsame Abarbeitung sein. GDI-Drucker bleiben im Szenario Printerbox in vielen Fällen außen vor, auch wenn einige Geräte immerhin ein Mindestmaß an PCL-Kommandos verstehen und sich mit einem generischen Treiber ansprechen lassen.

Zum direkten Anschluss eines Druckers ist USB aktuell das Mittel der Wahl. Das ältere, parallele Centronics-Interface steht bei den meisten PCs nicht mehr zur Verfügung. Printerboxen mit parallelem oder seriellem RS232C-Anschluss werden glücklicherweise noch angeboten, sodass diese sich für den Weiterbetrieb von "Legacy Devices" besonders gut eignen.

InterNet Printing Port

Einige Printerboxen sind mit der Funktion "InterNet Printing Port" (IPD) ausgestattet. Um über das Internet direkt auf einem Printserver ausdrucken zu können, ist die Einrichtung eines E-Mailkontos auf POP3/SMTP-Basis beim lokalen E-Mailserver erforderlich. In regelmäßigen Abständen fragt die Printerbox den Mailserver ab, ob ein Druckauftrag per E-Mail eingegangen ist. Clientseitig wird auf einem

Computer ein spezieller Druckertreiber eingerichtet, der, sobald er als

auszuführender Drucker ausgewählt wird, die E-Mailadresse des Printservers als Ziel zur Eingabe anfordert. Der Druckauftrag wird in eine E-Mail eingebettet und per Mailclient versendet. Gemäß den Einstellungen erhält der Absender nach vollzogenem Druckauftrag eine Bestätigungsmail. Der Druckauftrag erhält zudem ein Deckblatt vorangestellt, auf dem der Absender kenntlich gemacht wird. Neben dem IPD firmiert unter der Abkürzung IPP eine weitere Möglichkeit, auf den Printserver zu gelangen. Das "Internet Printing Protocol" (IPP) ermöglicht den Druckdienst über die URL-Adresse des Printservers. Microsoft hat diese Funktionalität ab dem Internet Information Server (IIS) 6 integriert.

Insgesamt kommen die kleinen Printserver von verschiedenen Herstellern in unterschiedlichen Ausbaustufen daher. Ein Netgear PS121 mit den Maßen 86,5 x 59 x 24,5 mm ist beispielsweise kleiner als eine Zigarettenschachtel. Im Inneren des Printservers arbeitet ein 1 MByte Flash-RAM für das Betriebssystem und die System-einstellungen und 4 MByte SD-RAM für einen kontinuierlichen Datenfluss zum Drucker. Anschluss findet ein einzelner USB-basierender Drucker gemäß der Spezifikation 1.1. Schon bei der Geschwindigkeitsangabe "10 MBit" für das Ethernet dürfte der Administrator misstrauisch werden. Vergleichen Sie die effektive Druckgeschwindigkeit dieses Mini-Printservers mit einem etwas größeren und auch teureren Gerät aus dem Hause Allnet, so benötigt der PS121 mit 68 Sekunden knapp doppelt so lang für eine Vergleichstestseite, wie ein Allnet Printserver XIV. Der in Bielefeld ansässige Spezial-Hersteller SEH bietet eine besonders umfangreiche Palette an verschiedenen Printerboxen an. In größeren Geräten von SEH ist zudem die am Markt verbreitete ThinPrint-Technologie implementiert, was die Geschwindigkeit des Ausdrucks, besonders in WAN-Umgebungen, beschleunigen kann. ThinPrint wollen wir im zweiten Teil unserer Serie denn auch genauer betrachten. (dr)



Bild 4: Mini-Printserver, auch Printerboxen genannt, bieten sich für die Drucker an, die über keinen eigenen Netzwerkanschluss verfügen



Quelle: Kelly Samanthia – Fotolia.com

Grundlagen der Storage-Sicherheit

Speichern, aber sicher

von Florian Thiessenhusen

Storage spielt in den meisten Unternehmen weit mehr als nur eine Nebenrolle. Nicht erst durch den Einsatz von iSCSI finden sich komplexe SAN-Infrastrukturen auch in kleinen bis mittelständischen Unternehmen.

Durch die immer zentralere Bedeutung dieser Technologien rückt ein weiterer Punkt in das Interesse vieler Unternehmen: Storage Security. Dieser Artikel stellt Gefährdungslagen dar und gibt Empfehlung zur Absicherung.

Um die Gefährdungslagen aus dem Bereich Storage zu überblicken, müssen zunächst die verschiedenen Technologien verstanden werden. Im Speicherumfeld lassen sich im Wesentlichen drei Arten unterscheiden:

- NAS: Network Attached Storage
- SAN: Storage Area Network
- DAS: Direct Attached Storage

Ein NAS beschreibt einen Storage, der (häufig im gleichen Netzsegment) direkt von Hostsystemen angesprochen werden kann. Die Administration der Freigaben und Berechtigungen erfolgt über eine eigene Administrationsschnittstelle. Darin besteht auch einer der größten Nachteile solcher Lösungen. Jedoch sind diese einfach zu betreiben und werden in fast allen Fällen mit Ethernet-Schnittstelle ausgeliefert. Da für solche Systeme keine dedizierten Hostsysteme vorgesehen sind, ist eine eigene Schnittstelle für Freigaben, Sicherheit und Netzwerkintegration nötig. Damit es immer und überall erreicht werden kann, läuft ein NAS standardmäßig mit NFS (Network Filesystem) und CIFS (Common Internet File System, erweiterte Version von SMB (Windows)).

Im Gegensatz zum NAS stellen SANs für das Netzwerk lediglich Laufwerke dar. Dort finden sich keine Freigaben, die mit CIFS oder NFS anderen Geräten zur Verfügung gestellt werden. Diese Laufwerke werden

von Hostsystemen (Servern) propagiert und durch selbige verwaltet. Als Übertragungsmedium kann Fibre Channel oder iSCSI genutzt werden. iSCSI hat in den letzten Jahren enorm an Bedeutung gewonnen, schon aufgrund der vergleichsweise günstigen Beschaffung der Hardware.

Eine Storage-Technologie, die in Unternehmen sehr selten anzutreffen ist, ist das "Direct Attached Storage", kurz DAS. Dabei verwaltet ein Hostsystem analog zum SAN ein Storage, das via USB oder Firewire angeschlossen ist. Diese Art des Speichers wird im weiteren Verlauf des Artikels auch nicht weiter verfolgt, da solche Konstellationen im Unternehmensumfeld kaum anzutreffen sind.

Angriffs- und Absicherungszenarien

Das größte Sicherheitsproblem bei NAS-Geräten ist hausgemacht: Datentransferprotokolle wie CIFS und NFS sind direkt aktiv. NAS-Geräte stellen sich für einen Angreifer von außen dar wie ein normaler Windows-Server. Dadurch, dass das NAS-Gerät im Büronetz auch direkt verfügbar ist, wird dieses intern nicht durch eine Firewall geschützt. Man-in-the-Middle-Angriffe lassen sich damit leicht durchführen. Diese Art von Attacke wird benutzt, um einem anfragenden Client vorzugaukeln, der Hacker-Rechner sei das NAS-Gerät. Der Angreifer leitet diese An-

fragen auch an das NAS weiter, das Client-system soll schließlich keine Unregelmäßigkeit feststellen. Der Clou dabei: Alle transferierten Daten werden mitgeschnitten und ausgewertet. Nun kommt eine entscheidende Lücke innerhalb von CIFS zum Tragen: Wird eine freigabenbasierte Authentifizierung genutzt, kommen nur drei Authentifizierungsarten in Frage:

- Share-Level Authentication: Nicht nur, dass für diese Art der Authentifizierung kein Benutzername vorausgesetzt wird, fliegt das Kennwort in Klartext durch das Netzwerk. Ein Zugang zum LAN genügt damit, um dieses Kennwort abzuheben. Des Weiteren gibt es standardmäßig keinen Schutz gegen Brute-force-Attacken. Effektive Tools prüfen mehrere tausend Passwörter pro Minute, es ist also nur eine Frage der Zeit, bis das Kennwort geknackt ist.
- Lanman/NTLM: Lanman sollte eigentlich nicht mehr eingesetzt werden. Jedoch – und auch dies ist ein Problem mit solchen Geräten – wird das Verfahren genutzt, um eine Kompatibilität mit alten Systemen zu garantieren, beispielsweise unter OS/2 oder Windows 95/98. Lanman bietet keine wirklich effektive Verschlüsselung. Der Algorithmus ist als unsicher zu bezeichnen und schnell knackbar, wenn der Hashwert bekannt ist. Dieser lässt sich per Man-in-the-Middle-Angriff leicht mit-schneiden. NTLM stellt die Weiterent-

wicklung zu Lanman dar. Zum Einsatz kommt hier eine Verschlüsselungskombination aus DES und MD4. Ein daraus generierter Hash kann jedoch auf Standardhardware innerhalb von 24 Stunden errechnet werden. Hier fällt das Mitschneiden des Hashes jedoch schwieriger, denn zusätzlich zur NAS-Komponente muss auch der Active Directory-Domänencontroller belauscht werden.

- Kerberos (Active Directory): Kerberos sollte alles Dagewesene in den Schatten stellen. Es wurde als Nachfolger zu NTLM entwickelt und wird auch heute noch in den Windows-Betriebssystemen eingesetzt. Die Kommunikation zwischen Server und Client erfolgt im Handshake-Verfahren. Anstelle des Kennwortes werden Tickets übertragen. Jedoch erfolgt bei der initialen Verbindungsherstellung mit dem NAS-Device eine Übertragung des Passwort-Hashes, woraufhin ein Ticket erstellt wird. Gelingt es, dieses Ticket mitzuschneiden, hat ein Angreifer

genügend Zeit, auf dieses offline eine Brute-force-Angriffe zu starten. Besagte Tools sind sehr erfolgversprechend.

Mit Benutzerdaten kann ein Angreifer zwar auf Daten zugreifen, aber das NAS-Device hat er dadurch nicht unter Kontrolle. Daher bietet sich ein Angriff auf die Administrationsschnittstelle des NAS an. Diese wird häufig über Web via unverschlüsseltem HTTP oder über Konsole (Telnet unverschlüsselt) realisiert. Kennwörter werden über das gesamte Netzwerk im Klartext übertragen. Es ist damit auch hier ein Leichtes, an diese Daten zu gelangen.

Damit wird ersichtlich, dass ein erfolgreicher Angriff meist über "Sniffing" stattfindet. Ein Angriffsvektor, der sich jedoch auch beseitigen lässt dank

- Netzsegmentierung: In Kombination mit einer dazwischen geschalteten Firewall sehr erfolgversprechend, jedoch ist mit Performanceeinbußen zu rechnen.
- Verschlüsselung: Jede Art von Kommu-

nikation, in der sensible Daten übertragen werden, sollte verschlüsselt werden. Hierbei könnten SSH (Administration), IPSec (Kerberos) oder SSL (Webinterface) eine sehr große Rolle spielen. Jedoch werden diese meistens nicht von den NAS-Geräten unterstützt. Eine effektive Verschlüsselung macht Abhören nahezu unmöglich.

Sicherheit im SAN

Als Angriffsziel wesentlich interessanter, weil auch verbreiteter, ist das SAN. Klassischerweise werden SANs in separaten Netzsegmenten aufgebaut, was es für einen Angreifer schwierig macht, einen direkten Zugriff auf die SAN-Infrastruktur zu erhalten. Wir gehen in den nachfolgenden Beispielen davon aus, dass ein netzwerktechnischer Zugriff besteht.

Das SAN-Übertragungsprotokoll, das über Fibre Channel läuft, ist dem von TCP/IP ähnlich. Es basiert auf ähnlichen Prinzipien bei der Verbindungsherstellung und

NETGEAR® FÜR KLEINE UND MITTLERE UNTERNEHMEN

Sicherheit ist kostbar. Und kostengünstig.

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

UTM50

STM600

NETGEAR® entwickelt passgenaue Lösungen für kleine und mittlere Unternehmen – und bietet deshalb Enterprise-Class-Qualität mit erheblichen Kostenvorteilen. In NETGEAR® ProSecure™ Security-Appliances kommt die beste verfügbare Sicherheitsarchitektur zum Einsatz. Sie bieten durch die 1,2 Mio. bzw. 3,2 Mio. Signaturen einen effektiven Schutz vor Viren und Malware und arbeiten durch die Stream-Scanning-Technologie bis zu fünfmal schneller als herkömmliche Lösungen.

UTM50 mit integrierter Firewall für 50+,
STM600 für 600+ Computer-Arbeitsplätze.

www.prosecure.netgear.de
www.netgear.de

NETGEAR®
Connect with Innovation™

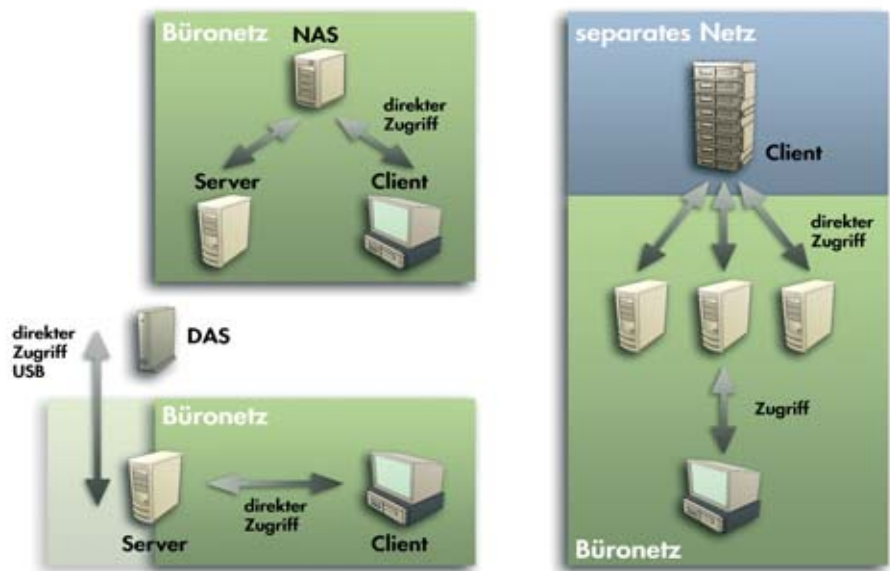


dem Sessionhandling. Dabei kommen ebenfalls Sequenznummern zum Einsatz, die jedoch unverschlüsselt übertragen werden. Es besteht also die theoretische Möglichkeit, durch Manipulation der Sequenznummern den Verkehr umzuleiten. Im Gegensatz zu IP-Netzwerken ist dies jedoch nicht so einfach, da höhere Geschwindigkeiten und andere Hardware anzutreffen sind. Jedoch bietet diese Schwachstelle innerhalb des Protokolls hervorragende Möglichkeiten, Man-in-the-Middle Attacks durchzuführen. Der Aufwand ist sehr hoch, aber das Ergebnis ist für den Angreifer verlockend.

Ähnlich verhält es sich mit einer Adressierungsschwachstelle innerhalb von Fibre Channel. Bei einem Zugriff auf ein LUN von einem Server werden FLOGI (Fabric Login), PLOGI (Port Login) und NLOGI (Node Login) ausgetauscht – ein 24 Bit langer Wert (jeweils 8 Bit), der dazu dient, Server am SAN zu authentifizieren. Da keinerlei Verschlüsselung für diese Adressen genutzt wird, kann diese Adresse durch einen Angreifer mitgeschnitten und modifiziert werden. Diese Methode ist auch hilfreich, um LUNs auf dem SAN zu enumerieren.

WWN Spoofing

World Wide Names ähneln MAC-Adressen von Host Bus Adaptern (HBAs). Sie sind eindeutig und einmalig. Im Ethernet-Umfeld vertraut man schon lange nicht mehr nur auf den Zugriffsschutz durch MAC-Filterregeln wie zum Beispiel auf WLAN-Routern oder bei NAC-Lösungen. Obwohl vergleichbar, werden Access Control Lists (ACLs) im FC-Umfeld nur mit WWN-Zuordnungen umgesetzt. Dies ist vergleichbar mit einem unverschlüsselten WLAN, das lediglich mit MAC-basierten ACLs arbeitet. Jeder versierte PC-Nutzer weiß, dass dieses Verfahren unsicher ist, da MAC-Adressen sehr leicht fälschbar und vortäuschbar sind. Genauso verhält es sich mit WWNs. LUN-Zuordnungen werden, wenn überhaupt, ausschließlich auf dieser Basis durchgeführt. Dabei sind WWNs ähnlich einfach mitzulesen und



Sowohl was die Anbindung als auch die Angriffe angeht, unterscheiden sich NAS, SAN und DAS voneinander

vortäuschbar. Durch Modifikation der Name-Server-Tabelle (analog zu ARP-Tabelle) auf dem FC-Switch kann außerdem der Verkehr umgeleitet werden oder Zugriff zu unberechtigten LUNs erfolgen. Der Aufwand ist auch da um einiges höher als in IP-Netzwerken, schon allein wegen der differierenden Hardware.

Management-Konsolen

Jegliche Netzsegmentierung von SAN-Infrastrukturen kann leicht ihr Ziel verfehlen, wenn die für das SAN zuständigen Administrationssysteme zentral und ungeschützt im Core-Netzwerk verfügbar sind. In den meisten Fällen sind Managementkonsolen auf Systemen installiert, die sich am Übergang zum SAN-Netzwerk befinden. Die Administratoren erleichtern sich so ihre Arbeit, denn alles ist über die eigene Workstation erreichbar. Nicht selten wird dann noch mit Telnet oder HTTP unverschlüsselt gearbeitet, was einem Angreifer die Arbeit ungemein erleichtert, Administrationskonten auszuspähen. Und selbst wenn alle Sicherheitsmaßnahmen getroffen wurden, wie zum Beispiel verschlüsselter Zugang zu Administrations-Interfaces, so ist der Administrator längst nicht auf der sicheren Seite. So haben zwei IT-Spezialisten vor einiger Zeit eindrucksvoll die Administrationsoberfläche eines SANs mithilfe

von einfachsten SQL-Statements überwunden. Der Fehler war hier systembedingt, ein Firmwareupdate wurde herstellerseitig geliefert.

Es ist längst kein sicherheitstechnischer Geheimtipp mehr, SAN-Netzwerke vom eigentlichen Büronetzwerk zu trennen. Dies wird schon alleine aus Performancegründen in den meisten Fällen getan. Nur gibt es selbst hierfür verschiedenste Möglichkeiten, auch dieses Zoning als Angreifer zu überwinden. Ein Blick auf die verschiedenen Netzwerkkomponenten bei einem Zoning verrät, weshalb:

- Server: Dieser ist meist mit zwei Netzwerkkarten ausgestattet und bildet den ersten Angriffspunkt. Diese Angriffe könnten über Schwachstellen im System (nicht vorhandenes Patchmanagement), im Protokoll (SMB, CIFS, Kerberos) oder einfach fehlerhafte Konfigurationen (versehentlich als Gateway für das SAN-Netzwerk konfiguriert) erfolgen.
- FC-Switch: Meist nicht direkt zu erreichen, da dieser nur im SAN-Netzwerk vorhanden ist. Jedoch hat auch dieser eine Ethernet-Schnittstelle für die Administration (SSH, Telnet, HTTP/S). Da die wenigsten Infrastrukturen ein dediziertes Administra-

tion-Netzwerk betreiben, gilt es, an die Administrationsdaten zu gelangen.

- SAN: Für das eigentliche SAN gilt das Gleiche wie für den FC-Switch. An die Daten direkt zu gelangen, setzt logischen Zugang und eine Menge Wissen über das System voraus. Viel einfacher ist es doch, das Administrationsinterface zu überwinden (SQL Injection, Passwort-attacken, Man-in-the-Middle).

Strikte Zoning-Regeln sollten daher eingehalten werden. So darf es keine direkten Zugriffe aus dem Core-Netz geben. Die Zuordnungen von Server zu SAN sollten zudem direkt und nicht über geteilte Netze erfolgen. Auch der Einsatz von Firewalls ist in diesem Zusammenhang zu prüfen. Verhindern Sie also gemeinsame Zugriffe aus unterschiedlichen und gleichzeitig potenziell unsicheren Netzwerkzonen, beispielsweise wenn Webserver aus der DMZ auf das gleiche SAN-Segment wie der Datenbankserver aus dem Core-Netzwerk zugreifen. Ein kompromittierter

Webserver könnte in diesem Beispiel als Einfallstor für unbefugte Zugriffe dienen.

Um Man-in-the-Middle-Attacken effektiv zu verhindern, sollten Sie alle verfügbaren Verschlüsselungsmethoden auch nutzen. Für Managementkonsolen und alle verwendeten Komponenten (Switch, SAN, Server, Admin-Interfaces) sind das SSH und HTTPS. Zusätzlich sind sichere Kennwörter zu verwenden und bestenfalls keine Standardbenutzer ("admin", "root"). Dies erschwert einem Angreifer die Arbeit enorm.

In den Angriffsszenarien wurde zudem viel über schwache Sequenznummern und WWNs gesprochen, die Man-in-the-Middle Attacks ermöglichen. Dadurch, dass diese Technologien standardmäßig nicht zusätzlich verschlüsselbar sind, sollten Gegenmaßnahmen auf dem Switch konfiguriert werden. Beispielsweise definieren Sie Portsperrungen, so dass nur bestimmte Ports auf LUNs beziehungsweise auf das SAN zu-

greifen dürfen. Änderungen in den Name-Servertabellen (Zuordnung Port zu WWN) sollten überwacht werden, Alarmierung sollte gegebenenfalls implementiert werden.

Fazit

Storage, ganz gleich welcher Art, stellt Unternehmen vor eine neue Herausforderung in Sachen Sicherheit. Leider haben dies viele Systemverantwortliche noch nicht erkannt und auch die Hersteller entsprechender Systeme müssen hier noch nacharbeiten. Aufgrund fehlender Standards ist ihnen daraus auch kein Vorwurf zu machen. Es liegt also beim Administrator, eine sichere Infrastruktur aufzubauen und mögliche Angriffsvektoren schon bei der Implementierung derartiger Systeme zu berücksichtigen und zu eliminieren. Durch einfache Hilfsmittel ist dies auch ohne weiteres möglich. (dr)

Florian Thiessenhusen ist IT-Security Consultant bei der adMERITia AG. Seinen Blog finden Sie unter: blog.port389.de

Lernen - Diskutieren - Virtualisieren

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

VMgoes2010 ermöglicht Ihnen direkten Zugriff auf qualitativ hochwertige, pädagogische Inhalte und zu den führenden Anbietern aus den Bereichen: Virtualisierung und Cloud-Computing. Somit erfahren Sie aus erster Hand wie die neuesten Trends mögliche Auswirkungen auf die zukünftigen IT-Bedürfnisse Ihrer Organisation aufweisen können.

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

*Bemerkung: Nicht alle Organisationen sind an den fünf Standorten vertreten. Besuchen Sie unsere Webseite für weitere Informationen.

vmgoes2010

berlin • düsseldorf • wien • münchen • frankfurt
02.11 04.11 09.11 17.11 23.11

www.vmgoes2010.com

Sponsorship Kontakt:
VMgoes2010@angelbcl.co.uk

Platinum Sponsor:

vmware®

Gold+ Sponsors*



*Please note: Not all companies are participating at all locations. Please check website.



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. Für jeden Tipp, der veröffentlicht wird, bedanken wir uns mit einem Gutschein über 20 Euro für den Internetshop getDigital.de.



Im Internet habe ich gelesen, dass sich bei Windows 7 das **Kontextmenü des Windows Explorers** um die Funktionen "In Ordner verschieben" und "In Ordner kopieren" erweitern lässt. Da ich diesen **direkten Weg sehr praktisch** finde, würde ich diese Einträge gerne einfügen. Wie mache ich das?

Mit der in Windows 7 im Normalzustand versteckten Funktion können Sie bei Rechtsklick auf eine Datei im Windows Explorer das Kopieren beziehungsweise Verschieben erheblich vereinfachen. Dazu müssen Sie lediglich zwei Werte in der Registrierungsdatenbank ändern. Drücken Sie die Windows-Taste und "R", geben Sie dann *regedit* ein und bestätigen Sie mit der Eingabetaste. Navigieren Sie nun zum Schlüssel "HKEY_CLASSES_ROOT \ AllFilesystemObjects \ shellx \ ContextMenuHandlers". Mit einem Rechtsklick wählen Sie die Option "Neu", dann "Schlüssel" und geben folgenden Wert ein:

(C2FBB630-2971-11D1-A18C-00C04FD75D13)

Hiermit haben Sie die Option "In Ordner kopieren" im Kontextmenü des Windows Explorer angelegt. Um auch

"In Ordner verschieben" anzulegen, wiederholen Sie die oben genannten Schritte und tippen Sie noch diese Ziffernfolge ein:

(C2FBB631-2971-11D1-A18C-00C04FD75D13)

Schließen Sie jetzt den Registrierungs-Editor. Die neuen Einträge im Kontext-Menü des Windows Explorer sollten Ihnen ab sofort zur Verfügung stehen. (In)



Mehr nützliche Tipps und interessante Neuigkeiten rund um System-Administration und Virtualisierung finden Sie in den Blogs von Sepago: <http://blogs.sepagode.de>

Um während einer Präsentation schnellen Zugriff auf mehrere Rechner zu haben, habe ich unter Windows Server 2008 R2 mit Hilfe von Hyper-V R2 diverse **virtuelle Maschinen als Demo-PCs** laufen. Es ist nun jedoch schon mehrfach vorgekommen, dass sich die virtuellen Computer während einer Session mit einem **Bluescreen** verabschiedet haben. Nach einem Reboot gibt die Ereignisanzeige **Bugcheck 0x00000101** als Grund für den Absturz aus. Wo liegt hier das Problem und wie kann ich es lösen?

Der von Ihnen beschriebene Bluescreen beruht auf dem sogenannten "CLOCK_WATCHDOG_TIMEOUT"-Problem, das auf Computern mit einem oder mehreren Intel-CPU's

mit dem Codenamen Nehalem auftritt. Ein CPU-Fehler verursacht fehlerhafte Interrupts, weswegen Windows einen Bluescreen auslöst. Microsoft stellt betroffenen Kunden kostenlos einen Hotfix zur Verfügung, mit der Windows Server 2008 R2 das Hardwareproblem abfangen kann. Sie finden diesen Hotfix in der Microsoft Knowledge Base unter dem Eintrag 975530. Nach dessen Installation sollten Sie zumindest von dieser Art Bluescreen verschont bleiben. (In)

Nach einem **In-Place-Upgrade auf Windows Server 2008 R2** wollte ich auf dem entsprechenden Rechner das **Active Directory Migration Tool 3.1** deinstallieren. Dies klappte jedoch nicht. Woran liegt das und wie bekomme ich das Werkzeug von der Festplatte?

Das Active Directory Migration Tool 3.1 (ADMT) ist rein auf den Betrieb unter Windows Server 2008 ausgelegt

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



– die Datei *Admtsetup.exe* funktioniert unter R2 also nicht. Da diese Komponente aber ebenso zur Deinstallation benötigt wird, lässt sich diese nicht abschließen. Wenn Sie also ADMT nicht schon vor dem Upgrade entfernt haben, müssen Sie auf folgenden Befehl zurückgreifen, den Sie in der Kommandozeile eingeben:

```
%windir%\system32\msiexec.exe /x
{F24F5CFB-B3AA-4EBB-BA61-
A916DBEE37D5} /norestart /qn /log
%windir%\ADMT\Logs\admtmsiuninstall.log
```

Sollten Sie im Zusammenhang mit ADMT auf eine Datenbank unter SQL Server 2005 Express zugegriffen haben und diese nicht mehr benötigen, können Sie diese ganz normal in der Systemsteuerung entfernen. (ln)



Nach der **Umstellung auf Exchange 2010 SP1** hatten wir sowohl beim Zugriff mit Outlook Web Access als auch über POP3 und IMAP **Probleme, eine Verbindung zum Mailserver herzustellen**. Stets waren wir mit der Fehlermeldung "imceaDomain must be a valid domain name" konfrontiert. So kamen wir darauf, dass der Name der entsprechenden Domäne nicht korrekt – sprich mit einem Leerzeichen – hinterlegt war. Nun bin ich mir nicht mehr ganz sicher, mit welchem Cmdlet sich die Domäne umbenennen lässt. Können Sie mir hier weiterhelfen?

Zunächst einmal können Sie mit dem Kommando *Get-AcceptedDomain | fl* die Konfigurationsinformationen aller akzeptierten Domänen auf den Bildschirm bringen. Fällt Ihnen in dieser Liste ein ungültiger Domänenname etwa mit einem Leerzeichen auf, so verwenden Sie folgenden Befehl, um die Domäne umbenennen:

```
Set-AcceptedDomain -Identity {Wert}
-Name "Gültiger SMTP-Domänenname"
```

Spätestens mit dem Setzen eines gültigen Domännennamens und einem Neustart des Servers sollten keine Probleme mehr beim Zugriff über OWA oder POP3 und IMAP auftreten. (ln)

Um unter Exchange 2010 auf die **Statistiken eines Postfachs** zuzugreifen und mir Daten wie die Mailbox-Größe oder den letzten Logon anzusehen, habe ich bisher immer die Exchange Management Console benutzt. Um mir diese Statistiken für alle Postfächer auf einem Server zu Gemüte zu führen, ist **ja das Cmdlet "get-mailboxstatistics" sehr nützlich**. Kann ich diesen Befehl verfeinern, so dass mir das System zum Beispiel nur diejenigen Mailboxes anzeigt, die größer als ein bestimmter Wert sind?

Das Cmdlet "get-mailboxstatistics" lässt sich durch diverse Parameter erweitern. Unter anderem können Sie mit Vergleichsoperatoren arbeiten. Eine Übersicht und eine kurze Erklärung dieser Operatoren rufen Sie mit dem Kommando *get-help about_operators* auf. Um eine Liste der Postfächer mit einer bestimmten Größe zu erhalten, verwenden Sie folgendes Kommando:

```
get-mailboxstatistics -server [Servername] | where {$_.totalitemsize
-gt "10KB"} | fl
totalitemsize,displayname
```

Dieser Befehl gibt Ihnen dann alle Mailboxen aus, die größer als 10 KByte sind. Bei Bedarf können Sie diese Auflistung nun noch aufsteigend sortieren. Tippen Sie dazu folgendes Kommando ein:

```
get-mailboxstatistics -server [Servername] | where {$_.totalitemsize
-gt "10KB"} | sort-object totalitemsize | fl totalitemsize,displayname
```

Statt diese Statistiken für einen Server abzufragen, können Sie diese mit dem Parameter "-database" statt "-server" auch für eine Postfachdatenbank zusammenstellen. Mit "-identity" werten Sie nur ein einzelnes Postfach aus. Aber das geht über die Management Console meist schneller. (ln)



Linux

Kommentare in **Linux-Konfigurationsdateien** sind ja grundsätzlich eine nützliche Sache und Leerzeilen helfen dabei, den

Überblick zu behalten. Manchmal fände ich es aber besser, lediglich die eigentlichen Konfigurationsanweisungen **ohne die ganzen Kommentare oder Leerzeilen** zu sehen. Gibt es hierfür eine Möglichkeit?

Um Konfigurationsdateien von nicht gewünschten Zeichen oder Zeilen zu befreien, greifen Sie am besten auf Tools wie *grep* oder *sed* zurück. Zusammen mit den passenden regulären Ausdrücken filtern die Werkzeuge die unerwünschten Füllzeichen heraus, etwa mit diesem Befehl:

```
# grep -v '^#\|^\$'
/etc/httpd/conf/httpd.conf
```

Zeilen, die mit einem Kommentar beginnen, finden Sie mit Hilfe des Ausdrucks "^#", Leerzeilen mittels "^\$". Grep erkennt Oder-Verknüpfungen der Ausdrücke mittels "|". Die Option "-v" bringt schließlich alles auf den Bildschirm, was nicht auf die angegebenen Ausdrücke passt – also alles, bis auf Leerzeilen und Zeilen, die mit einem Kommentar beginnen. (Thorsten Scherf/ln)

Auf einem Testrechner mit einem modernen **Sechskern-Prozessor von AMD** habe ich neulich openSUSE 11.3 installiert. Nach einigen Performance-Tests musste ich jedoch feststellen, dass die **Leistung des PCs unter den Werten von nominell nicht so schnell**

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

len CPUs liegt. Wie kann das sein und kann ich hier irgendwie für Abhilfe sorgen?

Die von Ihnen beobachteten Leistungseinbußen sind reell und treten bei fast allen derzeit aktuellen Linux-Kernen auf. Das Problem ist die von AMD mit den neuen Sechskernprozessoren wie dem Phenom II X6 1090T eingeführte Technologie "Turbo Core". Diese Funktion sorgt für ein Übertakten einzelner Prozessorkerne, wenn andere Kerne im Leerlauf sind und soll eigentlich den Kühlungsbedarf für das gesamte Rechenherz vermindern. Dieses Technologie kommt jedoch den Stromsparfunktionen des Betriebssystems in die Quere: Der Kernel kann die korrekten Prozessorfrequenzen nicht aus den ACPI-Tabellen auslesen und erreicht so meist nicht einmal seine Nominalfrequenz. Je nach Linux-Distribution wurde das Problem durch ein Kernel-Update bereits behoben. Ist dies bei Ihrer Version nicht der Fall, bleibt Ihnen nur, im BIOS die Stromsparfunktion "Cool'n'Quiet" zu deaktivieren. Damit steigt zwar die Leistungsaufnahme des Systems, dafür können Sie dann aber auf die volle Kraft des Prozessors zurückgreifen. (ln)



Tools

Für VMware-Administratoren sind Drittanbietertools, die ein **umfassendes Management, Kapazitätsplanung, Change Management oder auch Reporting** zur Verfügung stellen, oft ein teures Vergnügen. Dabei sind derartige Funktionen auch für kleine VMware-Infrastrukturen mit nur einem oder wenigen Hosts unverzichtbar, um die Vorteile virtualisierter Systeme auszunutzen. Wer also sein Budget schonen muss, für den hält Veeam eine Antwort parat.

Der kostenlose **Veeam Reporter Free Edition** enthält alle Kernfunktionen der Vollversion des Veeam Reporter, wie umfassende Datensammlung, Multi-User-Unterstützung und Microsoft SQL Server Backend. Die Anzahl der Hosts, virtuellen Maschinen, Benutzer oder die Größe des Archivs sind nicht begrenzt. Veeam Reporter hilft zudem bei der Verrechnung

von Rechenkapazitäten einer virtualisierter Infrastruktur an ihre Nutzer (Chargeback). Wie die Vollversion ist Veeam Reporter Free Edition für vSphere 4 und VI3 als "VMware Ready" zertifiziert. Das Werkzeug ist in der Lage, IT-Verantwortlichen sowohl eine technische als auch eine wirtschaftliche Sicht auf die VMs zu geben. So lässt sich einerseits über den Blick auf die Hosts der VMware-Installation ein klassisches Systemmanagement realisieren, andererseits lassen sich VMs und deren Nutzungsgrad Fachabteilungen oder ähnlichem zuordnen und so Abrechnungsmodelle oder SLAs realisieren. Umfassend ist zudem die Reporting-Funktion des freien Tools: Infrastrukturen – auch über mehrere vCenter hinweg – erkennt Veeam Reporter Free automatisch und erlaubt Administratoren aus den gewonnenen Daten schnell individualisierte Reports zu erzeugen. Hilfreich ist zudem das integrierte Change Management, das alle Veränderungen an der Infrastruktur aufzeichnet. Somit lassen sich beispielsweise mögliche Quellen von Performance-Problemen identifizieren. In der freien Version ist diese Funktion jedoch auf die letzten 24 Stunden begrenzt. (jp)

Quelle: www.veeam.com/vmware-esx-reporter-free.html

Auch in IT-Infrastrukturen, die als Standard auf Windows-Betriebssysteme setzen, sind Inseln mit **Unix-, Linux- und Mac-Benutzern sowie -Gruppen** unvermeidlich, zum Beispiel in der Grafikabteilung, im CAD oder der Entwicklung. Solche Clients in ein homogenes **Benutzer- und Identitätsmanagement** einzubinden, ist für den Admin nicht immer ganz einfach – besonders wenn es gilt, diese User möglichst in das **Active Directory** einzubinden.

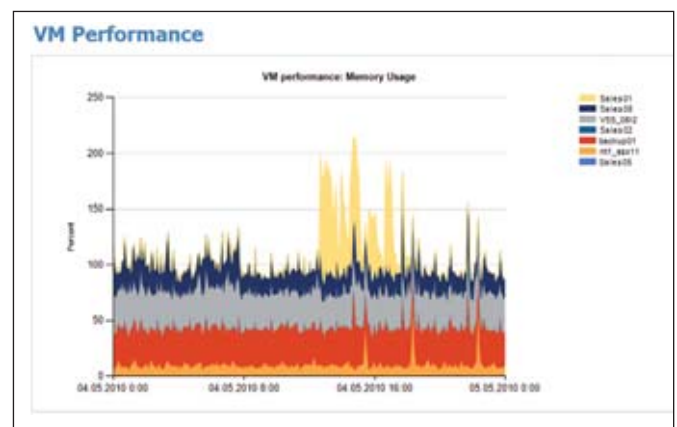
Quest bietet dazu die Freeware

Quest Identity Manager for

Unix kostenlos zum Download. Das Tool ermöglicht die einfache Verwaltung von Unix-, Linux- und Mac-Benutzern sowie -Gruppen, stellt die wichtigsten Identitäts- und Gruppen-Informationen aus diesen Systemen zusammen. Die wichtigsten Funktionen im Überblick:

- Das Management von lokalen Benutzern und Gruppen
- Administratoren können für die Verwaltung aller Unix-Account-Informationen ein Tool verwenden, unabhängig davon, wo sich die Informationen befinden.
- Neue Benutzerkonten können über mehrere Unix-Systeme hinweg über eine zentrale Konsole angelegt und abgelaufene Konten gelöscht werden.
- Passwörter lassen sich zentral über alle bestehenden Unix-Systeme hinweg zurücksetzen.
- Es stehen granulare Berichte zu Unix-Identity-Informationen zur Verfügung, die sich schnell und unkompliziert erstellen lassen, einschließlich aller lokalen Konten, die mit einem Single User in Beziehung stehen, sowie aller Mitglieder spezieller Unix-Gruppen.
- Die Darstellung aller lokaler Unix-Accounts und Systemparameter aus der Vogelperspektive hilft Administratoren unter anderem dabei zu bestimmen, welche Systeme sich für die erweiterten Funktionen wie Active Directory-Bridge-Technologien eignen. (jp)

Quelle: www.freeunixiam.com



Veeam Reporter Free zeigt die CPU-Nutzung verschiedener VMs

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



Virtuelle Welten sicher gestalten **Feste Schutzzäune für flexible Umgebungen**

von Adam Hufnagel

Virtualisierungstechnologien haben in vielen Unternehmen längst Einzug gehalten. Sie sind an verschiedenen Stellen der Unternehmens-IT vorzufinden und sorgen für eine deutliche Flexibilisierung. Auch die dadurch erreichbaren Kosteneinsparungen sind seitens der Verantwortlichen gern gesehen. Bei all diesen Überlegungen muss jedoch stets auch die Sicherheit fest im Blick behalten werden. In diesem Beitrag gehen wir deshalb auf die Besonderheiten ein, die beim Thema Security für virtualisierte Umgebungen gelten.

Der Virtualisierungsvorgang an sich hat im Allgemeinen kaum Einfluss auf die spezifischen Schwachstellen und Angriffsvektoren der virtualisierten IT-Ressourcen, diese bleiben auch nach der Virtualisierung unverändert. Doch das Umfeld, in dem diese IT-Ressourcen nun betrieben werden – die virtuelle IT-Infrastruktur – kann aus Security-Sicht sowohl Vor- als auch Nachteile haben. In Bezug auf die Sicherheitsaspekte ist unter anderem zu beachten, dass die Vorzüge virtueller Maschinen, wie beispielsweise ihre Mobilität, nicht nur technisch und administrativ bestmöglich unterstützt werden.

Virtualisierung und Sicherheit als Ganzes

Darüber hinaus ist sicherzustellen, dass die etablierten Maßnahmen der IT-Security auch in der virtuellen Welt umgesetzt und – sehr wichtig – an die speziellen Gegebenheiten der virtuellen Infrastruktur adaptiert werden. So muss in einem virtualisierten Rechenzentrum zum Beispiel nicht nur das Zonen-Konzept effektiv und ohne Kompromisse realisierbar sein, sondern auch die einzelnen VMs und der Hypervisor selbst sind vor möglichen Angriffen oder versehentlichen Konfigurationsfehlern optimal zu schützen. Je nach Umfeld können sich

hier sehr unterschiedliche Lösungsansätze als wirtschaftlich und technologisch sinnvoll erweisen.

So muss unter anderem die Frage beantwortet werden, ob die durch einen Hypervisor hergestellte Isolation der VMs – also eine logische Partitionierung der Ressourcen – ausreichend ist. Hilfreich auf dem Weg zu dieser Antwort ist zuvor die Klärung einer weiteren Frage: Wie werden aktuell die Netzwerkdatenströme der fraglichen Anwendungen getrennt – durch ein VLAN? Sind hier aufgrund von Security-Anforderungen getrennte physische Netze vorgesehen, ist eine physische Partitionierung der Ressourcen anzuraten.

Anspruchsvolles Management virtueller Maschinen

Ein neuralgischer Punkt für den sicheren Betrieb virtueller IT-Infrastrukturen ist der Umgang mit nicht aktiven VMs – Images und Snapshots. Die Nutzung vorgefertigter Vorlagen für ganze IT-Systeme kann durch die damit verbundene Standardisierung und Automatisierung einen positiven Einfluss auf die IT-Sicherheit haben. Ein spontan erstellter Snapshot eines laufenden Systems inklusive Speicherinhalt kann erheblich

zur Aufdeckung bestimmter Angriffe beitragen. Doch wie so oft gibt es auch hier Schattenseiten. Zum einen können die Abbilder sensible Informationen wie persönliche Daten oder Passwörter enthalten. Das ist bei einem physischen System zwar auch so, doch lassen sich VMs wesentlich einfacher mitnehmen als ein Server oder eine Festplatte. Deshalb können Snapshots für einen potenziellen Angreifer besonders ergiebig sein, enthalten diese doch auch die RAM-Inhalte des laufenden Systems. Neben Daten, die nie auf eine Festplatte geschrieben werden, ist damit auch ein bestimmter Status des Systems eingefroren, in dem unter Umständen ein Anwender oder sogar ein Administrator für den Zugriff auf hochsensible Daten oder Systeme autorisiert wurde.

In diesem Zusammenhang ist auch das Phänomen der scheinbar haltlosenervielfältigung der VMs (VM Sprawl) zu betrachten. Es ist eben nicht nur für die Administratoren verlockend, einfach “mal eben” einen Snapshot oder ein Image anzulegen und dann noch eines und noch eines. Diese Möglichkeiten haben oft genug auch viele Anwender. Die damit verbundenen negativen Auswirkungen auf die produktiv verfügba-

ren Ressourcen und die damit verbundenen IT-Kosten sind ein Problem. Ein anderes, nicht minder gravierendes Problem stellen hierbei die Sicherheitsimplikationen dar. Denn wer hat jederzeit den Stand der System-Patches, Sicherheitseinstellungen und der Virensignaturen dieser VMs unter Kontrolle? So ist es nicht immer einfach sicherzustellen, dass ein Snapshot einer VM nicht, auch nicht versehentlich, in einem sensiblen Bereich des produktiven Netzwerkes zum Leben erweckt wird.

Berechtigungen resolut setzen

Es ist offensichtlich, dass der Umgang mit Images und Snapshots in einer virtuellen IT-Infrastruktur geregelt werden muss. Die Einhaltung dieser Regeln ist dabei nicht nur aus Compliance-Gründen durchzusetzen. Dies lässt sich nur erreichen, wenn die Funktionsvielfalt der Virtualisierungs-Lösung, die interne Organisation, aber auch andere Infrastrukturkomponenten (beispielsweise im Storage-Umfeld) mit wirkungsvollen Werkzeugen und Richtlinien unterstützt werden.

Ein angemessen restriktiver Umgang mit administrativen Berechtigungen, sowohl innerhalb der Management-Konsolen als auch im Storage, ist unerlässlich. Es ist beispielsweise nicht notwendig, dass der Administrator einer bestimmten Anwendung vollen Zugriff auf alle Funktionen der virtuellen IT-Infrastruktur und auf alle Ablageorte für VMs im Unternehmen hat. Rollenbasierte Administration wird von fast allen relevanten Virtualisierungslösungen unterstützt – sie muss lediglich genutzt werden. Fehlende Funktionen müssen von den Anwender-Unternehmen beim Hersteller direkt eingefordert werden.

Die Erstellung von VMs nach Bedarf muss durch anwenderfreundliche Automatisierungsverfahren und -Portale eingedämmt werden. Dies sollte jedoch nicht die produktive Kreativität der Anwender einschränken. Zu einer umfassenden

Konzeption der virtuellen IT-Infrastruktur gehört die Implementierung regelmäßiger, automatischer Überprüfungen inaktiver VMs, Snapshots und Images auf aktuellen Patch-Stand und korrekte Security-Einstellungen. Mithilfe abgestufter administrativer Berechtigungen und der Bereitstellung passend vorkonfigurierter VM-Vorlagen lässt sich sicherstellen, dass eine noch nicht zur produktiven IT-Umgebung zugehörige VM ausschließlich in einem besonders abgesicherten Quarantäne-Netz aktiviert werden kann.

Bewusstsein für Virtualisierung schaffen

Es ist wichtig, dass die getroffenen Maßnahmen den Anforderungen der IT-Security genügen und gleichzeitig die notwendige Flexibilität und Agilität der virtuellen IT-Infrastruktur, und damit die Produktivität der Anwender, erhalten. Virtualisierung führt auch im IT-Betrieb zu einem Paradigmenwechsel. Für die Mitarbeiter der IT-Organisation heißt es, gemeinsam eine Leistung für das Unternehmen und die Geschäftsziele zu erbringen, die zum Teil weit über den Horizont der einzelnen fachlichen Spezialisierungen hinausgeht. Dies erfordert, dass Netzwerk-, Security-, Server- und Anwendungsspezialisten mit den Verfechtern der Virtualisierung gemeinsam an technisch und wirtschaftlich sinnvollen Konzepten für den jeweils spezifischen Anwendungsfall arbeiten.

Es ist heute jedoch noch häufig der Fall, dass die einzelnen Organisationseinheiten in den Unternehmen eher für sich stehenden Wehrtürmen gleichen. Jede umfangreichere Aufgabe wird in aufeinander folgende Schritte aufgeteilt, die von Spezialisten erledigt werden. Diese Personen haben – organisationsbedingt – hauptsächlich ihren Bereich beziehungsweise ihre Aufgabe vor Augen. Der Blick auf das Gesamtergebnis, den eigentlichen Zweck und die wirklichen Anforderungen einer unternehmens-

Worüber Administratoren morgen reden

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

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

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

Jetzt einfach und kostenlos bestellen unter:



www.it-administrator.de/newsletter

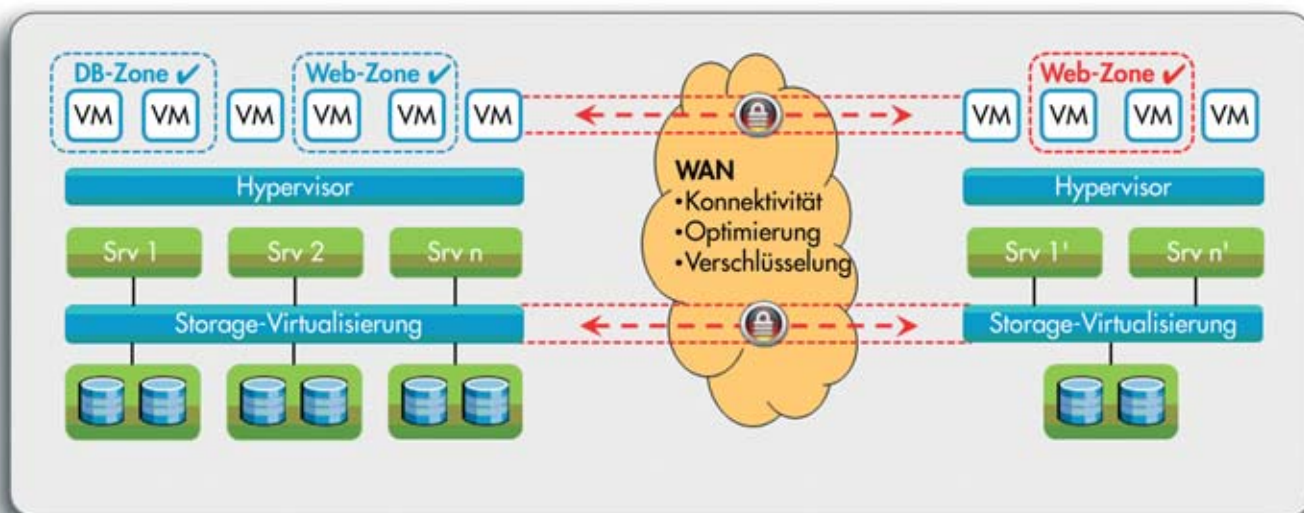


Bild 1: Ein wichtiger Security-Aspekt innerhalb einer virtuellen IT-Infrastruktur ist die logische Segmentierung über die Standortgrenzen hinweg

weiten Virtualisierungs-Strategie ist häufig nicht gegeben. Hier bedarf es einer offenen Kommunikation und eines starken Dirigenten, der stets das Ganze im Blick behält.

Sattelfeste Einbindung ins Netzwerk

Zum sicheren und effizienten Betrieb virtualisierter Rechenzentren gehört auf der technischen Seite eine tragfähige Integration in das bestehende Netzwerk. In größeren IT-Umgebungen wird die mangelnde Integration einiger Virtualisierungs-Konstruktionen in die vorhan-

dene physische Netzwerkinfrastruktur recht schnell offensichtlich. Der Server-Administrator – häufig auch der Virtualisierungs-Admin – kommt in die Verlegenheit, selbst die passenden Netzwerke für die VMs auszuwählen. Die Netzwerkkommunikation der VMs in einer virtuellen Infrastruktur ist für das physische Netzwerk und alle dort befindlichen Management-, Monitoring- und Troubleshooting-Maßnahmen transparent. Das Gesamtkonzept muss ein Monitoring des Netzwerkverkehrs der VMs auf verdächtige Aktivitäten (Anomalien) unterstützen.

Moderne Software unterstützt hier nicht nur durch eigene Funktionen, sondern auch durch offene Schnittstellen. Diese ermöglichen es Spezialisten, ihre langjährige Erfahrung aus der physischen Welt in die virtuelle Infrastruktur einzubringen. Weitere Herausforderungen liegen im Bereich der einheitlichen Konfiguration der Systeme. Die IT-Fachkräfte sind oft gezwungen, zum Teil ohne die notwendige Transparenz und gelegentlich auch außerhalb ihrer Kernkompetenz, zu agieren. Dies hat gravierenden Einfluss auf die verschiedenen Aspekte der IT-Security. Das Prinzip des "Segregation of Duties" hat nach wie vor seine Gültigkeit.

Auch innerhalb einer virtuellen Infrastruktur ist es nicht nur aus Effizienz- und Sicherheitsgründen sinnvoll, die technischen Aufgabengebiete zu trennen. Effektive Möglichkeiten zur einheitlichen Netzwerkkonfiguration der VMs sowie eine Transparenz, die den Gegebenheiten in physischen Netzwerken entspricht, sind also die Elemente, die bei der Konzeption einer virtualisierten Umgebung ganz oben auf der Prioritätenliste stehen sollten. (In)

Adam Hufnagel ist als Product Manager Application Delivery bei der Controlware GmbH tätig.



Bild 2: Auf Kundensituationen abgestimmte Dienstleistungsangebote erleichtern den Weg zu einer langfristig tragfähigen Lösung



Planen und Implementieren von IP-Kommunikationsnetzen

Reibungslose Migration

von Dirk Srocke

Mit dem Konzept von Unified Communications und Collaboration (UCC) sollen verschiedene Kommunikationsmedien zusammengefasst werden. Für Endanwender bedeutet das im Idealfall eine nahtlose Kommunikation ohne Medienbrüche, während sich die IT-Abteilung über ein erleichtertes Management eines konsolidierten Netzwerks freuen sollte. Ganz unproblematisch ist eine Umstellung freilich nicht.

UCC wird nicht zufällig auch als Real-Time Communication bezeichnet. In Echtzeit ausgetauschte Informationen beschränken sich dabei nicht auf relativ unkritische E-Mails oder Präsenzmeldungen. Die Übertragung von Video-konferenzen und Telefonaten über das Datennetz stellt erhöhte Anforderungen an die vorhandene Infrastruktur im Unternehmen. Als Referenz für Telefongespräche im geschäftlichen Umfeld gilt nach wie vor ISDN. Ein Maß für die Qualität von Telefonaten ist der "Mean Opinion Score" (MOS). Der Wert zwischen 1 und 5 wird subjektiv ermittelt. Einem Anwenderkreis werden dabei Hörproben vorgespielt. Diese werden von jedem Einzelnen bewertet und anschließend gemittelt. Für ISDN ist typischerweise mit Werten zwischen 4 und 4,5 zu rechnen. Um eine vergleichbare Qualität auch für VoIP-Telefonate zu erreichen, müssen verschiedene Faktoren betrachtet werden. Neben Qualität der verwendeten Telefone (Mikrofone und Lautsprecher) sowie Codecs spielt das eigentliche Netzwerk die entscheidende Rolle – da Sprache in IP-Netzen in Datenpakete zerstückelt und verbindungslos übertragen wird.

Geforderte Übertragungsleistungen des Netzwerks

Voraussetzung für eine ordentliche Sprachvermittlung ist zum einen die verfügbare Bandbreite im Netzwerk. Für ein einfaches Telefongespräch sind rund 100 KBit/s einzuplanen. Außerdem sollten

Quelle: Gino Sanders – Fotolia.com



Damit VoIP nicht zum Reinform wird, sind einige Grundlagen zu beachten

die Datenpakete rechtzeitig und ohne größere Verluste ankommen. Damit Echtzeitdienste wie Telefonie störungsfrei funktionieren, darf die Laufzeit (Latenz) zwischen zwei Clients nicht über 150 ms betragen. Experten ziehen davon bereits 50 ms für interne Berechnungen ab, womit für die eigentliche Datenübertragung noch 100 ms übrig bleiben. Firewalls und Proxyserver können sich mit Verarbeitungszeiten bis zu 1.000 ms zudem extrem negativ auf Laufzeiten auswirken. Mit der Latenz eng verknüpft ist der sogenannte Jitter. Dieser bezeichnet den Unterschied in der Laufzeit verschiedener

Datenpakete. Bei (sequenziellen) Sprachübertragungen kommen alle Datenpakete idealerweise mit der gleichen Laufzeit an. Ein Jitter-Puffer kann zwar geringe Varianzen ausgleichen, dies geht dann aber zu Lasten der Laufzeit. Zu beachten ist des Weiteren die Paketverlustrate. Gemeinhin gilt ein Wert von fünf Prozent verlorener Pakete noch als tolerabel für die gesprochene Kommunikation. In der Praxis könnte das jedoch schon zuviel sein, wenn einander folgende Datenpakete ausfallen oder große Pakete mit hoch komprimierenden Audio-Codecs verwendet werden.

Service Level klären

Die beschriebenen Anforderungen an eine Sprachübermittlung im geschäftlichen Umfeld legen bereits eine Priorisierung von Daten und garantierte Dienstgütern nahe. Diese kann das Internet mit dem Ansatz des "Best Effort" naturgemäß nicht liefern. Dennoch bieten verschiedene Dienstleister Sprachdienste samt virtueller Telefonanlage im Internet an. Die besonders an Privatkunden oder kleinere Unternehmen gerichteten Lösungen haben durchaus ihren Charme: Es muss kein VoIP/ISDN-Gateway installiert werden, Endnutzer können die Telefonanlage per Webbrowser steuern und weltweit nutzen. Auf die Frage nach der Verfügbarkeit antworten die Anbieter jedoch oft ausweichend. So garantiert Dienstleister Sipgate lediglich eine Verfügbarkeit von 97 Prozent für die eigenen Server. Für die Datenleitungen des Internets kann und will das Unternehmen jedoch weder Garantien noch Erfahrungswerte abgeben. Von den "ziemlich stabilen" Verbindungen könnten sich Interessenten immerhin per kostenlosen, befristeten Test überzeugen.

Für kleine Firmen mag eine solche gehostete Lösung samt SIP-Trunk einen interessanten Ansatz darstellen, um sanft und kostengünstig auf VoIP zu migrieren. Größere Unternehmen sollten bei der Verbindung eigener Telefonanlagen per WAN jedoch mehr fordern. Mit Multiprotocol Label Switching (MPLS) können Datenpakete verbindungsorientiert übertragen werden. Entsprechende Mechanismen für Quality of Service (QoS) bringt das Protokoll bereits mit. Beim Vertragsabschluss mit dem jeweiligen Provider ist jedoch Verhandlungsgeschick gefragt. Die Service Level Agreements sollten nicht nur Aussagen zur Verfügbarkeit der Datenleitung beinhalten. Zusätzlich sollten Administratoren den Provider zu einer garantierten Gesprächsqualität drängen, etwa einen mit ISDN vergleichbaren MOS-Wert von mindestens 4.

Analyse und Update des eigenen Netzes

Bevor Administratoren mit der Implementierung einer umfassenden UCC- oder

VoIP-Lösung beginnen, müssen sie sich zwingend ein grundlegendes Verständnis für die Topologie und Nutzung des eigenen Netzwerks verschaffen. Zu klären ist, wieviele Mitarbeiter gleichzeitig telefonieren und welche Gespräche davon an externe Gesprächspartner vermittelt werden sollen. Ein besonderes Augenmerk gilt dabei den WAN-Verbindungen und externen Mitarbeitern. Die entscheidende Frage hierbei: Gibt es nach außen hin mögliche Flaschenhälse und wie lassen sich diese beheben? Zusätzlich sollten IT-Verantwortliche mögliche Lastspitzen beobachten und wissen, wann FTP-Downloads oder größere Updates anstehen. Eine gewisse Flexibilität nach oben ist sinnvoll, um ein absehbares Wachstum einzuplanen.

Spätestens im Laufe der Umstellung auf eine umfassende UCC-Lösung sollten Administratoren alle Hubs aus dem Netzwerk entfernen. Damit Sprache im LAN vernünftig übertragen werden kann, sind QoS-fähige Switches Pflicht. Unnötiges Kabelgewirr lässt sich umgehen, indem VoIP-Telefone per Ethernet mit Strom gespeist werden. Für Power over Ethernet (PoE) genügen erfahrungsgemäß Cat5-Kabel. Mit diesen lassen sich bereits Distanzen bis zu 80 Metern überbrücken. Prinzipiell spricht auch nichts dagegen, Endgeräte per WLAN ins Firmennetz zu bringen. Cisco etwa bietet mit seiner Lösung "Unified Mobile Communicator" eine entsprechende Lösung für Smartphones verschiedener Hersteller an. Damit mobile Mitarbeiter beim Rundgang durch Büro oder Produktionshalle nicht mit Verbindungsabbrüchen kämpfen müssen, sind die passenden Gegenstellen Pflicht. Um QoS-Kriterien zu entsprechen, sollten die Zugangspunkte den Standard IEEE 802.11e erfüllen. Stand der Technik sind zudem per WLAN-Controller gekoppelte Access Points. Die unterstützen dann auch das Roaming, also die Gesprächsübergabe von einer Funkstation zur nächsten.

Die Sprachqualität messen

Damit eine Echtzeitkommunikation geschäftlichen Ansprüchen gerecht wird, muss

ein reibungsloser Datenverkehr garantiert werden. Optimisten können sich dabei auf vorhandene Ressourcen verlassen, beispielsweise beim Einsatz von Internet-Telefonie über Anbieter virtueller Telefonanlagen. Zusätzlich ließen sich die eigenen Netze entsprechend großzügig dimensionieren. Auf Dauer empfehlenswert ist eine solche Überdimensionierung allerdings nicht. So verschlingen gerade überdimensionierte WAN-Verbindungen unnötig Kosten. Auch technisch spricht einiges gegen ein gedankenloses Erhöhen der verfügbaren Bandbreite. Denn großzügig dimensionierte Netze laden dazu ein, auch großzügig genutzt zu werden. Daher müssen Administratoren die eigene Infrastruktur ständig überwachen, um steigende Bandbreitenansprüche zu erkennen. Wenn zentrale Knoten zusammenbrechen, sind Ausfälle sehr wahrscheinlich. In Spitzenzeiten können auch in überdimensionierten Netzen Verstopfungen auftreten, die dann zu Verzögerungen (Latenz) und Paketverlusten führen. Was für reguläre Datenverbindungen noch akzeptabel wäre, ist für Echtzeitsdienste nicht zu tolerieren.

Die Alternative zur Überdimensionierung ist das so genannte Rightsizing. Der Ansatz wird vorwiegend in GBit-Netzen kleiner und mittlerer Unternehmen genutzt und soll Überlastungen im Netzwerk auf Ausnahmefälle reduzieren, um Jitter und Paketverluste zu minimieren. Grundlage für das Rightsizing ist eine optimierte Netzwerkarchitektur. Diese soll durch eine geringe Anzahl von Hops Engpässe vermeiden. Im Vergleich zur Überdimensionierung lässt sich Rightsizing kostengünstiger umsetzen, erfordert aber ein noch engmaschigeres Monitoring. Wenn Datenströme aber mit Video- oder Sprachdaten um Kapazitäten konkurrieren, stößt auch das Rightsizing an seine Grenzen.

Den Ausweg aus dieser Misere bilden QoS-Verfahren, die Datenströme priorisieren und eine Echtzeitkommunikation bevorzugen. Ein Ansatz hierfür sind Virtuelle LANs (VLANs) auf Layer 2. Sprachkomponenten lassen sich hier einem dedizierten VLAN



zuordnen. Zu beachten ist dabei, dass getrennte, logische Netze nach IEEE 802.1Q eher als Sicherheitskonzept entwickelt wurden. Um eine hinreichende Dienstgüte zu erreichen, setzen die VLANs idealerweise auf dem Standard IEEE 802.1p zur Datenpriorisierung auf. Beim Übergang ins WAN ist es zudem sinnvoll, die VLANs auf entsprechende MPLS-Kanäle zu mappen. Die Kombination IEEE 802.1p/Q priorisiert einzelne Verkehrsklassen, bezieht sich also direkt auf konkrete Anwendungen. Genutzt werden die Verfahren vorrangig für einzelne LANs oder Segmente. Mit Differentiated-Services (DiffServ) steht ein alternatives Verfahren auf OSI-Layer 3 zur Verfügung. Mit DiffServ lassen sich Daten unabhängig von deren Inhalt bevorzugt transportieren. In den Netzwerktopologien mit Level-2- und Level-3-Switches lassen sich beide Verfahren kombinieren.

Ein weiterer QoS-Ansatz ist das Traffic Shaping auf den Layern 2 bis 7. Das Verfahren soll die zur Verfügung stehenden Bandbreiten besser ausnutzen, indem Datenflüsse unidirektional gesteuert werden. Das funktioniert auch ohne Steuerinformationen der Gegenseite. Per Traffic Shaping lassen sich verschiedene Applikationen oder Protokolle gezielt priorisieren. Administratoren können so zeitunkritische Anwendungen zugunsten geschäftskritischer Prozesse deutlich ausbremsen oder ganz anhalten. In der Regel nutzen Traffic-Shaper eine Deep-Packet-Inspection (DPI). Datenpakete werden dabei von speziell angepassten Prozessoren (ASIC) gefiltert.

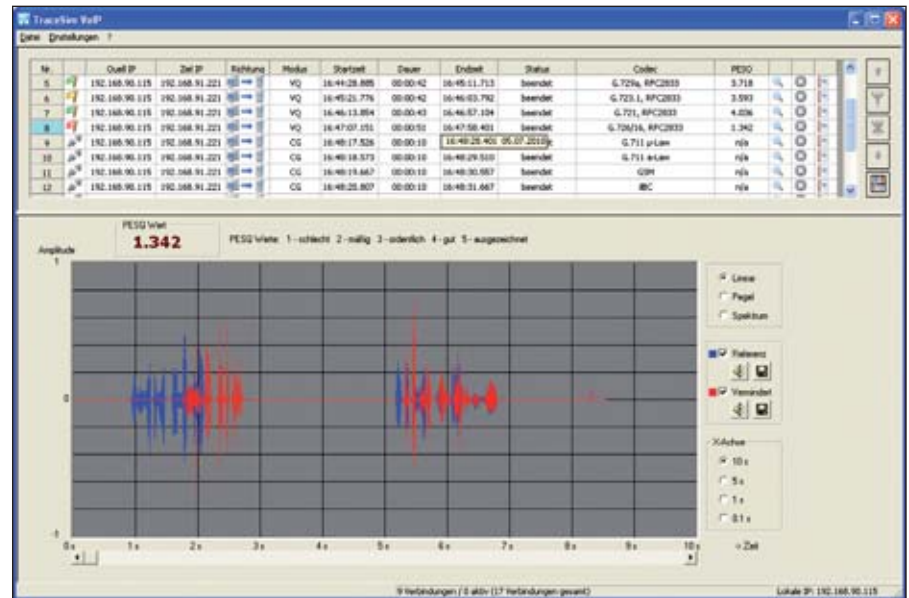


Bild 1: Ein Maßstab für die Sprachqualität ist der PESQ-Wert. Er liegt zwischen -0,5 und 4,5

Sicherheit für Gespräche und Netzwerk

Da im Geschäftsumfeld häufig vertrauliche Informationen ausgetauscht werden, stellt sich auch beim Thema UCC die Frage nach Sicherheit und Datenschutz. Hier sollte jedes Unternehmen eine stimmige Lösung für sich finden – allgemein gültige Aussagen zu diesem Thema bieten sich nicht an. Eine Behauptung lautet etwa, analoge Telefonie und ISDN-Verbindungen seien nicht schwerer abzuhören als unverschlüsselt per IP übertragene Sprachdaten. Wer sich mit dieser laxen Ansicht nicht anfreunden mag, kann Datenströme über verschiedene Wege absichern. Ein erster Schritt wäre bereits die Trennung des sonstigen Datenverkehrs

von Telefongesprächen per VLAN. Zu bedenken wäre ebenfalls eine Tunnelung per Virtual Private Network (VPN). Kommen proprietäre Verschlüsselungsmethoden einzelner Hersteller zum Einsatz, ist darauf zu achten, dass diese durchgehend im Netzwerk unterstützt werden. Probleme könnten beispielsweise bei Verbindungen untereinander nicht kompatibler VoIP-Telefone auftreten. Weitere Fehlerquelle ist die Umsetzung von VoIP-Gesprächen ins herkömmliche Telefonnetz (Public Switched Telephone Network, PSTN).

Auch an anderer Stelle droht Gefahr. Das für das Initiieren von Verbindungen gebräuchliche Session Initiation Protocol

EBOOK
SYSTEMS

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



(SIP) nutzt dynamisch vergebene UDP-Ports. Sollen Verbindungen über Netzwerkgrenzen stattfinden, müssen vorhandene Firewalls entsprechend konfiguriert werden. Das heißt: Ports im Tausenderbereich müssen geöffnet werden – ein Albtraum für Security-Verantwortliche. Ein möglicher Ausweg besteht in alternativen und weniger Port-hungrigen Protokollen, wie dem InterAsterisk Exchange (IAX) der Open-Source-Telefonanlage Asterisk.

Pre-Deployment, Lasttests und Monitoring

Mit der Verlegung von Telefonaten auf das Datennetz fällt auch eine gewisse Redundanz weg. Funktionieren LAN oder WAN nicht, schränkt das die Telefonie komplett oder teilweise ein. Ein generelles Misstrauen in die konvergente Infrastruktur ist jedoch fehl am Platze: In Zeiten von Cloud Computing und geschäftskritischen E-Mails würden funktionierende Telefone bei einem Netzwerkausfall auch nur bedingt weiterhelfen. Grundlegende Gedanken sind dennoch angebracht. So gilt es zu überlegen, ob eine zweite Vermittlungsanlage für den Notfall nötig ist oder ob das eigene Unternehmen auch eine Fehlerbehebung erst am nächsten Werktag übersteht. Gleiches gilt für redundante WAN-Kanäle. Nach allen Vorüberlegungen und Netzupdates mit QoS-fähigen Geräten sollte die Infrastruktur für eine Migration gerüstet sein. So ist von UCC-Anbietern auch gern die Aussage zu hören, dass ein zeitgemäßes Netzwerk reibungslos mit Echtzeitkommunikation zurechtkommen würde. Auch wenn dies prinzipiell stimmen mag, sind Fehlkonfigurationen nie mit letzter Sicherheit auszuschließen. Daher ist es ratsam, die Qualität des Netzwerks mit entsprechenden Tools zu testen. Hierbei gibt es verschiedene Lösungen unterschiedlicher Komplexität. So bietet Paessler mit dem "PRTG Network Monitor" etwa eine Software an, die über Softwareagenten (Sonden) im Netzwerk für VoIP relevante Daten sammelt und auswertet. Das System untersucht dabei Jitter, Paketverzö-

gerung und Paketverlust. Mit den erhobenen Daten sollte sich die VoIP-Qualität eines Netzes gut abschätzen lassen, behauptet der Hersteller.

Systembedingt eignet sich die beschriebene Lösung aber ausschließlich für durchgehende IP-Netze. Außerdem lässt das Werkzeug keine Rückschlüsse auf Qualitätsverluste aufgrund unterschiedlicher Codecs zu. Hier setzt der Softwarehersteller Nextragen mit dem Werkzeug TraceSim VoIP an. Das Tool bewertet Sprachkommunikation End-to-End, über alle Netzwerktopologien und Codec-Umwandlungen hinweg. Die dabei genutzte Methode heißt "Perceptual Evaluation Speech Quality" (PESQ, ITU-Empfehlung P.862) und vergleicht die tatsächliche Sprachqualität mit einem Referenzsignal. Als Ergebnis liefert PESQ eine mit dem MOS-Wert vergleichbare Ausgabe zwischen -0,5 und 4,5. Das Werkzeug simuliert über längere Zeiträume auch ansteigende Netzwerklasten und gibt so wertvolle Anhaltspunkte zur benötigten Bandbreite. Diese Daten lassen sich natürlich auch nach einer Migration nutzen. Unvorsichtige Stresstests und Hunderte von simulierten VoIP-Gesprächen sollte man jedoch außerhalb der Geschäftszeiten durchführen.

Implementierung mit den Mitarbeitern

Zu einer guten Planung gehört auch, den Faktor Mensch mit ins Projekt UCC-Migration einzubeziehen. Wie bereits erwähnt, sind Anwender von ISDN eine hohe Sprachqualität gewöhnt. Gerade bei der Umstellung auf VoIP können gelegentlich aber kleine Störungen auftreten. Es kann nicht schaden, schon im Vorfeld für das Projekt zu werben und Mitarbeiter über den Stand der Migration zu informieren. Ein Migrationsplan hilft dabei, außergewöhnlich wichtige Telefonate eventuell etwas zu verschieben. Empfehlenswert ist ebenso, das Portfolio vorhandener Komfortmerkmale vor und nach der Umstellung zu vergleichen. Zu klären ist etwa, ob eventuell wegfallende Zu-

satzfunktionen verschmerzbar oder nachzurüsten sind. Vielleicht tröstet auch ein Mehrwert der neuen Anlage über die eine oder andere vermeintliche Einschränkung hinweg. Vorteile eines umfassenden Konzeptes sind etwa die enge Integration mit CRM-Systemen oder die Möglichkeit für Videogespräche.

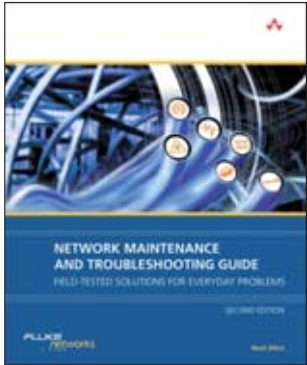
Bei Unternehmen bis zu 200 Mitarbeitern raten Netzwerkexperten zu einer kompletten Migration auf VoIP in einem Rutsch. Die Umstellung ist an einem Wochenende machbar und eine Teilmigration wäre im Einzelfall mit erhöhten Kosten verbunden. Es sei nicht auszuschließen, dass die auszumusternde Telefonanlage dabei nochmals teuer aufgestockt werden müsste, um Gespräche per QSIG weiterzuleiten. Bei Firmen bis zu 500 Anschlüssen kann eine sanfte Migration sinnvoll sein, das hängt jedoch von der Netzwerktopologie ab. Ein zusammenhängender Standort lässt sich logischerweise einfacher umstellen als ein weitschweifiges Filialnetz. Insgesamt sollten die organisatorischen Herausforderungen bei der Umstellung auf UCC/VoIP nicht unterschätzt werden. Während die Konfiguration und Einrichtung des Netzwerks vergleichsweise rasch machbar ist, kann etwa das Auspacken und Anstöpseln hunderter Telefone einige Zeit in Anspruch nehmen.

Fazit

Wurde das Unternehmensnetz erfolgreich auf UCC und VoIP umgestellt, gilt es das Potential des neuen Netzes auch zu nutzen. Das vereinheitlichte Kommunikationsnetz nutzt für Daten- und Sprachdienste nun gemeinsame Router und Zugangsleitungen. Das senkt nicht nur Kosten für Telefonate zwischen verschiedenen Firmenstandorten, sondern sorgt auch für eine einheitliche Administration. Ausnutzen lässt sich das beispielsweise mit flexiblen Routing-Mechanismen, die eingehende Gespräche immer zum passenden Mitarbeiter weiterleiten, ganz gleich, an welchem Standort sich dieser befindet. (dr)



Network Maintenance and Troubleshooting



Vor Fachbüchern auf Englisch schrecken manche Administratoren zurück. Doch beim Grundlagenwerk "Network Maintenance and Troubleshooting" sollten selbst Fremdsprachenmuffel eine

Ausnahme machen. Fundierter und praxisnäher lassen sich Basisinformationen über das Funktionieren des Netzwerks nicht präsentieren. Im Gegensatz zu vielen Büchern, die auf dem Zusammenspiel der Komponenten aufsetzen und das OSI-Schichtmodell als notwendiges Übel auf ein paar Seiten abhandeln, geht Autor Neal Allen anders vor. Er baut auf die sieben Schichten des OSI-Modells als Gliederung auf, jeder Schicht ist ein Kapitel gewidmet. Auf den ersten Seiten jedes Kapitels gibt es zunächst eine ganze Menge an Theorie. Das mag anstrengend sein, ist aber laut Allen wichtig, um die Implikationen von Fehlern auf den spezifischen Schichten zu verstehen. Generell gilt, dass die Ausführungen sehr anschaulich sind. So viel Technik mit so klaren Beschreibungen ist selten zu finden. So ist es allein das Kapitel über Glasfaserkabel wert, sich das Buch anzuschaffen.

Dennoch erfordern besonders die Theorieabschnitte technisches Grundwissen und zumindest mittelmäßige Netzwerkkenntnisse. Doch wer wirklich vom Buch profitieren will, sollte sich die Mühe machen und zumindest einmal den Anfang der Kapitel lesen, um eine Vorstellung der technischen und logischen Zusammenhänge jeder Schicht zu bekommen. Manches mag für gelegentliche Fehlersucheinsätze zu ausführlich sein, beispielsweise die Frame-Zusammensetzung im MAC-Layer der unterschiedlichen Netzwerktechniken. Ab

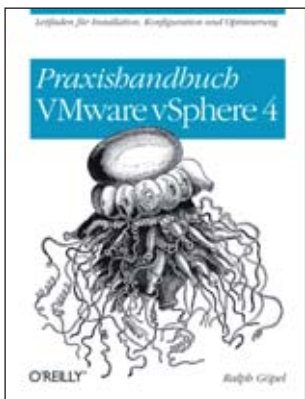
Kapitel 9 geht es dann mit der eigentlichen Fehlersuche los. Auch hier arbeitet sich der Autor von unten nach oben hoch. Dabei kommen zahlreiche Screenshots und Fotos von Fluke-Testgeräten zum Einsatz, Allen ist schließlich Senior Staff Engineer bei Fluke. Fast immer sind die Beispiele aber so beschrieben, dass sie die Leser mit jedem beliebigen Netzwerkanalyzer nachvollziehen können.

Fazit: Das ist das Buch der Bücher für den Administrator, der den Dingen auf den Grund gehen will. Es gibt wohl nichts Besseres, um die Basis der Netzwerktechnik und die Fehlersuche vom Praxisstandpunkt aus kennenzulernen. Allerdings müssen ausreichende Englischkenntnisse vorhanden sein.

Elmar Török

Autor:	Neal Allen
Verlag:	Addison-Wesley
Preis:	28,99 Euro
ISBN:	978-0-321-64741-2
Bewertung:	★★★★★

Praxishandbuch VMware vSphere 4



Für die allermeisten Administratoren ist Virtualisierung mittlerweile ein alter Hut, zumindest die Grundkonzepte sind klar. Dafür haben Dutzende von Fachbüchern und Hunderte von Artikeln gesorgt. Doch wenn es ans Eingemachte

geht und die diffusen Kenntnisse in die Praxis umgesetzt werden sollen, tauchen immer wieder Fragen auf. Die beantwortet, zumindest für VMware vSphere, am besten ein Praxisbuch von Ralph Göpel. Ohne lange Grundlagenklärungen beschäftigt sich der Autor mit den typischen Fragen,

die bei einem Admin mit Vorkenntnissen auftauchen, wenn er vSphere einsetzen will. Die einzelnen Komponenten werden kurz vorgestellt, die Editionen mit ihren Features verglichen und auf Einschränkungen hingewiesen. Alles wird von Göpel knapp, aber exakt beschrieben, wo möglich nutzt er Tabellen und Listen für die einfache Gegenüberstellung.

Durch die griffigen Beschreibungen ist das "Praxishandbuch VMware vSphere 4" der ideale Begleiter für einen Admin, der VMware bereits kennt, aber noch keine Erfahrungen mit vSphere gesammelt hat. Mit dem Buch auf dem Schreibtisch läuft die Installation von Host und VMs schnell und korrekt ab, Nacharbeiten werden vermieden. Die Informationen treffen genau die richtige Balance aus Detailtiefe und Praxisrelevanz: Zu tiefes Einsteigen vermeidet der Autor, weist aber auf mögliche Stolpersteine zuverlässig hin. Neben dem eigentlichen Host wird auch die Ar-

beit mit vCenter Server sowie vApp und VMware Update Manager und Converter beschrieben. Weil Aufsetzen und Konfigurieren nur die Hälfte der Administration ausmachen, gibt es Kapitel über die Datensicherung mit einer Backup-Appliance und die Sicherheit des Hosts und der virtuellen Maschinen.

Fazit: Das "Praxishandbuch VMware vSphere 4" ist ein sehr informatives Buch, das den Umgang mit vSphere praxisgerecht und ohne Lücken abhandelt. Wer Virtualisierung bereits kennt und einen praktischen Begleiter für den ersten Einsatz von VMware vSphere sucht, findet hier den perfekten Begleiter.

Elmar Török

Autoren:	Ralph Göpel
Verlag:	O'Reilly
Preis:	49,90 Euro
ISBN:	978-3-89721-619-8
Bewertung:	★★★★★

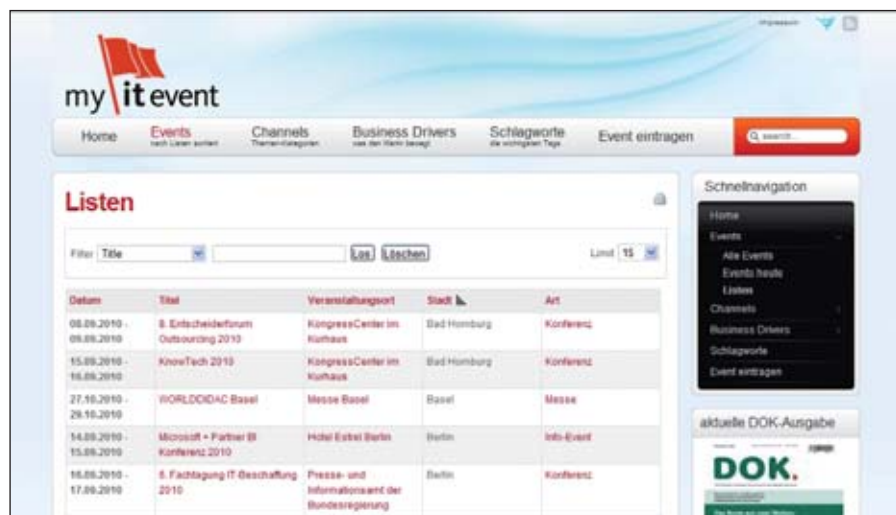
www.my-itevent.de Übersichtlicher IT-Kalender

IT-Events sind fester Bestandteil im Berufsleben eines Admins. Auf ihnen erfahren IT-Profis die aktuellsten Trends, lernen neue Produkte kennen und können Kontakte zu Herstellern und Kollegen knüpfen. Neben den üblichen Großveranstaltungen à la Cebit und seit 2009 die it-sa zählen hierzu auch kleinere Hausmessen und Vortragsreihen. Doch da jeder Veranstalter für seine eigene Messe oder Kongress wirbt, fällt der Überblick über die verschiedenen Termine oft schwer. Und so ärgert sich so mancher über ein verpasstes Event, das er gerne besucht hätte.

Abhilfe schafft hier die Website my-itevent.de. Auf dem Portal, das sich selbst als Online-Terminkalender für die traditionellen "Musts" der Branche wie auch die regionalen Events der Dienstleister, Hersteller und Anwender sieht, finden sich in unterschiedlichen Kategorien zahlreiche Terminhinweise. Dabei lassen sich die eingetragenen Events nach dem Veranstaltungsort, der Art des Events – also Konferenz, Messe, Workshop, Social Event oder Info-Event – sowie nach Titel und Datum sortieren. Da-

neben haben die Nutzer der Seite die Möglichkeit, ihren Termin in neun thematischen Bereichen zu suchen, darunter Business Applications, IT-Management oder Recht & Sicherheit. Schließlich hilft noch eine Volltextsuche weiter, sollte sich die gewünschte Veranstaltung partout nicht finden lassen.

Derzeit weist der Online-Kalender rund 190 Einträge auf. Insgesamt sollen es seit der Gründung des Portals 754 sein. Als kleines Schmankerl bietet die Seite dabei auch eine per Maus steuerbare Suchwolke, die die wichtigsten Schlagworte auflistet. Zudem gibt es auf my-itevent.de die Möglichkeit, eigene Veranstaltungen kostenfrei einzutragen. Um zu verhindern, dass reine Werbeveranstaltungen dabei ihren Weg in den Kalender finden, schaltet der Anbieter die Einträge erst nach einer Prüfung frei. Auch kurze Events, die nur wenige Stunden dauern, sowie Zertifizierungen haben auf der Plattform nichts verloren. Übrigens, auch unter www.it-administrator.de/seminar-markt/ finden Sie regelmäßig IT-Veranstaltungen chronologisch sortiert und mit weiterführenden Informationen versehen. Und für Events außerhalb der IT-Branche bietet sich ein Besuch auf eventfinder.de an. Dort kann auch der Admin mal bei einer gemütlichen Lesung oder einer Operette abschalten und den Alltag hinter sich lassen. (dr)



Auf my-itevent.de finden Sie wichtige IT-Veranstaltungen übersichtlich aufgelistet

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:**

Anwenderbericht:

Wasserdichtes Disk-Backup

Die Anwaltskanzlei Baker & McKenzie beschäftigt weltweit mehr als 13.000 Mitarbeiter in 70 Büros. Eine der größten Herausforderungen bei der Datensicherung besteht darin, dass Juristen sehr selten Dokumente löschen. Gleichzeitig müssen die Anwälte stets Zugriff auf die digitalen Dateien haben. Lesen Sie in unserem Online-Fachartikel, wie das Unternehmen über ein zentrales, Disk-basiertes Backup für Sicherheit sorgt und durch die integrierte Deduplizierung gleichzeitig Speicherplatz spart.

www.it-administrator.de/themen/storage/fachartikel/86697.html

Virtualisierung erfordert neues Sicherheitsdenken

Nach der Server- und Storage-Virtualisierung folgt in einer zweiten nicht weniger heftigen Welle derzeit die Desktop-Virtualisierung. Leider vernachlässigen viele Unternehmen dabei die Sicherheit. Zwar scheinen auf den ersten Blick virtuelle Ressourcen den gleichen Bedrohungen ausgesetzt wie in der physischen Welt. Dennoch versagt hier oft das etablierte Konzept des Sicherheitsperimeters. In unserem Beitrag im Web stellen wir Ihnen einen neuen Ansatz vor, um die Herausforderungen meistern zu können.

www.it-administrator.de/themen/virtualisierung/fachartikel/86698.html

Nutzen von Cloud Storage Services

Storage-Dienstleistungen in der Wolke sind derzeit eine vieldiskutierte Angelegenheit. Für derartige Angebote existieren jedoch unterschiedliche Einsatzmöglichkeiten. In unserem Online-Artikel setzen wir uns mit dem Nutzen von Cloud Storage Services in den Themenfeldern Backup, Failover und Webhosting sowie im Rahmen eines Content Delivery Networks auseinander. Außerdem erklären wir, warum eine hybride Lösung mit eigenem Storage und zusätzlich gemieteten Kapazitäten gerade für kleinere Unternehmen interessant ist.

www.it-administrator.de/themen/storage/fachartikel/86699.html

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

»Benutzer sind oft interessante Ideengeber«

Marcel Engel (36) ist als Leiter für die IT-Administration am Standort Hamburg-Altona des Johann Heinrich von Thünen-Instituts (vTI) verantwortlich. Das vTI ist eines von vier Bundesforschungsinstituten im Geschäftsbereich des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV). In 15 Fachinstituten wird an verschiedenen Standorten fachgebietsübergreifend in den Bereichen Ökonomie, Technologie, stoffliche Nutzung nachwachsender Rohstoffe, Klima, Biodiversität und ökologischer Landbau geforscht.

Welche Ausbildung haben Sie gemacht?

Ursprünglich bin ich gelernter Kfz-Mechaniker, habe aber später ein Informatikstudium mit der Fachrichtung Netzwerk und Kommunikation aufgenommen und erfolgreich abgeschlossen.

Warum sind Sie IT-Administrator geworden?

Ich arbeite gern mit Computern und Servern, brauche aber auch die Benutzer als Feedback und Ideengeber. Am Beruf des Administrators gefallen mir besonders der hohe Praxisanteil sowie das breit gefächerte Betätigungsfeld.

Welche IT-Umgebung betreuen Sie?

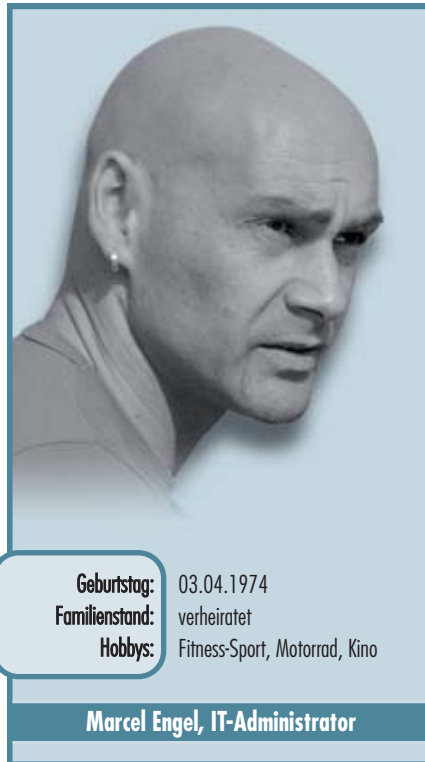
Ich bin für das Johann Heinrich von Thünen Institut am Standort Hamburg-Altona der leitende IT-Administrator. Mein Kollege Siegfried Schneider und ich betreuen die IT-Umgebung von drei verschiedenen Instituten mit sieben Servern. Wir setzen auf die Netzwerkbetriebssysteme Windows 2003 oder 2008 und haben zusätzlich eine Firewall sowie ein Routersystem installiert. Insgesamt betreuen wir 180 PCs für ebenso viele Arbeitsplätze. Im Anwendungsbereich nutzen wir Standardapplikationen wie MS Office, setzen aber auch Open Source-Lösungen wie Firefox oder Thunderbird ein. Darüber hinaus laufen in den jeweiligen Abteilungen zusätzlich noch fachspezifische Programme.

Welches Netzwerk- und Systemmanagement nutzen Sie?

Wir nutzen bislang nur die Verwaltungstools der Windows-Server. Allerdings denken wir gerade darüber nach, den System Center Configuration Manager (SCCM) von Microsoft einzuführen.

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

An erster Stelle steht für uns die Zufriedenheit der Benutzer. In einer komplexen Forschungs-Umgebung ist es von beson-



Geburstag: 03.04.1974
Familienstand: verheiratet
Hobbys: Fitness-Sport, Motorrad, Kino

Marcel Engel, IT-Administrator

derer Wichtigkeit, dass es keine Systemausfälle gibt und alle benötigten Anwendungen einwandfrei laufen, damit Abläufe und Forschungsprojekte nicht stillstehen.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Die wichtigste Aufgabe für uns Administratoren ist es momentan, die Zentralisierung und Virtualisierung unserer IT-Landschaft weiter voranzutreiben.

Was macht Ihnen an Ihrem Job am meisten Spaß?

Mir gefällt es, dass ich in meinem Beruf immer wieder Neues erkunden und neue Technologien kennen lernen kann. Darüber hinaus gefällt mir der direkte Kontakt mit den Usern, die uns auch wichtige Impulse für unsere Arbeit geben.

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

Die Entsorgung von Altgeräten gehört zu den wenigen Dingen, die ich an meinem Job gar nicht mag.

Was tun Sie für Ihre Fort- und Weiterbildung?

Ich suche im persönlichen Gespräch den regelmäßigen Austausch mit Kollegen. Darüber hinaus bediene ich mich aus den Informationspools von Internet-Foren und -Portalen.

Was war der größte persönliche Flop oder Fehler, den Sie gemacht haben?

Einen Tag vor meinem Sommerurlaub habe ich eine Software auf einem Server installiert, ohne vorher ein Backup zu machen. Dank Murphys Gesetz ging natürlich alles schief, was schief gehen kann. Die Folge war eine Nachtaktion mit einer vollständigen Server-Neuinstallation.

Was war Ihr größter Erfolg als IT-Administrator?

Stolz bin ich darauf, dass es mir gelungen ist, im Rahmen der Neueinführung einer Software die Einweisung und Schulung für rund 350 Leute zu planen und erfolgreich zu realisieren.

Was war der dümmste Anwenderfehler, der Ihnen untergekommen ist?

Ein Anwender hatte etliche Male auf Icons geklickt und sich hinterher bei mir über die vielen offenen Fenster auf seinem Monitor beschwert.

Was sehen Sie als die größte Herausforderung der IT in den nächsten drei Jahren?

Die stetige Virtualisierung aller Komponenten wird im IT-Umfeld eine der größten Herausforderungen sein. Da spielt dann auch die Sicherheits- und Storage-Problematik mit hinein. 

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 11/10 erscheint am 3. November 2010

Schwerpunktthema:

Storage

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

Unsere Ausgabe im **Dezember** hat sich zum Schwerpunkt **WiFi, VoIP und WLAN-Management** gesetzt. In einem unserer Tests nehmen wir den Trafficlyser TraceSim VoIP von Nextagen unter die Lupe. In den Workshops befassen wir uns unter anderem mit der Priorisierung von Datenströmen und effizienten Sniffing-Methoden.

Als Schwerpunkt im **Januar** folgt dann das Thema **Virtualisierung**.

Im Test: Dot Hill AssuredSAN 3000

Einkaufsführer: Solid State Storage

Workshop: Database Availability Groups in Exchange 2010

Workshop: Hochverfügbares SAN im Eigenbau

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

Redaktion

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

Daniel Richey (dr), *Stellv. Chefredakteur*
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, Florian Frommherz,
Marc Grote, Jürgen Heyer, Adam Hufnagel, Thomas Joas,
Nils Kaczinski, Robert Lindemeier, Sandra Lucifora,
Ulf B. Simon-Weidner, Dirk Srocke, Florian Thiessenthusen,
Elmar Török, 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 Triltsch
Print und digitale Medien GmbH
Johannes-Gutenberg-Straße 1-3
97199 Ochsenfurt-Hohestadt

Vertrieb

Anne Kathrin Heinemann
Vertriebsleitung
kathrin@it-administrator.de
Tel.: 089/4445408-20

Abo- und Leserservice

Vertriebsunion Meynen GmbH & Co. KG
Stephan Orgel
Große Hub 10
65344 Elville
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 vorbehalten. Reproduktionen und Verbreitung, gleich welcher 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 Zeichnungen frei von gewerblichen Schutzrechten sind.

Haftung

Für den Fall, dass in IT-Administrator unzutreffende Informationen oder in veröffentlichten Programmen, Zeichnungen, Plänen oder Diagrammen Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlags oder seiner Mitarbeiter in Betracht. Für unverlangt eingesandte Manuskripte, Produkte oder sonstige Waren übernimmt der Verlag keine Haftung.

Manuskript-Einsendungen

Die Redaktion nimmt gerne Manuskripte an. Diese müssen frei von Rechten Dritter sein. Mit der Einsendung gibt der Verfasser die Zustimmung zur Verwertung 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 Elville
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

Baramundi	S. 13	it-sa 2010	S. 41
compTIA	S. 25	LANCOM	S. 02
DeviceLock	S. 11	Log.in Consultants	S. 47
Giritech	S. 84	Matrix42	S. 27
Hewlett Packard	S. 21	NETGEAR	S. 65

Paessler	S. 37
SNW	S. 29
VM goes 2010	S. 67

INSERENTENVERZEICHNIS

Die Ausgabe enthält eine Teilbeilage der Firma
Galileo Computing.



Erscheinungstermin:
Ende Oktober 2010

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 Abonummer (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

Geldinstitut: _____

Kto.: _____

BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

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

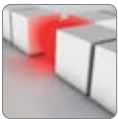
ITA 1010

Grenzenloser Zugriff auf
die Cloud und virtualisierte IT

Mobile Enterprise · Mobile Workplace · Collaboration · Secure Mobility

G/On™ - Workplace der Zukunft. Ohne Limits!

Client-Virtualisierung - Aufwand und Kosten senken



G/On unterstützt den Zugriff auf virtualisierte Clients oder Streamed Applications in einfachster Weise - zentral gemanaged, zuverlässig und mit drastisch reduziertem Verwaltungsaufwand.

Business Continuity - Arbeiten in Krisensituationen



Nicht nur Pandemie-Szenarien, auch Elementarschäden können den Normalbetrieb verhindern. G/On sorgt für störungsfreies Arbeiten, zum Beispiel konfigurationsfrei vom privaten PC aus.

Cloud Computing - unternehmensübergreifend

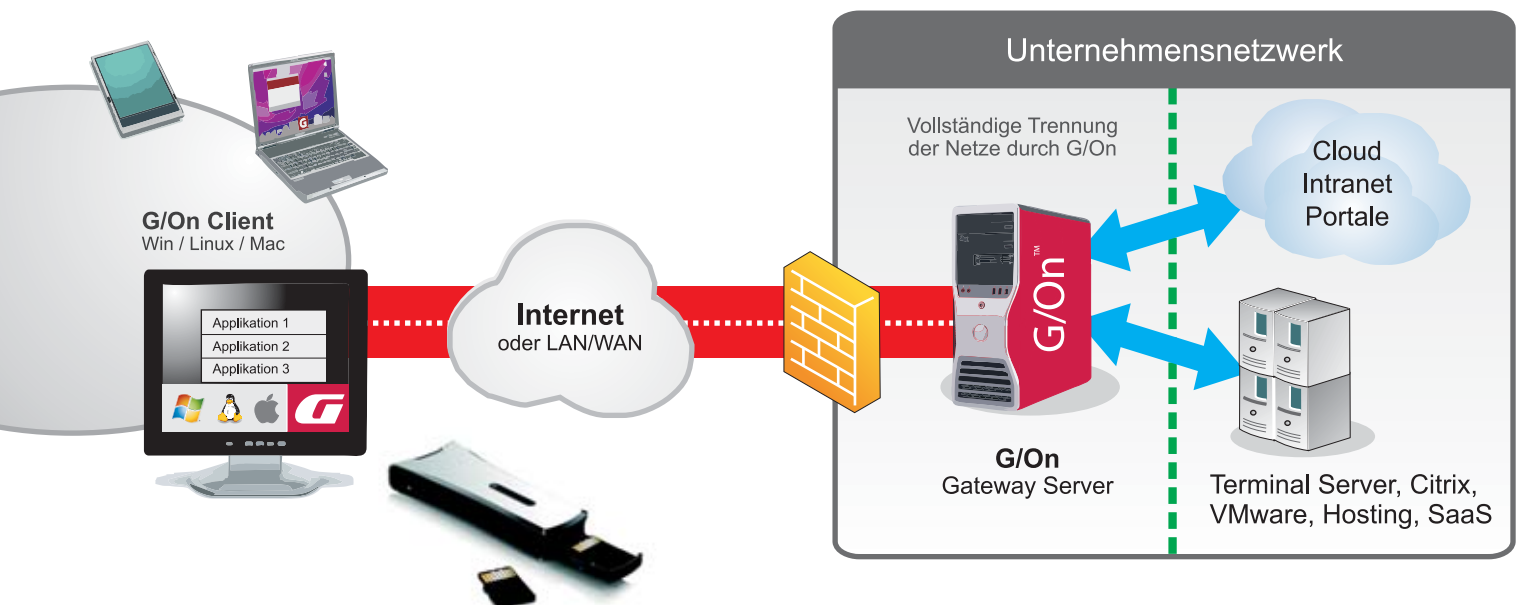


G/On sorgt für flexiblen und in höchstem Maße sicheren Access, damit Organisationen Ihren Nutzern unternehmensübergreifende Cloud-Services anbieten können.

Collaboration - Einbindung von Außenstellen & Partnern



In Minuten ermöglichen Sie externen Benutzern einen G/On-gestützten Zugriff auf definierte Applikationen, ohne dabei die Sicherheit des Unternehmens zu gefährden.



Giritech ist offizieller Partner von

T-City Friedrichshafen

Ein Gemeinschaftsprojekt der
Deutschen Telekom und der Stadt Friedrichshafen

Success Stories, Videos und Downloads auf
www.giritech.de