IT-ADMINISTRATOR.DE

03/2010

€ 12,60 ISSN 1614-2888

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

Rechenzentrums-ausstattung

Intelligente Technologien für einen smarten Planeten

Wie man Flexibilität ins Unternehmen einbaut.

Bis heute wenden Unternehmen Milliarden auf, um automatische Systeme zu entwickeln, die vertikale Prozesse im Unternehmen steuern – wie ERP, CRM, SCM. Das Manko dabei: Diese Systeme waren nie dafür geschaffen, um miteinander zu kommunizieren. Kein Wunder also, wenn jeder Mitarbeiter durchschnittlich über 5 Stunden pro Woche vergeudet, weil er mit ineffizienten Insellösungen arbeiten muss. Die umfassenden Business Process Management-Lösungen von IBM dagegen verbinden all diese isolierten Prozesse und ermöglichen so reibungslose Abläufe. Schon über 5.000 Unternehmen hat IBM geholfen, die nötigen Einblicke in alle Bereiche zu erlangen und Prozesse zu automatisieren – um schneller auf eine wechselnde Nachfrage zu reagieren und intelligenter zu arbeiten: von einem Logistik-Unternehmen, das seine Entwicklungskosten um 30 % senkte, bis hin zu einem Energie-Unternehmen, das seine Ölfelder in Echtzeit überwacht und so seine durchschnittliche Ausbeute verdoppelt.

Smarte Unternehmen brauchen intelligente Software, Systeme und Services.
Also: Machen wir den Planeten ein bisschen smarter. Wie, erfahren Sie unter ibm.com/bpm/de

IBM

smarter together
IBM auf der CeBIT 2010
2. bis 6. März, Halle 2 & 9
ibm.com/de/cebit

O&M IBM IT 4/10

EDITORIAL

Einen Gang hochschalten

Liebe Leser,

haben Sie sich je gefragt, warum Amerikaner eigentlich Sportwagen kaufen? Die passende Infrastruktur für die teuren Flitzer fehlt und bei 75 Meilen pro Stunde ist auf den Highways Schluss. Auch in Deutschland, dem Traumland vieler Autofahrer, sieht die Lage oft nicht besser aus. Verstopfte Autobahnen, ewige Baustellen und zahllose LKWs – welcher Sportwagen-Liebhaber oder Vielfahrer kann davon kein Lied singen. Ein Blick auf den Hefttitel ist jetzt übrigens nicht nötig, Sie halten tatsächlich den IT-Administrator in Händen. Nur was hat das alles mit Ihrem Netzwerk zu tun?

Stellen Sie sich vor, Sie haben Ihren Serverraum soeben mit neuen Hochleistungsblades ausgestattet, um Ihren Usern die nötigen Applikationen zu bieten. Was am anderen Ende des Netzwerks jedoch an Performance ankommt, entspricht nicht gerade dem, was Sie reingeschickt haben. Paket-Stau. Mühsam quälen sich die Datenpäckchen von Voice over IP, Online-Anwendungen, VPN und Co. durch die Engpässe im LAN. Ihnen fehlt die passende Infrastruktur. Natürlich hätten wir Sie die vorangegangenen Zeilen nicht lesen lassen, gäbe es keine Abhilfe. Sie heißt 10-GBit-Ethernet. Zunächst als kaum möglich und dann als zu teuer abgetan, wird die Technologie nun marktreif. Was derzeit Stand der Dinge ist, zeigen wir Ihnen ab Seite 46. Und wie Ihre Switches auch mitziehen und nicht zu überlasteten Autobahnkreuzen verkommen, erfahren Sie ab Seite 76.

VoIP als zeitkritische Applikation reagiert besonders empfindlich, wenn es um Verzögerungen im Netz geht. Mit den richtigen Messungen und Hangriffen lässt sich der Weg für die Sprachpakete freischaufeln, wie die Teilnehmer in unserem VoIP-Workshop Ende Februar erfahren konnten. Ein Aspekt, der jedoch nicht in Vergessenheit geraten sollte, ist die Sicherheit. Können Angreifer den IP-basierten Sprachverkehr doch wesentlich leichter abhören als ISDN-Verbindungen. Ab Seite 61 lesen Sie, welche Ansätze sich hierfür am besten eignen: Vorhang auf für IPSec, S/MIME, SRTP und SCTP. Damit kommen Ihre VoIP-Pakete nicht nur rechtzeitig, sondern vor allem sicher beim Empfänger an.

Und nun viel Spaß beim Lesen unserer extra-dicken März-Ausgabe.

Ihr

Daniel Richey,
Stellv. Chefredakteur IT-Administrator

LANCOM

. . . connecting your business

Made in Germany

VPN von LANCOM.
Das Beste für Ihr Netz!

Hochverfügbarkeit, Virtualisierung, Kostenkontrolle, Voice – bei VPN geht es heute um mehr als „nur" die sichere Vernetzung von Standorten.

Mit VPN Routern, Gateways und Clients von LANCOM erfüllen Sie spielend alle Anforderungen. Ganz egal, ob für HomeOffices, mobile User, mobile Netzwerke oder Tausende von Filialen.

Von „One-Click-VPN" und dem praktischen Budget-Manager im VPN Client über den UMTS-Router mit Hochverfügbarkeitsgarantie bis zum neusten VPN Gateway mit ungekannter Performance – LANCOM vernetzt Standorte schnell und sicher, über alle DSL-Anschlüsse, WLAN oder UMTS.

VPN von der deutschen Nummer EINS! Exzellenter Service & kostenlose Updates inklusive.

CeBIT
HANNOVER
2.– 6. 3. 2010
HALLE 13
STAND C28
kostenlose Tickets
www.lancom.de/
cebit2010

LANCOM
Systems

www.lancom.de

INHALT

IT-Administrator – Ausgabe März 2010

Rechenzentrumsausstattung

Im Test: Matrix42 Package Robot 8.5

Jede Software erfordert bei der Installation individuelle Eingaben oder Angaben zur Personalisierung, die bei einer bedienerlosen Einrichtung automatisch beantwortet werden müssen. Wer zur Lösung dieses Problems nicht gleich in eine komplexe Softwareverteilung investieren möchte, für den kann Package Robot diese Automatisierung übernehmen. IT-Administrator hat genauer untersucht, wie gut sich mit diesem Tool komfortable Installationen und Deinstallationen sowie allgemeine Prozessabläufe ohne weitere Benutzereingaben paketieren lassen.

Seite 24

Remote-Administration mit UltraVNC

Für Administratoren gibt es kaum etwas Lästigeres, als sich von PC zu PC hangeln zu müssen, um dort – oft durch unsachgemäße Handhabung verursachte – Probleme zu lösen. Der Arbeitsablauf lässt sich mit dem richtigen Werkzeug erheblich optimieren: Greifen Sie doch zur freien Remote-Software UltraVNC. In diesem Workshop erklären wir Ihnen den Umgang mit diesem Werkzeug und beschreiben dessen wichtigste Kniffe.

Seite 40

Themenübersicht

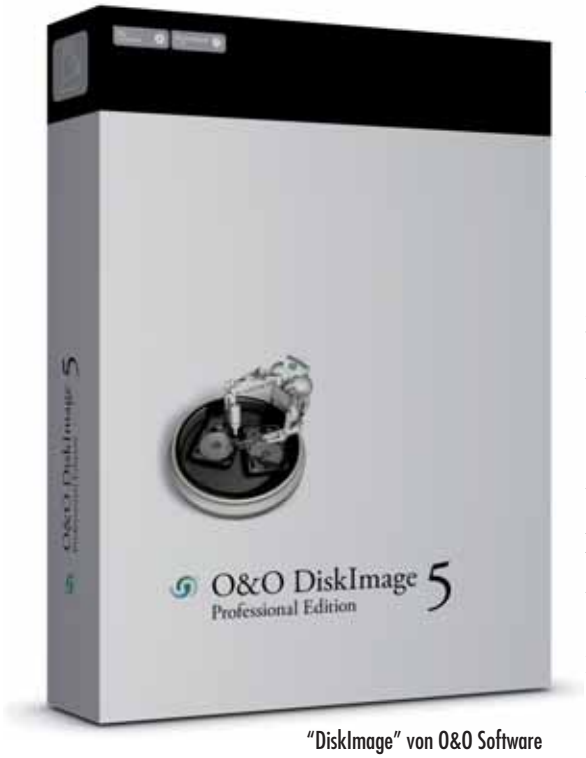
- Server- und Systemmanagement
- Clientmanagement
- Storage
- Sicherheit
- Messaging
- Virtualisierung
- Netzwerkmanagement
- Job/Weiterbildung
- Recht

Neue Router für VPN, WLAN und UMTS

Funkwerk bietet sechs neue Router der Reihe **Bintec RS** an. Alle Geräte unterstützen Hardware-beschleunigte IPSec-Tunnel. Zudem beinhalten die Router für den Anschluss an das Netzwerk einen GBit-Ethernet-Switch und erlauben das Einrichten einer Demilitarisierten Zone (DMZ). Das kleinste Modell, der Router **RS120**, verfügt über fünf GBit-Ethernet-Ports, die frei für LAN, WAN oder DMZ konfiguriert werden können. Die Variante **RS120wu** bietet zudem ein integriertes UMTS-Modem mit HSxPA, EDGE, GPRS und GSM-Unterstützung. Diese lassen sich sowohl als primäre Internet-Anbindung oder als Backup verwenden. Für eine schnellere DSL-Anbindung eignet sich das Modell **RS230a**. Das integrierte ADSL 2+ Modem des Routers unterstützt den ADSL-Standard Annex A (ADSL over POTS) nach ITU G992.1. Das Gerät verfügt, wie auch seine größeren Brüder der RS23x-Reihe, ab Werk bereits über eine Lizenz für fünf Hardware-beschleunigte IPSec-Tunnel. Die WLAN-Variante heißt **RS230aw** und funkt, wie auch der kleinere **RS120wu**, im 802.11n-Standard. Schließlich stehen für mittlere Umgebungen noch die Modelle **RS232b** beziehungsweise die WLAN-Version **RS232bw** zur Verfügung. Diese Geräte bieten zu den ADSL-Anschlüssen noch eine ISDN-Unterstützung. Ab sofort sind die Netzwerkschaltstellen für 200 bis 600 Euro erhältlich. Ausnahme: Die Modelle RS230a und RS230aw sollen erst im Mai auf den Markt kommen. *(dr)*

Funkwerk: www.funkwerk-ec.com

Die neue Router-Familie von Funkwerk umfasst sechs Modelle mit und ohne Wireless-N-WLAN



"DiskImage" von O&O Software kommt bei der Rückspielung von System-Abbildern auch mit veränderter Hardware zurecht

Flexible Systemschnappschüsse

O&O Software stellt **Version 5** des Tools **DiskImage** vor. Mit der Software lassen sich nun auch Images auf Systemen mit abweichender Hardware einspielen und nutzen. So können nach dem Zurückspielen der Sicherung Anpassungen an die neue Hardware durchgeführt und das System wieder bootfähig gemacht werden. Mit dem Tool lässt sich zudem die Identität (Computername und Computer-SID) verändern, um etwa die Sicherheit in Arbeitsgruppenumgebungen sowie für Wechselmedien im Netzwerk zu gewährleisten. Dies kann beim Ausrollen einer Systemsicherung auf mehrere Rechner im Netzwerk nützlich sein. Zudem lassen sich im laufenden Betrieb Sicherungen einzelner Datenträger oder ganzer Systeme durchführen, um Ausfallzeiten eines Produktivsystems zu vermeiden. Die Snapshot-Funktionalität mit integriertem Pufferspeicher garantiert, dass die gesicherten Daten exakt dem Stand zum Zeitpunkt des Sicherungsbeginns entsprechen: Änderungen am Datenbestand durch Anwendungen oder Benutzer wirken sich laut Hersteller nicht auf die laufende Sicherung aus. Für Nutzer der Kommandozeile unterstützt DiskImage zudem Skriptbefehle und ermöglicht es daneben, Sicherungen von virtuellen Festplatten des Typs Microsoft Virtual Hard Disc (VHD) in Sicherungsdateien von DiskImage zu konvertieren und umgekehrt. Die O&O DiskImage 5 Workstation Edition ist als Volumenlizenz verfügbar und kostet bei Abnahme von fünf Lizenzen 35 Euro pro Lizenz. *(dr)*

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

Großalarm bei Netzwerkangriff

COMCO bringt mit **IntraPROTECTOR Advanced Edition 2010** die neueste Version seiner **Security-Suite** auf den Markt. Die Software soll in insgesamt drei Schritten für Sicherheit im Unternehmensnetzwerk sorgen. An erster Stelle steht die Inventarisierung der gesamten Netzwerk-Infrastruktur, anschließend erfolgt die Implementierung von **Network Access Control**. Als letzten Schritt lassen sich zum Schutz vor internen Netzwerkangriffen weitere Module aktivieren. Die Lösung greift nicht nur auf die Analyse einzelner Datenpakete zurück, sondern nutzt über SNMP und Syslog die vorhandene Netzwerk-Infrastruktur, um Informationen über Sicherheitsverstöße oder Security-Meldungen zu sammeln und Abwehrmaßnahmen auszuführen. Zu den wesentlichen Funktionsmerkmalen und Neuerungen des IntraPROTECTOR gehört eine Adress-Datenbank, die nur zugelassene Netzwerkteilnehmer akzeptiert. Ist ein Gerät nicht bekannt, sendet das System einen Alarm und trennt den unbekannten Teilnehmer mittels Portabschaltung vom Netzwerk oder leitet ihn in ein Quarantäne-Netz um. Das Reporting-Modul erstellt Berichte und Analysen zur Dokumentation oder Erfüllung von Compliance-Vorgaben. Das System bietet zudem eine revisionssichere Shadow-Datenbank sowie ein mehrstufiges Berechtigungskonzept. Personenbezogene Daten werden dabei nicht analysiert. Neben der Möglichkeit, die Software auf VMware-Basis zu betreiben, ist das System auch als Appliance erhältlich. Die Sicherheits-Suite ist ab sofort verfügbar und kostet als Software in der Advanced Edition inklusive Lizenzen für 100 Clients 2.300 Euro. *(ln)*

COMCO: www.comco.de/intraprotector/

Überarbeitete Firewall

Stonesoft erweitert mit der **Firmware-Version 5.1** den Funktionsumfang der **StoneGate Firewall/VPN** und des **StoneGate Management Center** im Bereich Netzwerksicherheit und -management. Die neuen Versionen bieten einen optionalen Web-Filter (URL-Filter) und unterstützen drahtlose 3G-Netzwerkverbindungen sowie 64-Bit-Betriebssysteme. Dadurch sollen sie besser vor komplexen Netzwerkbedrohungen schützen, die Netzwerkleistung erhöhen und die Ereignisverwaltung von Fremdgeräten verbessern. Mithilfe der neuen Web-Filter-Option lässt sich nun der Zugriff auf bekannte Malware- und Phishing-Websites blockieren. Darüber hinaus gewährleistet eine umfassende URL-Datenbank mit Millionen von URLs in 77 Kategorien laut Hersteller eine vollständige Transparenz aller Webbrowsing-Aktivitäten. Administratoren können den Zugriff auf Websites kontrollieren, indem sie weitere Kategorien direkt zu den Sicherheitsrichtlinien der Firewall hinzufügen. Dank individuell anpassbarer Berichts- und Protokollfunktionen lassen sich die Webbrowsing-Aktivitäten in Echtzeit oder mithilfe von terminierten Übersichtsberichten verfolgen. StoneGate Firewall/VPN 5.1 unterstützt zudem nun auch drahtlose 3G-Schnittstellen als primäre oder Backup-Verbindung. Die StoneGate-Firewall FW-310 kostet beispielsweise 1.990 Euro zuzüglich 398 Euro für das Web-Filtering. *(dr)*

Stonesoft: www.stonesoft.de

Die StoneGate-Firewalls von Stonesoft erhalten mit Firmware-Version 5.1 mehr Funktionen

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

Mit Modell **ESW-520-24P** bringt **Cisco** einen neuen **Switch für den KMU-Einsatz** in den Verkauf. Das Gerät verfügt über 24 Fast-Ethernet-Anschlüsse, zwei GBit-Uplink-Ports sowie zwei Kombinations-Steckplätze, die sich mit optionalen SFP-Modulen bestücken lassen. Die PoE-Funktion versorgt die Anschlüsse jeweils mit maximal 15,4 Watt. Zugriffskontrolllisten dienen der Zugriffsbeschränkung auf sensible Netzwerkabschnitte, die Priorisierung von verzögerungsempfindlichem Netzverkehr erfolgt gemäß IEEE 802.1p. Die Netzwerkkomponente ist ab sofort für rund 700 Euro erhältlich. *(ln)*

www.cisco.de/mittelstand/

GDS bietet kleineren Geschäftskunden ein kostengünstiges Komplettpaket für Vor-Ort- und Online-Backup. Neben dem Erstellen eines lokalen Images auf einem externen Speichermedium erfolgt ein per AES verschlüsseltes Online-Backup. Die Sicherung geschieht dabei auf Basis des Programms NovaBACKUP xSP. Das Einstiegspaket für 15 Euro stellt 2 GByte an Speicherplatz bereit, der redundant in zwei Rechenzentren gesichert wird. Im Preis enthalten sind technischer Support und Virenschutz. *(ln)*

www.online-sicherung.net

Ipswitch stellt **Version 7.5** des **WS_FTP Servers** vor. Das neue Release soll einen sicheren Austausch von Dateien innerhalb und zwischen Organisationen ermöglichen. Es unterstützt hierfür Verschlüsselung, Authentifizierung, End-to-End-Überwachung und ein umfassendes Management von File Transfers. Dateien können nun auch sicher aus Microsoft Outlook oder einem Web-Browser heraus verschickt werden. Für 546 Euro ist der FTP-Server erhältlich. *(dr)*

http://de.wsftp.com/products/ws_ftp_server/

FrontRange gibt die Verfügbarkeit von **Discovery 9** bekannt. Die Software für das **Software Asset Management** (SAM) ermöglicht es, physikalische und virtualisierte Umgebungen zu verwalten. IT-Verantwortliche können mit der neuen Version ab sofort auch virtualisierte Komponenten wie Server, Desktops oder Anwendungen auf Thin Clients automatisch erkennen und administrieren. Zudem liefert das Werkzeug alle Daten vom Guest-Host-Verhältnis für virtualisierte Umgebungen: von der Anzahl der physikalischen CPU-Kerne pro Host, der CPU-Geschwindigkeit, dem zur Verfügung stehenden Hauptspeicher, den PCI-Anwendungen und BIOS-Prozessen bis hin zu Software-Angaben wie Hersteller, ESX-Version und Versionsnummer. Discovery 9 unterstützt VMware ESX 3.5, Virtual Server 2.0, Workstation 6.5 sowie Microsoft Hyper-V. Bei Thin Clients lassen sich zudem sämtliche Citrix XenApp-Umgebungen der Versionen 4.5 und 5.0 verwalten. Je nach Netzwerkgröße fallen pro Client Kosten ab 34 Euro an. *(ln)*

www.frontrange.com/discovery/

Anwendungen unter Überwachung

Riverbed präsentiert mit **Cascade 8.4** eine neue Version seiner Software zur Analyse und zum Monitoring von **Netzwerkverkehr und Anwendungsperformance**. Neu sind eine ausgebaute Reporting-Funktion und ein verbessertes Zusammenspiel mit anderen Produkten zur **WAN-Optimierung** des Herstellers. Cascade kommt auf den gleichnamigen Appliances zum Einsatz und beruht auf einem behavioristischen Ansatz: Die Lösung misst kontinuierlich die Performance beim Endanwender und erlernt dabei das normale Netzwerk- und Anwendungsverhalten. Die Analyse, die auf per Netflow-Protokoll übermittelten Messdaten beruht, beinhaltet mehrere Kennzahlen: Der Anwendungsdurchsatz gibt die Werte an, mit denen Applikationsdaten das Netz durchqueren. Der Datendurchsatz pro Nutzerverbindung ist ein Parameter für die subjektive Geschwindigkeits-Einschätzung des Endanwenders. Die Verbindungsdauer kommt zum Tragen, wenn die Performance von transaktionsorientierten Anwendungen untersucht werden soll. Weiterhin führt Riverbed mit dem **Cascade Sensor-VE** eine rein Software-basierte Komponente ein, die als Sensor für die virtualisierte Riverbed Services Platform (RSP) fungiert. Dabei handelt es sich um eine virtualisierte Partition auf der Appliance **Steelhead**. Auf diese Weise will der Hersteller die Messung der Anwendungs-Performance in Niederlassungen vereinfachen, da dort nur noch der virtualisierte Sensor auf bereits bestehender Hardware zum Einsatz kommt und keine zusätzliche Cascade-Appliance mehr nötig ist. Der Preis der Installation richtet sich nach der Anzahl der überwachten UDP/TCP-Verbindungen und beginnt bei 30.000 US-Dollar. *(ln)*

Die Appliance "Cascade" von Riverbed misst über einen Software-basierten Sensor auch die Anwendungs-Performance in Außenstellen

Riverbed: www.riverbed.com/products/cascade/

Appliance gegen Daten-Dubletten

FalconStor Software bringt **Version 2.0** des **FalconStor File-Interface Deduplication System** (FDS) auf den Markt. Die Lösung richtet sich an kleine bis mittelgroße sowie an große Unternehmen, die Speicherplatz und -kosten reduzieren möchten. Dank eines Aktiv-Passiv-Clusterings ermöglicht die Appliance nun den hochverfügbaren Betrieb. In Kombination mit Symantecs OpenStorage (OST) bietet das Deduplication System zudem 5,4 TByte pro Stunde Durchsatz an Backup-Daten sowie eine Ingest-Rate von 1,5 GByte pro Sekunde über zwei 10-GBit-Ethernet-Verbindungen. Über ein verbessertes Replikationsdashboard können IT-Verantwortliche die Arbeit des Systems in Echtzeit überwachen, während die Lösung nun auch eine granularere Replikation auf Ordner-Ebene unterstützt. Eine Kollisionsvermeidung soll daneben die Datenkonsistenz gewährleisten und Datenverlust verhindern. Die virtuelle Appliance des FDS startet bei 2.400 Euro mit 1 TByte Deduplizierungs-Repository. Die Storage Appliances (SA307R) mit 7 TByte Deduplizierungs-Repository sind ab 36.000 Euro verfügbar. *(dr)*

FalconStor: www.falconstor.com

Switches für die Datenautobahn

Für den Netzwerk-Core stellt **Extreme Networks** zwei neue **BlackDiamond-8900-XL-Module** mit 48 GBit-Ethernet-Ports sowie eine XL-Variante mit acht 10-GBit-Ethernet-Ports vor. Durch ihre Portdichte und effiziente Bauweise sollen es die Module auch großen Rechenzentren ermöglichen, die Schichten in ihrem Netzwerk zu reduzieren und gleichzeitig immer mehr virtuelle Maschinen zu unterstützen. Die ebenfalls neuen hochskalierbaren **Layer-2/3-Switches Summit X480** gibt es in festen Konfigurationen mit bis zu 48 10/100/1000-Ethernet-Ports sowie mit einem Slot für einen Uplink mit 40 GBit/s. Die Geräte saugen Frischluft an der Vorderseite an und führen ihre Abluft an der Geräterückseite ab. Beide integrierte Netzteile sowie die Lüfter sind während des Betriebes austauschbar. Bis zu acht dieser Switches lassen sich per Stacking-Technologie stapeln und als ein virtuelles Chassis verwalten. Diese virtuellen Chassis ermöglichen es Rechenzentren, 1,8 TBit/s an Switching-Kapazität in einem einzigen administrierten Gerät zu kontrollieren. Ein optionaler VIM2-Slot für 40-Gigabit-Ethernet nimmt ein mit vier Ports ausgestattetes 10-Gigabit-Ethernet-Uplink-Modul oder ein Stacking-Modul auf, die einen Durchsatz von 40 GBit/s beziehungsweise 128 GBit/s ermöglichen. Die Preise für die Summit-X480-Switches beginnen bei 10.495 US-Dollar. Die BlackDiamond-8900-XL-Module sind ab 16.795 Dollar erhältlich. *(dr)*

Extreme Networks: www.extremenetworks.de

Die neuen Summit X480-Switches von Extreme Networks bieten bis zu 48 GBit-Ethernet-Ports

PROSECURE™ SECURITY ARCHITECTURE BY NETGEAR

ALL-IN-ONE SECURITY. REALTIME.

NETGEAR ProSecure UTM:
Web- und E-Mail-Sicherheit für KMUs

UTM5/UTM10/UTM25:
Router, Application, Proxy Firewall, VPN, IPsec & SSL VPN für bis zu 30 User

Die neuen ProSecure **U**nified **T**hreat **M**anagement Appliances garantieren als All-in-one-Lösung ein Höchstmaß an Sicherheit und Performance für Web- und Mailanwendungen in kleinen und mittleren Unternehmen zu einem äußerst attrraktiven Preis.

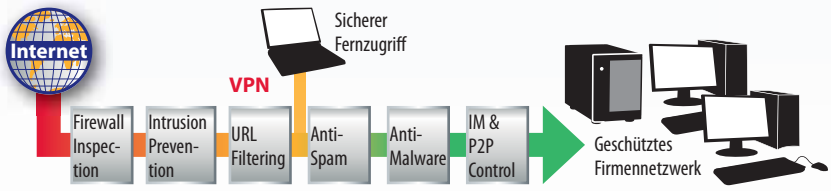
Sie können umfassende Viren- und Malware-Datenbanken von NETGEAR und Sophos bei hoher Performance einsetzen. Die flexible, modulare Architektur der UTM-Linie überprüft Dateien und Datenverkehr bis zu fünf mal schneller als konventionelle Methoden.

NETGEAR bietet kleinen und mittleren Unternehmen außerdem den Support erfahrener Sicherheitsexperten.

- Mail-, Web-, FTP- und Netzwerksicherheit bei hoher Performance.
- Real Time Protection durch stündliche Updates
- Einfaches Management und unkomplizierte Konfiguration
- Keine nutzerabhängigen Lizenzgebühren
- Über 1.000.000 Antivirus Signaturen
- ICSA Labs certified

Mehr Infos unter:
www.prosecure.netgear.de

NETGEAR Green



CeBIT
HANNOVER 2.–6.3.2010

Besuchen Sie uns auf der CeBIT:
Halle 14/15 (Planet Reseller) Stand Nr. K35
und in Halle 11 Stand Nr. D03

PROSUPPORT™

Das NETGEAR Serviceportfolio. Sichern Sie Ihr Netzwerk mit unserem Serviceangebot OnCall 24x7 oder mit dem XPressHW Hardwareaustausch.

NETGEAR® SMB SOLUTIONS

Alle NETGEAR® ProSafe-Produkte sind auf Basis von Enterprise-Technologien nach strengsten Qualtitätsmaßstäben hergestellt, um höchste Performance und Funktionssicherheit für kleine und mittlere Firmennetzwerke zu bieten – kostengünstig und bedarfsgerecht erweiterbar.

NETGEAR®
PROSAFE®
BUILT FOR BUSINESS

IT-Administrator-Workshop "Virtualisierung mit Hyper-V R2" am 22. April 2010 in Köln

Hyper-VWorkshop

von John Pardey

Mit dem Release der zweiten Version des Microsoft-eigenen Hypervisors Hyper-V positionieren sich die Redmonder gezielt in einem Marktsegment, das bisher von VMware dominiert wurde. Hyper-V Server 2008 R2 bietet etwa mit der Live-Migration neue Features, die den produktiven Einsatz attraktiver machen sollen. Zwar wird VMware nicht müde zu betonen, dass das eigene Produkt einen technologischen Vorsprung habe, aber dieser Vorsprung besteht eben nicht nur in der Technologie, sondern auch im Preis. So prüfen derzeit sicher nicht wenige IT-Verantwortliche, inwieweit Hyper-V R2 aktuellen Anforderungen gerecht wird. Unser Workshop im April wendet sich dieser Fragestellung zu, indem wir einerseits die Leistungsfähigkeit des Hypervisors unter die Lupe nehmen und andererseits den Aufbau sowie die Verwaltung einer Hyper-V-Infrastruktur beleuchten.

Einer auf der VMworld 2009 vorgestellten Studie der Burton Group zufolge ist Hyper-V R2 nicht reif für den Einsatz in produktiven Umgebungen. Dass Platzhirsch VMware diese Studie mit Begeisterung aufgegriffen und "vermarktet" hat, ist kaum verwunderlich. Zentrale Aussage dieser Studie ist, dass es Hyper-V R2 an drei zentralen Features mangelt, als wichtigstes die Fault Tolerance. Letztendlich bewertet die Studie Microsofts Hypervisor mit knapp 90 Prozent in Bezug auf die "erwarteten" Bewertungskriterien, die Konkurrenz von VMware und Citrix erreichte die vollen 100 Prozent. Blicken wir in die Historie von Microsoft-Produkten aller Art, dürfte IT-Verantwortlichen ein sehr kostengünstiges "90 Prozent-Produkt" in der ein oder anderen Form bekannt vorkommen. Und so verwundert es wenig, dass sich IT-Abteilungen aufgrund des nicht zu vernachlässigenden Potentials zur Kostenreduktion intensiv mit dem neuen Hyper-V beschäftigen.

Planung und Administration

So werfen wir auch im Rahmen unseres Workshops zunächst einen vergleichenden Blick auf die drei großen Hypervisoren. Die Teilnehmer erhalten einen guten Einblick in die Leistungsfähigkeit der verschiedenen Lösungen. Allerdings ist der Hypervisor an sich nur ein Teilaspekt, sowohl der Kosten- als auch der Technologiebetrachtung. So wenden wir uns im Anschluss daran der Planung einer Hyper-V-Implementierung zu und zeigen auf, was in Sachen Storage und Host auf Sie zukommt. Und natürlich fehlt im Rahmen eines IT-Administrator-Workshops nicht der technische Blick unter die Haube sowie Tipps und Tricks für den laufenden Betrieb. So nehmen wir Hyper-V R2 nach Abschluss der Planung in Betrieb und zeigen Ihnen die Arbeit mit den wichtigsten neuen Features, wie der angesprochenen Live-Migration, aber auch den Snapshots und vieles mehr. Den Abschluss bildet ein Block zu den Managementtools für Hyper-V.

Schnell anmelden!

IT-Verantwortliche und Administratoren, die Hyper-V im Unternehmen einsetzen oder dies planen, sollten diesen Workshop nicht verpassen. Die Anmeldeinformationen finden Sie im Kasten auf dieser Seite. Der für alle Abonnenten kostenlose Workshop steht ab sofort zur Registrierung offen und wir würden uns freuen, Sie Ende April bei unserem Workshoppartner und Gastgeber sepago in Köln begrüßen zu dürfen.

iTANet
Die System und Netzwerk User Group

Die Agenda des Workshops

13.00 Uhr: Begrüßung

13.15 Uhr: Hyper-V Server 2008 R2

- Leistungsfähigkeit von Hyper-V R2 unter der Lupe – Gegenüberstellung mit XEN/VMware
- Planung der Hyper-V-Installation (Storage-Planung und Kapazitätsplanung auf dem Host)
- Was alles unter der Haube steckt (Snapshots, Live-Migration, Backup)
- Management des Hyper-V mit SCVMM

Dozenten: sepago GmbH, Köln

17.30 Uhr: Ende des Workshops

Ort: sepago GmbH,
Dillenburger Straße 83,
51105 Köln

Teilnahmegebühren:
Für IT-Administrator Abonnenten kostenlos.

Anmeldung bis zum 16. April unter
www.it-administrator.de/workshops/

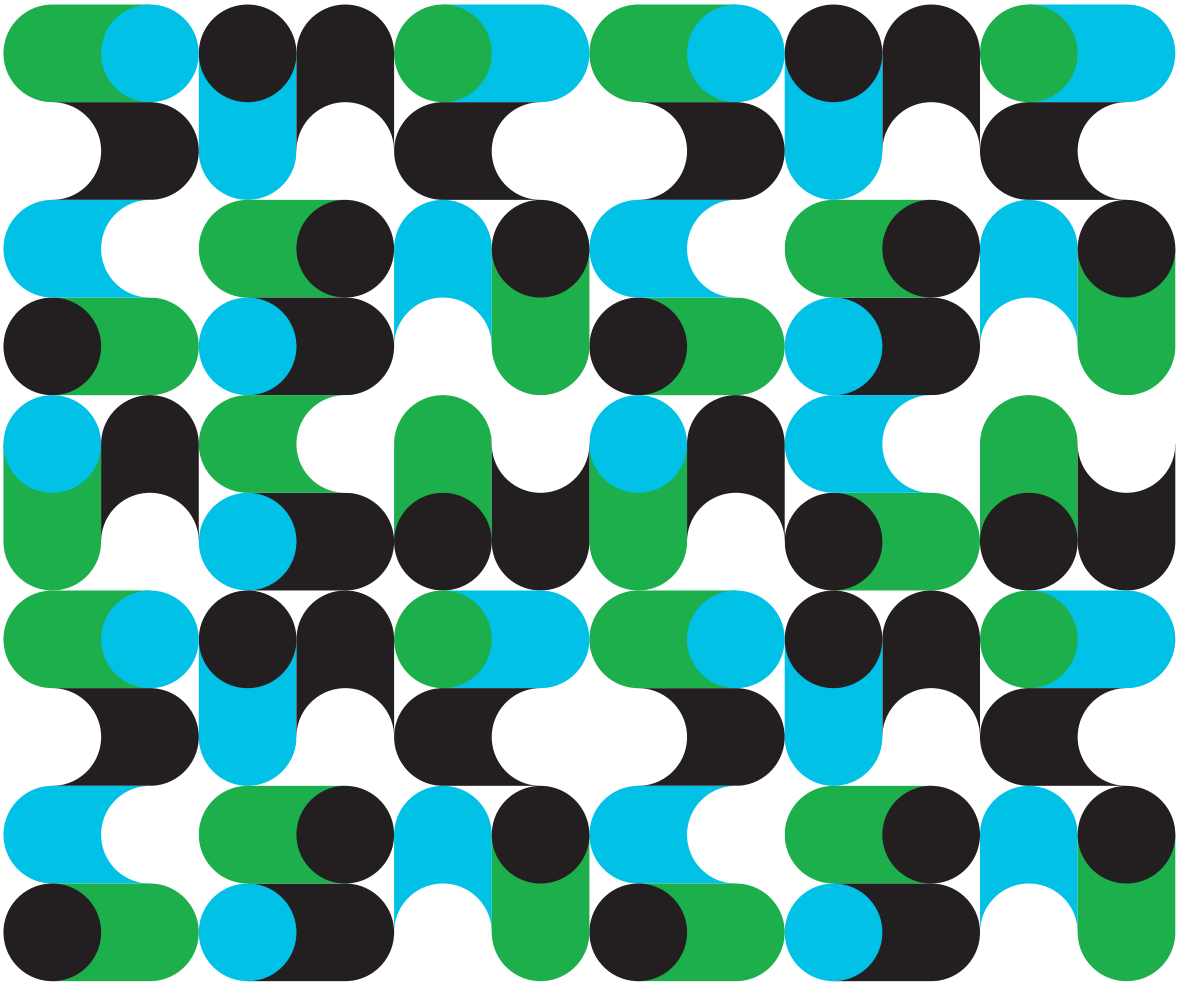
Workshop "Virtualisierung mit Hyper-V R2" am 22. April

Intelligente Technologien für einen smarten Planeten

Wie wird die IT zum Nervensystem des gesamten Unternehmens?

Das Rechenzentrum ist heute weit mehr als nur das Herzstück der IT, es ist das Nervenzentrum des ganzen Unternehmens. IBM unterstützt Unternehmen dabei, ihre IT nicht als Ansammlung einzelner Teile zu sehen, sondern als integriertes System, das alle digitalen und realen Bestandteile des Unternehmens mit dem Rechenzentrum vernetzt – und so eine weitaus vielseitigere Infrastruktur schafft: von Bahnlinien, die ihre Wartung selbst im Voraus organisieren, über Produktionsanlagen, die sich selbsttätig neuen Anforderungen anpassen, bis hin zu Stromnetzen, die Angebot und Nachfrage automatisch ins Gleichgewicht bringen. An solchen Lösungen arbeitet IBM gemeinsam mit Tausenden von Kunden. Für besseren Service, mehr Flexibilität und bis zu 50 % weniger Betriebskosten.

Smarte Unternehmen brauchen intelligente Software, Systeme und Services.
Also: Machen wir den Planeten ein bisschen smarter. Wie, erfahren Sie unter ibm.com/infrastructure/de



smarter together
IBM auf der CeBIT 2010
2. bis 6. März, Halle 2 & 9
ibm.com/de/cebit

O&M IBM IT 7/10

Im Test: Tandberg Data VTL DPS1100 und DPS1200

Wie eine Fata Morgana

von Jürgen Heyer

Nicht nur bei Servern hat sich die Virtualisierung durchgesetzt, auch bei teuren Tape Libraries hält dieser Trend Einzug. Statt eines komplexen Gebildes aus Bandlaufwerk und Wechsler-Einheit erledigt bei der DPS1000-Serie von Tandberg Data ein als Appliance konfigurierter, kompakter Standardserver diesen Job schneller und preiswerter. IT-Administrator hat die Virtual Tape Library bezüglich ihrer Stärken und Schwächen genauer unter die Lupe genommen.

Mit den Modellen DPS1100 und DPS1200 hat Tandberg Data zwei Virtual Tape Libraries (VTL) auf den Markt gebracht, die auch kleineren Unternehmen einen preiswerten Einstieg in diese Technik ermöglichen. Die von uns getestete DPS1100 ist letztendlich ein kompakter Server in 19-Zoll-Rackbauweise mit einer Bauhöhe von 1 U (45 Millimeter), in Administratorkreisen auch "Pizzablech" genannt. Die DPS1200 ist mit 2 U doppelt so hoch.

Bessere Performance beim Disk-Backup

Eine VTL ist in der Regel ein Server mit einem Plattenarray entsprechender Größe, der nach außen hin eine Tape-Library (auch Tape-Silo, Tape-Jukebox oder auf Deutsch Bandbibliothek genannt) mit einem oder mehreren Bandlaufwerken und diversen Schächten für die Bänder emuliert. Dadurch, dass sich die Appliance nach außen hin genau wie eine Bandbibliothek verhält, lässt sie sich sehr einfach mit herkömmlicher Backupsoftware wie beispielsweise CA Arcserve, Symantec Backup Exec oder Tivoli Storage Manager ansprechen. Im Übrigen soll eine derartige virtuelle Bibliothek das klassische Backup auf Bänder nicht unbedingt ersetzen, sondern vielmehr effizienter und schneller machen sowie die Performance und Zuverlässigkeit von Festplatten mit der langfristigen Sicherheit sowie den niedrigen Kosten von Bändern kombinieren. Das Schlagwort hierfür ist Backup-to-Disk-to-Tape (B2D2T). Aufgrund der Emulation können bisherige Backup-Konzepte wie beispielsweise die Großvater-Vater-Sohn-Sicherung (GFS) beibehalten werden. Die Sicherung erfolgt aber nicht direkt auf ein Band, sondern in eine VTL und damit auf Festplatten.

Eine VTL bietet den Vorteil, dass die Datensicherung mit optimaler Geschwindigkeit abläuft und sich das Plattensystem optimal an den Datendurchsatz anpasst. Bei echten Bandlaufwerken ist der Shoeshine-Effekt gefürchtet, wenn die Daten nicht mit ausreichender Geschwindigkeit beim Bandlaufwerk angeliefert werden. Bei diesem Problem reißt der Datenstrom am Bandlaufwerk immer wieder ab, das Laufwerk muss ständig vor- und zurückspulen und sich neu positionieren. Dabei verschlechtert sich zum einen die Performance massiv. Zum anderen erfahren die Bänder eine sehr hohe Beanspruchung und verschleißen dadurch deutlich schneller. Mit einer VTL-Lösung lässt sich diese Problematik sicher umgehen. Trotzdem können die virtuellen Bänder auf richtige Bänder in einer physikalischen Library ausgelagert werden. Dies kann tagsüber entkoppelt von der Produktion und mit für die Bandlaufwerke optimierter Geschwindigkeit erfolgen. Bei diesem Vorgang handelt es sich im übertragenen Sinne nur um ein Umkopieren von Bändern.

Kompakte, aber laute Technik

Die von uns getestete VTL DPS1100 von Tandberg Data basiert auf einem Server von Supermicro mit einem angeschlossenen Plattensystem. Eingebaut ist ein Raid-Controller Areca-1212 mit 256 MByte Cache, der vier SAS-Festplatten (Seagate Barracuda ES.2) mit 7200 Umdrehungen pro Minute und je 750 GByte Kapazität anspricht. Diese sind als Raid 5 konfiguriert, so dass abzüglich der Betriebssystempartition die Nutzkapazität rund 2 TByte beträgt. Der Hersteller gibt hier 3 TByte an, wovon sich Interessenten jedoch nicht täuschen lassen sollten, denn dies ist eine reine Bruttoangabe. Wie bei physikalischen Bandlaufwerken kommt aber auch die übliche Kompression zum

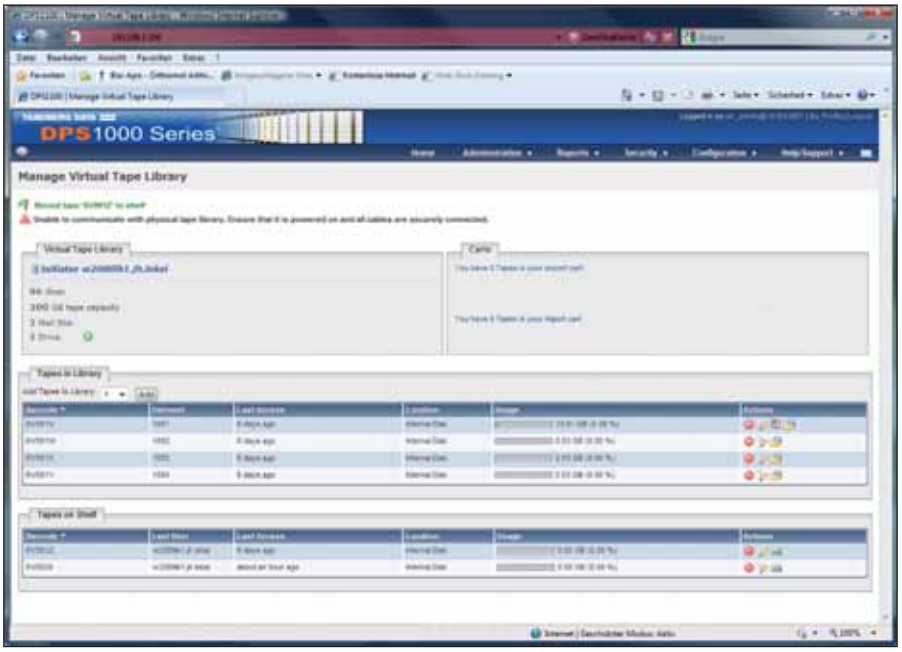


Bild 1: Die Admin-Weboberfläche liefert zu jeder angelegten VTL umfassende Informationen zur Datenbelegung

Tragen, so dass sich – abhängig von den Datentypen – in der Regel zumindest die doppelte Datenmenge speichern lässt.

Als 19-Zoll-Einschub mit einer Dicke von einer Höheneinheit ist das Gerät sehr kompakt, mehrere entsprechend kleine Lüfter mit einem unangenehm hohen Geräusch machen es aber auch sehr laut. Der Betrieb in einem vom Arbeitsbereich abgetrennten Serverraum ist unbedingt erforderlich. Im Test war das Surren auch außerhalb des Labors bei geschlossener Tür noch gut zu hören. Bei dem verwendeten Servergehäuse ist zu beachten, dass der obere Deckel nicht nur durch zwei einfach lösbare Rasten verschlossen, sondern zudem noch einmal seitlich verschraubt ist. Das ist für den RZ-Einsatz nicht optimal, da die kleine Schraube schnell herunterfallen kann und dann unter Umständen in einem Lüftungsschlitz verschwindet. Die Stromversorgung erfolgt über ein fest verschraubtes Netzteil, ein redundanter Betrieb mit zwei Netzteilen und gegebenenfalls von zwei Stromschienen ist bei der DPS1100 nicht möglich. Nur die DPS1200 verfügt über redundante Netzteile. Zumindest aber sind die Festplatten in Hot-Plug-Rahmen eingebaut, um im laufenden Betrieb gewechselt werden zu können. Die Kapazität der DPS1100 lässt sich über zwei eingebaute SAS-Anschlüsse mittels Erweiterungseinheiten (DPS Expansion Module) vergrößern. Jedes Modul hat wiederum 7,5 TByte Nutzkapazität und es lassen sich insgesamt fünf anschließen, so dass sich eine Gesamtgröße von 39 TByte ergibt.

Die DPS1100 ist als Appliance konzipiert und wird komplett vorkonfiguriert geliefert. Als Betriebssystem kommt die Linux-Distribution Fedora 6 (Kernel 2.6.19) zum Einsatz, der administrative Zugriff erfolgt über ein Web-Interface. Die Verbindung der DPS1100 mit den zu sichernden Systemen geschieht via LAN, wozu die Library zwei GBit-Anschlüsse besitzt, auf denen iSCSI aktiviert ist. Die DPS1100 unterstützt auch Jumbo Frames, Voraussetzung für eine Nutzung ist allerdings, dass alle Komponenten bis hin zum sichernden Server diesen Paket-Typ unterstützen.

Einfache Inbetriebnahme

Da die Library, wie bei einer Appliance üblich, vorkonfiguriert ist, sind für deren Betrieb keine Linux-Kenntnisse erforderlich. An die DPS1100 lassen sich zwar auch Monitor, Maus und Tastatur anschließen, dies ist jedoch nicht auf Dauer notwendig, hilft aber am Anfang beim Auslesen der per DHCP empfangenen IP-Adresse oder der Vergabe einer festen Adresse. Die notwendigen Schritte sind detailliert in einer Schnellstartanleitung beschrieben. Im normalen Betrieb erfolgt die Administration durch eine Web-Oberfläche. Dabei wird eine sichere SSL-Verbindung eingerichtet, anfangs mit einem selbstsignierten Zertifikat, welches die DPS1100 erzeugt. Dieses lässt sich später auf Wunsch durch ein offizielles Zertifikat ersetzen. Standardmäßig sind für die Administration zwei Benutzer mit etwas unterschiedlichen Rechten angelegt. Der normale "admin" in der Rolle eines Application-Administrators ist für die grundlegende Konfiguration wie IP-Adresse, Alarmierung und so weiter zuständig. Der "str_admin" ist der Rolle Storage-Administrator zugeordnet, die für die Einrichtung der iSCSI-Initiatoren, das Anlegen weiterer Benutzer sowie die Konfiguration der Library-Funktionen (Auslagern von Bändern, Hinzufügen eines weiteren virtuellen Laufwerks et cetera) autorisiert ist. Bezüglich des Anlegens weiterer Benutzer sei erwähnt, dass es nur genau die zwei erwähnten Rechterollen gibt, die sich auch nicht ändern lassen. Inwiefern also das Anlegen mehrerer Benutzer Sinn macht, sei dahingestellt, der Vorteil besteht allenfalls darin, dass sich innerhalb der Log-Dateien Aktivitäten der verschiedenen Benutzer nachvollziehen lassen.

Damit die Zeitangaben in den Logs und in den Benachrichtigungsmails stimmen, ist der Abgleich mit einem NTP-Server möglich. Für den Mailversand unterstützt die DPS1100 SMTP. Hier ist zu beachten, dass das Modell mit den Standardeinstellungen kaum Mails verschickt, sondern nur bei kritischen Sicherheitsvorkommnissen. Der Versand bei Problemen mit der Speichereinheit, den Platten, dem Raid-System und dem System an sich muss erst mit Vorgabe des Schweregrads (Info, Warnung, Fehler, Kritisch) eingerichtet werden. Besser wäre es hier unseres Erachtens, standardmäßig erst einmal möglichst alles zu melden. Der Administrator kann dies dann reduzieren, wenn es ihm zu viel ist. Wer aber zu Beginn die Einstellungen nicht modifiziert,

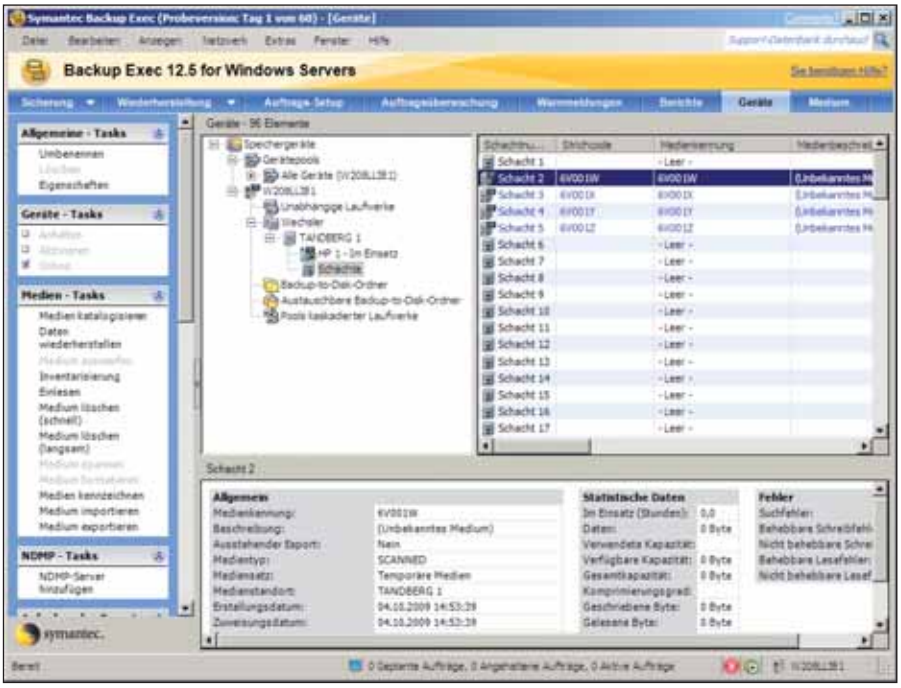


Bild 2: In Verbindung mit Symantec Backup Exec wird die DPS1100 automatisch erkannt, so dass der Wechsler mit Laufwerk und Schächten ohne weitere Aktionen als Sicherungsziel verwendet werden kann

wiegt sich womöglich bei einem gravierenden Fehler in trügerischer Sicherheit. Gut ist, dass die Benachrichtigung wahlweise an bestimmte angelegte Benutzer, eine Rolle oder auch beliebige Mailadressen erfolgen kann. SNMP findet übrigens keine Unterstützung.

Wie schon eingangs erwähnt, geschieht die Anbindung an die zu sichernden Server mittels iSCSI. Für jeden Initiator legt die DPS1100 automatisch eine VTL mit einem Laufwerk, fünf Bändern und 96 Slots an. Für eine iSCSI-Namensauflösung unterstützt das Gerät iSNS (Internet Storage Name Service), in kleineren Umgebungen kann aber ebenso ohne diese Funktion gearbeitet werden. Standardmäßig ist hinsichtlich einer iSCSI-Verbindung keinerlei Authentisierung aktiviert, was auch bedeutet, dass für jeden Initiator, der den Betrieb aufnimmt, ohne weitere Prüfung eine VTL wie beschrieben eingerichtet wird. In einer Produktionsumgebung ist daher eine Authentisierung mittels CHAP dringend zu empfehlen, wobei dann jeder Initiator, der Zugriff erhalten soll, vorher durch einen Benutzer in der Rolle des Storage-Administrators angelegt werden muss.

Wenn nicht zu viel Wechsel stattfindet, ist es auch denkbar, am Anfang alle Initiatoren der zu sichernden Server ohne Authentisierung an der Library automatisch anlegen zu lassen, dann auf CHAP umzustellen und nur die entsprechenden Passwörter nachzutragen. Ist die VTL einmal konfiguriert, lassen sich die Einstellungen speichern und auch wiederherstellen.

Problemlose Anbindung an Zielserver

Getestet haben wir die DPS1100 in Verbindung mit mehreren Windows 2008-Servern und der Sicherungssoftware Symantec Backup Exec. Zuerst ist auf dem Windows-Server iSCSI zu aktiveren, was aber sehr einfach durch den Programmaufruf des Verwaltungstools geschieht. Darin ist eine Verbindung zur Library zu konfigurieren. Wird ohne CHAP gearbeitet, legt die DPS1100 tatsächlich sofort nach der iSCSI-Anmeldung eine VTL mit einem Laufwerk und fünf Bändern an. Im Gerätemanager werden daraufhin ein HP Ultrium-3-Bandlaufwerk und ein anfangs unbekannter Medienwechsler sichtbar. Durch eine Online-Treiberaktualisierung wird letzterer schließlich auch erkannt, wobei dies bei uns im Labor nicht zwingend erforderlich war, da Backup Exec seine eigenen Treiber nutzt und alle Komponenten bereits kennt.

Innerhalb der Sicherungssoftware sind die Komponenten somit ebenfalls sichtbar und können als Backup-Ziel verwendet werden. Für den Anwender macht es nun absolut keinen Unterschied, ob er tatsächlich eine physikalische Bandbibliothek anspricht oder eine VTL. Im Handbuch ist die Konfiguration anderer Sicherungsprodukte gut beschrieben, wobei es letztendlich nur darum geht, eventuell passende Treiber einzuspielen, da sich wie bei Backup Exec auch an der Handhabung der Sicherungssoftware nichts ändert.

Ausbaufähiges Bandmanagement

Wie schon erwähnt, legt die Library standardmäßig für jeden Initiator ein virtuelles Bandlaufwerk mit 96 Schächten und fünf Bändern an. Über das Web-Portal der DPS1100 lassen sich sowohl weitere Bänder anlegen als auch zusätzliche Sicherungslaufwerke ergänzen. Gut ist, dass sich jederzeit virtuelle Bänder in ein sogenanntes Shelf auslagern lassen, was verhindert, dass diese weiter benutzt werden. Maximal 100 Hostverbindungen werden unterstützt, davon können höchstens 64 gleichzeitig aktiv sein. Auf die gleiche Menge sind die virtuellen Bandlaufwerke begrenzt. Auf Wunsch können für einzelne Bänder sprechende Namen vergeben werden. Das ist für die Verwaltung an sich nicht notwendig, hilft aber dem Administrator, wenn er beispielsweise aus einem bestimmten Anlass wie vor einem Systemupdate eine Sicherung durchführt und dieses Band nun eine kurze Zeit aufbewahren muss. Die individuelle Bezeichnung hilft ihm dann beim schnellen Wiederfinden. Die DPS1100 unterstützt den Anschluss eines physikalischen Bandlaufwerks oder auch einer Bandbibliothek. Momentan werden hier nur Modelle von Tandberg Data unterstützt, es ist seitens des Herstellers aber angedacht, sich zu öffnen und zukünftig auch Geräte von Fremdher-

stellern zu unterstützen. Die Unterstützung physikalischer Laufwerke wird in der Weboberfläche der DPS1100 einfach per Mausklick aktiviert, wodurch einige zusätzliche Menüpunkte hinzukommen, unter anderem eine Import-/Export-Funktion. Für eine Automatisierung steht ein Export-Zeitplaner zur Verfügung, in dem die gewünschten Jobs anzulegen sind. Die DPS1100 unterstützt mehrere Exportarten wie einen Full Export mit oder ohne Zurücksetzen des Archiv-Bits und differentielle sowie inkrementelle Exports.

Werden im Rahmen einer Rücksicherung Daten von einem Band benötigt, muss dieses die Library zuerst wieder importieren. Tandberg Data plant aber auch hier eine erweiterte Funktionalität, so dass sich in Zukunft exportierte Bänder von einem beliebigen Laufwerk aus für eine Rücksicherung verwenden lassen sollen. Bezüglich solcher zusätzlicher Funktionen ist anzumerken, dass die DPS1100 standardmäßig mit drei Jahren Garantie und einem Jahr Vor-Ort-Hardwareunterstützung sowie Software-Updates verkauft wird. Die Export-Funktionen konnten wir unter Live-Bedingungen nicht testen, da uns keine zusätzliche Bandbibliothek zur Verfügung stand, wir haben den Hersteller aber eingehend zur Funktionalität befragt.

Licht und Schatten beim Plattenausfall

Um im Labor das Verhalten bei einem Defekt der VTL zu testen, zogen wir im laufenden Betrieb eine Festplatte und simulierten damit deren Ausfall. Sofort begann die DPS1100 mit einem deutlichen Piepsen in kurzen Abständen – nicht zu überhören, sofern sich jemand im Rechnerraum befindet. Da die DPS1100 aber wie erwähnt recht laut ist und daher irgendwo gut isoliert untergebracht sein sollte, ist nicht sichergestellt, dass diese akustische Warnung auch wirklich jemand hört. Für den Reparaturfall ist es übrigens ärgerlich, dass sich das Piepsen manuell nicht abstellen lässt.

Mit etwas Verzögerung beobachteten wir zudem eine Änderung der Anzeige in der Web-GUI. Statt auf der Homepage vier grüne Rechtecke zu sehen, die den OK-Status des Raid-Verbundes symbolisieren, waren nun eines rot und drei gelb. Damit dies auffällt, ist aber vorausgesetzt, dass ein Administrator die GUI geöffnet hat. Eine Mail, die uns über den Plattenausfall informiert, erhielten wir wider Erwarten nicht. Erst nachdem wir die Platte wieder eingesteckt hatten, kam eine Mail an mit der Info, dass das System einen Rebuild durchführt, inklusive der Angabe des Prozentsatzes. Als wir den Hersteller darauf ansprachen, erhielten wir als Antwort, dass es durchaus zehn Minuten dauern kann, bis das System eine Mail versendet. Daraufhin wiederholten wir den Test, erhielten aber auch nach über 30 Minuten noch keine Benachrichtigung. Nun erstellten wir auf Anforderung von Tandberg ein Troubleshooting-Log, was in der Web-GUI mit wenigen Mausklicks erledigt ist und schickten die gepackte Datei an den Support. Anhand der Informationen konnte Tandberg das Problem nachstellen und machte in Verbindung mit dem Firmware-Stand unserer Test-Library einen Fehler bei der Mailversendung ausfindig. Diese Problematik will der Hersteller durch ein Update beheben.

Gut gefallen hat uns, dass die DPS1100 nach dem Ersetzen einer defekten Platte automatisch mit einem Rebuild beginnt, ohne dass weitere Aktionen notwendig sind. Der Rebuild dauerte im Test rund 3,5 Stunden. In diesem Zeitraum blinkt an der wieder einzubindenden Platte eine rote LED. Von Vorteil ist auch, dass ein laufender Rebuild nach einem Neustart der Appliance an der Stelle vor dem Reboot fortfährt und nicht von vorne beginnt.

Fazit

Die DPS1100 ermöglicht einen relativ preisgünstigen Einstieg in die VTL-Technik und ist erfreulich einfach zu bedienen. Allerdings verfügt die Hardware nur über begrenzte Redundanz, da sich beispielsweise kein zweites Netzteil einstecken lässt. Durch die zusätzlich erhältlichen Erweiterungseinheiten lässt sich die Kapazität nach Bedarf gut individuell erweitern. Die DS1100 ist sowohl als alleinige Backupeinheit als auch in Verbindung mit einer physikalischen Bandbibliothek als Backup-to-Disk-to-Tape-Lösung einsetzbar. Festgestellte Probleme mit der Mailbenachrichtigung sollten bis zur Veröffentlichung dieses Artikels behoben sein. *(ln)*

Produkt
Virtuelle Bandbibliothek (VTL, Virtual Tape Library).

Hersteller
Tandberg Data
www.tandbergdata.com

Preis
Die DPS1100 mit 3 TByte Kapazität kostet 7.920 Euro, die DPS1200 mit doppelter Kapazität 14.260 Euro. Ein DPS Expansion Modul mit Controller und 4,5 TByte kostet 7.525 Euro, die Erweiterung um weitere 4,5 auf 9 TByte zusätzlich 2.455 Euro.

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

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

Installation/Bedienung	9
Performance	8
Hardwareausstattung	7
Mailbenachrichtigung	7
Dokumentation	5

Dieses Produkt eignet sich

optimal in einem GBit-Netzwerk für das Backup mittlerer Datenmengen oder als Bindeglied in einer Backup-to-Disk-to-Tape-Lösung.

bedingt zur Sicherung sehr großer Datenmengen aufgrund der maximalen Ausbaufähigkeit sowie der begrenzten LAN-Bandbreite.

nicht für das Backup von Datenmengen mit einem Gesamtvolumen deutlich kleiner als 2 TByte, da sich dann die Investition nicht rechnen dürfte.

DPS1100 / DPS1200

1&1 WebHosting bietet beste

HOMEPAGE-

„Dank unserer Homepage konnten wir einen messbaren Gewinn an Neukunden verzeichnen. Bei 1&1 können wir uns darauf verlassen, dass unsere Seiten auch immer verfügbar sind."
www.folienbau.de

Mit über 20 Jahren Erfahrung und Hochleistungs-Rechenzentren in Europa und den USA bietet 1&1 mehr Leistung, mehr Service, mehr Innovation. Über 9 Millionen Kundenverträge sprechen für sich.

Top-Sicherheit!

Unsere Hochleistungs-Rechenzentren zählen zu den sichersten und leistungsfähigsten in Europa und den USA. Mit mehr als 70.000 High-End-Servern im Parallelbetrieb.

Top-Technik!

Die Rechenzentren der 1&1 Gruppe sind mehrfach redundant an die wichtigsten Internet-Knoten angebunden. Für schnellstmögliche Verbindungen mit über 130 GigaBit/s Außenanbindung.

*1&1 Homepage Business und 1&1 Perfect Shop jeweils 6 Monate für 6,99 €/Monat, danach für 14,99 €/Monat. Die .de-Domain gibt es im 1. Jahr für 0,29 €/Monat, danach für 0,49 €/Monat; die .at-Domain gibt es im 1. Jahr für 0,99 €/Monat, danach für 1,99 €/Monat. Einmalige Einrichtungsgebühr beträgt 9,60 € beim 1&1 Perfect Shop und 14,90 € beim 1&1 Homepage Business-Paket (die Einrichtungsgebühr von 9,60 € entfällt bei der .de- und .at-Domain). 12 Monate Mindestvertragslaufzeit. Preise inkl. MwSt.

MEMBER OF united internet

0180 5 / 001 535 14 ct/Min. aus dem Dt. Festnetz, Mobilfunk höchstens 42 ct/Min.

0800 / 100 668 Anrufe aus dem österr. Festnetz und Mobilfunknetz kostenfrei.

QUALITÄT!

1&1 HOMEPAGE BUSINESS

Die Komplett-Lösung für den perfekten Internet-Auftritt:

- 3 Inklusiv-Domains
- 5 GB Webspace
- Unlimited Traffic
- 5 MySQL-Datenbanken
- 500 E-Mail-Postfächer
- 1&1 Newsletter-Tool
- 1&1 WebStatistik
- 1&1 Suchmaschinen-Tools
- 24h-Profi-Hotline, 7 Tage die Woche

6 MONATE 50 % RABATT

~~14,99 €/Monat*~~

6,99 €/Monat*

6 Monate für 6,99 €/Monat, danach nur 14,99 €/Monat.*

1&1 PERFECT SHOP

Einfache Einrichtung ohne Programmierkenntnisse:

- Bis zu 200 Artikel
- Shop-Designer
- Inklusive hochwertigem 1&1 WebHosting-Paket
- PayPal bereits vorinstalliert

PayPal · ipayment · ebay Kompatible Anwendung

6 MONATE 50 % RABATT

~~14,99 €/Monat*~~

6,99 €/Monat*

6 Monate für 6,99 €/Monat, danach nur 14,99 €/Monat.*

1&1 DOMAINS

Sichern Sie sich jetzt Ihre individuelle Internet-Adresse:

- Schnelle Domain-Aktivierung
- DNS-Verwaltung
- E-Mail-Adresse mit Weiterleitung an bestehende E-Mail-Postfächer
- Weitere Angebote finden Sie im Internet, z. B. gibt es die .at-Domain schon für günstige 0,99 €/Monat im ersten Jahr.*

.de

KEINE EINRICHTUNGS-GEBÜHR!

0,29 €/Monat*

Im 1. Jahr für 0,29 €/Monat, danach nur 0,49 €/Monat.*

Top-Features!

Die 1&1 Spezialisten entwickeln ständig Innovationen für hochwertige Websites – vom Design über Technik bis zum Marketing profitieren Sie bei 1&1 von vielen Funktionen, die Sie bei anderen Webhostern oft extra bezahlen müssen.

Top-Service!

Kostenloser E-Mail-Service und auf Wunsch kümmert sich ein fester Ansprechpartner persönlich um Sie.

www.1und1.info

1&1

Im Test: Men & Mice Suite 6.1

Verlässliches Adressbuch für Netzwerker

von Thomas Bär

Dass eine sauber funktionierende Namensauflösung eine entscheidende Rolle in Unternehmen spielt, weiß jeder Administrator, der sich schon einmal mit seltsamen Zugriffs-Phänomenen auseinandersetzen durfte. Verzeichnisdienste etwa haben eine sehr hohe Abhängigkeit zur Namensauflösung. Wenn die Anzahl von Maschinen wächst und neben Windows-Servern auch noch andere Betriebssysteme zum Einsatz kommen, sind die Bordmittel sehr schnell erschöpft und es bedarf einer ausgewachseneren Lösung für ein zentrales Management. Die Software "Men & Mice" der gleichnamigen Firma ist eines dieser hochspezialisierten Programme und musste im IT-Administrator-Test ihre Leistungsfähigkeit unter Beweis stellen.

Die Men & Mice Suite 6.1 (MMS) besteht in der Summe aus vielen einzelnen Programmen, die verteilt auf den unterschiedlichen Servern mit einer zentralen Konsole über den TCP-Port 1231 kommunizieren. Drei Hauptarbeitsoberflächen kommen dabei zum Einsatz:

- die Men & Mice Management Console als primäres Interface,
- die Kommandozeilenprogramme (Men & Mice Command Line Interface – CLI),
- und die Men & Mice Web Oberfläche.

Für die Verwendung der Web Oberfläche ist ein Microsoft Internet Information Server (IIS) oder eine Apache 2-Installation erforderlich.

Für den ersten Start ist in jedem Fall eine Windows-Maschine als Client erforderlich, da der "Start Up Wizard" nur unter dem Betriebssystem aus Redmond läuft. Ist dieser Assistent noch nicht durchgelaufen, so lassen sich weder das CLI noch die Web-Oberfläche zur Steuerung der DNS- und DHCP-Server verwenden. Da es in jedem Unternehmen, und sei es auch nur auf einem Laptop, irgendwo eine Windows-Installation gibt, mag dies in der Praxis kein Nachteil sein – verwunderlich ist es dennoch, dass ein Softwarehaus, welches so viele Betriebssysteme unterstützt, ausgerechnet bei einer Banalität eine solche Anforderung stellt.

Für die Datenspeicherung verwendet die Software in der Standardauslieferung eine integrierte SQLite-Datenbank. Für größere Umgebungen besteht die Möglichkeit, eine zusätzliche Oracle-Installation zu verwenden. Da die MMS besonders größere und komplexere Umgebungen adressiert, stellt sich die Frage bezüglich der Ausfallsicherheit. Es darf stets nur eine Installation von Men & Mice Central verwendet werden. Zusätzliche Installationen können für den Fall eingerichtet werden, dass die Primärinstallation einmal nicht verfügbar sein sollte. Ein darüberhinausgehendes Konzept zur Ausfallsicherheit bietet die MMS nicht. Der Ausfall der MMS hat glücklicherweise keine negativen Auswirkungen auf die durch sie kontrollierten Server, da die Software als "nicht invasives" Programm die Verwaltungs- und Auswertungsmöglichkeiten lediglich erweitert, ohne die Standardprogramme zu modifizieren.

Auf jedem zu steuernden Server mit DNS- und DHCP-Dienst ist die ent-

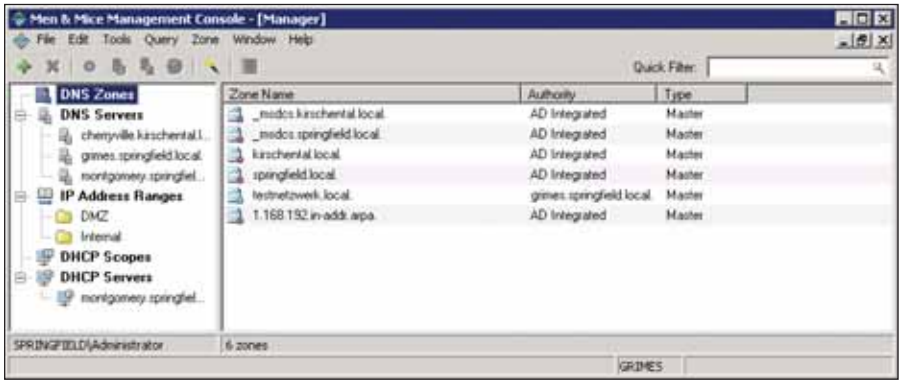


Bild 1: Alle DNS- und DHCP-Server mit den dazugehörigen Einstellungen sind in einer einzigen Oberfläche zusammengefasst – unabhängig davon, ob es sich um Windows-, Unix- oder Linux-Maschinen handelt. Ein domänenübergreifender Zugriff stellt ebenfalls kein Problem dar.

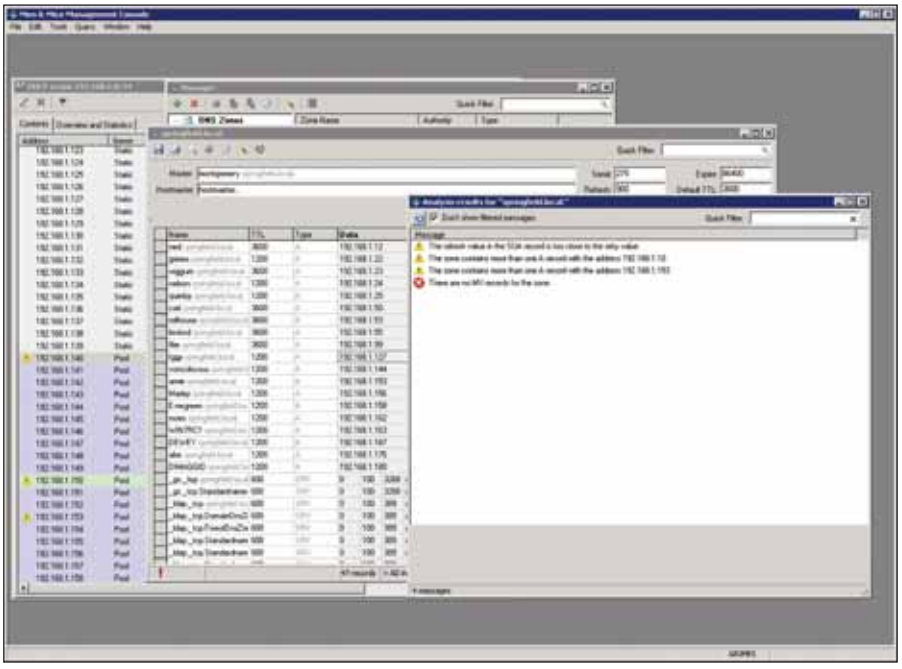


Bild 2: Das Analyse-Tool überprüft, ob die Konfiguration der DNS-Server korrekt vorgenommen wurde und macht auf Fehler aufmerksam

sprechende Server Controller Agent-Software zu installieren. Die Installationspakete für Windows sind nicht einmal 3 MByte groß und innerhalb weniger Augenblicke eingerichtet. Die Agent-Software kommuniziert mit dem entsprechenden Management-Server über die Ports 1337/TCP für DNS und 4151/ TCP für DHCP. Für beide Ports sind etwaige interne Firewalls entsprechend anzupassen, so dass die Kommunikation nicht blockiert wird. Alle verwendeten Ports der Software sind korrekt bei der IANA gemeldet und sind auf der Liste der "Well Known Ports" entsprechend vermerkt.

Einfache Installation und flexibler Einsatz

Die Firma Men & Mice bietet ihre Software als Testversion mit einer Laufzeit von 21 Tagen auf ihrer Homepage an. Ob es sich bei der Konfiguration um eine Testinstallation oder Vollinstallation handelt, wird einzig durch die verwendeten Lizenzschlüssel bestimmt. Durch die Eingabe der kostenpflichtigen Lizenzschlüssel wird somit aus einer Testinstallation die Vollversion – das erspart ein neues Aufsetzen der Software. Der Download aller Komponenten inklusive der jeweiligen PDF-Anleitungen umfasst rund 30 MByte. Die Installation der Software selbst dauert nur einige Minuten. Die notwendigen Angaben beschränken sich auf Annahme der Lizenzbedingung und die Auswahl des Zielpfades.

In einer einfachen Installation wird die MMS höchstwahrscheinlich schlicht mit Single Sign On (SSO) durch den Domänenadministrator verwendet. In komplexeren Umgebungen bietet sich die feinere Rechtesteuerung an. Zugriffsrechte beispielsweise für einzelne Domänen, Sub-

Systemvoraussetzungen

Während die Management-Konsole einzig auf Windows-Computern gestartet werden kann, ist die Serverunterstützung für unterschiedliche Plattformen sehr groß. Windows 2000 oder höher, Solaris 9 für UltraSparc oder Solaris 10 und höhere Versionen für die x86-Umgebung. Linux in den Ausprägungen Red Hat Enterprise ab Version 4, Fedora Core 7 oder höher, SuSE ab Version 10 und Ubuntu 6.06 und höher. Die Linux Betriebssysteme sind laut Dokumentation ausschließlich in der x86-Ausprägung nutzbar. Men & Mice unterstützt darüber hinaus auch MacOS X 10.4 oder höher über das BSD-Subsystem, jedoch mit der Einschränkung, dass die Webkonsole erst ab Version 10.5 auf dem Gerät selbst genutzt werden kann.

Mit der Server-Betriebssystem-Unterstützung allein ist es bei einer spezifischen Software für das Management von DNS und DHCP natürlich nicht getan. Bei den DNS-Servern kann es sich um Microsoft-Varianten oder um BIND 8.3 und höher oder BIND 9.2 oder später handeln. Bei den DHCP-Servern arbeitet die Software mit Microsoft DHCP, ISC DHCP 3.0.6 - 3.1.0 und Ciscos IOS 12.3 - 12.4 mit DHCP-Support zusammen.

Folgende Tipps sorgen für eine möglichst fehlerfreie Namensauflösung in Windows-Umgebungen. Jeder Server und jeder Client-Computer muss sich im DNS mit Forward- und Reverse-Lookupzone automatisch eintragen. Ist dies nicht der Fall, so könnte dies auf einen Fehler in der Namensauflösung hindeuten. Unabhängig von der in diesem Artikel betrachteten Software von Men & Mice sollten Sie diese Vorschläge berücksichtigen:

1. Konfigurieren Sie alle Domänencontroller als DNS-Server.
2. Richten Sie zwei Domänencontroller, sofern vorhanden, zusätzlich als WINS-Server ein.
3. Der DNS-Zonen-Name ist identisch mit dem Namen des Active Directory.
4. Der Name des Active Directory sollte der gebräuchlichen DNS-Syntax entsprechen und mindestens einen Punkt beinhalten. Die Verwendung von Top Level Domain Suffixen (.de oder .com) ist möglich und vereinfacht möglicherweise die Konfiguration eines Exchange-Servers. Die Verwendung von .local ist ebenfalls möglich.
5. Aktivieren Sie die Konfigurationsoption "Active-Directory-integriert mit sicheren Updates zulassen". Durch diese Einstellung ist ein wiederholtes Einrichten der Zonen nicht notwendig. Alle Domänen-Controller, die als DNS-Server konfiguriert sind, beziehen die Zone automatisch. Dieser Vorgang kann, in Abhängigkeit zur Größe des Netzwerks, einige Zeit dauern.
6. Reverse-Lookup-Zonen im eigenen Netzwerk sind zwar nicht erforderlich, helfen aber möglicherweise beim Ausschluss von potentiellen Fehlerquellen.
7. Teilen Sie über DHCP allen Clients mindestens zwei der Domänencontroller als DNS mit. Das Eintragen der DNS-Server-Adressen des Providers ist nicht hilfreich, da diese die interne Namensauflösung nicht durchführen. Um Internet-Adressen auflösen zu können, statten Sie den DNS-Server mit einer Weiterleitung auf einen oder mehrere DNS-Server aus.
8. Nehmen Sie die Einträge des DNS-Servers auch in der TCP/IP-Konfiguration der Domänen-Controller vor. Der Assistent für DCPROMO trägt hier das Loopback-Interface 127.0.0.1 ein, diese sollten Sie durch die echte IP-Adresse des Servers ersetzen.
9. Im Idealfall mit mehr als einem DC/DNS-Server nehmen Sie die Einträge über Kreuz vor. DC/DNS-Server A erhält die IP-Adresse von DC/DNS-Server B als primäre DNS-Adresse und vice versa.
10. Die Domänencontroller müssen unbedingt im DNS korrekt eingetragen sein, mit A-, SRV- und PTR-Einträgen. Durch Ausführung der Kommandozeilenbefehle *ipconfig /flushdns, ipconfig /registerdns, net stop netlogon* und *net start netlogon* in dieser Reihenfolge stellen Sie dies sicher.

10 Windows-DNS-Tipps

netze und IP-Adressen können so an untergeordnete Administratoren oder Help-Desk-Mitarbeiter vergeben werden. Durch die Installation und Verwendung der MMS werden die Bordmittel der Betriebssysteme glücklicherweise nicht außer Kraft gesetzt. Mitarbeiter, die sich primär mit den Themen DNS und DHCP auseinandersetzen, können die erweiterten Fähigkeiten der Software verwenden, während andere Kollegen, beispielsweise aus dem Support, im Zweifelsfall über die ihnen bekannten Mittel weiterarbeiten. Die Koexistenz beider Verwaltungswege erhöht die Akzeptanz einer Software in der Einführungsphase, da bereits gesammelte Erfahrungen in den ursprünglichen Oberflächen nicht verloren gehen. Dass sich die MMS für die Verwaltung besser eignet, wird jedem Anwender spätestens dann klar, wenn viele verschiedene Server gleichzeitig betrachtet werden sollen.

Nach der Installation auf einem Windows-Server findet sich die Software ganz typisch im Startmenü. Die Anleitung mit rund 200 Seiten in englischer Sprache wird als PDF-Dokument ebenfalls über das Startmenü geöffnet. Die Programmoberfläche der Suite ist sehr einfach und klar gegliedert – die Hauptmaske enthält den so genannten "Object Browser" mit Zugriff auf die verwalteten DNS-Zonen, IP/DHCP-Bereiche und die dahinterstehenden Server. Bevor jedoch eine einzige Aktion aus der Konsole möglich ist, müssen die Agent-Software-Komponenten auf den DNS/DHCP-Servern installiert werden. Ist dies nicht bereits geschehen, so gibt die Software eine Fehlermeldung aus, dass keine Kommunikation möglich ist.

Zentral gesteuerte Namensauflösung

Ist ein DNS-Server mit dem Agent ausgestattet, so lassen sich alle Einstellungen bequem zentral über die MMS steuern. Das Programmfenster listet in einer Tabellenansicht alle DNS-Einträge auf, die durch einfaches Anklicken und Eingaben modifiziert werden können. Such- und Filterfunktionen erleichtern das schnelle Auffinden gewünschter Einträge. Die aktuelle Seriennummer des DNS-Eintrags für den "SOA Resource Record", Refresh- und Retry- oder Expire-Einstellungen werden für die DNS-Zone ausgegeben und sind ebenfalls modifizierbar. Sehr angenehm ist die Tatsache, dass alle Einträge, die IT-Verantwortliche anpassen oder vornehmen, erst durch einen Klick auf die Speicher-Schaltfläche tatsächlich ausgeführt werden. In einem Bestätigungsfenster werden die Anpassungen noch einmal aufgelistet und lassen sich mit einem Kommentar versehen. Diese Kommentare werden in der Historie der Änderungen zusätzlich zum Zeitstempel, Benutzernamen und der Änderung selbst gespeichert und erleichtern so die Dokumentation. Wird beispielsweise der Refresh-Wert für DNS von 900 auf 899 Sekunden gesenkt, so protokolliert die Software dies mit "changed Record … 285 900 300 86400 to … 285 899 300 86400 3600".

Einträge lassen sich in der Suite über einen Wizard erstellen oder anpassen. Dieser leitet den Benutzer Schritt für Schritt durch die Erstellung neuer Einträge, das Anlegen von Alias (CNAMEs), die Neuanlage von Name-Servern oder die Eingabe von neuen Mail-Routen. Wer jedoch auf kontextsensitive Hilfestellungen hofft, der wartet vergeblich. Lediglich kleine Kommentare, wie beispielsweise, dass ein Name aktuell nicht auflösbar ist, was bei Anlage eines sich darauf beziehenden CNAMEs zu Schwierigkeiten führen wird, zeigt die Software an. Wenn sich ein Hersteller eines solch geflügelten Wortes wie "Wizard" bedient, sollte dieser den Benutzer bei seinen Vorhaben besser unterstützen. Ein weiteres Kommando in der Menüleiste ist die Analyse der Zonen-Einstellung. Da das Icon eher einem "Refresh"-Button ähnelt, klickt der Benutzer auf kurz oder lang zwangsläufig darauf und ist überrascht, einen kurzen Report zu erhalten. Zu den soeben exemplarisch vorgenommenen Anpassungen des SOA Refresh-Werts (steuert, in welchem Sekundenabstand

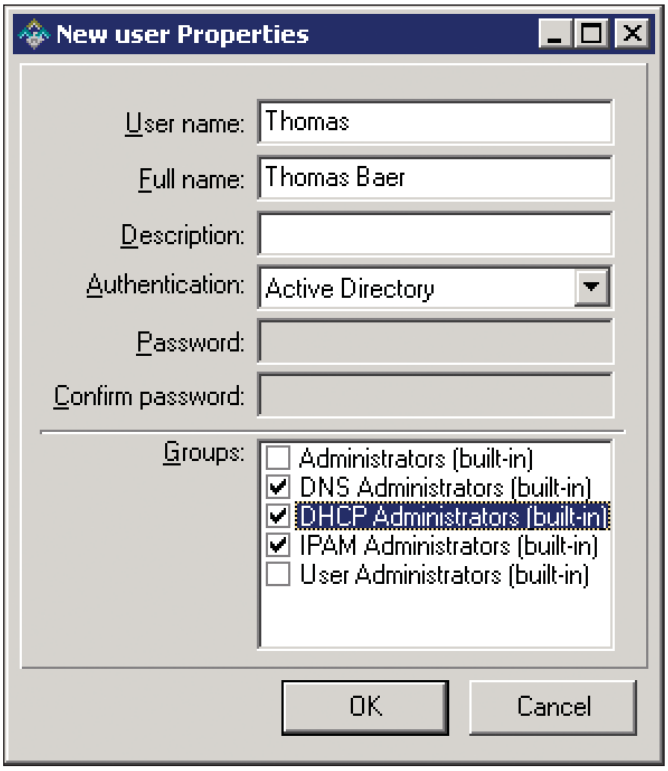


Bild 3: Die Benutzerverwaltung der Suite integriert sich auf Wunsch in das Active Directory oder bietet eine eigene Benutzerdatenbank

DNS-Slave-Server anfragen, ob eine Änderung vorliegt) gibt die MMS den Warnhinweis "The refresh value in the SOA record is too close to the retry value" aus. Der Refresh-Wert soll, gemäß der Software, mindestens dreimal größer gewählt werden wie der dazugehörige Retry-Eintrag. Interessanterweise gibt die Software jedoch keinen Hinweis darauf, dass laut RIPE-203 die empfohlene Refresh-Einstellung der Zonenübertragung 86400 und der Retry-Wert 7200 Sekunden betragen. Viele Fehler, wie beispielsweise unklare Einträge in der Namensauflösung, werden korrekterweise beanstandet und lassen sich direkt über die Oberfläche korrigieren.

Für weiterführende Auswertungen zur Namensauflösung bietet der Hersteller den so genannten "DNS Expert" an, den es auch in einer Variante für Active Directory im Zusammenspiel mit der Suite gibt. Der DNS Expert überwacht nicht nur einfach die Erreichbarkeit eines DNS-Servers, sondern überwacht im 24x7-Betrieb über 200 verschiedene Parameter und Einstellungen. Da der DNS-Expert auch als Einzelprodukt angeboten wird, bietet sich das Programm auch für Support-Mitarbeiter und Consultants an, die sich regelmäßig mit Fehlern in der Namensauflösung beschäftigen.

IP-Bereiche und DHCP Scopes verwalten

Neben der zentralen Verwaltung der Namensauflösung ist das Management der IP/DHCP-Bereiche das zweite Standbein der MMS. Für die sicherlich in absehbarer Zukunft anstehende Umstellung von IPv4 auf IPv6 ist die Software schon heute gerüstet und verwaltet beide IP-Versionen problemlos parallel. Ein White Paper zur Umstellung von IPv4 auf IPv6 mit der MMS findet sich auf der Homepage des Herstellers [1].

Wird die Baumstruktur des Menüs erstmalig geöffnet, so ist der IP/DHCP-Bereich erwartungsgemäß leer. DHCP-Bereiche füllen sich automatisch, nachdem die MMS Kontakt zu einem DHCP-Server aufgenommen und die Daten ausgelesen hat. Wie beim DNS, so ist die Software auch hier nicht an Domänen- oder Systemgrenzen gebunden und verwaltet die unterschiedlichen Strukturen in einer einzigen zentralen Oberfläche.

Soll ein neuer DHCP-Bereich angelegt oder ein vorhandener Bereich vergrößert beziehungsweise verkleinert werden, so geschieht dies mit einem einzigen Befehl aus dem Kontextmenü der Software. Für den besseren Überblick bietet es sich an, verschiedene Ordner anzulegen, die frei benannt verschiedene IP-Bereiche beinhalten können. An dieser Stelle mit der nötigen Ordnung vorzugehen, zahlt sich aus, wenn es darum geht, etwa mehrere DMZ-Bereiche zu verwalten, die traditionell in einem 192.168.1.n-Adressbereich eingerichtet wurden.

In das Kontextmenü ist das PING-Kommando integriert, was bei einer Prüfung das Öffnen eines zusätzlichen Kommandozeilen-Fensters erspart. Leider blockiert eine nicht antwortende Adresse das komplette Interface für mehrere Sekunden,

selbst andere Programmfenster, auf die ansonsten gleichzeitig zugegriffen werden kann, entziehen sich weiterer Ein- und Ausgaben.

Die Anlage von Lease-Reservierungen aus der MMS heraus ist sehr angenehm gelöst: Hat sich das gewünschte System bereits eine DHCP-Adresse gezogen, so ist die MAC-Adresse bereits eingetragen und kann per Zwischenablage kopiert werden. Soll die aktuelle Lease als Reservierung verwendet werden, so beschränkt sich der Aufwand auf das schlichte Bestätigen der Reservierung. Passen IP-Einträge nicht zu den auf dem DNS-Server gespeicherten Informationen, so macht die Software durch ein kleines Ausrufezeichen darauf aufmerksam.

Auf der Kommandozeile

Mit rund 50 Befehlen bietet das Men & Mice Command Line Interface (CLI) beinahe den vollen Umfang der Funktionen des Standard-Benutzerinterfaces. Das CLI von Men & Mice lässt sich entweder interaktiv durch das Ausführen der Kommandos Zeile für Zeile oder als Batch-Ablaufdatei nutzen. Script-Files, die über Argumente von außen mit Daten versorgt werden können, werden über das EXECUTE-Kommando ausgeführt.

Das CLI eignet sich für die Automatisierung von Massenänderungen, automatisierten Prozessen oder Schnittstellen zu anderen Datenbanken. Für die regelmäßige Sicherung der Men & Mice-Datenbank ist das CLI ebenfalls das geeignete Programm, ohne dass auf eine externe Backuplösung zurückgegriffen werden muss, die beispielsweise das Serververzeichnis selbst sichert.

Links

[1] Whitepaper zur Migration nach IPv6
http://www.menandmice.com/files/PDF/IPv6_migration_planning_with_MM_Suite_09.pdf

Im Browserbetrieb

Das MMS-Webinterface auf Basis einer Apache 2- oder Microsoft Internet Information Server (IIS)-Installation bietet einige der Befehle direkt in einer Browsersitzung. Im Vergleich zu vielen anderen Programmen, die eine Integration einer Weboberfläche bieten, ist der Leistungsumfang bei der MMS jedoch deutlich überschaubarer. Das Menü des Webinterfaces besteht aus lediglich vier Tabs.

In "Advanced Zone View" lassen sich DNS-Zonen-Konfigurationsänderungen vornehmen. Wie bei Verwendung der regulären Konsole so wird auch in der Weboberfläche ein Kommentarfeld für jede Änderung angeboten. Änderungen in der Konfiguration werden jedoch nicht erst bis zu einem Speichervorgang im Sinne eines "Commits" gesammelt, sondern sofort ausgeführt. Neue DNS-Einträge oder Änderungen an bestehenden DNS-Einträgen lassen sich für die unterschiedlichen Zonen aus diesem Tab heraus schnell und unkompliziert vornehmen. Das zweite Tab, die "Basic Zone View", erlaubt einen eingeschränkten Zugriff und bietet sich für Benutzer mit geringeren Kenntnissen rund um die Namensauflösung an.

Änderungen an DHCP-Scopes und IP-Bereichseinstellungen werden über das dritte Tab "IP Address Management" vorgenommen. Die Eingabe von Reservierungen im DHCP-Scope ist hier ebenfalls möglich, was sich bei Vor-Ort-Einsätzen beim Aufbau neuer PCs, Drucker oder Thin Clients anbietet. Im Tab "Reporting" werden die Protokolle "Utilization", "Activity" und "Access" mit unterschiedlichen Filterkriterien, wie beispielsweise Benutzernamen, Datum oder Beschreibung, ausgegeben. Die Ergebnisse können zur Weiterverarbeitung in die Zwischenablage oder als XML-Datei exportiert werden.

Fazit

Zusammengefasst handelt es sich bei der Men & Mice Suite um eine sehr einfach einzusetzende Software für eine einheitliche und standortübergreifende Sicht auf die DNS- und DHCP-Daten. Anstelle unterschiedliche Benutzeroberflächen auf einzelnen Servern zu verwenden, bietet Men & Mice alle Funktionen auf einen Blick und erweitert diese durch Reporting-Funktionen. Angesichts der heute üblichen Dimensionen von Netzwerken, in denen jeder Drucker schon über eine eigene IP-Adresse verfügt, ist die manuelle Pflege von Excel-Tabellen wahrlich nicht mehr zeitgemäß. *(jp)*

Produkt
Software zum zentralen Management von DNS und DHCP.

Hersteller
Men & Mice
www.menandmice.com

Preis
Die Preisgestaltung von Men & Mice basiert auf der Anzahl der tatsächlich verwendeten IP-Adressen, die über das System verwaltet werden. In kleineren Netzwerkumgebungen liegt der Preis zwischen 3,57 und 4,76 Euro je IP-Adresse. In größeren Umgebungen mit beispielsweise 50.000 IP-Adressen sinkt der Preis pro Adresse auf 3,09 Euro.

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

Integration in die Infrastruktur	9
Bedienung	7
DNS-Verwaltung	7
DHCP-Verwaltung	7
Management komplexer Umgebungen	7

Dieses Produkt eignet sich

gut für große und komplexe Umgebungen mit vielen verschiedenen DHCP/DNS-Bereichen.

bedingt für mittlere Netze mit häufigen Änderungen an der DNS/DHCP-Konfiguration.

nicht für kleinere Netzwerke beziehungsweise Umgebungen, in denen selten Änderungen der DNS/DHCP-Konfiguration erforderlich sind.

Men & Mice Suite 6.1

So bekommt Ihr Online-Support Flügel!

Mit Netviewer Support sorgen Sie per Mausklick für einen besseren Kundenservice bei niedrigeren Kosten. Anfragen lösen Sie schnell und unkompliziert – und Ihre Kunden werden Sie für einen Engel halten.

Weitere überraschende Anregungen erhalten Sie im kostenlosen Netviewer-Buch. Gleich bestellen und Gratis-Testversion anfordern unter **0721 35 44 99 400** oder:

www.netviewer.com/engel

Online-Meeting-Kultur jetzt leben!

netviewer

Im Test: Matrix42 Package Robot 8.5

Pakete selbst geschnürt

von Jürgen Heyer

Jede Software erfordert bei der Installation individuelle Eingaben oder Angaben zur Personalisierung, die bei einer bedienerlosen Einrichtung automatisch beantwortet werden müssen. Wer zur Lösung dieses Problems nicht gleich in eine komplexe Softwareverteilung investieren möchte, für den kann Package Robot diese Automatisierung übernehmen. IT-Administrator hat genauer untersucht, wie gut sich mit diesem Tool komfortable Installationen und Deinstallationen sowie allgemeine Prozessabläufe ohne weitere Benutzereingaben paketieren lassen.

Package Robot 8.5 von Matrix42 basiert als OEM-Version auf WinRobots und ist im Kern eine mit Visual Basic 6 erstellte Skriptsprache zur Steuerung von Fremdanwendungen oder auch des Betriebssystems selbst per Code (API-Aufrufe), simulierten Tasteneingaben und Mausaktivitäten. Der Ablauf erfolgt anhand eines normalen ASCII-Skripts, das zeilenweise interpretiert wird. Für eine Installation ruft das Tool dazu die vom jeweiligen Hersteller gelieferte Installationsprozedur auf, wobei das mit Matrix42 Package Robot (MPR) erstellte Skript alle Abfragen automatisch beantwortet, so dass keinerlei zusätzliche Benutzerinteraktionen erforderlich sind. Gleiches gilt für Deinstallationen.

Um die Skripterstellung zu vereinfachen, liefert der Hersteller zwei Aufzeichnungstools (InstaRec-Rekorder) für die Installation sowie Deinstallation mit, mit denen sich diese Prozesse komfortabel mitschneiden lassen. Diese übernehmen in vielen Fällen die Hauptarbeit bei der Skripterstellung, erst beim Feintuning oder falls die Aufzeichnung unbefriedigende Ergebnisse liefert, ist der erfahrene Programmierer mit Know-how gefragt. Die beiden InstaRec-Rekorder sind exklusive Komponenten von MPR und kein Bestandteil von WinRobots, das übrigens auch in Produkten von Baramundi und Materna zur Anwendung kommt.

Installation der vier zentralen Bausteine

Bei der Installation legt das Programm auf dem Desktop Verknüpfungen zu den vier wichtigsten Werkzeugen an, im Startmenü finden sich darüber hinaus noch diverse weitere sinnvolle Tools, die für die Erstellung eigener komplexer Skripte sehr hilfreich sind und weiter unten beschrieben werden. Für den Einstieg reichen die über die Desktopverknüpfungen erreichbaren Bausteine. Einer ist eine Quickstart-Hilfe, deren Studium durchaus empfehlenswert ist, da hier die grundlegenden Ablaufschritte beschrieben sind. Zusätzlich zu dieser Hilfe startet beim ersten Aufruf des Package Robot Editors ein Tutorial mit mehreren Punkten, das die wichtigsten Funktionen erklärt. Interessant ist diese Lehrübung insofern, da es sich dabei selbst um ein mit MPR erstelltes Skript handelt und sich während der Ausführung in einem zusätzlichen Ansichtsfenster der Skriptablauf beobachten lässt. Dies vermittelt einen guten Eindruck über die Möglichkeiten und die Leistungsfähigkeit. Letztendlich kann MPR nicht nur Fremdprogramme steuern, sondern auch eigenständig für derartige Abläufe verwendet werden.

Achtung, Aufnahme!

Für die ersten Arbeiten mit MPR empfiehlt sich der Einsatz des automatischen Rekorders "InstaRec Install". Für den Start einer Aufzeichnung wird die zu installierende Applikation mit der Maus auf das

Systemvoraussetzungen

Matrix42 Package Robot läuft unter Windows 95 / 98 / ME / NT4 / 2000 / XP / Vista / 7 sowie Windows Server 2003 / 2008 (32- und 64-Bit) und stellt keine besonderen Anforderungen, die über die normalen Betriebssystemempfehlungen hinausgehen. Zu beachten ist nur, dass für einen späteren vollautomatischen Skriptablauf bei Windows Vista / 7 und Server 2008 die UAC (User Access Control) abzuschalten ist. Ist dies nicht der Fall, muss der Anwender die Programmmausführung jedes Mal bestätigen. Administrative Rechte werden darüber hinaus für Installationen nach wie vor benötigt.

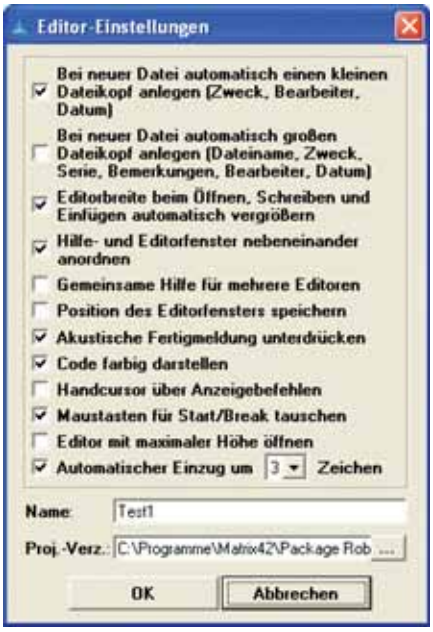


Bild 1: Der Administrator kann die Einstellungen des Package Robot Editors individuell anpassen

Rekorder-Icon gezogen. Nun öffnet sich das Rekorder-Fenster und die Installation beginnt. Das Rekorder-Fenster besteht aus einer Leiste mit acht Schaltflächen und einem Bereich zur Skriptanzeige. Jede Aktion wird aufgezeichnet und ergänzt das Skript um einen Schritt. Für eine gute Aufzeichnung ist es wichtig, die Installation zügig und zielstrebig durchzuführen, da sämtliche Aktionen mitgeschnitten werden – inklusive der Zeit zwischen den Schritten. Allerdings gibt es diverse Möglichkeiten, bereits bei der Aufzeichnung korrigierend einzugreifen. So kann der Administrator jederzeit die Aufnahme aussetzen, um andere Aktionen durchzuführen wie beispielsweise die Mails zu lesen oder etwas im Internet nachzusehen.

Ein fehlerhafter Schritt lässt sich durch Drücken der "Back"-Taste sofort wieder löschen. Weiterhin kann der Administrator einen Marker setzen, um eine Stelle beispielsweise für eine anschließende Nachbearbeitung besser zu finden. Außerdem gibt es eine Behandlungsroutine für unvorhergesehene beziehungsweise nur unter bestimmten Voraussetzungen erscheinende Popup-Fenster. Dazu muss der Administrator beim Erscheinen eines solchen Fensters dieses bestätigen und anschließend die "PopUp Rec"-Taste drücken. Dann weiß MPR, dass dieses Fenster bei Erscheinen bestätigt werden muss, bei Nichterscheinen aber die Installation fortgeführt wird, ohne auf das Fenster zu warten. Die "Clear All"-Taste letztendlich ist dazu gedacht, die gesamte Aufzeichnung zu löschen, um von vorne zu beginnen.

Standardmäßig ist MPR so eingestellt, dass es auf dem Desktop einen Ordner anlegt, in dem es das Installationsskript speichert und in den es auch die Installationsquelldateien hineinkopiert. Letztendlich aber gibt es drei Ablagemöglichkeiten: Entweder befinden sich alle Dateien in einem beliebigen, gemeinsamen Verzeichnis oder das Installationsskript befindet sich bezogen auf die Installationsquellen in einem Unterverzeichnis namens "\RemFiles\" oder im Skript ist der Pfad zu den Quellen angegeben.

Die Aufzeichnung einer Deinstallation läuft weitgehend ähnlich ab. Hierzu wird allerdings direkt die "InstaRec Uninstall"-Verknüpfung aufgerufen, woraufhin ein Fenster mit allen installierten Softwareprodukten erscheint. Nach der Auswahl des gewünschten Elements wird es deinstalliert und der Vorgang aufgezeichnet. Bei dieser Vorgehensweise stehen am Ende getrennte Skripte für Installation und Deinstallation. Mit etwas Programmieraufwand ist es aber auch möglich, beide Skripte in eine Datei zu packen. In diesem Fall findet beim Aufruf eine Prüfung dahingehend statt, ob die Applikation bereits installiert ist oder nicht, und der Skriptablauf verzweigt entsprechend.

Anpassungsfähige Skripte

Sind die Skripte erstellt, lässt sich durch einen entsprechenden Aufruf schnell prüfen, ob der gesamte Ablauf passt. Damit eine Weitergabe der Skripte an andere Clients, auf denen MPR nicht installiert ist, möglich ist, lassen sich die Skripte in rund 2 MByte große EXE-Dateien kompilieren. Werden diese mit den Installationsquellen weitergegeben, steht einem Aufruf auf beliebigen Clients prinzipiell nichts mehr im Wege. Im Test haben wir die (De)-Installationen für mehrere Programme wie beschrieben aufgezeichnet, die Skripte kompiliert und dann auf verschiedene Clients mit unterschiedlichen Betriebssystemen installiert. Bei nicht zu komplexen Setups klappte das hervorragend und ein unter Windows XP Professional erstelltes Skript führte sogar auf einem Windows 2008 Server mit 64 Bit eine fehlerfreie Installation durch. Auch verarbeitete MPR Anpassungen des Zielpfades korrekt, indem es eine manuelle Änderung des Unterverzeichnisses richtig übernommen und zugleich Betriebssystem-spezifische Pfad-Variablen wie die Installation nach "C:\Programme" unter Windows XP und nach "C:\Programme (x86)" auf einem Windows 2008 Server berücksichtigt hat. Trotzdem ist natürlich zu beachten, dass eine Installation nicht erfolgreich sein kann, wenn diese beispielsweise auf ein Laufwerk erfolgen soll, welches auf einem anderen Client gar nicht vorhanden ist.

Der InstaRec-Rekorder registriert bei der Aufzeichnung auch die jeweiligen Zeitspannen zwischen den Befehlen. Diesen entsprechend, trägt er für jede Aktion eine maximale Wartezeit ein, die standardmäßig der dreifachen Zeit bei der Aufzeichnung entspricht, aber mindestens 30 Sekunden lang ist. Erscheint innerhalb dieser Zeit das erwartete Fenster für die nächste Aktion nicht, bricht MPR die Skriptabarbeitung mit einer Fehlermeldung ab. Das soll vermeiden, dass ein Skript bei einem Fehler im Ablauf auf Dauer hängenbleibt. Sollen nun Skripte auf sehr unterschiedlich schnellen Systemen zur Ausführung kommen, so ist gegebenenfalls eine Nachbearbeitung der Zeitspannen erforderlich, der Standardfaktor drei sowie die Mindestwartezeit lassen sich grundsätzlich aber ändern.

An die Grenzen stieß die automatische Aufzeichnung im Test bei komplexeren Setups wie beispielsweise der Installation des MS SQL Server 2005. Die Aufzeichnung klappte zwar nach einigen Versuchen noch augenscheinlich, bei der Ausführung blieb die Installation aber regelmäßig an der gleichen

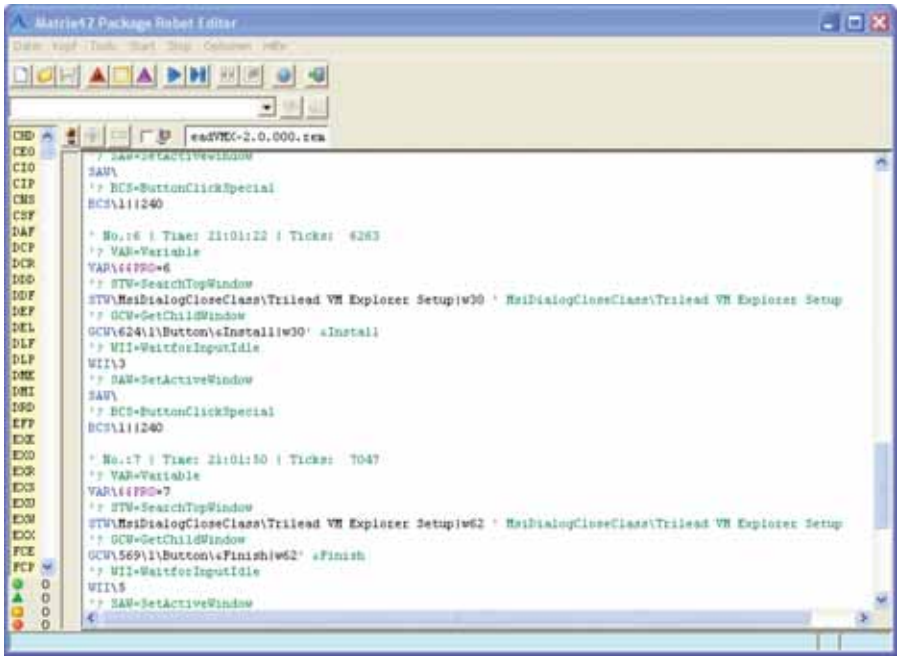


Bild 2: Dank umfassender Analysemöglichkeiten des MPR erlaubt die gelbe Leiste links einen halbautomatischen Aufbau des Skripts aus den notwendigen Schritten bei einer Installation

Stelle stehen. Tatsächlich ist es so, dass der automatische Rekorder im aktuellen Entwicklungsstadium in erster Linie für einfache Setups gedacht ist, die den bisher üblichen Fenster-orientierten Aufbau (mit Haupt-(Top)- und Kind-(Child)-Fenstern) verwenden. Neuere Browser-orientierte Anwendungen sowie die neuen Microsoft-Setups wie beispielsweise auch die Installation von MS Office 2007 arbeiten fensterlos und benötigen daher ein neues Erkennungsverfahren für die zu betätigenden Objekte. Dieses aber ist erst zum Teil in den automatischen Rekorder integriert.

Skripte im Eigenbau

Wer MPR über die automatische Aufzeichnung hinaus intensiv nutzen will, kommt um das Erlernen der Programmiersprache nicht herum. Sehr von Vorteil ist hier, dass bei MPR eine manuelle Programmierung nicht bedeutet, dass alles penibel eingetippt werden muss. Vielmehr kommt dann ein intuitives, quasi halbautomatisches Verfahren zum Einsatz. Dabei spielen die sogenannte "gelbe Liste" und die Zusatztools "Windows Analyzer" sowie "Accessibility Analyzer" tragende Rollen. Hierzu gibt es diverse Schulungen, außerdem sind eine gewisse Übung und ein Verständnis zum prinzipiellen Aufbau der Sprache erforderlich. Die MPR-Skriptsprache besteht aus aufeinander folgenden RCL (Remote Code Language)-Anweisungen, wobei jeder RCL-Ausdruck aus einem Befehls- und einem Datenteil besteht, die durch einen Backslash von einander getrennt sind. Es gibt allerdings auch Befehle ohne Datenteil.

Jeder Befehl besteht aus einer drei Buchstaben langen Abkürzung, beispielsweise CNS für "CreateNewShortcut" oder SKA für "SendKeyAscii". Der Datenteil ist in jeder Hinsicht flexibel und kann Informationen zu Dateien, zu Steuerelementen oder numerische Werte in Form von Ziffern beinhalten. MPR verfügt aktuell über rund 800 Befehle, die im Package Robot Editor am linken Rand als gelb unterlegte Leiste eingeblendet sind. Beim Darüberstreichen mit der Maus erscheint der Befehl in voller Länge, beim Anklicken steht umfangreiche Hilfe bereit.

Die grundsätzliche Vorgehensweise beim Erstellen eines Skripts sieht so aus, zuerst eine oder mehrere Anweisung(en) zu geben, um das Zielobjekt wie ein Steuerelement – etwa einen Button oder ein Kontrollkästchen – zu lokalisieren, also auf dem Bildschirm zu suchen. Nach erfolgreicher Suche sind Daten wie die Koordinaten zu ermitteln und anschließend eventuell notwendige Zusatzinformationen zur Lokalisierung einzutragen (zum Beispiel bei einer Listbox der Text oder die Indexnummer des anzuklickenden Eintrags). Schließlich wird die auszuführende Operation festgelegt (Mausklick, MouseEvent, Doppelklick, rechte Maustaste, Texteingabe). Die Lokalisierung erfolgt normalerweise stufenweise, ausgehend vom Desktop bis hin zum Zielobjekt. Als Angaben müssen jeweils die Klasse und die Beschriftung beziehungsweise der Text des jeweiligen Fensters beziehungsweise eindeutige Teile davon eingetragen werden, und zwar wieder durch ein Backslash getrennt.

Damit der Programmierer, wie schon erwähnt, nicht jeden Befehl aus der gelben Leiste heraussuchen und die sonstigen Angaben manuell ergänzen muss, gibt es ein recht bequemes, trickreiches Verfahren, um alle Anweisungen möglichst einfach zusammenzuklicken. Das wichtigste Werkzeug bei Fenster-orientierten Setups ist der Windows-Analyzer. Er listet die aktuell unter dem Mauscursor befindlichen Fenster in hierarchischer Reihenfolge mit Handle, ID, Klassennamen und Text oder Property auf. Aus dem Editor heraus gestartet lässt sich eine Fensterbeschreibung direkt in den Programmiertext übernehmen.

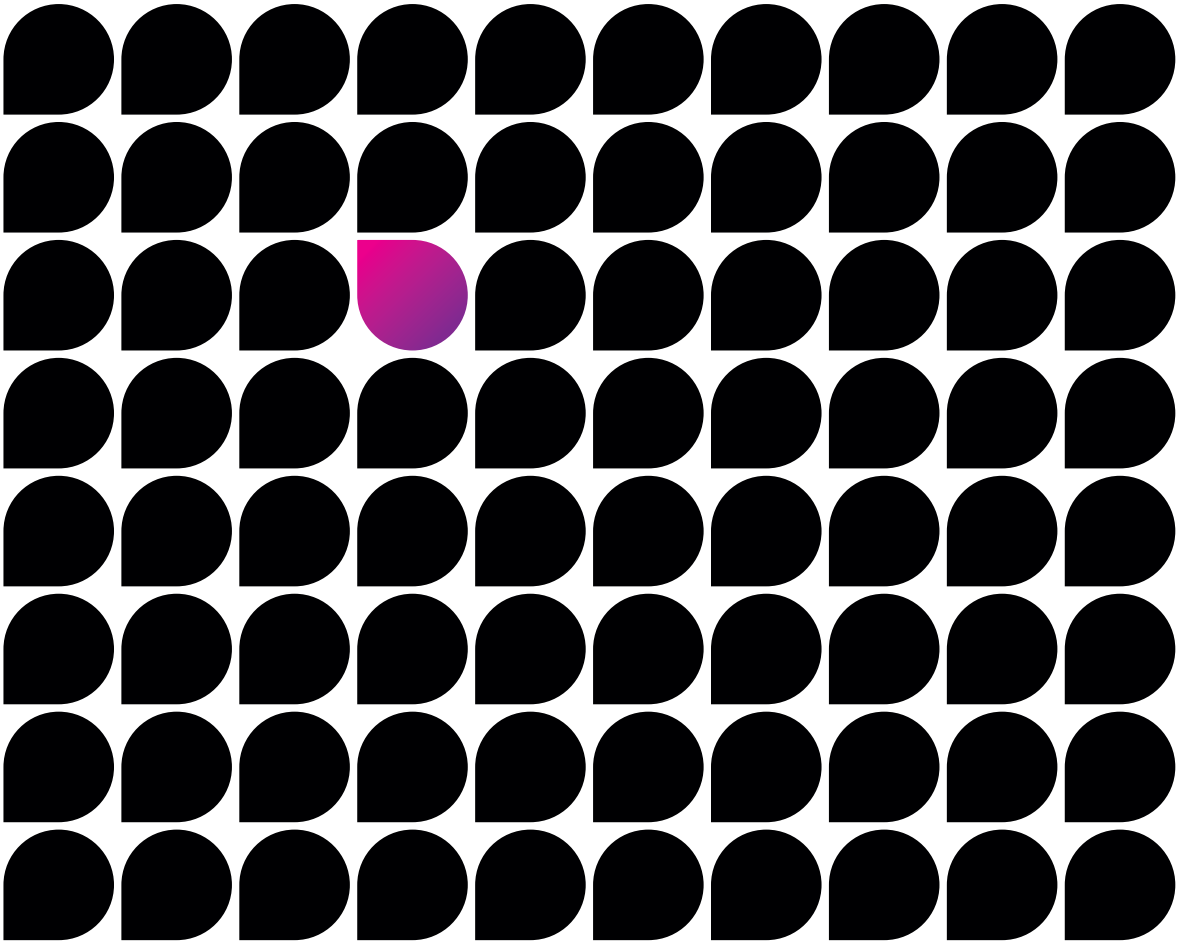
Um ein Skript für eine Installation zu schreiben, wird zuerst der Package Robot Editor mit dem Windows Analyzer gestartet, anschließend das zu automatisierende Setup. Sobald hier das erste Fenster mit einem Button oder einer Abfrage erscheint, bewegt der Programmierer die Maus auf das zu betätigende Objekt und im Analyzer erscheinen die dazugehörigen Parameter. Beim Klick mit der rechten Maustaste auf dieses Objekt kommt nun das in MPR integrierte Expertensystem zum Einsatz und es erscheint die wichtige gelbe Leiste mit allen an dieser Stelle möglichen Befehlen.

Intelligente Technologien für einen smarten Planeten

Wie man das Außergewöhnliche in alltägliche Dinge hineinbringt.

Schon in einem Jahr werden mehr als 100 Millionen Zeilen Software-Code die Elektronik eines ganz normalen Autos steuern – bei einem Passagierflugzeug über 1 Milliarde. Wir erreichen bald einen Punkt, an dem ein Auto, eine Bank oder ein Flugzeug mehr als nur die Summe ihrer Einzelteile sind. Was all diese Dinge tatsächlich auszeichnet, ist die zugrundeliegende Software – dieses unsichtbare Netz, das alles mit Intelligenz durchdringt. Kein Wunder, dass im letzten Jahr schon 66 % aller entwickelten Produkte mit eingebetteter Software liefen. Heute ist Software von zentraler Bedeutung, um Unternehmen strategisch auszurichten. Aber: 41 % aller Software-Projekte scheitern immer noch daran, den Geschäftsnutzen und die Rentabilität zu steigern. IBM hat die einmalige Erfahrung, die Ressourcen und die Lösungen, damit international führende Unternehmen Software effizient entwickeln und bereitstellen können.

Smarte Unternehmen brauchen intelligente Software, Systeme und Services.
Also: Machen wir den Planeten ein bisschen smarter. Wie, erfahren Sie unter ibm.com/delivery/de



smarter together
IBM auf der CeBIT 2010
2. bis 6. März, Halle 2 & 9
ibm.com/de/cebit

O&M IBM IT 10/10

Dabei versucht MPR auch, die wahrscheinlichste Benutzereingabe zu ermitteln und wählt die am besten geeignete Befehlsfolge aus, die dann mit einem Kreuz markiert ist. Der Programmierer muss nun diese Auswahl prüfen, gegebenenfalls ändern und kann diese dann inklusive der Informationen des Analyzers durch Klick auf den obersten OK-Eintrag in der gelben Leiste in den Editor übernehmen. Bei Bedarf ergänzt er die Befehle und fügt beispielsweise Wartezeiten hinzu, da das Skript standardmäßig abbricht, wenn ein erwartetes Objekt innerhalb von 30 Sekunden nicht erscheint. Dies kann aber durchaus der Fall sein, wenn beispielsweise eine größere Installationsdatei zu entpacken ist.

Sonderfall fensterlose Installationsroutinen

Nachdem neuere Setups von Microsoft und Browser-orientierte Steuerungen mittlerweile fensterlos arbeiten, liegen deren Bedien- und Anzeigeelemente nicht in Form eigenständiger (Kind)-Fenster vor, so dass sie für den Windows Analyzer nicht sichtbar sind. Hier ist der Accessibility Analyzer ein geeignetes Hilfsmittel zur Analyse. Er zeigt für die aktuelle Mausposition die wesentlichen Eigenschaften vom darunter liegenden "Accessible Object" an.

Für eine einfachere Fehlersuche und Analyse des Ablaufs kann der Benutzer Einsprung- und Haltepunkte setzen, um ein Skript erst ab einer bestimmten Stelle oder bis zu einem festgelegten Punkt ablaufen zu lassen. Ähnlich wie bei der Visual Basic-Programmierung selbst werden im Editor Start-, Stopp- und Haltepunkte durch verschiedene Symbole in unterschiedlichen Farben in einer Spalte vor dem Programmiercode angezeigt. Für die Simulation der Maus- und Tastatureingaben sind in MPR zwei Engines integriert. Die langsamere, aber kompatible Vorgehensweise sendet die Eingaben an Windows, worauf das Betriebssystem diese an die Applikation weitergibt. Voraussetzung ist hier ein angemeldeter Benutzer. Die zweite Variante schickt die Eingaben direkt an die Applikation. Die Werte der Steuerelemente lassen sich hierbei direkt setzen, so dass der Desktop nicht benötigt wird, was auch ohne angemeldeten Benutzer funktioniert. Diese Variante ist schneller, bedingt aber, dass die Applikation dies unterstützt. Die im Skript verwendeten Befehle bestimmen letztendlich, welches Verfahren zur Anwendung kommt.

Im Test fiel auf, dass ohne besondere Vorkehrungen eventuell schützenswerte Eingaben, wie beispielsweise das Passwort des sa-Benutzers, bei der Installation eines MS SQL-Servers im gemischten Modus im Klartext im Skript zu lesen sind. Gleiches gilt für Lizenzschlüssel, die im Laufe einer Installation abgefragt werden. Für derartige Fälle verfügt MPR über mehrere Vorkehrungen, die je nach Situation einzusetzen sind: Falls sich ein Skript, wie oben beschrieben, ohne angemeldeten Benutzer ausführen lässt, bietet das die größte Sicherheit, da es sich einspielen lässt, ohne dass ein Anwender zugleich Zugriff hat. Weiterhin gibt es die Möglichkeit, ein Skript unter einem anderen Benutzer ausführen zu lassen, was auch von Vorteil ist, wenn der normal angemeldete Benutzer nicht über Administratorrechte verfügt. Die dritte Möglichkeit besteht darin, Angaben innerhalb eines Skripts zu verschlüsseln. Letzteres bietet zwar keine perfekte Sicherheit, da die Möglichkeit besteht, einen Brute-Force-Angriff zu starten, in der Regel aber sollte dieser Schutz ausreichend sein.

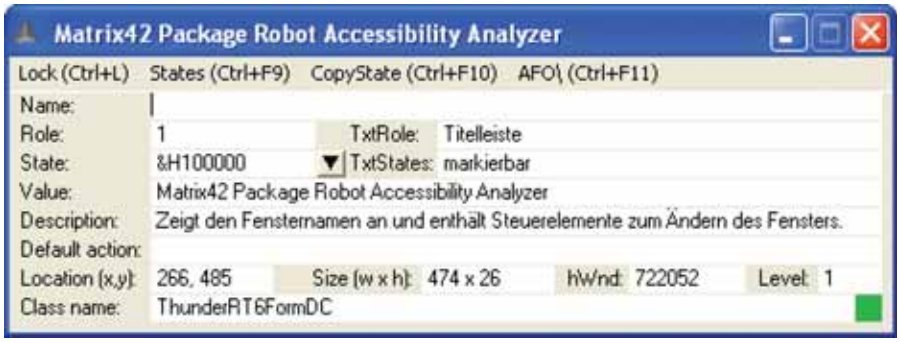


Bild 3: Der Accessibility Analyzer liefert alle notwendigen Daten, um ein dargestelltes Objekt mit MPR anzusprechen

Überzeugende Alternative zur Antwortdatei

Der große Vorteil von MPR ist die weitgehend universelle Einsetzbarkeit, denn der Administrator muss nur ein Werkzeug beherrschen, um (De)-Installationsskripte für unterschiedlichste Applikationen zu erstellen. Außerdem kann er mit MPR nicht nur (De)-Installationen automatisieren, sondern jegliche Programmsteuerungen nachbilden, also auch sonstige, immer wiederkehrende Abläufe. Hinsichtlich der Installation haben die Softwarehersteller für fast alle Programme die Möglichkeit geschaffen, über eine individuelle Antwortdatei einen automatischen Ablauf ohne Benutzereingaben zu realisieren. Hierzu ist es aber erforderlich, jedes Mal die Angaben für die Generierung oder Modifikation dieser Antwortdatei zu studieren, denn letztendlich verwendet jeder Hersteller seine eigene Syntax. Weiterhin sind dabei unterschiedliche Aufrufparameter erforderlich, während es bei MPR reicht, auf das kompilierte Skript zu klicken. MPR erlaubt es zudem, neben der reinen Installation noch andere Aktionen in ein Skript zu packen.

Bei sehr komplexen Installationen mag es aber gelegentlich von Vorteil sein, der individuellen Antwortdatei einer Software den Vorzug zu geben. Hier hat der Hersteller bereits die Funktionsfähigkeit überprüft und steht dafür gerade. Während MPR quasi von außen steuert und den Anwender ersetzt, erfolgen die Abfragen bei einem individuellen Antwortskript direkt aus der Installationsroutine heraus. Letztendlich aber kann ein Administrator immer individuell entscheiden, ob er für eine Automatisierung zu MPR greift oder die Antwortdatei des jeweiligen Herstellers verwendet. MPR übernimmt übrigens nicht die Aufgaben einer Softwareverteilung, lässt sich aber damit kombinieren. So

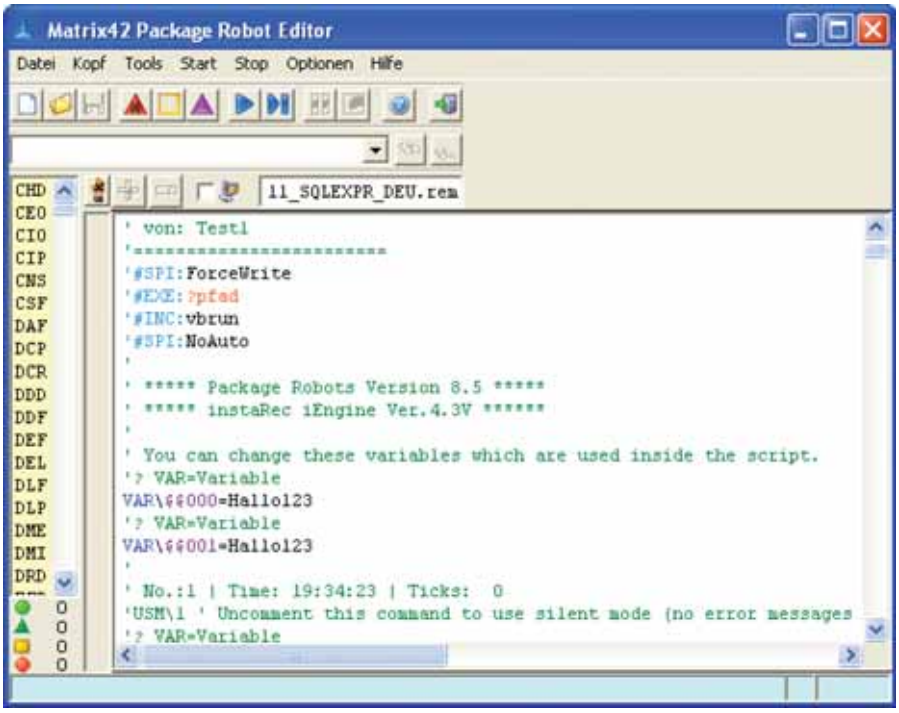


Bild 4: Ohne besondere Vorkehrungen sind bei einer Installation einzugebende Passworte im Klartext im Skript zu finden

setzt MPR voraus, dass das Skript und die Installationsdateien am Client erreichbar sind, entweder durch eine lokale Bereitstellung oder über eine Freigabe. Zudem ist noch ein Aufruf entweder manuell oder über ein anderes Skript wie etwa beim Login notwendig. Eine Softwareverteilung kann hier den Verteilungsprozess sowie den Skriptaufruf übernehmen.

Vielseitige Helfer an Bord

Wer mit MPR eigene Skripte bauen und sich nicht nur auf die Rekorder verlassen möchte, bekommt von Matrix42 verschiedenste Hilfen an die Hand. Anhand des bereits erwähnten Tutorials, das mit MPR geschrieben wurde, sieht der Betrachter recht gut, was mit der Skriptsprache alles möglich ist. Weiterhin gibt es eine über 400 Seiten starke Beschreibung in Buchform. Außerdem werden diverse Schulungen angeboten, deren Besuch bei der Anschaffung von MPR zu empfehlen ist, um die Einarbeitungszeit zu verkürzen und die Lernkurve zu steigern.

Die Hilfsmittel Windows Analyzer und Accessibility Analyzer haben wir bereits eingehend beschrieben. Darüber hinaus gibt es einen Process Analyzer, der alle auf dem System aktiven Prozesse mit ihrer PID auflistet, inklusive der zu jedem Prozess gehörigen Handles mit Klassennamen und Beschriftung. Weitere kleine Hilfstools sind unter anderem ein Programm, welches von allen Dateien eines Ordners den Schreibschutz entfernt, ausführbare Dateien zum Löschen einer Datei oder eines Verzeichnisses, ein Tool zum Überwachen von Verzeichnisinhalten und ein Programm zur Analyse von Tastatureingaben.

Fazit

Package Robot von Matrix42 hat im Test gezeigt, dass es eine sehr gute Hilfe ist, wenn ein Administrator auf die Schnelle eine einfache Installation, eine Deinstallation oder einen beliebigen, häufig wiederkehrenden Ablauf automatisieren möchte. Auch für die Automatisierung komplexer Setups ist das Tool unserer Meinung nach bestens geeignet, nur steigt der Aufwand für die Programmierung eines zuverlässigen Skripts dann deutlich. In manchen Fällen ist abzuwägen, ob MPR oder der vom Softwarehersteller implementierte Weg für eine unbeaufsichtigte Installation schneller zum Ziel führt. Prinzipiell spricht aber nichts dagegen, beide Wege je nach Aufgabenstellung parallel zu nutzen. MPR ist nicht dafür gedacht, eine komplette Softwareverteilung zu ersetzen, schon allein deswegen nicht, weil es keine zentrale Überwachungsmöglichkeit der Clients beispielsweise über Agenten gibt. Denkbar ist aber eine Kombination, indem mit MPR automatisierte Setups verteilt und deren Ablauf zentral gesteuert werden. *(ln)*

Produkt
Programm zur Erstellung individueller Softwarepakete.

Hersteller
Matrix42
www.matrix42.de

Preis
Lizenziert wird Package Robot anhand der Anzahl der Endgeräte, 100 Lizenzen kosten 812 Euro, für größere Mengen gibt es Staffelpreise.

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

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

Installation	9
Automatische Aufzeichnung	7
Manuelle Programmierung	8
Befehlsumfang	9
Dokumentation	7

Dieses Produkt eignet sich

optimal für beliebige Prozessabläufe sowie die automatische Installation von Softwarepaketen in Umgebungen jeglicher Größe in Kombination mit einer Softwareverteilung oder einer Systems-Management-Software.

bedingt für den alleinigen Einsatz ohne Softwareverteilung oder Systems-Management-Software in großen Umgebungen zur Steuerung komplexer Prozessabläufe und Softwareinstallationen, da dazu eine zentrale Überwachungskomponente fehlt.

nicht für Nicht-Windows-Umgebungen.

Package Robot 8.5

Im Kurztest: IS Decisions WinReporter 4

Administrator mit Überblick

von Sandro Lucifora

Administratoren benötigen jederzeit eine klare Übersicht der gesamten Infrastruktur ihres Windows-Netzwerkes. Für die komplexer werdenden Strukturen, welche die Aktualisierung der Infrastruktur-Daten erschweren, ist das automatische Erfassen aller angeschlossenen Geräte die Lösung. Mit WinReporter 4 testeten wir eine Software des französischen Herstellers IS Decisions, die das Netzwerk nach Windows-Computern scannt. Dabei differenziert die Lösung zwischen Servern und Workstations und speichert alle gewonnenen Informationen wie Computerkonfiguration, die Kapazität der Festplatten, installierte Programme, Microsoft Updates, User, Benutzergruppen oder Sicherheit in einer zentralen Datenbank ab. Aus den gewonnenen Daten erstellt das System periodisch fest definierte, aber auch individuell konfigurierbare Berichte.

Hardware

CPU, RAM, verwendeter RAM, BIOS, Grafikkarten, Netzwerkkarten (TCP/IP-Konfiguration), Partitionen, Festplatten, Modell und Seriennummer, Drucker

Software

Installierte Anwendungen, Dateiinformationen, Dateiversionen, Dateiberechtigungen

Windows

Betriebssystem, installierte Service Packs und Hotfixes, Internet Explorer, Dienste, SAM/AD (Benutzer und -gruppen), Shares, Shareberechtigungen

Event Logs

Dateizugriffe, Anmelde-/Abmeldevorgänge, Druckaufträge

Welche Informationen sammelt WinReporter?

Gezielt Daten sammeln und speichern

Um die gewünschten Informationen zu erhalten, scannt WinReporter die gewünschten Geräte in einem definierten Netzwerk. Dabei muss der Benutzer, unter dem WinReporter 4 ausgeführt wird, auf allen zu scannenden Maschinen Administratoren-Rechte besitzen. Im Test haben wir hierzu den Domänen-Administrator benutzt, was problemlos funktionierte.

Ein Wizard führt von Beginn durch die Einrichtung. Wir definierten dabei, welche Daten gesammelt (Hardware-, Software- und allgemeine Informationen) werden sollen. Die Daten werden wahlweise in eine AM Access-Datenbank oder auf einem MS SQL- oder Oracle-Server gespeichert. Die Tabellen sind treffend benannt, wodurch der Zugriff auf Informationen auch durch Drittprogramme möglich ist.

Automatische Reports

Um die gesammelten Informationen in einem Report anzeigen zu lassen, starteten wir die Report-Generierung. Zunächst wählten wir einen der 50 vordefinierten Reports aus und starteten mit dem "Display"-Button die Generierung. Je nach Datenumfang dauerte es bis zur Anzeige einige Sekunden bis zu Minuten. Die Berichte liessen sich nun ausdrucken oder als PDF-Datei speichern.

Die manuelle Erstellung ist jederzeit möglich und interessant, wenn die Berichte mit den Echtzeit-Daten benötigt werden. Spannend wird es, wenn der Bericht in regelmäßigen Intervallen erstellt und dem Administrator zugesendet wird. Hierzu bedient sich WinReporter 4 dem Windows-Scheduler, indem die Software entsprechende Tasks erstellt. Das Sammeln der Daten richteten wir auf stündlich, von 7 bis 18 Uhr, ein, um so auch die Geräte zu erfassen, die im Laufe des Tages ein- und ausgeschaltet werden, sowie Notebooks, die nur sporadisch im Netzwerk sind. Das Versenden des Berichts erfolgte täglich um 19 Uhr.

Fazit

Die Software sammelt an Daten, was möglich ist, und bereitet diese umfangreich auf. Sie verleitet dadurch aber auch dazu, sich zu viele Berichte erstellen zu lassen. Wer weiss, was er an Informationen benötigt und sich an die eigenwillige Bedienung gewöhnt hat, stellt sich mit den vielfältigen Optionen schnell seine individuellen Berichte zusammen. Diese entsprechen zudem den internationalen Richtlinien und Standards. Insgesamt zeigt sich WinReporter 4 als zuverlässige Software, die ihre Aufgabe gut erledigt. *(jp)*

Produkt

Inventarisierungs-Software für Windows-basierte Server und PCs.

Hersteller

IS Decisions
www.isdecisions.com

Preis

Lizenzierung nach Geräte-Anzahl: zum Beispiel 75 Euro für einen Server. Die 30 Tage-Testversion ist kostenlos für acht Workstations und zwei Server.

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

Umsetzung	7
Handhabung	8
Aufwand der Konfiguration	7
Zuverlässigkeit	10
Kosten-/Nutzen	8

WinReporter 4

Auswahlkriterien für Rack-Systeme

Das Rückgrat der IT

von Dieter Henze

Die Welt der IT-Racks wird nicht von schnelllebigen Trends und Hype-Technologien bestimmt. Vielmehr ist die Grundkonstruktion seit Jahren scheinbar gleich: eine stabile und robuste Plattform für die 482,6 mm-Komponenten (19 Zoll). Umso wichtiger ist eine sorgfältige Auswahl bei der Anschaffung. Denn die Schränke für Server und Netzwerktechnik haben eine Lebensdauer von zehn bis fünfzehn Jahren. IT-Administrator zeigt Ihnen, worauf es bei der Auswahl ankommt.

Um auch zukünftige Anforderungen zu erfüllen, sind Qualität und Flexibilität wichtige Kriterien. Dabei trennt sich die Spreu vom Weizen häufig im Detail: Neben der eigentlichen Schranktechnik sind wichtige Systemtechnologien rund um Klimatisierung, Stromabsicherung und Rack-Management von hoher Bedeutung. Um diese möglichst reibungslos zu integrieren, hilft es, wenn Rack und IT-Infrastruktur aufeinander abgestimmt sind. Bei der Auswahl gibt es daher einige Faktoren, die grundsätzlich beachtet werden sollten. Andere hängen vom Einsatzort und -zweck ab. Denn je nachdem, ob sich der Schrank in einem Rechenzentrum (RZ) befindet, innerhalb von Büroumgebungen mit Mischbestückung oder als Etagenverteiler aufgestellt ist, variieren die Anforderungen.

Der Server-Schrank ist ein Baustein im gesamten IT-Infrastrukturkonzept, welches das "System Rechenzentrum" bildet

Modular und stabil soll es sein

Eine grundsätzliche Feststellung vorweg: Racks halten lange. Im Gegensatz zu den IT-Geräten, die sie beherbergen und die nach etwa drei Jahren veraltet sind, hat ein Schrank eine Lebensdauer von zehn bis 15 Jahren. Bei der Anschaffung sollte daher grundsätzlich darauf geachtet werden, dass das Rack-System mit der Unternehmens-IT wachsen kann und auch zukünftigen Anforderungen gerecht wird. Daher empfiehlt sich die Auswahl von Lösungen, die von vornherein modular und somit skalierbar aufgebaut sind. Konkret bedeutet dies, dass die Schränke in allen Richtungen erweiterbar sein sollten, in unterschiedlichen Abmessungen zur Verfügung stehen und einen kompatiblen Zubehörumfang bieten, damit Veränderungen der Einbauten und Anwendungen über die gesamte Lebensdauer einfach und schnell unterstützt werden können. Solch ein modular aufgebautes Rack eignet sich sowohl für den Einsatz im Rechenzentrum als auch als Standalone-Lösung. Es verbindet zu einem relativ niedrigen Preis hohe Sicherheit mit Flexibilität.

Ein weiteres Kriterium, das bei der Auswahl des Racks ganz oben auf der Liste stehen sollte, ist die Stabilität. Die platzsparende Anordnung von IT-Komponenten innerhalb von Racks bis zu 42 Höheneinheiten (HE) führt zu einer hohen Packungsdichte und somit niedrigeren Flächenkosten. Daraus resultiert jedoch in der Praxis, dass ein Server-Rack Lasten bis zu 1.000 kg aufnehmen muss, die Heavy-Duty-Varianten tragen sogar bis zu 1.300 kg. Mit Blick auf die Zukunft nicht zu unterschätzen, denn Blade-Systeme und moderne Switches bringen immer mehr Masse in den Schrank. Voraussetzung für hohe Tragkraft ist unter anderem ein verschweißtes und mehrfach profiliertes Rahmengerüst, das dann mit Seitenwänden und Türen verkleidet wird. Gleichzeitig sollten auch die Geräteböden und Gleit-

schienen für hohe Lasten ausgelegt sein. Das spielt vor allem beim Innenausbau eine große Rolle. Böden mit einer Traglast von mindestens 30 kg sind Pflicht. Erstklassige Racks verkraften bis zu 150 kg pro Boden oder Schiene.

Flexibilität in der Tiefe

Moderne Server-Hardware fordert immer tiefere Racks. 1.000 mm Tiefe sind heute Standard. Einige Anbieter haben Schränke mit Tiefen bis zu 1.200 mm im Programm. Das ist hilfreich, um vor und hinter den Systemen noch Platz für Stromverteilung, Kabel und einen freien Kühlluftfluss zu lassen. Wenn heterogene Server-Systeme im selben Rack installiert sind oder wie häufig bei kleinen Unternehmen oder Filialen eine Mischbestückung mit Servern und Netzwerktechnik vorgenommen wird, sind tiefenvariable Ausbauten hilfreich. Sie erleichtern die Montage und garantieren, dass am Ende alles zusammenpasst. Bei flexiblen Lösungen lassen sich Frontabstand und der Abstand der Ebenen in Rasterschritten oder sogar völlig frei einstellen. Ein symmetrischer Aufbau des Racks sichert außerdem einen vielfältig nutzbaren Innenraum und gestattet die Anreihung von Racks in alle Richtungen – nebeneinander, über Eck und sogar nach oben. Sind solche Erweiterungen im laufenden Betrieb möglich, wirkt sich das positiv auf Kosten und IT-Verfügbarkeit aus. Anreihbarkeit und jederzeitige Erweiterbarkeit sind darüber hinaus Voraussetzung für leistungsfähige, rackbasierte Kühlkonzepte. Dabei wird die Kühlluft aus Luft-Wasser-Wärmetauschern direkt am Rack horizontal von der Seite vor die Einbauebene eingeblasen. Ein weiterer Punkt, auf den im Hinblick auf eine wachsende IT geachtet werden sollte. Denn in Umgebungen mit hoher Packungsdichte fallen Verlustleistungen an, die mit konventionellen Klimatisierungslösungen nicht ohne weiteres abgeführt werden können.

Häufig unterschätzt wird bei der Auswahl von Racks die Bedeutung des Oberflächenschutzes. Dabei ist dieser eine Voraussetzung für den jahrelangen Einsatz der Racks und trägt somit zur nachhaltigen Nutzbarkeit bei. Im täglichen Gebrauch, etwa beim Einbau schwerer Switches, kommt es schnell zu mechanischen Beschädigungen. Mehrstufige Verfahren bei der Oberflächenbeschichtung schützen vor solchen Schäden und nachfolgender Korosion.

Das "System Rechenzentrum"

Während die zuvor genannten Punkte grundsätzliche Kriterien darstellen, die bei der Auswahl aller Racks zu beachten sind, gibt es eine Reihe von Faktoren, die je nach Unternehmen beziehungsweise Einsatzort und -zweck variieren. Der Server-Schrank ist nur ein Baustein im gesamten IT-Infrastrukturkonzept, welches das "System Rechenzentrum" bildet. Andere Komponenten des Systems sind die unterbrechungsfreie Stromversorgung (USV), die Stromverteilung, Klimatisierung und Überwachungslösungen. Für einen reibungslosen IT-Betrieb müssen sich alle Teile harmonisch zusammenfügen. Für den Administrator äußert sich das in ganz praktischen Eigenschaften: Stromschienen beispielsweise, die sich flexibel in die Systemlochung des Racks oder entsprechende Systemchassis integrieren lassen. Dadurch kann die benötigte Anzahl an Steckdosen genau dort angebracht werden, wo die Server im Schrank untergebracht sind. Oder USV-Anlagen, deren hoher Wirkungsgrad die Betriebskosten deutlich reduziert.

Je nachdem, wie das Rechenzentrum aufgebaut ist, ergeben sich Konsequenzen für die Racks. In einem RZ stehen die Schränke nie für sich alleine, sondern sind in ein umfassendes Infrastrukturkonzept eingebunden, das nicht nur die Bereiche der IT-Abteilung berührt. Gebäudeverkabelung, Klimatisierung und Sicherheit müssen berücksichtigt werden und sind in größeren Unternehmen häufig beim Facility Management angesiedelt. Dabei sind auch scheinbar triviale Fragen zu beachten. Bei der Anreihung von Schränken unterschiedlicher Hersteller können sich beispielsweise Probleme bei der Kabelführung zwischen den Racks ergeben, da die Schottwände und Kabelöffnungen unterschiedliche Höhen aufweisen. Aber auch bei Stand-alone-Lösungen ist der Systemgedanke relevant. Für Büroumgebungen etwa gibt es vorkonfigurierte Racks, die vom Kabelmanagement bis zur aktiven Klimatisierung die Infrastrukturvoraussetzungen passgenau berücksichtigen.

Sonderfall Netzwerkschrank

Auch wenn sich die Racks vom grundsätzlichen Aufbau her nicht unterscheiden, gibt es bei Netzwerkschränken einige Besonderheiten zu beachten. Mittlerweile haben auch viele kleine und mittlere Unternehmen ihre Telefonanlagen auf VoIP umgestellt oder planen den Technologiewechsel zumindest. Damit wandert ein weiterer geschäftskritischer Basisdienst in die Hoheitsgewässer der Administratoren. Die Unterbringung von Netzwerktechnik unterscheidet sich aber in einigen Punkten von reinen Server- oder Storage-Racks. Zum einen saugen viele Switches die Kühlluft seitlich an und nicht frontal wie die Server. Zweitens übertragen die Datenkabel seit dem Siegeszug von Power over Ethernet (PoE) auch noch den Strom, den die Endgeräte benötigen. Und drittens müssen durch das häufige Umswitchen an den Ports die Kabel in den Netzwerkschränken deutlich häufiger neu verlegt werden als das in Serverschränken der Fall ist.

Stellt etwa ein Unternehmen seine alte PBX-Anlage auf VoIP-Telefonie um, ändern sich nicht nur die Switches im Schrank. Die PoE-Kabel sind deutlich schwerer, dicker und biegesteifer als die Standard Cat-5-Kabel. Dazu kommt eine höhere Portdichte durch die zusätzlichen Endgeräte. Die neuen Kabel beeinträchtigen außerdem die Luftzirkulation, was zu einem Hitzestau im Schrank führen kann. Zusätzliche Klimatisierungsmöglichkeiten werden nötig, an die vermutlich bei der Anschaffung eines Netzwerkschrankes keiner gedacht hatte. Das Beispiel zeigt, wie komplex die Auswirkungen einzelner Änderungen in der Systemlandschaft sein können. Es empfiehlt sich daher auch beim Netzwerkschrank, das Zubehör im Auge

zu behalten. Das Kabelmanagement fängt bei Dachblechen und Sockeln an. Das Einführen der Datenleitungen an diesen Stellen erleichtert die Nachrüstung und sorgt für kurze Kabelwege.

Die vertikale Führung innerhalb der Racks ist abhängig von der verbauten Technik. Kabeltrassen führen die Stränge sauber an den Innenseiten entlang zu Komponenten mit vielen Ports. Sind kleinere Switche auf den Höheneinheiten verteilt, sorgt eine kaskadierte Kabelführung – beispielsweise mittels Trunkkabeln – für freien Zugriff auf die Komponenten. Die horizontale Feinverteilung auf die einzelnen Stecker kann über Rangierkanäle oder Kabelpanel erfolgen. Da sich gerade bei der Kabelverteilung schnell Änderungen ergeben können, sind modular aufgebaute Schranksysteme mit einem durchgängig kompatiblen Zubehörkonzept von Vorteil. Auch auf Nachrüstmöglichkeiten bei der Klimatisierung ist zu achten. Das Spektrum reicht hier von optionalen Dachblechen und Entlüftungsaufsätzen zur passiven Klimatisierung über Dach- und Einschublüfter bis zu Dachkühlgeräten. Neben der Vielfalt des Zubehörs ist auch wichtig, dass es über den gesamten Lebenszyklus verfügbar ist. Wieder ein scheinbar trivialer Punkt, aber nur dann ist auch für die nötige Investitionssicherheit gesorgt.

Sicher verwahrt

Inhalte von Server- und Netzwerk-Racks sind wertvoll und in der Regel empfindlich. Noch wertvoller sind allerdings die Daten, die auf den Servern liegen. Ein Totalverlust kann ein Unternehmen durchaus in den Ruin treiben. Racks haben daher immer auch die Funktion, die Technik zu schützen und einen unautorisierten Zugriff zu verhindern. Der Zugriffsschutz ist insbesondere bei frei zugänglichen Aufstellorten von Bedeutung. Ein erstes Bollwerk ist eine solide Vier-Punkt-Verriegelung. Sie schützt den Inhalt mechanisch gegen Unbefugte. Öffnen lässt sie sich wahlweise per Schlüssel, mittels eines elektronischen Zugangssystems oder durch biometrische Erkennungsverfahren.

Ein nicht zu unterschätzendes Risiko stellen aber auch physikalische Gefahren dar: Feuer, Rauch und Löschwasser kommen zum Glück selten vor, können aber ganze Rechenzentren vernichten. Interessanterweise liegen die Brandherde in den meisten Fällen außerhalb der IT. Um einzelne Racks zu schützen, lassen sich sogenannte Modulsafes einsetzen. Die Systeme sind feuerfest, wasserdicht und mit Kühlung, Energieversorgung, Notstrom und Monitoring ausgestattet. Sie empfehlen sich besonders als Mittelstandslösung. Sollte sich der IT-Bedarf des Unternehmens erhöhen, können drei oder vier dieser Modulsafes miteinander verkettet werden.

Fazit

Für viele Administratoren sind Racks "nur" eine notwendige Voraussetzung, um die eigentliche IT unterzubringen. Dabei unterscheiden sich die einzelnen Produkte im Detail deutlich. Vor allem bei der Verarbeitungsqualität und beim Zubehör liegen Welten zwischen scheinbar identischen Produkten. Bei der Kaufentscheidung sollten die Verantwortlichen daher genau hinsehen und bedenken, in welchem Umfeld sie den Schrank einsetzen wollen. Denn ein Rack ist immer ein Teil des ganzen Systems "IT" – für mindestens ein Jahrzehnt. Dabei ist das Rack ein integraler Baustein einer kompletten IT-Infrastruktur und Netzwerklösung und sollte daher die weiteren Disziplinen wie Klimatisierung, Stromabsicherung oder Überwachung unterstützen. *(dr)*

Dieter Henze ist Abteilungsleiter Produktmanagement Modulare Schaltschranksysteme bei Rittal in Herborn

Auswahlkriterien für Rack-Systeme

Merkmal	Kleine Unternehmen	Mittlere Unternehmen	Große Unternehmen
Alle Komponenten in einem Rack integriert und vom Hersteller komplett geliefert	sehr wichtig	wichtig	wichtig
Optimale Integration der Komponenten innerhalb des Racks	sehr wichtig	sehr wichtig	sehr wichtig
Format der Racks ermöglicht eine effiziente Aufstellung	weniger wichtig	sehr wichtig	sehr wichtig
Erweiterung der Racks und der Infrastruktur ist sichergestellt	wichtig	sehr wichtig	sehr wichtig
Racks passen bei einer Erweiterung zueinander	weniger wichtig	wichtig	sehr wichtig
So viele Komponenten wie möglich müssen in den Racks untergebracht werden und Stromversorgung sowie Kühlung müssen gesichert sein	weniger wichtig	sehr wichtig	sehr wichtig
Stabilität für bis zu 1.000 kg Belastung	wichtig	wichtig	wichtig
Schutz vor physikalischen Zugriffen (etwa mit Schlüsseln oder Keypad)	wichtig	sehr wichtig	sehr wichtig
Interne oder externe Absicherung gegen Stromausfälle	sehr wichtig	sehr wichtig	sehr wichtig
Ausreichende Kühlung für einen zuverlässigen Betrieb	wichtig	sehr wichtig	sehr wichtig
Fern- und Vor-Ort-Überwachung der Komponenten	weniger wichtig	wichtig	sehr wichtig
Kosten für den Betrieb in Relation zu den Vorteilen für das Unternehmen	sehr wichtig	sehr wichtig	sehr wichtig

System Center Virtual Machine Manager 2008 R2

Schaltzentrale für Hyper-V

von Nico Lüdemann

Mit der neuen Version 2 des Microsoft Hyper-V ist eine Vielzahl an neuen Funktionen in das Produkt gewandert, die auch in Umgebungen mit mehreren Virtualisierungshosts zentral verwaltet werden wollen. Microsofts Antwort auf diese Anforderungen ist der "Virtual Machine Manager" aus dem System Center-Portfolio. In seiner aktuellen Version 2008 R2 wurde sein Funktionsumfang erneut ausgebaut und um die Unterstützung von VMWare-Umgebungen erweitert.

Beim System Center Virtual Machine Manager 2008 R2 – kurz: VMM – handelt es sich um die Komponente des System Center-Portfolios, die für die Verwaltung und Steuerung von virtualisierten Systemumgebungen zuständig ist. Um an dieser Stelle eine möglichst breite Unterstützung bieten zu können, kann der VMM in seiner aktuellen Version für die Verwaltung von Microsoft Virtual Server 2005 R2 SP1 (oder höher) in 32 Bit und 64 Bit, Hyper-V (R1 und R2) sowie VMWare ESX/vSphere über das Virtual Center genutzt werden. Hierbei setzen Sie den Virtual Machine Manager als Verwaltungsinstanz für die Virtualisierungs-Infrastruktur ein, indem Sie die Hosts durch die Installation von VMM-Agenten an den VMM andocken und ab diesem Zeitpunkt über ihn verwalten.

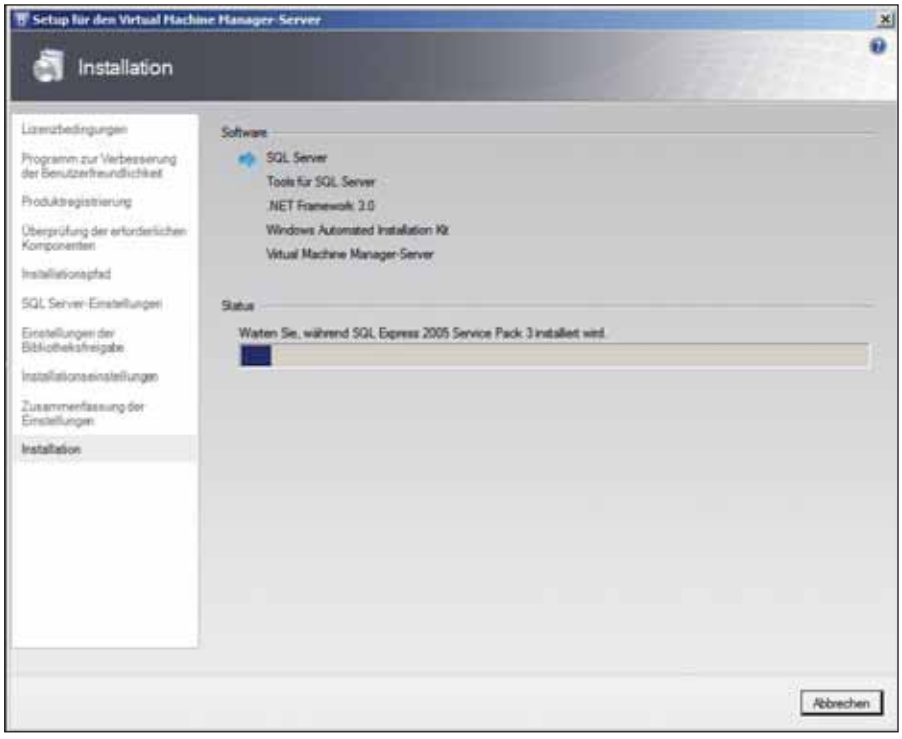


Bild 1: Die nötigen Komponenten finden bei der Installation ihren Weg auf das System

Die besondere Stärke des Virtual Machine Manager 2008 R2 liegt natürlich in der Verwaltung von Microsoft Hyper-V R2-Systemen, die sich direkt dem Management hinzufügen lassen. Sofern Hyper-V auf dem Zielsystem noch nicht installiert sein sollte, wird die Rolle über den Assistentenprozess automatisiert auf dem Zielserver eingerichtet. Hierbei kommt der zentralistische Ansatz der bisherigen Versionen weiterhin zum Einsatz. So können Sie beispielsweise durch die Nutzung des System Center Configuration Managers auf diese Weise eine Vielzahl von Bare-Metal Systemen innerhalb kurzer Zeit als Virtualisierungshosts bereitstellen und zentral verwalten. Auch werden vom VMM 2008 R2 alle Funktionen genutzt, die im Hyper-V R2 hinzugekommen sind – Funktionen wie die Live Migration von virtuellen Maschinen zwischen Windows 2008 R2 Clustered Hosts gehört hier ebenso auf die Liste wie etwa die Möglichkeit, virtuelle Datenträger im laufenden Betrieb zu einem virtuellen System hinzufügen oder vom ihm entfernen zu können. So gesehen, spielt eine Hyper-V R2-Infrastruktur erst durch den Einsatz des Virtual Machine Manager 2008 R2 ihren gesamten Funktionsumfang aus.

Installation des VMM

Für die Installation einer VMM 2008 R2-Umgebung benötigen Sie im Wesentlichen drei Komponenten, die Sie sowohl alle auf dem gleichen System als auch getrennt voneinander installieren können. Hierbei handelt es sich zunächst um den

eigentlichen VMM-Server, der die notwendigen Dienste sowie die Funktion des "Default Library Server" ausführt. Die zweite Komponente ist die VMM-Datenbank, die ab einem SQL Server 2005 mit Service Pack 3 oder einer SQL Express Edition betrieben werden kann. Sollten Sie sich für die zweite Option entscheiden, lässt sich die benötigte Express Edition-Instanz automatisiert während der Installation des Servers mitinstallieren. Möchten Sie eine vorhandene Instanz auf einem anderen Server verwenden, konfigurieren Sie während der Serverinstallation die entsprechende Auswahl des Systems und der notwendigen Verbindungseinstellungen. Die dritte benötigte Komponente ist die VMM-Administratoren-Konsole, über die Sie auf den Virtual Machine Manager zugreifen und ihn verwalten.

Als Plattform für die Installation empfiehlt sich der Einsatz eines Windows Server 2008 R2, wobei während der Installation die notwendigen Komponenten bei Bedarf automatisiert mitinstalliert werden können, wie Bild 1 zeigt. Insbesondere für kleinere Umgebungen oder erste Tests sollten Sie auch alle Komponenten auf dem gleichen Server installieren, da Sie hierdurch den Einrichtungsaufwand reduzieren können – für größere Umgebungen mit mehr als zehn zu verwaltenden Hosts sollten die Komponenten (insbesondere VMM-Datenbank und VMM-Server) aber voneinander getrennt werden, um eine bessere Skalierung zu ermöglichen.

Konfiguration auf mehreren Wegen

Die Konfiguration des VMM kann über die Administrator-Konsole oder über PowerShell erfolgen. Bei der Administrator-Konsole finden Sie die gleiche Oberflächenstruktur vor, wie sie mittlerweile von der Mehrheit der System Center-Produkte geteilt wird (siehe Bild 2). Somit steht Ihnen ein dreiteiliges Fenster zur Verfügung, wobei Sie links die Navigation der Oberpunkte finden. In der Mitte finden sich die eigentlichen Inhalte und in der rechten Spalte die mit der Microsoft Management Console 3.0 eingeführte "Action Pane" ("Aktionen"), in der Sie die jeweils zur Verfügung stehenden Aktionen für ein im mittleren Bildschirm aktiviertes Objekt sehen können. Interessant ist hierbei zu wissen, dass die grafische Konsole – wie auch schon in den vorherigen Versionen – ausschließlich als Oberfläche für PowerShell-Befehle dient. Sie haben bei jedem grafisch ausgeführten Konfigurations- oder Assistentenschritt am Ende die Möglichkeit, sich das aus Ihren Einstellungen generierte PowerShell-Skript anzeigen zu lassen.

Dies gibt Ihnen einen guten Einblick in die zur Verfügung stehenden Befehle und Optionen, was den Einstieg in die Administration über die PowerShell vereinfacht. Natürlich sollte Ihr langfristiges Ziel darin liegen, auf diesem Weg eine vollständige Automatisierbarkeit der Umgebung über PowerShell-Skripte erreichen zu können. Insbesondere für größere Umgebungen wird diese Möglichkeit für Sie verstärkt eine Rolle spielen, da sie Ihnen die Chance bietet, den manuellen Aufwand auf ein Minimum zu reduzieren.

Integration von Host-Systemen

Über den Punkt "Aktionen" auf der rechten Seite der Administratorkonsole fügen Sie neue oder weitere Hosts zu Ihrer Umgebung hinzu, auf denen – im Fall von Windows Server 2008 und Hyper-V – auch direkt die notwendigen Rollen installiert werden. Ein Assistent leitet Sie dabei durch die anfallenden Schritte, wie etwa die Auswahl des Zielsystems und des Verbindungskontos oder die Auswahl der gewünschten Hostgruppen-Zuordnung. Die so getroffe-

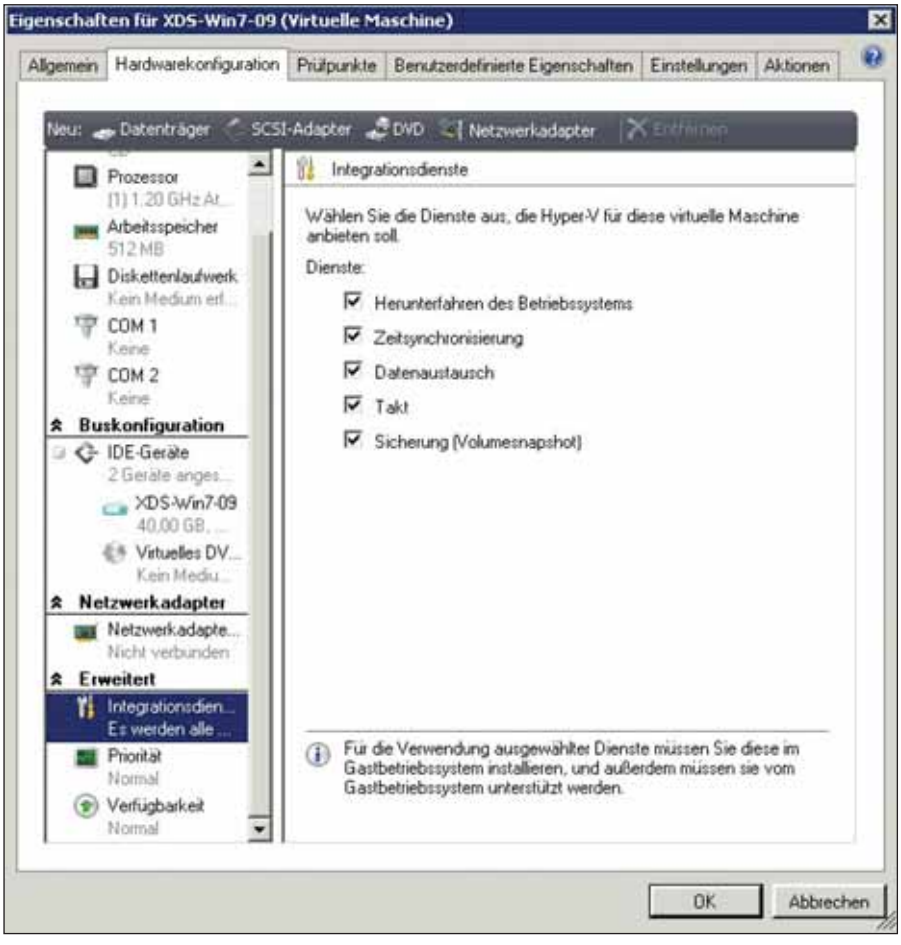


Bild 2: Die Integrationstiefe lässt sich über wenige Angaben konfigurieren

nen Einstellungen werden anschließend in Form von PowerShell-Skripten auf das Zielsystem und den VMM angewendet. Eine manuelle Installation der Virtualisierungsplattform auf den Zielsystemen ist somit nicht mehr notwendig. Sie können es natürlich trotzdem tun beziehungsweise bereits vorhandene Hostsysteme mit einbinden, was sich über die Installation des VMM-Agents realisieren lässt. Sobald Sie die gewünschten Host-Systeme ausgewählt und installiert haben, können Sie diese als Plattform für virtuelle Maschinen verwenden. Für eine bessere Übersicht und Verwaltbarkeit haben Sie die Möglichkeit, die angebundenen Host-Systeme in sogenannten Hostgruppen zusammenzufassen. Das bringt Ihnen besonders in größeren Umgebungen eine deutliche Erleichterung. Auf die gleiche Art würden auch etwa VMware-Systeme in die Konsole integriert.

Neben der Installation und Integration von Virtualisierungshosts sind natürlich der Speicherort der virtuellen Maschinen und die Vorbereitung einer möglichst einfachen Handhabung von größter Bedeutung. Um Ihnen auch an dieser Stelle die Arbeit zu erleichtern, arbeitet VMM mit sogenannten "Bibliotheken" (Libraries), in denen Sie virtuelle Festplatten im VHD-Format oder auch komplette virtuelle Maschinen sowie Vorlagen ablegen können. Auf die angelegten und mit Inhalten gefüllten Bibliotheken können Sie später von den einzelnen Virtualisierungshosts zugreifen, um die Inhalte nutzen zu können. Im Standard wird Ihr erster Server mit dem VMM auch gleichzeitig Ihr erster Bibliotheksserver.

Erstellen und Verwalten von virtuellen Systemen

Nach der Installation des Virtual Machine Manager und der Zuordnung der Virtualisierungshosts können Sie damit beginnen, virtuelle Maschinen bereitzustellen. Hierzu wählen Sie unter "Aktionen" den Punkt "Neue virtuelle Maschine" aus, woraufhin ein entsprechender Assistent startet. Insbesondere, wenn Sie viele virtuelle Maschinen mit einheitlichen Einstellungen und Konfigurationen zur Verfügung stellen wollen, empfiehlt sich der Einsatz von Vorlagen. Darin können Sie virtuelle Maschinen vollständig definieren und konfigurieren, so dass Sie diese Arbeiten nicht mehrfach für die Erstellung von identischen Systemen durchführen müssen.

Nachdem Sie die von Ihnen benötigten Vorlagen erstellt haben, sind Sie innerhalb kürzester Zeit in der Lage, eine große Anzahl von virtuellen Systemen zu provisionieren. Im Optimalfall speichern Sie Ihre Vorlagen in einer Bibliothek, um Sie später von allen Virtualisierungshosts Ihrer Umgebung aus nutzen zu können.

Natürlich können Sie die Eigenschaften einer virtuellen Maschine auch im Nachhinein noch anpassen. Hierzu öffnen Sie einfach über einen Rechtsklick auf der VM die Eigenschaften und wählen in der Menüstruktur den gewünschten Bereich aus, an dem Sie Anpassungen durchführen wollen. Wie Bild 2 zeigt, können Sie hierbei sogar bis auf die Integrationstiefe der Virtualisierungsplattform hinab konfigurieren, wie die virtuelle Maschine sich verhalten soll und welche Aufgaben die Plattform automatisiert übernimmt.

Haben Sie die virtuellen Maschinen erstellt, können Sie sie auf den Virtualisierungshosts Ihrer Umgebung ausführen. Im Vergleich zu den Vorgängerversionen des VMM und des Hyper-V haben Sie mit der aktuellen Version einige interessante Funktionen hinzubekommen, wobei die Live Migration die Funktionsliste aus der Sicht vieler Administratoren dominiert. Während noch in der direkten Vorgängerversion virtuelle Systeme für eine Migration heruntergefahren und

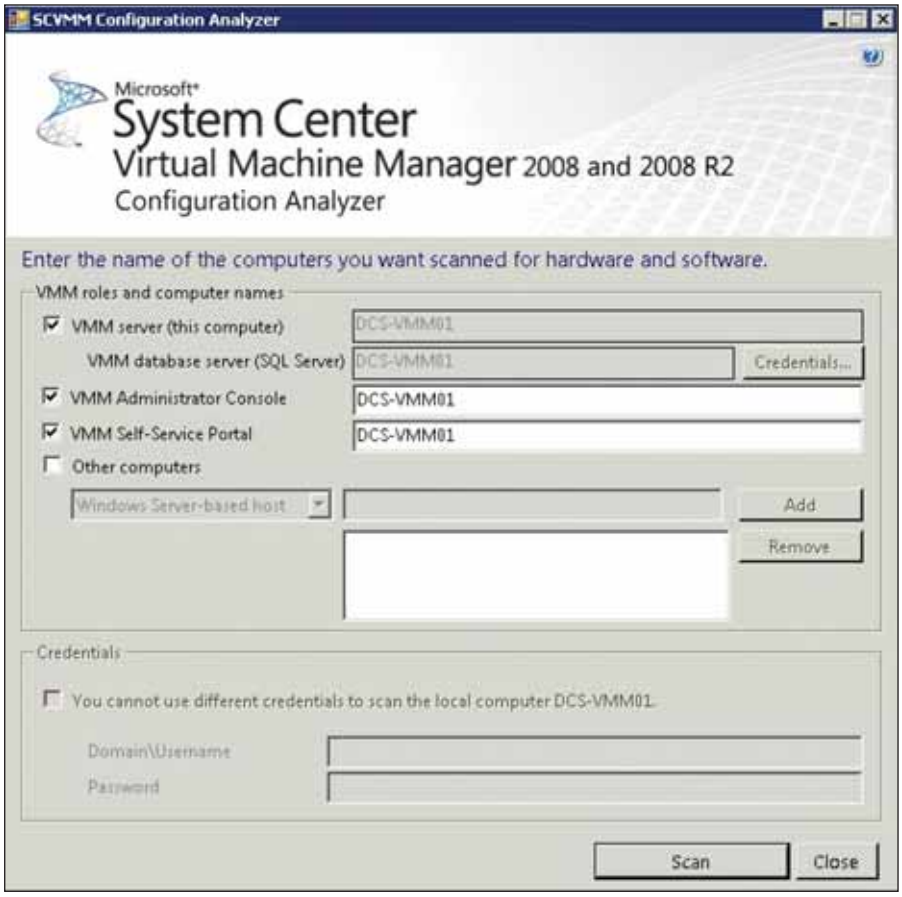


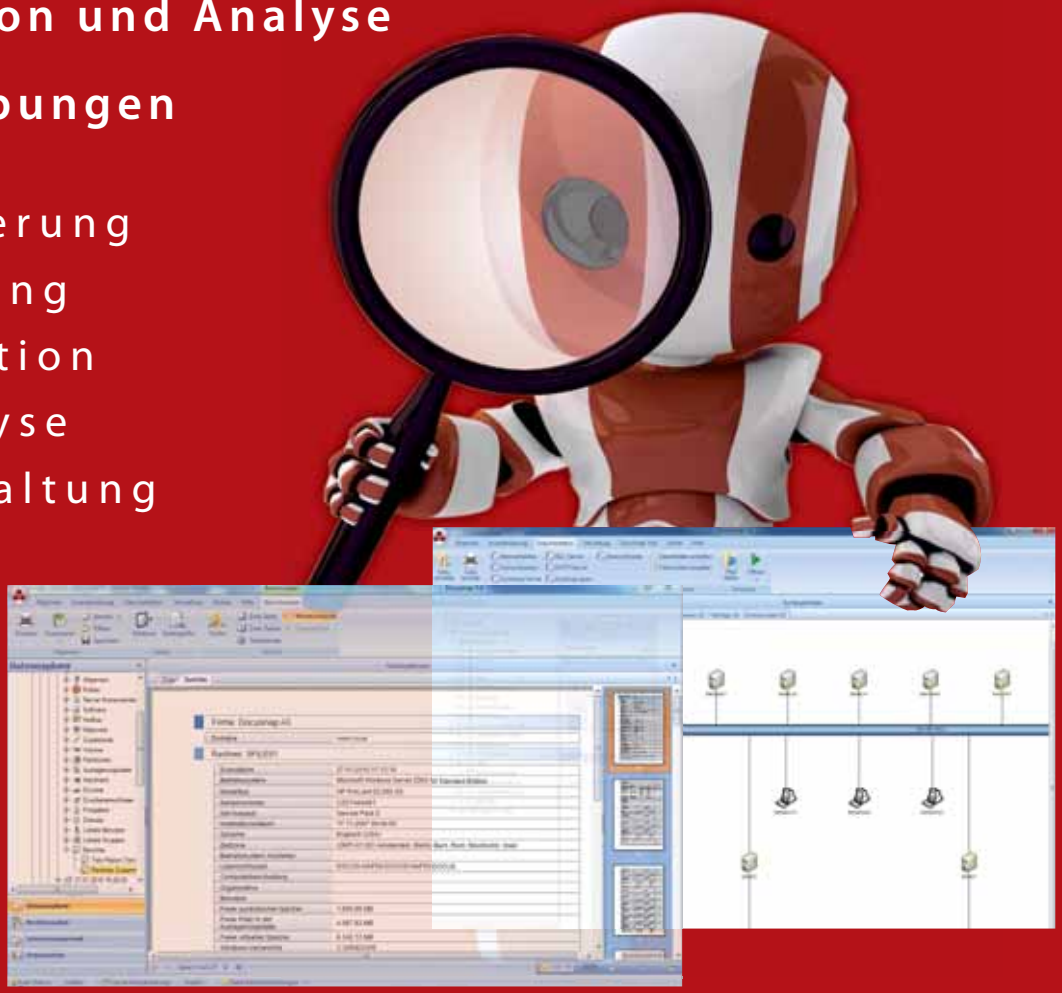
Bild 3: Der Configuration Analyzer übernimmt den Vorab-Check

Docusnap®

Schluss mit dem IT-Chaos!

Dokumentation und Analyse von IT-Umgebungen

- Inventarisierung
- Visualisierung
- Dokumentation
- Rechteanalyse
- Lizenzverwaltung



www.docusnap.de

auf dem Zielhost neu gestartet werden mussten, steht nun ein Verschieben der Systeme im laufenden Betrieb zur Verfügung. Die einzige Voraussetzung hierfür ist der Betrieb von Windows 2008 R2 Clustered Hosts. Ältere oder andere Versionen einer Virtualisierungsplattform unterstützen diese Funktion nicht.

Erweiterungen und Integration

Ein weiteres interessantes Werkzeug für die Arbeit mit VMM ist der Configuration Analyzer. Wie Bild 3 zeigt, können Sie mit diesem kleinen Tool die Leistung und Konfigurationsparameter Ihrer Umgebung analysieren. Hierdurch sind Sie in der Lage, schnell und komfortabel Konfigurationsfehler oder sonstige Probleme in Ihrer Umgebung zu finden.

In der Realität wird aber wahrscheinlich nicht VMM selbst die Komponente sein, die Ihnen Probleme bereitet – vielmehr werden es die virtuellen Maschinen sein, die es zu dimensionieren und zu überwachen gilt. Ebenso wird sich Ihnen im Vorfeld oftmals die Frage stellen, welche der vorhandenen Systeme sich überhaupt für eine Virtualisierung eignen und welche – beispielsweise aus Last- oder Leistungsgründen – lieber als physikalische Server bestehen bleiben sollten. Und bei genau dieser Fragestellung spielt der Virtual Machine Manager 2008 R2 einen seiner größten Trümpfe aus: die Integration mit dem System Center Portfolio und insbesondere dem System Center Operations Manager.

Sofern Sie einen SC OpsMgr im Einsatz haben und Ihre Systeme mit einem entsprechenden Agenten überwachen, kann VMM die hierbei gewonnenen Daten verwenden, um eine Beurteilung und Empfehlung für die Virtualisierung eines Systems zu erstellen. Nur wenn die erfassten Lastdaten eine Virtualisierung des Systems erlauben würden, erhalten Sie einen entsprechenden Vorschlag für die Virtualisierung. Gleiches gilt für bereits virtualisierte Systeme: Wie skaliert Ihre Umgebung und welche Leistungsreserven stehen Ihnen noch zur Verfügung? Sind Ihre Systeme bereits ausgelastet oder können Sie noch weitere virtuelle Maschinen aufbringen? Auf diese Fragen kann Ihnen der Operations Manager eine Antwort geben, sofern Sie ihn mit den entsprechenden Management Packs für VMM und die eingesetzte Virtualisierungsplattform – also etwa Hyper-V R2 – ausgestattet haben. Wie auch bei den anderen Produkten des System Center-Portfolios sind sehr viel Logik und Know-how in den Management Packs hinterlegt, die Ihnen eine qualifizierte Informationsbasis bieten, auf der Sie Ihre Entscheidungen aufbauen können.

Eine weitere interessante Komponente, die auch schon in früheren Versionen des VMM vertreten war, ist das Self-Service-Portal. Diese Komponente, die Sie separat von der Installations-CD nachinstallieren können, ist eine Web-basierte Anwendung, über die Sie Benutzern erlauben, eigene virtuelle Maschinen zu erstellen und zu verwalten. Über entsprechende Rollen steuern Sie hierbei, welche Aktionen ein Benutzer auf seinen virtuellen Maschinen ausführen können soll und welche Formate und Vorlagen ihm hierfür zur Verfügung stehen. Das Erstellen und Konfigurieren der Rollen geschieht in der Administrations-Konsole unter "Verwaltung / Benutzerrollen". Im daraufhin erscheinenden Assistenten können Sie den gewünschten Namen, die zuzuordnende Gruppe und die Zugriffseinstellungen konfigurieren. Nach der Auswahl der bereitzustellenden Vorlagen können Sie die zu vergebenden Berechtigungen verwalten. Mit Hilfe dieser Komponente und ihrem Rollen-basierten Steuerungsmodell stellen Sie beispielsweise für Schulungs-, Entwicklungs- oder Testszenarien innerhalb kürzester Zeit sehr leistungsfähige Umgebungen bereit, was für Ihr Unternehmen nicht nur einen technischen, sondern auch organisatorischen Mehrwert bieten kann. Um den Benutzern bei eventuell trotzdem auftretenden Problemen eine Hilfestellung bieten zu können, können Sie unter "Verwaltung / Allgemein / Self-Service-Kontakt für Administratoren" eine Mailadresse hinterlegen, welche Sie für Informationsmeldungen und Anforderungen verwenden wollen.

Wenn die Anwender hierdurch selbst in der Lage sind, ihre benötigten virtuellen Systeme bereitstellen und verwalten zu können, muss dies nicht mehr von

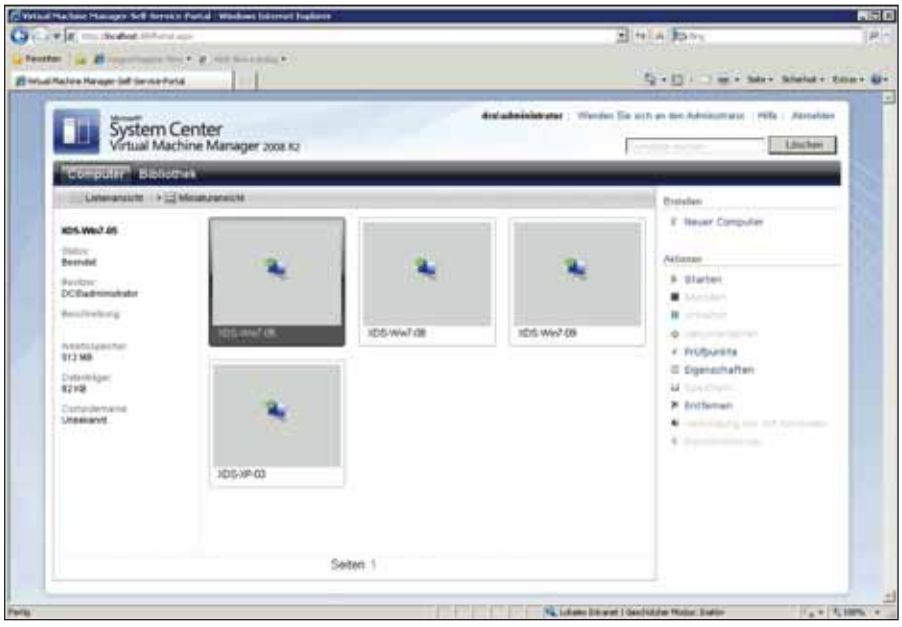


Bild 4: Das Self-Service-Portal kommt sehr übersichtlich daher

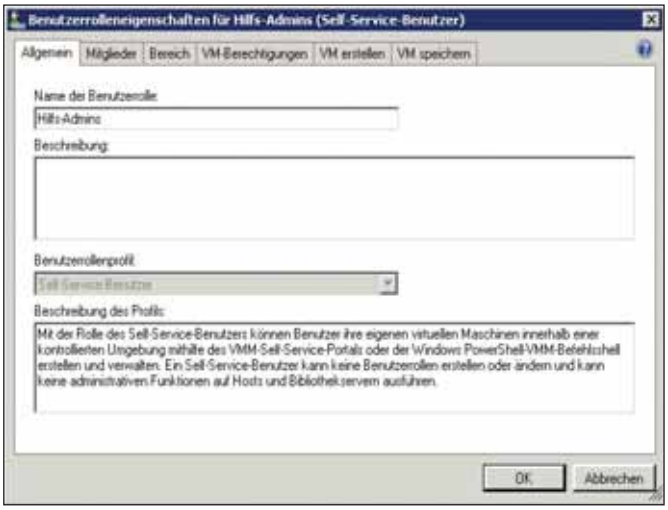


Bild 5: Das Konfigurieren der Rollen mit Hilfestellung

Ihnen erledigt werden. Eine Verkürzung der Prozesskette kann an dieser Stelle für Sie einen direkten Zugewinn an Zeit und Anwenderzufriedenheit bedeuten.

Fazit

Wie auch schon seine Vorgänger reiht sich der Virtual Machine Manager 2008 R2 nahtlos in das System Center ein und verfügt über eine Vielzahl von Schnittstellen zu den weiteren Komponenten des Produktportfolios. Besonders hervorzuheben ist hierbei natürlich die Integration mit dem System Center Operations Manager und dem System Center Configuration Manager, über den Sie das Monitoring, die Informations- und Lastauswertung sowie das Konfigurationsmanagement realisieren können. Aber auch Funktionen wie das Self-Service Portal, über das Sie ausgewählten Benutzern einen Zugriff auf einzelne virtuelle Maschinen geben können, sind eine Bereicherung der Lösung. Nicht zuletzt schafft sie hierdurch den Sprung von einer reinen Backend-Plattform bis nach vorne zu den Benutzern, was den Stellenwert der Virtualisierung weiter erhöht.

Sollten Sie sich in einer reinen Microsoft-Umgebung mit dem Thema der Servervirtualisierung auseinandersetzen, wird für Sie kein Weg am System Center Virtual Machine Manager vorbeiführen. Aber auch für den Fall, dass Sie etwa bereits über eine Servervirtualisierung von VMware verfügen, können Sie diese nun reibungslos in den VMM integrieren und Ihre ESX/vSphere-Umgebung hierüber in einer zentralen Oberfläche verwalten. Auf diese Weise wird Ihnen der Ein- beziehungsweise Umstieg auf die Microsoft Virtualisierung mit Hyper-V wesentlich vereinfacht, da Sie eine Von-jetzt-auf-gleich-Migration Ihrer virtualisierten Systeme vermeiden können und somit in Ruhe das notwendige Wissen und die notwendigen Erfahrungen mit dem SC VMM aufbauen können. *(dr)*

Remote-Administration mit UltraVNC

Die Einfach-Fernbedienung

von Dr. Holger Reibold

Für Administratoren gibt es kaum etwas Lästigeres, als sich von PC zu PC hangeln zu müssen, um dort – oft durch unsachgemäße Handhabung verursachte – Probleme zu lösen. Der Arbeitsablauf lässt sich mit dem richtigen Werkzeug erheblich optimieren: Greifen Sie doch zur freien Remote-Software UltraVNC. In diesem Workshop erklären wir Ihnen den Umgang mit diesem Tool und beschreiben dessen wichtigste Kniffe.

Remote-Control-Software gibt es wie Sand am Meer. Neben einer Vielzahl an kommerziellen Lösungen haben sich insbesondere die verschiedenen VNC-Lösungen (Virtual Network Computing) etabliert. Sie haben inzwischen einen derart hohen Reifegrad erreicht, dass sie bedenkenlos in Produktionsumgebungen eingesetzt werden können. Unter den frei verfügbaren Remote-Control-Lösungen genießt UltraVNC [1] einen hervorragenden Ruf und dürfte insbesondere für die Fernwartung von Windows-Systemen die beliebteste Lösung sein.

Mithilfe von UltraVNC können Sie den Monitorinhalt eines entfernten Rechners über ein beliebiges Netzwerk auf dem lokalen PC anzeigen. UltraVNC erlaubt Ihnen die vollumfängliche Steuerung des PCs. Sie können mit dem Remote-Rechner arbeiten, als säßen Sie direkt davor. Dank verschiedener Erweiterungen wie beispielsweise SingleClick muss nicht einmal eine vorinstallierte Software auf dem Rechner installiert sein und es ist auch sonst kein kompliziertes Verfahren erforderlich, um die Remote-Control-Unterstützung nutzen zu können. Das vielleicht einzige Manko: UltraVNC lässt sich nur zur Remote-Verwaltung von Windows-Systemen nutzen. Die Steuerung selbst ist dank eines Java-basierten Viewers von jeder beliebigen Plattform aus möglich.

Große Funktionsvielfalt

UltraVNC hat neben dem einfachen Remote-Zugriff auf Drittsysteme eine ganze Menge an interessanten Zusatzfunktionen zu bieten. Nicht umsonst gilt das Tool als das VNC-Derivat mit den umfangreichsten Ausstattungsmerkmalen. Die Umgebung nutzt eine typische Client-Server-Architektur, wobei der Server auf den zu steuernden Systemen ausgeführt wird. Der Zugriff erfolgt von einem beliebigen Client aus. Für Windows-Rechner steht der Client mit den umfangreichsten Steuerfunktionen zur Verfügung. Daneben gibt es spezielle Viewer, die sich beispielsweise im Webbrowser oder auf einem PDA- oder Blackberry-Gerät ausführen lassen.

Da die verschiedenen VNC-Derivate allesamt per RFB (Remote Framebuffer Protocol) miteinander kommunizieren, kann ein UltraVNC-Client auf andere VNC-kompatible Server zugreifen und analog können andere VNC-Viewer andere UltraVNC-Server steuern. UltraVNC-Server und -Client können Ihre Verbindung mithilfe eines 128-Bit-RC4-Schlüssels absichern. Zudem lassen sich zwischen Client und Server über einen speziell konfigurierbaren Datenkanal Dateien zwischen den Systemen transferieren. Die Übermittlung basiert auf P2P-Technologie.

Spezialtreiber für schnelle Grafikübermittlung

Ein weiterer Vorteil: Die Steuerung eines entfernten PCs ist quasi unabhängig von der Netz- und Leitungskapazität, weil VNC ein optimiertes Übertragungsprotokoll verwendet. Das gilt insbesondere für die Grafikdarstellung aufseiten des Clients. Der UltraVNC-Mirror-Treiber wird auf dem Remote-System als Videotreiber installiert, so dass er der Windows-Installation eine Grafikkarte simuliert. Dadurch lassen sich die Bildschirminhalte bereits auf Kernel-Space-Ebene abgreifen, was die CPU-Belastung des UltraVNC-Servers erheblich reduziert. Ferner können Sie dank der Multicast-Unterstützung von einem Viewer aus gleichzeitig mehrere Server steuern.

Schneller Zugriff ohne Installation

Eine weitere Besonderheit von UltraVNC trägt die Bezeichnung SingleClick: Damit können Sie einen verkleinerten und optimierten UltraVNC-Server so konfigurieren, dass dieser bei seiner Ausführung versucht, einen im Listen-Mode befindlichen Viewer auch über das Internet oder im

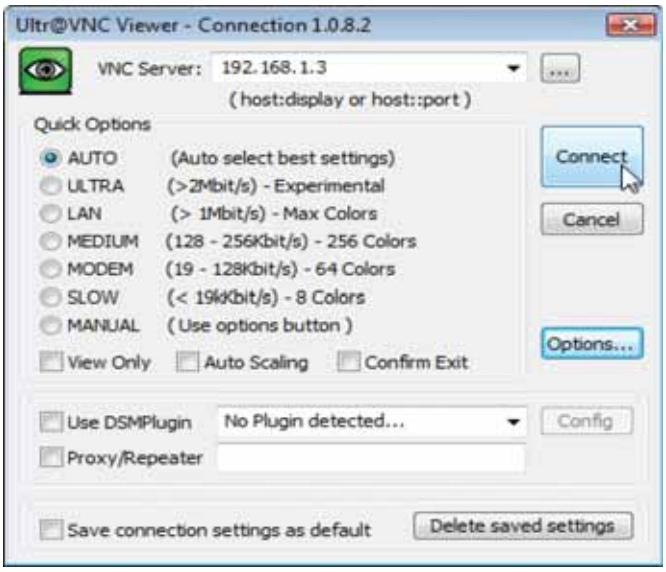


Bild 1: Bei der Eingabe der IP-Adresse des UltraVNC-Servers lassen sich gleichzeitig die wichtigsten Verbindungsoptionen festlegen

LAN zu erreichen. Es handelt sich dabei um eine einzelne ausführbare Datei, die vorzugsweise dafür verwendet wird, Kunden bei Softwareproblemen eine einfache Möglichkeit zu bieten, sich mit einem Kundensupport in Verbindung zu setzen.

Gute Chatfunktion, eingeschränkte Verschlüsselung

Die textbasierte Chat-Funktion eignet sich hervorragend für die Kommunikation der beteiligten Nutzer über eine bestehende VNC-Verbindung. Der Viewer bietet außerdem eine stufenlose Skalierung, die den Server-Bildschirm durch die Angabe der entsprechenden Option auf die passende Bildschirmauflösung des Viewers überträgt. Die Angabe der Skalierung erfolgt in Prozent-Werten. Während einer Verbindung lässt sich eine Vielzahl an Routinetätigkeiten über die Viewer-Toolbar abrufen oder initiieren. Das Werkzeug unterstützt außerdem verschiedene Authentifizierungsverfahren. Der Zugriff auf den Server ist durch ein Passwort geschützt, bei dem jedoch nur die ersten acht Stellen durch DES verwendet werden. Dieser sicherheitstechnische Kritikpunkt ist indes nicht UltraVNC anzulasten, sondern vielmehr dem RFB-Protokoll. Zusätzlich besteht aber die Möglichkeit, das MS-Logon-I-Verfahren für NT-Domänen zu verwenden. Ein weiterer Weg ist das MS-Logon-II-Verfahren für die Anbindung an einen Verzeichnisdienst wie beispielsweise ein Active Directory.

Konfiguration des Servers

Die Inbetriebnahme und Nutzung der Grundfunktionen von UltraVNC ist denkbar einfach: Sie laden das aktuelle Server-Installationspaket von der UltraVNC-Website herunter und führen auf den zu wartenden PCs das Setup aus. Serverseitig können neben der eigentlichen Server-Variante auch der Viewer, Verschlüsselungs-Plug-Ins und ein Repeater installiert werden. Die benutzerdefinierte Installationsvariante erlaubt Ihnen zudem die Konfiguration von UltaVNC als Dienst und von MS Logon II. Unter Windows Vista sollten Sie die Programmausführung auf ein Benutzerkonto beschränken. Nach dem Abschluss der Installation können Sie den Server über das Tray-Icon mit Admin Properties konfigurieren. Die Benutzerschnittstelle von UltraVNC ist in einer deutschsprachigen Variante verfügbar, doch hinkt die Lokalisierung bei neuen Programmversionen immer hinterher. Daher beschränken wir uns hier auf die aktuelle englischsprachige Fassung.

Auf Seiten der Server-Administration können Sie die Art und Weise steuern, wie das Remote-Tool eingehende Verbindungsanfragen behandelt, welche Authentifizierungsschema es für den Zugriff auf den Server verwendet, ob der Dateitransfer möglich ist und welche Plug-Ins nutzbar sind. Zunächst sollten Sie im Bereich "Incoming Socket Connections" mit der Option "Accept Socket Connections" sicherstellen, dass der Server Remote-Verbindung annimmt und so die Fernsteuerung überhaupt möglich machen. Unter Ports können Sie die Verbindungsaufnahme auf einen bestimmten Port beschränken. Sie sollten die Voreinstellung "Auto" beibehalten, damit Client und Server die Port-Verwendung selbst aushandeln. Wenn Sie auf dem Zielrechner den Client und Server installiert haben, können Sie zu Testzwecken die Verwendung von Loopback-Verbindungen mithilfe der Option "Allow Loopback Connections" aktivieren. Wenn Sie mithilfe eines Webbrowsers auf den Server zugreifen wollen, stellen Sie sicher, dass die Option "Enable Java-Viewer" aktiviert ist.

Der Bereich "Authentication" ist naturgemäß einer der wichtigsten. Hier weisen Sie dem Server das Passwort zu, das der Viewer für den erfolgreichen Verbindungsaufbau benötigt. Sollten Sie die MS-Logon-Funktionalität nutzen wollen, so aktivieren Sie das entsprechende Kontrollkästchen und geben bis zu drei Gruppen in dem Dialog "MS logon setup" an. Beachten Sie, dass die Gruppen eins und zwei über Vollzugriff auf den UltraVNC-Server verfügen, Gruppe drei hingegen nur Leserechte besitzt. Noch einen Schritt weiter geht die Authentifizierung per MS Logon II. Hiermit gewähren Sie Gruppen Zugriff, die in einem Active Directory angelegt sind. Der Vorteil: Der Zugriff ist über Domänengrenzen hinweg möglich. Mithilfe des integrierten Kommandozeilenprogramms *MSLogonACL.exe* können Sie Ihre Listen bei Bedarf im- und exportieren. Das vereinfacht die Nutzung auf Drittsystemen. Für den Export verwenden Sie folgenden Befehl:

```
MSLogonACL.exe /e /exportdatei.txt
```

Der entsprechende Importbefehl lautet:

```
MSLogonACL.exe /i /a
  /exportdatei.txt
```

Die Server-Konfiguration wird übrigens in der Konfigurationsdatei *ultravnc.inf* hinterlegt. Es handelt sich um eine einfache

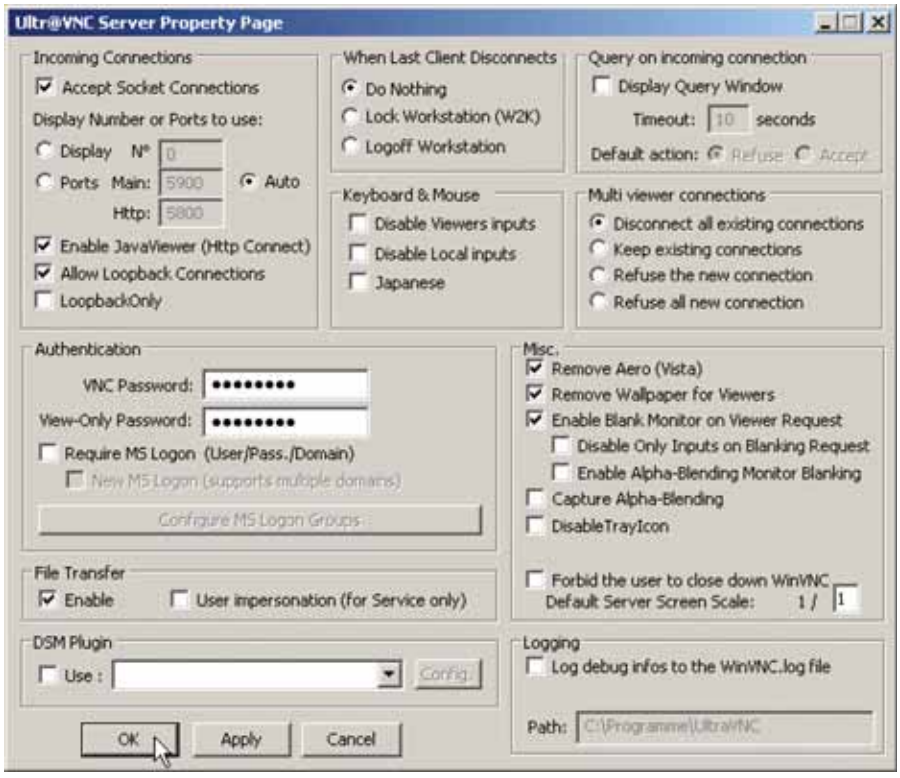


Bild 2: Ein erster Blick auf die UltraVNC-Server-Konfiguration

Textdatei, die Sie mit einem Editor Ihrer Wahl bearbeiten und bequem auf Drittsysteme übertragen können. Um den Datentransfer zwischen dem Viewer und dem Server zu ermöglichen, aktivieren Sie unter "File Transfer" die Option "Enable". Wenn Sie unter "Authentication" das VNC-Passwort definiert haben, müssen Sie die Option "User impersonation (for Service only)" aktivieren, da es ansonsten zu Problemen im Datenübertragungsmodus kommen kann. Auf Seiten des Servers stehen Ihnen über das Tray-Icon weitere nützliche Funktionen zur Verfügung. Sie öffnen mit dem Kommando "List all Clients" einen Dialog, der die aktuell verbundenen und die auf eine Verbindung wartenden Clients anzeigt. Über diesen Dialog ist ebenso die Chat-Funktion verfügbar.

Konfiguration des Viewers

Als Nächstes sollten Sie sich der Konfiguration des Viewers widmen. Dieser steht im Download-Bereich des UltraVNC-Projekts als Standalone-Applikation zur Verfügung. Nach dem Start des Viewers geben Sie im Eingabefeld "VNC Server" die IP-Adresse und bei einer benutzerdefinierten Server-Konfiguration den Port an. Unter "Quick Options" können Sie die verfügbare Übertragungskapazität zwischen Server und Client für die optimale Datenübertragung zwischen beiden bestimmen. In der Regel sollten Sie das mit der Option "Auto" den beiden selbst überlassen. Sollten Sie ein Plug-In verwenden, müssen Sie es im Auswahlmenü "Use DSMPlugin" aktivieren und konfigurieren. Über die Options-Schaltfläche können Sie zudem verschiedene Maus-, Tastatur- und Darstellungs-spezifische Einstellungen wie die Ansicht der Viewer-Werkzeugleiste anpassen.

Ein Klick auf die Schaltfläche "Connect" fragt das Passwort für den Server-Zugriff ab und stellt die Verbindung zum UltraVNC-Server her. Auf Seiten des UltraVNC-Servers wird eine Server-Komponente installiert, die den Zugriff über einen Standard-Browser erlaubt. Für den Zugriff verwenden Sie folgende URL: http://{Hostname oder IP-Adresse}:5800. Nach der Annahme des Zertifikats startet die Java-basierte Schnittstelle und Sie können nach der Passwortübermittlung auf den UltraVNC-Server zugreifen. Über die JavaViewer-Leiste stehen Ihnen die Grundfunktionen wie beispielsweise der Dateitransfer zur Verfügung.

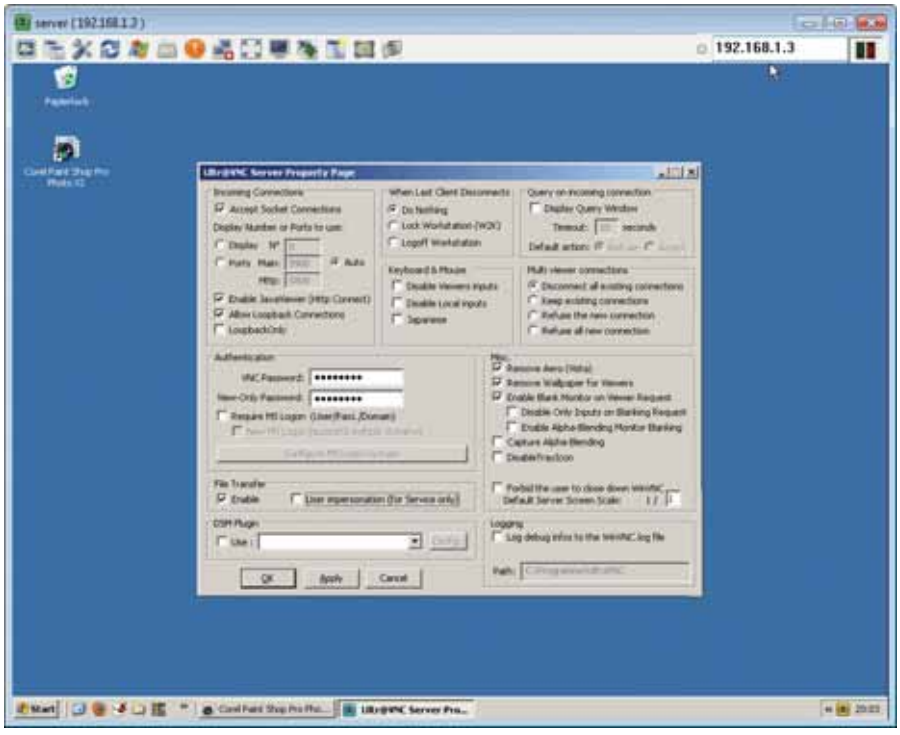


Bild 3: Der UltraVNC-Viewer und seine Einstellungen

Bestellen Sie jetzt

das IT-Administrator

Sonderheft II/2009!

180 Seiten Praxis-Know-how + Tools-CD
rund um das Thema

Virtualisierung

zum Abonnenten-Vorzugspreis* von

nur € 29,90!

** IT-Administrator Abonnenten erhalten das Sonderheft II/2009 für € 29,90.*
Nichtabonnenten zahlen € 34,90.

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

administrator Das Magazin für professionelle System- und Netzwerkadministration

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

☐ **Ja**, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft II/2009 + Tools-CD zum **Abonnenten-Vorzugspreis** von nur **€ 29,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft II/2009 + Tools-CD zum Preis von **€ 34,90** 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.

ITA 0310

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

E-BOOK SYSTEMS
Abos und Einzelhefte gibt es auch als E-Paper

Heinemann Verlag
Leopoldstraße 85
D-80802 München
Tel: 089-4445408-0
Fax: 089-4445408-99
Geschäftsführung:
Anne Kathrin Heinemann
Matthias Heinemann
Amtsgericht München HRB 151585

Mehr Leistung und Komfort durch Plug-Ins

Die Grundfunktionalität von UltraVNC lässt sich durch Plug-Ins erweitern. Bei einer Server-Standardinstallation sind bereits drei Erweiterungen enthalten, die Ihnen helfen, die Kommunikation zwischen dem Server und dem Viewer sicher zu gestalten. Sie aktivieren und konfigurieren die Plug-Ins in der Server-Konfiguration, indem Sie unter "DSM Plugin" das Kontrollkästchen "Use" aktivieren und dann eine der Erweiterungen auswählen. DSM steht dabei für Data Stream Modification. Die Plug-In-Konfiguration erfolgt über die Schaltfläche "Config". Das Plug-In MSRC4Plugin erlaubt die Verwendung eines RC4-Schlüssels. In der Plug-In-Konfiguration bestimmen Sie die Schlüssellänge (von maximal 128 Bit) und erzeugen die Schlüssel. Die beiden DSM-Plug-Ins SecureVNCPlugin und SecureVNCPluginARC erlauben jeweils das Erzeugen eines Server- und eines Viewer-Schlüssels.

Nützliche Helfer für VNC-Administratoren

Wenn Sie hohe Ansprüche an Ihre VNC-Umgebung stellen und intensiv mit dieser Remote-Lösung arbeiten wollen, so werden Sie feststellen, dass UltraVNC hier und da an seine Grenzen stößt. Mit den richtigen Tools kommen Sie trotzdem weiter. Wenn Sie nicht wissen, wo sich in Ihrer Infrastruktur bereits VNC-Server befinden, so hilft Ihnen der freie VNC Manager [5]. Hierbei handelt es sich um einen Scanner, der die in Ihrem Netzwerk betriebenen VNC-Server aufspürt. Beachten Sie, dass das Tool leider nicht mehr weiterentwickelt wird, aber Ihnen dennoch wertvolle Dienste leistet. Nach dem Scan-Vorgang präsentiert Ihnen der VNC Manager die gefundenen Server und erlaubt die Verbindungsaufnahme. Sie können die Ergebnisliste übrigens ins Text- oder HTML-Format exportieren. Der VNC-Manager kann auch Nicht-Windows-Server finden und verwalten.

Um einen UltraVNC-Server auf einem System zu installieren, müssen Sie – zumindest mit UltraVNC-eigenen Mitteln – den Installationsvorgang auf jedem System selbst durchführen. Dies kann eine sehr zeitintensive Angelegenheit werden, wenn Sie UltraVNC auf vielen Systemen, womöglich über viele Abteilungen, Gebäude oder gar Standorte hinweg, ausrollen müssen. Dieses Problem lösen Sie mit ChrisControl [6]. Dieses Spezialtool erlaubt ab Version 1.7 die Installation von einem zentralen System aus. Alternativ dazu können Sie auf VNCon [7] zurückgreifen. Dieses Administrations-Werkzeug erlaubt die Ferninstallation von VNC-kompatiblen Systemen auf Fremdrechnern, den Fernzugriff und das Versenden von Nachrichten an VNC-Server. Sie können mit VNCon sogar auf eine ganze Gruppe von VNC-Systemen identische Einstellungen anwenden. Leider wird auch dieses Werkzeug nicht weiterentwickelt.

Speziell für den Einsatz in Klassenräumen ist iTALC [8] konzipiert. Diese Remote-Steuerzentrale erlaubt das An- und Ausschalten einzelner Systeme, das Senden von Nachrichten, das Sperren von Rechnern und das Erstellen von Schnappschüssen. In eine ähnliche Richtung geht die Zielsetzung von BigBrother [9]. Auch diese VNC-basierte Lösung ist für den Einsatz in Schulungsräumen konzipiert. Ein weiteres sehr interessantes Managementwerkzeug ist VNC Control [10]. Dieses Tool vereint mehrere Funktionen unter einer Haube. Sie können damit zunächst Ihr Netzwerk auf (Ultra)VNC-Installationen durchsuchen, die gefundenen Server dann beispielsweise in Gruppen zusammenfassen und auf diese verschiedene Einstellungen anwenden.

So optimieren Sie die Grafikübermittlung

Das Prinzip einer VNC-Umgebung ist einfach: Zwischen Server und Viewer besteht eine Kommunikationsverbindung, die Maus-, Tastatureingaben und das Grafiksignal in Echtzeit über das Netzwerk übermittelt. Für die Übermittlung der Daten ist das RFB-Protokoll zuständig. Da sich die Bildschirmauflösungen und die Menge der übertragenen Daten zunehmend nach oben verändern, ist dieses altertümliche Protokoll oft überfordert. Die Lösung für diese gewachsenen Anforderungen sind sogenannte Mirror-Treiber, die speziell für die Übermittlung von grafischen Daten über eine Netzwerkverbindung entwickelt wurden. Für die UltraVNC-Komponenten steht unter [2] der passende Treiber zum Download bereit.

Nach der Installation finden Sie im Windows-Geräte-Manager den neuen Grafikkarteneintrag "Winvnc video hook driver". Vergleichbare Treiber kommen bei Videokonferenzlösungen zum Einsatz. Im Hintergrund sorgt die *vnchook.dll* für die verbesserte Übertragung. Der Mirror-Treiber für UltraVNC ist inzwischen allerdings recht betagt. Er stammt aus dem Jahre 2004, was seiner Leistung aber keinen Abbruch tut. Wenn Sie den UltraVNC-Mirror-Treiber unternehmensweit installieren wollen, sollten Sie zu einer speziellen Netzwerkinstallationsvariante greifen, die unter [3] verfügbar ist. Wenn Sie einen Treiber neueren Datums vorziehen, so können Sie alternativ zum Mirror-Treiber Demoforce Mirage greifen. Dieser Treiber [4] wurde eigentlich für Tight-VNC ausgearbeitet, lässt sich aber auch unter UltraVNC einsetzen.

Add-ons für fast jeden Zweck

UltraVNC ist in seiner Standardvariante bereits ein Werkzeug, mit dem sich die allermeisten Aufgaben bei der Remote-Administration bewerkstelligen lassen. Wer in der Praxis trotzdem an Grenzen stößt, kann diese mit dem richtigen Hilfsmittel lösen. Wenn Sie UltraVNC in einer typischen Netzwerkinfrastruktur betreiben und über Firewall-, Router- oder Proxy-Server-Komponenten hinweg kommunizieren wollen, so ist der Einsatz eines Repeaters erforderlich. Sie finden den Repeater unter [11]. Nach dem Entpacken müssen Sie ihn nur noch auf dem System ausführen und konfigurieren, dass er als Signalverstärker dienen soll.

Der Repeater kann in zwei verschiedenen Modi arbeiten. In Modus I betreiben Sie mehrere UltraVNC-Server, die über das Internet ansprechbar sein sollen. Der Repeater ermöglicht es, dass Sie nicht jeden Server einzeln ansprechen müssen, sondern auf dem Repeater werden die Daten gebündelt und an den Viewer übermittelt. Über den Repeater ist so insbesondere die Kommunikation über einen NAT-Router möglich. Bei Modus II besitzt der Repeater-Rechner eine direkte Internet-Verbindung. Auf dem Repeater werden die Anfragen der Viewer, Server und SingleClick-Installationen gebündelt. In der Praxis funktioniert das allerdings nicht immer zuverlässig. Sie sollten sich in Produktionsumgebungen auf Modus I beschränken.

Mit NAT2NAT [12] gibt Ihnen das UltraVNC-Team eine weitere praktische Lösung an die Hand, mit der Sie Verbindungen zwischen Server und Viewer hinter einem

Bild 4: Das Add-on VNCon durchforstet Ihr Netzwerk nach VNC-Servern und erlaubt sogar deren Remote-Installation

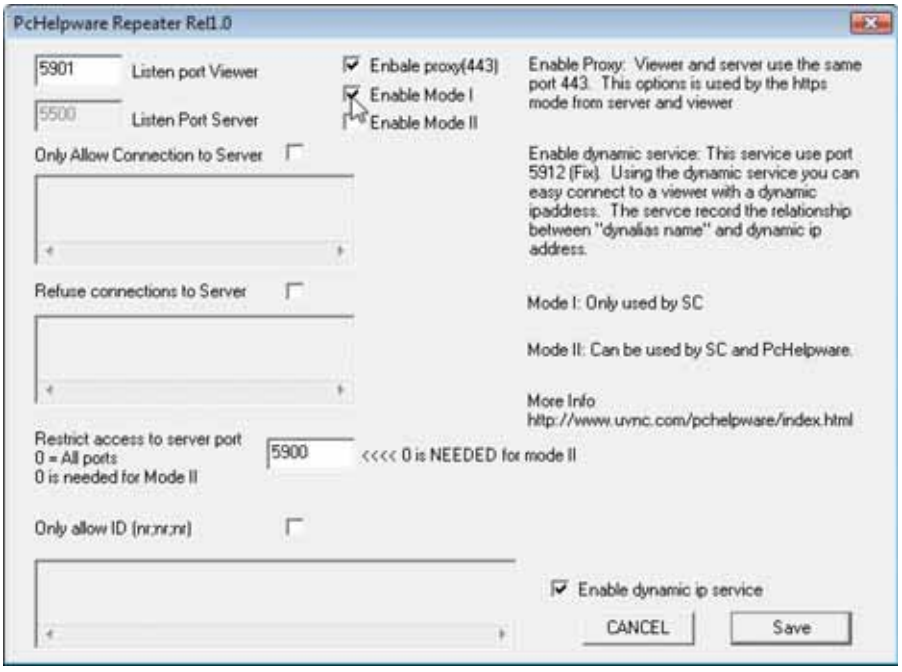


Bild 5: Die Einrichtung eines Repeaters ermöglicht die Fernwartung über Firewalls und Proxy-Server hinweg. Beschränken Sie sich hier aber auf Modus I, da in Modus II mit verschiedenen Problemen zu rechnen ist.

NAT-Router herstellen können, ohne dass dabei eine Anpassung der Router-Konfiguration erforderlich ist. Sollten Sie Zugriff auf einen NAT-Router haben, so können Sie mit dem Add-on Port Forwarding [13] UltraVNC-Ports weiterleiten. Beim Einsatz des Add-ons ist kein Repeater erforderlich. Schließlich finden Sie auf der UltraVNC-Website noch eine SingleClick-Variante [14], die speziell für den Helpdesk-Einsatz konzipiert ist. Neben diesen offiziellen Add-ons existiert eine Menge weiterer Ergänzungen, Zusätze und sonstiger Helfer, die Ihnen das Leben mit (Ultra)VNC-Umgebungen leichter machen. Mehr dazu erfahren Sie im Kasten "Nützliche Helfer für VNC-Administratoren".

Fazit

Mit UltraVNC steht Ihnen die benutzerfreundlichste VNC-Variante zur kostenlosen Verwendung zur Verfügung. Sie bietet alle notwendigen Funktionen für die Fernsteuerung und Wartung von Clients sowie die täglich anfallenden Helpdesk-Anforderungen. Dank der sehr aktiven Community können Sie sicher sein, dass sich diese VNC-Variante weiter verbessern wird und Sie bei Problemen Unterstützung erhalten. *(ln)*

Links

[1] UltraVNC – Download, Dokumentation und Foren
www.uvnc.com

[2] Mirror-Treiber für optimierte Grafikübermittlung
http://prdownloads.sourceforge.net/ultravnc/UltraVnc-DriverSetup.zip?download

[3] Netzwerk-Variante des Mirror-Treibers
http://prdownloads.sourceforge.net/ultravnc/UltraVnc-DriverSetupSilent.zip?download

[4] Mirror-Treiber Demoforce Mirage (auch für TightVNC)
www.demoforge.com/dfmirage.htm

[5] VNC Manager – Werkzeug zum Aufspüren und Verwalten von VNC-Servern
http://sysworksoft.net/products/vncmng.html

[6] ChrisControl – Tool zur Remote-Installation von VNC-Servern
www.chall.plus.com/winpe/

[7] VNCon – Zentrales Management mehrerer VNC-Umgebungen
http://vncon.chronetal.co.uk

[8] iTALC – VNC-Steuerzentrale für den Einsatz in Schulungsräumen
http://italc.sourceforge.net

[9] BigBrother – Alternative zu iTALC
http://medien.bildung.hessen.de

[10] VNC Control – Management-Konsole für VNC-Umgebungen
http://vnccontrol.hit.bg

[11] Repeater für Firewall- und Proxy-Umgebungen
www.uvnc.com/addons/repeater.html

[12] NAT2NAT – Verbindungsherstellung über NAT-Router hinweg
www.uvnc.com/addons/nat2nat.html

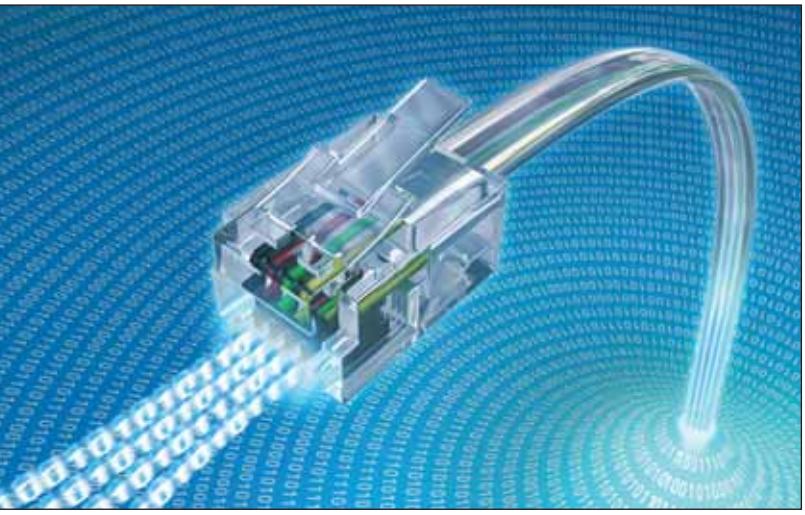
[13] Port Forwarding – Weiterleitung von UltraVNC-Ports auf NAT-Router
www.uvnc.com/addons/routerconf.html

[14] SingleClick-Verbindungsaufbau speziell für den Helpdesk-Einsatz
www.uvnc.com/addons/singleclick.html

10-GBit-Ethernet über Kupferverkabelungen

Twisted Pair bläst zum Angriff

von Mathias Hein



Das 10-GBit-Ethernet hat ein Problem: Auf Glasfaser hat sich die Technik in Backbones bereits etabliert. Mit der Adaption auf Kupfer – und vor allem auf vorhandene Twisted-Pair-Verkabelungen – hat die Technik aber ihre Schwierigkeiten. Dies liegt unter anderem daran, dass passende Netzwerkkomponenten bisher nur unzureichend verfügbar sind. Erstaunlich, denn 10-GBit-Ethernet über Twisted-Pair wird immer preiswerter und ist zudem recht sparsam beim Energieverbrauch. In diesem Artikel beschäftigen wir uns mit der Frage, ob die Kupfer-Variante eines Tages preiswert und leistungsfähig genug sein wird, um flächendeckend zum Einsatz zu kommen.

Die meisten realisierten Projekte auf Basis von 10-GBit-Ethernet nutzen die Glasfaser als Übertragungsmedium. Im Jahr 2009 wurden trotz der weltweiten Krise etwa 1,5 Millionen Switch-Ports installiert. Diese Zahlen stehen jedoch im krassen Gegensatz zu den Umsätzen im Bereich des 1-GBits- (über 100 Millionen Ports) und Fast-Ethernets (über 200 Millionen Ports). Der größte Teil der 10-GBit-Produkte wird zurzeit noch in den Server-Farmen und Rechenzentren verbaut. 10-GBit-Switches sind eine Voraussetzung für die effiziente Nutzung von Blade-Servern. Was die Vernetzung bis zum Arbeitsplatz betrifft, sind die Glasfaserkonzepte bisher aufgrund der hohen Kosten gescheitert. Nur Kupfervarianten versprechen die hier notwendige wirtschaftliche Flexibilität. 10-GBit-Ethernet über Kupferkabel könnte diese Anforderungen erfüllen.

Die technischen Grundlagen

Was noch vor fünf Jahren als unmöglich galt, ist inzwischen marktreif: Mit normalen Kupferkabeln ist heute der Aufbau eines Netzwerks mit Datenraten von 10 GBit/s möglich. Hierzu hat die IEEE den 802.3an-Standard (10GBASE-T) veröffentlicht. Dieser ermöglicht die Übertragung von 10-GBit-Ethernet über geschirmte oder ungeschirmte Twisted-Pair-Kupferkabel (STP/UTP). 10GBASE-T nutzt wie auch das GBit-Ethernet alle vier Aderpaare eines Twisted-Pair-Kabels. Die Datenrate pro Aderpaar reduziert sich dadurch auf 2,5 GBit/s. Die Maximalfrequenz des Kabels begrenzt jedoch die Übertragungsbandbreite, so dass die Kanalkapazität durch andere Kodierungstechniken erhöhet werden muss. Der 802.3an-Standard nutzt hier eine Pulse Amplitude-Modulation mit 16 Stufen (PAM16), welche die Störeinflüsse aus benachbarten Aderpaaren kompensiert und dadurch mehr Bit pro Übertragungsschritt kodieren kann als GBit-Ethernet. Die Übertragung auf einem Aderpaar erfolgt auch beim 10GBASE-T in beide Richtungen gleichzeitig. Die in den Ethernet-Chips integrierten Schaltungen subtrahieren immer das eigene, bekannte Sendesignal vom Empfangssignal, sodass der Empfangszweig nur das Signal der Gegenstelle erhält.

Doch bevor über ein 10GBASE-T-Interface Daten fließen können, müssen die Schnittstellen an den Kabelenden im Trainingsmodus den Übertragungskanal ausmessen. Dabei generiert jedes Interface sogenannte Trainings-Frames, anhand derer sich die Gegenseite synchronisiert und die Parameter (Variable Gain Amplifier, Echo- und Crosstalk-Kompensation) der Empfänger anpasst. Außerdem wird die aktuelle Aderpaar-Zuordnung und Polarität über eine Symbolsequenz geprüft. Durch internes Umlenken der Datenströme werden Abweichungen von der Standardbelegung kompensiert und die Crossover-Kabel entfallen. Die Kupfervariante des 10-GBit-Ethernet setzt voraus, dass die Twisted-Pair-Verkabelung eine Grenzfrequenz von 500 MHz unterstützt. Aus diesem Grund lässt sich 10GBASE-T wegen der zu niedrigen Grenzfrequenz nicht auf CAT5e-Kabeln realisieren. Während der Entwicklung des Standards zeigte sich, dass selbst CAT6

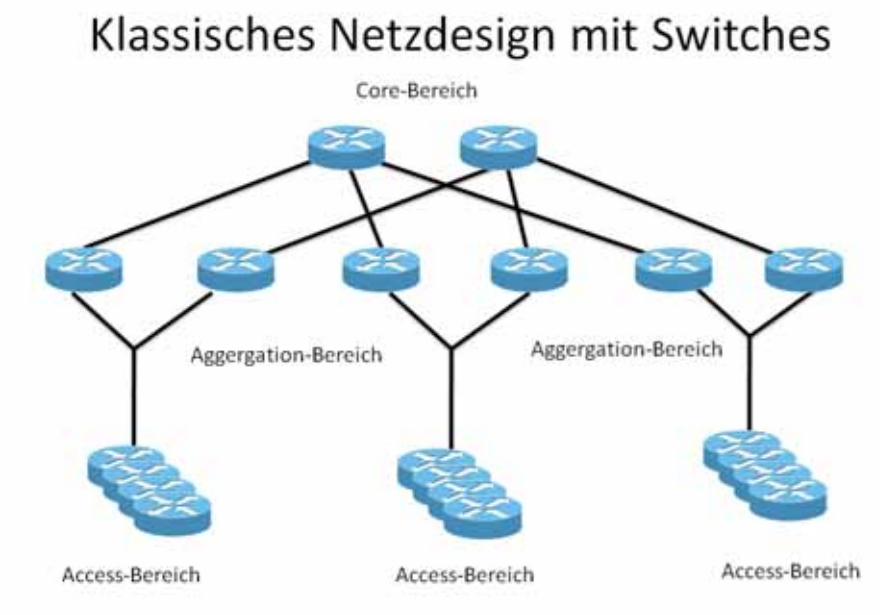


Bild 1: Das klassische Netzwerkdesign zeichnet sich durch eine dreistufige Einteilung aus

noch nicht ausreicht. Aus diesem Grund wurde die Kategorie 6 noch einmal in weitere Klassen unterteilt:
- CAT6 (Grenzfrequenz von 250 MHz)
- CAT6e (Grenzfrequenz von 500 MHz)
- CAT6a (mit bis zu 625 MHz).

Über CAT6a-Kabel schafft 10GBASE-T die angestrebten 100 Meter, über die CAT6e-Variante immerhin noch 55 Meter. CAT6a und CAT6e bestehen wie ihre Vorgänger aus acht Adern, die paarweise verdrillt sind. Jedes Paar trägt ein komplementäres Signal. Die Verdrillung reduziert unerwünschte Abstrahlungen und den Einfluss von außen induzierter Störungen. Als RJ45-Verbinder kommt entweder die ungeschirmte Version nach IEC 60603-7-4 oder die geschirmte Variante nach IEC 60603-7-5 zum Einsatz. Bei deren Anschluss ist entscheidend, dass die Verdrillung der Aderpaare und die Schirmung so weit wie möglich erhalten bleiben.

Neue Chipsets sparen Strom

Neue Chipsets halbieren die Kosten und den Stromverbrauch, eine Dual-Port 10GBASE-T-PHY benötigt inzwischen nur noch 6 Watt Energie pro Port. Da die 10GBASE-T-PHYs rückwärts-kompatibel zu langsameren Varianten des Ethernets sind, lassen sich die neuen 10G-Switches und Netzwerkkarten in bestehenden Netzen problemlos einsetzen. Die Entwicklung neuer Switches profitiert am meisten von den neuen PHYS. Inzwischen werden bereits 1U hohe Switches mit 48 10GBit-Ports angeboten. Auf einer 19 Zoll breiten Platine lassen sich maximal 24 RJ45-Buchsen nebeneinander unterbringen. Bei einer Anordnung auf der Frontplatte in zwei Reihen sind in einem Switch maximal 48 Ports möglich.

Theoretisch ließe sich noch eine dritte RJ45-Buchsenreihe auf der Frontplatte unterbringen. Dieser Variante steht jedoch die Physik entgegen, da der Abstand der Buchsen zum Chipset zu lang wird und somit Signalverzerrungen und Fehler auf den Datenleitungen hervorruft. Aufgrund des geringen Stromverbrauchs der neuen Chipgeneration benötigt ein 10GBit-Switch mit 24 Ports weniger als 500 Watt Leistungsaufnahme. An den reinen Zahlen gemessen, ist die Leistungsaufnahme noch immer recht hoch, doch bietet ein solcher Switch die gleiche Bandbreite, wie sie zehn 24-Port-GBit-Ethernet-Switches zur Verfügung stellen. Diese würden zusammen eine Leistungsaufnahme von 10 x 150 Watt, also 1,5 KW, beanspruchen. Kommende Generationen der 10GBit-Ethernet-PHYs werden zusätzlich noch den Energiesparmodus unterstützen und die Leistungsaufnahme drosseln, wenn nicht die volle Bandbreite erforderlich ist. Auch steht eine Nachfolgelösung für die Kupfervariante mit Übermittlung über maximal 15 Meter (10GBA-SECX4) zur Verfügung. Die Interface-Variante SFP + Direct Attach erfordert einen geringeren Energiebedarf, ist leichter zu installieren und die Switches lassen sich mit der gleichen Basistechnologie mit Kupfer- oder LWL-Transceivern bestücken.

Die Experten sind sich jedoch einig, dass das 10GBASE-T-Ethernet alle anderen Kupfervarianten langfristig auf dem Markt verdrängen wird. Hat die erste Generation 10-GBit-PHYs noch rund 10W pro Port an Energie benötigt, erfordert die zweite Generation (in den Produkten ab diesem Jahr integriert) nur noch 5 bis 6 Watt pro Anschluss. Langfristig streben die Hersteller sogar einen Leistungsaufnahme von 2 Watt an.

10-GBit-Ethernet verändert mittelfristig das Netzdesign

Durch die Verfügbarkeit von 10-Gigabit-Ethernet, die Virtualisierung der Server und die Integration immer intelli-

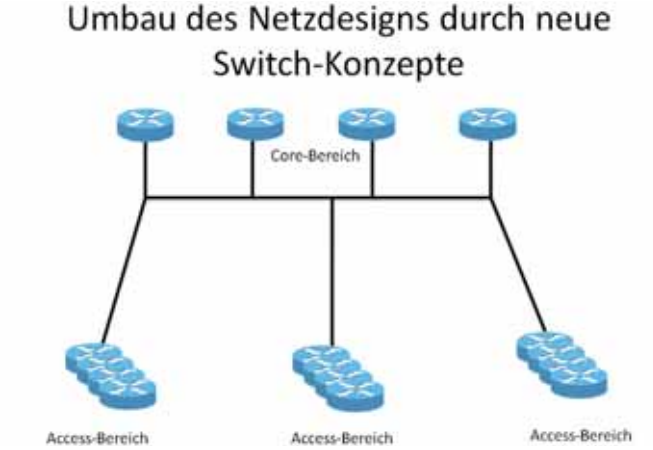


Bild 2: Das neue Netzdesign kommt mit zwei Ebenen aus

genterer Applikationen (beispielsweise Unified Communications) in die Netze ist eine Änderung des Netzwerk-Designs absehbar: Die bisher installierten dreischichtigen Switching-Architekturen werden sich auf ein zweischichtiges Netzdesign reduzieren.

Eine Drei-Schichten-Architektur besteht aus den Zugangs-, den Aggregation- und den Core-Switches. Fast alle Unternehmen haben in ihren Netzen in den letzten Jahren dieses Netzdesign umgesetzt. Dabei wurden die Desktop-PCs, die Drucker, WLAN Access Points und andere LAN-Geräte an den Zugangs-Switch angeschlossen. Die Verbindungen zu den auch Etagen-Switches genannten Geräten wurden in Aggregation-Switches gesammelt. Diese wiederum konzentrierten sich im Core-Switch.

Besonders bei der Realisierung von Cloud Computing-Umgebungen, modernen Datenzentren sowie der Virtualisierung von Servern und Storage ist die durch eine dreistufige Switching-Architektur hervorgerufene Verzögerung nicht mehr ausreichend. Außerdem ist die zur Verfügung stehende Bandbreite in den Unternehmen durch unzureichende Switch-Konzepte oftmals überbucht. Überbuchungen von 3:1 bis 10:1 gehören nicht selten zum Alltag. Die verschiedenen Anwendungen kämpfen dadurch permanent um eine begrenzte Bandbreite. Dies wirkt sich in einer Erhöhung der Reaktionszeit und einer Verschlechterung der Services aus. Neue Anwendungen, wie beispielsweise Voice over IP, Unified Communication oder Video Conferencing erfordern eine berechenbare Leistung, minimale Verzögerung und einen definierten Quality of Service (QoS) für den Broadcast-, Multicast- und Unicast-Verkehr.

Durch verbesserte Datendurchsätze und reduzierte Produktkosten der 10-GBit-Ethernet-Switches entfällt die Notwendigkeit für die Installation eines Aggregation-Switches. Stattdessen werden die Etagen-Switches über Glasfaser direkt mit den Core-Switches im Rechenzentrum verbunden. An diesen finden die Server direkt Anschluss an das Kern-Netz über 10-GBit-Ethernet auf Kupferbasis. Dies bietet den Vorteil, dass eine quasi verlustfreie Systemarchitektur entsteht, die eine sehr geringe Verzögerung aufweist.

Virtualisierte Rechenzentren mit einer optimierten Switching-Architektur garantieren eine Ende-zu-Ende-Verzögerung von weniger als 10 Mikrosekunden. Um diese kurzen Übermittlungszeiten erreichen zu können, müssen so viele Schaltstufen im Netzwerk wie möglich eliminiert werden. Bei der Virtualisierung mittels Blade- oder Rack-Server übernehmen die Server selbst die Rolle des Access Switches im Netz. Der Hypervisor oder Virtual Machine Monitor verwaltet die Ressourcenverteilung für einzelne virtuelle Maschinen und sorgt für das Switching der Server-Daten. Wird die Server-Virtualisierung durch eine I/O-Virtualisierung ergänzt, lassen sich die im Netzwerk zur Verfügung stehenden Bandbreiten den jeweiligen VMs individuell zuweisen.

In einem zweistufigen Switch-System kann ferner auf den Spanning-Tree-Algorithmus verzichtet werden. Bisher bestimmt dieser Mechanismus die aktiven Pfade zwischen dem Daten-Center und den Endgeräten. Die Anforderungen an ein modernes Netzdesign, das eine schnelle und verlustfreie Anbindung der virtualisierten Rechenzentren bei geringsten Verzögerungen garantieren soll, ist mit der Nutzung des Spanning-Trees nicht mehr vereinbar. Stattdessen werden parallele Verbindungen zwischen den Switches im Netzwerk aktiviert und die Daten über mehrere parallele Wege übermittelt. Diese Switches überwachen kontinuierlich die Übermittlungswege und beseitigen automatisch potenzielle Engpässe im Netz.

iSCSI über 10-GBit-Ethernet

Durch die iSCSI-Unterstützung in VMware etabliert sich jetzt auch das 10-GBit-Ethernet im Storage-Markt und bedrängt hier zusehends die klassischen Fibre Channel-Technologien. Die Analysten prognostizieren für das kommende Jahr für 10-GBit-Ethernet den Durchbruch im Markt der Enterprise-Storage-Arrays und Server. Hierfür sind hauptsächlich die geringen Kosten der iSCSI-Storage-Lösungen die Ursache. In der Praxis kostet eine Ethernet-Infrastruktur nur den Bruchteil einer High-End-Fibre-Channel-Lösung. Außerdem erfordert die Ethernet-Technologie im Gegensatz zum Fibre-Channel kein spezielles Fachwissen.

Fazit

Der Treiber für den extrem hohen Bedarf an Bandbreite ist die Virtualisierung von Servern und die Konsolidierung von Rechenzentren. Trotzdem hat sich die Einführung von 10GBASE-T eher schleppend entwickelt. Der Grund hierfür liegt in den fehlenden Komponenten für die Infrastruktur. Erst mit der Verfügbarkeit neuer Ethernet-Switches und entsprechenden Server-Adaptern zieht die 10-GBit-Ethernet-Technologie in die Rechenzentren ein. *(ln)*

Netzwerk-Fernanalyse via Remote Probes

Netzwerke „grenzenlos“ monitoren

Unternehmen mit mehreren Standorten sind auf eine performante IT-Infrastruktur angewiesen. Reibungslos ablaufende IT-Prozesse und eine zuverlässige Kommunikation zwischen einzelnen Firmenstandorten sowie mit Kunden und Partnern sind Schlüsselfaktoren für den sicheren Geschäftsbetrieb. Um die örtlich verteilten Netzwerke und deren Verfügbarkeit sowie Bandbreitenauslastung jederzeit im Blick zu haben, ist ein zuverlässiges Monitoring ratsam. Es liefert wichtige Informationen über den Zustand der Netzwerke und warnt beim Erreichen kritischer Werte.

IT-Administratoren, die sich um den Betrieb mehrerer verteilter Netzwerke kümmern müssen, tragen eine große Verantwortung. Systemausfälle und -einbrüche wirken sich zumeist sofort negativ auf die Arbeitsprozesse in Unternehmen aus. Beispielsweise führt dies zu Umsatzeinbrüchen oder Fertigungsengpässen und beeinträchtigt so die Wettbewerbsfähigkeit nachhaltig. Ein permanentes Netzwerk-Monitoring wirkt dem entgegen, indem es alle erforderlichen Informationen der verteilten Netze zusammenträgt, visualisiert und im Ernstfall den Verantwortlichen alarmiert. Damit kann die Verfügbarkeit von Anwendungen und Geräten sowie ausreichende Bandbreite sichergestellt werden. Zudem liefern Auslastungstrends frühzeitig Hinweise auf drohende Engpässe und Verbindungsfehler. Dies ermöglicht es den Administratoren, den Netzwerkverkehr alternativ zu routen oder Neuanschaffungen frühzeitig zu planen bzw. geeignete Optimierungen vorzunehmen.

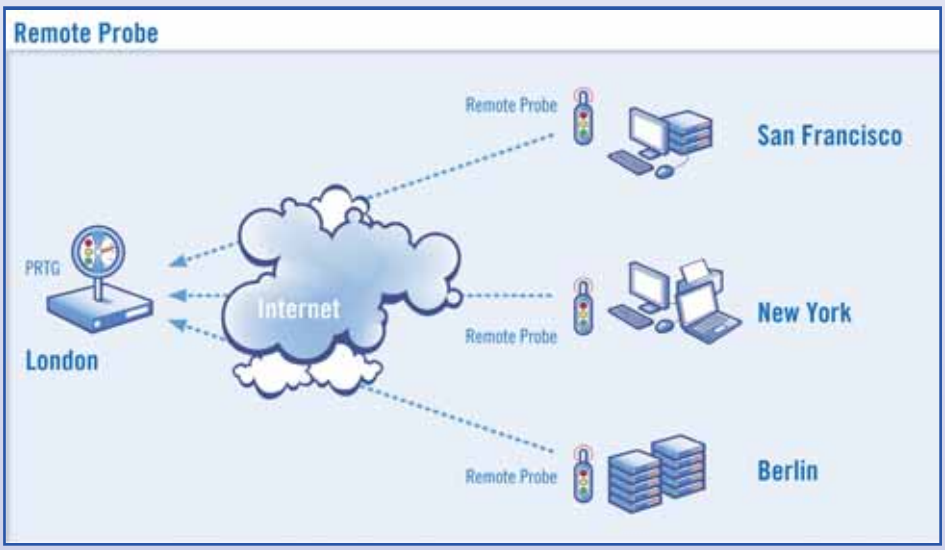
Für die zentrale Überwachung mehrerer räumlich verteilter Netzwerke verfügt die Lösung PRTG Network Monitor mit den Remote Probes über ein spezielles Feature. Nachdem sie in allen Niederlassungen installiert sind, sammeln diese Sonden eigenständig alle relevanten Daten und senden sie zur Auswertung an die zentrale Instanz. Die Datenübertragung von der Probe zum Core Server erfolgt sicher unter SSL-Verschlüsselung. Diese Funktion ist bereits ab der Basislizenz in PRTG enthalten und verursacht so keine Zusatzkosten.

Fernüberwachung als Dienstleistungsservice

Die Remote Probes ergänzen auch das Angebotsportfolio von IT-Dienstleistern um ein strategisch wichtiges Tool. Kunden können die Monitoring-Lösung als Service buchen. Der Dienstleister kann die verteilten Netzwerke seiner Kunden zentral überwachen, Probleme schnell erkennen und gegebenenfalls sofort beseitigen – die Grundlage für einen guten Service und Kundenbindung. Oder er setzt die Lösung zur Qualitätssicherung der eigenen Leistungen ein. Denn PRTG kontrolliert die Verfügbarkeit von Hardware-Ressourcen, Bandbreiten, Webseiten, Speicher, Plattenplatz etc. Bei Ausfällen oder Erreichen definierter Grenzwerte erfolgt eine automatische Benachrichtigung an den Administrator. Dieser kann umgehend entsprechende Maßnahmen einleiten. Darüber hinaus ermöglicht das Sammeln, Archivieren und Auswerten der Monitoringdaten langfristige Analysen des Netzwerks. Auf dieser Basis können gezielt Optimierungen durchgeführt werden.

Weitere Informationen zum Einsatz des Remote Probes-Features stehen unter http://www.de.paessler.com/distributed_monitoring zur Verfügung.

Lizenzen für die Netzwerk-Monitoring Software PRTG beginnen bei 250 Euro (zzgl. MwSt.) inklusive vier Probes: https://de.paessler.com/order/prtg.



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

Ansprechpartner:
Christian Twardawa

Automatische Installation von Windows 7 (2)

Virtuell booten

von Thomas Joos

Neben den klassischen Verteilmethoden für Windows 7, die wir im ersten Teil dieser Workshopserie untersuchten, stehen IT-Verantwortlichen mit dem neuen Client auch weitergehende Möglichkeiten auf Basis virtueller Festplatten zur Verfügung. Zunächst zeigen wir Ihnen, wie Sie Windows 7 über ein Computer-Abbild und ImageX-Verfahren installieren. Abschließend geht dieser Workshop auf Parallelinstallationen von Windows 7 und älteren Windows-Versionen ein.

Zum Abschluss des ersten Teils dieser Workshopserie passten wir die Antwortdatei zur automatischen Partitionierung an. Auf dieser Basis arbeiten wir nun weiter.

Computerabbild installieren

Wollen Sie Windows 7 mit der erstellten Antwortdatei installieren, benötigen Sie eine Windows 7-DVD oder einen USB-Stick mit den Installationsdateien von Windows 7. Sie müssen sicherstellen, dass der Computer von diesem Laufwerk bootet. Die weiteren Schritte zeigen wir Ihnen nachfolgend:

1. Starten Sie den Computer, legen Sie die Windows 7-DVD in das Laufwerk und schließen Sie den USB-Stick an, der die Antwortdatei enthält. Verbinden Sie den USB-Stick mit einem der primären USB-Anschlüsse des Computers.
2. Schalten Sie nun den Computer ein, startet das Windows 7-Setup automatisch. Standardmäßig durchsucht das Setup das Stammverzeichnis aller Wechselmedien nach einer Antwortdatei mit dem Namen *AutoUnattend.xml*.
3. Um den Computer klonen zu können, sollten Sie nach der Installation noch den Befehl *sysprep* mit der Option "/generalize" verwenden sowie die Option "/oobe", um die Windows-Willkommensseite beim nächsten Neustart zu aktivieren. Wählen Sie aus der Liste "Systembereinigungsaktion" die Option "Out-of-Box-Experience (OOBE)" für "System aktivieren" aus. Aktivieren Sie noch "Verallgemeinern" und wählen Sie die Option "Herunterfahren" aus. Durch die Ausführung des Befehls werden Standardgerätetreiber aus dem Windows-Abbild entfernt.

Wenn Sie während der Installation Standardgerätetreiber hinzufügen und das Windows-Abbild aufzeichnen möchten, legen Sie für die Einstellung "PersistAllDeviceInstalls" der Komponente "Microsoft-Windows-PnpSysprep" in der Antwortdatei die Option "True" fest. Bei Verwendung dieser Einstellung entfernt Sysprep die erkannten Gerätetreiber nicht. Sie können Sysprep auch über eine Eingabeaufforderung ausführen, indem Sie den Befehl *c:\windows\system32\sysprep\sysprep.exe /oobe /generalize /shutdown* eingeben.

Vorbereiten und Erstellen einer Windows-PE-CD

Wollen Sie eine Windows PE-CD erstellen, um Computer im Netzwerk mit der PE-Umgebung zu booten, verwenden Sie ebenfalls das WAIK für Windows 7 und Windows Server 2008 R2. Gehen Sie zur Erstellung einer solchen Datei nach den folgenden Schritten vor: Nachdem Sie das WAIK installiert haben. klicken Sie auf "Alle Programme / Windows AIK / Eingabeaufforderung für Bereitstellungstools". Führen Sie nun den Befehl *copype.cmd {Systemvariante} {Verzeichnis}* aus. Als Systemvariante können Sie entweder "x86", "amd64" oder "ia64" verwenden, abhängig davon, welches System Sie einsetzen. Als Verzeichnis geben Sie ein beliebiges Verzeichnis auf der Festplatte des Admin-

PCs an, zum Beispiel "C:\winpe". Das Verzeichnis müssen Sie vorher nicht erstellen, der Assistent erledigt dies automatisch und legt die Dateien im Anschluss in diesem Verzeichnis ab.

Anschließend sollten Sie zusätzliche Tools in dieses Verzeichnis kopieren, das Sie beim Starten von Windows PE benötigen, zum Beispiel *imagex.exe*, das Sie für das Erstellen von Images verwenden. Sie finden das Werkzeug unter "C:\Programme\Windows AIK\Tools\x86". Kopieren Sie das Tool in das Unterverzeichnis "ISO" im gerade erstellten PE-Verzeichnis auf Ihrer Festplatte. Im nächsten Schritt erstellen Sie die ISO-Datei, die schließlich die Windows PE-Installation enthält. Um die ISO-Datei zu erstellen, geben Sie den Befehl

```
Oscdimg -n -bc:\winpe\etfsboot.com
  c:\winpe\ISO c:\winpe\winpe.iso
```

ein. Achten Sie darauf, das Verzeichnis ISO auch mit Großbuchstaben zu schreiben. Brennen Sie im Anschluss diese ISO-Datei auf CD und booten Sie den Master-PC mit dieser CD.

Erweiterte Optionen von ImageX

Weitere Optionen von ImageX:

- **/append** hängt ein Image an eine vorhandene WIM-Datei an.
- **/apply** stellt ein Image in einem bestimmten Laufwerk wieder her.
- **/capture** erstellt ein Image in einer neuen WIM-Datei.
- **/commit** übernimmt die Änderungen für eine WIM-Datei.
- **/compress** legt die Kompression auf "keine", "schnell" oder "maximal" fest. Die genaue Syntax erfahren Sie durch *imagex /?*.
- **/config** verwendet die in der angegebenen Datei festgelegten erweiterten Optionen.
- **/delete** löscht ein Image aus einer WIM-Datei mit mehreren Images.
- **/dir** zeigt eine Liste der Dateien und Ordner in einem Image an.
- **/export** überträgt ein Image von einer WIM-Datei zu einer anderen.
- **/info** gibt die XML-Beschreibungen für eine bestimmte WIM-Datei zurück.
- **/ref** legt die WIM-Referenzen für das Wiederherstellen fest.
- **/scroll** gibt alle Ausgaben am Stück aus.
- **/split** teilt eine vorhandene WIM-Datei in mehrere schreibgeschützte Teile.
- **/verify** überprüft doppelte und extrahierte Dateien.
- **/mount** stellt ein Image schreibgeschützt in einem bestimmten Ordner bereit.
- **/mountrw** stellt ein Image mit Lese- und Schreibzugriff in einem bestimmten Ordner bereit. Durch diesen Befehl können Dateien ausgetauscht werden, und Sie können auf den Inhalt des Image zugreifen.
- **/unmount** hebt die Bereitstellung eines Image in einem bestimmten Ordner auf.

Installation von Windows 7 über ein ImageX-Image

Wollen Sie ein Image nur auf einem einzelnen Computer ohne die WDS installieren, booten Sie den Zielcomputer mit einem Windows PE-Datenträger und stellen Sie sicher, dass der Datenträger korrekt konfiguriert ist. Sollte die Festplatte des Zielcomputers noch vollkommen leer sein, so können Sie mit dem Befehl *diskpart* auf dem Zielcomputer eine ausreichend große, aktive Partition erstellen. Geben Sie dazu die folgenden Befehle ein:

```
diskpart
select disk 0
clean
create partition primary size=20000
select partition 1
active
format
exit
```

Im nächsten Schritt wird die Image-Datei von der Netzwerkfreigabe auf die lokale Festplatte des PCs kopiert. Im Anschluss installieren Sie das Image mit dem folgenden Befehl auf dem Computer:

```
Imagex.exe /apply
  C:\mein-image.wim c:
```

Virtuelle Festplatten mit Windows 7

Windows 7 bietet in allen Editionen die Möglichkeit, über die Festplattenverwaltung virtuelle Festplatten zu erstellen und diese in das Betriebssystem einzubinden. Über eine solche VHD-Datei lässt sich Windows 7 sogar booten, allerdings nur mit der Ultimate Edition. Sie können virtuelle Festplatten, die als physische Datei auf normalen Datenträgern liegen, wie eine normale Festplatte verwenden, alle Daten dieser Festplatte liegen in einer einzigen Datei. Der Computer bootet ganz normal von dieser virtuellen Festplatte, daher kann auch nur immer eine Instanz von Windows gestartet sein. Kopieren Sie einfach diese Datei, haben Sie damit das komplette System gesichert. Die Leistung ist dabei unmerklich eingeschränkt. Im Internet kursieren dazu Werte zwischen 1 und 5 Prozent Leistungsminderung, was kaum auffällt und gegen die erlangten Vorteile eher vernachlässigt werden kann. Bitlocker und Ruhezustand funktionieren auf solchen virtuellen Festplatten jedoch nicht.

Das VHD-Format verwenden zum Beispiel auch Virtual PC oder auch Hyper-V in Windows Server 2008 und Windows Server 2008 R2. Neben der Möglichkeit zum Booten lassen sich solche Festplatten auch als normaler Datenträger einbinden und auch hier haben Sie den Vorteil, durch das Sichern einzelner Dateien die komplette Festplatte sichern zu können.

Erstellen und Verwalten von virtuellen Festplatten

Die Steuerung und Erstellung von virtuellen Festplatten finden Sie in der Datenträgerverwaltung über das Menü "Aktion". Die Datenträgerverwaltung starten

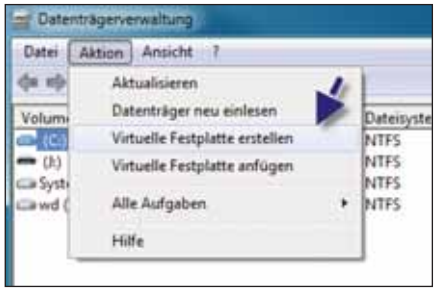


Bild 1: Das Anlegen oder Verbinden von virtuellen Festplatten in Windows 7 nehmen Sie über den Festplattenmanager vor

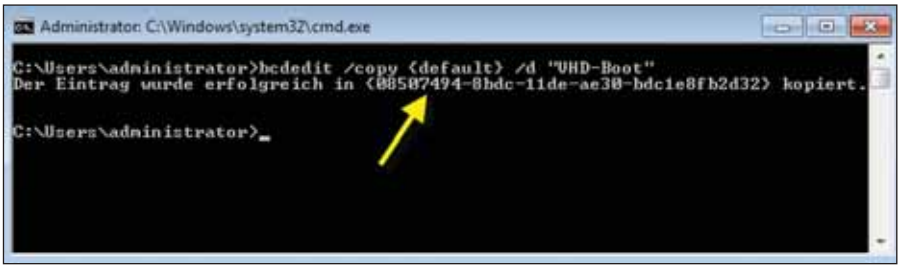


Bild 2: Erstellen eines Eintrags für VHD-Boot im Bootmanager von Windows 7

Sie entweder über die Computerverwaltung oder indem Sie den Befehl *diskmgmt.msc* in das Suchfeld des Startmenüs eingeben.

Klicken Sie auf den Menüpunkt "Virtuelle Festplatte erstellen", um den Assistenten zu starten. Im Assistenten legen Sie fest, wo Sie die *.vhd-Datei der Festplatte speichern und wie groß die Festplatte sein soll. An dieser Stelle definieren Sie auch, ob die Festplatte anwachsen darf oder ob Sie eine feste Größe verwenden. Wählen Sie den Befehl "Virtuelle Festplatte anfügen" aus, können Sie bereits bestehende Datenträger an den Computer anbinden. Virtuelle Festplatten müssen mindestens eine Größe von 3 MByte haben, außerdem sind diese Festplatten immer als Basis-Platten konfiguriert.

Nachdem Sie virtuelle Festplatten angelegt, in der Datenträgerverwaltung initialisiert und formatiert haben, stehen diese im Explorer, wie alle anderen Laufwerke auch, zur Verfügung. Das Verbinden und Trennen von bereits existierenden virtuellen Festplatten lässt sich alternativ auch in der Befehlszeile mit *Diskpart.exe* durchführen:

```
diskpart
select vdisk file=c:\windows7.vhd
attach vdisk
select volume {Volumenummer, mit
  list volume abfragen}
assign letter=v
exit
```

Wie Sie virtuelle Festplatten mit *diskpart* erstellen, zeigen wir Ihnen später. Nachdem Sie die virtuelle Festplatte erstellt haben, zeigt Windows die Installation des Treibers an, um virtuelle Festplatten ansprechen zu können.

Abhängig von der Größe dauert die Erstellung einige Minuten. Anschließend steht der virtuelle Datenträger in Windows wie jeder andere Datenträger zur Verfügung. Bei der Verwendung gibt es keine Unterschiede zu physischen Datenträgern, aber alle Daten der Festplatte liegen in der beschriebenen *.vhd-Datei. Nachdem Sie den Datenträger angelegt haben, müssen Sie diesen, wie jeden anderen Datenträger auch, initialisieren und formatieren. Klicken Sie dazu nach dem Anlegen der Festplatte mit der rechten Maustaste auf den freien Speicherplatz. Über das Kontextmenü des virtuellen Datenträgers können Sie diesen zeitweise offline schalten, also für die Verwendung deaktivieren, oder Sie können den Datenträger wieder vom System entfernen.

Virtuelle Festplatten booten

Sie können *.vhd-Dateien sehr leicht bootfähig machen, allerdings nur wenn Sie die Ultimate Edition von Windows einsetzen. Dazu haben Sie mehrere Möglichkeiten: Sie können eine solche Festplatte erstellen und diese im Bootmanager eintragen oder bereits während der Installation von Windows 7 eine solche virtuelle Festplatte erstellen, in diese Festplatten installieren und von dieser gleich booten. Stellen Sie sicher, dass sich die *.vhd-Datei direkt im Stammverzeichnis von C: befindet und Sie die Festplatte mit dem System verbunden haben.

Zur Anbindung an das Bootmenü verwenden Sie das Verwaltungstool *bcdedit.exe*, das Sie über eine Befehlszeile steuern. Allerdings ist der Befehl nicht gerade einfach. Bevor Sie jedoch Änderungen am Bootspeicher vornehmen, sollten Sie diesen über die Option "/export" sichern, zum Beispiel mit dem Befehl *bcdedit /export c:\bcdbackup*. Anschließend können Sie den Bootspeicher bearbeiten: Der erste Befehl kopiert dazu den Eintrag einer bestehenden Installation und fügt dem Bootmanager einen neuen Eintrag hinzu:

```
bcdedit /copy {current} /d
  "Booten von VHD"
```

Diesen neuen Eintrag bearbeiten Sie als Nächstes mit den Befehlen im nächsten Abschnitt. Als Bezeichner-ID verwenden Sie die Daten, die der gerade eben gezeigte Befehl ausgibt. Klicken Sie oben links auf das kleine Symbol, können Sie mit "Bearbeiten/Markieren" die GUID des Eintrags in die Zwischenablage kopieren, inklusive der

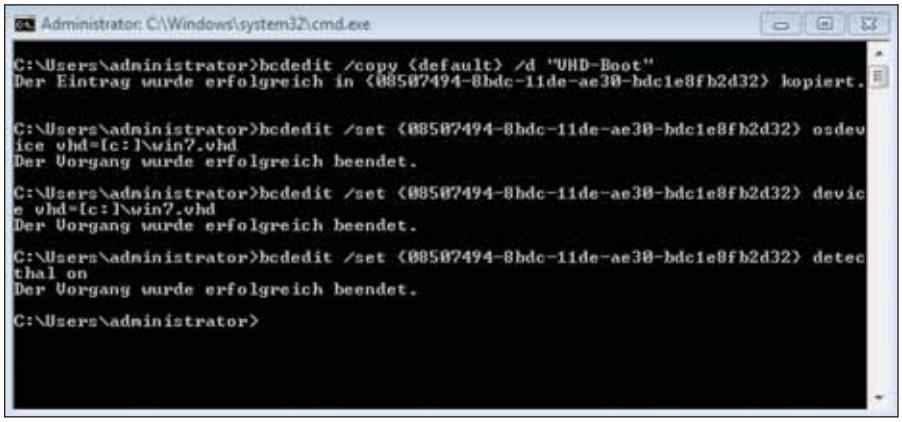


Bild 3: Bearbeiten des Windows 7-Bootmanagers für Dualboot mit VHD-Datei

CeBIT 2010 Special

Vortragsraum in Halle 4, Stand A26

Lernen Sie vom 2. bis 6. März Microsoft®-Innovationen für Softwareentwickler und IT-Professionals kennen wie Silverlight™ 4, Windows Server® 2008 R2 oder SQL Server® 2008 R2. Nutzen Sie die Gelegenheit, sich mit Microsoft-Experten und -Partnern auszutauschen. Wir erwarten Sie in unserem MSDN®-und-TechNet-Vortragsraum!

Besuchen Sie uns auch online: www.msdn-online.de/cebit

msdn® Microsoft® | TechNet

CeBIT
HANNOVER
2.– 6. 3. 2010
cebit.com

GUTSCHEIN

Gegen Vorlage dieses Gutscheins erhalten Sie am MSDN-TechNet-Stand die aktuelle Webcast DVD kostenlos.

geschweiften Klammern. Markieren Sie dazu den Eintrag und klicken Sie auf "Enter/Return":

```
bcdedit /set {Bezeichner-ID}
  osdevice vhd=[C:]\{Datei}.vhd
bcdedit /set {Bezeichner-ID} device
  vhd=[C:]\{Datei}.vhd
```

Den nächsten Befehl benötigen manche x86-Systeme, damit die virtuelle Festplatte ordnungsgemäß funktioniert:

```
bcdedit /set {Bezeichner-ID}
  detecthal on
```

Starten Sie den Computer, sehen Sie den neuen Eintrag im Bootmenü. Dieser Eintrag bootet dann von der virtuellen Festplatte. Erhalten Sie einen Fehler, müssen Sie den Computer mit dem Befehl *sysprep.exe* wieder auf den Ursprungszustand zurücksetzen. Sysprep finden Sie im Verzeichnis "\Windows\System32\Sysprep". Wählen Sie die Option "Out-of-Box-Experience" und dann "Verallgemeinern". Booteinträge löschen Sie, indem Sie *msconfig* in das Suchfeld des Startmenüs eingeben. Auf der Registerkarte "Start" sehen Sie alle Einträge des Bootmanagers und können Einträge auch wieder löschen.

Windows 7 parallel zu XP auf einer VHD installieren

Mit den hier beschriebenen Möglichkeiten können Sie auch leicht Windows 7 parallel zu einem anderen Betriebssystem installieren, indem Sie bereits im Windows-Setup die Virtualisierung konfigurieren. Der hier beschriebene Weg funktioniert auch, wenn Sie auf einem Computer gar kein Betriebssystem installiert haben und Windows 7 ausschließlich virtuell installieren wollen. Auch wenn Sie nur eine einzige Festplatte und eine Partition im System haben, funktioniert die hier beschriebene Vorgehensweise.

Stellen Sie dazu sicher, dass auf dem Computer, auf dem Sie Windows 7 parallel auf einer virtuellen Festplatte installieren wollen, noch mindestens 12 bis 15 GByte Festplattenplatz frei ist. Legen Sie zunächst die Windows 7-DVD in das Laufwerk und booten Sie den Computer. Bestätigen Sie dann die Installationssprache und das Tastaturlayout und klicken Sie auf "Weiter". Auf der nächsten Seite des Installationsassistenten starten Sie mit der Tastenkombination "Shift + F10" eine Befehlszeile. Geben Sie den Befehl *diskpart* ein und bestätigen Sie (das Aufrufen des Programmes kann etwas dauern). Über den Befehl *list disk* lassen Sie sich nun die eingebauten Festplatten und mit *list volume* die erstellten Partitionen anzeigen. Als Nächstes erstellen Sie über

```
create vdisk file=c:\windows7.vhd
  type=expandable maximum=15000
```

eine neue virtuelle Festplatte. Die Festplatte kann 15 GByte groß sein, ist am Anfang aber noch leer, kann aber durch die Option "expandable" noch wachsen. Bevor Sie die Datei erstellen, achten Sie aber darauf, dass Sie diese auch auf der Partition erstellen, die über genügend Festplattenplatz verfügt. Die C-Partition Ihres Computers muss bei der Boot-DVD von Windows 7 nicht unbedingt den Buchstaben C: erhalten. Sie testen dies, indem Sie mit C:, D: oder E: die verschiedenen Partitionen wählen und mit *dir* anzeigen lassen. Erstellen Sie die virtuelle Festplatte am besten direkt auf der Festplatte, auf der Ihr bisheriges Betriebssystem installiert ist.

Im nächsten Schritt wählen Sie die neue virtuelle Festplatte mit *select vdsik file=c:\Windows7.vhd* aus. Danach aktivieren Sie diese mit *attach vdisk* für die Installation. Geben Sie anschließend zweimal das Kommando *exit* ein, um Diskpart und dann die Befehlszeile zu verlassen. Klicken Sie dann auf "Jetzt installieren", um das Setup zu starten. Nachdem Sie die Lizenzbedingungen bestätigt haben, wählen Sie als Installationsvariante "Benutzerdefiniert" aus. Als Festplatte wählen Sie den neuen Festplattenplatz aus, der als "Nicht zugewiesen" hinterlegt ist.

Führen Sie jetzt die Installation normal fort. Die Fehlermeldung spielt keine Rolle. Wichtig ist nur, dass Sie die virtuelle Festplatte auf einem Datenträger erstellt haben, der über genügend Plattenplatz verfügt und auf den der Installationsassistent auch zugreifen kann. Jetzt passt der Installationsassistent den Bootmanager

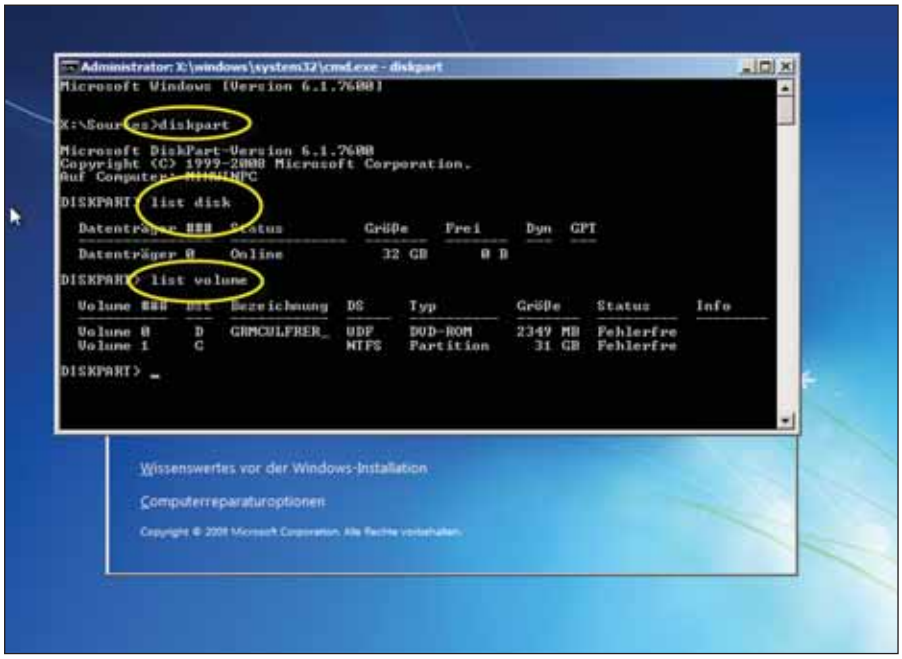


Bild 4: Aufrufen der Informationen der eingebauten Festplatten mit Diskpart

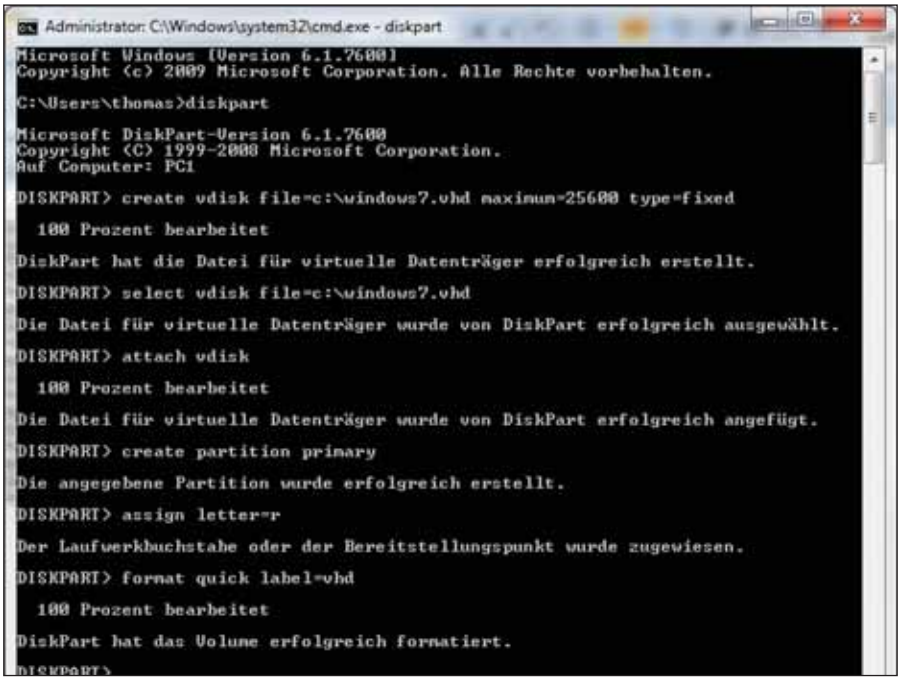


Bild 5: Erstellen und Bearbeiten einer bootfähigen virtuellen Festplatte für Windows 7

automatisch an. Bei der virtuellen Festplatte mit Windows 7 handelt es sich um das Laufwerk C, während Windows Vista jetzt auf D: liegt. Booten Sie mit Windows Vista, hat wiederum Vista den Buchstaben C: und die virtuelle Festplatte den Buchstaben D:

Windows 7 für Unternehmens-Deployment virtuell booten

Windows 7 bietet auch die Möglichkeit, ausschließlich als *.vhd-Datei zu booten, ohne dass auf dem Computer ein Betriebssystem installiert ist. Diese Möglichkeit ist zum Beispiel für automatische Verteilungszwecke sinnvoll. Dazu erstellen Sie eine voll funktionsfähige Installation von Windows 7 auf einer virtuellen Festplatte und konfigurieren den Computer, mit dieser Festplatte zu booten. Auf den Zielsystemen muss dazu nichts installiert sein, sondern das Booten findet virtuell statt. Die Geschwindigkeit des Betriebssystems ist bei aktueller Hardware kaum von einer physischen Installation zu unterscheiden.

Was Sie dazu brauchen ist das kostenlose Windows Automated Installation Kit (WAIK) für Windows Server 2008 R2 und Windows 7 [1]. Das Kit enthält Tools um Windows 7 in eine Abbilddatei zu sichern und die Möglichkeit einen speziellen Boot-Datenträger zu erstellen, der auf Windows 7 basiert. Installieren Sie zunächst auf einem Computer das WAIK, um die in diesem Abschnitt besprochenen Punkte durchführen zu können. Der erste Schritt besteht darin, dass Sie eine virtuelle Quell-Festplatte erstellen, in die Sie dann Windows 7 integrieren. Der schnellste Weg dazu führt über das mehrfach erwähnte Befehlszeilen-Tool Diskpart. Starten Sie eine Befehlszeile, geben Sie *diskpart* ein und gehen Sie dann wie folgt vor, um eine Festplatte mit einer festen Größe von 25 GByte zu erstellen, der Sie den Laufwerksbuchstaben "R" zuweisen, der Buchstabe ist beliebig.

```
diskpart
create vdisk file=c:\windows7.vhd
  maximum=25600 type=fixed0
select vdisk file=c:\windows7.vhd
attach vdisk
create partition primary
assign letter=r
format quick label=vhd
exit
```

Im nächsten Schritt übertragen Sie ein bestehendes Abbild einer Windows 7-Installation als *.wim-Datei. Wechseln Sie mit dem Befehl *cd /d "c:\program files\{Pfad zum WAIK}\Tools\{Architecture}\"* in das Verzeichnis, in dem das Tool ImageX liegt. Geben Sie *imagex /apply {Pfad zur *.wim-Datei} 1 r:* ein. Daraufhin schreibt der Assistent den Inhalt der *.wim-Datei auf die virtuelle Festplatte mit der Beschreibung. Bestehende Windows 7-Installationen lassen sich mit ImageX in eine WIM-Datei speichern.

ImageX basiert auf der Windows Imaging-Technologie (WIM) und ist das wichtigste Tool beim Rollout von Windows 7 und Windows Server 2008. Nachdem auf dem Mastercomputer Windows 7 installiert ist, erstellen Sie ein Image der Installation über

```
Imagex.exe /compress fast /capture
  C: C:\mein-image.wim "{Beschrei-
  bung}" /verify
```

Statt "mein-image.wim" können Sie eine beliebige Bezeichnung für das Image verwenden. Nachdem Sie die Daten komplett übertragen haben, trennen Sie mit Diskpart die virtuelle Festplatte vom Computer:

```
diskpart
select vdisk file=c:\windows7.vhd
detach vdisk
exit
```

Sie können jetzt die virtuelle Festplatte entweder über das Netzwerk zur Verfügung stellen oder Sie kopieren diese auf eine externe Festplatte, um einen Zielcomputer damit zu starten. Übrigens ist auch das Standardinstallations-Medium von Windows 7 nichts als eine Image-Datei im WIM-Format. Sie können daher dieses Image leicht auf einen USB-Stick mit entsprechender Größe kopieren und auf diesem Wege Windows 7 installieren, zum Beispiel auf Netbooks ohne DVD-Laufwerk.

Idealerweise sollten Sie auf dem Zielcomputer, auf dem Sie die virtuelle Festplatte als System einrichten wollen, alle Daten entfernen. Sie starten dazu den Computer mit einer Windows 7-DVD und öffnen eine Befehlszeile, in dem Sie auf dem Fenster mit den Computerreparaturoptionen die Tastenkombination "Shift + F10" drücken. Wir haben diese Schritte im vorangegangenen Abschnitt bereits behandelt. In der Eingabeaufforderung starten Sie zunächst wieder Diskpart und löschen mit den folgenden Befehlen eventuell bereits vorhandene Daten:

```
diskpart
sel disk 0
clean
```

Im Anschluss erstellen Sie eine Systempartition, in der später der Bootmanager untergebracht wird. Hier reicht eine Größe von etwa 200 MByte aus. Sie erstellen die Partition am schnellsten ebenfalls mit Diskpart:

```
create partition primary size=200
format quick fs=ntfs
assign letter=s
active
```

Beenden Sie Diskpart noch nicht, Sie benötigen das Tool noch einmal, um eine weitere Partition zu erstellen. Die Systempartition wird so auch gleich aktiv geschaltet. Nur dann ist das Booten möglich. Als nächstes erstellen Sie eine primäre Partition C auf der Sie später die *.vhd-Datei kopieren. Auf der Festplatte ist nichts installiert, sondern die *.vhd-Datei als Systemplatte hinterlegt. Physisch liegt diese Datei auf der Festplatte C, sodass keine Geschwindigkeitsnachteile entstehen. Sie verwenden dazu im bereits geöffneten Diskpartfenster die Befehle:

```
create partition primary
format quick fs=ntfs
assign letter=c
exit
```

Im letzten Schritt stellen Sie jetzt die virtuelle Festplatte auf dem Zielcomputer bereit. Dazu kopieren Sie die Datei auf den Computer in das Stammverzeichnis der Festplatte C. Jetzt aktivieren Sie in Diskpart die virtuelle Festplatte:

```
diskpart
select vdisk file=c:\windows7.vhd
attach vdisk
```

Nun müssen Sie mit dem Befehl *list volume* den Laufwerksbuchstaben in Erfahrung bringen, den Windows der virtuellen Festplatte zugewiesen hat. Der nächste Schritt besteht darin, dass Sie den Bootmanager für das neue System erstellen. Dazu benötigen Sie das Tool BCDboot, welches Sie im Verzeichnis "\System32" der virtuellen Festplatte für Windows 7 finden. Verwenden Sie folgende Befehle:

```
cd d:\windows\system32
bcdboot d:\windows /s s:
```

Statt "D:" tragen Sie den Laufwerksbuchstaben ein, den Windows Ihrer virtuellen Festplatte zugewiesen hat und trennen dann die virtuelle Festplatte wieder mit Diskpart:

```
diskpart
select vdisk file=c:\windows7.vhd
detach vdisk
exit
```

Booten Sie jetzt den Computer neu. Das Betriebssystem sollte jetzt fehlerfrei von der *.vhd-Datei starten.

Parallele Installation von Windows 7 auf Computern mit Windows XP

Unter manchen Umständen kann es sinnvoll sein, Windows 7 parallel zu Windows XP zu installieren, zum Beispiel, wenn Sie nicht sicher sind, ob spezielle Programme unter dem neuen Betriebssystem funktionieren. Auch wenn Sie nur eine Festplatte im Rechner einsetzen, ist das möglich.

Neben der Möglichkeit, Windows 7 virtuell zu booten, können Sie eine bestehende Partition auch verkleinern. Dazu starten Sie den Computer mit Windows 7-DVD. Klicken Sie anstatt auf "Jetzt installieren" auf "Computerreparaturoptionen" und wählen Sie im Fenster Systemwiederherstellungsoptionen "Weiter", damit Sie zu den Tools gelangen, die Windows 7 zur Verfügung stellt (startet der Assistent für die Windows-Wiederherstellung, brechen Sie diesen ab, bis das Fenster mit den Systemwiederherstellungstools erscheint). Wählen Sie bei den Systemwiederherstellungsoptionen die Eingabeaufforderung aus und tippen Sie dort den Befehl *diskpart* ein und bestätigen Sie. Anschließend wechselt die Eingabeaufforderung in die Diskpart-Eingabe.

Über *list disk* erhalten Sie die Anzeige der Festplatte. Geben Sie nun *select disk 0* ein, wenn es sich um die Festplatte 0 des Systems handelt, also der ersten Platte im Rechner. Nun benötigen Sie die folgenden Kommandos:

```
list partition
select partition 1
shrink minimum=20000
```

Der letzte Befehl sorgt für genügend Festplattenplatz. Nach der Verkleinerung starten Sie den Rechner neu und booten von der Windows 7-DVD. Starten Sie die normale Installation über "Jetzt installieren", wählen auf dem Fenster zur Installationsauswahl aber nicht "Upgrade" aus, sondern "Benutzerdefiniert". Wählen Sie auf dem nächsten Fenster den freien Speicherplatz aus, den Sie zuvor von der Windows XP-Systempartition verkleinert haben. Daraufhin beginnt Windows 7 mit seiner Installation. Schließen Sie diese ab und booten Sie den Rechner neu, bis das neue Bootmenü erscheint. *(jp)*

Links

[1] WAIK
http://tinyurl.com/krnrdd

Neuerungen im Active Directory unter Windows Server 2008 R2

Verzeichnisdienst in neuem Glanz

von Klaus Bierschenk

Windows Server 2008 R2 springt mit einer ganzen Reihe an Neuerungen aus dem Startblock. Neben grundsätzlichen Erweiterungen wie etwa der Einführung von Hyper-V 2.0 oder einer aufgebohrten PowerShell haben sich die Entwickler aus Redmond auch ausgiebig dem Active Directory (AD) gewidmet und dem Verzeichnisdienst – neben einer neuen Admin-Console – eine Menge sinnvoller Funktionen verpasst.

Alle Jahre wieder, wenn Microsoft ein neues Server-Betriebssystem auf den Markt bringt, halten Administratoren Ausschau nach Funktionen und Werkzeugen, die ihnen ihre tägliche Arbeit erleichtern. So liest sich auch diesmal die gesamte Liste mit Erweiterungen recht spannend und der eine oder andere wird sicher wieder Brauchbares finden. So zum Beispiel beim Active Directory: Erweiterungen wie der Offline-Domänenbeitritt, ein Papierkorb oder gar das nagelneue Active Directory-Verwaltungscenter versprechen, die administrativen Tätigkeiten zu vereinfachen.


Quelle: Magdalena Mirowicz - Fotolia.com

Offline-Domänenbeitritt

Bislang kontaktierte ein Client einen Domänencontroller, wenn sein Computerkonto einer Active Directory-Domäne hinzugefügt wurde. Eine bestehende Netzwerkverbindung war hierfür unumgänglich. Diese Zeiten sind jetzt vorbei und bei der Installation muss hierauf keine Rücksicht mehr genommen werden. Zumindest gilt dies für Windows 7 und Windows Server 2008 R2 Computerkonten. Der Domänenbeitritt lässt sich bei diesen Installationen auf den Zeitpunkt des ersten Rechnerstarts verlagern, auch ist kein sofortiger Neustart mehr erforderlich. Die hierzu notwendigen Schritte erledigen Sie mit dem neuen Befehlszeilentool *dsjoin.exe*. Im ersten Schritt kommt das Tool auf einem Admin-PC zur Ausführung. Hierbei legt es Informationen in einer Konfigurationsdatei ab und erstellt die Metadaten für das Computerkonto im AD. Während der Installation des Clients verarbeitet dieser dann ebenfalls mit dsjoin.exe die zuvor erstellte Konfigurationsdatei und das Computerkonto ist nach dem abschließenden Neustart des Rechners online.

Neues Verwaltungscenter

Seit der ersten Version des AD lassen sich die Objekte mit der Management Console "AD Benutzer und Computer" bearbeiten. Lange Zeit war dies ein adäquates Werkzeug und erfüllte meist seinen Zweck. Mittlerweile ist es allerdings recht angestaubt und im heutigen Enterprise-Umfeld gerade bei vielen Domänen kaum

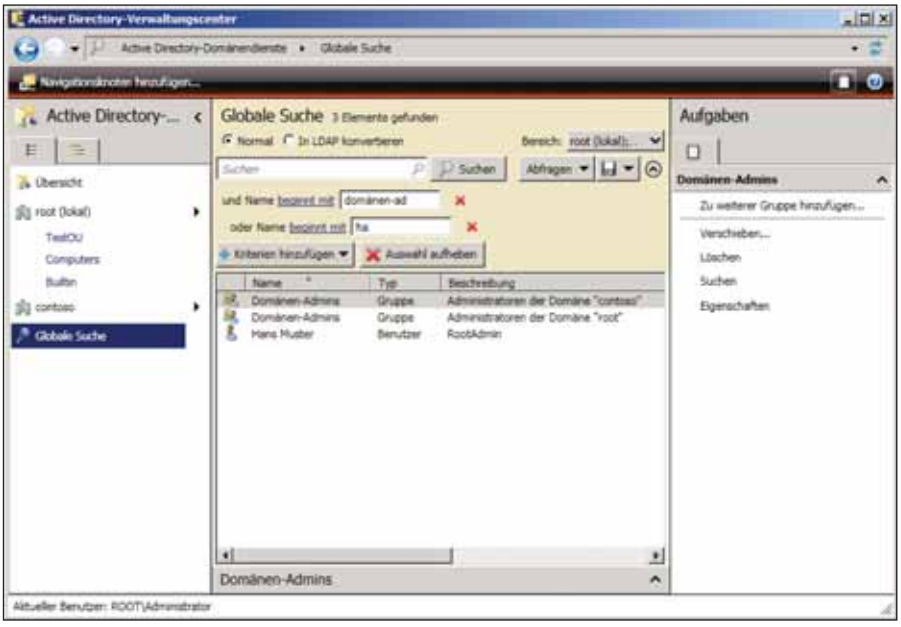


Bild 1: Noch nie war das Suchen im AD so einfach. Dank dem neuen AD-Verwaltungscenter funktioniert dies nun auch domänenübergreifend.

mehr hilfreich. Das neue AD-Verwaltungscenter schafft hier Abhilfe. Es folgt nicht mehr dem Prinzip der Microsoft Management Console (MMC), sondern ist eine eigenständige Applikation, deren intuitiver Aufbau die ersten Schritte erleichtert. Nach ein paar Klicks sollte sich jeder auskennen, dem das Active Directory vertraut ist. Im linken Teil des Programmfensters zeigt sich der Navigationsbereich. Je nach Vorliebe des Administrators sind hier zwei Darstellungsarten möglich: Einmal die gewohnte Konsolenansicht, bei der sich die Knoten selektieren und dadurch ein- und wieder ausblenden lassen. Des Weiteren gibt es eine Listenansicht, die sich einer flachen Darstellungsart bedient. Unabhängig von der gewählten Ansicht ist der Startpunkt für die Navigation immer frei wählbar. Anders als beim bekannten AD-Benutzer und -Computer, dessen Darstellung immer beim Domänenknoten beginnt. Ausgangspunkt in der Navigation kann eine beliebige Organisationseinheit sein, aber auch Container und sogar andere Domänen aus der Gesamtstruktur sind hier zugelassen. Im Verwaltungscenter, "Navigationsknoten" genannt, lassen diese sich zu jeder Zeit frei definieren. Damit ist schon eine der Stärken genannt: Die Darstellung in der GUI ist nicht mehr auf eine Domäne fokussiert, hier sind die aufgeführten Informationen aus der Gesamtstruktur beliebig kombinierbar.

In punkto Navigation und Suche gibt es aber noch weitere Raffinessen. Die globale Suche beispielsweise orientiert sich an den Navigationsknoten, die sich zum Zeitpunkt der Suche im Navigationsbereich befinden. Auf diese Art lässt sich selbst in den größten ADs mit hunderttausenden von Objekten schnell das Objekt der Begierde orten. Abgerundet werden die neuen Möglichkeiten durch aufgabenbasierte Filterkriterien, die anzuzeigende Objekte im Detailbereich zusätzlich eingrenzen. Objekte, die durch eine Suche gefunden wurden, lassen sich durch Mehrfachselektion in einem Schritt bearbeiten. Hier ist der Spielraum ebenfalls nicht auf eine Domäne begrenzt und die zu bearbeitenden Objekte dürfen verschiedenen Domänen der Gesamtstruktur entstammen.

Auffällig sind die Änderungen im Detailbereich zu einem Objekt. Beispielsweise bei der Darstellung der Benutzerinformationen. Hier hat Microsoft auf die bisherige, in Karteireiter geordnete Darstellung verzichtet. Der Weg geht hin zu einer Ansicht, die versucht, möglichst viele Informationen in einem Fenster zu bündeln. Dies ist letztendlich eine Frage des Geschmacks. Trotzdem fällt es angenehm auf, dass bei der Suche nach bestimmten Informationen zu einem Objekt das lästige Durchklicken durch die verschiedenen Tabs nicht mehr notwendig ist.

Das AD-Verwaltungscenter verrichtet seine Arbeit auf Basis von darunterliegenden Powershell-Skripten. Dabei ist allerdings schade, dass sich die Befehle nicht anzeigen lassen. Mit dieser Möglichkeit ließe sich für PowerShell-Unerfahrene der Zugang

Bild 2: Aufgabenbasierte Filterkriterien im AD-Verwaltungscenter vereinfachen wiederkehrende Arbeitsschritte

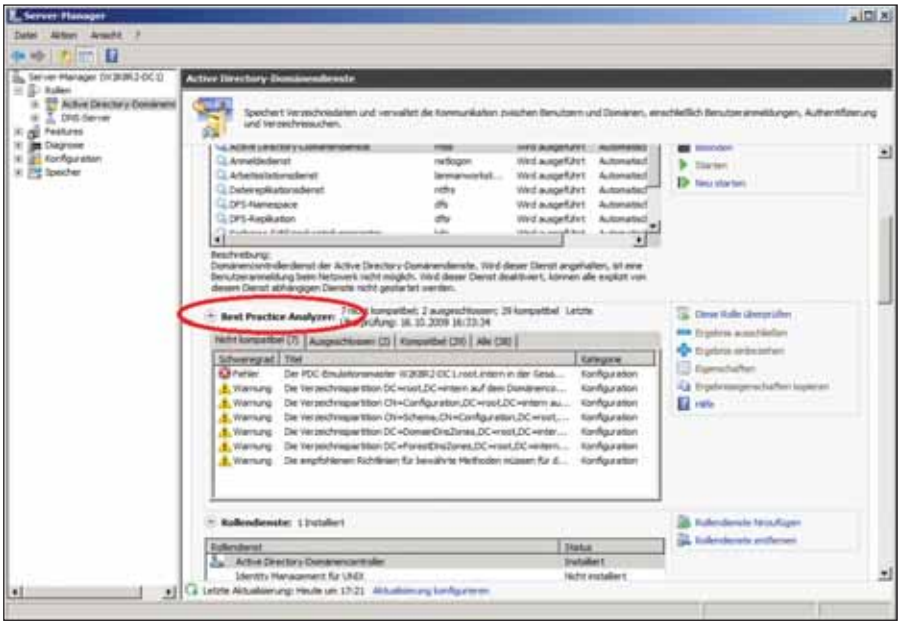


Bild 3: Der Best Practice Analyzer untersucht die aktuelle Umgebung und zeigt anhand von Microsoft-Empfehlungen Verbesserungspotenzial

zu der Sprache ebnen. Desweiteren ließen sich hierdurch Aktionen grundsätzlich designen, um sie dann im Anschluss für ein Skript an beliebige Bedürfnisse weiter anzupassen. Laut Microsoft ist dies eine Option für eine künftige Version.

Fehlkonfigurationen schnell erkennen

Der Best Practise Analyser (BPA) ist für verschiedene Dienste von Windows Server 2008 R2 verfügbar. Neben dem Active Directory lassen sich die Terminal Services, DNS oder auch die AD-Zertifikatsdienste in Bezug auf Fehlkonfigurationen hin untersuchen. Die Funktionsweise ist schlicht: Der BPA vergleicht vorgegebene Regelsätze mit dem, was er in der aktuellen Umgebung vorfindet. Bei Abweichungen quittiert er diese mit Warnungen oder gar Fehlern. Die Einstufung ist fest vorgegeben und folgt den Best Practices von Microsoft. Unter der Haube des BPA arbeiten ebenfalls PowerShell-Skripte, welche die umfangreichen Tests im Active Directory durchführen. Allerdings ist im Fehlerfall der BPA nicht das richtige Tool, um mögliche Ursachen für Probleme aufzuspüren. Der Einsatzzweck dürfte eher nach größeren Installationen gegeben sein oder aber einfach nur, um von Zeit zu Zeit zu sehen, ob noch alles richtig tickt.

Der BPA hat sich übrigens gut versteckt. Er befindet sich im Server Manager bei den installierten Rollen. Unterhalb der Rolle "Active Directory Domänendienste" lässt er sich aufrufen und die analysierten Daten können dort direkt eingesehen oder in die Zwischenablage kopiert werden. Möglichkeiten für einen Report oder einen Export der ermittelten Informationen sind nicht vorgesehen. Nachteilig ist das kleine Fenster, das innerhalb des Servermanagers einen gedrängten Eindruck hinterlässt.

Endlich da: Der Papierkorb für AD-Objekte

Gelöschte Objekte im AD gibt es immer wieder und dies lässt sich im administrativen Alltag wohl kaum vermeiden. Bislang ein Ärgernis, da der Weg, diese als "tombstoned" bezeichneten Objekte wiederherzustellen, äußerst umständlich ist. Autorisierter und nicht autorisierter Restore sind zeitaufwendig. Hinzu kommen fehlende Backlinks (Referenzen zu Infos, die nicht beim Objekt gespeichert werden, wie etwa Gruppenmitgliedschaften), um die es sich zu kümmern gilt, nachdem das gelöschte Objekt wieder an Ort

und Stelle ist. Ein solches Verfahren kann eigentlich keinem Administrator gefallen, ist doch meist Eile geboten, wenn ein Objekt versehentlich gelöscht wurde.

Mit R2 hat das Active Directory nun einen Papierkorb an Bord und die Arie zur Wiederherstellung gelöschter Objekte ist deutlich kürzer. Einfach gesagt: Wird ein Objekt gelöscht, wird es nicht wie bisher zum Tombstoned-Objekt, sondern verweilt noch eine Zeit (standardmäßig 180 Tage, analog zur Tombstone-Lifetime) im Papierkorb. Dies ist quasi eine Zwischenstufe vor dem bisher bekannten Löschprozess. Erst danach werden die Backlinks entfernt, was bedeutet, dass ein im Papierkorb befindliches Objekt, wie etwa ein Benutzerkonto, noch über alle Informationen verfügt, nachdem das gelöschte Konto wiederhergestellt wurde. Der Papierkorb als solches ist in der GUI der verschiedenen Admin-Tools übrigens nicht aufzutreiben. Seine Bedienung vollzieht sich ausschließlich über ein Cmdlet namens "Restore-ADObject". Voraussetzung für den Papierkorb ist, dass die Funktionsebene für die Gesamtstruktur auf den neuen Level Windows Server 2008 R2 heraufgestuft wurde und dass der Papierkorb grundlegend aktiviert ist.

Das Cmdlet zum Wiederherstellen gelöschter Objekte bietet eine Menge weiterer Möglichkeiten, die über die Funktion eines einfachen Papierkorbes hinausgehen. Daher lohnt es sich, in einer ruhigen Minute damit herumzuspielen, um für den Ernstfall gerüstet zu sein. Unabhängig vom Papierkorb und R2 lassen sich AD-Objekte übrigens vor versehentlichem Löschen schützen. Hierzu muss diese Option in den Objekteigenschaften entsprechend vermerkt sein.

Sonstige Neuerungen

Wer so oft, wie es geht, auf die Maus verzichten möchte, für den hat Microsoft rund 30 zusätzliche Cmdlets in das Active Directory Modul für die Powershell gepackt. Die gleichnamige Eingabeaufforderung lässt sich über das Startmenü aufrufen und eine Übersicht über alle Cmdlets liefert das Kommando *Get-Command *-AD**. Die Liste ist mittlerweile recht umfangreich und derjenige, der die Cmdlets geschickt einzusetzen weiß, hat jenseits der grafischen Verwaltungswerkzeuge ganz andere Möglichkeiten, sein AD zu administrieren. Mit dem Kommando *Get-Help {cmdlet name} -Full* lässt sich eine detaillierte Hilfe zu einem bestimmten Cmdlet anzeigen.

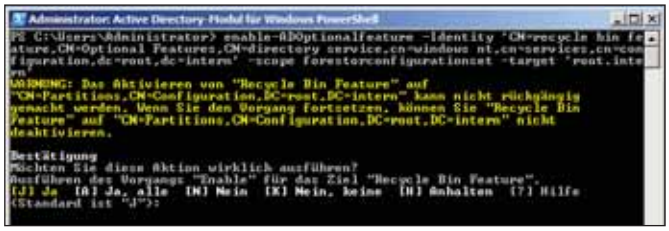


Bild 4: Auf einen optischen Papierkorb müssen Admins verzichten. Bislang erfolgt die Bedienung ausschließlich über die Powershell

Managed Service Accounts sind ein weiteres neues Feature in R2 mit der Möglichkeit, die Administration von Dienstkonten weitestgehend zu automatisieren, einschließlich der Verwaltung des Kennwortes für das Dienstkonto. Damit dürfte endlich Schluss sein mit hängenden Diensten auf Applikationsservern, die nicht starten, weil das Passwort in der Domäne zurückgesetzt wurde oder gar das Konto gesperrt ist. Bei den Managed Service Accounts handelt es sich wiederum um eine neue Funktion, die ohne GUI daherkommt und deren Bedienung ausschließlich über Powershell-Befehle erfolgt.

Eine Technet-Webseite [1] bietet diverse Step-by-Step Guides an, die anhand praktischer Beispiele in die neuen Funktionen des Active Directories einführen. Zudem findet sich dort ein Migrationsleitfaden [2], der auf die wesentlichen Aspekte bei einem Wechsel eingeht und abhängige Dienste wie etwa DNS, die bei einer Migration auch Thema sind, nicht ausklammert.

Blick in die Zukunft

Spätestens jetzt dürfte der Zeitpunkt gekommen sein, an dem sich AD-Administratoren mit der Powershell auseinandersetzen sollten. Microsoft zeigt mit der Entwicklung des R2-Servers, dass die Powershell zunehmend an Bedeutung gewinnt. Die neue Powershell-basierte GUI und die Tatsache, dass bestimmte Funktionen ausschließlich per Powershell auszuführen sind, so etwa die Administration der Managed Service Accounts, sprechen eine deutliche Sprache.

Entscheider, die vor der Wahl stehen, ihre Active Directory zu erneuern, können es langsam angehen lassen. Nachdem das Schema (mittels *adprep.exe* auf der Server DVD) angepasst wurde, lässt sich der erste R2-Domänencontroller der Domäne hinzufügen. Der weitere Ausbau kann sukzessive erfolgen. Zu beachten ist nur, dass bei bestimmten Funktionen die Funktionsebene der Gesamtstruktur auf höchstem Level sein muss und in diesem Release keine DCs älterer Versionen mehr zulässig sind.

Fazit

Der neue Server von Microsoft bringt im Bereich Active Directory gewinnbringende Neuerungen. Allein das AD-Verwaltungscenter ist es wert, seinem AD einen Windows Server 2008 R2 DC zu spendieren. Offline Domänenbeitritt oder der Papierkorb runden die gelungenen Funktionen im Bereich Active Directory ab. Wie bei kaum einem anderen neuen Betriebssystemrelease empfiehlt es sich diesmal, die neuen AD-Funktionen in einer Versuchsumgebung durchzuspielen. Die Powershell-Befehle sind mitunter recht zickig und ihr Umgang verlangt Geduld. Diese wird allerdings belohnt. *(ln)*

[1] Windows Server 2008 R2 Active Directory
http://technet.microsoft.com/de-de/library/dd378801(WS.10).aspx
[2] Migrationsleitfaden für Server 2008 R2
http://technet.microsoft.com/de-de/library/dd379558(WS.10).aspx

Links

VoIP-Umgebungen schützen

Abhörsichere Leitung

von Mathias Hein


Quelle: Arik Levy - Fotolia.com

Die Vereinheitlichung der Kommunikationstechnologie – also die Vereinigung von Daten, Video und Sprache – wird Konvergenz genannt. Diese trägt zu einer signifikanten Senkung der Betriebs- und Beschaffungskosten bei. Jede Technologie hat aber ihre Stärken und Schwächen. Daher muss bereits bei der Planung eventuellen Sicherheitsproblemen entgegengewirkt werden. In diesem Beitrag zeigt IT-Administrator aktuelle Schwachstellen und Gefährdungen der VoIP-Telefonie auf und stellt sinnvolle Schutzmaßnahmen vor.

In den vergangenen Jahren entwickelte sich die IP-Telefontechnik zu einem der wichtigsten Standards für die Zukunft der Kommunikation. Selbst die traditionellen Telefonanbieter bewegen sich in immer schnellerem Tempo weg von ihren ursprünglichen Märkten. Daneben drängen im Anbietermarkt auch alternative Telefonanbieter in den Markt. Diese nutzen die VoIP-Technologie, um über den Preis und die Leistung möglichst viele Endkunden (Consumer und Geschäftskunden) an sich zu binden. Auch die klassischen Anbieter von Telefonanlagen bauen ihr Portfolio drastisch um und bieten fast nur noch VoIP-Produkte an.

Die Anfänge von VoIP wurden mehr durch das Marketing als durch verfügbare Technologie angetrieben. Die traditionellen Telefonunternehmen argumentierten gegen den VoIP-Ansatz mit fehlenden Standards und vor allem mit der zu geringen Verfügbarkeit beziehungsweise Zuverlässigkeit der Netzwerkprodukte. Inzwischen stehen die passenden Netzwerkprodukte (Switches) zur Verfügung und Problembereiche wie beispielsweise Echos, Verzögerungen, Paketverluste und Jitter gehören durch ein ordentliches Netzdesign und durch die Integration von QoS-Funktionen der Vergangenheit an.

Die Einführung der IP-Telefonie öffnet jedoch automatisch Spammern ein neues Tor in das Unternehmensnetz. Die Verbreitung von Spams ist über konventionelle Telefonsysteme unmöglich, aber Spam over Internet Technology (SPIT) stellt Unternehmen vor neue Sicherheitsbedrohungen. Die IP-Telefonanlage stellt in der Praxis nichts anderes als einen im Netzwerk eingebundenen Server dar. Daher sind diese Komponenten DoS-Attacken oder Abhörangriffen ausgesetzt.

Abhören der Sprachinformationen

Die über die Netzwerke übermittelten Sprachinformationen lassen sich mit Hilfe eines Sniffers aufzeichnen beziehungsweise abhören. Dies war bei den analogen und digitalen Telefongesprächen nicht anders. Bei der klassischen Telefonie genügte bereits ein einfacher Kopfhörer, um ein Gespräch auf der Leitung mithören zu können. Für das Abhören von ISDN benötigte der Mithörer einen ISDN-Analysator. Nur eine Verschlüsselung der Leitungen konnte das Mitlesen/Mithören verhindern. Diese Geräte waren teuer und recht umständlich zu bedienen.

Als Schutz gegen ein Mitlesen der Sprachströme im Netz helfen bereits simple Schutzmechanismen:

- Die Sprachkommunikation zwischen den Netzen eines Unternehmens, zu Partnerfirmen, zu Mitarbeitern im Home-Office oder mobilen Mitarbeitern (inklusive der WLAN-Verbindungen) erfolgt über das Internet nur über eine verschlüsselte VPN-Verbindung (inklusive Verschlüsselung und Authentifizierung).
- Das Abhören der Daten/Sprachströme zwischen den Mitarbeitern innerhalb des Unternehmens ist in der Regel durch Betriebsvereinbarungen verboten. Die neuen SIP-Telefone und Softphones unterstützen das IPSec-Protokoll (via VPN-Clients) und ermöglichen somit eine sichere Unternehmenskommunikation.

Unsicherheit der Betriebssysteme, Anwendungen und Server

Die zentralen VoIP-Komponenten für die IP PBX, VoIP-Gateways, Signalisierungs- und SIP-Proxies, nutzen norma-

le Server-Komponenten. Durch die auf den Servern eingesetzten Betriebssysteme (Windows, Linux, Unix) unterliegen diese Ressourcen den normalen Angriffen durch Würmer, Trojaner und Viren. Für einen Hacker bietet ein zentrales VoIP-System ein natürliches Angriffsziel. Wird der Signalisierungsserver lahm gelegt und steht kein Backupsystem bereit, ist es um die Sprachkommunikation im Unternehmen geschehen. Auf den VoIP-Servern müssen alle unnötigen Services abgeschaltet beziehungsweise beseitigt werden, um die Angriffsfläche zu verkleinern. Außerdem erfordern diese Systeme bei den zyklischen Sicherheitsüberprüfungen ein besonderes Augenmerk auf Auffälligkeiten.

Reguläre Telefone sind "dumme" Endgeräte. Beim VoIP dreht sich das Bild: Die Endgeräte enthalten alle Intelligenz und interagieren selbständig mit den VoIP- und Netzwerkressourcen. Besonders VoIP-PCs (Softphones) bieten durch die gleichzeitige Nutzung von Sprache und Daten (über die betreffenden Applikationen) auf der gleichen Plattform attraktive Ziele für Hacker, um Trojaner oder andere schädliche Programme zu installieren, um anschließend die Angriffe auf das Sprachnetzwerk zu starten.

Eine wirkungsvolle Verteidigungsstrategie besteht darin, die Sprach- und Datennetze logisch durch VLANs zu trennen. Durch diese Netzsegmentierung hat ein Angriff auf das Datennetz nicht zwangsläufig Auswirkungen auf den Sprachverkehr. Auch die Zugänge zur Außenwelt (die VoIP-Gateways) erfordern einen Schutz gegen Viren und Attacken. Die ersten Angriffe auf die klassische Telefonie bestanden darin, in ein Telefonsystem (eines Betreibers oder des Telefonanbieters) einzudringen und auf deren Kosten zu telefonieren. Diese so genannten "Phone Phreaks" sind auch im Internet zu finden. Daher ist erforderlich, auch das VoIP-System gegen einen solchen Missbrauch und die daraus resultierenden Kosten zu schützen.

Überlastete Firewalls

Das größte Problem besteht jedoch darin, dass die meisten bisher eingesetzten Sicherheitstechnologien (Firewalls und Intrusion Detection Systeme; IDS) mehr oder weniger nutzlos bei Angriffen auf die "neuen" Ziele im Netzwerk sind. Aufgrund der Echtzeitnatur der VoIP-Services sollten diese beim Durchgang durch die Firewalls nicht verzögert werden. Der SIP-Mechanismus nutzt das TCP zur Signalisierung und zum Verbindungsaufbau und UDP zur Nutzdatenübertragung. Versteht eine Firewall das SIP, öffnet und schließt diese die Ports für den VoIP-Verkehr automatisch. Diese Ports bleiben jedoch nur bis zur Beendigung des betreffenden Anrufs offen. Darüber hinaus werden die Nutzdaten beim VoIP per Real-Time Protocol (RTP) übermittelt. Dieses nutzt dynamisch die Ports von 1024 bis 65.5534.

Bei vielen Firewalls werden die Probleme erst bei steigendem Sprachverkehr sichtbar. Der VoIP-Verkehr erfordert eine tiefere Inspektion der SIP-Pakete durch die Firewall. Dies resultiert in einer höheren CPU-, Puffer- und Memoryauslastung. Mit steigender Anzahl von Sprachströmen kann bereits die von der Firewall erzeugte Verzögerung über die Grenze von 50 bis 100 Millisekunden steigen und führt automatisch zur Verschlechterung der Sprachqualität.

Die Paketgröße hat natürlich auch eine direkte Auswirkung auf die Firewall-Performance. Sämtliche Netzkomponenten benötigen für die Übermittlung kurzer Pakete wesentlich mehr interne Ressourcen als für die Übertragung langer Pakete. Der typische VoIP-Verkehr weist Längen zwischen 64 bis 200 Byte auf. Eine Firewall kann theoretisch mehrere 100 MBit/s-Interfaces unterstützen, aber die CPU wird in der Regel bei einer hohen Anzahl an kurzen Paketen schnell in die Sättigung kommen. Übernimmt die Firewall auch noch die VPN-Gateway-Funktion, muss sichergestellt werden, dass diese beim Tunneln und Verschlüsseln/Entschlüsseln keine zusätzlichen Verzögerungen verursacht. Eine Alternative besteht im Einsatz von Voice Proxies, die auf den Umgang mit Multimedia-Verkehr spezialisiert sind. Diese

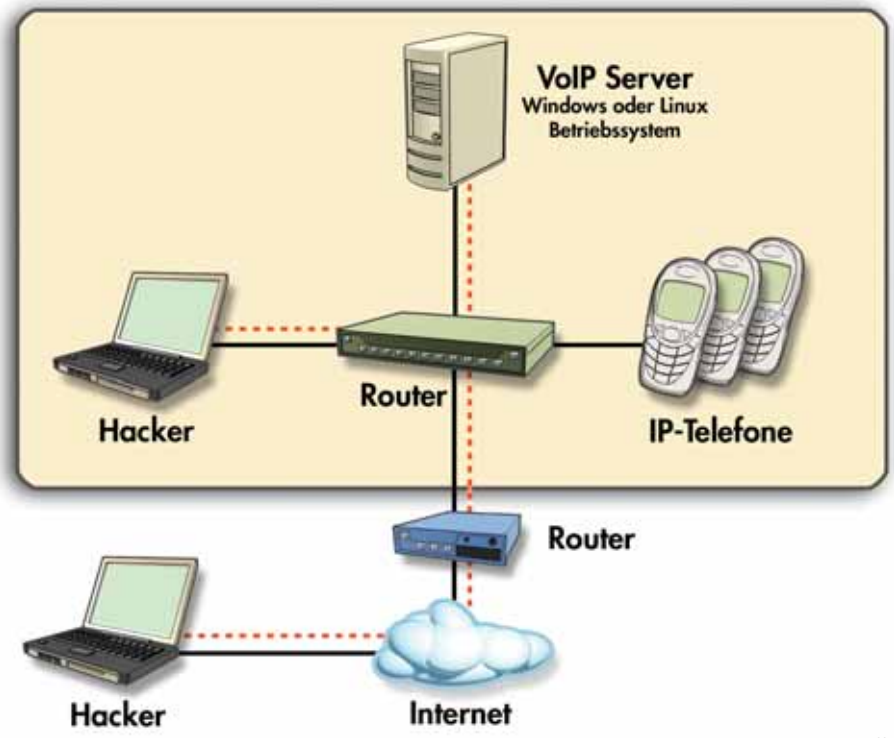


Bild 1: Mögliche Angriffe auf IP-Telefonanlagen

Komponenten signalisieren der Firewall, welche Ports geöffnet werden sollen und wie zusätzliche Aufgaben wie die Network Address Translation (NAT) umgesetzt werden. Die IETF erarbeitet im Moment einen Protokoll- und Architekturvorschlag (Arbeitsname: Middlebox Communication Architecture and Framework; MIDCOM) zur direkten Integration der Proxies in traditionellen Firewalls.

Neue Angriffsarten

Der Großteil der Angriffsarten auf die VoIP-Ressourcen ähnelt denen der Datennetze. Neue Angriffsarten sind jedoch bereits in Entwicklung. Diese Exploits nutzen die Sicherheitslöcher im Zusammenspiel zwischen den Sprach- und Datenressourcen aus. Beispielsweise ist vermehrt vom Registration- beziehungsweise Call-Highjacking von SIP-Telefonen zum öffentlichen VoIP-Anbieter zu hören. Dabei wird die gültige IP-Adresse eines IP-Telefons auf eine beliebige IP-Adresse des Hackers umkonfiguriert. Das Resultat: Alle über das VoIP-Netz eingehenden Anrufe für den betreffenden Benutzer erreichen diesen nicht.

Auch ist die Übernahme und ein Denial of Service von SIP-Telefonen möglich. Zum Glück für den VoIP-Administrator erfordern diese Angriffe noch detaillierte technische Kenntnisse um die jeweiligen Produkte und gehen weit über die Fähigkeiten der Script-Kiddies oder der normalen Hacker hinaus, aber demonstrieren doch eindrucksvoll, welche Angriffsfläche konvergente Netze bieten.

Folgende Maßnahmen sollten in jedem Unternehmen berücksichtigt werden, um die Sicherheitsrisiken von VoIP deutlich zu minimieren:

- Einführen von Benutz-Logins: Jeder User sollte sich für IP-Telefonie mit einem Benutzer-Kennwort einloggen. Somit stellen Sie wie bei der PC-Nutzung sicher, dass nur autorisierte Anwender über das Netzwerk telefonieren.
- Verschlüsselung der Daten: Um Lauschangriffe von Hackern zu vermeiden, sollten die Daten auf jeden Fall verschlüsselt werden.
- Einsatz von Firewalls: Eine Firewall vor dem VoIP-System hilft, die Attacken rechtzeitig zu filtern.
- Alle Patches installieren: Die neu verfügbaren Patches zum Schutz des VoIP-Systems müssen immer sofort aktualisiert werden. Dieser Update-Ablauf sollte bei den Verantwortlichen an oberster Stelle stehen.
- Vorausschauende Planung: Fällt das Netzwerk aus, ist auch das VoIP-System und somit die gesamte Telefonanlage außer Betrieb. Damit das Tagesgeschäft nicht unterbrochen wird, müssen bereits bei der Netzplanung diese Ausnahmefälle berücksichtigt werden.

VoIP-Telefonie vor Angriffen schützen

Es gibt einige Vorgehensweisen, mit denen sich viel für den Schutz der IP-Anlagen erreichen lässt. Für die IP-Telefonie sollten die gleichen Grundsätze zum Schutz des Netzwerks gelten wie bei anderen IP-Systemen auch. Dabei geht es einmal darum, eine umfangreiche Strategie zu entwickeln, um möglichst viele Komponenten der IP-PBX zu schützen. Neben dem Netzwerk sollten Unternehmen auch die IP-Telefone nicht vergessen. Es geht darum, zu klären, wie und wo die Apparate installiert sind und wie das Netzwerk aussieht.

Eine beliebte Methode, um das Netzwerk zu schützen, ist, bestimmte Komponenten in einem VLAN zu isolieren. Viele VoIP-Telefone besitzen bereits integrierte Mini-Switches, die 802.1p/Q-Trunks von den Telefonen zum Etagen-Switch (Edge) aufbauen. Damit lässt sich der Sprach- vom Daten-Verkehr trennen, vom Telefon bis zur IP-Anlage. VLANs erhöhen die Sicherheit, aber sie richten nicht alles. So kann ein Angreifer in das Voice-VLAN kommen, indem er sich an eine LAN-Buchse hängt und das VLAN per Software emuliert. Es lassen sich aber die UDP- und TCP-Ports begrenzen, die auf die PBX vom LAN her zugreifen dürfen. Hierzu gibt es Access-Control-Lists (ACLs) auf Switchen oder Routern. Auch eine Firewall kann dazu dienen, die TCP- und UDP-Ports zu begrenzen. Auch die Ethernet-Adressen einzuschränken, die auf die Ports beziehungsweise das VLAN zugreifen dürfen, ist eine Möglichkeit.

Ein separates VLAN für die Telefone erleichtert es zudem, die Bandbreite zu kontrollieren, um QoS sicherzustellen. Dies schützt auch die IP-PBX bei Denial-of-Service-Attacken (DoS), die von Würmern innerhalb des LANs kommen. VoIP verbraucht nicht so viel Bandbreite, aber es reagiert empfindlich bei Paket-Verlust und Verzögerungen.

Administratoren sollten auch vorsichtig mit Protokollen für Autokonfiguration

Sicherheitsmechanismen für VoIP						
Mechanismus	Vertraulichkeit	Integrität	Authentizität	Zugriffskontrolle	Verbindlichkeit	Verfügbarkeit
Architektur						
L2/L1-Sicherheit	h	h	–	(h)	–	–
DoS Protection	–	–	–	–	–	x
Stateful Firewall	–	–	–	x	–	–
Intrusion Detection	–	–	–	–	–	x
Netzstruktur	–	–	–	–	–	x
Session Border Controller	–	–	(x)	x		x
Protokolle						
IPsec / VPN	h	h	h	(h)	–	–
TLS/SIPS	h,sig	h,sig	h,sig	–	–	–
S/MIME	x,sdp	x,sig	x,sig	–	x,sig	–
SRTP	x,media	x,media	x,media	–	–	–
SCTP	–	–	–	–	–	x,sig
Authent./Digest	–	(x)	x	x	x	–

x = vorhanden, (x) = eingeschränkt vorhanden, – = nicht vorhanden, h = nur Hop-by-Hop
(sig = nur Signalisierung, sdp = nur SDP-Daten, media = nur Medienströme)

wie LLDP-MED (Logical-Link-Discovery-Protocol-Media-Endpoint-Device) oder dem proprietären CDP (Cisco-Discovery-Protocol) umgehen. Sie erleichtern zwar die Netzwerkverwaltung, lassen sich aber auch leicht fälschen.

Mit dem Einsatz von Verschlüsselung sind VoIP-Gespräche besser geschützt als bei den herkömmlichen Telefonen. Allerdings gilt dies nur innerhalb des Unternehmensnetzwerks. Für Telefonate in das öffentliche Netz funktioniert dies nicht mehr. So wie SRTP (Secure-RTP) das eigentliche Gespräch schützt, übernimmt dies SIPS (SIP-Secure) für die Signalisierung. Dies ist einmal wichtig, weil über SIP die Schlüssel für den anschließenden SRTP-Einsatz übertragen werden. Zum anderen verhindert SIPS, dass der Angreifer Informationen über die Telefonie wie Telefonnummern bekommt.

Regeln in der Firewall sollten verhindern, dass jeglicher Internet-Verkehr zu den IP-Telefonie-Servern, den Gateways oder den IP-Apparaten gelangt. Außerdem geht es darum, den Übergang zwischen Telefonie-VLAN und IP-PBX zu begrenzen. Session-Border-Controller sind eine Überlegung wert. Sie analysieren die Verkehrsmuster, um etwa das Netz vor SIP-DoS-Attacken zu schützen.

VPNs sind ein gutes Mittel, um den Zugang zum Unternehmensnetz für mobile Mitarbeiter bereitzustellen. Beim Einsatz von Softphones kann es aber passieren, dass ein Eindringen in das VPN auch das Telefonie-System betrifft. Ein VPN führt auch zu einer deutlich höheren Verzögerung bei einem Gespräch, weshalb der Einsatz von VoIP hier dann auch scheitern kann.

Fazit

In absehbarer Zeit werden klassische Telefonanlagen nicht mehr erhältlich sein und müssen durch VoIP-Technologien ersetzt werden. Die Vereinigung von Sprache, Video und Daten in einem gemeinsamen Netzwerk erfordert jedoch ein noch besseres Sicherheitsmanagement und zusätzliche Sicherheitsfunktionen. Das Aufspüren dieser neuen Angriffe erfordert ein Wissensupgrade und neue Strategien zur Abwehr. *(jp)*

DNS-Fehler in Windows finden und beheben (1)

Training für das Namensgedächtnis

von Thomas Joos

Aufgabe des "Domain Name System" – kurz DNS – ist das Auflösen von Computernamen zu IP-Adressen, auch Forward-Lookup genannt. Eine weitere Aufgabe ist das Auflösen von IP-Adressen zu Computernamen – das Reverse-Lookup. Da viele Serverdienste von einer sauberen Namensauflösung abhängen, funktionieren diese nicht mehr richtig, wenn das DNS-System fehlerhaft arbeitet. Vor allem bei der Nutzung eines Active Directory liegt die Ursache für Fehler oft im DNS. In unserer zweiteiligen Workshopserie zeigen wir Ihnen, wie Sie die Namensauflösung in Ihrem Netzwerk am Laufen halten.

Ohne funktionierende Namensauflösung finden sich die Rechner nicht mehr

Computernamen im DNS bestehen nicht nur aus einem NetBIOS-Namen, wie zum Beispiel dc01, sondern zusätzlich aus dem Domänennamen wie contoso.com. Ein vollständiger Rechnername wird auch als voll qualifizierter Domänenname (Full Qualified Domain Name, FQDN) bezeichnet. Der FQDN eines Servers dc01 in der Domäne contoso.com ist dc01.contoso.com. Die beiden Rechner dc01.contoso.com und dc01.contoso.int sind damit zwei vollkommen unterschiedliche Systeme. Um eine Verbindung mit einem dieser Systeme aufzubauen, reicht es nicht aus, nur den Namen dc01 auflösen zu können. Es ist wichtig, dass die beteiligten Computer, welche die Verbindung zu den beiden Servern aufnehmen sollen, beide Domänennamen auflösen können. DNS-Domänen, wie in diesem Beispiel contoso.com und contoso.int, werden auf DNS-Servern in so genannten Zonen verwaltet.

Eine Zone kann mehrere Subdomänen einer Domäne verwalten, zum Beispiel de.contoso.com oder fr.contoso.com. Allerdings kann eine Zone auf einem DNS-Server nicht verschiedene Namensräume verwalten, wie zum Beispiel contoso.com und contoso.int. In diesem Fall müssten für diese beiden DNS-Domänen zwei getrennte Zonen angelegt werden. Eine weitere wichtige Aufgabe von DNS ist das Auflösen von SRV-Records (Service-Records). In SRV-Records befinden sich Informationen zu speziellen Serverdiensten, die in DNS veröffentlicht sind. Ein Beispiel wäre der bekannte SRV-Record "MX" (Mailexchange), der festlegt, welche Mailserver es in einer Domäne gibt und wie die IP-Adresse dieser Server lautet. Aber auch das Active Directory legt solche SRV-Einträge an: Wollen Computer spezielle Dienste im Active Directory erreichen, zum Beispiel einen globalen Katalogserver, können die DNS-Server befragt werden, die alle SRV-Records der globalen Katalogserver kennen.

Erweiterte DNS-Einstellungen beachten

Auf der Registerkarte "DNS" in den erweiterten Netzwerkeinstellungen eines Windows Server 2000 bis 2008 lassen sich Einstellungen vornehmen, um den Rechner besser in eine Windows-Domäne einzubinden. Zunächst sind standardmäßig nur die folgenden Optionen aktiviert:

- Primäre und verbindungsspezifische DNS-Suffixe anhängen
- Übergeordnete Suffixe des primären DNS-Suffixes anhängen
- Adressen dieser Verbindung in DNS registrieren

Diese Optionen spielen bei der Namensauflösung in einer DNS-Infrastruktur eine erhebliche Rolle. **Primäre und verbindungsspezifische DNS-Suffixe anhängen** legt fest, dass der Rechner versucht, bei der Auflösung von Rechnernamen immer automatisch das konfigurierte primäre DNS-Suffix des eigenen Computernamens anzuhängen. Wollen Sie zum Beispiel einen Rechnernamen mit der Bezeichnung dc01 auf-

Bild 1: Erweiterte DNS-Einstellungen für Windows Server 2008

lösen, versucht der Rechner eine Namensauflösung nach dc01.contoso.com, wenn das primäre DNS-Suffix des Servers contoso.com ist.

Die Option **Übergeordnete Suffixe des primären DNS-Suffixes anhängen** bewirkt, dass auch die Namen von übergeordneten Domänen bei der Namensauflösung verwendet werden. Wenn Sie zum Beispiel in einer untergeordneten Domäne mit der Bezeichnung muenchen.de.contoso.com einen Servernamen dc05 auflösen wollen, versucht der Rechner zunächst die Auflösung über dc05.muenchen.de.contoso.com, falls dies das primäre DNS-Suffix des PCs oder Servers ist. Im Anschluss versucht der Server, den Namen über dc05.de.contoso.com und dann über dc05.contoso.com aufzulösen, da diese Domänen der Domäne muenchen.de.contoso.com übergeordnet sind.

Zusätzlich haben Sie noch dank **DNS-Suffix für diese Verbindung** die Möglichkeit, in diesem Bereich ein weiteres beliebiges DNS-Suffix einzutragen. Wenn der Rechner den eingegebenen Namen bei seinem konfigurierten DNS-Server nicht über sein eigenes primäres DNS-Suffix finden kann, versucht er es mit dem DNS-Suffix in diesem Feld. Wollen Sie zum Beispiel den Servernamen dc06 auflösen, versucht der PC oder Server zunächst die Auflösung in dc06.contoso.com, sofern das sein primäres DNS-Suffix ist. Tragen Sie im Feld "DNS-Suffix für diese Verbindung" noch ein Suffix in der Form muenchen.de.microsoft.com ein, versucht der PC auch den Namen nach dc06.muenchen.de.microsoft.com aufzulösen.

Auch die Option **Adressen dieser Verbindung in DNS registrieren** ist bereits standardmäßig aktiviert. Ein DNS-Server unter Windows Server 2003/2008 hat die Möglichkeit, Einträge dynamisch zu registrieren. Durch dieses dynamische DNS müssen Hosteinträge nicht mehr manuell durchgeführt werden. Sobald sich ein Rechner im Netzwerk anmeldet, versucht er seinen FQDN beim konfigurierten DNS-Server automatisch einzutragen. Dieser Punkt ist für die interne Namensauflösung in einem Active Directory-Netzwerk von sehr großer Bedeutung.

Außer den standardmäßig aktivierten Optionen gibt es noch weitere Möglichkeiten, die Sie in diesem Fenster konfigurieren können. Wenn Sie die Option **Diese DNS-Suffixe anhängen** aktivieren, können Sie DNS-Suffixe konfigurieren, nach denen unvollständige Rechnernamen aufgelöst werden. Dabei verwendet der Server weder das primäre DNS-Suffix des Servers noch die DNS-Suffixe dieser Verbindung. Er hängt die DNS-Suffixe in der Reihenfolge an, die im Feld "Diese DNS-Suffixe anhängen (in Reihenfolge)" konfiguriert sind. Achten Sie bei der Konfiguration darauf, dass möglichst das DNS-Suffix der Windows-Domäne, in der dieser Server Mitglied ist, als Erstes in dieser Liste eingetragen ist. Diese Option wird häufig verwendet, um die Namensauflösung in Gesamtstrukturen mit mehreren Strukturen zu lösen. Dazu tragen Sie in der Reihenfolge alle Strukturen der Gesamtstruktur ein, um eine Namensauflösung innerhalb des Active Directorys zu gewährleisten.

Schalten Sie schließlich die Option **DNS-Suffix dieser Verbindung in DNS-Registrierung verwenden** ein, registriert sich der Server im DNS mit seinem Computernamen und seinem primären DNS-Suffix. Zusätzlich wird der Name mit dem DNS-Suffix auch beim DNS-Server registriert, der im Bereich DNS-Suffix für diese Verbindung konfiguriert ist.

Fehler in den DNS-Einstellungen beheben

Funktioniert die Namensauflösung nicht, sollten Sie strukturiert vorgehen, um den oder die Fehler zu finden. Auch wenn der Fehler auf den ersten Blick nichts mit DNS zu tun hat, lohnt es sich zu überprüfen, ob sich alle Namen korrekt auflösen lassen. Prüfen Sie, ob sich der Server sowohl in der Forward- als auch in der Reverse-Lookupzone korrekt eingetragen hat. Öffnen Sie danach eine Befehlszeile und geben Sie den Befehl *nslookup* ein. Die Eingabe des Befehls darf keinerlei Fehlermeldungen verursachen. Es muss der richtige FQDN des DNS-Servers und seine IP-Adresse angezeigt werden. Sollte das nicht der Fall sein, gehen Sie Schritt für Schritt vor, um den Fehler einzugrenzen:

1. Sollte ein Fehler erscheinen, versuchen Sie es einmal mit dem Befehl *ipconfig /registerdns* in der Befehlszeile.

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

2. Sollte der Fehler weiterhin auftreten, überprüfen Sie, ob das primäre DNS-Suffix auf dem Server mit dem Zonennamen der DNS-Zone übereinstimmt.
3. Stellen Sie als Nächstes fest, ob die IP-Adresse des Servers stimmt und der Eintrag des bevorzugten DNS-Servers in den IP-Einstellungen korrekt ist.
4. Überprüfen Sie in den Eigenschaften der Zone, ob die dynamische Aktualisierung zugelassen wird und ändern Sie gegebenenfalls die Einstellung, damit die Aktualisierung stattfinden kann. Sie können diese Einstellung ändern, indem Sie mit der rechten Maustaste auf die Zone klicken und die Eigenschaften auswählen.

Wenn sich ein Servername mit *nslookup* nicht auflösen lässt, gehen Sie auch hier am besten Schritt für Schritt vor:

1. Ist in den IP-Einstellungen des Servers der richtige DNS-Server als bevorzugt eingetragen?
2. Verwaltet der bevorzugte DNS-Server die Zone, in der Sie eine Namensauflösung durchführen möchten?
3. Wenn der Server diese Zone nicht verwaltet, ist dann auf der Registerkarte "Weiterleitungen" in den Eigenschaften des Servers ein Server eingetragen, der die Zone auflösen kann?
4. Wenn eine Weiterleitung eingetragen ist, kann der Server, zu dem weitergeleitet wird, die Zone auflösen?
5. Wenn dieser Server nicht für die Zone verantwortlich ist, leitet er dann wiederum die Anfrage weiter?

In Ausnahmefällen kann es vorkommen, dass die Aktualisierung der Reverse-Lookup-Zone nicht funktioniert hat. In diesem Fall ist der Server zwar in der Forward-Zone hinterlegt, aber nicht in der Reverse-Zone. In diesem Fall können Sie einfach den Eintrag des Servers manuell ergänzen. Dazu müssen Sie lediglich einen neuen Zeiger (Pointer) erstellen. Ein Zeiger oder Pointer ist ein Verweis von einer IP-Adresse zu einem Hostnamen. Kurz nach der Installation kann dieser Befehl durchaus noch Fehler melden. Versuchen Sie die IP-Adresse des Domänencontrollers erneut mit *ipconfig /registerdns* zu registrieren. Nach einigen Sekunden sollte der Name fehlerfrei aufgelöst werden. Sobald Sie *nslookup* aufgerufen haben, können Sie beliebig Servernamen auflösen. Wenn Sie keinen FQDN, sondern nur den Computernamen eingeben, ergänzt der lokale Rechner automatisch den Namen durch das primäre DNS-Suffix des Computers beziehungsweise durch die in den IP-Einstellungen konfigurierten DNS-Suffixe. Sie können von dem lokalen Rechner aus auch andere DNS Server mit der Auflösung befragen. Geben Sie dazu die Befehlszeile *nslookup {host}{server}*, also zum Beispiel

```
nslookup dc02.microsoft.com
  dc01.contoso.com
```

ein. Bei diesem Beispiel versucht *nslookup*, den Host dc02.microsoft.com mit Hilfe des Servers dc01.contoso.com aufzulösen.

Anstatt den zweiten Eintrag, also den DNS-Server, mit seinem FQDN anzusprechen, können Sie auch die IP-Adresse angeben. Wenn Sie als Servereintrag bei dieser Befehlszeile einen DNS-Server mit seinem FQDN eingeben, muss der verwendete DNS-Server zwar nicht den Host dc02.microsoft.com auflösen können, aber dafür den Server dc01.contoso.com. Der DNS-Server dc01.contoso.com wiederum muss dann den Host dc02.microsoft.com erfolgreich auflösen, damit keine Fehlermeldung ausgegeben wird. Sie können also mit *nslookup* sehr detailliert die Schwachstellen Ihrer DNS-Auflösung testen. Um mehrere Hosts hintereinander abzufragen, müssen Sie nicht jedes Mal den Befehl *nslookup {host}{server}* verwenden, sondern starten nslookup mit dem Befehl *nslookup –{server}*, wobei der Eintrag "server" der Name oder die IP-Adresse des DNS-Servers ist, den Sie befragen wollen – zum Beispiel *nslookup -10.0.0.11*. Beide Optionen lassen sich auch kombinieren. Wenn Sie zum Beispiel *nslookup* so starten, dass nicht der lokal konfigurierte DNS-Server zur Namensauflösung herangezogen wird, sondern der Remote-Server 10.0.0.11, können Sie innerhalb der nslookup-Befehlszeile durch Eingabe von {host} {server} wieder einen weiteren DNS-Server befragen.

Nslookup ist dabei so konfiguriert, dass das Tool den DNS-Server 10.0.0.11 zur Namensauflösung verwendet. Das Tool überprüft, ob der lokal konfigurierte DNS-Server in seiner Reverse-Lookupzone die IP-Adresse 10.0.0.11 zu einem Servernamen auflösen kann (siehe Abschnitt 1 in Bild 2). Da das funktioniert, zeigt die Ausgabe als Standardserver für diese nslookup-Befehlszeile den DNS-Server 10.0.0.11 mit seinem FQDN dc01.contoso.com an. Wäre an dieser Stelle eine Fehlermeldung erschienen, dass der Servername für 10.0.0.11 nicht bekannt ist, würde das bedeuten, dass der DNS-Server, der in den IP-Einstellungen des lokalen Rechners konfiguriert ist, in seiner Reverse-Lookupzone den Servername nicht auflösen kann. In diesem Fall sollten Sie die Konfiguration der Reverse-Lookupzone überprüfen und sicherstellen, dass alle Zeiger (Pointer) korrekt eingetragen sind. Zu einer konsistenten Namensauflösung per DNS gehört nicht nur die Auflösung von Servername zu IP (Forward), sondern auch von IP zu Servernamen (Reverse).

In der nächsten Zeile (Abschnitt 2 im Bild 2) soll der Rechnername dc02.microsoft.com vom Server 10.0.0.13 aufgelöst werden. Der Server 10.0.0.13 kann jedoch den Servernamen dc02.microsoft.com nicht auflösen. In diesem Fall liegt ein Problem auf dem Server 10.0.0.13 vor, der die Zone microsoft.com nicht auflösen kann. Sie sollten daher auf dem Server 10.0.0.13 entweder in den Eigenschaften des DNS-Servers auf der Registerkarte "Weiterleitungen" überprüfen, ob eine Weiterleitung zu microsoft.com eingetragen werden muss, oder eine sekundäre Zone für microsoft.com auf dem Server 10.0.0.13 anlegen, wenn dieser Rechnernamen für die Zone microsoft.com auflösen können soll. Als Nächstes wird versucht, den gleichen Servernamen dc02.microsoft.com über den

Standardserver dieser nslookup-Befehlszeile aufzulösen (siehe Bild-Abschnitt 3). Der Standardserver kann den Servernamen problemlos auflösen, was zeigt, dass diese Konfiguration in Ordnung ist.

Zusätzlich können Sie mit *nslookup* auch die SRV-Records des Active Directory überprüfen. Clients können im DNS nachfragen, welcher Host im Netzwerk für die einzelnen Serverdienste verantwortlich ist. Das Active Directory baut stark auf diese SRV-Records auf. Aus diesem Grund ist eine Diagnose dieser Einträge mit *nslookup* durchaus sinnvoll. Alle SRV-Records des Active Directorys befinden sich parallel in der Datei *\Windows\system32\config\netlogon.dns*. Die Datei lässt sich mit einem Editor auch anzeigen. Fehlen Einträge in den DNS-Zonen, die das Active Directory benötigt, hilft es oft, wenn Sie den Befehl *dcdiag /fix* ausführen. Dabei versucht das Tool auch fehlende Einträge aus der Datei *netlogon.dns* einzubauen. Unter Windows Server 2003 verwenden Sie dazu das Tool netdiag mit der Option "/fix". Bei Windows Server 2003 stehen dcdiag und netdiag aber erst nach der Installation der Support-Tools von der Windows Server 2003-CD zur Verfügung. Bei Windows Server 2008 ist dcdiag automatisch installiert.

IPconfig für die DNS-Diagnose verwenden

Ein weiteres wichtiges Tool ist *ipconfig.exe*, das ebenfalls zum Lieferumfang von Windows Server 2008, 2003, Windows 2000, XP sowie Windows Vista und 7 gehört. Vor allem die beiden Optionen "/registerdns" und "/flushdns" sollten jedem Administrator bekannt sein, der einen DNS-Server verwaltet. Wenn Sie eine DNS-Diagnose durchführen und Fehlerbehebungsmaßnahmen daraus ableiten, müssen Sie aufpassen, dass Ihnen der lokale DNS-Cache keinen Strich durch die Rechnung macht. Wenn Sie mit *nslookup* Namen auf dem DNS-Sever überprüfen, versucht der Client zunächst, den Namen aus seinem lokalen DNS-Cache zu lesen. Haben Sie einen eventuell vorhandenen Fehler behoben, kann dennoch der lokale DNS-Cache fehlerhafte Einträge enthalten. Löschen Sie daher immer vor der erneuten Abfrage den lokalen DNS-Cache in der Befehlszeile mit *ipconfig /flushdns*. Auch der DNS-Server verwendet einen eigenen Cache, der bei einer Fehlerdiagnose störend sein kann. Wenn ein Client in seinem DNS-Cache keinen Eintrag finden kann, gibt er die Abfrage an den DNS-Server weiter. Bevor der Server in seinen Zonen überprüft, ob er die Anfrage beantworten kann beziehungsweise die Anfrage weitergeleitet wird, sucht er in seinem eigenen Server-Cache. Sie sollten daher bei einer Fehlerbehebung diesen Cache ebenfalls löschen lassen. Sie finden diese Möglichkeit im Kontextmenü des DNS-Servers im Snap-In "DNS".

Startet ein Windows-Client, registriert er sich automatisch am DNS, wenn die lokalen Dienste "Anmeldedienst" und "DNS-Client" gestartet werden. Da Sie bei einer Fehlerbehebung nicht jedes Mal die beiden Dienste neu starten oder den ganzen Server durchbooten wollen, können Sie in der Befehlszeile mit dem Befehl *ipconfig/registerdns* eine manuelle Aktualisierung der Einträge auf dem DNS durchführen. Nach der Eingabe des Befehls sollten die Einträge recht schnell auf dem DNS aktualisiert sein. Sollte das dynamische Aktualisieren noch immer nicht funktionieren, überprüfen Sie in den Eigenschaften der Zone, ob die dynamische Aktualisierung aktiviert ist. Wenn sich an der Zone auch Arbeitsstationen und Server dynamisch registrieren sollen, die nicht Mitglied der Gesamtstruktur sind, können Sie auch die Option "Nicht sichere und sichere" aktivieren.

Bild 2: Diagnose von DNS-Problemen mit nslookup

Replikationsprobleme beheben

Jeder Domänencontroller im Active Directory hat neben seinem Host A-Namen, zum Beispiel dc01.contoso.com, noch einen zugehörigen CNAME, der das so genannte DSA (Directory System Agent)-Objekt seiner NTDS-Settings darstellt. Dieses DSA-Objekt ist als SRV-Record im DNS unterhalb der Zone der Domäne unter dem Menüpunkt "_msdcs" zu finden.

Der CNAME ist die GUID dieses DSA-Objektes. Domänencontroller versuchen ihren Replikationspartner nicht mit dem herkömmlichen Host A-Eintrag aufzulösen, sondern mit dem hinterlegten CNAME. Unter Windows 2000 Server und Windows Server 2003 ohne installiertes SP1 war die Namensauflösung im DNS für die Replikation deutlich fehleranfälliger. Versucht ein Domänencontroller mit diesen älteren Betriebssystemständen, einen Replikationspartner mit diesem CNAME über DNS aufzulösen und misslingt dies, bricht die Replikation mit einem Fehler ab. Ein Windows Server 2003-Domänencontroller mit installiertem SP1 oder Windows Server 2008-Domänencontroller versuchen nach der erfolglosen Namensauflösung des CNAME eines Domänencontrollers, einen HOST A-Eintrag zu finden. Schlägt auch das fehl, versucht der Domänencontroller den Namen mit NetBIOS aufzulösen, entweder über Broadcast oder einen WINS-Server. Jeder Domänencontroller braucht einen eindeutigen CNAME, der wiederum auf seinen Host A-Eintrag verweist. Überprüfen Sie bei Replikationsproblemen, ob

diese Einträge vorhanden sind. Sollte die Namensauflösung mit DNS noch immer nicht funktionieren, steht Ihnen noch das Tool *dnslint.exe* zur Verfügung, mit dem die SRV-Records im Active Directory überprüft werden können.

Sie können sich das Werkzeug bei Microsoft unter [1] herunterladen. Für das Tool gibt es insgesamt drei verschiedene Funktionen, die jeweils DNS überprüfen und einen entsprechenden HTML-Bericht generieren. Diese drei Funktionen sind:

- *dnslint /d* diagnostiziert mögliche Ursachen einer langsamen Delegierung.
- *dnslint /ql* überprüft benutzerdefinierte DNS-Datensätze auf mehreren DNS-Servern.
- *dnslint /ad* überprüft DNS-Datensätze, die speziell für die Active Directory-Replikation verwendet werden.

Die Syntax für das Werkzeug lautet:

```
dnslint /d {Domänenname} | /ad
  [{LDAP_IP_Adresse}] | /ql
  {Input_Datei} [/c [smtp,pop,imap]]
  [/no_open] [/r {Report_Name}] [/t]
  [/test_tcp] [/s {DNS_IP_Adresse}]
  [/v] [/y]
```

Einsatz von DNSLint

Bei der Ausführung von DNSLint müssen Sie eine der Befehlszeilenoptionen "/d", "/ad" oder "/ql" verwenden. Mit *dnslint.exe /ad* überprüfen Sie, ob Ihre Domänencontroller die DNS-Einträge im Active Directory zur Replikation abrufen können. Geben Sie zur Überprüfung den Befehl

```
dnslint /ad {IP-Adresse des ersten
  DCs} /s {IP-Adresse des zweiten
  DCs}
```

ein. Das Tool benötigt einige Sekunden und überprüft, ob im Active Directory die notwendigen _msdcs-Einträge vorhanden sind. Geben Sie an dieser Stelle nicht den DNS-Namen der beiden Server an, die Replikationsprobleme haben, sondern die IP-Adressen. Die Option "/ad" dient zur Angabe eines Domänencontrollers, der die notwenigen GUIDs im DNS auflösen können muss. Jeder Domänencontroller muss in der Lage sein die Namen dieser GUIDs per DNS aufzulösen.

Fehlende GUIDS

Testen Sie daher auf jedem Server mit DNSLint, ob die einzelnen Server Probleme bei der Auflösung dieser GUIDs haben. Treten in diesem Bereich Fehler auf, liegen die Replikationsprobleme zunächst an diesen fehlenden GUIDs. Die Option "/s" dient dazu, dem Befehl einen DNS-Server mitzuteilen, der die Zone _msdcs des Active Directory verwaltet. Der Server hinter der Option "/ad" dient daher zum Verbindungsaufbau per LDAP, während der Server hinter "/s" zum Auflösen per DNS dient. Sie müssen nicht unbedingt zwei unterschiedliche Server angeben, sondern können auch zweimal die gleiche IP-Adresse verwenden. Nachdem der Befehl abgeschlossen ist, wird Ihnen ein detaillierter HTML-Bericht angezeigt, mit dessen Hilfe Sie die Probleme der GUID-Auflösung mit DNS nachvollziehen können. Der Bericht umfasst die Auflösung der einzelnen GUIDs der Domänencontroller und die vorhandenen Fehler. Beim Starten des Befehls verbindet sich DNSLint zunächst mit dem Domänencontroller, um alle GUIDs der Gesamtstruktur abzufragen. Die Abfrage erfolgt mit LDAP. Aus diesem Grund müssen Sie vor der Ausführung sicherstellen, dass Sie den Befehl unter einem Benutzerkonto starten, das über genügend Rechte verfügt.

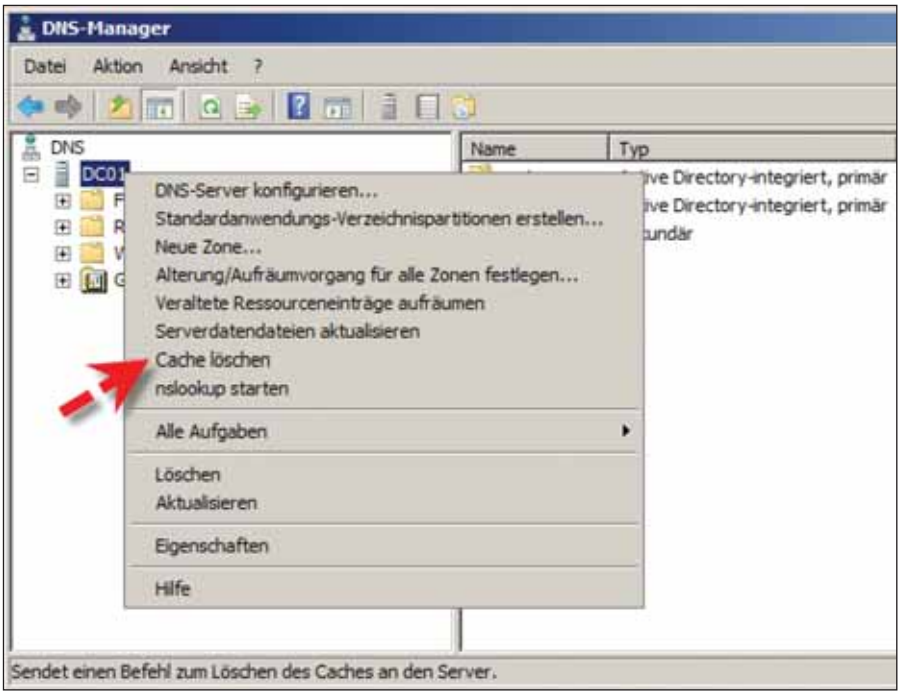


Bild 3: Löschen des DNS-Server Caches in der DNS-Verwaltung

Sobald die GUID-Liste vom LDAP-Server zurückgegeben wird, versucht DNSLint über den mit der Option "/s" konfigurierten DNS-Server, diese GUIDs zu ihrer IP-Adresse aufzulösen. Durch DNSLint erhalten Sie daher ausführlich Informationen über die korrekte DNS-Konfiguration Ihrer Gesamtstruktur. Mit der Befehlszeilenoption "/d" fordern Sie Domänennamentests an. Diese Befehlszeilenoption ist für die Behandlung von Problemen in Bezug auf eine langsame Delegierung nützlich. Sie müssen den zu testenden Domänennamen angeben. Sie können die Befehlszeilenoption "/d" nicht in Verbindung mit der Option "/ad" verwenden. Mit der Befehlszeilenoption "/ad" rufen Sie einen Active Directory-Test auf. Mit der Befehlszeilenoption "/ql" fordern Sie DNS-Abfragetests von einer Liste ab. Die Option "/ql" versendet die DNS-Abfragen, die in einer Texteingabedatei angegeben wurden. Sie müssen den Namen und

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.*

Liefertermin:
Ende März 2010

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

---

iT administrator Das Magazin für professionelle System- und Netzwerkadministration

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

☐ **Ja**, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft 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.

ITA 0310

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

E-BOOK SYSTEMS
Abos und Einzelhefte gibt es auch als E-Paper

Heinemann Verlag
Leopoldstraße 85
D-80802 München
Tel: 089-4445408-0
Fax: 089-4445408-99
Geschäftsführung:
Anne Kathrin Heinemann
Matthias Heinemann
Amtsgericht München HRB 151585

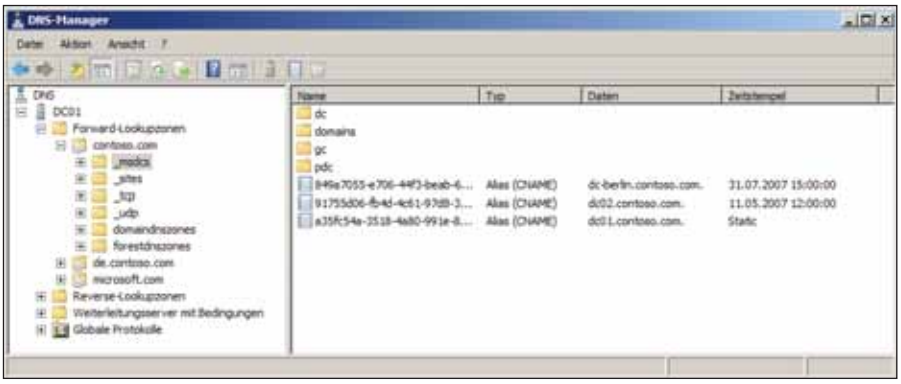


Bild 4: Anzeigen der DNS-DSA-Objekte von Domänencontrollern

den Pfad der Eingabedatei angeben. Die Option "/ql" unterstützt A-, PTR-, CNAME-, SRV- und MX-Datensatzabfragen. Sie können eine Beispieleingabedatei erstellen, indem Sie den folgenden Befehl ausführen: *dnslint /ql autocreate*. Dabei lässt sich "/ql" nicht in Verbindung mit den Optionen "/d", "/ad" oder "/c" verwenden. Mit "/c" veranlassen Sie Konnektivitätstests auf Mailservern. Die Befehlszeilenoption "/c" testet dazu SMTP-, POP- und IMAP-Ports auf den gefundenen E-Mail-Servern. Es werden standardmäßig alle drei Ports (SMTP, POP und IMAP) getestet.

Sie können nur einen Port oder eine Kombination aus mehreren Ports festlegen. Verwenden Sie hierzu eine kommagetrennte Liste, zum Beispiel "/c pop,imap,smtp". Mit der Befehlszeilenoption "/no_open" verhindern Sie, dass Berichte automatisch geöffnet werden. Die Option ist besonders in Skripten nützlich. Mit "/r" legen Sie den Namen der erzeugten Berichtsdatei fest. Dem Berichtsnamen wird automatisch die Dateinamenerweiterung *.htm angehängt, der Bericht also im HTML-Format erstellt. Der Standardname des Berichts lautet *Dnslint.htm*. Verwenden Sie "/s", um einen WHOIS-Lookup zu umgehen. Sie können hier IP-Adressen von DNS-Servern angeben, statt diese bei InterNIC abzufragen. Die Befehlszeilenoption "/s" startet die Überprüfung von DNS-Datensätzen unter Verwendung der angegebenen IP-Adresse. Es werden nur gültige IP-Adressen akzeptiert, keine Namen. Verwenden Sie diese Option beispielsweise zur Überprüfung von Domänennamen, die InterNIC nicht unterstützt. Wenn Sie "/ad" nutzen, müssen Sie auch die Option "/s" verwenden, um einen DNS-Server anzugeben, der für die _msdcs-Unterdomäne in der Stammdomäne der Active Directory-Struktur autorisierend ist. Bei "/ad" können Sie auch den Befehl */s localhost* ausführen, um festzustellen, ob das lokale System die Datensätze auflösen kann, die bei den Active Directory-Tests gefunden werden. Verwenden Sie "/t", um die Ausgabe in eine Textdatei anzufordern. Die Textdatei hat denselben Namen wie der HTML-Bericht, der Textdatei wird jedoch die Dateinamenerweiterung *.txt angehängt. Sie landet im gleichen Verzeichnis wie die HTML-Berichtsdatei.

Verwenden Sie "/test_tcp" für einen Test des TCP-Ports 53. Standardmäßig wird nämlich nur der UDP-Port 53 getestet. Diese Option kann jedoch nicht in Verbindung mit der Option "/ql" verwendet werden. Mit "/v" bewirken Sie eine ausführliche Ausgabe auf dem Bildschirm. Bei dieser Option zeigt das Tool auf dem Bildschirm an, welche Schritte es ausführt, um Daten zu sammeln. Verwenden Sie "/y", um eine vorhandene Berichtsdatei zu überschreiben, ohne dass der Benutzer den Überschreibvorgang bestätigen muss. Die Befehlszeilenoption "/d" (Domänennamentest) können Sie zum Testen eines bestimmten DNS-Domänennamens verwenden. Sie hilft bei der Diagnose möglicher Ursachen einer langsamen Delegierung sowie weiterer einschlägiger DNS-Probleme. Der Domänenname, den Sie testen, kann ein Name sein, der für die Verwendung im Internet registriert ist, oder es kann sich um einen Namen handeln, der in einem privaten Namespace verwendet wird. Wenn Sie Domänennamen in einem privaten Netzwerk oder im Internet registrierte Domänennamen mit einer Tiefe von mehr als zwei Ebenen testen, müssen Sie die Option "/s" verwenden.

Geben Sie "/c" mit an, versucht DNSLint standardmäßig, auf jedem gefundenen Mailserver Verbindungen zu allen drei Ports herzustellen – also zu TCP-Port 25 für SMTP, zu TCP-Port 110 für POP und zu TCP-Port 143 für IMAP. Das Tool zeigt für jeden Port den jeweiligen Status an: "Listening", "Not Listening" oder "No Response". Stellt DNSLint fest, dass der Port horcht, meldet es auch eine etwaige Antwort des Ports. Wenn zum Beispiel ein SMTP-Port horcht, gibt er typischerweise eine Antwort zurück, die der SMTP-Protokollspezifikation entspricht. Der Befehl *dnslint /y /v /c /d microsoft.com* erzeugt beispielsweise einen Bericht mit dem Namen *Dnslint.htm*, der einen bereits vorhandenen Bericht mit demselben Namen überschreibt, ohne dass der Benutzer das Überschreiben bestätigen muss. Da die Option "/c" angegeben wurde, wird an das Ende des DNSLint-Standardberichts ein zusätzlicher Abschnitt angehängt. Wenn ein Ziel-E-Mailserver auf einen Verbindungsversuch über einen seiner E-Mailports nicht reagiert, versucht DNSLint drei Mal, die Verbindung herzustellen.

Damit endet der erste Teil der Workshopserie zu DNS-Fehlern. In Teil zwei gehen wir auf spezifische Fehler ein und zeigen, wie Sie diese beheben können. *(dr)*

Links

[1] Download von DNSLint 2.04
http://download.microsoft.com/download/2/7/2/27252452-e530-4455-846a-dd68fc020e16/dnslint.v204.exe

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.

Tipps & Tricks ohne Gewähr

Microsoft Windows

Bei den meisten Windows-Versionen ist es ja möglich, das **während der Anmeldung gezeigte Hintergrundbild anzupassen**. Geht das auch bei Windows 7 und wenn ja, wie?

Wollen Sie das Anmeldebild von Windows 7 anpassen, müssen Sie eine Änderung in der Registry vornehmen. Öffnen Sie dazu über das Startmenü durch Eingabe von *regedit* den Registry Editor. Navigieren Sie zu "HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Authentication \ LogonUI \ Background" und setzen Sie "OEMBackground" auf den Wert "1". Ist der REG_DWORD-Wert noch nicht vorhanden ist, legen Sie ihn einfach an und setzen Sie ihn auf den Wert "1". Das von Ihnen gewünschte Hintergrundbild darf eine maximale Größe von 256 KByte haben und benötigt die Bezeichnung *backgroundDefault.jpg*. Außerdem muss die Datei im Ordner "C:\ Windows \ System32 \ oobe \ info \ backgrounds" liegen. Ist der Ordner nicht vorhanden, müssen Sie diesen anlegen. Nach dem nächsten Bootprozess startet der Anmelde-Screen dann mit dem neu ausgewählten Hintergrundbild. *(ln)*

Kürzlich habe ich auf dem von mir genutzten Rechner Windows 7 installiert. Bei Arbeiten mit dem Betriebssystem fiel mir auf, dass das System **Prozessen, die nicht mehr reagieren**, relativ lange Zeit lässt, doch noch eine Antwort zu schicken. Diese Gnadenfrist verlangsamt den Computer jedoch ziemlich. Gibt es eine Möglichkeit, diese **Wartezeiten zu verkürzen und Windows 7 damit zu beschleunigen?**

Sie haben die Möglichkeit, über entsprechende Einträge in der Registry das Verhalten von Windows bei abgestürzten Prozessen zu bestimmen. Gehen Sie dazu zum Schlüssel "HKEY_CURRENT_USER \ Control Panel \ Desktop" und erzeugen Sie durch einen Rechtsklick im rechten Bereich des Fensters den REG_SZ-Eintrag "HungAppTimeout" und geben Sie diesem den Wert "1000". Dieser Parameter bestimmt, wie lange Windows nach einem Klick auf den Button "End Task" im Task Manager noch wartet, bis es den Prozess wirklich beendet. Der Standardwert liegt hier bei 5000 (Millisekunden) – ein doch recht langer Zeitraum. Weiterhin können Sie festlegen, wie das Betriebssystem verfährt, wenn es mit einem nicht mehr antwortenden Vorgang konfrontiert ist. Normalerweise richtet Windows eine Rückfrage an den Anwender, ob es dieses oder jenes Programm beenden soll. Mit dem Eintrag "AutoEndTasks" und dem Wert "1" an gleicher Stelle wie oben legen Sie fest, dass keine Rückfrage mehr erscheint und ein hängender Prozess automatisch ins Jenseits befördert wird. Last but not least lässt sich noch das Herunterfahren des Rechners beschleunigen. Die Option "WaitToKillAppTimeout" bestimmt, wie lange es dauert, bis beim Shutdown die Aufforderung erscheint, hängende Prozesse zu terminieren. Auch hier gibt das Betriebssystem dem Vorgang mit 20 Sekunden sehr lange Zeit. Ein Wert wie "3000" sollte hier ausreichend sein. Und wenn Sie schon einmal am Beschleunigen sind: Mit dem Eintrag "MenuShowDelay" unter dem Wert "0" klappen Menüs in Zukunft deutlich flotter auf. *(ln)*

Ich habe gehört, dass Windows 7 sowie Server 2008 über ein **integriertes Tool** verfügen, das die **Energie-Einstellungen des Rechners überprüft** und in einem speziellen Report auf mögliche Probleme hinweist. Wo finde ich dieses Bordmittel und wie setze ich es ein?

In der Tat verfügen die neuesten Windows-Versionen über ein kleines Tool, das den Computer 60 Sekunden lang überwacht, dabei die Energieeffizienz des Rechners prüft und mögliche Probleme diagnostiziert. Das kleine Programm lässt sich allerdings nur über die Kommandozeile starten. Geben Sie dazu

powercfg /energy ein und drücken Sie die Eingabetaste. Nach der einminütigen Diagnose-Phase meldet das Tool die Anzahl der gefundenen Probleme und legt eine Protokoll-Datei namens *energy-report.html* im Verzeichnis "C:\windows\system32\" ab. In dieser Liste finden Sie ausführliche Informationen zu den gefundenen Schwierigkeiten und Tipps zum Verbessern der Power-Settings. Bevor Sie die Datei mit einem Browser öffnen, sollten Sie sie allerdings an einen anderen Ort kopieren. Sowohl Internet Explorer als auch Mozilla Firefox haben Schwierigkeiten damit, auf HTML-Files direkt im Windows-Systemverzeichnis zuzugreifen. *(ln)*

Linux

Ohne größere Mühe ist es mir nach der Umrüstung meines Notebooks gelungen, **Ubuntu 9.10 auf einem Flash-basierten SSD-Speicher** abzulegen. Soweit funktioniert alles sehr gut, mein System hat bei der Performance um einiges zugelegt. Nun meine ich zu wissen, dass bestimmte **Verhaltensweisen des Systems während des Plattenzugriffs** beim Einsatz einer SSD nicht mehr nötig oder sogar kontraproduktiv sind. Bisher habe ich dazu aber noch keine genaueren Informationen gefunden. Können Sie mir hier weiterhelfen?

Wie Sie richtig erkannt haben, sind Betriebssysteme ab Werk für den Einsatz von konventionellen Festplatten konfiguriert. Sollten Sie in Ihrem Rechner eine SSD verbaut haben, empfiehlt sich das Abändern einiger Werte. Dazu zählt unter Ubuntu 9.10 unter anderem das Abschalten des Dienstes "sreadahead". Dieses Tool bewirkt bei magnetischen Festplatten eine Beschleunigung des Bootvorgangs, hat bei Flash-basierten Speicherelementen aber genau den gegenteiligen Effekt. Um diese Funktion zu deaktivieren, müssen Sie zunächst die Datei */etc/init/sreadahead.conf* mit einem Texteditor Ihrer Wahl öffnen. In diesem File kommentieren Sie dann folgende Zeile aus:

```
exec /sbin/sreadahead -t 0
```

Danach sollten Sie sich daran machen, das Steuerprogramm "Elevator-Scheduler" zu deaktivieren. Dieser Scheduler ist dafür zuständig, die sequentiellen Lese- und Schreibvorgänge auf einer magnetischen Platte zu optimieren. Da Lese- und Schreibzugriffe auf einer SSD jedoch anders ablaufen, ist der Einsatz dieses Programms ebenfalls kontraproduktiv. Editieren Sie dazu die Datei */boot/grub/grub.cfg* wie folgt:

```
linux /boot/vmlinuz-2.6.31-15-gene-
  ric root=UUID=b5c7bed7-58f1-4d03-
  88f4-15db4e367fa0 ro quiet splash
  elevator=noop
```

Mit einem letzten Trick sorgen Sie für noch mehr Performance beim Zugriff auf die SSD: Durch eine Modifikation der Mount-Option des Dateisystems erreichen Sie, dass beim Lese-Zugriff auf eine Datei keine Information über diesen Zugriff ins File-System geschrieben wird. Weniger Schreibvorgänge beschleunigen das System und verlängern zudem die Lebensdauer des Flash-Speichers. Hierzu müssen Sie die Datei */etc/fstab* abändern und den Parameter "noatime" ergänzen. Die Datei sollte dann letztendlich so aussehen:

```
/dev/sda1 / ext4 noatime,
  errors=remount-ro 0 1
```

Nach diesen Änderungen starten Sie Ihren Rechner neu. Durch den beschleunigten Zugriff auf die SSD sollte sich die Performance insgesamt noch einmal deutlich verbessert haben. *(ln)*

Vor allem zum schnellen Web-Zugriff von unterwegs habe ich mir ein Netbook zugelegt und mich dabei für den Acer Aspire One mit **vorinstalliertem Linux-System** entschieden. Nun habe ich festgestellt, dass im Datei-Manager keine Funktion vorhanden ist, um **im Netzwerk auf freigegebene Ordner eines NAS zuzugreifen**. Besteht hier eine Möglichkeit, den Zugriff nachträglich zu implementieren?

Da die Menüs in der Linux-Variante des von Ihnen gekauften Netbooks recht abgespeckt sind, bietet der File-Manager von Haus aus das Öffnen von Shares nicht an. Mit etwas Handarbeit können Sie den Zugriff auf freigegebene Ordner jedoch im Nachhinein einrichten. Klicken Sie dazu in der Desktop-Ansicht zunächst auf das Icon "MyFiles" und erstellen Sie dort ein neues Verzeichnis, etwa mit dem Namen "Netzordner". Öffnen Sie nun eine Terminalsitzung, zum Beispiel mit einem Rechtsklick auf den Desktop und Anklicken der Option "Open Terminal here". Nun geben Sie folgendes Kommando ein:

```
sudo mount -t cifs //{IP-Adresse des
  Zielsystems}/{Verzeichnisname}
  Netzordner
```

Mit diesem Befehl haben Sie den vorhin erstellten Ordner mit der Netzfreigabe verknüpft. Wurde für diese Freigabe ein Nutzername und ein Passwort erteilt, müssen Sie dies beim Zugriff auf den neuen Ordner eingeben. *(ln)*

Tools

Die **Automatisierung von Prozessen** spart Administratoren viel Zeit. Gerade bei der Installation von Clients und Servern mit allen nötigen Schritten ist die Schaffung eines vollautomatisierten Prozesses sehr hilfreich. Dabei kommen die unterschiedlichsten Methoden und Mittel zum Einsatz. Eine der wichtigsten Maßnahmen ist die Härtung des Servers durch Setzen von Rechten auf Dateien, Order, Registry-Schlüssel, Drucker, Diensten und Netzwerk-Freigaben – kurz: **Die Konfiguration der Access Control Lists (ACL)**. Mit Bordmitteln lässt sich das nur sehr aufwändig

und mit einer Menge an unterschiedlichen Tools bewerkstelligen. Ein kleines Werkzeug jedoch bringt die vielen Arbeitsschritte unter einen Hut.

Das Open Source-Tool SetACL für die Befehlszeile ist ein vollwertiger Ersatz für das Windows-eigene *CACLS.EXE* und geht noch weit darüber hinaus. Nicht nur, dass es die Rechte für Dateien, Order, Registry-Schlüssel, Drucker, Dienste und Netzwerk-Freigaben setzen kann: Sie können auch ein komplettes Listing von ACLs für Ordner und deren Unterordner erstellen. SetACL ist durch die Verwendung in der Kommandozeile für Skripte und Batchfiles prädestiniert und existiert zudem als ActiveX-Control. *(sepago/ln)*

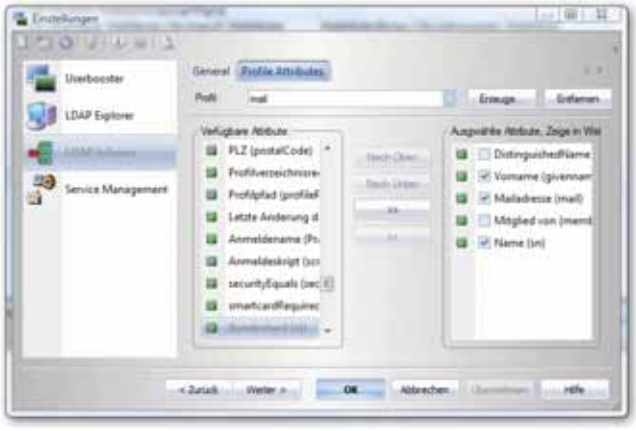
blogs.sepago.de

Eine ausführliche Beschreibung des Tools finden Sie unter http://www.helge.mynetcologne.de/setacl/

Die **Verwaltung eines Verzeichnisdienstes** wie etwa Microsofts Active Directory oder anderer LDAP-basierter Dienste ist aufgrund der oftmals vier- oder gar fünfstelligen Anzahl von Objekten im Verzeichnis an sich schon eine komplexe Aufgabe. Erschwert wird die Administration beispielsweise noch durch die Vielzahl an Verwaltungsoberflächen, die zu durchlaufen sind, wenn an einem Objekt mehrere, unterschiedliche Aktivitäten wie etwa das Erstellen von Postfachkonten, die Modifikation von Dateisystemrechten oder das Verwalten von Gruppenmitgliedschaften notwendig sind. Das Tool **Userbooster** tritt daher an, die Administration zu homogenisieren und so Zeit zu sparen und Fehler zu minimieren.

Das Programm liegt in zwei Versionen vor: Userbooster Light und Userbooster Professional. Das hier betrachtete Userbooster Light ist in einer Freeware-Version verfügbar, die jedoch nur die Verwaltung von bis zu 10 Benutzerobjekten erlaubt, was in einem ausgewachsenen Verzeichnisdienst nicht allzu weit helfen sollte. Da die Vollversion jedoch schon ab 11 Euro zu haben ist, weichen wir an dieser Stelle eine Winzigkeit von unserer Vorgabe ab, nur völlig kostenlose Werkzeuge vorzustellen. Userbooster Light liegt aktuell in der Version 4.0 vor und wurde vor allem in Sachen Benutzeroberfläche und **Statistiken** im Vergleich zu den Vorgängerversionen deutlich aufgebohrt. Neben der Verwaltung des Verzeichnisdienstes über eine einheitliche GUI erlaubt das Tool, zusätzliche **Aufgaben im Zusammenhang mit der Anlage eines Benutzerobjektes** in einem Arbeitsschritt zu realisieren. Dazu gehören die Erstellung einer Mailbox, die Erzeugung von Profil- beziehungsweise Heimlaufwerken mit den jeweiligen Rechten im Dateisystem oder die Unterstützung von DFS (Distributed File System). Die Software arbeitet darüber hinaus mit Platzhalter-Variablen, die die Verwaltung der speziellen Anforderungen in einer generischen Vorlage ermöglichen. Zusätzlich ist die Integration in MS Office ein weiteres Hilfsmittel bei der Erstellung von Template-Vorlagen. Das direkte Importieren und Exportieren in MS Excel reduziert die notwendigen Anpassungen auf das absolute Mindestmaß. *(jp)*

Quelle: www.userbooster.de



Userbooster erleichtert die Administration LDAP-basierter Verzeichnisdienste

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

Krankt ein Server an einem **Hardwaredefekt**, der so weit führt, dass das Gerät nicht mehr bootet, ist eine Diagnose oftmals schwierig. Stürzt das System etwa sporadisch ab oder bootet gelegentlich nicht, ist der **Arbeitsspeicher** neben unzureichender CPU-Kühlung der Hauptverdächtige. Im ersten Fall hat der Systemverantwortliche zum einen die Möglichkeit, durch Ausbau und Ersatz die Speicherriegel nacheinander durchzutesten oder den Speicher mit **Memtest86+** auf Herz und Nieren zu testen.

Das kostenlose Programm überprüft den Arbeitsspeicher des Computers. Um Memtest86+ zu nutzen, lässt es sich entweder als ISO-Datei auf eine CD-Rom brennen oder auf einen USB-Stick kopieren. Vom jeweiligen Medium bootet der Administrator dann den schadhaften Rechner. Daraufhin startet Memtest86+ sofort den **Test des kompletten Arbeitsspeichers**, indem es Daten in das RAM schreibt und diese Informationen anschließend wieder ausliest. Stimmen geschriebene und gelesene Daten nicht überein, liegt wahrscheinlich ein Hardwaredefekt vor. Da kein Betriebssystem geladen ist, analysiert die Software im Gegensatz zu Konkurrenzprogrammen nahezu den kompletten Speicher und erlaubt so eine differenzierte Diagnose. Der einzige Nachteil dabei ist die lange Laufzeit des Tests, für den mindestens einige Stunden eingeplant werden müssen. *(jp)*

Quelle: www.memtest.org

Switches für das Rechenzentrum

Kompakt, schnell und virtuell

von Olaf Hagemann

Ein altes Maklersprichwort besagt, dass bei der Wahl der richtigen Immobilien ganz genau drei Eigenschaften entscheidend sind: die Lage, die Lage und – die Lage. Ganz so einfach ist es bei der Beschaffung von Switches für ein Rechenzentrum nicht. Denn je nach Einsatzbereich gilt es, verschiedene Faktoren zu berücksichtigen. In diesem Beitrag untersuchen wir, warum bei der Auswahl der richtigen Netzwerkkomponenten vor allem die Geschwindigkeit, die Port-Dichte, die Energieeffizienz und die Unterstützung von virtuellen Umgebungen so wichtig sind.

Bild 1: Mit leistungsstarken Switches und Modulen mit hoher Port-Dichte lassen sich heute bis zu 582 10-GBit-Ethernet-Ports in einem Netzwerkschrank unterbringen

Klassische Unternehmensnetzwerke bestehen ab einer bestimmten Größe aus zwei oder drei Schichten. Am Netzwerkrand – auch Edge genannt – stehen typischerweise Switches, die etwa die Arbeitsplatzrechner einer Abteilung mit dem Firmen-LAN verbinden. Mehrere Edge-Switches sind in großen Gebäuden oft sternförmig an einen Aggregation-Switch pro Stockwerk angeschlossen. Aggregation-Switches verschiedener Etagen stellen wiederum eine Verbindung zu einem oder mehreren Core-Switch(es) in einem zentralen Rechenzentrum her. In diesem Beispiel spricht man daher von einem 3-Tier-Netzwerk. Da moderne Switches über hohe Switching-Kapazitäten und eine hohe Port-Dichte verfügen, verzichten Unternehmen heute wenn möglich auf die Aggregationsebene und binden ihre Edge-Switches direkt an den Netzwerk-Core an. Auf diese Weise wird aus einem 3-Tier-Netz wieder ein 2-Tier-Netzwerk. Voraussetzung dafür ist neben der Port-Dichte im Core vor allem, dass die Verkabelungs-Situation vor Ort diese Reduktion zulässt.

Ähnlich sieht es im Rechenzentrum von Unternehmen aus. Die erste Ebene (Tier 1) bilden auch hier die Core-Switches. Zur Anbindung von Servern kommen dann entweder so genannte Top-of-Rack-(ToR)- oder End-of-Row-(EoR)-Switches zum Einsatz. ToR- und EoR-Switches sind wiederum entweder direkt mit dem Core (2-Tier-Architektur) oder über Aggregation-Switches (3-Tier-Architektur) angeschlossen. Doch im Gegensatz zum Unternehmensnetz ist im Rechenzentrum oft noch nicht Schluss. So kommen beispielsweise in Blade-Centern eigene Switches zum Einsatz, die ihre Serverblades über Uplinks mit einem ToR- oder EoR-Switch verbinden. Laufen auf einem Blade-Server mehrere virtuelle Server, arbeitet innerhalb des Hypervisors des Blade-Servers noch ein virtueller Switch. Dieser ermöglicht den verschiedenen virtuellen Maschinen (VMs) die Kommunikation untereinander und stellt eine Verbindung mit der physikalischen Netzwerkkarte im Blade-Server her. Im Extremfall findet sich in einem Datacenter daher eine 5-Tier-Architektur (siehe Bild 2). Je nach betrachteter Ebene ergeben sich verschiedene Kriterien, die bei der Auswahl entsprechender Geräte Berücksichtigung finden sollten.

10-GBit-Ethernet ist bald Pflicht

Angelehnt an Gordon Moores Gesetz verdoppeln sich Datenvolumen und Netzwerkbandbreite in Rechenzentren alle 18 Monate, während sich die Zahl der an das Netzwerk angeschlossenen Geräte alle zweieinhalb Jahre verdoppelt. Server in Rechenzentren sind heute meist per GBit-Ethernet mit einem ToR- oder EoR-Switch verbunden. Entsprechende Netzwerkschnittstellen finden sich normalerweise bereits auf dem Motherboard der Server. Während 1 GBit/s für Single-Core-Server absolut ausreichend war, um deren Daten über das Netzwerk zu transportieren, entwickelt sich GBit-Ethernet für moderne leistungsstarke Server mit Mehrkernprozessoren zunehmend zum Flaschenhals. Um der steigenden I/O-Leistung von modernen Servern und Anwendungen gerecht zu werden, empfiehlt sich daher in entsprechend leistungsstarken Geräten der Einsatz von 10-GBit-Ethernet-Adaptern. Mit Verabschiedung des IEEE-Standards 802.3an im Jahr 2006 ist eine Übertragung von 10 GBit/s auch via Kup-

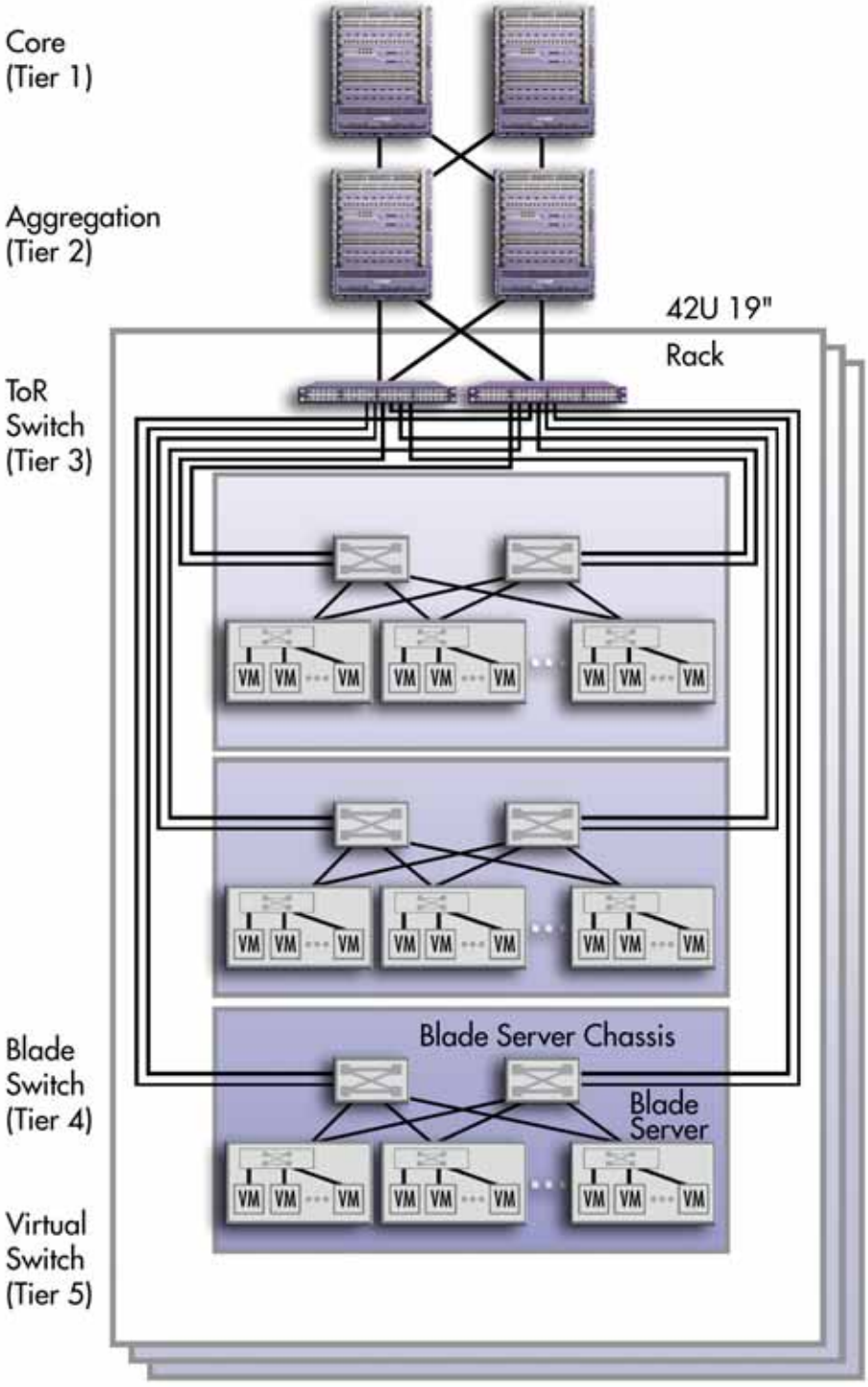


Bild 2: In einem Rechenzentrum gibt es bis zu fünf Netzwerkebenen (Quelle: Extreme Networks)

ferkabel über 100 Meter möglich, was zusammen mit den extrem gesunkenen Kosten pro Port dem Standard weiteren Aufwind verleiht. 10GBase-T funktioniert über bestehende Cat-5e-Kabel immerhin über Distanzen von bis zu 45 Metern, was selbst für die Anbindung leistungsstarker Server an EoR-Switches ausreicht.

Ein weiteres treibendes Moment für den Einsatz von 10GbE im Rechenzentrum ist die Virtualisierung von Servern. Laut neuester Studien greifen in Unternehmen bereits zwischen fünf und zehn virtuelle Maschinen auf eine physische Netzwerkkarte eines Servers zu. Mittelfristig schätzen die Analysten, dass bis zu 30 VMs in einem Server möglich sind. Auch hier hilft dann nur mehr Geschwindigkeit auf der Netzwerkstrecke zwischen physikalischem Server und Switch, damit nicht die Netzanbindung selbst zum Flaschenhals wird. Für Unternehmen sowie Betreiber von Datacentern bedeutet dies, dass 10-GBit-Ethernet nicht nur im Core, sondern zudem an der Aggregation-Ebene und am Edge Einzug halten wird und das Netzwerk entsprechend darauf vorbereitet sein sollte. Bei der Auswahl von zukunftsfähigen Switches ist dabei sowohl auf eine ausreichende Port-Zahl in hoher Geschwindigkeit als auch auf eine entsprechend hohe Switching-Kapazität der Switching-Fabric zu achten. Bei aktuellen Management-Switch-Modulen sind Übertragungsraten von 100 GBit/s pro Slot eines modularen Datacenter-Switches kein Problem.

Hohe Port-Dichte auf allen Ebenen

In einem Rechenzentrum einen Server gegen ein leistungsfähigeres Modell gleicher Größe auszutauschen, ist relativ einfach. Schwieriger wird es, wenn der Bedarf an Stellplatz, Energieversorgung oder Kühlung die Parameter überschreitet, die beim ursprünglichen Design des Rechenzentrums zu Grunde gelegt wurden. Daher strebt jeder Betreiber danach, möglichst viel Leistung auf möglichst wenig Platz unterzubringen. Dies fängt bereits im Serverschrank bei den ToR-Switches an. Jede Höheneinheit, die ein Switch einnimmt, fehlt den darunter liegenden Servern und mindert so die maximale Rechenleistung eines Racks. Ein guter ToR-Switch sollte daher in der Lage sein, 24 10-GBit-Ethernet-Ports auf einer Höheneinheit unterzubringen.

Ebenso spielt im Core eine hohe Port-Dichte eine große Rolle. Denn einerseits bedeuten weniger Switches weniger Investitionen bei der Anschaffung. Zudem sinken durch weniger Geräte die Betriebskosten, vor allem durch den reduzierten Energieverbrauch. Wer beispielsweise eine 3-Tier-Architektur im Unter-

nehmensnetz auf eine 2-Tier-Architektur reduzieren möchte, der benötigt automatisch auf seinen Core-Switches mindestens einen, in der Praxis aber aus Redundanzgründen meist zwei Ports pro Edge-Switch. Stehen dann am Edge den Endgeräten 1-GbE-Ports zur Verfügung und erfolgt der Uplink mit 10 GBit/s, müssen die in der Regel modular aufgebauten Core-Switches über entsprechend viele 10-GbE-Module mit hoher Port-Dichte verfügen. Mit leistungsfähigen Switches ist es heute bereits möglich, in nur einem Netzwerkschrank 582 10-GbE-Ports zur Verfügung zu stellen. Wer mittelfristig den Austausch seiner Core-Switches plant, sollte diesen Wert auf alle Fälle im Hinterkopf behalten.

Doch nicht nur im Core, auch am Edge oder auf der Aggregationsebene bedeutet eine hohe Port-Dichte immer weniger Geräte, weniger Energieverbrauch und weniger Aufwand bei der Administration. Kommen hier nicht-modulare Switches zum Einsatz, sollten diese auf alle Fälle über eine leistungsfähige Stacking-Möglichkeit verfügen. Während einige Hersteller hier beispielsweise nur Verbindungen von Edge-Switches untereinander über einen GbE-Port auf der Vorderseite des Geräts zur Verfügung stellen, können andere Switches über ein entsprechendes Stacking-Modul auf der Rückseite bis zu acht Switches mit 256 GBit/s ringförmig miteinander verbinden. Der Administrationskonsole präsentiert sich der Stack trotzdem wie ein physischer Switch.

Gleiches gilt für die Reduzierung der Netzwerkebenen im Datacenter selbst. Wer beispielsweise die Blade-Server eines Blade-Centers nicht über den Blade-Center-Switch, sondern direkt an den Core anschließt und so das Blade-Tier und gegebenenfalls einen Aggregation-Switch eliminiert, steigert im Core zwar deutlich den Bedarf an Hochgeschwindigkeits-Ports. Doch als Lohn winkt weniger Komplexität im Netz, weniger Latenz und – was nicht zu unterschätzen ist – eine klare Trennung der Verantwortlichkeiten zwischen Server- und Netzwerkadministratoren, zumindest was die Verwaltung des eliminierten Blade-Switches betrifft.

VEPA für mehr Übersicht bei der Virtualisierung

Die organisatorische Trennung der Verantwortlichkeiten von Server- und Netzwerkadministratoren ist auch im Bereich der Servervirtualisierung eine Herausforderung. Denn um virtuelle Maschinen miteinander kommunizieren zu lassen, stellen Hypervisoren wie bereits erwähnt einen virtuellen Switch in ihrer Software bereit. Auf diesen virtuellen Switches müssen Funktionen wie VLANs, Access Control Lists (ACL) oder Quality of Service (QoS) zur Verfügung stehen, die auch die realen Switch-Kollegen bereitstellen. Da die Administration von Hypervisoren normalerweise der Server-Gruppe obliegt, der Rest des Netzwerks aber von der Netzwerkabteilung verwaltet wird, sind Reibereien oft an der Tagesordnung. Denn jede Fehlersuche oder Umkonfiguration des Netzwerks erfordert einerseits die Abstimmung zwischen den beiden Abteilungen. Andererseits kommen unterschiedliche Tools bei der Administration von physikalischen und virtuellen Switches zum Einsatz, was die Bedienung nicht gerade einfacher macht. Schließlich stellen verschiedene Hersteller von Virtualisierungslösungen unterschiedliche Funktionen in ihren virtuellen Switches zur Verfügung.

Ein zukunftsträchtiger Ansatz zur Lösung dieses Problems ist, die Aufgaben der virtuellen Switches wieder auf die physikalischen Switches zu übertragen. Statt einem virtuellen Switch erhält ein Hypervisor dazu einen so genannten Virtual Ethernet Port Aggregator (VEPA), der den Datenverkehr aller virtuellen Maschinen entgegennimmt und einfach an einen externen Switch zur Verarbeitung weiterleitet. VEPA befindet sich noch im Standardisierungsprozess des IEEE. Wer in naher Zukunft den Kauf eines Datacenter-Switches zum Anschluss von Servern plant, sollte darauf achten, dass dessen Hardware VEPA bereits unterstützt und sich die entsprechenden Funktionen nach Ratifizierung des Standards per Firmware-Update nachrüsten lassen.

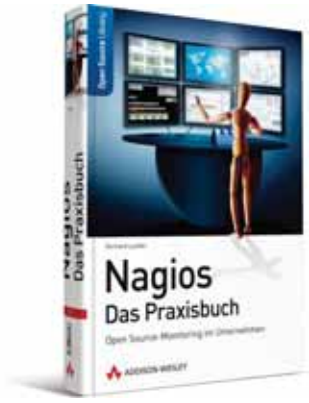
Doch bis VEPA bereit für die Praxis ist, haben Netzwerkadministratoren noch mit weiteren Herausforderungen beim Einsatz virtueller Server zu kämpfen. Ein Beispiel ist die Konfiguration von ACLs, VLANs oder QoS-Parametern an einem Switch-Port. Kommt dabei zur Identifikation eines Servers dessen MAC-Adresse zum Einsatz, kann ein Umzug einer virtuellen Maschine auf einen anderen physikalischen Server große Probleme bereiten, wenn dessen physikalischer Switch-Port nicht entsprechend provisioniert ist. Zum Glück gibt es für diese Herausforderung bereits heute konkrete Lösungen. Dabei kommuniziert ein Hypervisor beispielsweise über eine XML-Schnittstelle mit einem physikalischen Switch und informiert diesen über den bevorstehenden Umzug einer virtuellen Maschine auf einen anderen Server. Auf diese Weise ist dann der Switch in der Lage, automatisch entsprechende Einstellungen für Sicherheit und Quality-of-Service an den betroffenen Ports vorzunehmen. Voraussetzung hierfür ist ein Switch-Betriebssystem, das über entsprechende Schnittstellen verfügt.

Fazit

Ein zukunftsfähiges Netzwerk im Datacenter stellt Servern wie Anwendern hohe Bandbreiten bei hoher Port-Dichte und Verfügbarkeit bei geringem Energieverbrauch zur Verfügung und ist gleichzeitig in der Lage, die Besonderheiten virtueller Umgebungen zu berücksichtigen. Da vielen Unternehmen die Evaluation entsprechender Produkte selbst nicht möglich ist, sind Referenzinstallationen ein guter Weg, um sich über die Eignung von Datacenter-Switches für einen bestimmten Einsatzzweck zu informieren. *(ln)*

Olaf Hagemann ist Presales Manager DACH bei Extreme Networks.

Nagios – Das Praxisbuch



Nagios ist in vielen Unternehmen eine echte Alternative zu kommerziellen Monitoringlösungen geworden. Das Open Source-Framework lässt sich an so gut wie jede Situation anpassen und wird durch zahlreiche Plug-Ins und Zusatzmodule erweitert. Die vielfältigen Optionen in den Griff zu bekommen, ist keine leichte Aufgabe. Gerhard Laußers Nagios Praxisbuch setzt genau hier an. Der Autor ist kein Unbekannter und hat selbst mehrere wichtige Plug-Ins für Nagios programmiert. Sein Buch ist weniger Buch als vielmehr ein Workshop. Selbst im ersten Kapitel, in dem die Installation beschrieben wird, ist der Theorieanteil im Text minimal. Am besten haben die Leser während der gesamten Lektüre ein Nagios-System vor sich, um die Beispiele gleich nachzuvollziehen. Einziges Manko: Das geht nur mit guten bis sehr guten Programmierkenntnissen, am besten in Perl. Trotz des hohen technischen Detaillevels sind die Texte angenehm zu lesen, Kapitel werden mit kleinen, imaginären Geschichten aus einer Beispielfirma eingeleitet.

Die Kapitel sind streng an konkrete Überwachungsaufgaben angelehnt. Dies beginnt bei Netzwerkdruckern und endet mit SAP. Dazwischen zeigt der Autor, wie eigene Plug-Ins programmiert, dokumentiert und für die Community freigegeben werden – ein wichtiger Punkt für Laußer. An den Kapiteln gibt es nichts auszusetzen. Sie sind umfassend und extrem praxisorientiert, Quellen werden vollständig angegeben, Alternativen, wo vorhanden, genannt. Trotzdem gilt wie gesagt: Programmierkenntnisse sind unbedingt erforderlich. Dass darüber hinaus noch die üblichen Admin-Fähigkeiten vorhanden sein müssen, sowohl unter Windows als auch Linux-Betriebssystemen, ist ohnehin klar.

Fazit: Das perfekte Buch für Nagios-Kenner, die klare und sehr professionelle Anweisungen für den Praxiseinsatz von Nagios suchen. Wer programmieren kann, braucht kein anderes Nagios-Buch mehr, alle anderen müssen zunächst intensiv mit Perl Bekanntschaft schließen. *Elmar Török*

Autor:	Gerhard Laußer
Verlag:	Addison-Wesley
Preis:	39,95 Euro
ISBN:	978-3-8273-2800-7
Bewertung:	★★★½☆

Hyper-V

Microsofts Virtualisierungsplattform Hyper-V hat bei ihrer Einführung hohe Wellen geschlagen, einige Marktbeobachter sahen schon das Ende von VMware und Xen. Mittlerweile koexistieren die Virtualisierungslösungen weitgehend friedlich. Hyper-V ist ein recht zugängliches Produkt, die meisten Admins kommen mit der Lösung ohne Zusatzkenntnisse klar, zumindest bei den ersten Tests. Wer das Produkt im produktiven Betrieb nutzen will, hat eher den Anspruch, alles richtig zu machen und Best-Practices zu folgen, wo es diese schon gibt. Für diese Zielgruppe eignet sich "Hyper-V" von Dirk Larisch optimal. Es gibt ein eigenes Best Practice-Kapitel am Ende des Buchs mit fast 100 Seiten, in denen häufig vorkommende Probleme und Fragestellungen konkret gelöst werden. Dieser Abschnitt ist auch für sehr kenntnisreiche Admins empfehlenswert.

Am Anfang war die Historie und davon weicht auch Dirk Larisch nicht ab. Immerhin 40 Seiten lang geht es um Virtualisierungsarten, die Vorgängerprodukte von Microsoft und Allgemeines zur Technologie. Dann startet der Autor endlich mit der Installation von Hyper-V, erfreulicherweise geht er sowohl auf die Rolle als auch auf die Variante Core und deren Unterschiede ein. Bei den Gastsystemen beschränkt sich das Buch leider auf Windows, Linux oder Unix kommt noch nicht mal in einer Fußnote vor. Genauso Microsoft-zentrisch zeigt sich das nächste Kapitel mit den Migrationen. Beschrieben wird nur die Übernahme von virtuellen Maschinen von Virtual PC und Virtual Server, kein Wort zu VMware oder Xen. Das ist schade, viele Anwender hätten sicherlich gerne mehr darüber erfahren, ob und wie man eine VM des VirtualPlayers in Hyper-V integrieren kann.

Weiter geht es mit der ausführlichen Beschreibung von Festplatten- und Netzwerksystem. Sinnvolle Diagramme und Screenshots lockern den Text immer wieder auf. Das hilft auch Anfängern beim Verständnis. Ein weiteres umfangreiches Kapitel trägt den etwas missverständlichen Namen "Optimierung und Tuning". Leistungssteigerung kommt zwar darin vor, Larisch gibt aber viel mehr Tipps und Anleitungen zu typischen Anwendungsfällen. So beschreibt er den Einsatz von Exchange in einem Gastsystem und das Klonen von VMs, und was dabei hinsichtlich MAC, IP-Adresse, SID et cetera zu beachten ist. Am Ende werden die Managementwerkzeuge im Schnelldurchlauf abgehandelt.

Fazit: Wer die wichtigsten Infos zu Hyper-V sucht, ist hier richtig. Die Beschreibungen sind umfassend und gut verständlich. Sehr schade ist, dass der Autor seinen Blickwinkel komplett auf Microsoft fokussiert. *Elmar Török*

Autoren:	Dirk Larisch
Verlag:	Hanser
Preis:	25,90 Euro
ISBN:	978-3-446-41687-1
Bewertung:	★★★½☆

www.techsupportalert.com

Freeware-Wiki

Hin und wieder ist wohl jede IT-Abteilung mit einem Problem konfrontiert, das eben mal schnell beseitigt werden muss, für das aber aktuell kein Tool zur Hand ist. Dann schweift der suchende Blick des Administrators auch schon einmal ins Internet auf der Suche nach einem geeigneten Freeware-Werkzeug. Dort findet sich eigentlich zu jedem Problem eine Lösung. Sucht der Sysadmin etwa nach einer Software, um ein versehentlich gelöschtes File wiederherzustellen, so finden sich in Suchmaschinen etwa eine Million Treffer. Die Frage lautet nunmehr, welches das wirklich geeignete Tool ist.

Hier kommt unser Webtipp des Monats ins Spiel: unter techsupportalert.com finden Administratoren das "Wikipedia der Freeware" – so lautet jedenfalls die Beschreibung des Betreibers Ian Richards. Ursprünglich als Newsletter für Supportmitarbeiter gestartet, fokussiert sich die Website seit nunmehr knapp zwei Jahren auf die Katalogisierung und Bewertung von kostenloser Software. Ein äußerst sinnvoller Service vor dem Hintergrund des oben angesprochenen "Such-Problems".

Als Basis dazu teilt die Website die Tools zunächst in Kategorien wie "Disk & File Tools", "Networking" oder "System Tools" ein. Klickt der Besucher einen dieser Bereiche an, gelangt er zu einer Übersicht verschiedener Werkzeugtypen, die sich dahinter verbergen.

Nach einer erneuten Auswahl landet der Suchende dann an dem Punkt, der wirklich den Unterschied zu herkömmlichen Downloadsites ausmacht: einer kommentierten Auswahl der besten kostenlosen Werkzeuge eines bestimmten Genres. Hier schildern die Autoren in der Regel zuerst Sinn und Zweck der Tools – oft mit erfrischender Ehrlichkeit, so etwa bei RAM-Optimierungstools. Viele Programme, die zu diesem Zweck ins Internet gestellt werden, halten die Autoren schlicht für nutzlos. Dem folgt eine kommentierte Auswahl der besten Werkzeuge, so dass der Administrator einen sehr guten Eindruck davon erhält, welches Tool ihm am meisten nutzt.

Neben diesem umfangreichen Softwarekatalog finden sich auch zahlreiche How-to-Anleitungen in Schrift und Video sowie ein Forum zum Support in Sachen Freeware. Zwar finden sich auf der Site auch zahlreiche Tools, die sich eher an den Heimanwender richten, aber die Mühe und Arbeit, die Richards und seine mittlerweile 60 Autoren in die Beschreibung der Tools gesteckt haben, macht sich auch für den IT-Profi bezahlt. *(jp)*

Ian "Gizmo" Richards und sein Team kennen fast jedes freie Tool

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: Zentrales Smartphone-Management bei der simyo

Die mobilen Mitarbeiter des Mobilfunk-Discounters simyo sind mit Smartphones ausgestattet. Das Ziel: Die schnelle Bearbeitung von Informationen auch unterwegs. Damit die Geräte reibungslos funktionieren, ist die im Hintergrund installierte Technik von großer Bedeutung. In der simyo-Zentrale kommt daher eine Client-Management-Software für mobile Geräte zum Einsatz. Lesen Sie in unserem Anwenderbericht, wie die Administratoren die Smartphones mittels Push-Technik konfigurieren und so viel Zeit sparen.

www.it-administrator.de/themen/netzwerkmanagement/fachartikel/74904.html

Die Wahl des richtigen iSCSI-Initiators

Das iSCSI-Protokoll verspricht Unternehmen einige Vorteile. Bei der Planung eines iSCSI-Netzwerks stehen Administratoren jedoch vor der Frage, ob ein Hardware- oder Software-basierter Initiator zum Einsatz kommen soll. Je nach Art und Größe der transferierten Daten lässt sich diese Frage unterschiedlich beantworten. Unser Online-Beitrag zeigt, dass es nicht immer ein Host Bus Adapter sein muss und Software-basierte Lösungen für viele Einsatzgebiete ausreichend Datendurchsatz bieten.

www.it-administrator.de/themen/storage/fachartikel/74905.html

Anwenderbericht: Das Handy als digitaler Schlüsselbund

Um sich für eine Sicherheitszone im Rechenzentrum zu autorisieren, sind heute meist Chipkarte oder Transponder im Einsatz. Die BlueID-Technologie macht Bluetooth-fähige Mobiltelefone zum digitalen Schlüsselbund. Das System öffnet Eingangstüren und erfasst die Zutritts-Zeiten per Tastendruck – sicher verschlüsselt mit 512 bis 4.096 Bit. Unser Anwenderbericht verrät Ihnen, wie die noris network AG mittels BlueID in ihren Rechenzentren individuell und flexibel Zugangsrechte erteilt, ändert und sperrt.

www.it-administrator.de/themen/sicherheit/fachartikel/74906.html

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

»Die IT-Begeisterung der Schüler ist sehr motivierend«

Die Staatliche Wirtschaftsschule Freising ist für viele Schüler ein Sprungbrett zu einer weiterführenden Ausbildung, beispielsweise an einer Fachoberschule oder in einem Büroberuf. Der praxisorientierte Unterricht orientiert sich stark an wirtschaftswissenschaftlichen Fächern. So arbeiten die Schüler in einer fiktiven Firma, deren Grundlage ein gut ausgerüstetes IT-Netzwerk ist. Mathematiklehrer Johann Müller sorgt in einem Team als Systemadministrator für das IT-Netzwerk der Schule.

Welche Ausbildung haben Sie gemacht?

Nach meiner Ausbildung zum Bankkaufmann absolvierte ich ein Studium der Wirtschaftspädagogik mit einem Abschluss als Diplom-Handelslehrer für wirtschaftswissenschaftliche Fächer und Mathematik. Analog zu diesem Studium machte ich einige Scheine am Informatik Lehrstuhl der Uni München.

Warum sind Sie IT-Administrator geworden?

Während des Studiums habe ich dann als Tutor im PC-Labor der Fakultät für Betriebswirtschaft an der Uni München gearbeitet und mich in die Thematik vertieft. Systemadministrator für das Schulnetzwerk zu werden, war dann der logische Schritt.

Welche IT-Umgebung betreuen Sie aktuell?

Zu meinem Aufgabengebiet gehören neben meiner Tätigkeit als Lehrer die Instandhaltung, Neuanschaffungen, die Pflege des IT-Netzwerks, die Betreuung der Schul-Homepage, Schulverwaltung, Notenmanager und einiges mehr. Zusammen mit einem Kollegen betreue ich derzeit zwei Windows- und zwei Linux-Server, die als Proxy für den Internet-Zugang dienen, sowie rund 200 Arbeitsplatzrechner. Die IT-Landschaft wird von etwa 750 Schülern und 50 Kollegen täglich genutzt. Wenn das Netz nicht läuft, wird der Unterricht behindert.

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

Als Systemadministratoren müssen wir im Team sicherstellen, dass jeglicher Unterricht am PC ohne große Schwierigkeiten jeden Tag stattfinden kann.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Wir arbeiten gerade am Einsatz unserer e-learning-Plattform Moodle. Die Installation, Pflege und Fortbildung für diese

Geburtstag: 11.10.1973
Familienstand: verheiratet, ein Kind (bald zwei)
Hobbys: Familie und Fußball

Johann Müller, IT-Administrator

Plattform beansprucht momentan das Gros meiner Arbeitszeit.

Was macht Ihnen an Ihrem Job am meisten Spaß?

Mir gefällt es, anderen Leuten bei Problemen am PC zu helfen und Schwierigkeiten aus dem Weg zu räumen. Es macht zudem Spaß zu sehen, mit welcher Begeisterung Schüler am PC arbeiten, dafür lohnt sich jeder Aufwand.

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

Der hohe Verwaltungsaufwand, beispielsweise bei der Beschaffung neuer Hardware, ist ein Wermutstropfen, aber Teil meiner Aufgabe.

Was tun sie für Ihre Fort- und Weiterbildung?

Es gibt speziell für Lehrer Fortbildungsangebote im IT-Bereich. Diese Maßnahmen werden von Lehrern für Lehrer durchgeführt und sind daher sehr praxisnah und berufsorientiert. Weitere Informationsquellen sind Fachzeitschriften und natürlich das Internet.

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

Ich habe sicherlich schon viele Fehler gemacht, aber glücklicherweise noch keinen, der wirklich spektakulär war. Wichtig dabei ist aber, dass sich die Fehler nicht wiederholen und man daraus lernt.

Was war Ihr größter Erfolg als IT-Administrator?

Das war eindeutig die relativ problemlose Umstellung von einem Novell-Server auf Windows Server. Am Ende eines Schuljahres ist es auch immer wieder schön, wenn die Abschlussprüfungen auf dem PC problemlos stattfinden können.

Was war der dümmste Anwender oder Anwenderfehler, der Ihnen untergekommen ist?

Während des Studiums kam ein Student und meinte, der Rechner könne seine CD nicht lesen. Als im CD-Laufwerk keine CD lag, kamen wir drauf, dass er sie zwischen die Verblendung geschoben haben musste. Nachdem wir den Rechner aufgeschraubt hatten, tauchte die CD wieder auf.

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

Das sind sicher die Themen Sicherheit und Virtualisierung. Wünschenswert wären in meinen Augen mehr effektive Innovationen auf dem Bildungssektor. Da herrscht ein enormer Nachholbedarf.

Das Interview führte Petra Adamik

Möchten Sie sich künftig mit Ihren IT-Kollegen und den Heftmachern austauschen? Dann melden Sie sich einfach in unserer neuen Gruppe in Xing an unter *www.xing.com/net/itanet*. Wir freuen uns auf Sie!

Werden Sie Mitglied in unserer Xing-Gruppe

Die Ausgabe 4/10 erscheint am 5. April 2010

Schwerpunktthema:

Desktop-Virtualisierung

Im Test: XenDesktop 4 und VMware View 4

Workshop: Desktop-Virtualisierung mit Windows Server 2008 R2

Workshop: Hyper-V-Manager auf Windows 7 installieren

Workshop: Desktop-Wartung mit Citrix Provisioning Server

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

Unsere Ausgabe im **Mai** steht unter dem Schwerpunkt **Remote-Accesss, VPN und Gateway-Schutz**. In unserer Test-Rubrik nehmen wir darin die VPN-Software HOB RD VPN sowie eine UTM-Appliance von Cyberoam unter die Lupe. In einem unserer Workshops lesen Sie außerdem, wie Sie das Microsoft VPN-Protokoll SSTP nutzen.

Als Schwerpunkt im **Juni** folgt dann das Thema **Server-based Computing**.

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, Klaus Bierschenk, Olaf Hagemann, Mathias Hein, Dieter Henze, Jürgen Heyer, Thomas Joos, Sandro Luciforo, Nico Lüdemann, Dr. Holger Reibold, Elmar Török

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

Erscheinungsweise
monatlich

Bezugspreise
Einzelheftpreis: € 12,60
Jahresabonnement Inland: € 135,-
Studentenabonnement Inland: € 67,50
Jahresabonnement Ausland: € 150,-
Studentenabonnement Ausland: € 75,-
Jahresabonnement Inland mit Jahres-CD: € 144,84
Studentenabonnement Inland mit Jahres-CD: € 77,34
Jahresabonnement Ausland mit Jahres-CD: € 159,84
Studentenabonnement Ausland mit Jahres-CD: € 84,84
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.

Internet
www.it-administrator.de

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

So erreichen Sie den Leserservice
Leserservice IT-Administrator
Stephan Orgel
65341 Eltville
Tel.: 06123/9238-251
Fax: 06123/9238-252
E-Mail: leserservice@it-administrator.de

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

So erreichen Sie die Redaktion
Redaktion IT-Administrator
Heinemann Verlag GmbH
Leopoldstr. 85
80802 München
Tel.: 089/4445408-10
Fax: 089/4445408-99
E-Mail: redaktion@it-administrator.de

So erreichen Sie die Anzeigenabteilung
Anzeigenverkauf IT-Administrator
Anne Kathrin Heinemann
Heinemann Verlag GmbH
Leopoldstr. 85
80802 München

Tel.: 089/4445408-20
Fax: 089/4445408-99
E-Mail: kathrin@it-administrator.de

INSERENTENVERZEICHNIS

Die Ausgabe enthält eine Umschlagflappe der Firma Aagon und eine Teilbeilage der Firma proSoft.

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/

Oder Sie sind Neukunde? Hier können Sie bestellen:

www.it-administrator.de/abonnements/jahresabo/

www.it-administrator.de

Heinemann Verlag
Im Dialog mit Spezialisten.

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 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

Ihr Clientmanagement

kostenfrei testen

Download oder DVD => www.aagon.de

CeBIT 2. - 6. März 2010 Halle 3, Stand H09

A|C|M|P efficient networks

sales@aagon.com