IT-ADMINISTRATOR.DE

11/2009

€ 12,60 ISSN 1614-2888

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

IT-Desaster-Management – Backup & Recovery

DURCHDACHT BIS INS LETZTE DETAIL.

Leistungsstark.
Intelligent.

DER NEUE PRIMERGY RX200 S5

Verbessern Sie Ihre Energieeffizienz im Rechenzentrum mit dem innovativen PRIMERGY Cool-safe™ Systemdesign der neuen RX200 Rack Server Generation. Erhalten Sie mehr Leistung, verbesserte Erweiterbarkeit und Zuverlässigkeit in Kombination mit einem umfassend verbesserten Verhältnis von Leistung zu Energie – all dies bietet ihnen der neue PRIMERGY RX200 mit Intel® Xeon® Prozessoren in nur einer Rackeinheit.

Fujitsu ist weltweit drittgrößter Anbieter von umfassenden IT-Infrastrukturen. Bei Entwicklung und Produktion setzt Fujitsu international auf „Made in Germany“. So wurde die Verantwortung für strategische Produktbereiche wie x86-basierte Server, Storagesysteme und die Entwicklung innovativer Umwelttechnologien in Deutschland konzentriert. Fujitsu ist ein kundenorientiertes IT-Unternehmen, das flexibel und anpassungsfähig auf alle Anforderungen reagiert. Fujitsu bietet Unternehmen aller Größenklassen qualitativ hochwertige Produkte, Lösungen und Services für die IT-Infrastruktur, die auf weltweit führenden High-Performance-Informationstechnologien basieren.

Mehr Informationen unter http://de.ts.fujitsu.com oder 01805 372 100 (14 ct/Min.)

FUJITSU

EDITORIAL

I need backup!

Liebe Leser,

wer obigen Ausspruch vernimmt, befindet sich wahrscheinlich in einem Kinosaal und verfolgt angespannt, wie der einsame Held eines Polizeikrimis kurz vor dem Ausräuchern des Gangsternestes Verstärkung anfordert. In der englischen Sprache kennt "Backup" mehrere Bedeutungen, neben Verstärkung unter anderem Beistand, Deckung und Absicherung. Womit wir aus dem dunklen Kino auch schnell im hellen Rechenzentrum wären, denn eine funktionierende Sicherheitskopie stellt die beste Absicherung gegen Datenverlust dar. Und wer im Schadensfall entscheidende Unternehmensdaten nicht schnell wieder einspielen kann, steht in der Firma bald ohne Unterstützung da.

Dies scheint den meisten IT-Verantwortlichen bewusst zu sein, denn laut einer Studie von NetApp sichern 95 Prozent aller kleinen und mittelständischen Unternehmen ihre Daten regelmäßig. Vergleicht man dies mit früheren Werten, hat sich das Sicherheitsbewusstsein der allermeisten Firmen deutlich verbessert. Die NetApp-Studie bemängelt zwar nicht ganz ohne Eigeninteresse, dass vielfach das Medium der Speicherung ("USB-Stick") und deren Regelmäßigkeit ("je nach Bedarf") zu wünschen übrig ließen, insgesamt gesehen befindet sich jedoch auch im KMU-Bereich schon längst kein Admin mehr im Backup-Tiefschlaf.

Damit Sie Ihre Backup-Strategien optimieren können, haben wir in diesem Heft einige spannende Themen zusammengestellt: In unserer Test-Rubrik untersuchen wir ab Seite 12 unter anderem, was Online-Backups und die darunter liegende Software wirklich taugen. In einem weiteren Praxistest ab Seite 22 muss Acronis Backup & Recovery 10 sein Können unter Beweis stellen. Unsere Workshops erklären Ihnen ab den Seiten 28 beziehungsweise 44, wie Sie ein Datenrettungs-Konzept für Microsoft Exchange erstellen und wie Sie bei einem Stromausfall auch virtuelle Maschinen schnell und trotzdem kontrolliert in den Ruhezustand versetzen.

Das Proben des Ernstfalls kann ferner nie schaden, um die Abläufe bei der Wiederherstellung von Daten zu verinnerlichen. "Recovery" wird im Englischen im Bereich des Gartenbaus übrigens auch in der Bedeutung von Ausbeute verwendet. Sichern Sie sich also ausreichend ab, und Sie werden eine gute Ernte einfahren.

Viel Spaß beim Lesen, Ihr

Lars Nitsch
Redakteur 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 Hochverfügbarkeits-garantie 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.

INNOVATIONSPREIS 2008
initiative mittelstand
AUSZEICHNUNG

LANCOM 1751 UMTS

FINALIST
BEST
Wireless Broadband Security Innovation
09 WBI Awards

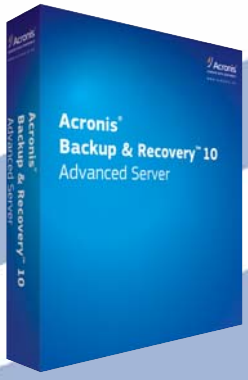
LANCOM Systems

www.lancom.de

INHALT

IT-Administrator – Ausgabe November 2009

IT-Desaster-Management – Backup & Recovery



Im Test: Acronis Backup & Recovery

Je mehr ein Unternehmen von der Verfügbarkeit seiner Daten abhängig ist, umso wichtiger ist deren zeitnahe Wiederherstellung, sollte ein Rechner seinen Dienst verweigern. Mit True Image Echo hat Acronis schon Ende 2007 ein Backup-Konzept für den Einsatz in Unternehmen präsentiert. Nun startet der Hersteller mit Backup & Recovery in die zehnte Runde. Wie die Neuerungen im Einzelnen aussehen und ob Backup & Recovery 10 eine sinnvolle Weiterentwicklung ist, haben wir für Sie in diesem Test herausgefunden.

Seite 22

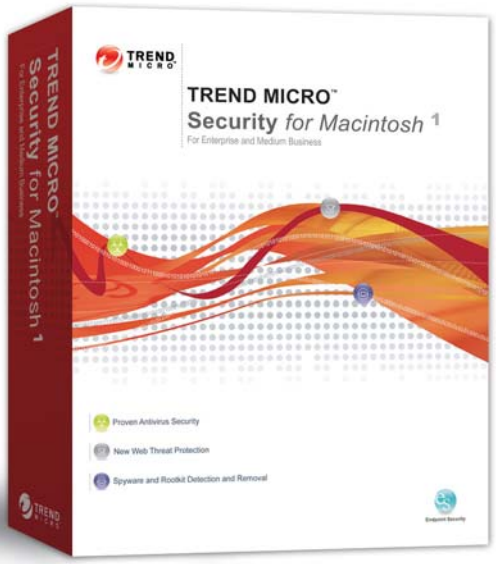
Die wichtigsten Neuerungen im Windows Server 2008 R2

Viele IT-Verantwortliche schauen auf Windows 7, denn XP verstaubt langsam und Vista erweist sich als Dauer-Flop in Unternehmen. Dabei wird leicht vergessen, dass Microsoft im Schatten des Client-Betriebssystems auch seinen Server runderneuert hat – und die wahre Macht ruht ja bekanntlich hinter dem Thron. IT-Administrator hat sich Windows 7 für Server alias Windows Server 2008 R2 vorab angesehen und stellt die zentralen Neuerungen vor.

Seite 32

Themenübersicht

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



Auch Macintosh-Rechner finden ab sofort unter der sicheren Schutzwolke von Trend Micro Zuflucht

Cloud-Schutz für Mac-Rechner

Trend Micro baut mit **Trend Micro Security for Mac** sein Angebot an **Endpoint-Security-Lösungen** aus. Mit der Software will der Hersteller Unternehmen adressieren, die sowohl Windows- als auch Mac-Plattformen nutzen und diese schützen möchten. Dabei soll die Lösung Mac-Nutzer in Unternehmen vor Viren, Spyware, Mischangriffen und webbasierten Angriffen schützen. Hiefür nutzt die Software das "Smart Protection Network" des Herstellers. Basierend auf einer der nach Herstellerangaben weltweit größten Domain-Reputationsdatenbanken, soll dieser Ansatz Schutz vor Webbedrohungen aus der Cloud bieten. So verhindere die Technologie, dass Mitarbeiter und Applikationen innerhalb und außerhalb des Unternehmensnetzes bösartige oder infiltrierte Webseiten aufrufen. Für die Administration lässt sich die Mac-Software in der "OfficeScan" Client-Server-Suite integrieren. IT-Verantwortliche haben mit der Lösung die Möglichkeit, für bis zu 1.000 Mac-Rechner Gruppenrichtlinien zu verwalten. Daneben sollen ortsbezogene Web Reputations-Richtlinien für Schutz innerhalb und außerhalb des Unternehmensnetzes sorgen. Ab sofort ist die Software erhältlich. Eine 50-User-Lizenz kostet 1.211 Euro als Plug-In für OfficeScan 10. *(dr)*

Trend Micro: www.trendmicro.de

Mehr Sicherheit für Thin Clients

LISCON stattet seine **Linux-basierten Thin Clients** mit neuen Features aus. Sowohl für das Betriebssystem **LISCON OS** als auch die Administrationssoftware **LMC** (LISCON Management Console) steht Anwendern ab sofort ein neues Release zum Download bereit. LISCON OS 2.27.1 verfügt über neue Funktionen, die den Einsatz der Thin Clients im Unternehmensnetzwerk sicherer machen sollen. Das Feature Single-Sign-On ermöglicht via Active Directory für Sessions über Citrix ICA, Microsoft RDP oder VMware View einen komfortablen Zugriff des Users, der sich lediglich einmal am Thin Client selbst anmelden muss. Für die weiteren Sitzungen sind keine erneuten Eingaben der Authentifizierungsdaten notwendig. Um Sicherheitsrisiken durch an den Thin Client angeschlossene USB-Geräte zu reduzieren, bietet die neue Version von LISCON OS erstmals die Möglichkeit, USB-Ports selektiv nur für bestimmte Geräte freizugeben. So lassen sich die Anschlüsse per Seriennummer beispielsweise lediglich für firmeneigene USB-Sticks freischalten. Andere USB-Geräte können an dem Client dann nicht verwendet werden. Bislang konnten die USB-Anschlüsse lediglich komplett gesperrt werden, mit dem neuen Release wird eine flexiblere Nutzung ermöglicht. Weitere Neuerungen in LISCON OS 2.27.1 umfassen neben zahlreichen Detailverbesserungen unter anderem die Integration des originalen VMware View 3.1 Clients. Dabei sollen sich mit der USB-Redirection-Funktion verschiedene USB-Geräte in virtualisierten Desktop-Umgebungen besser einbinden lassen. Neu ist schließlich ein grafischer Setup-Wizard für die Einrichtung des Thin Clients. Die Client-Images sind für alle Kunden ab sofort gratis verfügbar, für das LMC-Update ist ein bestehender Wartungsvertrag notwendig. *(dr)*

LISCON: www.liscon.com

Mehr Storage für virtuelle Umgebungen

NetApp erweitert die Einstiegsproduktfamilie FAS2000 um die **Speicherappliance FAS2040**. Das neue Modell soll Kunden mehr Performance und Kapazität bieten, um konsolidierten Microsoft Windows-Storage und virtualisierte Umgebungen auf einem einzigen System zu nutzen. Auf Basis der Unified Storage-Architektur und der integrierten Storage-Effizienz-Tools des Herstellers erhalten Nutzer der FAS2040 die doppelte Leistung bestehender FAS2000-Systeme und um bis zu 30 Prozent mehr Speicherkapazität. Bis zu 136 TByte speichert das System und weist die laut Hersteller notwendigen Verbindungsmöglichkeiten für FC- und IP-SAN sowie erweiterten Support für Ethernet- und SAS-Ports auf. Zudem ist die FAS2040 für die neue Version des NetApp Storage-Betriebssystems Data ONTAP 8 vorbereitet. Die FAS2020 ist innerhalb des vorhandenden Systems auf die neue Variante FAS2040 umstellbar. Ab sofort ist die neue Appliance erhältlich, die Preise für die FAS2000er Reihe beginnen bei 6.400 Euro. *(dr)*

NetApp: www.netapp.com/de/products/storage-systems/fas2000/

Das neueste Modell der FAS2000-Reihe von NetApp heißt FAS2040 und speichert bis zu 136 TByte

Desaster-Management in virtuellen Umgebungen

Die **Desaster-Recovery-Software Rear** ("Relax and Recover") ermöglicht das vollautomatische Recovery eines Linux-Servers, selbst bei komplizierten Setups. Hierfür unterstützt das Tool Software-RAID und LVM und nimmt die Einrichtung und Initialisierung eines Hardware-RAIDs bei den Servern gängiger Hersteller vollautomatisch vor. Nun ist ReaR dazu in der Lage, einen Server auf einer grundlegend geänderten Hardwareplattform wiederherzustellen. Damit kann die Software ab sofort für den automatischen Umzug von einst physikalischen Servern in eine virtualisierte Umgebung ("P2V-Migration") genutzt werden. Die Module für Netzwerkkarten- und Festplatten-Controller werden dabei automatisch erkannt und geladen, alle notwendigen Anpassungen im System werden vorgenommen. Auch die Extras einer virtuellen Umgebung berücksichtigt die Software und löst das Netzwerk-Bonding automatisch auf. Virtuelle Server können umgekehrt zurück auf echte Hardware ziehen oder von einer Virtualisierungstechnik in eine andere umgezogen werden. Auf sourceforge.net ist das Open Source-Tool zum Download verfügbar. *(dr)*

ReaR: http://rear.sourceforge.net/

Drucken mit Festtinte

Xerox präsentiert mit den Geräten der Serie **ColorQube 9200** ein neues **Multifunktionssystem auf Solid Ink-Basis**. Dabei handelt es sich um eine wachsähnliche Festtinte, die erst unmittelbar vor dem Druckvorgang verflüssigt und auf das Papier aufgetragen wird. Die Multifunktionsgeräte vereinen Drucker, Scanner und Kopierer und sollen die Kosten für Farbseiten im Vergleich zu herkömmlichen Laserdruckern um bis zu 62 Prozent senken. Der Hersteller bietet dazu ein neues Farbpreissystem an: Anstatt für jeden Farbdruck – unabhängig von der Farbdeckung – einen recht hohen Einheitspreis zu zahlen, sieht das neue System drei unterschiedliche Preise für geringe, mittlere oder hohe Farbflächendeckung vor. Die Serie ist in drei Varianten mit unterschiedlichen Druckgeschwindigkeiten erhältlich. Jedes Modell hat vier Druckköpfe, die über 150 Millionen Farbtropfen pro Sekunde drucken können. Dadurch steigt die Geschwindigkeit des Multifunktionssystems von 38 auf bis zu 85 Seiten pro Minute. Die verwendeten Sticks sind ungiftig und sauber und ohne zusätzliche Ummantelung in die Maschine einsetzbar. Zur zentralen Verwaltung der Drucker bietet der Hersteller die Software "Xerox CentreWare Web", mit der sich auch Geräte von anderen Herstellern administrieren lassen. Die Multifunktionssysteme ColorQube 9200 sind ab sofort zu einem Preis ab 15.080 Euro zu haben. *(ln)*

Xerox: www.office.xerox.com/color-printing-cost/dede.html

Xerox greift bei seinen Geräten aus der Reihe "ColorQube 9200" auf Festtinte zurück

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

Fortinet präsentiert die neueste Version seiner **FortiClient Endpoint Protection Suite** mit erweiterten Features für große, performanceintensive Enterprise-Umgebungen. Die aktuelle Version 4.1 umfasst SSL VPN, WAN-Optimierung, Application Detection und Endpoint Control. Zudem bietet sie eine umfassende Compliance-Infrastruktur, mit der sich Unternehmen vor Bedrohungen aus dem Internet schützen können. *(dr)*

www.fortinet.com

Netgear bringt mit Modell **WNR3500L** einen neuen Wireless-N Gigabit Router auf den Markt. Das Gerät basiert mit seiner Linux-Firmware auf Open Source und unterstützt laut Hersteller eine Vielzahl freier Anwendungen. Auf einer Community-Webseite erhalten Linux-Entwickler, freie Programmierer und Open Source-Anwender zahlreiche Informationen, Downloads und Quellcodes und können sich in Diskussionsforen und Blogs untereinander austauschen. Beliebte Linux-Firmwares wie DD-WRT, OpenWRT und Tomato sind bereits verfügbar und sollen es dem Anwender einfach machen, Applikationen zu entwickeln. Die Netzwerkkomponente ist ab sofort für 83 Euro erhältlich. *(ln)*

www.netgear.de

NAS-Speicher fürs Rack: Die Buffalo "TeraStation III" mit bis zu 8 TByte Speicherplatz

Vom Schreibtisch ins Rack

Buffalo Technology bringt seine **TeraStation III-Plattform** als **1HE-Rackmount** für eine noch einfachere Integration in eine bestehende Server-Umgebung auf den Markt. Für Anschluss ans Netzwerk sorgen zwei GBit-Ethernet-Ports. Dabei bietet der Server Transferraten bis zu 60 MByte/s dank Port Trunking sowie Funktionen wie NFS für die Einbindung von Unix-Clients, SMB für erweiterte Server-Dienste im Windows-Netzwerk und eine Active Directory-Unterstützung. Vor Datenverlusten soll der redundante Verbund der bis zu vier Festplatten mit bis zu 8 TByte Gesamtkapazität in den RAID-Modi 0, 1, 5 oder 10 schützen. Eine Authentifizierung der Benutzer und die Datenverschlüsselung mittels AES 128 Bit gewährleisten zudem den Schutz vor unbefugten Zugriffen. Zwei USB2.0-Schnittstellen stehen für den Anschluss weiterer Massenspeicher wie externen Festplatten zur Datensicherung sowie für den Anschluss einer unterbrechungsfreien Stromversorgung (USV) zum Schutz vor Stromausfall, Unter- oder Überspannung und Frequenzänderungen zur Verfügung. Das 19-Zoll-NAS wird vollbestückt mit den Kapazitäten 2, 4, 6 und 8 TByte sowie vorkonfiguriertem RAID 5 und Führungsschienen ausgeliefert. Die Preise beginnen bei 1.030 Euro. *(dr)*

Buffalo Technology: www.buffalo-technology.com/products/network-storage/terastation/

Zugriff von nah und fern

Raritan erweitert seine Produktreihe zur Serververwaltung um einen neuen **KVM-Switch**, der sich speziell an kleine bis mittelgroße Serverräume und Rechenzentren richtet. Das **Modell TMCAT17 LCD** verfügt über ein 17-Zoll Industrie-Display und ermöglicht den Zugriff auf mehrere Server von einer einzigen Konsole. Mit dem KVM-Switch lassen sich so gleichzeitig zwei getrennte KVM-Anwendersitzungen ausführen. Ein Anwender kann die LCD-Konsole des Switches zur Fehlerdiagnose und -behebung auf mehreren Servern nutzen. Die Konsole ist in den im Rack montierten Switch mit 1U-Formfaktor integriert. Der Switch gewährleistet dabei den Serverzugriff auf BIOS-Ebene, selbst wenn das Betriebssystem des Zielservers nicht mehr reagiert. Der zweite Anwender greift unterdessen über eine Cat 5-Kabelverbindung mit einer optionalen Workstation von einem weiter entfernten Standort auf den KVM-Switch zu. Deren Entfernung zum KVM-Switch kann laut Hersteller bis zu 195 Meter betragen, ohne dass die Monitorsignalqualität darunter leidet. Der neue KVM-Switch ist in zwei Ausführungen erhältlich. Das Modell TMCAT1728 für zwei Anwender verfügt über acht Ports und unterstützt bis zu acht Server gleichzeitig. Die Variante TMCAT17216 für zwei Anwender unterstützt mit 16 Ports bis zu 16 Server. Mit den Kaskadierungsfunktionen der Raritan MasterConsole CAT-Serie lassen sich beide Switches zur Unterstützung von bis zu 256 Servern skalieren. Ab sofort sind die beiden Modelle erhältlich. Das 8-Port-Gerät TMCAT1728 kostet 1.991 Euro und das 16-Port-Modell TMCAT17216 ist für 2.263 Euro zu haben. *(dr)*

Raritan: www.raritan.de/produkte/lcd-consoles/TMCAT17-lcd-kvm-switches/

Stromsparendes XenApp

Citrix Systems erweitert mit dem Feature Pack 2 seine Virtualisierungslösung **Citrix XenApp 5 um neue Funktionen**. Um die Leistung von Server-Farmen zu optimieren und den Stromverbrauch zu senken, ohne dabei den Zugriff der User auf Anwendungen einzuschränken, bietet XenApp 5 nun auch ein **richtlinienbasiertes Energiemanagement**: Durch das Zusammenlegen von Benutzersitzungen auf weniger Server werden Kapazitäten so aufgeteilt, dass ungleichmäßige oder geringe Auslastungen ausgeglichen werden. Zudem führen weitere Verbesserungen der Funktionen für Lasttests dazu, dass Kunden ab sofort intelligente Test-Szenarien erstellen können, um die Serverauslastung zu analysieren. Dadurch lässt sich für beliebige Umgebungen das beste Verhältnis von physischen und virtuellen Servern ermitteln und übermäßige Server-Kapazität vermeiden. Darüber hinaus baut der Anbieter sein Angebot an HDX-Technologien weiter aus. "HDX MediaStream für Flash" ist nun in XenApp 5 integriert und sorgt bei Nutzern von Flash-Anwendungen und Video-Inhalten für hochauflösende Bildqualität. Die Videodarstellung am Endgerät wird zudem beschleunigt und Client-seitige Ressourcen lassen sich für das Ausführen von Flash-Inhalten nutzen. Der Verbrauch an Bandbreite kann auf diese Weise deutlich reduziert werden. Mit dem ebenfalls neu zu XenApp 5 hinzugekommenen HDX Plug-and-Play haben Anwender unmittelbaren Zugriff auf ihre USB-Endgeräte. Citrix-Nutzer, die einen Branch Repeater einsetzen, sollen mit Hilfe der Funktion "HPX IntelliCache" zudem von einem schnelleren Streaming von Microsoft Outlook profitieren. Die neuen Features stehen ab sofort kostenlos zum Download zur Verfügung. *(dr)*

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

Flexibilisierung mit Risiko – auch Virtualisierung schützt nicht vor Datenverlusten

Virtualisierung ist in aller Munde. Die Technologie scheint die Lösung für alle Probleme eines Administrators zu sein, effizient und flexibel die immer größeren Datenbestände zu sichern. Doch die Erfahrung zeigt, dass auch neue Risiken des Datenverlustes entstehen.

Kein Anlass zur Sorglosigkeit
Richtige Virtualisierung kann Datensicherheit de facto erhöhen. Zum einen können so ganze Tape-Backups auf einer Festplattenumgebung emuliert werden. Ein ebenso wichtiger Vorteil ist das Anlegen oder Klonen von Images einer Virtual Machine. Mit Hilfe dieser Schablone kann dann bei Ausfall des Hosts die zentrale Verwaltungseinheit einer virtuellen Speicherverwaltung schnell wieder neu aufgesetzt werden.

Doch die scheinbare Einfachheit und neue Flexibilität hat ihre Tücken. Auch die virtuelle Welt kennt ihre reellen Risiken. Zu den ernsthaftesten Gefahren zählen Fehlfunktionen im virtuellen RAID, eine korrupte Systemdatei im Dateisystem der Virtual Machine sowie das versehentliche Löschen von Informationen auf den virtuellen Maschinen.

Fatal wird es, wenn die Physik in Form höherer Gewalt in die virtuelle Welt eindringt. Im virtuellen RAID5 einer hochrangigen Behörde mit 80 Festplatten à 320 GB fielen zum Beispiel nach einem Wasserschaden im Serverraum 24 Platten aus.

Rein physikalisch bestand das System aus 80 Festplatten. Die Gesamtheit der Platten war in 10 RAID5-Verbunden organisiert. In der zweiten Ebene, der Virtualisierungsebene, wurden die Daten noch einmal umorganisiert. Ein Drittel des Speicherbereichs wurde als erste logische Einheit (LUN) in RAID1 gespiegelt, eine zweite LUN aus Gründen des schnellen Zugriffs mit RAID0 „gestriped" und eine dritte LUN mit RAID5 eingerichtet. Der Controller für das ganze virtuelle System teilte in einer zentralen Liste alle Speicherbereiche den einzelnen LUNs zu. Um ein Verständnis für die Dimensionen zu erhalten: Allein das zentrale Verzeichnis des Controllers wurde aus Sicherheitsgründen auf Teilbereiche von vier einzelnen Festplatten gespeichert.

Ein unsachgemäßer Ausbau der Festplatte machte es Kunde wie Hersteller der Backup-Lösung endgültig unmöglich, die Informationen zu retten. Nur mit hohem zeitlichem und finanziellem Aufwand war die Rettung durch die Datenrettungsexperten von Kroll Ontrack möglich.

Doch darüber hinaus kommt es oft zu erstaunlichem Leichtsinn. Komplette virtuelle Maschinen sind einfach gelöscht, neu formatiert oder während des Kopierens aus unterschiedlichen Gründen verschwunden. Die Archivierung auf einem real existierenden ausgelagerten Tape-Laufwerk oder einer Library wird vernachlässigt. So wird nur auf virtuellen Tape Libraries archiviert, die auf demselben virtuellen Host liegen. In der neuen IT-Landschaft werden Backups offensichtlich noch seltener als früher tatsächlich überprüft, häufig sogar lediglich nur angedacht und das Risiko verdrängt.

Die Übersicht behalten
Administratoren dürfen die Sicherheitsaspekte nicht aus den Augen verlieren. Virtualisierung bedeutet eine komplexe Speicherorganisation durch die Virtual Machine. Fehler oder Änderungen der Datenorganisation auf dieser Ebene haben schnell Kettenreaktionen zur Folge.

Folgende Ratschläge können schon helfen:

1. Grundlage eines virtuellen RAID sollte ein solides RAID 6 mit großzügig bemessener realer Festplattenkapazität als Speicherpool sein. Hier sollte auch nicht am falschen Ort gespart werden.

2. Die Dateiorganisation muss übersichtlich bleiben. Je höher die Verschachtelung der Datenorganisation, je mehr Virtual Machines eingerichtet werden, je schneller neue zusätzliche virtuelle Partitionen eingerichtet werden, umso schneller kommt es zu einem Wildwuchs. Dieser ist dann für den Administrator im Notfall oder bei einer später beabsichtigten Neuorganisation der Speicherumgebung undurchschaubar.

3. Unbedingt zu vermeiden ist es, innerhalb der virtuellen Maschine Daten zu speichern. Die virtuellen Maschinen sollten ihre Daten in realen Speicherumgebungen ablegen, insbesondere bei Datenbanken.

4. Wichtig ist eine effektive Dokumentation. Administratoren müssen wissen, wie die Virtual Machines bezeichnet sind und in welchem Festplattenpool diese zwischen den einzelnen virtuellen Servern angelegt sind.

5. Das Backup bleibt auch in der virtuellen Umgebung Schlussstein der Datensicherung.

Edmund Hilt, Managing Director,
Kroll Ontrack GmbH, Böblingen
www.ontrack.de

KROLL ONTRACK®

IT-Administrator-Workshop am 24. November 2009 in München

Open Source ist mehr als billig

von John Pardey

ITANet Schirmherrschaft:

REALTECH

ITANet Workshop-Partner:

GeNUA

Fraglos bietet sich durch die Nutzung von Linux und quelloffenen Infrastrukturlösungen ein großes Potenzial zur Kostenreduktion. Dem gegenüber stehen jedoch oft das fehlende Know-how in der Administration derartiger Werkzeuge sowie die nicht unbegründete Angst vor fehlendem Support. Verdrängt wird bei derlei Diskussionen oft die enorme Leistungsfähigkeit, die Open Source-Lösungen den Anwendern heute bieten. Und so widmet sich der letzte Workshop des IT-Administrator in 2009 dem Thema, wie kleine und mittlere Unternehmen Open Source-Werkzeuge gewinnbringend in ihre Infrastruktur integrieren können. Beispielhaft betrachten wir dabei die Themen Storage, Virtualisierung, Security und Hochverfügbarkeit.

Um den Teilnehmern das Thema Open Source schmackhaft zu machen, startet Florian Thiessenhusen von der adMERITia GmbH den Workshopnachmittag mit einer Tour durch die "Perlen" unter den offenen Werkzeugen. Anhand diverser leistungsfähiger Programme hält er ein Plädoyer für Tools wie Nagios oder Xorp. Sein Kollege Thomas Gronenwald stellt Ihnen danach das freie Storagewerkzeug OpenFiler vor, das die Festplatten gängiger x86-Hardware im Netz bereitstellt. Und das nicht nur als Dateisystem, sondern als Gerät, das Administratoren zum Aufbau eines NAS nutzen können.

Zentrale Themen der IT mit Open Source

Sicherheit und Virtualisierung gehören zweifellos zu den wichtigsten Themen für IT-Verantwortliche. Kein Wunder also, dass sich hier auch im Open Source-Umfeld einiges bewegt. Joachim Ayasse von der GeNUA mbH stellt vor, wie sich mit der Open Source-Security-Suite "Anoubis" die Rechte von Anwendungen auf Unix-Clients beschränken lassen. Was Open Source im Bereich der Virtualisierung zu leisten vermag, erfahren die Teilnehmer dann am Beispiel von Red Hat Enterprise Linux 5.4. Matthias Kranz von Red Hat erläutert die erweiterten Virtualisierungsfunktionalitäten von RHEL 5.4. Ein Fokus stellt dabei die Integration der KVM-Technologie (Kernel-based Virtual Machine), der Intel Virtualization Technology for Directed I/O (Intel VT-d) und PCI-SIG SR-IOV dar.

Und das alles hochverfügbar

Im letzten Vortrag des Tages beschäftigt sich Dr. Michael Schwartzkopff von der MultiNET Services GmbH mit den Fähigkeiten, die Linux-HA in Version 3 mitbringt. Die wichtigste Neuerung ist dabei sicher die eingebaute Überwachung der Ressourcen. Anhand der Grundelemente "Ressource" und "Bedingung" zeigt Schwartzkopff, wie sich selbst komplexe Hochverfügbarkeits-Konfigurationen darstellen lassen. Abschließend geht der Dozent noch auf die Entwicklung des Projektes Linux-HA (Stichwort: "pacemaker") ein.

Ein Workshop also, der sich doppelt lohnt: Sammeln Sie neues Wissen und sparen Sie nach Ihrer Rückkehr in den Job Lizenzkosten. 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 in München begrüßen zu dürfen.

ITANet
Die System und Netzwerk User Group

Die Agenda des Workshops

13.00 Uhr:	Begrüßung	
13.15 Uhr:	Open Source-Perlen	*Dozent: Florian Thiessenhusen, adMERITia GmbH*
13.45 Uhr:	OpenFiler	*Dozent: Thomas Gronenwald, adMERITia GmbH*
14.15 Uhr:	Sicherheitskontrolle für Anwendungen	*Dozent: Joachim Ayasse, GeNUA mbH*
15.00 Uhr:	Pause	
15.15 Uhr:	Open Source-Virtualisierung mit Red Hat	*Dozent: Matthias Kranz, Red Hat GmbH*
16.15 Uhr:	Linux HA 3 – wohin geht die Reise?	*Dozent: Dr. Michael Schwartzkopff, MultiNET Services GmbH*
17.30 Uhr:	Ende des Workshops	

Ort: GeNUA mbH
Domagkstr. 7
85551 Kirchheim bei München

Teilnahmegebühren:
Für IT-Administrator Abonnenten kostenlos.

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

Workshop "Open Source in KMUs" am 24. November

Windows 7-Launch, 7. Oktober 2009, München

Chefsache Windows 7

von Daniel Richey

Nun ist es soweit – das neue Windows 7 löst das in Unternehmen weitgehend gefloppte Windows Vista ab und spielt in Zusammenarbeit mit dem Server 2008 R2 seine Stärken im professionellen Umfeld aus. Steve Ballmer persönlich präsentierte denn auch die neuen Betriebssysteme vor über 1.000 IT-Profis Anfang Oktober in München. Für ihn stand dabei besonders die Effizienzsteigerung für Unternehmen im Mittelpunkt.

Mit begeistertem Applaus empfingen rund 1.200 IT-Verantwortliche Steve Ballmer im Internationalen Congress Center München. Der Microsoft-Chef stellte ihnen Anfang Oktober in einer gut halbstündigen Keynote das neue Betriebssystem Windows 7 und den Server 2008 R2 vor. Die Veranstaltung war schon Wochen zuvor bis auf den letzten Platz ausgebucht. Zuvor war Ballmer im Rahmen einer Pressekonferenz bei BMW unterwegs und stellte den Automobilbauer als Referenzkunden für Windows 7 vor. Seit Anfang 2009 testet das Unternehmen den Vista-Nachfolger und will bis 2011 alle 85.000 Desktops auf Windows 7 umstellen.

Besonders die Effizienz in Unternehmen stand für Ballmer an oberster Stelle. Angesichts der wirtschaftlichen Lage würden viele Unternehmen ihre Denkweise über IT ändern und verbesserte Ressourcennutzung in den Mittelpunkt stellen. Windows 7 und Server 2008 R2 sollen ihren Beitrag dank zahlreicher neuer Features dazu leisten. So ergäben sich bei der Wartung eines Windows 7-Arbeitsplatzes nach einer Analystenschätzung Kosteneinsparungen von 60 bis 100 Euro jährlich. Überhaupt sei Server 2008 R2 der beste Weg, im Rechenzentrum Geld zu sparen, besonders angesichts der umfassenden Virtualisierungsmöglichkeiten. Für die IT-Branche prognostizierte der Microsoft-Chef derweil eine rosige Zukunft. So sollen laut einer Studie zwischen 2009 und 2013 allein in Deutschland 94.000 neue Arbeitsplätze entstehen.

Neue Funktionen für die Admins

Welche weiteren Neuerungen Windows 7, Server 2008 R2 und Exchange 2010 mitbringen, erfuhren die Teilnehmer im Verlauf des Tages in zwölf verschiedenen Sessions. Der Technical Evangelist Ralf Schnell etwa stellte Version 2 des Microsoft-Hypervisors Hyper-V vor, die im Server 2008 R2 enthalten ist. Während Version 1 der Virtualisierungslösung laut Schnell bereits über eine stabile Architektur verfügt, haperte es bislang an der Skalierbarkeit. Dies soll sich nun mit Version 2 verbessern. So unterstützt Hyper-V jetzt bis zu 64 GByte RAM pro virtueller Maschine und bietet darüber hinaus Features wie Live-Migration und Fail-over-Clustering.

Im Windows Server 2008 R2 stechen besonders die Änderungen im Active Directory sowie die PowerShell 2.0 hervor. Michael Korp, ebenfalls Technical Evangelist bei Microsoft, zeigte auf, wie Administratoren nun etwa den neuen Papierkorb im Active Directory nutzen können. Er nimmt wie sein Kollege auf dem Windows-Desktop gelöschte Dateien – in dem Fall Active Directory-Elemente – auf und stellt diese bei Bedarf per Mausklick wieder her. Ein neues Admincenter soll zudem tägliche Aufgaben mit dem Verzeichnisdienst vereinfachen, während die PowerShell 2.0 nun auch über ein grafisches Interface verfügt und parallele Jobs ermöglicht.

In Exchange 2010 spielt die Unified Communication eine zentrale Rolle. In seiner Keynote präsentierte Said Zahedani, Senior Director Developer Platform and Strategy Group, wie Anwender nun per Sprachsteuerung auf ihre Kalendereinträge und E-Mails zugreifen können. Dass dabei immer mehr dieser Funktionen in die Cloud ausgelagert werden, sollte die IT-Profis nicht beunruhigen. So hätten diese nun weniger mit der aufwändigen Wartung von Maschinen zu tun und somit mehr Zeit, sich auf innovative Aufgaben zu konzentrieren.

Für Steve Ballmer bedeuten Windows 7 und Server 2008 R2 mehr Effizienz und weniger Kosten für Unternehmen

Zum Redaktionsschluss dieser Ausgabe noch buchbare Launch-Events

- 20. November 2009 in Düsseldorf (Swissôtel)
- 23. November 2009 in Frankfurt am Main (Congress Center)

Mehr Informationen unter *www.microsoft.com/germany/jointlaunch09/Events.aspx*

Weitere Launch-Termine

Vergleichstest: Tools für das Online-Backup

Sicherung in die Ferne

von Jürgen Heyer

Schon seit einiger Zeit ist die Online-Datensicherung per Internet zu einem Backup-Provider ein Hype-Thema, das nun auch für größere Datenmengen interessant wird. Wir haben die Angebote auf dem Markt recherchiert und dabei hinter die Kulissen geschaut: Es gibt eine Vielzahl von Anbietern, doch die Menge der tatsächlich genutzten Sicherungsprodukte ist sehr überschaubar. Diese aber bestimmen letztendlich die Funktionalität und sollten ein gewichtiges Entscheidungskriterium sein.

In den letzten Jahren ist die Anzahl der Anbieter für Online-Backup-Lösungen kontinuierlich gewachsen. Fanden sich anfangs gerade mal eine Handvoll Provider, so ist das Angebot mittlerweile kaum noch überschaubar. Bei unserer Recherche haben wir hierzulande über 40 Anbieter gefunden, von denen rund 20 auf unsere Anfrage nach der von ihnen eingesetzten Software reagierten. Dort beantragten wir Testzugänge, um einen Blick auf die Sicherungsfunktionalität zu werfen. Dabei zeigte sich schnell, dass es momentan sechs verbreitete Sicherungswerkzeuge gibt und nur wenige Provider ein selbst entwickeltes Tool verwenden. Mehrfach zu finden sind Ahsay Online Backup, Asigra Televaulting, F-Secure Online Backup, Iron Mountain Digital Connected Backup for PC, Novastor Novanet Web und Onbackup ISP Server. Das Carbonite-eigene "Online PC-Backup" ist individuell auf diesen Provider zugeschnitten.

Wer nun den Einsatz eines Online-Backups plant und sich durch eines der genannten Produkte angesprochen fühlt, kann in der Marktübersicht (siehe Kasten) herauslesen, welcher Provider es nutzt und so eine Vorauswahl treffen. Abgesehen davon bieten fast alle Provider die Möglichkeit an, sich kostenlos einen 30-Tage-Testaccount einrichten zu lassen, um so zusätzlich einen praktischen Eindruck zu erhalten.

Auch wenn wir alle Produkte in Verbindung mit einem Provider getestet haben, ist es für ein Unternehmen ebenso möglich, für die Server und PC-Systeme sowohl in der Zentrale als auch in den Außenstellen in völliger Eigenregie eine eigene Online-Backup-Lösung aufzubauen. Alle vorgestellten Produkte außer dem Dienst von Carbonite sind auch als Kaufsoftware erhältlich. Ein eigener Betrieb hat verständlicherweise Vor- und auch Nachteile: Die Daten verlassen nicht das Haus und es entsteht keine Abhängigkeit zu einem externen Provider. Administrationsaufwand und Investition sind aber höher, da die Backupserver beschafft und betrieben werden müssen, dafür entfallen die monatlichen Zahlungen an den Provider. Letztendlich mündet dies in einer individuellen Abwägung der Argumente, wobei mit zunehmender Unternehmensgröße die Kaufvariante immer interessanter werden dürfte.

Ahsay Online Backup Manager

Bei der Anmeldung bei einem Provider, der den Ahsay Online Backup Manager (OBM) nutzt, erhält der Anwender eine E-Mail mit Anmeldename und Zufallspasswort, das nach der Installation geändert werden muss. Die Installation des 49 MByte großen Clients verlief im Test problemlos. Neben Windows sind auch Versionen für Linux, Unix, Macintosh und Novell erhältlich. Im Anschluss an das Clientsetup änderten wir das Passwort. Für die Verschlüsselung stehen Twofish 256 Bit, Triple-DES und AES 128/256 Bit zur Verfügung. Nach der Passwortänderung startet ein Assistent zur Einrichtung des ersten Backup-Sets, der innerhalb der eigenen Dateien das Dokumentenverzeichnis zur Sicherung vorschlägt. An dieser Stelle lassen sich problemlos Änderungen vornehmen und selbst die zu sichernden Verzeichnisse festlegen. Umfassende Möglichkeiten bietet der Scheduler, der neben täglichen, wöchentlichen, monatlichen und einmaligen benutzerdefinierten Sicherungen auch periodische Wiederholungen im Minuten- und Stundentakt erlaubt.

Weiterhin ermöglicht der OBM eine Continuous Data Protection (CDP), wobei er geänderte Dateien in festlegbaren Minutenabständen sichert. Insgesamt ist das Tool recht übersichtlich gestaltet, wobei im Hauptmenü die beiden großen Schaltflächen für Backup und Wiederherstellung ins Auge fallen. Gut ist die permanente Übersicht, wie groß der Datenpool ist und wie viel davon aktuell belegt ist. Der Abgleich, welche geänderten Dateien bei einem Backup zu sichern sind, geschieht recht schnell.

Unter www.it-administrator.de/markt/marktuebersichten/onlinebackup.pdf finden Sie eine aktuelle Marktübersicht der von uns getesteten Online-Backup-Dienstleister. Dieser ausführlichen Liste können Sie neben zahlreichen technischen Details auch entnehmen, welcher Anbieter mit welcher Software arbeitet.

Marktübersicht

Für eine Wiederherstellung wird die gesicherte Verzeichnisstruktur aufgelistet, wobei der Anwender sich alle Dateien oder nach Backup Set geordnet anzeigen lassen kann. Eine Wiederherstellung kann an den ursprünglichen Speicherort oder eine andere Stelle erfolgen. Die Dateiberechtigungen werden auf Wunsch mitgesichert und auch wiederhergestellt.

Ahsay unterstützt keine Deduplizierung, identische Dateien in verschiedenen Verzeichnissen werden also mehrfach gesichert, was zusätzliche Sicherungskapazität beim Provider kosten kann. Standardmäßig erfolgt die Sicherung inkrementell, es sind aber auch explizite Voll- und Differenzsicherungen definierbar. Eine wirksame Infile-Delta-Funktion sorgt dafür, dass wirklich nur geänderte Teile in einer Datei gesichert werden, was auch bei Outlook PST-Dateien funktioniert. Neben lokalen Dateien unterstützt der OBM auch die Sicherung von Freigaben im Netzwerk. Allerdings muss es sich hier um reguläre Freigaben handeln, der direkte Zugriff auf die administrativen Freigaben ist nicht vorgesehen.

Ein frei definierbarer Backup-Filter ermöglicht es, bestimmte Dateien entsprechend des Namens oder der Endung von der Sicherung auszuklammern. Weiterhin setzt OBM optional Vor- und Nachlaufkommandos ab, um beispielsweise Datenbanken zu stoppen und so für die Sicherung in einen konsistenten Zustand zu bringen, und unterstützt Schattenkopien (VSS). Auch den Rückhaltebereich, der bestimmt, nach wie vielen Tagen auf der Quelle gelöschte Dateien auch auf dem Sicherungsserver gelöscht werden, kann der Administrator frei bestimmen. Dass eine längere Aufbewahrung zusätzlichen Platz kostet und damit eventuell Mehrkosten verursacht, ist klar, aber rein funktional sind hier keine Grenzen vorgegeben. Neben der Sicherung via Internet ermöglicht das Werkzeug auch lokale Sicherungen – sowohl, um vor Ort zusätzliche Sicherungen zu haben, als auch für die Sicherung beispielsweise auf eine externe Festplatte, um diese für ein schnelles Initialbackup zum Provider zu schicken. Absolut vorbildlich sind die Mailbenachrichtigungen, die der Administrator direkt vom Provider erhält. Die E-Mails informieren über erfolgreiche Sicherungen inklusive der übertragenen Datenmenge und erinnern genauso bei fehlgeschlagenen oder nicht durchgeführten Backups.

Insgesamt erweist sich Ahsay Online Backup als vielseitig einsetzbares Werkzeug für Arbeitsplätze und Server, wobei für jedes System idealerweise ein eigenes Konto zu verwenden ist. Umfassende Konfigurationsmöglichkeiten erlauben eine individuelle Parametrisierung. Wünschenswert erscheint uns noch eine Deduplizierung. Beispielhaft ist die umfassende Mailbenachrichtigung. Optimal geeignet ist das Werkzeug zur unabhängigen Sicherung einzelner Server und Arbeitsplätze. Da neben Windows auch Linux, Solaris, Netware und Macintosh unterstützt werden, ist der Client vielseitig einsetzbar. Bedingt geeignet ist das Programm für eine zentrale Sicherung vieler Systeme, da jedes einzeln bedient werden muss.

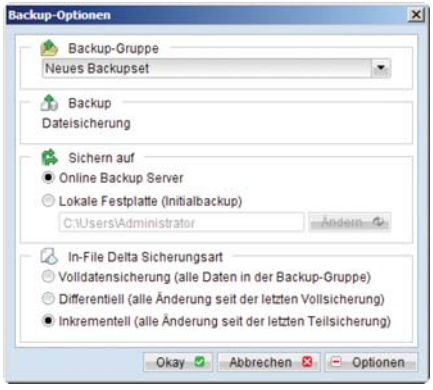


Bild 1: Als einziges Tool erlaubt der Ashay OBM neben inkrementellen auch differentielle Sicherungen

Asigra Televaulting

Der Marktführer im Segment Online-Backup ist der kanadische Hersteller Asigra mit seinem Produkt Televaulting. Es ist das einzige Werkzeug im Test, das weitere Rechner im Netzwerk über deren administrativen Freigaben agentenlos mitsichert. Es können aber ebenso mehrere Konsolen parallel installiert werden. Welcher Weg der bessere ist, hängt von der jeweiligen Internetanbindung und von der Firmenstruktur ab. Dient der Sicherungsrechner namens "DS-Client" mit dem Konsolenprogramm "DS-User" nicht nur als Sicherungssystem, sondern wie beispielsweise bei einem Notebook auch als Arbeitsplatz, lässt sich die CPU-Nutzung durch den Client begrenzen, damit ein paralleles Arbeiten noch möglich ist. Auf jeder Konsole wird für die Verwaltung der Sicherungsdaten eine SQL-Datenbank installiert, was die Ermittlung der entsprechenden Pakete sehr beschleunigt. Zur Sicherheit wird regelmäßig ein Datenbank-Dump zum Sicherungsserver übertragen, aus dem sich beim Verlust der lokalen Datenbank diese wiederherstellen ließe.

Trotz der umfassenden Netzwerkfähigkeit überzeugte das Tool im Test mit einer sehr übersichtlichen Bedienung. So unterstützt ein Assistent beim Anlegen von Sicherungsaufträgen. Sehr detailliert sind die Möglichkeiten zur Zeitplanung, die auch eine Sicherung mehrfach täglich in Stundenintervallen erlauben. Start- und Stoppkommandos vor und nach der Sicherung lassen sich individuell vorgeben, Datenbanken wie SQL und Oracle sowie Mailsysteme wie Lotus Notes und Exchange

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

Installation/Bedienung	9
Funktionsumfang	8
Scheduler	8
Eignung im Serverumfeld	8
Dokumentation	7
Gesamtwertung (max. 50)	**40**

Ahsay
www.ahsay.com

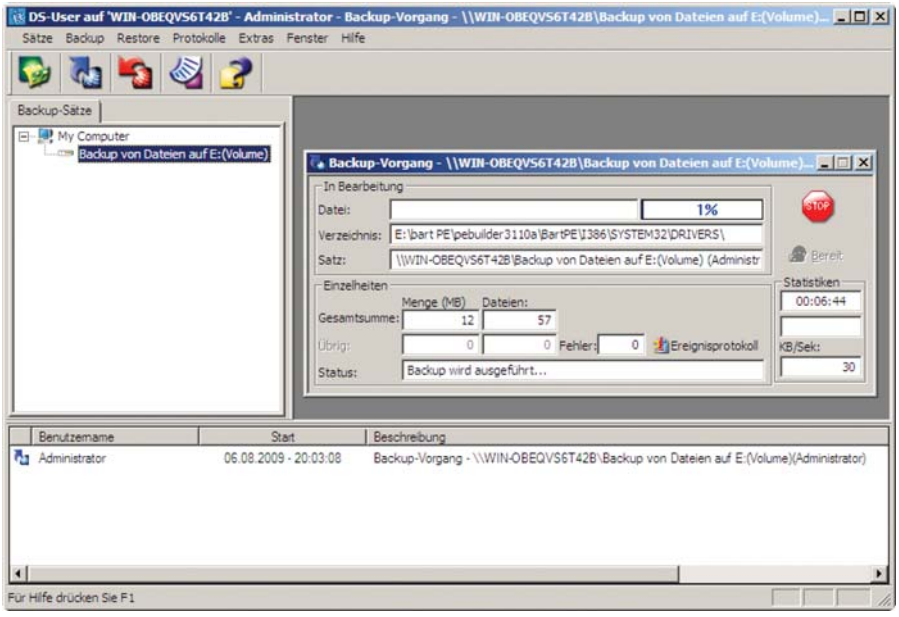


Bild 2: Der DS-Client von "Asigra Televaulting" zeigt den Sicherungsfortschritt übersichtlich an

werden ebenfalls verarbeitet. In diesem Zusammenhang ist auch die sehr breite Betriebssystemunterstützung inklusive Linux, Macintosh und Novell Netware positiv zu erwähnen. Zur Reduzierung der Datenmengen sichert das Tool von Dateien nur die geänderten Blöcke (Delta-Sicherung), identische Dateien mehrerer Clients werden nur einmal hochgeladen (Deduplizierung). Herausgefiltert werden auch typische Backup-, Swap- und temporäre Dateien, wobei eine Benutzer-definierte Angabe möglich ist.

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

Installation/Bedienung	9
Funktionsumfang	10
Scheduler	8
Eignung im Serverumfeld	9
Dokumentation	9
Gesamtwertung (max. 50)	**45**

Asigra
www.asigra.com

Möglich ist daneben ein lokales Initialbackup, um die Daten anschließend zum Provider zu schicken und so den ersten Abgleich zu beschleunigen. Asigra Televaulting arbeitet bei der Datenverschlüsselung mit einem privaten Schlüssel für jeden DS-Client und einem kundenspezifischen Konto-Schlüssel. Eine nachträgliche Änderung ist nicht möglich. Der Konto-Schlüssel wird dann benötigt, wenn mehrere Clients identische Daten sichern (Client-übergreifende Deduplizierung). Diese werden dann mit dem Konto-Schlüssel gesichert gespeichert, damit jeder Client zur Wiederherstellung darauf zugreifen kann. Normalerweise wird der Schlüssel nicht auf dem Backupserver gespeichert, dies lässt sich aber optional aktivieren. Eine Zugriffsbeschränkung auf IP-Adressen ist möglich, auf Wunsch lässt sich auch einstellen, dass neu installierte DS-Clients erst explizit am System registriert werden müssen.

Neben dem DS-Client sind noch diverse Zusatzmodule verfügbar, die allerdings von den Providern nur teilweise beziehungsweise optional angeboten werden. So ermöglicht das "LAN Storage Discovery"-Modul genaue Auswertungen der Dateistruktur im Vorfeld, um unter anderem den Grad der Duplizierung, die Änderungsrate, Dateigrößen und -typen sowie Zugriffshäufigkeiten zu ermitteln. Das hilft bei der Planung und Kalkulation von Sicherungsjobs. Das "Local Storage"-Modul erlaubt zusätzlich lokale Sicherungen für eine schnellere Wiederherstellung. Weiterhin gibt es die Option, bei Exchange, Lotus Notes und Groupwise einzelne E-Mails rücksichern zu können. Bei einem Sharepoint-Server lassen sich optional einzelne Objekte wiederherstellen. Das "Backup Lifecycle Management Module" (BLM) ergänzt den Online-Speicher um ein Archiv, in dem sich alte Daten günstiger aufbewahren lassen. Ein Disk/Tape-Modul dient dazu, einem Kunden im Disaster-Fall seine Daten schnell auf ein geeignetes Medium zu kopieren und zuzuschicken. Über ein optionales Web-Portal kann ein Kunde alle seine DS-Clients zentral verwalten und bei Bedarf auch neue anlegen. Zum Nachweis der Verfügbarkeit bietet Asigra ein SLA Availability Modul an und die Abrechnung wird über ein "DS Billing"-Modul erleichtert.

Wer Asigra Televaulting in Eigenregie betreiben möchte, dem stehen verschiedene Konfigurationskonzepte zur Verfügung, wie eine zentrale Datenbank statt einzelner auf den DS-Clients, außerdem eine Möglichkeit zum redundanten Aufbau sowie zur Datenreplikation, um alle Daten doppelt an zwei getrennten Standorten zu speichern. Insgesamt bietet Asigra Televaulting funktional mit Abstand die meisten Möglichkeiten, was sich bei den Providerangeboten allerdings auch in einem vergleichsweise hohen Preis niederschlägt. Die Lösung ist sowohl für die Sicherung einzelner Clients als auch das Backup ganzer Arbeitsgruppen oder Domänen optimal geeignet. Das Konzept des DS-Client ist ideal für eine zentrale Arbeitsweise. Mit zunehmenden Datenmengen wird eine Provider-orientierte Arbeitsweise allenfalls aufgrund des recht hohen Preises zunehmend uninteressanter.

Carbonite Online PC-Backup

Das Ziel des Backup-Dienstes von Carbonite ist eine Continuous Data Protection, für

die ausgewählte Dateien in der aktuellen Version vom Arbeitsplatz auf dem Backupserver von Carbonite gesichert werden. Die von Carbonite eingesetzte Software ist eine Eigenentwicklung. Nach der Installation erscheint ein zusätzliches Icon in der Taskleiste, über das der Anwender in das Info-Center gelangt. Für die Auswahl der zu sichernden Dateien hat sich Carbonite etwas Besonderes ausgedacht, indem im Explorer das Kontextmenü der rechten Maustaste um einen Eintrag erweitert ist. Über diesen Punkt lassen sich Dateien oder auch ganze Verzeichnisbäume in die Sicherung hinein- sowie auch herausnehmen. Die Sicherung erfolgt normalerweise im Abstand von 24 Stunden, wobei sich der Dienst an der aktuellen CPU-Last orientiert und erst nach einigen Minuten CPU-Leerlauf startet. Der Anwender kann aber im Info-Center jederzeit eine Sicherung der letzten Änderungen veranlassen. Neben dieser Vorgehensweise besitzt Carbonite auch einen einfachen Scheduler, um zu einer bestimmten Zeit an bestimmten Tagen eine Sicherung durchzuführen.

Der Dienst von Carbonite kennt keinerlei Versionierung, es wird stets nur der aktuelle Stand aufgehoben. Am Client gelöschte Dateien werden auf dem Backupserver nach 30 Tagen entfernt. Falls der Account beispielsweise beim Systemwechsel auf ein anderes Gerät übertragen werden muss, kann der Anwender über die Anmeldung im Internet bei Carbonite den Client in den so genannten Wiederherstellungsmodus versetzen. Dann führt der Client keinen Abgleich mit dem Zielsystem durch, was letztendlich bedeuten würde, dass alle Dateien als gelöscht markiert würden. Vielmehr ist er bereit für eine Wiederherstellung aller gesicherten Daten auf dem neuen System.
Ebenso wie F-Secure Online Backup ist Carbonite Online PC-Backup eine preiswerte Lösung für eine Grundsicherung von Arbeitsplätzen und vor allem für Notebooks, um auch auf Reisen immer eine aktuelle Kopie der wichtigen Daten auf einem Sicherungsserver zu haben. Optimal geeignet ist Online PC-Backup für eine kontinuierliche Sicherung der aktuellen Arbeitsdaten von Notebooks und Arbeitsplätzen. Nur bedingt geeignet ist der Dienst für die Sicherung von Servern, da nicht offiziell unterstützt. Im Rahmen eines fairen Gebrauchs ist der sehr günstige Preis (Flatratemodell) auch nicht mit der immensen Datenmenge eines Servers zu vereinen. Nicht geeignet ist das Programm, wenn die Rücksicherung verschiedener Versionen möglich sein muss.

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

Installation/Bedienung	8
Funktionsumfang	3
Scheduler	3
Eignung im Serverumfeld	2
Dokumentation	5
Gesamtwertung (max. 50)	**21**

Carbonite
www.carbonite-backup.de

F-Secure Online Backup

Ebenso wie Carbonite bieten die Provider, die das Produkt Online Backup von F-Secure einsetzen, den Dienst für einen Jahresbeitrag um die 50 Euro ohne Kapazitätsbegrenzung an. Damit lässt sich bereits erahnen, dass es sich um ein Tool für eine Continuous Data Protection (CDP) handelt. Dabei werden die Dateien nicht per Scheduler gesichert, sondern kurz nach deren Anlage. Bei der Anmeldung erzeugt das Tool zunächst eine individuelle Setupdatei, die zu installieren ist und alle Zugangsinformationen aufgrund der Anmeldedaten enthält. Diese müssen daher nicht noch einmal eingegeben werden.

Offiziell unterstützt werden Windows XP und Vista, im Test klappte die Installation unter Windows 2008 Server 64 Bit jedoch ebenso problemlos. Das Werkzeug ist in erster Linie darauf ausgelegt, bestimmte Dateiarten (Office-Dokumente, Bilder und Videos, Musik, E-Mail und eigene wichtige Dateien) zu sichern. Das Speichern verschiedener Versionen (bis zu fünf) ist nur bei Office-Dateien vorgesehen, ansonsten befindet sich auf dem Backupserver wie bei Carbonite nur eine Kopie der zu sichernden Dateien. Das hilft beispielsweise bei einem Notebook, um bei einem Diebstahl oder Verlust den letzten Stand wiederzubekommen. Gelöschte Dateien werden auf Wunsch noch 15, 30 oder 45 Tage aufbewahrt. Für die Sicherung von Datenbanken ist das Werkzeug nicht geeignet.

Bei Bedarf lässt sich die Upload-Geschwindigkeit begrenzen, was auch sinnvoll ist: Da die Dateien kurz nach der Anlage gesichert werden, ist die Wahrscheinlichkeit groß, dass das Tool arbeitet, während der Anwender noch aktiv ist. Eine Begrenzung des Durchsatzes verhindert dann merkliche Performanceeinbußen. Eine Kopplung mit der CPU-Last ist nicht möglich. F-Secure Online Backup verrät nichts über eine erzielte Komprimierung, sondern meldet nur die gesicherte Datenmenge. Auch eine Deduplizierung wird nicht durchgeführt. Da aber

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

Installation/Bedienung	6
Funktionsumfang	4
Scheduler	3
Eignung im Serverumfeld	2
Dokumentation	3
Gesamtwertung (max. 50)	**18**

F-Secure
www.f-secure.com

Wie eine kleine Kiste große Freiräume schafft.

Der Stromverbrauch ihrer Rechenzentren wird für Unternehmen mehr und mehr zur Herausforderung. Nicht nur wegen der Kosten – auch das Tagesgeschäft ist zunehmend betroffen: Etwa die Hälfte aller Unternehmen mussten laut einer aktuellen Studie bereits Ausfälle durch Strom- oder Kühlungsprobleme hinnehmen.[1] Kein Wunder, dass solche Störungen zunehmend die Prioritäten in der IT diktieren – und nicht die Anforderungen des Business.

Deshalb ist die ganze Architektur des HS22 in jeder Hinsicht auf maximale Produktivität ausgerichtet: von den hocheffizienten Intel® Xeon® 5500er-Prozessoren bis hin zu ausgefeilter Management-Software wie dem IBM Systems Director, der den Stromverbrauch aktiv überwacht und begrenzt. Eingebaute Sensoren optimieren die Kühlung, basierend auf Höhe und Luftdruck. Unter dem Strich sparen Sie so im Vergleich zur vorigen Generation von Rack-Servern bis zu 93 % Energie.

Wie Sie mit Hilfe des HS22 einen Return on Investment in nur 3 Monaten[2] erzielen können, erfahren Sie unter ibm.com/blade/de

Systeme, Software und Services für einen grünen Planeten.

[1] Quelle: IDC Market Analysis #215870, Band 1, Dezember 2008, Prognose über die weltweiten Energieausgaben für Server 2008–2012. [2] Die Berechnungen für die Kapitalrendite (ROI) und Energieeinsparungen basieren auf einem 11:1-Konsolidierungsszenario von 166 Intel 1U mit 2-Socket-Servern im Vergleich zu 14 BladeCenter HS22-Servern und den daraus resultierenden Einsparungen bei Energie, Software-Lizenzen und sonstigen Betriebskosten. Tatsächliche Kosten und Einsparungen werden je nach individueller Kunden-Konfiguration und -Umgebung unterschiedlich sein. Mehr Informationen finden Sie unter www.ibm.com/smarterplanet/claims

O&M IBM IT 27/09

der Zugang keine Kapazitätsbegrenzung besitzt, spielen diese Daten für den Endanwender nur eine untergeordnete Rolle.

Letztendlich bietet F-Secure Online Backup einen preisgünstigen grundlegenden Datenschutz an, der sich in erster Linie für Arbeitsplätze und vor allem für Notebooks eignet. Anwender können so auch auf Reisen ihre wichtigen Daten vom Notebook ins Netz sichern und haben dort zumindest eine aktuelle Kopie, falls das Gerät gestohlen oder verloren wird, einen Schaden hat oder ähnliches. Optimal eignet sich das Angebot für eine kontinuierliche Sicherung der aktuellen Arbeitsdaten von Notebooks und Arbeitsplätzen. Ferner unterstützt der Dienst die Sicherung von Servern nicht offiziell. Nicht geeignet ist das Programm zudem, wenn die Rücksicherung verschiedener Versionen möglich sein muss.

Iron Mountain Digital Connected Backup for PC

Iron Mountain Digital hat sein Produkt "Connected Backup/PC" vor kurzem in "Connected Backup for PC" umbenannt, auch wenn die alte Bezeichnung noch an vielen Stellen auftaucht. Der Softwarehersteller unterscheidet zwischen einer PC- und Server-Datensicherung, wobei die von den Providern genutzte und hier vorgestellte Variante stets für die PC-Sicherung bestimmt ist. Dies wird bei der Installation auch geprüft, unter Windows 2008 Server 64 Bit ist die PC-Version aber dennoch lauffähig. Das eigentliche Server-Produkt "Connected Backup for Server" wird als komplette Lizenz für den firmeninternen Einsatz vertrieben, bei dem ein Unternehmen auch die Backup-Server betreibt, um beispielsweise die Server in Außenstellen in die Zentrale sichern zu können.

Für die Installation von Connected Backup for PC führt der erste Schritt auf die Webseite des jeweiligen Providers. Nach einer Anmeldung muss der Anwender dort einen Client herunterladen, der im Zuge des Download-Prozesses individuell konfiguriert wird. Das bedeutet, dass in dem bereitgestellten Installa-tionspaket bereits die Anmeldedaten integriert sind und während der Einrichtung nichts mehr abgefragt wird.

Connected Backup for PC eignet sich nicht nur für die Sicherung einzelner PCs, sondern auch für das Backup kleiner Arbeitsgruppen. Dazu erhält der Administrator beim Provider einen Webzugang mit einer zentralen Managementoberfläche, in der er ein oder mehrere Profile für die eigentlichen Clients anlegt. Dabei kann er zwingend zu sichernde oder auch auszuschließende Verzeichnisse vorgeben und den Sicherungsplan sowie weitere Backupregeln festlegen. Dem Anwender sind dann Grenzen bei der individuellen Clientkonfiguration vorgegeben, und der Administrator kann in einem gewissen Rahmen das Backupszenario vorbestimmen.

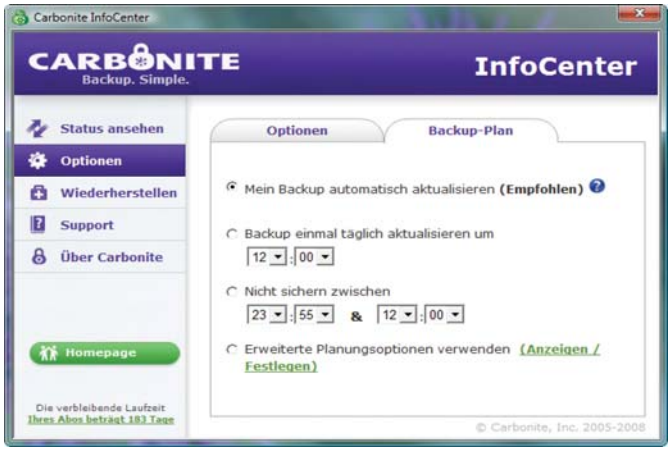


Bild 3: Carbonite orientiert sich beim Backup normalerweise an der Lastsituation des Clients, zeitgesteuerte Sicherungen sind aber trotzdem möglich

Als Desktop-Lösung konzipiert ist Connected Backup for PC nicht für die Sicherung von Datenbanken oder Mailsystemen geeignet. Insofern gibt es keine entsprechenden Sicherungsagenten und es lassen sich auch keine Start-/Stopp-Skripte hinterlegen. Beim Backup arbeitet das Tool sehr platzsparend, da es neben der Deltasicherung für Dateien eine Deduplizierung über den gesamten Datenbestand der Firma, also auch Client-übergreifend, durchführt. Identische Dateien von mehreren PCs werden also wie bei Asigra Televaulting nur einmal gesichert. Das macht sich hier allerdings in einem deutlich höheren Prüfbedarf bemerkbar. Da der Client nicht wie bei Asigra auf eine lokale Datenbank zurückgreifen kann, muss er die zu sichernden Dateien vorher mit dem Server abgleichen. Je nach Situation und Größe des Sicherungspools kann dies durch die aufwändigere Recherche relativ viel Vorlaufzeit kosten.

Aufgrund des Konzepts ist der Client funktional vergleichsweise einfach gehalten. So kann der Anwender den Backup-Zeitplan, der standardmäßig entsprechend des zentralen Profils konfiguriert ist, nur dann ändern, wenn dies laut Profil auch erlaubt ist. Bei den Sicherungsregeln werden durch den Administrator vorgegebene Regeln mit denen des Anwenders kombiniert. Bei widersprüchlichen Angaben greifen die des Administrators.

In der Tat liegt die Stärke dieser Lösung in der Sicherung von Arbeitsplätzen in Un-

So urteilt IT-Administrator (max. 10 Punkte)

Installation/Bedienung	8
Funktionsumfang	7
Scheduler	6
Eignung im Serverumfeld	4
Dokumentation	7
Gesamtwertung (max. 50)	**32**

Iron Mountain
www.ironmountain.de/digital/

ternehmen, wo ein Administrator zentrale Profile vorgeben will. Da das Werkzeug die Betriebssysteme von Servern offiziell nicht unterstützt, ermöglicht es zwar je nach Betriebssystem die Sicherung von Servern, ist hierfür allerdings nur bedingt geeignet. Zudem hat Iron Mountain Digital für die Server-Sicherung ein anderes Produkt vorgesehen. Nicht geeignet ist Connected Backup for PC, wenn auch Nicht-Windows-Clients gesichert werden sollen.

Novastor Novanet Web

Der Hersteller Novastor vermarktet mittlerweile das Produkt "NovaBackup xSP" als aktuelle Online-Backup-Software, was aber nicht bedeutet, dass die Provider auch gleich darauf umsteigen. Vielmehr ist bei diesen noch die vorherige Version Novanet Web 7 sehr verbreitet, die wir hier auch vorstellen.

Im Fokus von Novanet Web steht die Sicherung von Dateien und Verzeichnissen, für die Sicherung von Exchange und SQL-Server ist ein optionales Plugin verfügbar, teilweise auch als Novanet Web Advanced bezeichnet. Novanet Web beschränkt sich bei der Betriebssystemunterstützung ausschließlich auf Windows-Systeme, Clients für Linux und Macintosh gibt es nicht. Die Software ist übersichtlich aufgebaut und bietet diverse Einstellungen zur Einrichtung von Sicherungsjobs von mehrmals täglich bis hin zu monatlichen Backups. Weiterhin ist es möglich, eine Sicherung mit Ereignissen wie dem Systemstart, der Anmeldung oder auch freier Kapazität zu koppeln, und es lässt sich ein Backup in bestimmten Intervallen festlegen. Eine lokale Sicherung für ein schnelles Initialbackup ist allerdings nicht vorgesehen.

Um eine Sicherung einzurichten, bietet Novanet eine so genannte intelligente Auswahl an, der Administrator kann aber genauso einen individuellen Sicherungssatz über die Laufwerke und den Verzeichnisbaum auswählen. Die Sicherung von Netzwerkfreigaben ist möglich, wobei ebenso wie bei Ahsay OBM ein Zugriff über die administrativen Freigaben nicht vorgesehen ist. Somit ist bei späteren Änderungen der Freigaben Vorsicht geboten. Nicht am Client konfigurierbar ist der Rückhaltebereich (Retension-Regeln), also die Vorgabe, wie viele Sicherungen aufgehoben werden sollen. Dies muss der Administrator am Backup-Server festlegen, so dass dies mit dem Provider abzusprechen ist.

Novanet Web ermöglicht jederzeit die Änderung des Chiffrierschlüssels. Die Daten auf dem Server werden dann automatisch neu verschlüsselt, so dass stets nur der aktuelle Schlüssel gilt. Die Verschlüsselung erfolgt mit 128 Bit AES. Dazu wird entweder das Anmeldepasswort verwendet oder der Administrator legt einen eigenen Chiffrierschlüssel fest. Um dem Verlust des Schlüssels vorzubeugen, gibt es die optionale Möglichkeit, dass der Verwalter des Servers, also der Provider, die Daten trotz eines lokal festgelegten Geheimschlüssels wiederherstellen kann. Hier gilt es, das Vertrauen zum Provider und das Risiko gegeneinander abzuwägen.

Prinzipiell ermöglicht Novastor eine Mailbenachrichtigung über den Server, der Administrator sollte aber beim Provider nach-

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

Installation/Bedienung	8
Funktionsumfang	7
Scheduler	8
Eignung im Serverumfeld	7
Dokumentation	7
Gesamtwertung (max. 50)	**37**

Novastor
www.novastor.de

fragen, ob diese Funktion auch aktiviert ist. Darüber hinaus ist eine SMTP-Benachrichtigung über den Client konfigurierbar. Zur Reduzierung der Datenmenge unterstützt das Programm ein Delta-Backup, das auch bei PST-Dateien von Outlook greift. Identische Dateien in unterschiedlichen Verzeichnissen werden aber mangels Deduplizierungsfunktion mehrfach gesichert.

Abschließend können wir feststellen, dass sich Novanet Web insgesamt als recht leistungsfähig erweist. Umfassend sind die Schedulerfunktionen, die Reportdateien über erledigte Jobs sind übersichtlich und informativ. Einsetzbar ist Novanet Web nur im Windows-Umfeld, wünschenswert wäre, dass sich die Retensionregeln auch am Client konfigurieren ließen. Eine Deduplizierung könnte den Platzbedarf im Sicherungspool nochmals reduzieren. Das Werkzeug eignet sich bestens zur unabhängigen Sicherung einzelner Server und Arbeitsplätze im Windows-Umfeld. Bedingt geeignet ist das Programm für eine zentrale Sicherung vieler Systeme, da jedes einzeln administriert werden muss. Nicht eignet sich Novanet Web in heterogenen Umgebungen, in denen auch Linux- und Macintosh-Clients gesichert werden sollen.

ONbackup ISP Server

Noch nicht so lange auf dem Markt ist die Software "ONbackup ISP Server", die aber mittlerweile bei recht vielen Providern Einzug gehalten hat. Während der Clientinstallation sind relativ viele Eingaben erforderlich. Neben der Angabe der Benutzeranmeldedaten ist ein Kryptoschlüssel für die Verschlüsselung der Daten zu definieren. Eine Qualitätsanzeige wacht darüber, dass der Schlüssel ausreichend komplex ist und lässt vorher keine weiteren Schritte zu. Dann ist die Adresse des Sicherungsservers anzugeben und gegebenenfalls der zu nutzende Port. Dabei kommt zwingend eine SSL-Verbindung zum Einsatz.

Je nach Lizenz arbeitet der Client im Standard- oder Premium-Modus. Bei Letzterem kann neben den lokalen Laufwerken noch genau eine Netzwerkfreigabe mitgesichert werden, was im Vergleich der Produkte relativ restriktiv ist. Zur Einrichtung eines Backup-Jobs markiert der Administrator einfach die gewünschten Verzeichnisse – ein editierbarer Standardfilter verhindert, dass beispielsweise auch temporäre Dateien gesichert werden. Es ist auch möglich, eine Verzeichnisstruktur zu sichern, darin aber wiederum bestimmte Verzeichnisse auszuschließen. Beim Aufräumen alter Sicherungen unterscheidet der Client zwischen erfolgreichen und fehlgeschlagenen Sicherungen. Standardmäßig werden bei einem erfolgreichen Backup alle Sicherungen älter als sieben Tage gelöscht und bei einem fehlgeschlagenen älter als 14 Tage.

Relativ eingeschränkt ist der Scheduler. Entweder sichert er in Intervallen alle vier, acht, zwölf, 24 oder 48 Stunden oder an bestimmten Tagen zu einer festgelegten Uhrzeit. In der Regel sollten die Optionen aber ausreichen. Auf Wunsch verschickt der Client Benachrichtigungen per SMTP-Mail, wahlweise immer oder nur bei Fehlern beziehungsweise Warnungen. ONbackup nutzt VSS zur Sicherung offener Dateien, es lassen sich aber keine Start- und Stoppskripte aufrufen, die eine Datenbank anhalten, einen Dienst stoppen und starten oder ähnliches. Darüber hinaus verschickt der Backup-Server Mails bei durchgeführten Sicherungen sowie Wiederherstellungen und informiert bei fehlerhaften Anmeldungen. Vorteilhaft ist, dass ONbackup eine Deduplizierung unterstützt, so dass mehrfach vorhandene Dateien nur einmal gesichert werden. Bei der

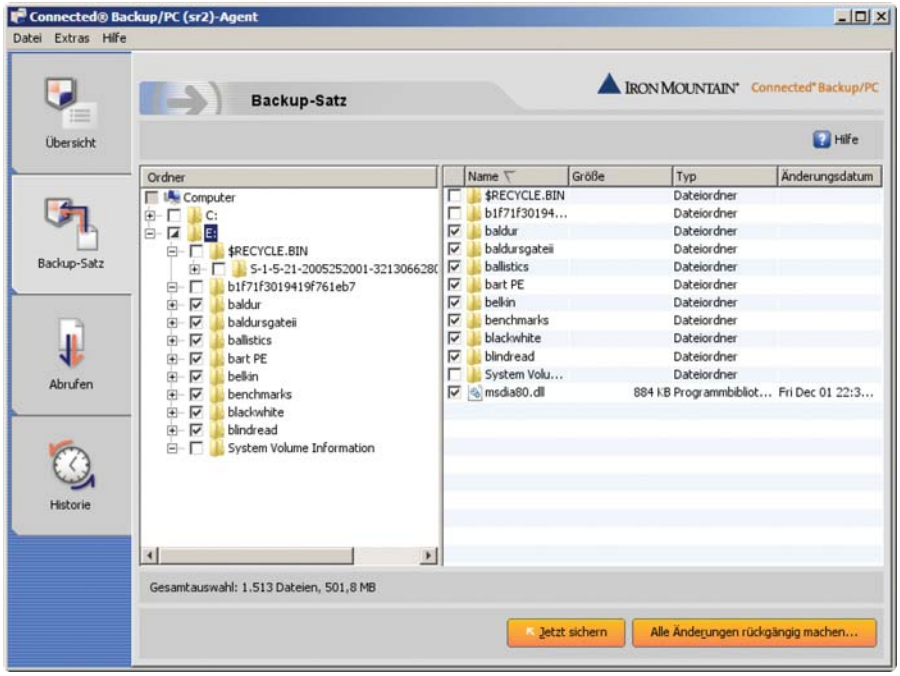


Bild 5: Recht übersichtlich ist die zentrale Benutzeroberfläche von "Connected Backup for PC" gestaltet

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

Installation/Bedienung	7
Funktionsumfang	7
Scheduler	5
Eignung im Serverumfeld	6
Dokumentation	7
Gesamtwertung (max. 50)	**32**

ONBackup
www.onbackup.de

Wiederherstellung fragt ONbackup sowohl den Account als auch den Kryptoschlüssel ab, beides lässt sich aus Sicherheitsgründen nicht speichern.

Insgesamt erweist sich ONbackup als ordentliches Sicherungswerkzeug, welches aufgrund von Deltabackup und Deduplizierung sparsam mit dem Speicherplatz umgeht. Wünschenswert sind allerdings eine umfangreichere Scheduler-Funktion und die Möglichkeit, mehr als nur eine Freigabe mitzusichern. Optimal geeignet ist das Werkzeug zur unabhängigen Sicherung einzelner Server und Arbeitsplätze im Windows-Umfeld. Bedingt geeignet ist das Programm für eine zentrale Sicherung vieler Systeme, da jedes einzeln bedient werden muss. Nicht geeignet ist die ONbackup-Lösung in heterogenen Umgebungen, wo auch Linux- und Macintosh-Clients gesichert werden sollen.

Fazit

Angesichts der vielen Angebote auf dem Markt dürfte für jeden etwas dabei sein. Allerdings ist es nicht damit getan, einfach auf den Preis zu schauen und den billigsten Anbieter zu wählen. Zwingend erforderlich ist zuerst eine eigene Bedarfsanalyse: Reicht eine einfache Sicherung oder sollen mehrere Versionen beim Provider gespeichert werden? Wie hoch ist der Umfang überhaupt? Sind Datenbanken oder Mailsysteme zu sichern? Handelt es sich nur um Windows-Clients oder auch andere Betriebssysteme? Soll das Backup dediziert auf jedem Client laufen oder soll ein Client mehrere Systeme im Netzwerk sichern? Handelt es sich um Arbeitsplätze oder Server?

Die beiden Werkzeuge von Carbonite und F-Secure bieten nur eine Grundsicherung und eignen sich nicht für den Servereinsatz. Vielmehr sind sie ideal, um zu einem sehr attraktiven Preis vor allem Notebooks mit einer Grundsicherung zu versehen. Bei einem vergleichsweise häufigen Verlust oder Defekt sind die Daten dann nicht verloren. Vorteilhaft ist, dass sich der Anwender nicht großartig um die Sicherung kümmern muss, sondern diese weitgehend automatisch läuft. Beispielsweise setzt der Autor dieses Artikels seit knapp zwei Jahren auf das Tool von Carbonite, um unter anderem die erstellten Artikel kontinuierlich zu sichern. Als vor gut einem halben Jahr plötzlich im Urlaub die Festplatte seines Notebooks ihren Geist aufgab, konnte er seine komplette Arbeit bis auf den letzten Arbeitsstand problemlos wiederherstellen.

Bei den übrigen Anbietern zeigt sich, dass die auf dem gleichen Produkt basierenden Angebote in der Regel bei geringem Kapazitätsbedarf auch ähnlich teuer sind, je höher der Bedarf ist, desto weiter spreizen sich dann die Angebote. Preislich attraktiv und funktional recht gut ausgestattet präsentieren sich die auf Ahsay Online Backup Manager basierenden Sicherungsdienste. Datenbanken werden hier ebenso unterstützt wie diverse Clientbetriebssysteme.

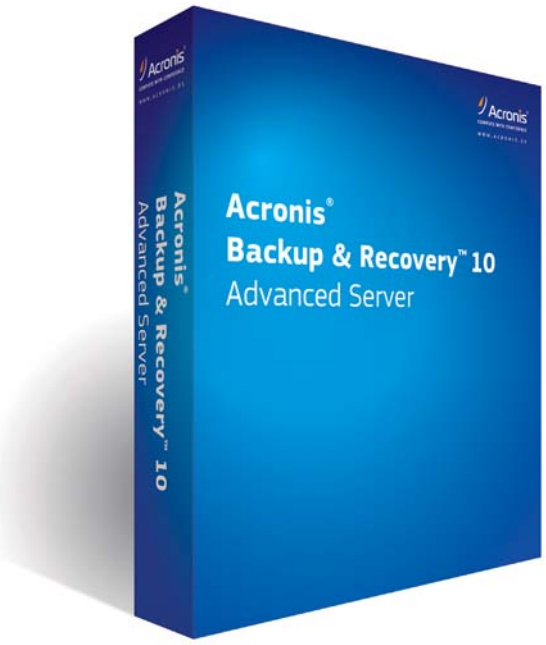
Die Software von Novastor ist beim Datenbank-Support nicht so vielseitig und auf Windows-Clients beschränkt. Anzumerken ist hier, dass die in unserer Online-Marktübersicht aufgeführten Provider noch auf das bewährte Novanet Web (Advanced) setzen, während Novastor bereits einen Nachfolger präsentiert hat. Während bei den Werkzeugen von Ahsay, ONbackup und Novastor der Fokus auf der unabhängigen Sicherung einzelner PCs oder auch Server liegt, kombiniert die Software von Iron Mountain Digital dies mit einer zentralen Administration, über die sich für alle Clients gemeinsame Profile vorgeben lassen.

Bei Asigra Televaulting liegt die Stärke in einer sehr guten Netzwerktauglichkeit zur Sicherung ganzer Arbeitsgruppen oder Domänen. Insgesamt bietet diese Software den besten Komfort und die größte Flexibilität. Allerdings äußert sich das auch in einem vergleichsweise hohen Preis bei den Providern. Die Werkzeuge von Ahsay, Asigra, Novastor und ONbackup unterscheiden nicht zwischen Server- und Workstation-Betriebssystemen. Connected Backup for PC ist nicht für den Servereinsatz gedacht, hier bietet Iron Mountain Digital ein getrenntes Produkt an.

Abschließend sei jedem empfohlen, bei Interesse am Online-Backup zuerst das Angebot vieler Provider bezüglich eines Testzugangs zu nutzen. Auf diese Weise lässt sich recht einfach ausprobieren, wie der Client arbeitet und ob die gebotenen Funktionen die eigenen Anforderungen erfüllen. *(dr)*

Im Test: Acronis Backup & Recovery 10

Mehr Kraft in Runde 10



von Sandro Lucifora

Je mehr ein Unternehmen von der Verfügbarkeit seiner Daten abhängt, desto wichtiger ist deren zeitnahe Wiederherstellung, sollte ein Rechner seinen Dienst verweigern. Mit True Image Echo hat Acronis schon Ende 2007 ein Backup-Konzept für den Einsatz in Unternehmen präsentiert. Nun startet der Hersteller mit Backup & Recovery in die zehnte Runde. Wie die Neuerungen im Einzelnen aussehen, haben wir für Sie in diesem Test herausgefunden.

Ein kurzer Blick zurück: In Ausgabe 3/2008 haben wir Acronis True Image Echo 9 vorgestellt. Der Fokus dieser Version war es, eine Gesamtlösung für das Backup im KMU-Bereich anzubieten. Insgesamt konnte das Konzept beim Praxistest überzeugen. Lediglich die Umsetzung, sprich die Software, hatte seinerzeit einigen Nachholbedarf und machte den Anschein, noch in den Kinderschuhen zu stecken. Im Lauf der Zeit hat Acronis dann über Software-Updates viele der angesprochenen Mängel beseitigt.

Wer seine gespeicherten Daten ruhigen Gewissens mit Acronis True Image Echo 9 sichert, stellt sich nun bestimmt die Frage, ob und warum er auf die neue Version umsteigen soll. Die Frage nach der Sinnhaftigkeit eines Umstiegs ist für uns die zentrale Überlegung, weshalb wir Ihnen in diesem Test einige Entscheidungshilfen dazu geben möchten.

Neues Konzept, neue Installation

Schon bei der Installation zeigt sich eine ganz neue Herangehensweise: Acronis liefert nicht mehr für jedes Modul eine eigene Installationsroutine, sondern kommt nur noch mit einer einzigen, 700 MByte großen Installationsdatei. Dahinter verbergen sich soweit alle Produkte; lediglich der Workstation-Agent ist hier noch außen vor.

Der Gedanke der Unternehmenslösung – das zentral gesteuerte Backup – hat sich bei Backup & Recovery 10 (BA 10) merklich gefestigt und ist auch in der Umsetzung wesentlich ausgereifter als noch in der 9er Version. Bei der Vorgängerversion wurden mit der rudimentären Konsolen-Lösung zwar alle Backup-Agenten über eine Oberfläche angesprochen und administriert, doch arbeiteten diese in ihrer Funktionsweise autark voneinander. Dabei kam der Groupware-Server zum Einsatz. Er erlaubte es, die einzelnen Tasks zentral zu konfigurieren, sie dann an die Agenten zu verteilen und schließlich auf den lokalen Systemen anzustoßen und abzuarbeiten.

Bei BA 10 hat sich Acronis bei dem bereits durch andere Lösungen bekannten Konzept eines Management-Servers bedient. Hierbei sind die Agenten nur noch die ausführenden Befehlsempfänger, deren komplette Funktionsweise remote durch den Management-Server gesteuert und angestoßen wird. Der zentrale Server überwacht und verteilt dabei sowohl das Zeitmanagement, den Scheduler als auch die Konfiguration. Dieses neue Konzept zwang uns, schon bei der Installation umzudenken. Acronis unterscheidet zwischen lizenzierten und lizenzfreien Komponenten. Die Lizenzierung wird zentral gemanagt, weshalb diese zuerst zu installieren ist, ist sie doch Voraussetzung für die Installation eines Lizenzproduktes. Der Lizenzserver verfügt über die aus True Image Echo bekannte Management-Konsole, mit der sich die Lizenzen für alle Geräte im Netzwerk verwalten lassen. Es ist wichtig, dass der Lizenzserver immer im Netzwerk erreichbar ist – er sollte daher

Update-Agent ohne Biss

Acronis liefert im Paket einen Update-Agenten, der die Konfiguration von Version 9 auf 10 konvertieren soll. Wir haben uns eingehend damit befasst und sind zur Erkenntnis gekommen, dass die Konvertierung nicht hilfreich ist. Das liegt nicht an einer Fehlfunktion, sondern daran, dass das gesamte Handling der Tasks und das zentrale Management sowieso eine manuelle Nacharbeit erfordern. So erscheint es uns sinnvoller, direkt alles neu anzulegen; vor allem, weil dies jetzt wesentlich komfortabler abläuft.

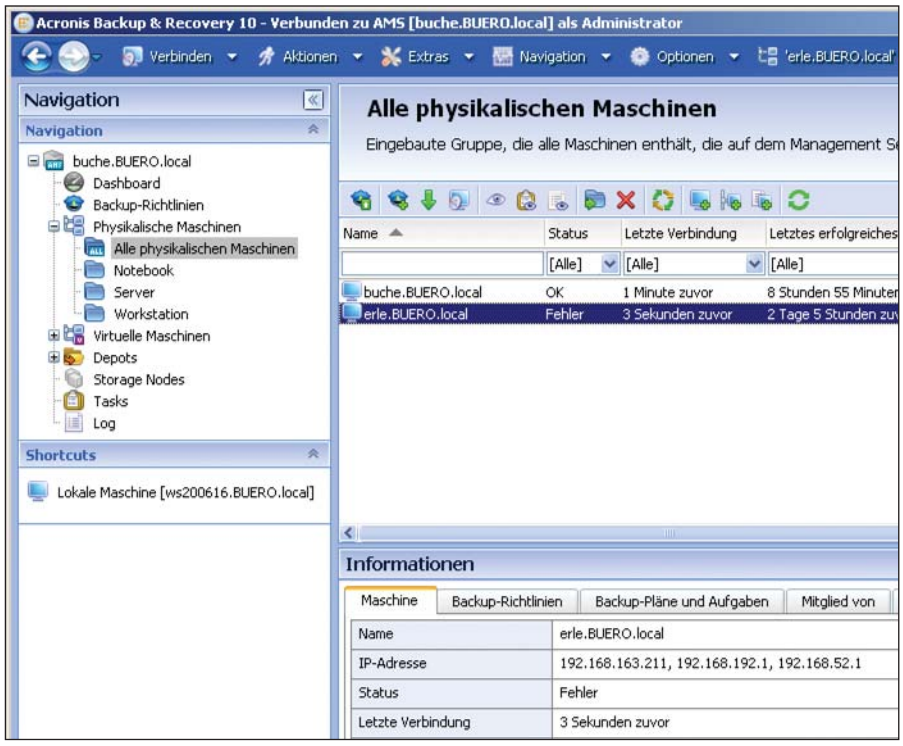


Bild 1: Die Management-Konsole dient sowohl der Administration einzelner Agenten als auch der Bedienung des Management-Servers

auf keinen Fall nur zeitweise auf einer Arbeitsstation installiert werden. Die einzelnen Acronis-Produkte prüfen nicht nur bei der Installation auf eine Lizenz, sondern auch während des laufenden Betriebs zeitweise ihre eigene Lizenzierung. Ist der Server länger nicht erreichbar, schaltet sich der entsprechende Dienst ab.

Als Nächstes installierten wir das neue Herzstück der Backup & Recovery-Lösung: Den Management-Server, der bei den Advanced-Versionen zum Einsatz kommt. Der Einsatz des Management-Servers ist nicht zwingend notwendig. Auf ihn lässt sich zum Beispiel verzichten, wenn die Backup-Software lediglich ein oder zwei Computer im Netzwerk sichern soll. Für diesen Test haben wir uns jedoch für den Einsatz des Management-Servers entschieden, da wir zwei physikalische und zwei virtuelle Server sowie drei Workstations in das Backup-Konzept mit eingebunden haben. Die Administration – sowohl des Management-Servers als auch der einzelnen Agenten – erfolgt mit der lizenzfreien Management-Konsole. Diese haben wir auf dem Arbeitsplatz des Administrators installiert. Alle weiteren Komponenten, also die Server-Dienste, können dezentral, auf unterschiedlichen Maschinen betrieben werden.

Planen Sie das Backup der einzelnen Computer möglichst zeitversetzt, sofern Sie die Images am selben Speicherort im Netzwerk ablegen. Da der Datendurchsatz begrenzt ist, lassen sich dadurch Peaks in der Datenübertragung auf den Netzwerkspeicher besser steuern und gegebenenfalls verhindern.

Vermeidung von Durchsatz-Engpässen

Die Agenten schwärmen aus

Zunächst ist die Frage zu klären, wohin die Backups zukünftig gesichert werden. Zudem müssen Sie ermitteln, ob Sie den Agenten auf mehreren Computern denselben Backup-Auftrag geben oder ob jeder Computer mit einem eigenen Backup-Task gesteuert wird. Für unseren Test nutzten wir den Backup-Speicher zentral auf einem NAS-Gerät. Um dieses zentral zu verwalten, installierten wir zusätzlich den Dienst des Backup-Servers. Die physikalischen als auch die virtuellen Server haben wir jeweils mit getrennten Jobs gesteuert, die Workstations leiteten wir zusammen in einer Gruppe mit demselben Backup-Task an. Bevor wir uns der Verwaltung zuwenden konnten, mussten wir im Netzwerk die Agenten auf den einzelnen Computern verteilen. Hierzu liefert die Management-Konsole über den Management-Server praktischerweise eine Routine zur Remote-Installation. Dabei haben wir im Test festgestellt, dass die Remote-Verteilung nicht immer funktionierte. Damit der Fernzugriff erfolgen kann, muss der Administrator prüfen, ob die lokalen Dienste COM+ und "Distributed Transaction Coordinator" gestartet sind.

Alle diese Dienste sind in der Regel mit dem Autostarttyp "manuell" versehen und werden nur bei Bedarf vom Betriebssystem gestartet. Dies funktioniert scheinbar nicht immer, und so blieb uns nur, den Dienst per Mausklick nachträglich zu starten. Ein anderer Grund für einen Fehler bei der Remote-Installation kann eine Firewall – sowohl auf dem Server als auch dem Client – sein. Eine Firewall muss den TCP-Port 9876 geöffnet haben. Trotz dieser manuellen Anpassungen gelang es uns auf einem Rechner mit Windows XP Professional SP3 nicht, den Agenten remote zu installieren. Auf den 2003- und 2008-Servern und der Vista-Workstation lief alles problemlos. So richteten wir den Agenten auf der Windows XP-Workstation mit der Setup-Routine lokal ein. Hier muss Acronis dringend nacharbeiten und die Remote-Installation fehlerfrei implementieren. Dass dies klappen kann, zeigen andere Hersteller.

Während der Agenten-Installation kommt auch der Lizenzserver zum Einsatz. Die Installationsroutine fragt beim Lizenzserver die verfügbaren Lizenzen an und prüft diese mit den auf dem Zielcomputer installierbaren Paketen. Das Ergebnis ist eine Auswahlbox der Lizenzen für Produkte, die für den jeweiligen Computer sinnvoll sind. Im Gegensatz zur Vorgängerversion ist im Rahmen der Installation sehr positiv aufgefal-

len, dass die Computer nach der Installation des Agenten nicht mehr neu gestartet werden müssen. Das ist vor allem bei der Einrichtung auf Servern und im laufenden Betrieb ein großer Pluspunkt.

Lizenz-Wirrwarr bei gebrauchten und virtuellen Maschinen

Neu in der Programm-Familie ist die Acronis Backup & Recovery 10 Advanced Server Virtual Edition. Der Unterschied zur normalen Edition ist, dass – installiert auf einem virtuellen Server wie einem VMware ESX-Server oder einem Windows Server 2008 mit Hyper-V – die betriebenen virtuellen Maschinen automatisch erkannt und als virtuelle Server in der Management-Konsole eingerichtet werden. Dies funktioniert jedoch nicht, wenn der VMware-Server als Windows-Applikation auf dem Host-Computer zum Einsatz kommt. In diesem Fall erkennt der Acronis-Agent die virtuellen Maschinen nicht selbstständig. So muss auf jeder VM der Agent nachinstalliert werden.

Obwohl lizenzrechtlich die Installation des Backup & Recovery Advanced Server mit einer Lizenz auf einer physikalischen und zusätzlich auf bis zu vier virtuellen Computern möglich ist, gelang es uns im Test nicht, dies auch so durchzuführen. Der Grund liegt darin, dass der Lizenzserver die Lizenz des Server-Agenten bei der Installation auf dem physikalischen Gerät als gebraucht markiert. Diese steht dann für eine weitere Installation nicht zur Verfügung. Als Workaround ist möglich, die Software zunächst auf den virtuellen Computern zu installieren und erst zum Schluss auf den physikalischen. Der Nachteil dabei: Ein nachträglich eingerichteter virtueller Server kann nicht mehr in das Acronis-Sicherungskonzept einfließen. Es sei denn, Sie deinstallieren den Agenten auf dem physikalischen Computer, installieren ihn in der virtuellen Maschine und dann wieder auf dem Host-System. Hier muss Acronis noch an einer verbesserten Umsetzung arbeiten.

Gruppen-basierte Jobvergabe

Sind die Agenten installiert, ist die Jobvergabe der nächste Schritt. Wie vorab schon beschrieben, lässt sich jeder Agent auch einzeln über die Management-Konsole administrieren. Wir bedienten uns im Test der Steuerung über den Management-Server. Nach der Verbindung ist der erste Punkt bei der Konfiguration das Anlegen von Gruppen. Wir haben im Test die Gruppen "Notebook" und "Workstation" eingerichtet. Jedem Server haben wir eine eigene Richtlinie zugewiesen. Der Grund dafür ist, dass im Task kein zeitversetzter Start für mehrere Agenten angegeben werden kann. Aus der True Image Echo-Sicherung haben wir gelernt, dass das gleichzeitige Sichern von mehreren Servern in einen Backup-Speicher zum Stau auf der Datenautobahn führen kann. Da wir uns für einen zentralen Speicherort entschieden haben, haben wir als Nächstes ein Speicher-Depot konfiguriert. Dieses lag im Testumfeld auf einem NAS-Gerät. Alternativ können Sie auch mehrere zentrale Depots, etwa für verschiedene Gruppen, einrichten und über den Backup-Server steuern.

Umfangreiches Regelwerk

Nun kamen wir zum Erstellen der Backup-Richtlinien. In den Standard-Optionen – der Dialog ist aus True Image Echo vertraut – lassen sich auch dazu die Grundeinstellungen festlegen. Neu hinzugekommen sind die Optionen "Bedingungen für den Task-Start" und "Task-Fehlerbehandlung". Als Bedingung für den Task zählen die Voraussetzungen, die in den Backup-Richtlinien eingerichtet sind. Ganz banal ist eine davon zum Beispiel die Erreichbarkeit des Backup-Speichers. Oftmals reicht ein Mausklick, damit die Sicherung weiterläuft. Und hier setzt die neue Option zur Steuerung der Task-Fehlerbehandlung an. Um beim Beispiel zu bleiben: Ist während der Sicherung kurzzeitig das Depot nicht verfügbar, bricht True Image Echo die Sicherung ab und wartet auf einen menschlichen Eingriff. In der Fehlerbehandlung können wir jetzt festlegen, ob, wie oft und in welchem Abstand der fehlgeschlagene Task neu gestartet wird. Zwei sinnvolle Neuerungen, die erfahrungsgemäß viel Ärger ersparen werden. Alle in den Standard-Optionen getätigten Einstellungen lassen sich bei jeder Backup-Richtlinie noch einmal individuell anpassen.

Nicht nur sind die Backup-Richtlinien selbst eine neue Errungenschaft von Backup & Recovery 10, auch diverse Task-Optionen wurden komplett neu entwickelt. So ist etwa die Auswahl der Backup-Quelle überarbeitet. Eine sinnvol-

Deduplizierung

Acronis bietet im Lizenzmodell jetzt auch die Option der Deduplizierung an. Sie hat zum Ziel, den Speicherplatz im Backup-Depot drastisch zu senken – der Hersteller spricht von bis zu 90 Prozent, was wir im Test so nicht feststellen konnten. Dies könnte aber durchaus zutreffen, wenn mehrere Systeme mit gleicher Basis, wie Betriebssystem und Software, gesichert werden. Im Groben wird als Deduplizierung der Prozess beschrieben, der mehrfach vorhandene identische Dateien nur ein Mal speichert und innerhalb des Backups darauf verweist. Hierzu gibt es verschiedene Methoden: Das "Reverse-Referencing" speichert das erste gemeinsame Element, und alle weiteren identischen verweisen auf das erste. Das "Forward-Referencing" speichert immer die zuletzt aufgetretene Datei und referenziert die vorherigen Elemente auf das neue.

Die Unterschiede dieser Methoden wirken sich auf die Performance aus, um Daten schneller zu verarbeiten respektive schneller wiederherzustellen. Die Vorgehensweisen "Inband" und "Outband" legen zudem fest, ob der Datenstrom in Echtzeit analysiert und darauf reagiert wird oder erst nachdem er am Zielort gespeichert wurde. Im ersten Fall darf beim Deduplizieren nur ein Datenstrom existieren, im zweiten können die Daten mittels mehrerer Datenströme parallel in Augenschein genommen werden. Acronis bietet bei der Integration von Deduplizierung einen weiteren Synergie-Effekt, da die regelmäßige Erstellung von Vollsicherungen den Deduplizierungsprozess noch weiter optimiert.

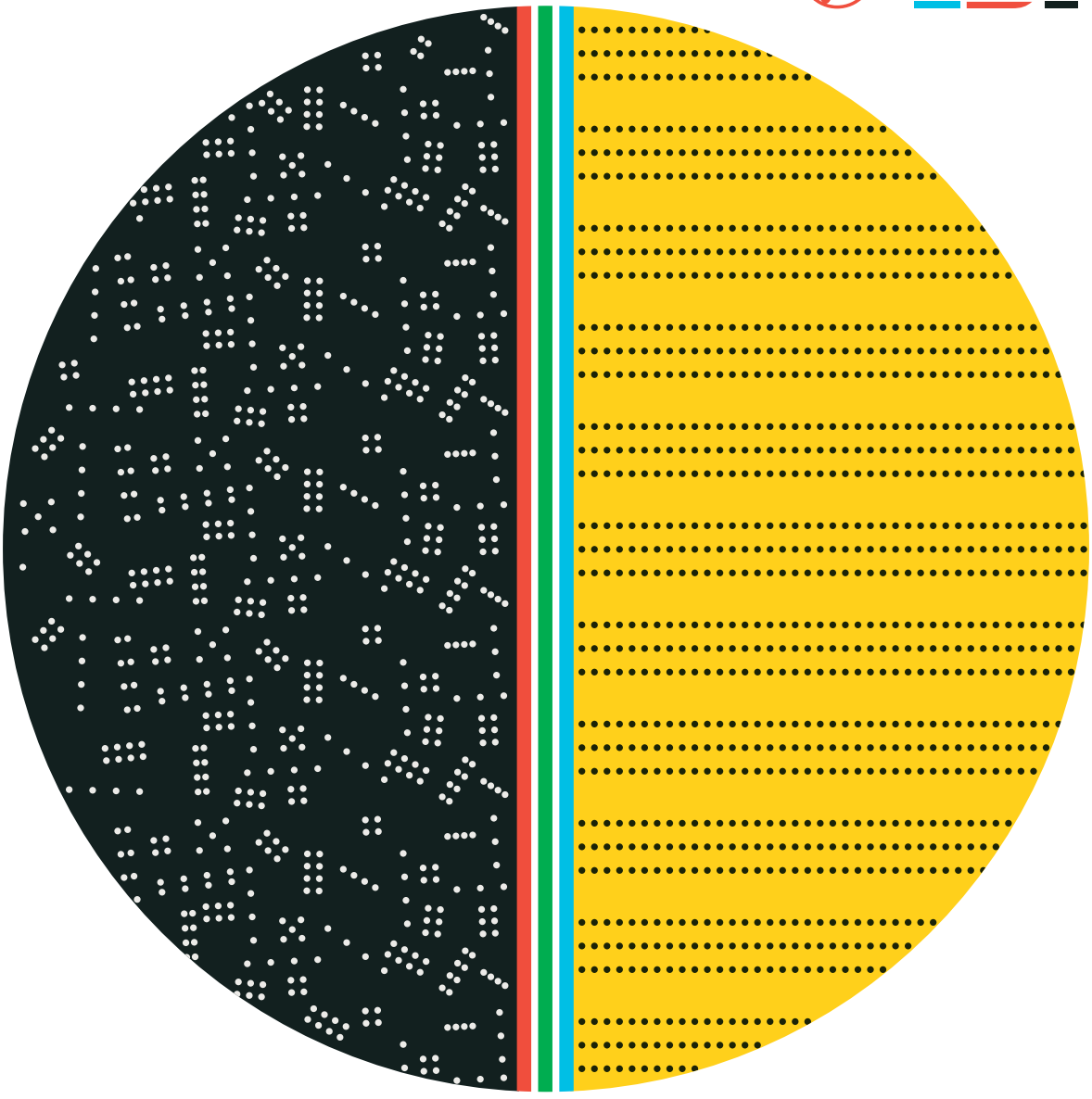
Beim Erstellen des Backups werden zuerst für inkrementelle Backups die seit der letzten Vollsicherung unveränderten Daten ermittelt und als Referenz an das Zielsystem übertragen. Damit fällt die Arbeitslast für den Deduplizierungsprozess an der Quelle lediglich für jene Dateien an, die sich geändert haben. Ergo: Die Erstellung von Komplettsicherungen nimmt wesentlich weniger Zeit in Anspruch. Voll-Backups lassen sich so in kürzeren Zyklen in den Sicherungsplan einbauen, was für die Wiederherstellung einzelner Dateien oder kompletter Systeme eine signifikante Vereinfachung bedeutet.

Intelligente Technologien für einen smarten Planeten

Wie organisiert man Dinge, die man weder sehen noch anfassen kann?

Immer mehr Unternehmen müssen feststellen, dass der virtuelle Wildwuchs neuer Systeme schnell ebenso komplex und undurchdringlich wird wie das Server-Dickicht, das man eigentlich lichten wollte. Heute hilft IBM Unternehmen mit einer breiten Palette von Lösungen dabei, sich mehr Überblick und Kontrolle über ihre virtuellen Ressourcen zu verschaffen: Server, Speicher, Anwendungen und vieles mehr. Damit können Sie virtualisierte IT-Umgebungen so weit vereinfachen und automatisieren, dass die Zuweisung und Konfiguration von Ressourcen nicht mehr Tage dauert, sondern Minuten. Unser offener Ansatz steigert die Effizienz und ermöglicht unseren Kunden Einsparungen von bis zu 30 % bei Kapital- und Betriebskosten. Sie sehen, die Zeit ist reif für Cloud Computing.

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



O&M IBM IT 29/09

le, neue Auswahl – die erst im Laufe des Tests als Update der Software hinzugekommen ist – heißt "Fixed Volumes" und ergänzt die Option "All Volumes". Diese Einstellung bewirkt, dass nur Festplatten und keine angeschlossenen Wechselmedien wie USB-Festplatten und -Sticks gesichert werden. Bei einem nachträglichen Einbau oder Austausch einer Festplatte in den Computer oder beim Ändern eines Laufwerksbuchstabens stellt diese Option sicher, dass die Partition weiterhin in der Sicherung berücksichtigt wird.

Die Auswahl des Backup-Speichers bietet neben dem zentralisierten und über den Backup-Server gemanagten Depot auch das Speichern in lokale Netzwerkordner sowie auf einen FTP- beziehungsweise SFTP-Server an. Natürlich ist die "Acronis Secure Zone" weiterhin als Option für den Speicherort verfügbar. Bei dieser Art des Backups sind die Schemen "Großvater-Vater-Sohn" und "Turm von Hanoi" neu hinzugekommen. Die letztgenannte Strategie macht nur dann Sinn, wenn Bänder oder andere Medien, die physikalisch austauschbar sind, Einsatz finden. Die Archiv-Validierung lässt sich jetzt differenzierter steuern und die Backup-Optionen – sofern Sie bei diesen Richtlinien vom Standard abweichen sollen – anpassen. Zu guter Letzt werden die Backup-Richtlinien entweder einer Gruppe oder einzelnen Maschinen zugewiesen.

Einfache Wiederherstellung im Notfall

Im Falle eines Rechner-Blackouts soll ein Backup in kürzester Zeit ein neues System zur Verfügung stellen. Es kann aber weiterhin notwendig sein, bei versehentlich gelöschten Daten lediglich einzelne Dateien wieder herzustellen. Acronis Backup & Recovery ermöglicht nach einem Datenverlust sowohl die vollständige Wiederherstellung des gesamten Systems – einen Bare Metal Restore – als auch die Wiederherstellung von individuellen Dateien und Verzeichnissen in nur wenigen Minuten. Ein Plus-Punkt stellt dabei die Systemwiederherstellung auf ein neues System mit abweichender Hardware dar, sogar in einer virtuellen Maschine. Auch die Wiederherstellung einer virtuellen Maschine auf physikalischer Hardware ist möglich. Hierzu ist jedoch die Lizenz für Universal Restore notwendig – die jederzeit nachträglich erworben werden kann, wenn sie noch nicht Bestandteil der gekauften Edition ist.

Um ein zielgerichtetes Restore eines beliebig gesicherten Computers durchzuführen, muss einmalig über die Management-Konsole ein bootfähiges Medium auf CD gebrannt werden. Diese beinhaltet alle notwendigen Komponenten, um eine vollständige Systemwiederherstellung durchzuführen. Sie benötigen zudem nur ein Medium für alle Arten der Wiederherstellung – was das Handling ungemein erleichtert. Im Test haben wir festgestellt, dass zur Wiederherstellung kein Lizenzserver und keine Lizenz für irgendein Acronis-Produkt notwendig sind. Das ist von großem Vorteil, denn auch der Lizenzserver selbst kann ausfallen.

Fazit

Zwischen True Image Echo 9 und Backup & Restore 10 liegen nicht Welten, wohl aber Länder und Kontinente. Durch die Tatsache der neuen Herangehensweise in der Administration, die gezielte Unterstützung von Wirtssystemen mit virtuellen Maschinen und die Implementierung der Deduplizierung ist die Überlegung für einen Umstieg berechtigt. Die Datensicherung selbst und die Wiederherstellung sind weiterhin so zuverlässig wie beim Vorgänger. Durch das neue Konzept des zentralen Managements sind viele Veränderungen hinzugekommen, die auch neue Fehler und Unwägbarkeiten mit sich gebracht haben. Insgesamt ist Backup & Recovery aus Admin-Sicht mit 7-Meilen-Stiefeln große Schritte vorwärts gegangen. Die Kernaufgabe der Sicherung und Wiederherstellung meistert Backup & Recovery 10 mit Bravour. *(ln)*

Die bekannten Lösungen "Acronis Recovery für Microsoft Exchange" und "Acronis Recovery für Microsoft SQL Server" sind weiterhin als Standalone-Lösungen erhältlich und sollen erst in Zukunft in das neue Management-Konzept von Backup & Recovery 10 eingebunden werden. Bis dahin lassen sich die aktuellen Lizenzen zusammen mit Backup & Recovery 10 nutzen.

Exchange- und SQL-Backup noch außen vor

Produkt
Programm zur Datensicherung und Wiederherstellung für Server und Workstation.

Hersteller
Acronis Germany GmbH
www.acronis.de

Preis
Acronis Backup & Recovery 10 für Server kostet je nach Betriebssystem zwischen 535 und 1.070 Euro.

Acronis Backup & Recovery 10 für Workstation ist je nach Edition ab 67 Euro pro Lizenz zu haben.

Weitere Zusatzfunktionen wie etwa Deduplizierung sind ab 90 Euro für Server beziehungsweise 27 Euro für Workstations erhältlich.

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

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

Installation und Konfiguration:	8
Zuverlässigkeit beim Backup	10
Handhabung bei der Rücksicherung	9
Aufwand zu Einrichtung der beteiligten Computer	7
Skalierbarkeit der Lizenzen	8

Dieses Produkt eignet sich

optimal für Netzwerk-Infrastrukturen mit Servern und Arbeitsplätzen unter Windows und auch Linux mit dem Einsatz einer Netzwerkspeicher-Lösung.

teilweise für Netzwerke mit 50 und mehr Usern.

nicht für den Schutz von Umgebungen mit hohem Datenverkehr.

Backup & Recovery 10

Im Kurztest: Pranas.Net SQLBackupAndFTP

Save it easy

von Sandro Lucifora

Zur Sicherung von Datenbanken – nicht nur in großen Netzwerken – dient SQLBackupAndFTP (SBAF) des Anbieters Pranas.Net. IT-Administrator hat das kostengünstige Werkzeug, eine MS-SQL-Server Backup-Software, die zeitgesteuerte Backups erstellt, im Kurztest unter die Lupe genommen. SBAF verpackt die Backups als ZIP und legt diese wahlweise lokal, im Netzwerk und/oder per FTP auf einem externen Server ab. Sowohl die freie als auch die Premium-Version arbeitet mit dem MS-SQL Server ab Version 2000 und MS-SQL Server Express ab 2005 zusammen. Die Premium-Version sichert dabei mehr als zwei Instanzen, versendet zusätzlich auch Status-E-Mails und verschlüsselt die ZIP-Dateien.

Die Sicherung einrichten

Die Installation zeigte sich einfach und war schnell erledigt. Nach dem ersten Start richteten wir nur noch die E-Mail-Einstellungen für den Versand der Status-E-Mails ein – und fertig. Nun baute SBAF die Verbindung zur SQL-Instanz auf. Der Zugriff erfolgt über die Windows-Authentifizierung mit abweichendem Usernamen und Passwort – je nachdem, wie die Zugriffsberechtigung auf die Instanz eingerichtet ist.

Nach der Verbindung listet die Software alle in der Instanz verfügbaren Datenbanken auf. Wir wählten "Backup all non-system databases", um auch die im Nachhinein der Instanz hinzugefügten Datenbanken zu sichern. Bei der manuellen Auswahl der Datenbanken werden nachträglich erstellte Datenbanken in der Instanz nicht automatisch gesichert und müssen ebenso manuell hinzugefügt werden. Als Ziel für die Sicherung steht neben dem lokalen Netzwerkpfad auch ein FTP-Speicher zur Verfügung – beide Sicherungsorte lassen sich zudem kombinieren. Sehr gut hat uns gefallen, dass wir je Speicherort tagesgenau festlegen konnten, über welchen Zeitraum die Historie der Sicherungsdaten aufbewahrt wird.

Backup und Restore

Jetzt mussten wir lediglich noch die Uhrzeit festlegen, zu der der Job gestartet wird, und SBAF richtete den geplanten Task unter Windows ein. An dieser Stelle fehlte uns allerdings die Möglichkeit, den Sicherungszyklus täglich oder wöchentlich beziehungsweise für einzelne Wochentage zu konfigurieren. Dies lässt sich zwar nachträglich direkt im Windows-Task vornehmen, doch werden die Einstellungen beim nächsten Speichern des Backup-Jobs wieder überschrieben. Bei Bedarf legen IT-Verantwortliche für jeden Job noch individuelle Einstellungen fest: Entspricht der User, über den der Task ausgeführt wird, nicht mit dem überein, über den der Netzwerk-Zugriff auf einen Netzwerkspeicher erfolgt, wird der User für den Netzwerkzugriff separat eingetragen. Hier legten wir auch die Komprimierungsstufe für das Packen der Sicherungsdatei fest und vergaben ein Kennwort für die Backup-Datei.

Seit der Version 3 steuert SBAF auch Remote-Backups für Datenbanken. Der Hersteller deklarierte diese Funktion bis zu unserem Test der Version 3.3.2 noch als Beta (was nach Herstellerangaben an der Skript-Funktion liegt). Bei lokalen Datenbanken verwendet die Software den Befehl *BACKUP DATABASE*, für die Remote-Steuerung jedoch T-SQL-Skripts. Hier sind noch nicht alle Funktionen implementiert und es kommt beim Backup von Datenbanken diverser ISP zu Problemen. In unserem Test sicherten wir im internen Netzwerk auf verschiedenen Servern liegende Datenbanken jedoch problemlos. Die Rücksicherung der Daten war mit ein wenig SQL-Know-how und dem Einsatz von *RESTORE DATABASE* jederzeit möglich. Alternativ bietet sich die Wiederherstellungs-Funktion des SQL Server Management Studio Express an.

Fazit

SQLBackupAndFTP bietet eine unkomplizierte und zuverlässige zeitgesteuerte Sicherung von MS SQL-Datenbanken. Über 150 Tage lief das Tool präzise und ohne dass Eingriffe notwendig waren. In der Zeit führten wir auch mehrere Rücksicherungen durch und alle Datenbanken ließen sich zu 100 Prozent wiederherstellen. Bei einer Investition von 49 US-Dollar bedarf es keiner großen Überlegung, denn nicht nur im Falle eines Server-Ausfalls, sondern auch für einen Datenbank-Umzug ist SQLBackupAndFTP die richtige Wahl.

Produkt
Software zur Sicherung von SQL-Datenbanken

Hersteller
Pranas.Net: www.sqlbackupandftp.com

Preis
Für bis zu zwei Instanzen kostenlos;
die Premium-Version kostet 49 US-Dollar

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

Handhabung	9
Usability	9
Zuverlässigkeit	10
Aufwand der Konfiguration	9
Kosten / Nutzen	9

SQLBackupAndFTP 3.3.2

Disaster Recovery-Konzepte für MS Exchange

Die Feuerwehr ist da

von Walter Steinsdorfer

Steht der Exchange-Server still, geht im Unternehmen nichts mehr: Bestellungen bei Lieferanten oder Kundenaufträge, in einigen Fällen auch Rechnungen sowie wichtige Alarmmeldungen von Gebäudeleitsystemen, werden heutzutage per E-Mail abgewickelt. Daher ist im Problemfall eine möglichst kurze Ausfallzeit der IT-Systeme, insbesondere von Exchange, geschäftskritisch. Die Verantwortlichen in der IT sind gefordert, Konzepte und Absicherungen der Infrastruktur zu entwickeln, um im Notfall Produktionsausfälle in anderen Abteilungen zu vermeiden. In diesem Workshop erläutern wir für den Exchange Server mögliche Disaster Recovery-Konzepte bei Teil- oder Totalausfall.

Grundsätzlich gilt, dass Verfügbarkeit – also die möglichst schnelle Rückkehr zu einem normalen Betrieb – je nach Anforderung auch (eine Menge) Geld kosten kann. Einige Maßnahmen lassen sich aber auch ohne oder mit nur geringem finanziellen Einsatz erreichen. Auch die Eintrittswahrscheinlichkeit von Ausfällen gilt es zu betrachten, denn für kleine Betriebe mit einer überschaubaren Infrastruktur kann es wirtschaftlich völlig unrentabel sein, alle Daten an einen anderen Standort zu übertragen, wenn der Server im Fehlerfall für einige Stunden nicht zur Verfügung stehen kann. Vor einer Konzeptentwicklung sollten Sie daher die ungefähre SLA für das E-Mailsystem und die umliegenden Komponenten kennen. Ein klärendes Gespräch mit dem Management und den anderen Abteilungen ist an dieser Stelle sinnvoll.

Exchange selbst funktioniert immer im Zusammenspiel mit einigen anderen Diensten. Ohne Internetzugang können Sie keine Kommunikation mit externen Partnern aufbauen, ohne globale Kataloge und Domänenkontroller funktionieren verschiedene Abfragen und die Zustellung von Elementen in die Postfächer nicht richtig. Ein weiterer Aspekt ist die Infrastruktur wie Switche, Verkabelung, Strom und Klimatisierung.

Datensicherung der Exchange-Server

Um zu wissen, wie Sie nach einem Ausfall möglichst rasch wieder in den Produktivbetrieb gehen , muss klar sein, welche Komponenten für den Betrieb wiederhergestellt werden müssen und wo Exchange welche Daten ablegt. Bei Exchange sind das neben den Datenbanken die IIS-Metabase und eventuell noch die Daten aus dem Programmverzeichnis.

Unter Exchange 2003 und Exchange 2007 auf Windows Server 2003 können Sie die Datensicherung mit dem integrierten NT-Backup vornehmen. Ab Exchange 2007 Service Pack 2 auf Windows Server 2008 ist die Sicherung ebenfalls mit dem integrierten Windows Server Backup möglich. Ob diese Option auch unter Exchange 2010 bestehen wird, ist derzeit leider noch offen. Die IIS-Metabase ist dabei Bestandteil des Systemstatus, lässt sich allerdings auch einzeln sichern [1]. In der Metabase sind beispielsweise die Einstellungen des virtuellen SMTP hinterlegt.

Active Directory und Domänenkontroller

Ein Teil der Exchange-Daten wird allerdings nicht direkt auf dem Exchange-Server selbst abgelegt. So sind im Active Directory in der Konfigurationspartition unter "Services, Exchange" viele Einstellungen, wie beispielsweise die Datenbanken, hinterlegt. In der Domänenpartition werden direkt am Benutzerobjekt die Beschränkungen der Mailboxgröße oder auch die E-Mailadressen gesichert. Sie müssen daher für eine umfas-

sende Disastervorsorge nicht nur eine Sicherung der Exchange-Mailboxdatenbanken und der Datenbanken für die öffentlichen Ordner vornehmen, sondern auch das Active Directory sollte regelmäßigen Datensicherungen unterzogen werden. Fällt das Active Directory aus, funktioniert auch der Exchange-Server nicht mehr. Daher ist es unter Umständen auch in kleineren Unternehmen notwendig, mehrere Domänencontroller einzusetzen.

Eine wichtiger Punkt, den Sie beachten sollten: Exchange auf einem Domänenkontroller verwendet nur den lokalen Domänekontroller beziehungsweise den lokalen globalen Katalog. Für eine möglichst ausfallsichere Lösung müssen Sie den Exchange-Server also getrennt von den Domänenkontrollern, das heißt auf einem gesonderten Rechner, installieren. Der von Exchange verwendete globale Katalog zum Erstellen des globalen Adressbuches ist im Exchange-Server nicht ausfallsicher gestaltet, ist jedoch für den regulären Betrieb nicht von Belang und lässt sich leicht händisch während des laufenden Betriebes umstellen.

Firewall und Internetprovider

Für das Disaster Recovery von Exchange müssen Sie zudem Ihre Firewall sowie die Leitung des Internetproviders betrachten: Eine Firewall einschließlich des ISA-Servers ist meistens relativ schnell wiederaufgebaut. Nehmen Sie vor allen Dingen regelmäßig eine Sicherung der Firewall-Regeln vor, dann sollten Sie auf der sicheren Seite sein.

Ein größeres Problem stellt der Internetprovider dar, der meist deutlich weniger als 99,9 Prozent Verfügbarkeit garantiert. In einem aktuellen Beispiel sind es lediglich 98 Prozent im Jahresmittel. Was auf den ersten Blick ganz gut aussieht, entpuppt sich bei näherem Hinsehen als problematisch für den reibungslosen Betrieb von Mailservern. Denn 98 Prozent Verfügbarkeit bedeutet etwas mehr als sieben Tage Ausfall im Jahr. Hier bietet sich zum Beispiel an, dass Sie an einem anderen Standort einen zweiten E-Mailserver betreiben, der in dieser Zeit die E-Mails entgegennimmt.

Installieren Sie auf diesem Server auf jeden Fall die gleichen Anti-Spam-Features und Anti-Virus-Engines wie auf dem Mailserver, der normalerweise die E-Mails empfängt. Oft versuchen Spammer, am zweiten eingetragenen MX-Server ihre Spam-Mails loszuwerden. Wenn dieser dann beim Provider steht und zum Beispiel keine Empfängerprüfung durchführt, endet dies nicht selten in einer Spamflut. Alternativ können Sie über die Einrichtung eines zweiten Providers mittels zusätzlicher Leitung oder einer Failoverlösung hin zu einer ISDN-Leitung nachdenken. Welche Lösung hier die günstigste ist, hängt natürlich stark davon ab, wie schnell der E-Mailversand wieder funktionieren soll.

Recovery von Exchange 2003

Bei einem Exchange-Server gibt es unterschiedliche Arten von Disaster: Einerseits kann der Server, also die Hardware, einen technischen Defekt erleiden, andererseits müssen wir uns mit einer kaputten oder unbeabsichtigt gelöschten Datenbank beschäftigen. Exchange 2003 hat leider nur wenige Onboard-Möglichkeiten, um hierfür Vorsorgemaßnahmen zu treffen. Die einzige Möglichkeit, um einem Hardwareschaden zu entgehen, ist das Clustering. Exchange 2003 benötigt dafür allerdings einen Shared Storage, auf dem die Datenbanken liegen. Zudem ist diese Art der Verfügbarkeitssicherstellung nur mit einer Enterprise Edition sowohl von Windows Server 2003 als auch von Exchange Server 2003 erreichbar. Vor einer defekten Datenbank schützt leider auch das nicht.

Im Folgenden zeigen wir auf, wie Sie sehr rasch von einem defekten Server wieder zu einem lauffähigen System gelangen. Am einfachsten gestaltet sich das mit einem Cold Standby-System, also ein möglichst baugleiches System, auf das Sie im Falle eines Ausfalls des Hauptsystems zurückgreifen. Im besten Fall ist in dem Cold Standby-System identische Hardware verbaut. In diesem Fall reicht es aus, den Systemstatus, die Exchange-Binaries und die Datenbanken zurückzusichern. Der Server sollte nach einem Neustart wie gewohnt laufen.

In einigen Fällen, etwa wenn zwischen der letzten erfolgreichen Datensicherung und der Wiederherstellung auf dem Cold Standby-System das Kennwort des Active Directory-Kontos des Servers geändert wurde, müssen Sie noch das Konto des Servers zurücksetzen. Führt dies nicht zum Erfolg, legen Sie auch das Computerkonto mit allen Gruppenmitgliedschaften wie vorher neu an und nehmen den restaurierten Server neu in die Domäne auf. Wenn der Rechner sich nicht an der Domäne anmelden kann, erhalten Sie im Übrigen die Fehlermeldung "Die Vertrauensstellung zur Domäne kann nicht hergestellt werden".

Sollten Sie die Exchange-Binaries nicht gesichert haben, stellen Sie die Installation wieder her, indem Sie das Setup von CD (inklusive des aktuellen Service Packs) auf der Kommandozeile mit dem Schalter "/disasterrecovery" aufrufen. Diese Art der Wiederherstellung kann, je nach Datenbankgröße, relativ lange dauern. Weil der Datenbankpfad im Active Directory hinterlegt ist, müssen auf dem Zielsystem übrigens die gleichen Partitionen bestehen wie auf dem ursprünglichen Server.

Eine interessante Möglichkeit bietet in diesem Fall das so genannte Dial-Tone-Recovery. Bei dieser Methode sichern Sie die Datenbanken nicht zurück, sondern mounten die Datebanken leer. Ab dem Zeitpunkt, zu dem die Datenbanken gemountet sind, können die Benutzer wieder arbeiten und E-Mails versenden. Die Outlook-Versionen im Cache-Mode werden zwar geleert, aber die Anwender können wieder arbeiten. In der Zwischenzeit richten Sie auf dem System eine "Recovery Storage Group" ein und sichern die Orginaldatenbank dorthin zurück. Bitte beachten Sie, dass die Datenbank als überschreibbar gekennzeichnet ist. Mit NTBackup schreiben Sie die Datenbank dann an den Orginalort zurück. Bei einer erfolgreichen Sicherung (das merken Sie daran, dass die nicht mehr benö-

tigten Transaktionsprotokolle abgeschnitten beziehungsweise gelöscht werden) sollte sich die Datenbank dann auch mounten lassen. Haben Sie auf dem Laufwerk, auf dem die kleinere Interims-Datenbank läuft, noch ausreichend Platz, passen Sie den Datenbankpfad vor dem Zurückschreiben an und legen ihn wenn möglich auf das gleiche Laufwerk.

Im nächsten Schritt dismounten Sie lediglich die beiden Datenbanken, benennen sie in die jeweils andere Datenbank um und verschieben beide an den anderen Speicherplatz. Hier zeigt sich auch der Vorteil, wenn Sie die Datenbank in der Recovery Storage Group auf das gleiche Laufwerk legen: Sie müssen in diesem Fall lediglich die Zeiger über den Speicherort anpassen. Beim Verschieben über Laufwerksgrenzen hinweg muss die Datenbank in der vollen Größe kopiert werden, was erheblich länger dauert. Nach dem Mounten der Datenbanken können die Benutzer jetzt wieder auf alle alten Inhalte zurückgreifen. Die in der Zwischenzeit aufgelaufenen Daten richten Sie durch einen Merge der Datenbank-Inhalte ohne Zutun der Benutzer ein. Klicken Sie hierzu im Exchange Systemmanager die Postfächer mit der rechten Maustaste an und wählen "Exchange Tasks". Jetzt öffnet sich ein Assistent, mit welchem Sie die Daten mittels eines "Merge" direkt in die Mailboxen zurückschreiben – bereits vorhandene E-Mails werden dabei nicht doppelt angelegt.

Die Vorteile dieser Methode liegen auf der Hand: Der Anwender muss nur einen kurzen Zeitraum warten, bis er wieder auf dem aktuellen Stand ist. Die Orginaldatenbank mittels Merge in die neu angelegte Datenbank zu überführen, dauert erheblich länger. Der Assistent verwendet MAPI für den Zugriff auf die Postfächer und das ist deutlich langsamer als das Kopieren beziehungsweise Verschieben von Files. Zudem sind etwa Abwesenheitsbenachrichtigungen und Regeln nur in der Orginaldatenbank vorhanden. Der Assistent zieht diese nicht mit um, insofern ist immer ein Dial-Tone-Recovery anzuraten.

Disaster unter Exchange 2007

Die zuvor beschriebene Methode des Dial-Tone-Restore ist auch unter Exchange 2007 und Exchange 2010 möglich. Allerdings hat Microsoft noch weitere Verfügbarkeitslösungen unter Exchange 2007 eingebaut. Neben der von Exchange 2003 bekannten Clusterlösung "Single Copy Cluster" können Sie unter Exchange 2007 noch auf die Local Continous Replication (LCR), Standby Continous Replication (SCR) und die Clusterd Continous Replication (CCR) zurückgreifen.

Wie die Namen bereits andeuten, werden bei diesen Methoden die Datenbanken komplett kopiert, inklusive aller Regeln und Abwesenheitsbenachrichtigungen der Benutzer. Bei einer LCR- oder SCR-Kopie benötigen Sie lediglich die Standard-Edition von Windows Server, bei CCR ist wegen der verwendeten Clusterkomponenten eine Enterprise Edition erforderlich. LCR erstellt eine fortlaufende lokale Kopie, SCR eine Kopie auf einem anderen Server. Bei einem Ausfall der Orginaldatenbanken können Sie die jeweiligen Kopien mounten.

Auch ein Restore ist bei Exchange 2007 jederzeit, anders als noch bei Exchange 2003, auf einen beliebigen Exchange Server 2007 in der gleichen Organisation möglich. Dieses "Database Portability" genannte Feature ermöglicht es Ihnen, falls Sie die Datenbank nicht mehr im Orginalserver mounten können, die Benutzer mittels dem Cmdlet *move-mailbox -configurationonly* auf den Ausfallserver umzuziehen. Dabei wird lediglich der Datenbankpfad im Active Directory am Benutzerobjekt angepasst. Bei der CCR-Methode erfolgt das Umschalten innerhalb von wenigen Minuten automatisch. Zudem kann bei der Verwendung von Windows Server 2008 ein sogenannter Streched Cluster erstellt werden, also ein Cluster, der sich über mehrere Subnetze erstreckt. In dieser Konfiguration ist die Exchange-Organisation dann auch gegen einen Ausfall eines Rechenzentrums abgesichert.

Alles wird anders unter Exchange 2010

Unter Exchange 2010 fehlen die in Exchange 2007 eingeführten Hochverfügbarkeitslösungen komplett. Mit Exchange 2010

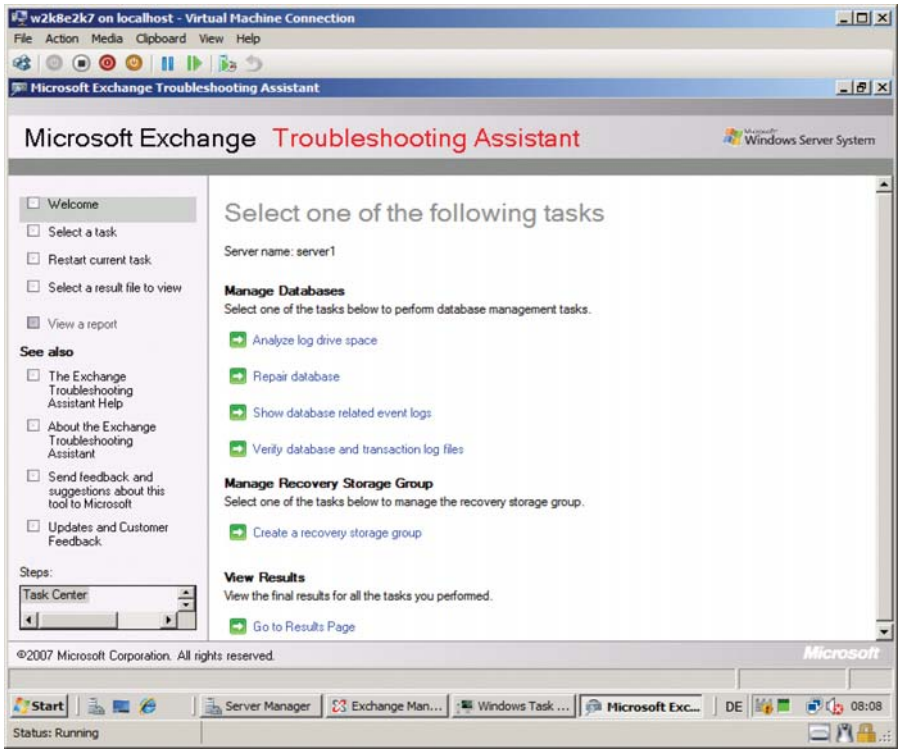


Bild 1: Der Troubleshooting-Agent von Exchange 2007 bietet unterschiedliche Notfallmaßnahmen an

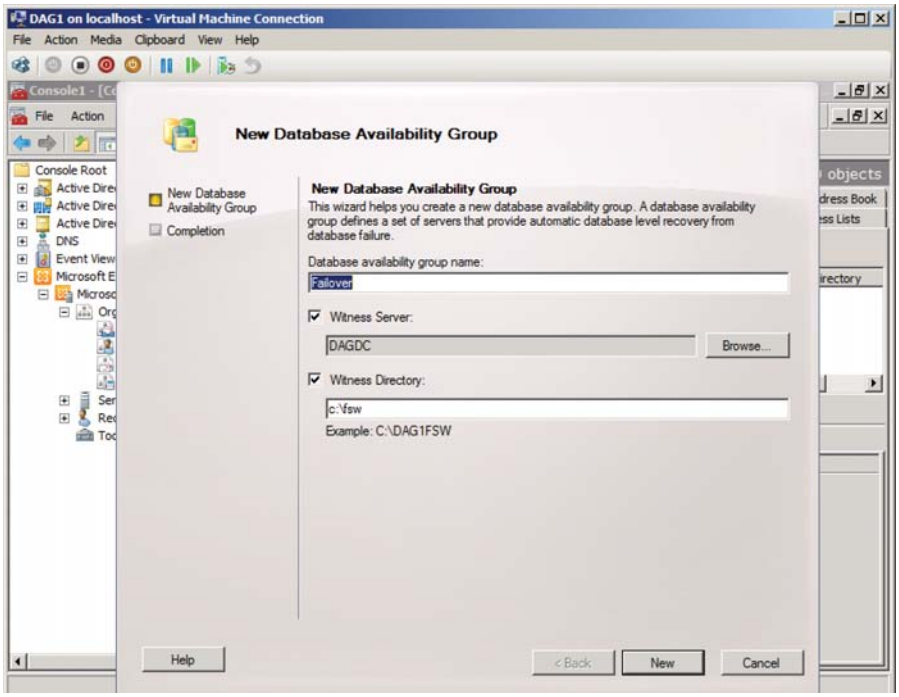


Bild 2: Die Database Availability Group (DAG) sichert Exchange 2010 gegen den Notfall

führt Microsoft dafür die Database Availability Group (DAG) neu ein. Das Konzept funktioniert ähnlich der Cluster Continous Replikation unter Exchange 2007. Einige Vorteile bietet DAG allerdings: Unter Exchange 2007 dürfen Sie in einem CCR-Cluster neben der Mailboxrolle keine weiteren Rollen installieren. Ab Exchange 2010 ist das nicht mehr der Fall, hier können alle Rollen auch auf einem geclusterten Server installiert werden. Der Nachteil sollte allerdings auch nicht verschwiegen werden: Die in einer DAG vorhandenen Mailboxserver benötigen wegen des Clusterdienstes eine Windows Server Enterprise Edition. Bei dem Ausfall eines Knotens geschieht das Umschalten auf einen anderen Knoten deutlich schneller als noch unter Exchange 2007 – Microsoft gibt hier eine Umschaltdauer von maximal 30 Sekunden an.

Mit einem DAG-Cluster können Sie dann zwar auf zwei Knoten die Client Access-Rolle installieren, über die ab Exchange 2010 neben Active Sync, Pop3 und IMAP auch die MAPI-Zugriffe erfolgen. Um jedoch die Client Access-Rolle ausfallsicher zu gestalten, ist ein NLB-Cluster notwendig. Da sich NLB-Cluster und normaler Clusterdienst auf einem Windows Server ausschließen, ist die Hochverfügbarkeit mit nur zwei Servern nicht gegeben. Eine Ausweichmöglichkeit, wenn Sie bei zwei Exchange-Knoten bleiben möchten, ist die Verwendung eines externen Loadbalancers. Ansonsten müssen Sie die Exchange-Rollen "Hub Transport" und "Client Access" wieder auslagern.

Fazit

Um möglichst schnell wieder handlungsfähig zu werden, sollten Sie die gängigsten Notfallszenarien wie Serverausfall, korrupte Datenbank oder den Datenverlust eines Mitarbeiters in einer Testumgebung durchführen. Je öfter Sie dies testen, um so eher bekommen Sie ein Gefühl dafür, wie lange im Ernstfall die Wiederherstellung wirklich dauert. Und wenn der Ernstfall vor der Tür steht, ist auch gleich weniger Nervosität vorhanden. Um in dieser hektischen Situation keine unnötigen Fehler zu begehen, sollten Sie eine ausgedruckte Notfallanleitung vorhalten, die Sie zusammen mit den wichtigsten Ersatzteilen in eine "Notfallkiste" legen. Diese sollten Sie zudem regelmäßig auf Vollständigkeit und Aktualität prüfen.

Ein Disaster trifft Sie immer unvorbereitet. Wie in diesem Artikel beschrieben, können Sie allerdings einige Vorsorgemaßnahmen treffen, um so rasch wie möglich wieder einen produktiven Betrieb herzustellen. Neben gut geschulten Mitarbeitern und einer parat liegenden Anleitung ist noch eines wichtig: Üben, üben, üben. Je häufiger ein Ausfall geprobt wird, desto schneller und besser werden die IT-Mitarbeiter bei einem tatsächlichen Ausfall reagieren. *(jp)*

Links

[1] Sicherung der IIS-Metabase
http://support.microsoft.com/kb/324277/

Die wichtigsten Neuerungen im Windows Server 2008 R2

Die Macht hinter Windows 7

von Jörg Geiger

Viele IT-Verantwortliche schauen auf Windows 7 und übersehen, dass Microsoft im Schatten des Client-Betriebssystems auch seinen Server runderneuert hat – und die wahre Macht ruht ja bekanntlich hinter dem Thron. IT-Administrator hat sich Windows 7 für Server alias Windows Server 2008 R2 vorab angesehen und stellt die zentralen Neuerungen vor.

Die strategischen IT-Entscheidungen finden heute im Backend statt. Je leistungsfähiger und flexibler die Serversysteme im Hintergrund sind, desto einfacher lassen sich Anwendungen integrieren und Benutzer verwalten – sprich, die IT-Landschaft nach den eigenen Bedürfnissen gestalten. Die Clients sind dabei meist nur Beiwerk für die Unternehmen. So ist Windows 7 zwar ständig in den Schlagzeilen, für viele Unternehmen ist aber viel wichtiger, was im Hintergrund mit Windows Server 2008 R2 passiert. Selten konnte sich Microsoft bei einem neuen Server-Release so entspannt zurücklehnen. Der Grund: Im Unterschied zu Vista ist der Windows Server 2008 ein Erfolg. So verwundert es nicht, dass der R2 im Kern eben immer noch Server 2008 ist, mit einigen Verbesserungen oben drauf. Doch die haben es in sich, denn soviel sei verraten: Microsoft hat diesmal wirklich auf die Nutzer gehört und wichtige Schrauben nachgezogen.

Zum Redaktionsschluss war der R2 noch als 180-Tage-Testversion [1] zu haben, doch im Herbst ist Microsoft mit der finalen Version durchgestartet. Die Neuheiten sind breit gestreut, viel passiert ist aber vor allem in den Bereichen Virtualisierung und Verwaltung. Und beides war längst überfällig, denn bei Virtualisierung ist VMware klarer Technologieführer und speziell beim Server-Management muss Microsoft gegen Linux punkten. Und eine weitere Zielgruppe soll der R2 erschließen – kleine Firmen ohne eigene Server-Infrastruktur und mit Teilzeit-Administratoren. Interessant im neuen Server-Release: Der R2 bietet sowohl bessere Scripting-Funktionen als auch aufgebohrte grafische Frontends. Microsoft arbeitet also an den Schwächen und ruht sich nicht auf den Stärken aus. Außerdem hat der R2 noch ein paar interessante Detailverbesserungen an Bord, etwa Stromsparfunktionen oder ein feineres Rollenkonzept.

Höhere Anforderungen, schnellerer Einstieg

Die Hardware-Voraussetzungen schraubt R2 nach oben: Microsoft kappt mit dieser Version die letzten Leinen in die 32-Bit-Welt, denn R2 wird es nur noch als 64-Bit-Variante geben. Wer auf den R2 setzt, muss ältere Hardware also tauschen. Doch es gibt auch Vorteile für Unternehmen: So stehen Ihnen schon in der Standardversion bis zu 32 GByte RAM zur Verfügung. Sollte Ihnen das nicht ausreichen, können Sie mit der Datacenter Edition bis zu 2 TByte Arbeitsspeicher adressieren. Außerdem lassen sich bei der Installation bis zu 256 logische Prozessoren ansprechen. Doch wie viel Hardware muss es mindestens sein? Microsoft schlägt eine 2 GHz-CPU vor, dazu 2 GByte RAM. So pauschal kann das natürlich nicht für alle Einsatzzwecke passen, denn ein Webserver mit viel Last kann sicher mehr Speicher gebrauchen als ein Fax-Server, der nur sporadisch genutzt wird. Eine gute Strategie ist es, bei der Anschaffung neuer Hardware einen gewissen Puffer einzuplanen. Ab 4 GByte RAM pro Maschine wird R2 richtig interessant – vor allem, weil es mit Hyper-V kein Problem ist, auch mehrere Server parallel auf einer Maschine zu betreiben. Gut: Bei der Installation übernimmt R2 das Rollenkonzept von Windows Server 2008. Je nach Einsatzgebiet lässt sich der Server passend konfigurieren. Und es war nie einfacher, einen Windows-Server zu installieren, denn es sind nur wenige Mausklicks nötig, um etwa die Sprache einzustellen und die Partition für das Betriebssystem auszuwählen.

Wie bei Vista und Windows 7 installiert sich das System danach alleine, ohne nervige Zwischenfragen und nur mit einem Neustart. Nach rund einer halben Stunde ist das System aufgespielt. Der Server ist direkt nach der Installation ordentlich vorkonfiguriert und die Firewall eingeschaltet. Rollen oder Funktionen sind dabei keine installiert und nur die notwendigsten Dienste laufen. Erst jetzt kommt der erste Unterschied zwischen Client- und Server-Betriebssystem: Administratoren führt der nächste Weg direkt in den Server Manager, um die passenden Rollen hinzuzufügen: Das kann Virtualisierung mit Hyper-V genauso sein wie DHCP- oder Webserver. Insgesamt bietet R2 17 verschiedene Rollen an, die sich aber je nach Edition unterscheiden [2]. Speziell bei den Internet Information Services, aktuell ist Version 7.5, hat Microsoft nachgelegt. Wichtigste Neuheit: Der Webserver lässt sich auch auf Server Core installieren. Das ging zwar auch mit Umwegen beim Vorgänger, doch fehl-

ten dann Funktionen wie ASP.NET an allen Ecken und Enden. Wer keinen grafischen Overhead wünscht, kann so den Webserver mit R2 schön schlank halten. Denn schlank ist gut, aber das soll ja nicht wieder heißen ohne die nötigen Features. Und das heißt es auch nicht, denn im Unterschied zum Vorgänger ist es beim R2 möglich, Server Core mit ASP.NET zu kombinieren. Der Vorteil: Web-Applikationen können das .NET Framework nutzen. Auch verschiedene Versionen des Frameworks lassen sich dabei parallel betreiben.

Virtualisierung 1.0 mit Hyper-V 2.0

Spannend ist auch die neue Version von Hyper-V, Microsofts Virtualisierungskomponente. Mit Hyper-V 2.0 rückt Microsoft der Konkurrenz rund um VMware enger auf die Pelle, wenn auch mit Funktionen, die der Marktführer bereits beherrscht. Lang ersehnt beherrscht der Windows Server 2008 R2 nun die Live-Migration zwischen zwei virtuellen Maschinen. Muss etwa ein Server gepatcht werden, dann lässt er sich mit wenigen Mausklicks aus einer virtuellen Maschine in eine andere VM umziehen. Die erste Instanz läuft weiter, die zweite wird gepatcht. So lassen sich gezielt Downtimes reduzieren, denn der Server läuft während des Umzugs weiter. Das Besondere daran ist, dass die Benutzer, die etwa mit einer Applikation auf dem Server arbeiten, der umgezogen wird, nicht getrennt werden und auch Dienste laufen weiter. Die Technik dahinter ist neu: R2 nutzt für den Live-Umzug sogenannte Cluster Shared Volumes (CSV), die ohne spezielles Cluster-Filesystem funktionieren.

Der Clou dabei ist, dass mehrere virtuelle Umgebungen im Cluster (Nodes) auf einen gemeinsamen Speicher zugreifen, auf dem die verwendeten virtuellen Festplatten als VHD-Dateien liegen. Fällt jetzt eine virtuelle Umgebung aus, kann einfach einer anderen Maschine der Zugriff auf die VHD-Datei gewährt werden. Das Besondere daran ist, dass für CSV kein spezielles Cluster-Dateisystem nötig ist, sondern das bekannte NTFS verwendet wird. Damit

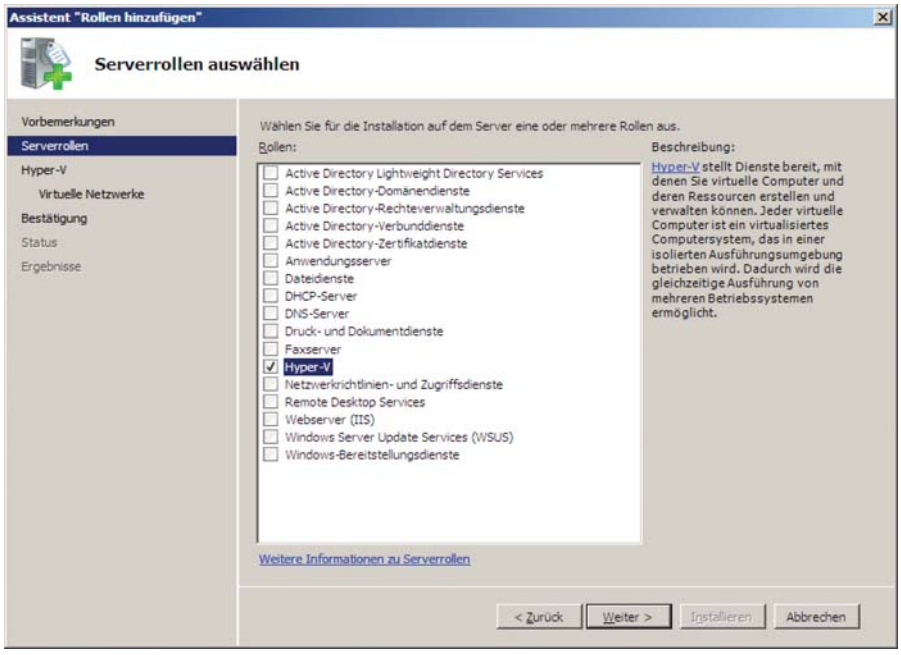


Bild 1: Hyper-V, der von Microsoft entwickelte Hypervisor, ist im R2 in neuer Version 2.0 dabei

sich VMs im laufenden Betrieb migrieren lassen, muss zusätzlich die Rolle Failovercluster installiert sein, die es erst ab R2 Enterprise gibt. Doch wer sich jetzt schon auf das fröhliche Hin- und Herschieben der VMs freut, der sollte auch die Einschränkungen kennen: So ist immer nur eine Live-Migration möglich, paralleles Verschieben klappt nicht. Außerdem muss die CPU-Architektur aus der gleichen Prozessorfamilie stammen. Wer also von AMD auf Intel umziehen will, hat Pech. In den seltensten Fällen setzen Firmen komplett auf physikalische oder virtuelle Server-Systeme, in der Praxis kommt meist eine Mischung aus beiden Welten zum Einsatz. Microsoft liefert im R2 eine verbesserte Management-Konsole für Hyper-V, in der die täglichen Verwaltungsaufgaben übersichtlich zusammengefasst sind. Die Konsole integriert sich dabei in den Server-Manager, so dass Admins eine Sicht auf alle Server haben, egal ob dahinter physikalische oder virtuelle Maschinen stecken.

Nettes Detail: Auch bei der Bereitstellung von Speicherplatz für virtuelle Maschinen hat Microsoft nachgebessert. VHD-Dateien lassen sich über den virtuellen SCSI-Controller ohne Neustart anschließen und entfernen. Das bringt mehr Flexibilität bei der Konfiguration von VMs. Falls Sie bei Server 2008 noch skeptisch waren, ob Hyper-V auch die nötige Performance bringt, sollten Sie sich Hyper-V im R2 ansehen. So findet nun die Second Level Address Translation (SLAT) Unterstützung. Dahinter steckt eine Technik, die neue Funktionen in aktuellen Prozessoren nutzt, um die Arbeitsbelastung des Hypervisors beim RAM-Zugriff so gering wie möglich zu halten. Hyper-V 2.0 kann außerdem flotter im Netzwerk unterwegs sein als der Vorgänger, denn es unterstützt jetzt Funktionen, die bisher physikalischen Installationen vorbehalten waren. Damit das virtuelle Netzwerk nicht zum Flaschenhals wird, nutzt Windows Server 2008 R2 TCP-IP-Offload und Jumbo Frames. Beim TCP-IP-Offload lagert die virtuelle Netzwerkkarte Arbeit an die tatsächlich verbauten Netzwerk- Interfaces im Server aus. Das reduziert die CPU-Last. Jumbo Frames bringen vor allem dann Vorteile, wenn große Dateien über das Netzwerk fließen.

Virtuelle Desktops

Virtuelle Desktops gehen im Vergleich zur Präsentationsvirtualisierung noch einen Schritt weiter und bilden nach virtualisierten Servern die nächste logische Stufe für Unternehmen. Statt den Zugriff auf

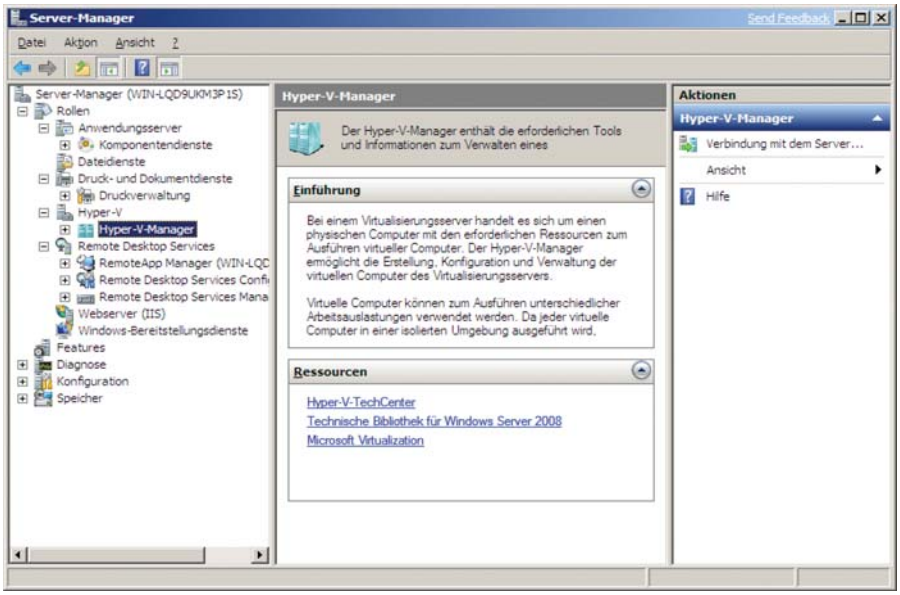


Bild 2: Virtuelle Server tauchen standardmäßig im Server-Manager auf und können wie physikalische Installationen verwaltet werden

einzelne Anwendungen per Netzwerk zu erlauben, stellt die Virtual Desktop Infrastructure komplette Arbeitsplatzumgebungen bereit. Der R2 liefert dafür einen VDI-Connection-Broker mit, mit dem Sie einen Pool von virtuellen Maschinen bestimmten Nutzern zuordnen können. Die Speicherung der kompletten Windows Arbeitsumgebung sowie deren Ausführung und das Management erfolgen dabei im Rechenzentrum. Der Client greift dann über das Netzwerk auf diese Umgebung zu. Vor dem PC sieht es so aus, als ob es sich um einen lokal laufenden Desktop handelt. In Wirklichkeit findet aber ein Fernzugriff auf die virtuelle Umgebung im Rechenzentrum statt. Die Desktopvirtualisierung profitiert dabei von neuen Funktionen, wie einer verbesserten personalisierten Verwaltung. So lassen sich etwa lokal am Computer angeschlossene Headsets für VoIP-Anwendungen nutzen.

Aufgebohrtes Management

Nicht nur der Server-Manager entdeckt seine Remote-Fähigkeiten, auch die neue PowerShell 2.0 legt bei der Fernwartung nach. Skripte und Cmdlets lassen sich jetzt auch auf entfernten Computern ausführen. Aber auch wer nicht auf der Kommandozeile zuhause ist, soll die PowerShell nutzen können. Es gibt jetzt eine grafische Oberfläche mit Syntax-Highlighting und Script-Debugger. Dabei können Sie Skripte auf einem oder mehreren Servern gleichzeitig starten. Rund 240 vorgefertigte Cmdlets sind bereits beim R2 dabei. Auch mehrere Administratoren können gleichzeitig via PowerShell auf einem Server arbeiten.

Was der PowerShell recht ist, ist dem Server-Manager billig. Wer grafische Werkzeuge bevorzugt, kann das Remote-Management auch über die zentralen Verwaltungskomponenten im R2 erledigen. In dieser Administrations-Zentrale fasst Windows Server 2008 R2 neue Verwaltungskonsolen speziell auch für Remote-Verwaltungsaufgaben über alle Serverrollen hinweg zusammen. So verwalten Sie etwa mit dem IIS-Manager-Modul einen Webserver aus dem Server-Manager heraus. Daneben hat Microsoft die Active Directory Domain Services sowie die Active Directory Federated Services gründlich überarbeitet. So können etwa gelöschte Domain-Objekte wieder restauriert werden. Computer lassen sich dabei auch offline zu einer neuen Domäne hinzufügen, was einen nervigen Stolperstein beim Deployment eliminiert. Auch das Passwort-Management für Service-Accounts vereinfacht Windows Server 2008 R2. Bisher war es ein Problem, wenn ein Passwort für einen Service-Account geändert wurde, denn alle laufenden Dienste mussten neu gestartet werden. Jetzt geht das auch ohne Neustart. Über die neue Funktion "Managed Service Account" lassen sich neue Passwörter automatisch mit laufenden Diensten abgleichen. Das Active Directory Administrative Center soll jetzt auch uner-

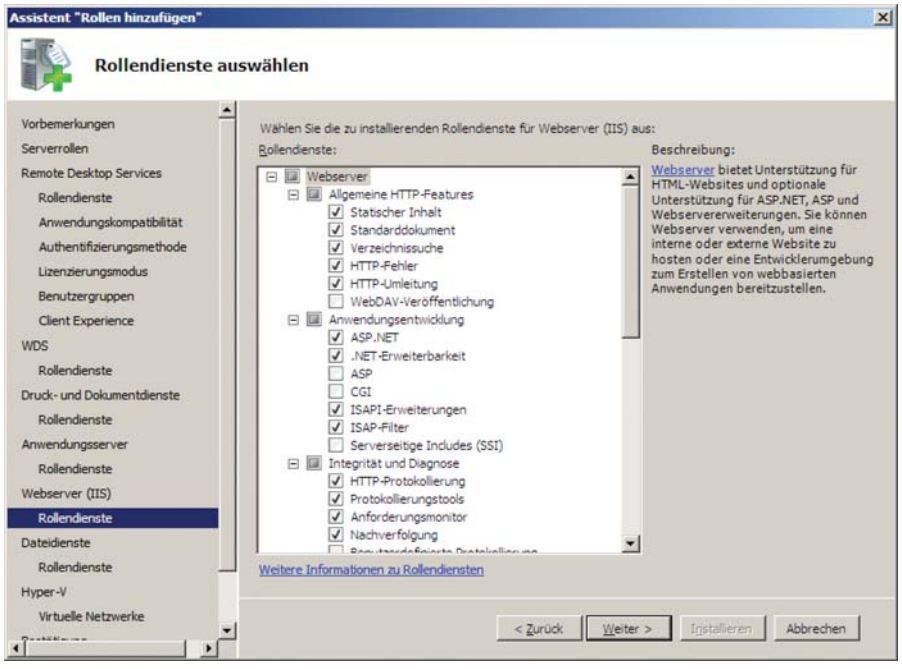


Bild 3: Windows Server 2008 R2 gefällt durch feinere Einstellungsmöglichkeiten für Rollen

fahrenen Administratoren besser unter die Arme greifen. Die Funktionen rund um das Active Directory werden deshalb aufgabenbasiert angeboten.

Grüner Server

Windows Server 2008 bietet bisher eine "ausgewogene" Energiesparrichtlinie an. Diese überwacht den Auslastungsgrad der Prozessoren des Servers und passt die Prozessor-Performance-Zustände daran dynamisch an, um den Stromverbrauch zu begrenzen, der für das Arbeitsaufkommen erforderlich ist. Windows Server 2008 R2 setzt auf diese Stromsparfunktionen Core Parking auf. Diese Funktion erlaubt es, das relative Arbeitsaufkommen jedes logischen Prozessorkerns im Verhältnis zu allen Kernen des Servers konstant zu verfolgen. Kerne, die nicht vollständig ausgelastet sind, können in einen Schlafmodus versetzt werden, bis ihre Leistung wieder benötigt wird. Diese Fähigkeit bedeutet zum Beispiel, dass ein Server mit 16 Kernen bei leichtem Arbeitsaufkommen zu einem Server mit vier Kernen werden kann. Steigt die Last wieder an, schalten sich die anderen Kerne wieder zu, so dass weitere CPU-Leistung binnen Millisekunden zur Verfügung steht.

Doch R2 kann nicht nur das Arbeitsverhältnis der einzelnen Kerne untereinander beeinflussen, sondern auch die Taktung für jeden Kern einzeln justieren. Über den ACPI-P-Status lässt sich die Leistung bei Bedarf auf bis zu 50 Prozent reduzieren. Den P-Status stellen Sie dabei bequem über eine Active Directory-Gruppenrichtlinie ein. Zusätzlich erlaubt es Windows Server 2008 R2 Administratoren, aktive Energierichtlinien zu entwerfen. Diese drosseln die Server unter Verwendung von DMTF-konformen Schnittstellen zur Remoteverwaltung außerhalb von Geschäftszeiten automatisch herunter. R2 kann außerdem aus einem Storage Area Network gebootet werden. Auf diese Weise lassen sich stromsparende Server ohne eigene Festplatte aufsetzen.

IIS 7.5 bringt zahlreiche Neuerungen

Neu sind auch die Internet Information Services 7.5 (IIS). IIS lässt sich jetzt auch auf Server Core nutzen, was die Plattform zu einem schlankeren Fundament für Web- und Applikationsserver macht. Wie in den Vorgängerversionen können Sie die Basisfunktionalität von IIS durch Extensions ge-

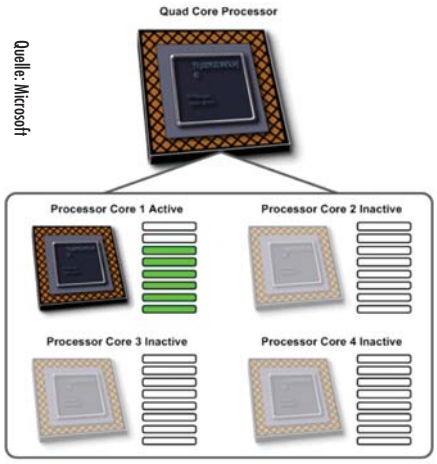


Bild 4: Core Parking verteilt die Rechenleistung so, dass möglichst wenig Prozessorkerne in Betrieb sind

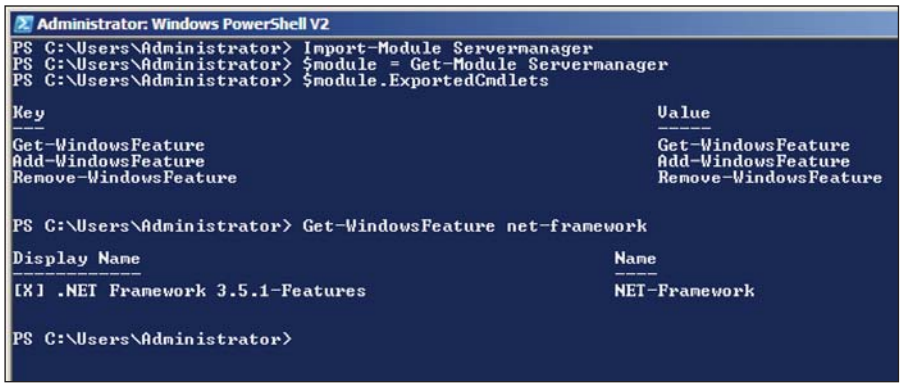


Bild 5: Die erweiterte PowerShell macht es Administratoren leichter, Windows zentral über die Kommandozeile zu verwalten

zielt erweitern. Neu ist jedoch, dass einige Erweiterungen schon in die IIS-7.5-Plattform selbst integriert wurden. Hier sind vor allem Funktionen zur Veröffentlichung von Inhalten zu nennen. So gehört etwa die WebDAV-Extension bereits zum Lieferumfang in Windows Server 2008 R2. Neu ist auch der eingebaute FTP-Server. Dieser ist vollständig in die Konfigurations- und Verwaltungs-Tools von IIS 7.5 integriert und gestattet sichere Übertragungen via FTP-over-SSL. Außerdem gut: Der neue FTP-Server erlaubt die Vergabe von virtuellen Hostnamen. Auf diese Weise können sich unterschiedliche FTP-Sites eine IP-Adresse teilen. Zu Analysezwecken gibt es jetzt auch erweiterte Logging-Mechanismen für FTP-Datentraffic. So können Administratoren auch beim Troubleshooting Zeit sparen.

Eine neue Installationsoption in Windows Server 2008 R2 erlaubt es außerdem, das .NET-Framework unter Server Core zu nutzen. Ein wichtiges Detail, denn für Webanwendungen bedeutet das, dass sich der komplette Funktionsumfang von ASP.NET nutzen lässt. Aber auch für die Verwaltung von Webservern ergibt sich daraus ein großer Vorteil: So können Administratoren IIS-Installationen auf Server Core Remote via Server-Manager oder PowerShell verwalten. Nette Dreingabe: IIS 7.5 kann parallel unterschiedliche Versionen des .NET-Framework für Webapplikationen verwenden.

Im neuen Windows-Server ist das bekannte IIS Administration Pack bereits integriert. Der aktualisierte IIS-Manager steht jetzt auch als Teil des Server-Manager-Verwaltungstools bereit. So arbeiten Administratoren mit nur einem Management-Tool und haben dabei alle Rollen im Griff. IIS-Manager selbst hat auch neue Module zu bieten. So lassen sich etwa Einstellungen zu FastCGI in einem eigenen Modul ohne Umwege konfigurieren – in den Vorgängerversionen waren diese Konfigurationsdetails noch versteckt. Sehr übersichtlich sind auch die Einstellungen zu ASP.NET in einer eigenen Komponente zusammengefasst. Fein-Tuning-Maßnahmen am IIS 7.5 können Sie zusätzlich über den Configuration Editor vornehmen. Dieses grafische Werkzeug hilft Ihnen bei der Zusammenstellung einer Webserver-Konfiguration und erzeugt automatisch aus den vorgenommenen Einstellungen Konfigurationsskripte, die für andere Server verwendet werden können. Bei Filterregeln, etwa für das Request-Filtering, integriert R2 die Funktionen des Security-Tools URLScan; auch hier stecken also in den IIS 7.5 deutlich mehr Funktionen als in der Vorgängerversion. So lässt sich festlegen, welche HTTP-Anfragen von den Internet Information Services bearbeitet werden dürfen und welche nicht.

Zur einfacheren Verwaltung trägt auch der neue Windows PowerShell-Provider für IIS bei. Dahinter verbirgt sich ein Snap-In für die PowerShell, das es ermöglicht, über eine Reihe aufgabenorientierter Cmdlets eine weit reichende Automatisierung der gängigen Webverwaltungsaufgaben auszuführen.

Troubleshooting-Tools

Trotzdem ist nicht zu erwarten, dass es mit dem R2 keine Server-Probleme mehr gibt. Läuft etwas schief, liefert der Windows Server 2008 R2 viele Informationen für die Fehlersuche. So gibt es etwa eine erweiterte Konfigurationsprotokollierung, die unabhängig vom verwendeten Tool alle Änderungen an Webserver und den Applikationen erfasst. Neu ist auch die Änderungsnachverfolgung. Damit lässt sich genau nachvollziehen, welche Änderungen am System welche Effekte auf dem Server ausgelöst haben. Außerdem prüft auf Wunsch der Best Practice Analyzer (BPA) die getroffenen Konfigurationseinstellungen für den Webserver. Der BPA steht für Analysen via Server-Manager und PowerShell bereit. Ein Schmankerl bietet der neue IIS auch für PHP-Entwickler: Fehlern im PHP-Code kommen Entwickler mit dem Failed Request Tracing jetzt leichter auf die Schliche. Dabei werden gezielt IIS-Trace-Calls in die Web-Applikation eingebaut. Der Vorteil dabei: Developer sparen sich den Aufwand für zusätzlichen Debug-Code.

Fazit

Mit dem Windows Server 2008 R2 hat Microsoft etliche interessante Neuerungen für den Admin eingeführt. Diese erlauben beim Aufsetzen und Verwalten von Infrastrukturen mehr Flexibilität und machen zugleich den etablierten Virtualisierungsanbietern Konkurrenz. Zusammen mit Windows 7 steht Unternehmen so ein Betriebssystem-Duo zur Verfügung, das den relativen Misserfolg von Vista in Firmen schnell vergessen lassen dürfte. *(dr)*

Links

[1] Windows Server 2008 R2 RC testen
www.microsoft.com/germany/windowsserver2008r2

[2] Rollenvergleich der R2-Editionen
www.microsoft.com/windowsserver2008/en/us/r2-compare-roles.aspx

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/

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 1109

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

Gemeinsame Benutzerverwaltung in Windows- und Linux-Netzwerken (1)

Handschlag zwischen den Welten

von Thorsten Scherf

Einheitliche Benutzerkonten in gemischten Windows- und Linux-Netzwerken – für viele Administratoren noch immer nur ein Traum. Eine entsprechende Konfiguration scheint oftmals zu schwierig und mit zu vielen Klippen und Hürden verbunden. Dass dies nicht sein muss, zeigt der erste Teil unserer Workshopserie zum Thema Benutzerverwaltung in heterogenen Netzwerken.

Heutige Computerlandschaften bestehen so gut wie immer aus einem Mix verschiedener Systeme. Historisch gewachsen ist dabei oftmals eine Microsoft-Struktur zum Verwalten von Benutzerkonten. Für gewisse Infrastruktursysteme, wie beispielsweise Web- oder Mailserver, kommen jedoch oftmals Linux-Systeme zum Einsatz. Sogar auf dem Desktop nimmt das freie Betriebssystem dem Konkurrenten aus Redmond immer mehr Marktanteile ab. Gerade in öffentlichen Verwaltungen finden sich in letzter Zeit immer mehr Linux-Desktops auf den Schreibtischen der Mitarbeiter wieder. Oft ist es so, dass getrennte Authentifizierungsdienste für die einzelnen Umgebungen entstehen. So kommt in der Windows-Welt ein Active-Directory oder ein NT-Domänencontroller für die Authentifizierung der Benutzer zum Einsatz, in der Unix- und Linux-Welt ein LDAP- oder NIS-Server.

Das Problem hierbei ist immer das gleiche: Die Benutzerkonten und Passwörter sind zwischen den einzelnen Authentifizierungsdiensten synchron zu halten, schließlich möchten Benutzer sich mit dem gleichen Namen und Passwort an allen Systemen anmelden können. Dies stellt in der Praxis jedoch einen großen administrativen Aufwand dar. Was liegt also näher, als die Verwaltung der Benutzerinformationen nur noch über einen einzelnen Dienst abzuwickeln. Dies ist jedoch leichter gesagt als getan, schließlich kommen in den beiden Welten unterschiedliche Protokolle und Methoden zur Authentifizierung von Benutzern zum Einsatz.

So verstehen sich die unterschiedlichen Protokolle

Microsoft setzte in den ersten Server-Versionen von Windows das sogenannte NTLM-Protokoll (NT LAN Manager) ein. Mit Windows 2000 hat Kerberos Einzug in die Active-Directory (AD) Umgebung gefunden. Dieses Protokoll gilt nicht nur als wesentlich sicherer als NTLM, sondern es bietet zusätzlich echtes Single-Sign-On (SSO). Benutzerkonten verwaltet AD in einem replizierten LDAP-Verzeichnis. Sowohl Kerberos als auch LDAP sind standardisierte Protokolle und somit auch in der Unix- und Linux-Welt bekannt. Trotzdem funktioniert die Authentifizierung hier ein wenig anders. Im Vergelich zu Windows stellt Linux ein wesentlich flexibleres System zur Authentifizierung von Benutzern bereit. So gibt es einmal den sogenannten "Name Service Switch" (NSS) [1]. Dessen primäre Aufgabe besteht in der Bereitstellung von Benutzer- und Gruppeninformationen.

Auf der anderen Seite kümmern sich die "Pluggable Authentication Modules" (PAM) [2] um die Authentifizierung und Autorisierung von Benutzern. Sowohl NSS wie auch PAM können mit unterschiedlichen Backend-Systemen arbeiten. Das heißt, der Name Service Switch kann seine Benutzerinformationen sowohl aus einer lokalen Datei wie beispielsweise */etc/passwd* beziehen oder aber einen LDAP-Verzeichnis-Server nach diesen Informationen befragen. Die NSS-Entwickler stellen für die verschiedenen Backends unterschiedliche APIs zur Verfügung. So kommt für die Abfrage eines LDAP-Servers beispielsweise die Bibliothek *libnss_ldap.so* zum Einsatz, für den Blick in die Datei */etc/passwd* hingegen greift das System auf *libnss_files.so* zurück. Welche API zum Einsatz kommt, be-

stimmt der Administrator in der Datei */etc/nsswitch.conf*.

PAM vermittelt zwischen den Welten

Ähnlich sieht es für das PAM-Subsysten aus. Wie der Name bereits verrät, stehen auch hier einzelne Module für die Abfrage unterschiedlicher Backends zur Verfügung. Enthält der bereits angesprochene LDAP-Server neben den klassischen Benutzerinformationen, wie beispielsweise Login-Shell und Gruppen-Mitgliedschaften, das Passwort des Benutzers, lässt sich zur Authentifizierung mittels *pam_ldap.so* darauf zurückgreifen. Liegt das Passwort stattdessen lokal in der Datei */etc/shadow*, benutzt das PAM-Subsystem die Bibliothek *pam_unix.so,* um an die notwendige Information zu gelangen. Damit eine Anwendung auf das modulare PAM-System zurückgreifen kann, muss diese auf die Bibliothek *libpam* zurückgreifen. Im Zweifelsfall hilft hier der Aufruf von *ldd* weiter, um zu verifizieren, ob eine Anwendung mit PAM zusammenarbeitet oder nicht. Das Tool *ldd* zeigt mit folgendem Kommando alle dynamisch gelinkten Bibliotheken für ein Programm an:

```
ldd 'which vsftpd'|grep libpam
libpam.so.0 => /lib/libpam.so.0
  (0x00b67000)
```

Die Konfiguration von PAM findet über das Verzeichnis */etc/pam.d/* statt. Jede Anwendung, die mit PAM zusammenarbeitet, verfügt in diesem Verzeichnis über eine Konfigurationsdatei. Unterschiedliche Sektionen gliedern hier die einzelnen Aufgabenbereiche. So ist die Sektion "auth" für die Authentifizierung von Benutzern zuständig, "account" kümmert sich um deren Autorisierung, "password" ist für die Einhaltung von Passwort-Regeln eingeteilt und über die Sektion "session" findet ein entsprechendes Management der Session statt.

Über sogenannte Kontroll-Flags können Sie das Verhalten von PAM im Fehlerfall regeln, also beispielsweise wenn ein Benutzer ein nicht korrektes Passwort eingegeben hat oder ein Passwort bereits abgelaufen ist. Der große Vorteil beim Einsatz von NSS und PAM liegt auf der Hand: Eine Applikation, die auf die beiden Subsysteme zurückgreift, muss das Rad – also beispielsweise die Überprüfung eines Passwortes – nicht immer wieder neu erfinden, stattdessen gibt sie diese Aufgabe einfach an PAM ab. Somit ist es dann Sache des Subsystems, die jeweiligen Tests durchzuführen und die aufrufende Anwendung über deren Ausgang zu informieren. Als Entwickler sparen Sie so nicht nur jede Menge Arbeit, sondern sind auch als Administrator sehr flexibel, was die Art der Authentifizierung angeht. Ob diese nun über einen Verzeichnisdienst wie LDAP, eine Chipkarte oder einen Windows-Domänencontroller stattfindet, hängt lediglich von der eingesetzten PAM-Bibliothek ab.

Wollen Sie nun also von einem Linux-System auf Benutzerkonten eines Windows Active Directory-Domänencontrollers zurückgreifen, so existieren hierfür mehrere Möglichkeiten. Diese sind in den folgenden Abschnitten aufgeführt.

Reine LDAP-Authentifizierung

Bei der LDAP-basierten Authentifizierung binden Sie sowohl NSS wie auch PAM an das LDAP-Interface des Active-Directory. Obwohl Windows zur Authentifizierung im Active Directory eigentlich Kerberos einsetzt, ist aus Gründen der Abwärtskompatibilität mit älteren NTLM-Clients ein Benutzer-Passwort zusätzlich im LDAP-Baum gespeichert. Selbst wenn eine rein LDAP-basierte Authentifizierung auf den ersten Blick verlockend scheint, so raten wir an dieser Stelle hiervon ab. LDAP überträgt Benutzerpasswörter im Klartext, somit ist der Einsatz von SSL/TLS zur Verschlüsselung der Kommunikation zwischen Linux-Client und Windows-AD unumgänglich. Des Weiteren ist das Windows-AD Schema um entsprechende Posix-Attribute zu erweitern. Um einen Linux-Benutzer und dessen Gruppenmitgliedschaften eindeutig zu kennzeichnen, bekommt jeder Benutzer und jede Gruppe eine eindeutige ID (UID und GID) zugewiesen. Windows kennt diese Benutzer- und Gruppenkennzeichen jedoch nicht.

Stattdessen kommen hier sogenannte Security-Identifiers (SIDs) zum Einsatz. Hiermit kann aber ein Linux-System nichts anfangen. Folglich ist das LDAP-Schema um entsprechende Attribute zu erweitern. Unter Windows Server 2000 können Sie hierfür die sogenannten "Services for Unix" (SFU) [3] einsetzen. Über die Microsoft Management Console (MMC) und das Snap-In zur Verwaltung von Domänenbenutzern ist es dann möglich, jedem Benutzer die notwendigen Posix-Attribute zuzuweisen. Da SFU nicht RFC 2307 kompatibel ist, müssen Sie auf der Linux-Seite für ein entsprechendes Mapping der Attribute sorgen. Hierfür stehen in der Datei */etc/ldap.conf* entsprechende Anweisungen ("nss_map_objectclass" und "nss_map_attribute") zur Verfügung.

Ab der Windows Server Version 2003 R2 liefert Microsoft seinen internen Active Directory-LDAP-Server mit einem RFC 2307-konformen [4] Schema aus. Somit ist die Zuweisung der Posix-Attribute für die einzelnen Benutzer unmittelbar möglich, eine Anpassung des Schemas ist also nicht mehr notwendig. Aber selbst diese Methode ist recht umständlich, vor allem dann, wenn bereits eine Vielzahl von Benutzern existiert, da diesen nachträglich die entsprechenden Attribute zuzuweisen sind. Dies geschieht üblicherweise über den Tab "Unix-Attribute" in den Eigenschaften eines Benutzers. Am einfachsten ist dieses Problem mit Hilfe eines kleinen Visual Basic-Skriptes zu lösen, welches automatisiert die LDAP-Benutzer- und Gruppen-Objekte um die notwendigen Attribute erweitert. Ein weiterer Nachteil bei dieser Art der Benutzer-Anmeldung besteht darin, dass die Windows-Domänencontroller statisch in den Konfigurationsdateien eines Linux-Clients einzutragen sind. Windows-Clients finden diese üblicherweise über einen entsprechenden Service Record Lookup (SRV) im Domain-Name-System (DNS).

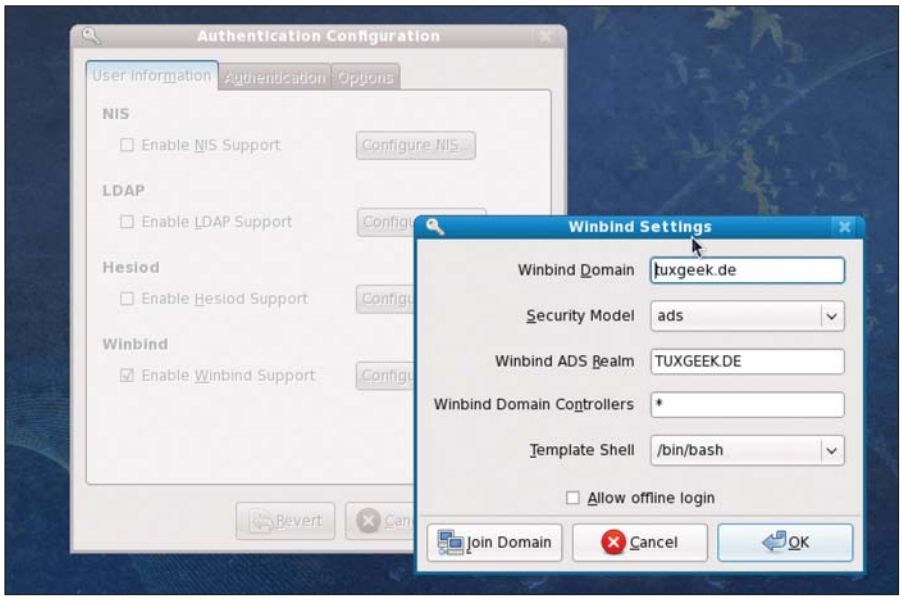


Bild 1: Mit Hilfe von "system-config-authentication" lässt sich sowohl das NSS- wie auch das M-Subsystem konfigurieren

LDAP- und Kerberos-Authentifizierung

Natürlich ist es zudem möglich, den Name Service Switch mittels LDAP an das Windows-AD anzubinden und die eigentliche Benutzer-Authentifizierung mit Hilfe von PAM über einen Windows Kerberos-Server durchzuführen. Das hat den Vorteil, dass das Passwort eines Benutzers niemals über das Netzwerk fließt. Allerdings ist auch diese Art der Konfiguration mit einem erheblichen administrativen Aufwand verbunden. So müssen Sie sich beispielsweise selbst darum kümmern, für die Maschinen-Accounts die notwendigen Kerberos-Principals zu erzeugen und diese in eine Keytab-Datei, beispielsweise */etc/krb5.keytab*, zu exportieren. Ansonsten existieren sämtliche Nachteile der vorher genannten Variante.

Winbind-Authentifizierung

Die eleganteste Methode zur Authentifizierung von Windows-Benutzern auf Linux-Systemen besteht im Einsatz von Winbind. Hierbei handelt es sich um einen Client-Dienst aus dem bekannten Samba-Projekt. Winbind agiert hierbei als eine Art Proxy zwischen Linux-Applikation und Windows-AD. In Abhängigkeit davon, welche Aktion der Client ausführen möchte, kommt das jeweils beste Protokoll zum Einsatz. So ist Winbind dazu in der Lage, LDAP, Kerberos, NTLM und MS-RPC zu sprechen. Das sind genau die Protokolle, die bei einer nativen Anmeldung eines Windows-Benutzers ebenfalls zum Einsatz kommen. Winbind und Samba [5] sind Bestandteil aller bekannten Linux-Distributoren. Eine Installation der beiden Pakete gelingt in den allermeisten Fällen aus dem Standard Software-Repository der jeweiligen Distribution. Auf einem Fedora-System sieht der entsprechende Aufruf wie folgt aus:

```
yum install samba-common
  samba-winbind
```

Das eigentliche Samba-Paket benötigen Sie im ersten Teil des Workshops noch nicht, da es hier lediglich um den Zugriff auf einen Windows-AD-Server geht. Sollen später eigene Freigaben für Windows-Clients hinzukommen, so ist natürlich auch das samba-Paket mit den beiden Diensten *smbd* und *nmbd* zu installieren. Mehr dazu im zweiten Teil des Workshops. Hat die Installation von Winbind geklappt, so erstellen Sie im nächsten Schritt zunächst eine Kopie der Datei */etc/samba/smb.conf* und löschen das Original. Die Samba-Konfigurationsdatei benötigt zur Winbind-Konfiguration lediglich einige wenige Informationen. Im einfachsten Fall erzeugen Sie diese mit einem entsprechenden Konfigurationstool. Auf Fedora-Systemen existiert hierfür das grafische Tool "system-config-authentication" (Bild 1). Jedoch ist auch das manuelle Anpassen der Datei ohne weiteres möglich.

Das Tool erzeugt, wie in Listing 1 beschrieben, die notwendigen Konfigurationseinträge für Winbind in der Datei *smb.conf* und passt nebenbei auch noch die Dateien für den NSS und PAM an. Die folgenden beiden Listings zeigen die entsprechenden Einträge aus den einzelnen Konfigurationsdateien:

```
/etc/nsswitch.conf
passwd: files winbind
shadow: files winbind
group: files winbind
```

```
/etc/pam.d/system-auth
Auth sufficient pam_winbind.so
  use_first_pass
account [default=bad success=ok
  user_unknown=ignore]
  pam_winbind.so
password sufficient pam_winbind.so
  use_authtok
```

Hier sind noch weitere Punkte zu beachten. Bereits weiter oben wurde das Problem der internen Kennzeichnung von Benutzern und Gruppen in der Linux- und Windows-Welt angesprochen. Kommt unter Linux eine User-und Gruppen-ID zum

```
/etc/samba/smb.conf:
[global]

   workgroup = Tuxgeek
   password server = *
   realm = TUXGEEK
   security = ads

   idmap backend = tdb
   idmap uid = 5000-9999
   idmap gid = 5000-9999
   template shell = /bin/bash
   template homedir = /home/%D/%U

   winbind enum users = yes
   winbind enum groups = yes
   winbind use default domain = false
   winbind offline logon = false
```

Listing 1: Konfiguration von Winbind in *smb.conf*

Einsatz, so verwendet Windows stattdessen die bereits erwähnten Security Identifiers (SIDs). Nun ist es die Aufgabe von Winbind, eine Zuordnung zwischen diesen beiden Identifikatoren herzustellen. Zur Lösung bietet Winbind verschiedene Backends zum Verknüpfen von SID und User-/Gruppen-ID an.

idmap backend = tdb

Hierbei handelt es sich um das default Backend von Winbind. Ein Mapping von SID in UID/GID findet über die Datei */var/lib/samba/winbindd_idmap.tdb* statt. Der große Nachteil ist jedoch, dass unterschiedliche Winbind-Instanzen auf mehreren Systemen nicht zwingend ein einheitliches Mapping durchführen. Das führt zu massiven Problemen, wenn Sie auf zentral gespeicherte Daten zugreifen, da in einem solchen Fall der gleiche Benutzer über unterschiedliche UIDs verfügen kann, wenn dieser von verschiedenen Rechnern auf die Daten zugreift:

```
[global]
idmap backend = tdb
idmap uid = 100000-199000
idmap gid = 100000-199000
```

idmap backend = ldap

Bei folgendem Backend speichert Winbind die Mapping-Informationen nicht lokal, sondern in einem Container eines zentralen LDAP-Servers. Alle Winbind-Instanzen sind dann in der Lage, auf diesen Server und die darauf gespeicherten Informationen zurückzugreifen:

```
idmap backend = ldap:ldap:
  //localhost/
idmap uid = 100000199999
idmap gid = 100000199999
idmap alloc backend = ldap
idmap alloc config : ldap_url =
  ldap://localhost/
idmap alloc config : ldap_base_dn =
  ou=idmap,dc=tuxgeek,dc=de
```

idmap backend = rid

Generiert Winbind bei den ersten beiden Beispielen die UID und GID noch selbstständig, so bezieht es diese Informationen in den nächsten Beispielen direkt aus dem Active-Directory. Deshalb werden diese Konfigurationen manchmal auch als READONLY-Backends bezeichnet. Beim rid-Backend extrahiert Winbind aus dem Windows SID den sogenannten Relative Identifier (RID). Hierbei handelt es sich um eine 32-Bit-Ganzzahl, mit deren Hilfe ein Benutzer innerhalb einer Domäne eindeutig identifizierbar ist. Der große Vorteil beim Einsatz von diesem Backend besteht darin, dass überhaupt keine Konfiguration im Active Directory notwendig ist und auf den Linux-Clients nur geringe Anpassungen notwendig sind:

```
idmap backend = rid
idmap range = 100000-199999
```

idmap backend = ad

Die letzte Methode erfordert wieder einige Anpassung auf den Windows Domänen-Controllern. Mit Hilfe des idmap ad-Backends bezieht Winbind alle notwendigen Benutzer- und Gruppen-Informationen aus dem Active-Directory. Das hat den Vorteil, dass auf den Linux-Clients keine Zuordnungsdaten zu speichern sind, aber auch den großen Nachteil, dass erneut jeder Benutzer im AD über Posix-Attribute verfügen muss. Möchten Sie auf dieses Backend zurückgreifen, so empfiehlt sich der Einsatz eines RFC 2307 konformen Schemas, wie es beispielsweise Windows Server 2003 R2 anbietet:

```
idmap backend = ad
idmap range = 100000-199999
```

Wir empfehlen an dieser Stelle den Einsatz des idmap ad- oder rid-Backends. Beide Backends beziehen Ihre Informationen bereits aus dem AD, somit sind relativ wenig Konfigurationsschritte auf den Linux-Clients notwendig. Haben Sie sich für das passende Backend entschieden, gilt es im nächsten Schritt, Ihrer Windows-Domäne beizutreten. Hierfür rufen Sie das Tool *net join* auf:

winbind use default domain = yes|no

Diese Anweisung legt fest, ob Winbind Ihre Benutzer- und Gruppen-Namen mit oder ohne vorangestellten Domänen-Namen darstellt.

winbind nested groups = yes|no

Hierbei kümmert sich Winbind um das "Auspacken" von verschachtelten (nested) Windows-Gruppen.

winbind nss info = template|sfu|rfc2307

Haben Sie Ihr Windows-AD Schema bereits um Posix-Attribute erweitert, so ist es natürlich nicht notwendig, in der Datei *smb.conf* noch einmal ein Template für diese Informationen zu bestimmen. Legen Sie einfach mit dieser Anweisung fest, in welchem Format (sfu oder RFC 2307) der NSS diese Informationen im AD erwarten kann.

winbind offline logon

Ein sehr nützliches Feature, gerade für Notebook-Benutzer. Hiermit weisen Sie Winbind an, die Mapping-Informationen, unabhängig davon, welches idmap backend Sie einsetzen, in einer lokalen Datei unterhalb von */var/lib/samba* zu cachen. Dann können Sie selbst dann auf Domänen-Konten zugreifen, wenn Sie gar nicht online sind. Voraussetzung dafür ist, dass sich die notwendigen Mapping-Informationen bereits in Ihrem Cache befinden. In diesem Zusammenhang ist die Option "winbind cache time" interessant. Diese bestimmt, wie lange die Informationen in Ihrem Winbind-Cache Gültigkeit besitzen.

winbind refresh tickets = true|false

Diese Option weist Winbind an, Kerberos-Tickets vor deren Verfall automatisch zu erneuern. Voraussetzung hierfür ist natürlich, dass Sie im Vorfeld die Kerberos-Funktion von Winbind aktiviert haben. Dieses geschieht über die Datei */etc/security/pam_winbind.conf* und den darin enthaltenen Parameter "krb5_auth = yes". Diese Datei enthält übrigens noch einen weiteren interessanten Parameter, "mkhomedir = yes". Hiermit können Sie Winbind anweisen, ein Benutzer-Homeverzeichnis automatisch anzulegen, falls dieses noch nicht existieren sollte. Beachten Sie bitte, dass hierbei die Dateien aus Ihrem Skeleton-Verzeichnis, üblicherweise */etc/skel/*, (noch) nicht übernommen werden:

```
/etc/security/pam_winbind.conf
[global]
# authenticate using kerberos
krb5_auth = yes

# when using kerberos, request a "FILE" krb5
   credential cache type
krb5_ccache_type = FILE

# create user homedirs when not already available
mkhomedir = yes
```

Winbind-Konfiguration

```
# net join ads -U Administrator
Joined Domain Tuxgeek.
```

Nach Eingabe des Administrator-Passwortes sollten Sie bereits eine Willkommens-Meldung der Domäne sehen. Für erste Tests, ob auch wirklich alles wie gewünscht funktioniert, bietet sich das Tool "wbinfo" an. Dieses listet alle bekannten Benutzer- und Gruppen-Konten Ihrer Windows-Domäne auf:

```
# wbinfo -g
BUILTIN\administrators
BUILTIN\users
domänen-admins
domänen-gäste
...
```

Das Tool kennt eine Menge weiterer nützlicher Optionen. So zeigt die Option "-D" Informationen zur Windows-Domäne an und mit "-i" holen Sie sich die Details zu einem bestimmten Benutzer aus dem Active-Directory. Hat alles funktioniert, so können Sie sich zum Testen der Authentifizierung einfach mit einem Windows-Domänenkonto an Ihrem Linux-System anmelden. Alternativ steht für wbinfo die Option "-a" zur Verfügung. Hiermit lässt sich ebenfalls die Authentifizierung über den Winbind-Dienst testen.

Hilfestellung über die Samba-Logdatei

Sollte es zu Problemen kommen, so hilft wie immer ein Blick in die Log-Datei des betreffenden Dienstes, in diesem Fall also */var/log/samba/log.winbindd*. Eventuell müssen Sie den Pfad der Datei für Ihre Linux-Distribution anpassen. Alle hier aufgeführten Pfade beziehen sich auf eine Fedora 11-Installation. Die in unserem Workshop vorgestellten Optionen reichen für eine grundlegende Konfiguration des Winbind-Dienstes aus, jedoch existiert natürlich noch eine Vielzahl weiterer Optionen, mit denen Sie das Verhalten des Dienstes sehr fein granuliert bestimmen können. Aus diesem Grunde versorgen wir Sie im Kasten "Winbind-Konfiguration" noch mit einigen praktischen Tipps.

Fazit

Abschließend sei gesagt, dass die Integration von Linux-Clients in eine bestehende Windows-Domäne keine Hexerei darstellt. Mit wenigen Konfigurationsschritten sind Sie bereits in der Lage, auf Konten Ihrer Windows-Domäne zuzugreifen. Wie immer lässt sich diese Konfiguration natürlich durch weitere Schritte erweitern und verfeinern.

Für gestandene Windows-Administratoren zum Schluss jedoch noch ein Wermutstropfen: Das Power-Tool schlechthin unter Windows, die Gruppenrichtlinien [6], ist mit der aktuellen Version von Samba leider nicht auf Linux-Clients anwendbar. Jedoch ist hier Licht am Ende des Tunnels zu erkennen. Die Entwickler haben diese Funktion bereits auf ihrer Roadmap. Im nächsten Teil der Samba-Artikelserie drehen wir den Spieß um, dann geht es um die Integration von Windows-Clients in eine Samba-Domäne mit LDAP-Backend. *(ln)*

Thorsten Scherf arbeitet als Senior Consultant für den Linux-Distributor Red Hat.

[1] **NSS, Name Service Switch**
www.gnu.org/software/libc/manual/html_node/Name-Service-Switch.html

[2] **PAM, Pluggable Authentication Modules**
www.kernel.org/pub/linux/libs/pam/

[3] **SFU, Windows Services for Unix**
www.microsoft.com/germany/windowsserver2003/technologien/sfu/default.mspx

[4] **RfC2307**
www.rfc-editor.org/rfc/rfc2307.txt

[5] **Samba und Winbind**
www.samba.org

[6] **Windows-Gruppenrichtlinien**
http://technet.microsoft.com/de-de/windowsserver/grouppolicy/

Links

Kompetentes Schnupperabo sucht neugierige Administratoren

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

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

Damit Sie sich Zeit,
Nerven und Kosten sparen.

Teamwork in Bestform.
Überzeugen Sie sich selbst!

6 Monate lesen

3 Monate bezahlen

www.it-administrator.de

Heinemann Verlag
Im Dialog mit Spezialisten.

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

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

Vertrieb, Abo- und Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville

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

Kontrolliertes Herunterfahren bei Stromausfall

Geplante Pause

von Thomas Bär

Quelle: Leo Blanchette – Fotolia.com

Stromausfälle sind in Deutschland glücklicherweise ein recht seltenes Phänomen. Tritt der Ernstfall trotzdem ein, ist dank unterbrechungsfreier Stromversorgungen zumindest ein kurzfristiger Weiterbetrieb der IT-Landschaft möglich, so dass die entscheidenden Systeme kontrolliert abgeschaltet werden können. In diesem Workshop lesen Sie, wie Sie sich auf einen Stromausfall vorbereiten und wie Sie auch virtualisierte Server sicher herunterfahren.

Das wirksamste Mittel gegen einen Stromausfall ist dessen Verhinderung. Während größere Server-Installationen über komplett vom Hausstromnetz getrennte Stromkreisläufe und über Notstromaggregate verfügen, ist eine solche Ausstattung an kleineren Standorten eher selten der Fall. Bevor jedoch ein Computersystem mit einer unterbrechungsfreien Stromversorgung (USV) gegen Stromausfälle abgesichert wird, steht die Stromversorgung selbst auf dem Prüfstand. So hat es etwa wenig Sinn, eine Serverinstallation am selben Leitungsschutzschalter – umgangssprachlich auch als Sicherung bezeichnet – zu betreiben wie andere Geräte.

In typischen, modernen Hausinstallationen kommt neben dem Leitungsschutzschalter noch ein Fehlerstromschutzschalter (FI-Schalter) zum Einsatz, der jedoch üblicherweise alle Leitungen gleichzeitig überwacht. Entsteht an einer Stelle im Hausstromkreislauf eine Stromdifferenz von mehr als 30 mA, so unterbricht der Leitungsschutzschalter die Stromzufuhr und schützt Personen gegenüber Stromschäden. Während sich durch unterschiedliche Leitungsschutzschalter eine Separierung von Computersystem und Hausstromnetz leicht realisieren lässt, ist dies beim Fehlerstromschutzschalter so leicht nicht möglich.

Gründe für Stromausfälle

Ein Stromausfall für eine Serveranlage kann folglich aus verschiedenen Gründen entstehen: Der Leitungsschutzschalter greift wegen Überspannung oder Kurzschluss und unterbricht die Stromversorgung für den jeweiligen Teilkreislauf. Oder der Fehlerstromschutzschalter erkennt eine Stromdifferenz und unterbricht die Stromzufuhr für den kompletten Kreislauf. Nicht zuletzt kann die Stromversorgung durch den Energielieferanten unterbrochen werden.

Ohne geeignete Sicherungsmaßnahmen ist jedes Computersystem durch Stromausfälle massiv gefährdet. Während ein einfacher Ethernet-Switch einen solchen Ausfall üblicherweise unbeschadet übersteht und bei Aktivierung der Stromversorgung innerhalb kürzester Zeit seine Aufgabe wieder wahrnimmt, so ist das bei Servern, Managed Switches und Routern schon anders. Befindet sich beispielsweise ein Managed Switch in einer Phase der Konfiguration, so hat ein Stromausfall in diesem Moment möglicherweise fatale Folgen. Computer- und Serversysteme reagieren auf das plötzliche Ausschalten im schlechtesten Fall mit Datenverlusten.

Es ist möglicherweise der zuweilen schlechten Stromversorgung in anderen Staaten der Welt zu verdanken, dass USV-Systeme recht kostengünstige Geräte sind, die bereits für unter 100 Euro auf dem Markt erhältlich sind. Trotz verschiedenster Technologien ist eine Funktionsweise allen USVs gemein: Sie versorgen die an ihnen angeschlossenen Geräte im Falle des Stromausfalls mit Strom aus einer wiederaufladbaren Batterie. Je nach Kapazität dieser Batterie und des Energieverbrauchs der daran betriebenen Geräte reicht die Versorgungsdauer von einigen Minuten bis zu Stunden.

Über Datenverbindungen per USB- oder RS232C-Schnittstelle teilt die USV dem angeschlossenen Gerät mit, dass die Stromversorgung auf Batterie umgestellt wurde. Die Auswertung dieser Signale übernimmt entweder eine speziell vom Hersteller mitgelieferte Software oder das Betriebssystem. Jeder, der schon mit einem Laptop gearbeitet hat, kennt die Einstellungsmöglichkeiten, die Windows für den Batteriebetrieb zu bieten hat. Während es bei einem tragbaren Computer schlicht um Einstellungen geht, die in einer möglichst

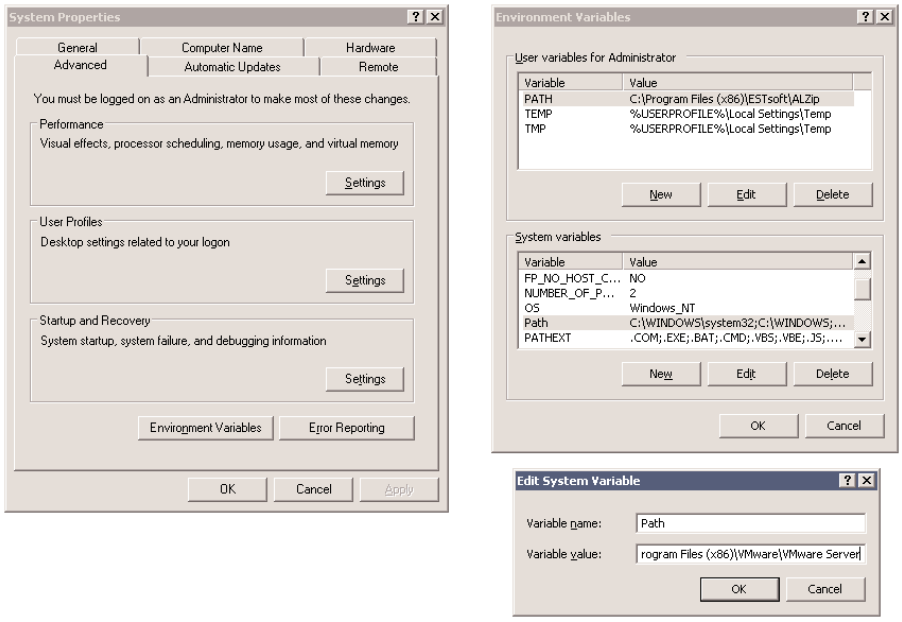


Bild 1: Pfadangaben unter Windows werden über die System-Einstellungen nach System oder Benutzer getrennt gespeichert

langen Akkulaufzeit münden, so sehen die Einstellungen bei Serversystemen ganz anders aus.

Spezielle Energieoptionen für Server

Serversysteme sollen nach einer gewissen Zeit im Akkubetrieb damit beginnen, Dienste korrekt zu beenden und ein geordnetes Herunterfahren des Betriebssystems zu initiieren. Je nach Art der Serverinstallation und der damit verbundenen Client-Landschaft ist die Einbindung von Infrastrukturgeräten zu berücksichtigen. Entsprechend unterscheiden sich die USV-Konzepte – Serverräume in Rechenzentren werden komplett durch eine große USV-Installation versorgt, während Kleinst-Anlagen oder Server in Verteilerschränken über einzelne USVs abgesichert werden.

Unabhängig von der Art des Aufbaus ist sicherzustellen, dass alle Server- und Computersysteme mit einem Betriebssystem, das dazu in der Lage ist, die Meldungen auszuwerten, mit dem geordneten Herunterfahren beginnen, sobald die sogenannte "autonome Versorgungszeit" abzulaufen droht. Übernimmt beispielsweise ein Überwachungs-PC die Signalauswertung, so beginnt dieser mit der Aussendung eines Shutdown-Kommandos an die übrigen Computer. Es versteht sich von selbst, dass die Netzwerkverbindung zu den anderen Computern ebenfalls gegenüber Stromausfällen abgesichert sein muss. Da dies jedoch nicht immer gewährleistet werden kann, sichern manche IT-Verantwortliche lieber jeden Server mit einer eigenen, deutlich kleineren USV ab, anstatt dies für alle Server mit einer großen USV zu tun. Wie so oft ist dies die bekannte Suche nach dem Single Point Of Failure. Die einzig richtige Variante wird es aber wohl auch bei der Stromversorgung nicht geben. So ist letztendlich die Auslegung des System-Planers entscheidend und die individuellen Anforderungen der Installation.

Sonderrolle für virtuelle Maschinen

Während das geplante Herunterfahren eines einzelnen physikalischen Servers durch die Energie-Einstellungen von Windows oder über eine Zusatzsoftware mit wenigen Mausklicks eingerichtet ist, gestaltet sich der Vorgang bei der Nutzung von virtuellen Maschinen ein wenig komplexer. Dank einiger Kommandos in einem Skript-Job lassen sich virtuelle Maschinen, die in einer VMware Virtual Server 2.0-Installation auf einem physikalischen Windows Server 2003 Host liegen, ohne größere Schwierigkeiten herunterfahren. Das Geheimnis ist der Befehl *vmrun*, über den sich virtuelle Maschinen auf VMware Virtual Server 1.x- und 2.x-Installationen und unter VMware Workstation vom Hostcomputer aus fernsteuern lassen.

Im konkreten Beispiel handelt es sich um einen physikalischen Server mit Windows Server 2003 x64, auf dem wir einen aktuellen VMware Server 2.0 mit zwei VMs betreiben. Bei der einen virtuellen Maschine handelt es sich um einen virtuellen 32-Bit Windows Server 2003, der als Domänen-Controller fungiert. Die zweite virtuelle Maschine ist eine Microsoft Exchange 2007-Installation auf einem 64-Bit Windows Server 2003. Der physikalische Server ist über eine kleine USV von APC vor Stromausfällen geschützt und erreicht eine Autonomiezeit von zwölf Minuten.

In der Konfiguration des VMware Servers haben wir festgelegt, dass bei einem Herunterfahren des Host-Systems auch die virtuellen Maschinen automatisch abgeschaltet werden sollen – ein Vorgang, der bei einem Exchange-Server durchaus einige Zeit dauern kann. Typischerweise sollte der Domänencontroller der Server sein, der als Letzter herunterfährt, so dass er allen noch im Shutdown befindlichen Maschinen zur Verfügung steht. Zunächst haben wir das Standardverfahren "Herunterfahren bei 50 Prozent der Batterie-Kapazität" über die Windows-Bordmittel verwendet. Einen Stromausfall später war aber klar, dass dies in der Praxis nicht funktioniert. Alle drei Server beklagten sich, dass sie ungeplant beendet wurden. Der Vorgang dauerte offensichtlich zu lang und ein Erzwingen der Beendigung von Prozessen hat für die virtuellen Maschinen die gleichen Folgen wie das Ziehen eines Stromsteckers.

Die Überlegung ging nun in die Richtung, bei Erreichen von 50 Prozent der

Batterie-Kapazität ein Skript zu starten, das die beiden virtuellen Server in den "Suspend"-Modus überführt und anschließend das Herunterfahren des physikalischen Hosts anstößt. Das Pausieren der Server mit "Suspend" funktioniert innerhalb weniger Sekunden, während "Shutdown", das normale Herunterfahren, mehr als sechs Minuten in Anspruch nehmen kann. Zeit, die im Falle des Stromausfalls nicht zur Verfügung steht.

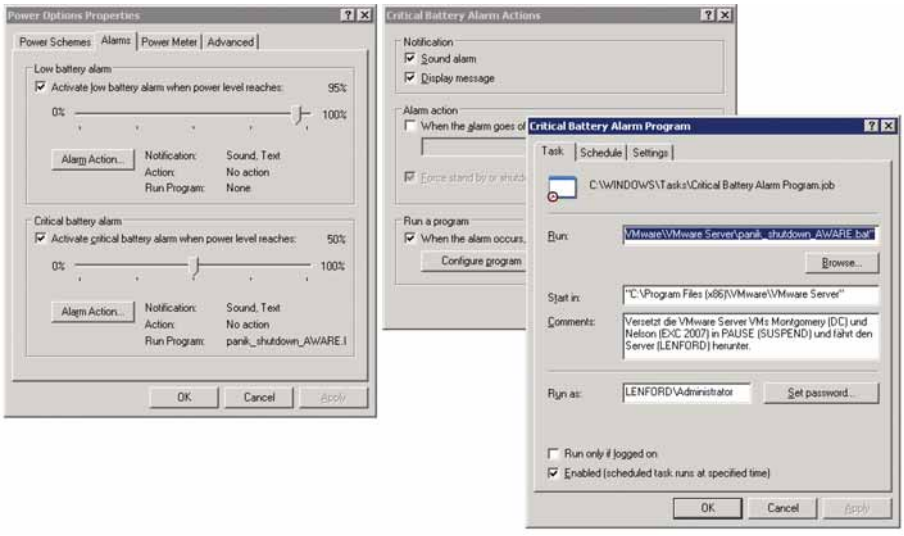


Bild 2: In den Energieoptionen von Windows wird das Skript im Stromausfall automatisch ausgeführt und die VMs sicher angehalten

Virtuelle Maschinen per Skript herunterfahren

Zwar bietet der virtuelle Server über das Webinterface eine Vielzahl von Optionen, die das Verhalten von virtuellen Maschinen in Bezug auf den Start und das Herunterfahren des Hosts regeln. Da in diesen Optionen jedoch der Ablauf für ein geordnetes Herunterfahren mit Time-Out-Zeiten von je 180 Sekunden pro Maschine festgelegt ist und eventuell weitere Maschinen in die Steuerung mit aufgenommen werden sollen, bleibt für den Notfall nur der Griff zum Skript-Job.

Schritt 1: Pfadangaben setzen

Im ersten Schritt müssen Sie dafür sorgen, die Variable "PATH" des Host-Servers um den Installationspfad des VMware-Servers zu erweitern. Dazu passen Sie den Arbeitsplatz in den System-Eigenschaften im Register "Erweitert" bei "Umgebungsvariablen" an. Im oberen Teil des Fensters tragen Sie die benutzerspezifischen Pfad-Variablen unter "PATH" ein, im unteren Bereich folgen die systemspezifischen. Da Sie nicht immer davon ausgehen können, mit Admin-Rechten angemeldet zu sein, empfiehlt sich eine systemspezifische Anlage durch Erweiterung des Eintrags mit einem Semikolon und dem Installationspfad des Servers ("C:\Program Files (x86)\VMware\VMware Server"). Wenn Sie nun die Eingabeaufforderung starten, so gibt der Befehl *VMRUN* den Hilfetext aus.

Schritt 2: Das Skript erstellen

Bei dem Skript handelt es sich um eine ganz normale Befehlsfolge für einen Batch-Job. Mit einem Editor legen Sie im Programmverzeichnis des VMware-Servers die Datei *panik_shutdown_AWARE.bat* an. Aus Layout-Gründen haben wir jede Zeile mit einem Zeilenumbruch getrennt.

```
vmrun -T server -h "https://local-
  host:8333/sdk" -u Administrator -p
  {PASSWORT} suspend "[standard]
  Montgomery/Windows Server 2003
  Standard Edition.vmx"

vmrun -T server -h "https://local-
  host:8333/sdk" -u Administrator -p
  <PASSWORT> suspend "[standard]
  Windows Server 2003 Enterprise x64
  Edition/Windows Server 2003 Enter-
  prise x64 Edition.vmx"

DATE/T > c:\panik.nul
TIME/T > C:\panik.nul

SHUTDOWN /s /f /t 10 /d 6:11 /c "Out
  of power - VM suspended - PANIK
  shutdown"
```

Der etwas schräge Dateiname soll versehentliche Doppelklicks unterbinden. Die beiden VMRUN-Befehle sind zwar komplex, erklären sich aber wie folgt: Der Befehlsschalter "T" (Target) ist für den VMware Server 2.0 gesetzt, "h" (Host) zeigt in Hochkommata auf die Web-Konsole des Servers mit der Erweiterung "/sdk". Die Schalter "u" und "p" tragen den Benutzernamen und das Passwort. Somit müssen Sie in jedem Fall dafür sorgen, dass kein Unberechtigter Zugriff auf das Skript erhält. Hinter dem Schlüsselwort "suspend" folgt, wieder in Hochkommata, der Verweis auf die Konfigurationsdatei der virtuellen Maschine.

Die Befehle *DATE* und *TIME* schreiben eine Datei mit Namen *PANIK.NUL* auf die Systempartition. Bei Ausführung des Skripts wird das aktuelle Datum und die aktuelle Uhrzeit eingetragen. Sie können somit mit einem Blick erkennen, wann das System zuletzt überstürzt heruntergefahren ist. Anschließend folgt der Windows Befehl *SHUTDOWN* in der eigentlich gültigen Server-Notation. Windows XP-Rechner verwenden anstelle des Slash-Symbols ein Minuszeichen. Was Microsoft dazu veranlasst hat, die beiden Befehle unterschiedlich anzulegen, bleibt in Redmond wohl ein großes Geheimnis. Die verwendeten Schalter besagen, dass in zehn Sekunden ("t") das System heruntergefahren ("s") wird und das Schließen der Programme erzwungen wird ("f"). Ferner wird ein Eintrag in der Ereignisanzeige mit dem Hinweis

auf ein Problem mit der Stromversorgung ("d 6:11") angelegt und mit einem beliebigen Hinweistext, hier "Out of power - VM suspended - PANIK shutdown", versehen. Auch wenn sich trefflich darüber diskutieren ließe, so handelt es sich bei "6:11" um ein Zeichen für ein unerwartetes Herunterfahren.

Schritt 3: Energie-Optionen anpassen

Im nächsten Schritt gilt es, das Skript automatisch bei Erreichen von 50 Prozent der Batteriekapazität ausführen zu lassen. Dazu müssen Sie das Register "Alarm" in den Energieoptionen in der Systemsteuerung anpassen. Windows unterscheidet zwischen zwei Zuständen – dem "niedrigen Batteriestand" (Low battery alarm) und dem "kritischen Batteriestand" (Critical battery alarm).

Für den niedrigen Batteriestand beließen wir es bei Sound- und Textausgaben bei 95 Prozent. Beim kritischen Batteriestand, eingestellt bei 50 Prozent, kommt das erstellte Skript (*C:\Program Files (x86)\VMware\VMware Server\panik_shutdown_AWARE.bat)* in der Administrator-Rolle zur Ausführung. Durch einen aussagekräftigen Eintrag im Kommentarfeld stellen Sie sicher, dass auch anderen Mitarbeiter in der IT schnell erkennen, was dieses Skript macht.

Schritt 4: Stecker ziehen

Haben Sie alles fertig eingerichtet, folgt der Praxistest: Ziehen Sie die Stromzufuhr an der USV-Einheit. Das Gerät schaltet nun augenblicklich auf Batteriebetrieb um und der Server läuft erwartungsgemäß weiter. Einige Pieps-Geräusche und Einträge in der Ereignisanzeige machen auf den Notstand aufmerksam. Zirka fünf Minuten später erreicht die Kapazität die definierte Marke von 50 Prozent.

Nun geht alles sehr schnell. Die VMs werden pausiert – ein Vorgang, der nicht einmal 60 Sekunden dauert. Das Host-System fährt nach einer letzten Warnung herunter. Wird der physikalische Server später wieder gestartet, so sorgen die in VMware Server 2.0 festgelegten Optionen dafür, dass die beiden VMs automatisch fortgesetzt werden. Glücklicherweise interpretiert die VMware-Software das "Start"-Kommando bei einem Neustart im Falle einer pausierten Maschine als "Fortsetzen".

Diese Lösung ist an sich nicht auf virtuelle Maschinen von VMware beschränkt, über den Aufruf eines VB-Skripts mit dem Inhalt

```
On Error Resume Next
Set objVS = CreateObject("Virtual-
  Server.Application")
Set objVM = objVS.
  FindVirtualMachine("{SERVERNAME}")
objVM.Pause()
```

versetzen Sie einen unter Microsoft Virtual Server 2005 betriebenen virtuellen Rechner in den Pause-Modus. *(ln)*

Active Directory-Recovery unter Windows Server 2008 R2

Admins neuer Papierkorb

von Ulf B. Simon-Weidner

Datensicherung und Rücksicherung ist besonders beim zentralen Verzeichnisdienst Active Directory immer wieder ein spannendes Thema. Zum einen dient der Verzeichnisdienst in einer Windows Server-Infrastruktur der Authentisierung und Autorisierung und ist damit der Speicherort für alle Benutzer, Computer und Gruppen. Zum anderen dient das Active Directory als Infrastrukturverzeichnis auch weiteren angeschlossenen Komponenten, wie der Verwaltung über Gruppenrichtlinien, der Darstellung der Standorttopologie für Replikation, den Datei- und Druckdiensten sowie Exchange (in einigen Versionen). Klar ist: das Active Directory ist unternehmenskritisch, es muss funktionieren und Ausfälle müssen minimiert werden. Beim neuen Windows Server 2008 R2 gibt es einen Papierkorb für das Active Directory, um Inhalte einfach wiederherstellen zu können. IT-Administrator zeigt auf, in welchen Fällen dieser geeignet ist und wie sich der Papierkorb in eine Datensicherungsstrategie integrieren lässt.

Tatsächlich läuft das Active Directory (AD) in den meisten Unternehmen sehr stabil, aber Ausfälle können schnell sehr kostspielig werden. Um sich abzusichern, sollte jedes Unternehmen daher in eine Sicherungsstrategie des Active Directory sowie das Know-how zur Wiederherstellung investieren. Dass das Thema brisant ist, zeigt sich auch in der jüngsten Entwicklung: Microsoft hat in Untersuchungen festgestellt, dass das Löschen von Objekten die häufigste Ursache für Wiederherstellungen ist, und hat daher mit dem Active Directory-Papierkorb (Active Directory-Recyclebin) speziell dieses Thema adressiert.

Mögliche Problemfälle

Wenn es zu einer Wiederherstellung des Active Directory kommt, so ist wahrscheinlich einer der folgenden Problemfälle eingetreten. Wir unterscheiden zwischen den Problemfällen, die ganze Systeme und Domänen betreffen und Problemfällen, die Inhalte betreffen. Wenn Systeme oder Domänen betroffen sind, gibt es die folgenden Fälle:

- Ein Domänencontroller ist defekt und muss ausgetauscht werden. Wenn dieser über eine Sicherung wiederhergestellt werden soll, so sollte das ausschließlich in der zusätzlichen Software begründet sein – oder dass nur ein Domänencontroller existiert (was nicht empfohlen ist). In allen anderen Fällen sollte der Domänencontroller neu aufgebaut und die Inhalte von den anderen Domänenkontrollern repliziert werden.
- Eine Domäne ist kaputt und kann über keinen anderen Weg gerettet werden. Dies ist ein hoffentlich seltener Fall und würde bedeuten, dass ein Domänencontroller von einer Sicherung wiederhergestellt werden muss, mit den anderen Domänen wieder kommunizieren muss und von diesem dann die Domäne mit weiteren Domänencontrollern wieder aufgespannt wird.
- Eine Gesamtstruktur aus mehreren Domänen ist kaputt: Auch dieser Fall ist recht selten und bedeutet zumeist die komplette Wiederherstellung der Unternehmensinfrastruktur. Auch in diesem Fall müssen die Domänen einzeln wiederhergestellt werden.

Häufiger sind die Fälle, in denen Inhalte des Active Directory wiederhergestellt werden müssen:

- Ein einzelnes Objekt wird gelöscht.
- Mehrere Objekte oder ein gesamter Baum an Objekten wird gelöscht (etwa beim Löschen einer Organisatorischen Einheit).
- Einzelne Werte von Attributen werden über mehrere Objekte hinweg fehlerhaft geändert oder gelöscht.

Diese Fälle erfordern aber auch besonderes Wissen, da spezielle Effekte auftreten, wenn nur einzelne Inhalte wiederhergestellt werden sollen. Was Sie

berücksichtigen müssen, ist der redundante Aufbau des Active Directory – jeder Domänencontroller einer Domäne hat die gleichen Informationen über alle Objekte dieser Domäne. Ein Spezialeffekt rührt daher, dass es Verknüpfungen zwischen Objekten gibt. Dies sind zum Beispiel die Mitgliedschaft von Benutzerkonten in Gruppen, die Mitgliedschaft von Gruppen in Gruppen oder auch Manager- und Mitarbeiter-Verknüpfungen, die im Active Directory gepflegt werden können. Bei diesen Verknüpfungen gibt es einen Vorwärtslink, der gepflegt wird (und beschreibbar ist), und einen Rückwärtslink, den das Active Directory automatisch berechnet. Im Fehlerfall können nur die Vorwärtslinks wiederhergestellt werden (da beschreibbar) und auch nur dann, wenn das Ziel bereits existiert.

Wird zum Beispiel zuerst eine Gruppe wiederhergestellt und ein Benutzer, den diese enthalten soll, erst später, dann ist der Benutzer nach der Wiederherstellung nicht mehr in der Gruppe. Jetzt wäre es einfach zu sagen, zuerst Benutzer wiederherstellen und dann Gruppen. Allerdings dürfen Sie nicht die Beziehungen zwischen Benutzerkonten (Manager) vergessen und, dass Gruppen in anderen Gruppen verschachtelt sein können und häufig auch sind. Dann kann es auch mehrere Domänen geben, was dazu führen kann, dass die bereits erwähnten Effekte domänenübergreifend auftreten. Wenn etwa eine Gruppe in einer Domäne einen Benutzer in einer anderen Domäne enthält, dieser nun gelöscht und wiederhergestellt wird, dann muss auch die Gruppe wiederhergestellt oder bearbeitet werden, damit sie den Benutzer wieder enthält.

Ausflug in die Vergangenheit

Das Active Directory, wie wir es kennen, wurde mit Windows 2000 geboren. Microsoft hatte bereits damals zwei Wiederherstellungsmethoden eingeführt: die autoritative und die nicht-autoritative Wiederherstellung. Bei der non-autoritativen Wiederherstellung wird ein kompletter Domänenkontroller wiederhergestellt, ohne jedoch das AD zu modifizieren. Da sich das AD aber Domänencontroller-übergreifend merkt, welche Änderungen erfolgt sind und zudem mit sogenannten "Tombstones" (Grabsteinen) einen Vermerk über das Löschen von Objekten repliziert, bekommt der nicht-autoritativ wiederhergestellte Domänencontroller, wenn er an der Replikation wieder teilnimmt, den gleichen Stand wie seine Kollegen. Diese Methode ist also nur geeignet, um einen Domänencontroller wiederherzustellen, wenn alle Inhalte des AD in Ordnung sind.

Die autoritative Wiederherstellung hingegen markiert vom IT-Administrator ausgewählte Objekte als neuer. Sie können eine autoritative Wiederherstellung direkt nach einer nicht-autoritativen Wiederherstellung durchführen, wenn Sie einen älteren Stand von Objekten oder Objektbäumen benötigen. Hierbei ist zu beachten, dass der Domänenkontroller in der Zwischenzeit nicht replizieren darf. Da beide Arten der Wiederherstellung im Verzeichnisdienstwiederherstellungsmodus erfolgen, in dem keine Replikation möglich ist, sind Sie auf der sicheren Seite, solange Sie den Domänencontroller nicht zwischendurch neu starten (beziehungsweise ihn vom Netzwerk trennen oder sicherstellen, dass Sie ihn wieder im Verzeichnisdienstwiederherstellungemodus starten). Interessant ist, dass sich eine autoritative Wiederherstellung auch ohne eine vorige nicht-autoritative Wiederherstellung durchführen lässt, wenn der Server, auf dem Sie diese durchführen, von der versehentlichen Änderung oder dem versehentlichen Löschen noch nichts erfahren hat (über die Replikation). Nach einer autoritativen Wiederherstellung werden die gewünschten Objekte als neuer markiert und "gewinnen" bei der Replikation gegenüber den alten Objekten, die gelöscht wurden oder die falschen Daten enthalten.

In den Communities sind damals Tricks aufgekommen, um ein gelöschtes Objekt (Tombstone) wiederzubeleben. Zwar hatte dieses fast keine Daten mehr, allerdings verfügte es noch über den gleichen Security-Identifier (SID). Und alle anderen Daten mussten eben per Hand gefüllt werden. Die Problematiken mit den verlinkten Attributen waren enorm und mussten mit großem Know-how berücksichtigt werden. Bei Windows Server 2003 hat Microsoft dann das Wiederbeleben der Tombstones über eine API offiziell unterstützt. Mit dem Servicepack 1 von Windows Server 2003 nahm der Hersteller dann erstmals das Thema mit den Verknüpfungen in Angriff: Wenn eine autoritative Wiederherstellung durchgeführt wird, werden Dateien mit der Erweiterung LDF (sogenannte LDIF-Dateien) erstellt, die die Links enthalten, die nicht wiederhergestellt werden konnten. Nachdem der Administrator diese Dateien nach der Wiederherstellung der Objekte in den entsprechenden Domänen mit dem Tool "LDIFDE.exe" eingespielt hatte, waren alle Verknüpfungen wiederhergestellt. Trotzdem war der Prozess aufwendig.

Bei Windows Server 2008 hat das Schicksal dazu geführt, dass ein weiteres maßgebliches Feature in diesem Bereich eingeführt wurde: In den ersten Beta-Versionen der eingebauten Datensicherung hatten die Entwickler vergessen, dass, um einen Domänencontroller zu sichern, eine "Systemstatussicherung" notwendig ist. Das Active Directory-Team reagierte mit der Entwicklung der Active Directory-Snapshots. Diese ermöglichen es dem Administrator, einen konsistenten Zustand der AD-Datenbank online zu einem beliebigen Zeitpunkt zu erstellen. Und mit dem Befehl *dsamain.exe* lässt sich sowohl der Schnappschuss der Datenbank wie auch eine Datenbank aus der Sicherung heraus als nur-lesbarer Verzeichnisdienst starten und die Inhalte lesen. Auf diese Inhalte können Sie auch mit Applikationen und Skripten zugreifen, so dass Sie mit relativ einfachen Mitteln Objekte online wiederbeleben und anschließend die Daten aus dem Snapshot einspielen können – ohne jemals in den Wiederherstellungsmodus zu wechseln.

Der Papierkorb für das Active Directory

In Windows Server 2008 R2 wurde das Thema jetzt zum ersten Mal konsequent adressiert: Die Wiederherstellung von Objekten muss einfacher werden. Dazu hat Microsoft die Möglichkeit geschaffen, gelöschte Objekte durch einen einfachen Befehl wieder komplett, mit allen Gruppenmitgliedschaften und sonstigen Verknüpfungen wiederherzustellen. Um die Funktionsweise zu erklären, müssen wir etwas ausholen. Wenn wir die Datenbankstruktur des AD vereinfacht betrachten, hat jedes Objekt in der Datentabelle eine Zeile, die einen primären Schlüssel hat. Daneben existiert eine Link-Tabelle, die zum Beispiel von dem Schlüssel für eine Gruppe auf den Schlüssel eines Benutzers verweist, wenn dieser Mitglied in der Gruppe ist. Wenn ein Benutzer gelöscht wird, werden bei Windows Server 2008 und in den vorherigen Versionen die meisten Eigenschaften des Objekts gelöscht, diese werden ja nicht mehr benötigt. Des Weiteren wird das Objekt in den "Deleted Objects"-Container verschoben, der Name wird verändert und der Wert "isDeleted" auf "wahr" gesetzt. Alle Links, die das Objekt referenzieren, werden gelöscht – und zwar direkt von jedem Domänencontroller. Das Objekt, das jetzt nur noch ein Tombstone ist, wird als solcher repliziert, damit bekommen alle DCs mit, dass es zu löschen ist und entfernen die Links.

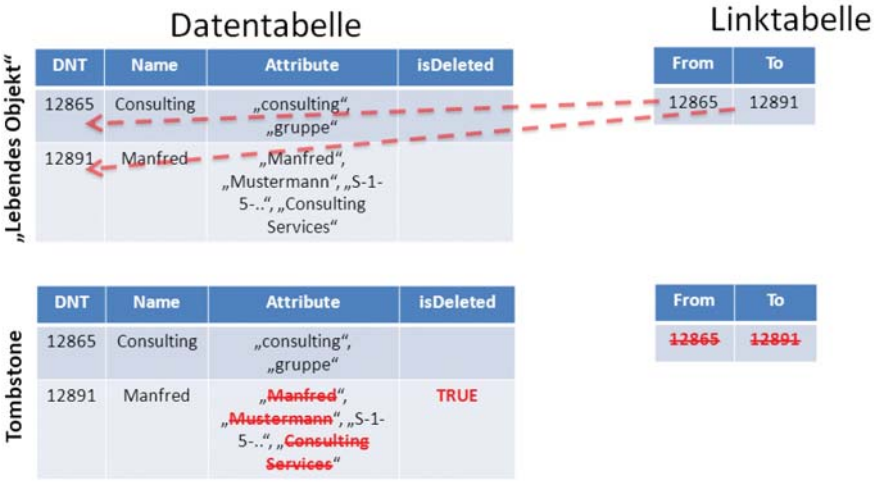


Bild 1: Wird ein Objekt unter Windows Server 2008 entfernt, so sind die meisten Eigenschaften und die Verknüpfungen ebenfalls gelöscht

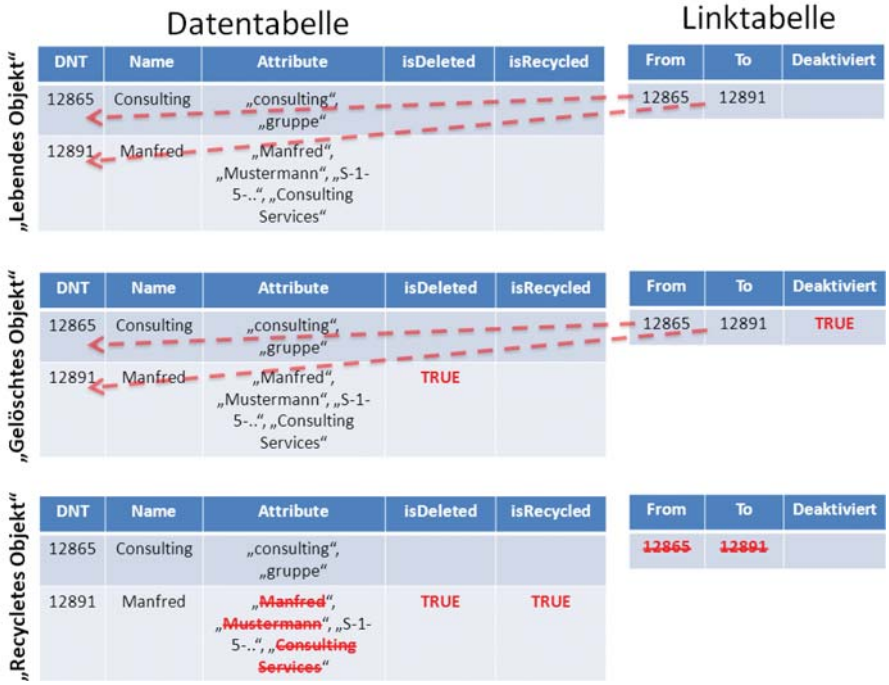


Bild 2: Der eingeschaltete Papierkorb führt dazu, dass beim Löschen alle Eigenschaften erhalten bleiben und die Verknüpfungen nur deaktiviert werden. Nachdem die "Deleted Objects Lifetime" abgelaufen ist, werden diese gelöscht und als "Tombstones / Recycled Objects" repliziert.

Beim Windows Server 2008 R2 können Sie den Active Directory Recyclebin einschalten. Dieser verändert das Verhalten wie folgt: es wird zwischen gelöschten und recycelten Objekten unterschieden. Gelöschte Objekte behalten die Werte aller Eigenschaften, werden jedoch als gelöscht markiert. Die Verknüpfungstabelle wird mit dem Einschalten des Papierkorbs erweitert – Verknüpfungen von gelöschten Objekten können deaktiviert werden. Diese gelöschten Objekte bleiben eine Zeit in der Infrastruktur erhalten, und zwar für die "Deleted Objects Lifetime". Wenn diese abgelaufen ist, werden die Objekte recycelt: die Werte der Eigenschaften und die deaktivierten Links werden gelöscht. Die recycelten Objekte werden für die Dauer der Tombstone-Lifetime repliziert (damit auch alle DCs von der Änderung erfahren) und danach komplett gelöscht. Dadurch können bei eingeschaltetem Papierkorb Objekte einfach wiederhergestellt werden, in dem sie wiederbelebt werden. Alle Eigenschaften und sogar die Gruppenmitgliedschaften bleiben erhalten.

Voraussetzungen für das Einschalten des Papierkorbs

Ein Wermutstropfen ist, dass diese Funktion einen neuen Gesamtstrukturmodus benötigt: alle Domänencontroller aller Domänen der Gesamtstruktur benötigen Windows Server 2008 R2 oder höher als Betriebssystem – nur dann lässt sich der Gesamtstrukturmodus anheben

und der Papierkorb einschalten. Wenn wir überlegen, wie der Mechanismus funktioniert, wird auch klar, warum: Das Löschen/Deaktiveren der Links erfolgt auf jedem DC einzeln, Verknüpfungen können auch domänenübergreifend existieren. Nur indem jeder Domänencontroller in der Lage ist, die Werte der Eigenschaften zu erhalten und die Links nur zu deaktiveren, kann das Feature überhaupt funktionieren.

Aber es existiert ein kleiner Lichtblick: Seit Windows Server 2008 R2 ist es außerdem möglich, das Anheben des Domänen- oder Gesamtstrukturlevels wieder rückgängig zu machen, solange keine Funktionen eingeschaltet werden, die dies verhindern. Der Recyclebin ist die einzige, derzeit existierende derartige Funktion. Also: Zunächst muss der Administrator den Level aller Domänen auf Windows Server 2008 R2 heben. Dann muss er den Level der Gesamtsstruktur auf Windows Server 2008 R2 heben. Wenn er sich sicher ist, dass er in dem Level bleiben wird und keine Windows Server 2008 (ohne R2) Domänencontroller mehr promoten möchte, kann er den Recyclebin einschalten.

Während das Höhersetzen des Domänen- und Gesamtstrukturmodus mit den üblichen Verwaltungskonsolen erfolgt, muss der Administrator sowohl für das Herunterstufen des Levels wie auch für das Einschalten des Papierkorbs die PowerShell unter Windows Server 2008 R2 (oder Windows 7 mit den Remote Server Administration Tools für Windows Server 2008 R2) verwenden, die die neuen Active Directory-Commandlets enthalten.

Am einfachsten starten Sie die PowerShell mit dem AD über "Startmenü / Verwaltung / Active Directory-Modul für Windows PowerShell". Sollten Sie die PowerShell über das Symbol in der Taskbar gestartet haben, laden Sie mit *Import-Module ActiveDirectory* die Active Directory-Module. Hierbei wird das AD-Modul geladen und ein virtuelles Laufwerk verbunden. Machen Sie sich damit vertraut, indem Sie *cd AD:* eingeben und *dir* und *cd* verwenden, um durch das AD zu navigieren (Achtung – Sie müssen immer den RDN, also zum Beispiel "cd cn=users" verwenden).

Nachdem das Active Directory-Modul geladen wurde, können Sie den Domänenmodus anheben (wenn alle Domänencontroller auf Windows Server 2008 R2 sind), in unserem Beispiel hat die Domäne den DNS-Namen "firma.de":

```
Set-ADDomainMode -identity firma.de
  -DomainMode Windows2008R2Domain
```

Wenn alle Domänen auf dem R2-Domänenmodus laufen, muss analog dazu der Gesamtstrukturmodus mit dem folgenden Befehl angehoben werden:

```
Set-ADForestMode -identity firma.de
  -ForestMode Windows2008R2Forest
```

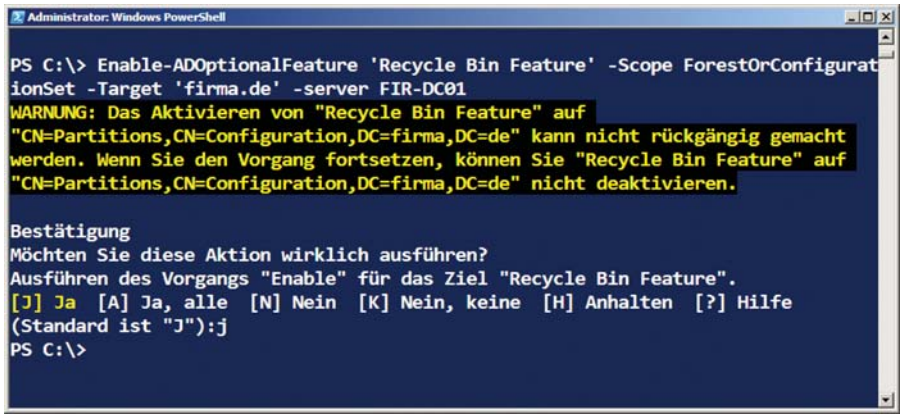


Bild 3: Vor dem Aktivieren weist Windows 2008 R2 darauf hin, dass dieser Schritt nicht umkehrbar ist

Ein Herunterstufen des Forest- und dann auch des Domänenmodus funktioniert ebenso mit "Windows2008Domain" und "Windows2008Forest" (auf niedrigere Modi wird das Herunterstufen nicht unterstützt). Um den Active Directory-Papierkorb einzuschalten, nutzen Sie:

```
Enable-ADOptionalFeature 'Recycle
  Bin Feature' -Scope ForestOrConfi-
  gurationSet -Target 'firma.de' -
  server FIR-DC01
```

Mit dem folgenden Befehl zeigen Sie eine Liste aller gelöschten Objekte, hier mit dem Vornamen "Ulf" an:

```
Get-ADObject -filter 'givenname -eq
  "Ulf"' -includeDeletedObjects
```

Diese Benutzer stellen Sie auch einfach wieder her, indem Sie die Objekte an das Cmdlet *restore-ADObject* weiterleiten. Hierbei muss beachtet werden, dass die OU, in der das Benutzerkonto Mitglied war, existieren muss, ansonsten geben Sie mit dem Parameter "–TargetPath" eine neue OU an:

```
Get-ADObject -filter 'givenname -eq
  "Ulf"' -includeDeletedObjects |
  restore-ADObject
```

Wissenswertes zum AD-Recovery

Microsoft unterstützt mit Windows Server 2008 R2 kein Wiederbeleben von Tombstones mehr, wie es bisher der Fall war. Auch Autoritative Restores sind nicht gerne gesehen, da sie die bisher – zumeist nicht im Detail bekannten – Schwierigkeiten mit sich bringen. Sobald alle Domänenkontroller Windows Server 2008 R2 sind und der Papierkorb eingeschaltet ist, können ab dann neu gelöschte Objekte einfach wiederhergestellt werden.

Eine Versionierung ist mit diesem Feature nicht möglich – ein Objekt wird genau in dem Zustand wiederhergestellt, in dem es gelöscht wurde. Wenn ein Objekt über den Papierkorb wiederhergestellt wird, muss entweder das ursprüngliche übergeordnete Objekt (normalerweise cn=Users oder eine OU) vorhanden sein oder ein neues übergeordnetes Objekt gewählt werden. Eine Gesamtstruktur kann nur über zusätzliche Skripte wiederhergestellt werden.

Neben diesem Feature können seit Windows Server 2008 (auch ohne R2 möglich) auch Objekte vor versehentlichem Löschen geschützt werden. Dies wird bei neuen OUs (mit der neuen Version der Managementkonsolen) automatisch erledigt, bei bisherigen sollte dies eingeschaltet werden.

Fazit

Der Active Directory-Papierkorb ist ein sehr interessantes Feature, um Löschungen im Active Directory rückgängig zu machen. Er hilft jedoch nicht, wenn Sie auf ältere Versionen der Objekte oder Attribute zurückgreifen wollen – in diesem Fall sind die Active Directory-Snapshots und ein bisschen Scripting (ab Windows Server 2008) eine Lösung (siehe IT-Administrator 03/2008 und 04/2008).

Des Weiteren ersetzt der Papierkorb keine Datensicherung oder Vorbereitung auf Wiederherstellungsszenarien, da diese für Domänen- oder Gesamtstrukturwiederherstellungen benötigt werden. In Kombination mit Datensicherung und eventuell Snapshots ist der Papierkorb aber eine sehr umfassend und überlegt konzipierte Funktion, die dem Administrator im Fall der Fälle sehr viel Arbeit erspart und in den häufigsten Fällen ausreichend sein dürfte. *(jp)*

Ulf B. Simon-Weidner ist MVP für Windows Server – Directory Services und arbeitet als Consultant und Trainer. Sein Weblog finden Sie unter msmvps.com/ulfbsimonweidner

Tombstone-Lifetime und Deleted Objects Lifetime

Die "Deleted Objects Lifetime" ist die Dauer, in der ein Objekt zwar gelöscht ist, aber zunächst noch vollständig erhalten bleibt und inklusive aller Verknüpfungen wiederhergestellt werden kann. Die Tombstone-Lifetime bezeichnet die Dauer, in der ein Objekt gelöscht ist und ohne die meisten Informationen aufgehoben wird, damit alle Domänencontroller mitbekommen, dass dieses zu löschen ist.

Standardmäßig entspricht die Deleted Objects Lifetime der Tombstone Lifetime. Diese wiederum ist davon abhängig, auf Basis welches Betriebssystems die Gesamtstruktur errichtet wurde:

- Vor Windows Server 2003 SP1: 60 Tage
- Windows Server 2003 SP1: 180 Tage
- Windows Server 2003 R2: 60 Tage
- Windows Server 2003 (R2) SP2: 180 Tage
- Windows Server 2008 und höher: 180 Tage

Links

[1] Active Directory Recycle-bin im Windows Server 2008 R2 TechCenter
http://technet.microsoft.com/en-us/library/dd391916(WS.10).aspx

[2] Active Directory PowerShell-Blog
http://blogs.msdn.com/adpowershell/

Neuerungen im Forefront Threat Management Gateway (2)

Den Schutzwall hochziehen

von Marc Grote

Im ersten Teil unserer Artikelserie vermittelten wir einen Überblick über die wesentlichen Neuerungen in Microsoft Forefront Threat Management Gateway (TMG). In diesem Teil gehen wir näher auf die vier wichtigsten Neuerungen in TMG ein – Network Inspection System (NIS), Malware-Schutz, HTTPS-Inspizierung sowie E-Mail-Schutz – und erläutern die einzelnen Funktionen. Abschließend betrachten wir die Vorgehensweise bei der Migration von ISA Server 2006 auf Forefront TMG.


Quelle: Pixelio.de

Das in TMG integrierte Network Inspection System (NIS) [1] ist Bestandteil der Intrusion Prevention-Systemfunktionen von Forefront TMG. Mit Hilfe von NIS stellt TMG eine effiziente Technologie zur Verfügung, um unerwünschten Datenverkehr für bekannte Exploits bereits am Gateway zum Internet zu blockieren.

Network Inspection System (NIS)

NIS bietet einen effektiven Schutz gegen so genannte Zero Day Exploits, bei denen eine bekannt gewordene Sicherheitslücke bereits von TMG blockiert wird, damit für die betroffenen Systeme Gegenmaßnahmen in Form von Windows Updates oder Ähnlichem durchgeführt werden können. NIS verwendet Signaturen von bekannten Verwundbarkeiten (Vulnerabilities), die das Microsoft Response Center zur Verfügung stellt. Das System beschränkt sich jedoch zurzeit auf den Schutz vor bekannten Exploits für Microsoft-Produkte auf Basis des GAPA-Protokolls (Generic Application Level Protocol Analyzer). Die NIS-Konfiguration erfolgt mit Hilfe der TMG-Verwaltungskonsole im Knoten "Intrusion Prevention System".

Forefront TMG wird mit einer Reihe von NIS-Signaturen ausgeliefert, die durch die integrierten Update-Mechanismen laufend aktualisiert werden, die TMG zudem mit neuen Signaturen aus dem Microsoft Response Center versorgen. Für jede NIS-Signatur finden sich auf der Registerkarte "Details" weitere Informationen und in jeder Signatur-Beschreibung verweist Microsoft auf das entsprechende Microsoft Security Bulletin, damit Administratoren sich Zusatzinformationen zu dem Exploit verschaffen können. Für die NIS-Signaturen können Sie zwei verschiedene Zustände konfigurieren: Einerseits lässt sich das Standardverhalten der NIS-Signatur auf eine reine Erkennungsfunktion festlegen oder andererseits auf das Blockieren von Netzwerkverkehr bei erkannter Signatur setzen. Sollen bestimmte Netzwerke, Subnetze oder einzelne Computer vor der Network Inspection ausgeschlossen werden, tragen Sie diese in der Verwaltungskonsole ein.

NIS ist nur so lange effektiv, wie sichergestellt ist, dass das System laufend aktualisiert wird und Signaturen erhält. Das in TMG integrierte Update Center sucht in regelmäßigen Abständen nach neuen Signaturen und Signatur-Aktualisierungen. Sollte das NIS einmal nicht so reagieren, wie Sie es sich wünschen, nutzen Sie die Benachrichtigungs-Funktion, um sich zum Beispiel per E-Mail über den Status von NIS zu informieren. Nach der Konfiguration von NIS können sich Administratoren von der Funktionsfähigkeit überzeugen, indem sie eine Testseite [2] aufrufen, auf welche die NIS-Funktion von Forefront TMG reagiert.

Schutz vor Malware einrichten

Forefront TMG bietet als erste Microsoft Enterprise Firewall die Möglichkeit, direkt am Übergang vom Internet zum privaten Netzwerk eine Prüfung des HTTP-Datenverkehrs auf schädliche Inhalte

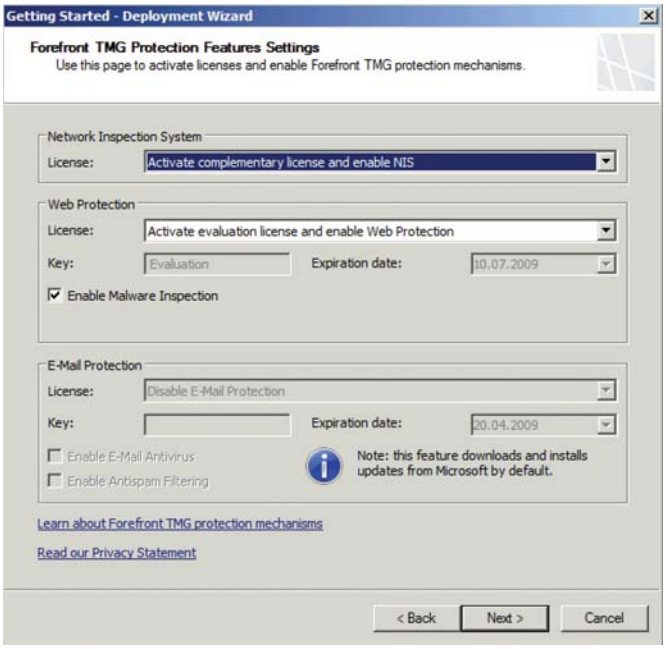


Bild 1: Auswahl der zu lizenzierenden Funktionen in TMG

durchzuführen und so zu verhindern, dass Malware auf den Arbeitsplatz-PC gelangt und dort Schaden anrichten kann. Das System schützt den HTTP-Datenverkehr vor Malware, indem es diesen auf Malware-Signaturen untersucht und nach Vorgaben des Administrators blockiert.

TMG verwendet die gleiche Malware-Protection-Engine, die auch von Microsoft Forefront Client Security (FCS), Live One Care und Windows Defender verwendet wird. Einige der Malware-Schutzfunktionen werden global konfiguriert, andere werden pro Firewall-Regel festgelegt. Administratoren können die Malware-Inspektion pro Firewall-Regel aktivieren und deaktivieren.

Ablauf einer Malware-Prüfung

Bei einer Prüfung, nachdem ein Client eine HTTP-Anforderung zum Download einer Datei an die gewünschte Webseite gesendet hat, fängt TMG die Anforderung ab, stellt fest, ob eine Firewall-Regel zur Malware-Prüfung zutrifft und scannt die Datenpakete gegebenenfalls durch. Sind die Dateien frei von Schadcode, sendet TMG die Anforderung an den Zielserver und dieser bedient die Anfrage entsprechend. Die Antwort wird von TMG empfangen und an die Proxy-Komponente von TMG gesendet und verarbeitet. Nun sendet die Proxy-Komponente den Text der HTTP-Anforderung an den Malware-Filter von TMG.

Der Malware-Filter sammelt die Inhalte der Datenpakete, plant den Download und übergibt die Kontrolle wieder zurück an die Proxy-Komponente. Wurden die angeforderten Datenpakete nicht als Malware identifiziert, übermittelt TMG den Inhalt an den ursprünglichen Client. Falls die Datenpakete infiziert sind und der Inhalt sich nicht bereinigen lässt, sendet TMG eine HTML-Seite an den Client mit dem Hinweis, dass der Inhalt verweigert wurde.
Während des Prüfungsvorgangs erhält der Client eine in TMG konfigurierbare, simulierte Download-Seite angezeigt, welche über den Fortschritt des Downloads berichtet. Das ist notwendig, da TMG die kompletten Datenpakete erst inspizieren muss, bevor diese an den Client übermittelt werden.

Konfiguration der Malware-Prüfung

Zur Konfiguration der Malware-Prüfung verwenden Sie die Forefront TMG-Verwaltungskonsole im Knoten "Web Access Policy". Auf der Registerkarte "Allgemein" aktivieren oder deaktivieren Sie die Malware-Prüfung global und konfigurieren, ob Netzwerkverkehr erlaubt oder verboten ist, wenn kein Malware Inspection Engine Update vorhanden ist. In der Verwaltungskonsole konfigurieren Sie zudem Webseiten und Clients, welche von der Überprüfung ausgeschlossen sind. Auf der Registerkarte "Inspection Settings" stellen Sie Details zur Konfiguration der Prüfung ein, unter anderem die Optionen, ob TMG versuchen soll, Malware-infizierten Datenverkehr zu bereinigen, ob verschlüsselte Dateien blockiert werden, bis zu welcher Tiefe verschachtelte Archive geprüft und ab welcher Dateigröße Downloads blockiert werden.

Auf der Registerkarte "Content Delivery" können Sie konfigurieren, wie den Benutzern der Download der angefragten Dateien aus dem Internet präsentiert wird, während TMG die oben erwähnte Prüfung der Inhalte durchführt. Da TMG für die Malware-Prüfung jeden Download überprüfen muss, ist auf dem Server für ausreichenden Speicherplatz zur temporären Speicherung der Dateien zu sorgen. Der Standardpfad ist das Systemlaufwerk, den Sie entsprechend ändern sollten. Auf der Registerkarte "Update Configuration" legen Sie fest, in welchen Abständen TMG nach neuen Malware Updates suchen soll. Dafür benötigt TMG ein aktuelles Abonnement.

Microsoft Telemetry Service

Eine Malware-Schutzfunktion ist nur so gut wie das Verständnis über die bestehende und aktuelle Malware-Technik. Um Microsoft über die Existenz neuer Malware zu informieren, lässt sich TMG so konfigurieren, dass Informationen über erkannte Malware oder verdächtige Inhalte an Microsoft übermittelt und dort gesammelt werden. Microsoft nennt

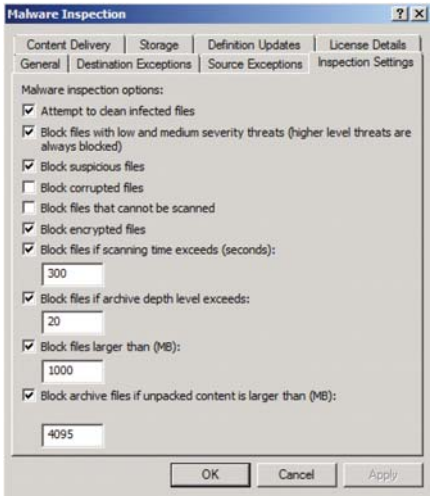


Bild 2: Bei gefundener Malware stellt TMG eine ganze Reihe möglicher Vorgehensweisen zur Auswahl

diesen Dienst "Telemetry Service" [3] und steht ihn als "Basis-" oder "Erweiterte Mitgliedschaft" zur Verfügung. Je nach Mitgliedschaft werden dann unterschiedlich viele Informationen an Microsoft übermittelt.

Bei der Basis-Mitgliedschaft werden nur Informationen über den Computer wie Quell- und Ziel-IP-Adresse, Port und URL (gekürzt auf den Domänennamen) an Microsoft übermittelt sowie ein Einweg-Hash des Netzwerkverkehrs und eine GUID, um den Computer eindeutig zu identifizieren. Im Rahmen der erweiterten Mitgliedschaft werden zusätzlich die komplette URL und Beispiele des Internet-Datenverkehrs übermittelt. Daten, welche bei der erweiterten Mitgliedschaft übertragen werden, können persönliche Informationen beinhalten, werden aber per SSL an Microsoft übertragen.

Ausgehenden HTTPS-Verkehr inspizieren

Forefront TMG ermöglicht es Administratoren, auch ausgehenden HTTPS-Datenverkehr zentral zu überprüfen, um so für eine Einhaltung der Unternehmensrichtlinien zu sorgen. In vorherigen Versionen der Microsoft Firewall war es nur möglich, eingehenden HTTPS-Datenverkehr in Reverse Proxy-Szenarien in Form von Webserververöffentlichungen mit HTTPS-Bridging zu überprüfen. Bei der ausgehenden HTTPS-Inspizierung [4] arbeitet TMG als so genannter Man in the Middle. Ein Benutzer, welcher eine HTTPS-Webseite öffnen will, wird direkt zum TMG-Server gelenkt, welcher ein Proxy-Zertifikat generiert und die eigentliche HTTPS-Kommunikation mit dem Zielserver, welchen der Client erreichen möchte, einrichtet. Damit eine ausgehende HTTPS-Überprüfung überhaupt möglich ist, muss TMG als Proxy für ausgehende Webanfragen fungieren. TMG erreicht das dadurch, dass entweder ein von TMG selbst erzeugtes Stammzertifizierungsstellen-Zertifikat oder das einer internen Zertifizierungsstelle verwendet wird.

Die Konfiguration der ausgehenden HTTPS-Inspizierung erfolgt über den Knoten "Web Access Policy" der TMG-Verwaltungskonsole. Auf der Registerkarte "General" legen Sie – neben der generellen Aktivierung beziehungsweise Deaktivierung der Funktion – für die HTTPS-Inspizierung fest, ob ein vom TMG-Server generiertes Zertifikat an die Clients verteilt werden soll oder das Stammzertifizierungsstellen-Zertifikat einer internen Zertifizierungsstelle verwendet werden soll. Letzteres importieren Sie auch an dieser Stelle in die TMG-Konsole. Soll TMG ein eigenes Zertifikat verwenden, wird dieses am TMG-Server erstellt und per Gruppenrichtlinienupdate-Prozess an die internen Clients verteilt. Dieser Prozess kann bis zu acht Stunden in Anspruch nehmen.

Um für bestimmte Webseiten oder anfragende Clients keine HTTPS-Inspizierung zu verwenden, konfigurieren Sie auf der Registerkarte "Exceptions" entsprechende Ausnahmen. Fore-

front TMG kann verschiedene Zertifikatsüberprüfungen auf der Registerkarte "Certificate Validation" durchführen. Es ist zum Beispiel möglich, abgelaufene Zertifikate nach einer definierten Anzahl von Tagen zu blockieren oder Server-Zertifikate zu blocken, die nicht validiert werden können.

Da eine ausgehende HTTPS-Inspizierung zu rechtlichen Problemen innerhalb der Unternehmen führen kann, ist es mit TMG möglich, eine Client-Benachrichtigung einzurichten, dass der HTTPS-Datenverkehr überprüft wird. Grund für diese Technik ist, dass ein Client, welcher eine HTTPS-Seite aufruft, nicht sieht, dass TMG den Datenverkehr inspiziert. Die Client-Benachrichtigung setzt jedoch den Einsatz des aktuellen TMG Firewall-Client voraus. Damit die Benachrichtigung funktioniert, müssen Sie eine Zugriffsregel erstellen, welche den UDP-Port 1745 von den Clients zum TMG-Server erlaubt.

URL-Filter einrichten

Mit TMG wird die URL-Filterung vom ISA Server-Entwicklungsteam wieder eingeführt (Stand RC und somit voraussichtlich auch in der finalen Version verfügbar). Die Nutzung der URL-Filterung ist an ein kostenpflichtiges Abonnement gebunden, damit TMG regelmäßig mit aktuellen URL-Updates versorgt wird. Die URL-Filterung [5] in TMG erlaubt es, den Aufruf von bestimmten Webseiten anhand einer dynamisch gepflegten URL-Datenbank zu verweigern. Zur Erleichterung der Administration wird die URL-Datenbank in Kategorien eingeteilt, die es ermöglichen, spezielle Webseiten zu blockieren (aktuell über 80 Kategorien). Der URL-Filter in Forefront TMG verwendet dazu den Microsoft Reputation Service (MRS). Bei MRS handelt es sich um ein Cloud-basiertes Objektkategorisierungssystem, das zurzeit über 10 Millionen URLs umfasst. Das Besondere an der MRS-Datenbank ist, dass Microsoft eigene URLs in der Datenbank zur Verfügung stellt, aber auch mit Drittanbietern zusammenarbeitet, welche die URL-Datenbank erweitern. Jede URL-Anfrage von TMG wird gegen das MRS gesendet. Damit die Performance von TMG nicht beeinträchtigt und nicht zu viel Bandbreite belegt wird, speichert TMG eine Reihe von aufgerufenen URLs und URL-Kategorien in einem Cache auf dem lokalen TMG-Server. Von TMG zwischengespeicherte URLs werden mit einer Time To Live (TTL) versehen.

Die Konfiguration der URL-Filterung erfolgt global und pro TMG-Firewallrichtlinie und erlaubt Ihnen festzulegen, welche URL-Kategorien für Webseitenaufrufe der Benutzer erlaubt oder verboten sind. Es ist möglich, Ausnahmen zu konfigurieren, um bestimmte URLs zu erlauben, welche normalerweise geblockt werden würden. Des Weiteren ist es möglich, eine URL-Abfrage zu starten, um festzustellen, zu welcher Kategorie die aufzurufende URL gehört. Zudem können Sie eine Meldung erstellen, die den Benutzer informiert, wenn sein Aufruf einer URL aufgrund einer Verweigerungsregel blockiert wird.

Schutzfunktionen für E-Mail

TMG beinhaltet zum Schutz von E-Mail einen integrierten SMTP-Proxy sowie integrierte Antivirus- und Antispam-Funktionen. So arbeitet TMG als SMTP-Gateway und führt gleichzeitig Antivirusüberprüfungen mit Hilfe von anderen Produkten der Forefront-Familie sowie Antispam-Überprüfungen mit Hilfe der Exchange Server 2007 Edge-Funktionen durch.

Für die Antispam-Funktionalität müssen Sie die Exchange Server 2007 Edge-Rolle vor der Installation von Microsoft Forefront TMG installieren. Eine nachträgliche Installation ist möglich, erfordert jedoch einen Zusatzschritt. Für die Antivirus-Funktionalität stellt TMG bis zu acht verschiedene Antiviren-Engines von Microsoft Forefront Security für Exchange zur Verfügung, von denen bis zu fünf gleichzeitig verwendet werden. Forefront Security für Exchange ist ebenfalls vor der Installation von TMG zu installieren. Zu den weiteren Funktionen gehören

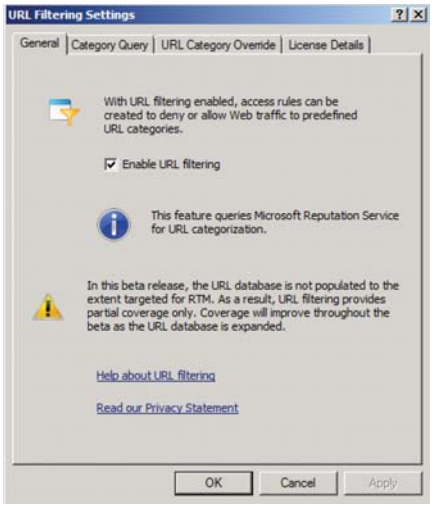


Bild 3: Die Konfiguration der URL-Filterung erfolgt auf dieser Registerkarte nach der Aktivierung des Dienstes

beispielsweise automatische Antivirus- und Antispam-Updates, Blocklisten-Updates, Inhalts- und Anlagen-Filterung sowie die automatische Synchronisation von sicheren Senderlisten (nur in Verbindung mit Exchange Server 2007).

Konfiguration des SMTP Gateway

Auf der Registerkarte "E-Mail Policy" konfigurieren Sie TMG als SMTP-Gateway. TMG stellt dazu einen Assistenten zur Verfügung, welcher die beteiligten E-Mailserver, E-Maildomänen und SMTP-Antwortdomänen konfigurieren kann. Die Konfiguration einer SMTP-Route stellt sicher, dass TMG E-Mails vom internen Mailserver annehmen und in das Internet senden kann sowie, dass eingehende E-Mails für die erlaubten Empfängerdomänen angenommen werden.

Zunächst geben Sie den internen E-Mailserver und die erlaubten Empfängerdomänen im Assistenten an. Es folgt die Auswahl des TMG Listener, auf welchem TMG auf E-Mailanfragen des internen Netzwerks reagiert und anschließend die Auswahl des Listener, welcher für ausgehende E-Mailanfragen an das Internet und für eingehende Anfragen verwendet wird. Für spezielle Konfigurationen können Sie noch TLS (Transport Layer Security) verwenden, um den E-Mail-Datenverkehr zu verschlüsseln. Zum Abschluss des Assis-

tenten wählen Sie noch aus, ob TMG den E-Maildatenverkehr auf Spam und Viren überprüfen soll. Die vorgenommenen Konfigurationen bezüglich des E-Maildatenverkehrs sehen Sie jetzt in der Exchange Server 2007-Verwaltungskonsole.

Antispam-Konfiguration

TMG erlaubt mit Hilfe der Exchange Server 2007 Edge-Rolle, die folgenden Antispam-Funktionen zu konfigurieren:

- Erlaubte IP-Listen und Anbieter für erlaubte IP-Adressen
- IP-Blocklisten und IP-Blocklisten-Anbieter
- Inhaltsfilterung
- Empfänger- und Senderfilterung
- Sender ID-Verfahren
- Sender-Reputation

Die Konfiguration der Antispam-Funktionen in TMG unterscheidet sich kaum von der Antispam-Konfiguration in Exchange Server 2007 [6].

Antivirus- und Inhaltsfilter-Konfiguration

Die Antivirus- und Inhaltsfilter-Konfiguration von Forefront TMG stellt drei Filtermöglichkeiten zur Verfügung: Datei-Filterung, E-Mail Schlüsselwort-Filterung und Antivirus. Mit Hilfe der Datei-Filterung kann TMG ein- oder ausgehende E-Mails auf verschiedene Dateitypen prüfen und festlegen, ob bei einer Übereinstimmung der E-Mailanhang gelöscht, markiert, die komplette E-Mail gelöscht oder ohne Prüfung weitergeleitet werden soll. Es ist hierbei möglich, nach genauen Dateinamen oder nach Dateitypen zu filtern. Die E-Mail Schlüsselwort-Filterung ermöglicht Ihnen, in E-Mails nach konfigurierbaren Schlüsselwörtern zu suchen. Die Aktionen bei einer Übereinstimmung des Filters sind dieselben wie bei der Datei-Filterung.

Die Antivirus-Filterung in Forefront TMG nutzt die selben Scan-Engines wie Microsoft Forefront Server Security. Administratoren können aus derzeit acht verfügbaren Scan-Engines maximal fünf gleichzeitig auswählen. Bei der Auswahl der Scan-Engines ist zwischen einem höchstmöglichen Scanergebnis und Geschwindigkeits-Aspekten abzuwägen. Aus unserer Sicht sollten mindestens zwei Scan-Engines zeitgleich arbeiten. Die Entscheidung, eine dritte Scan-Engine dazuzuschalten, sollte jeder Administrator für seine Umgebung selbst abwägen. Wollen Sie sich nicht auf bestimmte Scan-Engines festlegen, können Sie TMG die Entscheidung überlassen. Microsoft nennt diese Funktion "Intelligent Engine Selection Policy". Findet TMG einen Virus, können Sie festlegen, wie mit der E-Mail umgegangen wird: Skip (Nur Erkennen), Clean (Dateianhang reparieren) oder Delete (Infektion entfernen).

Migration von ISA Server 2006

Microsoft ermöglicht eine einfache Migration der vorhandenen ISA Server 2006-Konfiguration auf einen neuen Server mit Microsoft Forefront TMG. Dazu dient die in ISA Server und TMG integrierte Export- und Importfunktion. Ein direktes Update auf TMG auf gleicher Hardware ist nicht möglich, da ISA Server 2006 nur unter Windows Server 2003 32-Bit läuft, Forefront TMG aber nur unter Windows Server 2008 (R2) 64-Bit. Vor einem Update sind folgende Punkte zu beachten:

- Ein Update von ISA Server 2006 Enterprise auf Microsoft Forefront TMG ist seit Beta 3 ebenfalls möglich.
- ISA Server 2000 und 2004 können nicht direkt upgedatet werden. Es muss erst ein Update auf ISA Server 2006 durchgeführt werden.
- ISA Server 2006 Standard als Mitglied einer Arbeitsgruppe lässt sich (schon mit Beta 3) auf TMG migrieren. ISA Server 2006 muss dabei ein Domänen-Mitglied sein.
- Während der Migration werden angepasste Logfelder der SQL-Protokollierung nicht migriert und Einstellungen der ISA Reports werden nicht übernommen.
- Vor einem Update auf Forefront TMG muss geprüft werden, ob auf ISA Server 2006 installierte Drittanbieter-Programme auch für TMG zertifiziert sind.

Die Migration von ISA Server 2006 auf Forefront TMG besteht aus folgenden Schritten: Zunächst exportieren Sie die ISA Server 2006-Konfiguration in eine XML-Datei. Anschließend installieren Sie TMG auf einem 64-Bit Windows Server 2008. Nun exportieren Sie die Zertifikate von der ISA Server-Maschine auf das neu installierte Forefront TMG. Mit Hilfe der TMG-Managementkonsole importieren Sie jetzt die ISA Server-Export-Datei. Wenn die Überprüfungen der Konfiguration, Updates und der Ereignisanzeige erfolgreich waren, schalten Sie den alten ISA Server 2006 ab und nehmen TMG in Produktion.

Nachdem die ISA Server-Konfiguration erfolgreich zu Microsoft Forefront TMG migriert wurde, sind weitere Schritte erforderlich: Zuerst entfernen Sie die Netzwerk-Konnektivität von allen Netzwerkkarten des TMG-Servers. Übernehmen Sie nun alle IP-Adressen vom ISA Server zu TMG und schalten Sie den TMG-Server aus. Jetzt schließen Sie alle Netzwerkkabel des ISA-Servers an den TMG-Server an und fahren den ISA-Server herunter. Starten Sie anschließend den Forefront TMG-Server und überprüfen Sie dessen einwandfreie Funktion. Abschließend starten Sie den ISA-Server ohne Netzwerkverbindungen und deinstallieren ihn. *(jp)*

Links

[1] Network Inspection System
http://technet.microsoft.com/en-us/library/dd441065.aspx

[2] Microsoft Testseite TMG/NIS-Konfiguration
https://blogs.technet.com/isablog/archive/2009/04/12/exercising-nis-with-test-signature.aspx

[3] Telemetry Service
http://technet.microsoft.com/en-us/library/cc995230.aspx

[4] HTTPS-Inspizierung
http://technet.microsoft.com/en-us/library/dd441073.aspx

[5] URL-Filterung
http://blogs.technet.com/isablog/archive/2009/06/10/url-filtering-is-here.aspx

[6] Konfiguration der Antispam-Funktionen
http://technet.microsoft.com/de-de/library/aa996551.aspx

Tipps & Tricks ohne Gewähr

In jeder Ausgabe präsentiert Ihnen IT-Administrator Tipps, Tricks und Tools zu den aktuellen Betriebssystemen und Produkten, die in vielen Unternehmen im Einsatz sind. Wenn Sie einen tollen Tipp auf Lager haben, zögern Sie nicht und schicken Sie ihn per E-Mail an tipps@it-administrator.de. Für jeden Tipp, der veröffentlicht wird, bedanken wir uns mit einem Gutschein über 20 Euro für den Internetshop getDigital.de.

Microsoft Windows

Bei der **Fernwartung von Windows-Rechnern** empfinde ich es als äußerst umständlich, dass ich mir die **Versionsnummer des Betriebssystems** nur über die Systemsteuerung anzeigen lassen kann. Ich habe gehört, dass sich die entsprechende Information auch direkt auf dem Desktop einblenden lässt. Wie geht das?

Um sich die Versionsnummer samt etwaiger Service-Packs unmittelbar auf dem Desktop anzeigen zu lassen, bedarf es einer kleinen Änderung in der Registry. Rufen Sie diese unter "Start / Ausführen" mit dem Kommando *regedit* auf und navigieren Sie zum Verzeichnis "HKEY_CURRENT_USER \ Control Panel \ Desktop". Dort klicken Sie mit der rechten Maustaste auf den Eintrag "PaintDesktopVersion" und ändern dessen Wert auf "1". Ist der Schlüssel noch nicht vorhanden, legen Sie ihn als Typ "DWORD" an. Nach einem Neustart können Sie die Informationen zur Version des installierten Windows-Systems in der unteren rechten Ecke des Desktops ablesen. *(ln)*

Beim Öffnen der **Systemsteuerung unter Windows 7** zeigt mir das Betriebssystem immer nur eine kleine Auswahl aller Optionen an. Erst über einen Klick auf den Pfeil in der Adressleiste ganz oben im Fenster kann ich **mir alle wählbaren Unterpunkte anzeigen** lassen. Kann ich diesen Umweg irgendwie ausschalten und schneller zur Ansicht aller Systemeinstellungen gelangen?

Um auf Anhieb alle möglichen Optionen in der Systemeinstellung zu sehen, gibt es mehrere Möglichkeiten. Oben rechts im Fenster der Systemsteuerung finden Sie den Punkt "Einstellungen". Als Auswahl ist hier standardmäßig "Kategorie" eingestellt. Wenn Sie diese Auswahl auf "Große Symbole" oder "Kleine Symbole" ändern, bietet Ihnen die Systemsteuerung in Zukunft gleich von Beginn an sämtliche Unterpunkte an. Wollen Sie auf diese komplette Liste noch schneller direkt vom Desktop zugreifen, legen Sie dort eine Verknüpfung mit folgendem Ziel an:

```
explorer.exe ::{20D04FE0-3AEA-1069-A2D8-08002B30309D}\::{21EC2020-3AEA-1069-A2DD-08002B30309D}
```

Über einen Doppelklick auf das nun entstandene Symbol kommen Sie direkt zur Systemsteuerung, wo Sie sich die vollständige Liste aller Optionen zu Gemüte führen können. *(ln)*

Wie mir scheint, gibt es seit Windows Vista keine Möglichkeit mehr, eine für einen Ordner gewählte **Ansicht für sämtliche weiteren Verzeichnisse** zu verwenden. Vielmehr bestimmt das Betriebssystem diese Einstellungen je nach Ordnerinhalt, manuell kann ich lediglich das **Erscheinungsbild eines individuellen Ordners** ändern. Gibt es hier vielleicht nicht doch einen Workaround, um zu einer einheitlichen Ansicht zu gelangen?

Windows Vista und 7 arbeiten mit einem neuen Explorer-Feature – den sogenannten "Folder Views". Damit lässt sich von Haus aus keine Standardeinstellung für alle Ordner festlegen. Microsoft hat hierzu verschiedene Ordnertypen festgelegt. So ist etwa für Bildordner die Miniaturansicht definiert und für Musikordner die Detailansicht. Der Ordnertyp wird über seinen Inhalt bestimmt. Liegen im Ordner "Eigene Musik" mehr Bilder als Musikstücke, ändert sich automatisch der Ordnertyp. Leider lässt sich nicht ohne weiteres wie in Windows XP ein Standard für alle Ordnertypen festlegen, ohne jeden Ordnertyp einzeln zu konfigurieren. Es gibt jedoch eine Lösung. Mit Setzen des Registrierungsschlüssels "HKEY_CURRENT_USER \ Software \ Classes \ Local Settings \ Software \ Microsoft \ Windows \ Shell \ Bags \ AllFolders \ Shell" auf die Einstellung "FolderType=NotSpecified" lässt sich der Verzeichnistyp "All Items" über alle Ordner legen. Sollten aber noch spezifische Konfigurationen angelegt worden sein, sind diese unter "HKEY_CURRENT_USER \ Software \ Classes \

Local Settings \ Software \ Microsoft \ Windows \ Shell \ Bags" zu finden. Durch Löschen dieses Schlüssels setzen Sie auch diese Einstellungen zurück. *(ln)*

Mehr über Folder Views finden Sie unter http://blogs.sepago.de/nicholas/2009/04/23/fixing-folder-views-on-vistaserver-2008-using-citrix-upm/

Linux

Wenn ich mit Ubuntu und Gnome arbeite, gibt es zwischen dem **Anklicken eines Menüs** und dessen Aktivierung immer eine **minimale Pause**. Kann ich diese Verzögerung irgendwie ausschalten?

Die Verzögerung beim Anklicken eines Menüs ist gewollt und soll angeblich die Benutzerfreundlichkeit verbessern. Wenn Sie keine Lust auf die Zwangspause haben, gehen Sie folgendermaßen vor: Öffnen Sie ein Terminal und editieren Sie mit dem Befehl

```
nano ~/.gtkrc-2.0
```

die Datei, die für das Erscheinungsbild und die Funktionen des Gnome-Desktops zuständig ist. Fügen Sie dort die Zeile

```
gtk-menu-popup-delay = 0
```

hinzu, drücken Sie dann die Escape-Taste und speichern Sie die vorgenommenen Änderungen. In Zukunft sollten sich Ihre Menüs bei einem Mausklick deutlich schneller melden. *(ln)*

Da auf einem Rechner mehrere Betriebssystemversionen vorhanden sind, verwende ich dort als **Bootloader Grub**. Die OS-Auswahlliste ist jedoch immer sehr lange sichtbar, ich hätte gerne, dass das Standardsystem schneller gestartet wird, wenn keine Eingabe erfolgt. Kann ich denn irgendwie die **Wartezeit des Bootmenüs verkürzen?**

Um die Zeit bis zum automatischen Start des Standard-Betriebssystems zu verkürzen, öffnen Sie mit einem Texteditor Ihrer Wahl die Datei *menu.lst*, die Sie im Verzeichnis */boot/grub* finden. Suchen Sie nun den Eintrag

```
## timeout sec
# Set a timeout, in SEC seconds,
  before automatically booting the
  default entry
# (normally the first entry
  defined).
timeout 10
```

Die Zahl, in diesem Fall die 10, steht für die Sekunden, nachdem das Default-OS automatisch hochgefahren wird. Durch eine Änderung dieses Wertes können Sie den Vorgang schneller erzwingen. Beachten Sie, dass Sie zum Abändern dieser Vorgaben root-Rechte benötigen. Wenn Sie übrigens den Wert "timeout" mit einem "#" auskommentieren, bleibt das Bootmenü so lange stehen, bis eine manuelle Auswahl getroffen ist. *(ln)*

Microsoft Outlook

Im Unternehmen arbeiten wir mit Outlook 2007. Das Programm ist ja recht übersichtlich, manchmal würde ich mir jedoch wünschen, besonders häufig genutzte Funktionen schneller aufrufen zu können. Gibt es – von der Verwendung von Tastaturkürzeln einmal abgesehen – irgendeine Möglichkeit, häufig genutzte Tätigkeiten wie etwa das Öffnen eines neuen Terminfensters zu beschleunigen?

Wie Sie schon erwähnt haben, sind Shortcuts eine Möglichkeit, gewisse Funktionen schnell aufzurufen. Die Tastaturkombination "STRG+N" etwa öffnet einen neuen Termin beziehungsweise eine neue Mail. Ein Nachteil von Shortcuts ist, dass Sie sich dazu schon im Programm und außerdem im richtigen Menü befinden müssen. Noch direkter geht das Starten bestimmter Funktionen mit einem Befehl in der Eingabeaufforderung. Die Syntax hierzu lautet:

```
outlook /{Befehl}
```

Wollen Sie es sich besonders einfach machen, können Sie auch eine Verknüpfung mit der Datei *outlook.exe* auf dem Desktop anlegen und den Befehl über das Kontextmenü und die Eigenschaften im Reiter "Verknüpfung" dem Pfad hintenanstellen. Der Eintrag

```
"…\ Programme \ Microsoft Office \
  Office12 \ OUTLOOK.EXE"
  /c ipm.appointment
```

etwa würde direkt nach einem Doppelklick auf das Icon das Fenster für einen neuen Kalendereintrag generieren. Weitere nützliche Befehle sind */c ipm.contact* für das Erstellen eines neuen Kontakts oder */safe*, um Outlook im abgesicherten Modus ohne Erweiterungen, Vorschaufenster und Symbolleistenanpassungen zu starten. Neben für Anwender nützlichen Kommandos gibt es einige sehr hilfreiche Admin-Befehle: *firstrun* etwa startet Outlook wie bei der Erstinstallation, *safe:2* bewirkt einen Programmstart, bei dem keine Mails abgeholt werden und *cleanclientrules* entfernt alle Client-basierten Regeln. Eine Übersicht über alle Kommandos finden Sie unter http://office.microsoft.com/en-us/outlook/hp012185891033.aspx *(ln)*

Tools

Treten bei Windows **während eines Anmeldevorgangs Probleme** auf, haben es meine Kollegen und ich sehr schwer, den aufgetretenen Fehler herauszufinden. Gibt es irgendeine einfache Möglichkeit, die bei der Anmeldung **laufenden Vorgänge zu dokumentieren**, um so besser mögliche Schwierigkeiten analysieren zu können?

Wie Sie richtig bemerken, ist es beim Laden eines Profils sehr schwer, bei etwaigen Problemen deren Ursachen auf die Spur zu kommen. Es gibt je-

doch glücklicherweise mehrere Möglichkeiten, wie Sie hier Abhilfe schaffen können. Eine Vorgehensweise sieht so aus, dass Sie sich mit dem Tool "PsExec" behelfen. Die Software ist eine Art Telnet-Ersatz, mit der Sie wiederum das Sysinternals-Tool "Process Monitor" in der Session 0 auf dem Rechner starten können, so dass das Analyse-Werkzeug während des Ab- und Anmeldens weiterläuft. Eine andere Möglichkeit bietet Process Monitor selber: Mit Bordmitteln des Tools ist es möglich, das Boot Logging zu aktivieren. Bei einem Reboot startet nun Process Monitor sehr früh während des Bootvorgangs und schreibt die auftretenden Events nach *{SystemRoot}\Procmon.pmb*. Auf Basis dieser Informationen können Sie dann im Nachgang eine Fehleranalyse durchführen. *(ln)*

Weitere Infos zu den Tools finden Sie unter http://technet.microsoft.com/de-de/sysinternals/bb897553.aspx und http://technet.microsoft.com/de-de/sysinternals/bb896645.aspx

Trotz zahlreicher Anstrengungen diverser Hersteller für eine gesteigerte Fähigkeit, **Windows und Linux** zu integrieren, haben die beiden Systeme noch grundlegende Kommunikationsprobleme. Eins davon ist der **Zugriff auf das ext-Filesystem** von Windows aus, denn standardmäßig ignoriert Windows derartige Dateisysteme. Dergestalt kann ein Windows-Anwender das Linux-Dateisystem weder lesen noch beschreiben. Abhilfe schafft hier das "Ext2 Installable File System for Windows" von Stephan Schreiber. Das Freeware-Programm erlaubt Windows den vollen Lese- und Schreibzugriff auf Linux-ext2-Dateisysteme sowie den Zugriff auf Disketten, die mit dem ext2-Filesystem formatiert wurden. Auch ext3-Dateisysteme lassen sich mit dem Werkzeug in den Verzeichnisbaum einbinden, allerdings ohne die Vorzüge dieses Journaling-Dateisystems nutzen zu können. Die Software unterstützt Dateien, die größer als 4 GByte sind. Eine denkbare Nutzung ist beispielsweise, die Windows-Auslagerungsdatei *pagefile.sys* auf ein gemountetes ext2-Dateisystem zu legen. Vorsicht ist jedoch im Umgang mit den Zugriffsrechten geboten, denn diese berücksichtigt die Software nicht. Somit erhalten alle Benutzer eines Rechners vollständigen Zugriff auf alle Dateien der Linux-Partition. Dies gilt es zu beachten, sollten irgendwelche Passwörter in Dateien auf dem Linux-File-System hinterlegt sein, die normalerweise nur root auslesen darf. Nach dem Herunterladen ist der Treiber schnell installiert. Nun lassen sich in der Linux-Partition einfach Laufwerke zuweisen oder ändern. Über die Systemsteuerung unter "IFS Drives" findet sich das Werkzeug, welches ein einfaches Menü anbietet. Hier lässt sich der Linux-Partition ein Laufwerksbuchstabe zuweisen und schon findet sich die Platte im Windows-Explorer wieder. *(jp)*

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

Probleme mit der **Verfügbarkeit** oder dem **Datendurchsatz** im Netzwerk sind oftmals schwer einzukreisen. Um Layer 3-Problemen in Routern und Switchen auf die Schliche zu kommen, ist es hilfreich, das **NetFlow-Protokoll aufzuzeichnen und auszuwerten**. Die Datenströme dieser Geräte in Echtzeit zu analysieren, erlaubt eine zielgerichtete Verkehrsanalyse im Netzwerk.

Der freie Real-Time NetFlow Analyzer von Solarwinds erfasst, welche Arten von Datenverkehr auf dem Netzwerk vorkommen, wer welche Anteile davon sendet und stellt sie grafisch über die Zeitebene dar. NetFlow wird von allen Cisco-Routern und -Switches sowie zahlreichen anderen Herstellern unterstützt. Das Werkzeug stellt dem Administrator die Daten getrennt in ein- und ausgehenden Paketen dar. Die historische Ansicht bereitet die Daten getrennt nach Endgerät, Anwendung, Protokoll und mehr aus. In der freien Version besteht jedoch eine Beschränkung der Datensammlung auf 60 Minuten. Um die Funktionalität auf den Geräten freizuschalten, liefert Solarwinds ein eigenes Tool – den NetFlow Configurator – mit. Über SNMP-Befehle aktiviert dieses Werkzeug die Datensammlung am Router oder Switch. *(jp)*

Quelle: http://www.solarwinds.com/products/freetools/netflow_analyzer.aspx

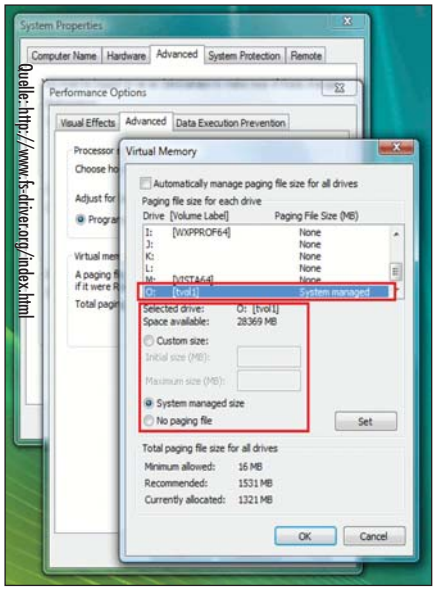


Bild 1: Die Windows-Auslagerungsdatei auf einem EXT-Filesystem

Versicherungsschutz für IT-Projekte

Gut gewappnet

von Erich Hartmann, Thorsten Thurau und Jens Krickhahn

Wenn ein IT-Projekt nicht optimal gelaufen ist und der Auftraggeber dadurch Verluste erleidet, muss der IT-Dienstleister mit Schadenersatzansprüchen rechnen. Insbesondere für kleinere IT-Unternehmen und Freelancer kann eine Forderung des Kunden unter Umständen existenzbedrohend werden. Damit IT-Profis gegen Risiken gut gewappnet sind, ist ein richtiger und auf die Branche zugeschnittener Versicherungsschutz von großer Bedeutung. IT-Administrator zeigt Ihnen, worauf Sie hierbei achten müssen.

Ein auf Antiviren-Software spezialisierter IT-Dienstleister stellte einem Kunden aus dem produzierenden Gewerbe ein Software-Update zur Verfügung. Nach der Installation brach aber das IT-System des Auftraggebers zusammen. Insgesamt 220 Arbeitsplätze waren von PC-Abstürzen, fehlerhaftem Versenden von E-Mails und langsamem Laden der Programme betroffen. Der Schadensersatz wurde mit 100.000 Euro angezeigt: erhöhter Personal- und Stundenaufwand, Produktivitätsverlust der Belegschaft, Produktionsausfall sowie Ausfall oder Verspätung von Lieferterminen trugen zu dieser Forderung bei.

Solche und ähnliche Schadensfälle passieren häufig: Laut einer Untersuchung von IAG Consulting scheitern 68 Prozent aller IT-Projekte – Computerworld.ch berichtet gar, dass 80 Prozent der IT-Projekte nicht wie geplant umgesetzt werden. Viele IT-Dienstleister sind sich nicht bewusst, welchen Risiken sie tagtäglich ausgesetzt sind und sind daher auch nicht umfassend versichert. Insbesondere bei Freelancern und kleineren IT-Dienstleistern ist zu beobachten, dass Versicherungen nicht ausreichend Aufmerksamkeit geschenkt wird. Viele schließen eine konventionelle Betriebshaftpflichtversicherung ab, die aber die am häufigsten auftretenden Schadensfälle überhaupt nicht abdeckt. Eine solche Versicherung deckt nämlich ausschließlich Personenschäden (Tötung, Verletzung des Körpers oder Schädigung der Gesundheit von Menschen), Sachschäden (Beschädigung, Verderben, Vernichtung oder Abhandenkommen von Sachen oder Geld) oder Vermögensfolgeschäden aus Personen- und Sachschäden, nicht aber reine Vermögensschäden.

Die häufigsten Risiken

In der Realität treten jedoch am häufigsten Erfüllungsfolgeschäden, Verzugsschäden oder gestörte Dauerschuldverhältnisse auf. Erfüllungsfolgeschäden entstehen wegen Nicht- oder Schlechterfüllung der Leistung und der Verletzung vertraglicher Nebenpflichten, zum Beispiel mit so schwerwiegenden Folgen wie entgangenem Gewinn aufgrund einer Betriebsunterbrechung beim Auftraggeber. Verzugsschäden oder Verzögerungen bei der Fertigstellung entstehen zum Beispiel bei einer umfangreichen Softwareentwicklung und -implementierung. Können beispielsweise beim Installieren einer Antiviren-Software die vereinbarten Zeiten nicht eingehalten werden, entstehen gestörte Dauerschuldverhältnisse.

Für die oben genannten Schäden gibt es jedoch eine spezielle Versicherung: die sogenannte "Errors & Omissions-Deckung" (E&O), die Vermögensschäden aufgrund von Fehlern und Unterlassungen deckt. Die aus dem angelsächsischen Raum stammende E&O ist auf die Bedürfnisse der IT-Branche zugeschnitten und in Deutschland auch als "Vermögensschadenversicherung" bekannt. Eine Vermögensschaden-Haftpflichtversicherung leistet im Gegensatz zur Betriebshaftpflichtversicherung Schadensersatz, wenn beim Auftraggeber reine Vermögensschäden entstehen (also nicht Personen- oder Sachschäden). Zu Vermögensschäden zählen zum Beispiel Schäden durch Programmierungs-, Implementierungs- und Beratungsfehler, Verlust oder Beschädigung von Daten inklusive der Kosten für die Wiederherstellung, Aufwendungen des Auftraggebers in Erwartung einer vertragsgemäßen Leistung (wie zum Beispiel die Anschaffung einer neu-

en EDV-Anlage für die in Auftrag gegebene Software) bis hin zu Betriebsunterbrechungsschäden beim Auftraggeber.

Versicherungsschutz als Wettbewerbsvorteil

Immer mehr Kunden überprüfen, ob die von ihnen beauftragten Softwarehäuser oder IT-Dienstleister auch einen adäquaten Versicherungsschutz haben. Im Schadensfall (zum Beispiel Erfüllungsfolgeschäden durch eine fehlerhafte Software) kann der Auftraggeber zwar Schadensersatzansprüche stellen und Recht bekommen, wird aber keine entsprechende Entschädigung erhalten, wenn der Dienstleister nicht versichert ist und mit dem eigenen Vermögen in Höhe des Schadens nicht aufkommen kann. Bei Ausschreibungen größerer Projekte ist die Vorlage einer entsprechenden Versicherung eine Grundvoraussetzung. Viele Auftraggeber führen vor der Vergabe der Projekte eine sogenannte "Due Diligence" (sorgfältige Prüfung und Bewertung des IT-Dienstleisters) durch. Daher kann eine umfassende Versicherung bei einer Ausschreibung einen Vorteil gegenüber den Mitbewerbern bedeuten.

Tipps zur optimalen Versicherung von IT-Dienstleistungen

Bei kleineren IT- und Software-Unternehmen ist der Bedarf an passenden Versicherungslösungen groß. Nicht jede Police, die auf dem Markt angeboten wird, bietet einen geeigneten Schutz für IT-Dienstleister. Versicherungsmakler können IT-Dienstleister bei dem Vergleich unterschiedlicher Versicherungsprodukte unterstützen. Die folgende Checkliste hilft, eine optimale IT-Haftpflichtversicherung zu finden:

1. Versicherungspolice prüfen: Zahlreiche IT-Dienstleister zahlen bereits Prämien für eine Betriebshaftpflichtversicherung, die längst nicht alle möglichen Risiken abdeckt. Wichtig ist zu prüfen, ob die bestehende Versicherungspolice eine weitgehende Deckung von Vermögensschäden bei Auftraggebern bietet.
2. Alle IT-Tätigkeiten absichern: IT-Dienstleister verändern und ergänzen zuweilen ihre Leistungs- oder Produktpalette. Dabei muss beachtet werden, dass der Versicherungsschutz alle Tätigkeiten des IT-Dienstleisters umfasst, sprich, dass im Vertrag keine Aufzählung der versicherten Tätigkeiten vorgenommen wird.
3. Erfüllungsfolgeschäden: Schäden resultieren überwiegend aus der Verletzung einer vertraglich vereinbarten Leistungspflicht zwischen IT-Dienstleister und Auftraggeber. Versicherungsschutz muss grundsätzlich alle Folgeschäden aus Schlecht- oder Nichterfüllung eines Vertrages beim Auftraggeber sowie Folgen mangelhafter Produkte oder Dienstleistungen, zum Beispiel Betriebsausfallschäden und entgangene Gewinne, abdecken.
4. Verzugsschäden bedenken: Mit der Police muss Sicherheit für die Folgen verspäteter Lieferung oder Leistung (Verzugsschäden) gewährleistet sein, und zwar für grundsätzlich alle Verzugsschäden und nicht mit Beschränkung auf bestimmte Ereignisse, die eine Verspätung ausgelöst haben.
5. Schutz während der Arbeit: Riskant ist die Tätigkeit des IT-Dienstleisters beim Auftraggeber auch schon, bevor der Auftraggeber die finale Freigabe des Auftrags erteilt hat. Daher ist Versicherungsschutz für Schäden wichtig, die zum Beispiel bereits während der Implementierungsphase eintreten, das heißt vor dem Abschluss und der Abnahme der Arbeiten.
6. Eigenschäden bedenken: Beim rechtmäßigen Zurücktreten des Auftraggebers von einem gescheiterten IT-Projekt kann es bedeutend sein, dass die bereits geleisteten Aufwendungen des IT-Dienstleisters abgesichert sind. Daher ist es insbesondere bei der Durchführung von größeren Projekten wichtig, dass der Versicherer den Ersatz der eigenen Aufwendungen des IT-Dienstleisters leistet, weil dieser bei berechtigtem Rücktritt des Auftraggebers nicht die Vergütung für seine vielleicht monatelangen Investitionen erhält.
7. Erfahrener Versicherer: Nicht alle gegen den IT-Dienstleister geltend gemachten Ansprüche sind berechtigt. Daher gewinnt, vor allem in Krisenzeiten, die Unterstützung des Versicherers an Bedeutung, der mit seiner Erfahrung gegen den IT-Dienstleister geltend gemachte Ansprüche prüft und gegebenenfalls als unberechtigt – notfalls gerichtlich – abwehrt.

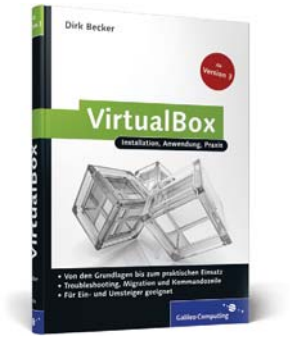
Neben wichtigen Deckungserweiterungen für Vermögensschäden bei Kunden des Versicherungsnehmers sollte automatisch auch der Eigenschaden bei Zerstörung der eigenen Website, grundsätzlich eine Vertrauensschadendeckung (zum Beispiel bei Betrug durch eigene Mitarbeiter) sowie optional eine Eigenschadenversicherung für vergebliche Aufwendungen des Versicherungsnehmers bei berechtigtem Rücktritt des Auftraggebers versichert sein. Die Betriebs- und Umwelthaftpflicht ist dabei etwa bei Hiscox ebenfalls über das Paket "Net IT" mitversichert. Damit müssen sich auch kleine IT-Dienstleister nicht vor großen Schäden fürchten. *(dr)*

Der studierte Rechtsanwalt Erich Hartmann ist Underwriting Manager bei Hiscox, unterrichtet unter anderem an der Deutschen Anwalt Akademie und ist Autor zahlreicher Publikationen zu versicherungs- und haftungsrechtlichen Themen.

Thorsten Thurau ist als Underwriter Berufliche Risiken mittelständische, national wie international agierende Maklerhäuser und Produktexperte für das Versicherungsgeschäft mit IT- und Telekommunikationskunden bei Hiscox tätig.

Jens Krickhahn ist bei Hiscox als Underwriting Manager TMT (Technology, Media und Telecommunications) tätig und trägt damit die Verantwortung über das gesamte TMT Portfolio bei Hiscox. Er ist zudem Dozent für IT-Haftpflicht an der Deutschen Versicherungsakademie.

VirtualBox



Virtualisierung im Unternehmensumfeld hat meist mit VMware, Citrix oder Microsoft zu tun. Doch auch VirtualBox, das mittlerweile zu Sun Microsystems gehört, ist eine ausgereifte Virtualisierungsumgebung. Dirk Becker liefert das passende Buch dazu, sein Titel "VirtualBox" ist nach eigener Aussage für Anfänger und Nutzer mit wenig Erfahrung gedacht. Das ist offensichtlich ernst gemeint, denn auf den ersten Seiten liefert der Autor die Geschichte des PC' und Grundlageninfos zur Virtualisierung. Doch zum Glück ist nach etwa 40 Seiten Schluss damit, danach widmet sich Becker ausschließlich VirtualBox. Das Tempo ist nicht nur für Anfänger geeignet, seine Erklärungen dürften auch bei fortgeschritteneren Benutzern gut ankommen. Sehr positiv ist, dass er die Kommandozeilen-Tools gleichberechtigt mit der grafischen Benutzeroberfläche behandelt. So sind bei allen Beispielen auch die entsprechenden Befehlszeilen mit angegeben.

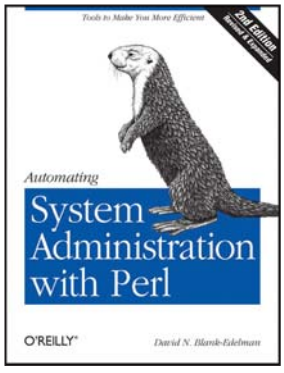
Schon das Kapitel zur Installation fällt angenehm auf, weil Becker zahlreiche Details erwähnt, die über das schlichte Motto "Screenshot mit Erklärung" hinausgehen. So wird Windows 7 und die Vergabe von Adminrechten ebenso besprochen wie die Installation unter Linux mittels erhöhter Privilegien (sudo). Auch wenn es an die Arbeit mit den virtuellen Maschinen geht, hat Becker einige Ideen parat, die ein Standardnutzer nicht unbedingt kennt – das Vergrößern und Verkleinern von virtuellen Partitionen per Boot-CD und Parted zum Beispiel. Hier könnten die Anleitungen jedoch ein wenig umfangreicher ausfallen, für ein Einsteigerbuch setzt der Autor auch stellenweise zu tiefe Linux-Kenntnisse voraus. Das gilt auch für das Kapitel, in dem Migrationen zwischen unterschiedlichen Virtualisierungsplattformen und physikalischen Computern erläutert werden. Die Listen mit Stichpunkten mögen für einen Profi ausreichen, der wird das Buch aber ohnehin nicht benötigen. Sehr praktisch hingegen ist die Befehlsübersicht am Ende des Buchs, in der alle Tools mit Optionen kurz erklärt werden. Das qualifiziert "VirtualBox" auch als Nachschlagewerk.

Fazit: "VirtualBox" ist ein gutes Einstiegswerk zur Virtualisierungsplattform von Sun. Entgegen der Ankündigung ist es nicht nur für Einsteiger brauchbar, auch ein Admin, der die Desktop-Virtualisierung ausreizen will, findet im Text viele wertvolle Hinweise. Abzüge gibt es nur, weil der Autor gerade bei den spannenden Kapiteln zur Migration und Integration zu kurz greift.

Elmar Török

Autor:	Dirk Becker
Verlag:	Galileo Computing
Preis:	34,90 Euro
ISBN:	978-3-8362-1374-5
Bewertung:	★★★½☆

System Administration with Perl



Über das Erleichtern von Adminaufgaben gibt es zahlreiche Bücher, fast allen liegt die Automatisierung zugrunde. Problematisch dabei ist oft die Wahl des passenden Werkzeugs. Es muss genügend Einfluss haben, um systemnahe Funktionen aufzurufen, darf aber nicht zu komplex in der Anwendung sein. Vor allem in der Unix-Welt ist Perl häufig die Antwort auf solche Anforderungen. Perl gilt zwar nicht als einfache Programmiersprache, ist aber sehr universell in der Anwendung und mit ein wenig Aufwand zumindest beherrschbar. Ob das verwaltete System unter Linux, Windows oder Mac OS X läuft, ist hingegen relativ egal. Wie David Blank-Edelman in seinem Buch "System Administration with Perl" erklärt, gibt es genügend Schnittstellen, um die gewünschten Aufgaben auf jedem Betriebssystem durchzuführen. Und so ist sein Buch zwar sehr auf die Administration fokussiert, streift aber alle Betriebssysteme, wenn auch mit einem Schwerpunkt auf den unix-basierten.

"System Administration with Perl" ist zwar kein Anfängerbuch, allerdings erklärt der Autor viele seiner Beispiele ausführlich, so dass auch Admins mit ausbaufähigen Perl-Kenntnissen nicht den Anschluss verlieren. Wo immer möglich, geht es um selbst erlebte Anwendungsfälle aus der Praxis. Der Autor erläutert beispielsweise den Umgang mit Dateien und Dateisystemen anhand einer Datenrettungsaktion bei seinem Notebook. Andere Kapitel kümmern sich um Directory Services, Sicherheit, E-Mail, SNMP, Logging und SQL-Administration. In den Lernabschnitten am Ende des Buchs zeigt er auch untypische Aufgaben für einen Admin auf und demonstriert Schritt für Schritt, was man mit Perl machen kann. Ebenfalls praktisch sind die Kurzanleitungen etwa zu SQL und SNMP im Anhang.

Fazit: "System Administration with Perl" ist mit Herzblut geschrieben und macht das Meiste aus dem recht trockenen Thema. Wer Perl beherrscht und damit typische Admin-Aufgaben automatisieren will, findet darin den passenden Begleiter. Für Perl-Anfänger steigt Blank-Edelman etwas zu hoch ein, der Leser benötigt sehr solide Programmierkenntnisse.

Elmar Török

Autoren:	David N. Blank-Edelman
Verlag:	O'Reilly
Preis:	30,95 Euro
ISBN:	978-0-596-00639-6
Bewertung:	★★★★☆

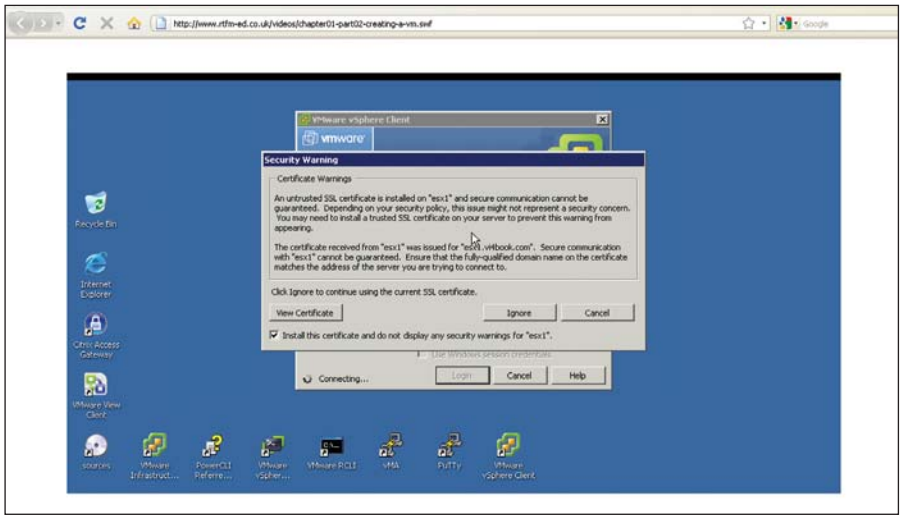
www.rtfm-ed.co.uk
vGuru

Besonders nervenden oder schlicht dummen Anwendern wirft der Systemverantwortliche – zumindest im Geiste – schon mal ein "Lies das verdammte Handbuch!" entgegen. Ein Blog unter diesem Motto, das auf Englisch unter dem Acronym RTFM noch ein wenig unfreundlicher daherkommt, verheißt vermeintlich nichts Gutes. Doch VMware-Blogger Mike Laverick versteht RFTM etwas anders und füllt Lücken, die bleiben, nachdem der Administrator jedes greifbare Stück Handbuch verinnerlicht hat. Dies hat Laverick, der seinen Blog seit Anfang 2005 betreibt, längst den Ruf eines VMware-Gurus eingebracht.

Das Herz der Website bildet Lavericks Blog, in dem er Neuigkeiten, Tipps und Tricks zur Arbeit mit ESX-Servern und vSphere 4 postet. Hier findet der Leser immer wieder Probleme, denen Laverick in der Praxis begegnet und natürlich die entsprechenden Lösungen. Darüber hinaus stellt der Autor hier interessante Produktneuigkeiten oder wichtige Termine für VMware-Verantwortliche vor. Neben den Kernprodukten des Anbieters interessiert sich Laverick zudem für den Einsatz der PowerShell, VMware-Zertifizierungen, VDI und vieles mehr.

Seinen Ruf als Guru untermauert der Blogger mit seinen umfangreichen Anleitungen, die teilweise sogar im Buchformat daherkommen, die erfreulicher Weise als kostenloser Download bereitstehen. In diese Kategorie fallen Lavericks Ausführungen zum "Site Recovery Manager" und "Virtual Infrastructure 3". Neben diesen umfangreichen Dokumenten hat der Leser aber auch Zugriff auf handlichere Guides, die vom "Quick Start to ESXi" über "Upgrade Guide to ESX 3 and Virtual Center 2" bis hin zu "P2V 2.x" viel Praxiswissen für den Systemadministrator bieten.

Und wer sowieso keine Lust hat, Handbücher zu lesen, der ist bei den kostenlosen Lernvideos der Seite bestens aufgehoben. So baut Laverick – dokumentiert in 16 Videos – beispielsweise eine vSphere-Infrastruktur von Null an auf. Verpackt in handliche Einzellektionen kann der Besucher der Seite selbst entscheiden, in welchem Kapitel er einsteigt. Die qualitativ hochwertigen Videos dokumentieren dabei jeden Arbeitsschritt und dauern zwischen zehn und 30 Minuten. Zwar stapelt Laverick im Einleitungstext zu den Videos tief ("It's just little ole me with decent mic and some screen grab software"), doch die geposteten Reaktionen der Zuschauer zeigen, dass er hier extrem nützliche Hilfestellungen gibt – jenseits des Handbuchs. *(jp)*



Mike Laverick stellt zahlreiche Lernvideos zu VMware kostenlos zur Verfügung

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 von IT-Administrator können Sie mit den folgenden Links 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:**

Sicherheit durch Datenkonvertierung

Unternehmen stehen vor der Aufgabe, ihre Datenbestände verfügbar zu halten. Zu den Hauptfeldern der Datenkonvertierung gehört die Medien-Konvertierung – also das Überspielen von bestehender auf aktuelle Hardware – und die Datenmigration. Jede Konvertierung ist dabei ein Projekt für sich. Oft sind die bestehenden Speicherlandschaften sehr unterschiedlich. Unser Online-Artikel beschreibt Grundkonstellationen und Lösungsmöglichkeiten bei der Datenkonvertierung.

www.it-administrator.de/themen/storage/fachartikel/69055.html

Anwenderbericht: Virenschutz an der Universität des Saarlandes

Das Netzwerk der Universität des Saarlandes erfüllt mit seiner vielschichtigen IT-Infrastruktur unterschiedliche Bedürfnisse: Es muss sowohl dem einzelnen Nutzer als auch den universitären Einrichtungen eine breite Palette an Ressourcen und Diensten bieten. Damit die Nutzer beim Studieren nicht von Viren, Würmern und Trojanern gestört werden, setzt die Alma Mater des Saarlandes mit derzeit über 15.500 Studierenden auf einen zuverlässigen Virenschutz.

www.it-administrator.de/themen/sicherheit/fachartikel/69056.html

Abgestufte Speicherverfahren: HSM, ILM und Tiered Storage

Abgestufte Speicherverfahren wurden in der Unternehmens-IT eigentlich immer betrieben. Auf verschiedenen Stufen eines Kontinuums von Servern stehen schnelle Primärspeicher für Daten für sofortigen geschäftlichen Zugriff, weniger schnelle Speicher für gelegentlichen Zugriff sowie Archivierungs-Medien für nicht-sofortigen Zugriff bereit. In unserem Online-Artikel stellen wir Grundlagen und Strategien für diesen, für den Anwender nicht sichtbaren Prozess dar.

www.it-administrator.de/themen/storage/fachartikel/69057.html

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

»Mir gefällt alles an meinem Job«

Timo Lehner (29) ist beim Logistik-Spezialisten Kurz in Wetzlar seit zwei Jahren als IT-Administrator tätig. Neben den klassischen Aufgaben einer Umzugsspedition bietet das Unternehmen auch logistische Individuallösungen, darunter eine Aktenarchivierung etwa für Krankenhäuser. Die IT-Landschaft ist eine wichtige Grundlage für den Betrieb dieser Anwendungen.

Welche Ausbildung haben Sie gemacht?

Nach der Schule habe ich ein Studium der Kommunikations- und Informationstechnik aufgenommen. Zurzeit mache ich darauf aufbauend eine berufsbegleitende Weiterbildung zum MCSE.

Warum sind Sie IT-Administrator geworden?

Die Aufgaben des IT-Administrators sind abwechslungsreich und interessant, man lernt ständig hinzu. Mir gefällt es, sowohl mit den Computern als auch mit den Anwendern zu arbeiten.

Welche IT-Umgebung betreuen Sie aktuell?

Ich bin als IT-Administrator für die gesamte IT sowie die Telekommunikation der Kurz Gruppe verantwortlich. Unsere Infrastruktur besteht aus 14 virtualisierten Maschinen, die auf drei physikalischen Servern eingerichtet sind. Hinzu kommen 60 Arbeitsplätze, davon einige mobile. Unsere IT-Landschaft läuft unter Windows Server 2003 und Windows XP sowie Windows Vista auf den Clients.

Welches Netzwerk- und Systemmanagement setzen Sie ein?

Wir nutzen das integrierte "MSP-Center Plus" von Adventnet. Damit können wir das Ticketing, Patching und die Netzwerküberwachung steuern.

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

Die grundlegende Herausforderung ist, die Infrastruktur Tag für Tag verfügbar zu halten. Die Virtualisierung und unsere stabile Umgebung erleichtert dabei vieles. So arbeiten wir im Storage-Bereich mit einem Netapp Metro-Cluster. Serverseitig verfügen wir über hochverfügbare Systeme von Fujitsu, die gut abgesichert sind.

Haben Sie besondere Vorkehrungen für das Desaster Management sowie für Backup und Recovery getroffen?

Wir haben stündliche Snapshots der virtuellen Server eingerichtet. Zusätzlich hierzu läuft eine HP-Bandsicherung, die täglich, wöchentlich und monatlich alle wichtigen Daten und virtuellen Server wegsichert.

Geburtstag: 18.11.1979
Familienstand: verheiratet, ein Kind
Hobbys: Familie, Freunde, Computer und Autos

Timo Lehner, IT-Administrator

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Wir planen eine Digitalisierung und Mikroverfilmung, um unsere Archivierungslösung zu erweitern. Die von uns gelagerten Kundenakten können dann digitalisiert zur Verfügung gestellt werden. Krankenhausakten beispielsweise müssen dann nicht mehr manuell aus dem Archiv geholt werden, sondern stehen über ein Webinterface per Mausklick zur Verfügung.

Was macht Ihnen an Ihrem Job am meisten Spaß?

Mir gefällt es, wenn der IT-Betrieb reibungslos läuft. Darüber hinaus macht es mir Spaß, mit den Usern zu arbeiten, ihnen bei Problemen zu helfen und nicht zuletzt sehe ich es als Aufgabe an, mögliche Probleme frühzeitig zu erkennen und schon im Vorfeld zu verhindern.

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

Es gibt keine Aufgabe, die ich ungern erledige. Mir gefällt an meinem Job einfach alles.

Was tun Sie für Ihre Fort- und Weiterbildung?

In nächster Zeit stehen Schulungen zu VMware und NetApp an. Hinzu kommen Infos aus Magazinen und dem Internet.

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

Glücklicherweise ist mein Fehlerkonto noch sauber. Aber ich bin ja auch noch nicht so lange IT-Administrator – vielleicht steht mir die große Panne noch bevor.

Was war Ihr größter Erfolg als IT-Administrator?

In den zwei Jahren, die ich nun als IT-Administrator arbeite, habe ich noch nicht das eine Projekt gehabt, auf das ich richtig stolz bin. Aber im Grunde genommen ist es ja schon ein persönlicher Erfolg, wenn alles Systeme laufen, das Unternehmen arbeiten kann und die Anwender zufrieden sind.

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

Unser Aktenarchiv ist durch ein biometrisches System geschützt. Kürzlich beschwerte sich ein Kollege, dass sein Zugang gestrichen sei. Es stellte sich heraus, dass er lediglich den falschen Finger auf das Lesesystem gelegt hat.

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

Datenschutz und Datensicherheit sind meiner Ansicht nach die entscheidenden Themen der kommenden Jahre. Hier gibt es bei vielen Unternehmen noch einen großen Nachholbedarf.

Das Interview führte Petra Adamik.

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

Was haben Sie zu sagen?

Die Ausgabe 12/09 erscheint am 1. Dezember 2009

Schwerpunktthema:

Mobiles Arbeiten, Home Office und Wireless

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

Unsere Ausgabe im **Januar** steht unter dem Schwerpunkt **Monitoring und Inventarisierung**. In unserer Test-Rubrik nehmen wir darin die Patch- und Threat-Management-Suite NetChk Protect 7 unter die Lupe. In einem unserer Workshops lesen Sie außerdem, wie Sie Hyper-V-Server fernwarten.

Als Schwerpunkt im **Februar** folgt dann das Thema **Sicherheit von Webservern und -applikationen**.

Im Test: Unified Messaging-Suite Tobit David.fx

Workshop: Wireless LAN im Unternehmen managen

Workshop: Virtual Private Networks im Eigenbau

Systeme: Neuerungen in Windows 7

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), *Redakteur*
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, Jörg Geiger, Marc Grote, Erich Hartmann, Jürgen Heyer, Jens Krickhahn, Sandro Lucifora, Thorsten Scherf, Ulf B. Simon-Weidner, Walter Steinsdorfer, Thorsten Thurau, Elmar Török

Anzeigen
Anne Kathrin Heinemann, *Anzeigenleitung*
verantwortlich für den Anzeigenteil
kathrin@it-administrator.de
Tel.: 089/4445408-20

Es gilt die Anzeigenpreisliste Nr. 6 vom 01.01.2009

LAC/2008

Produktion / Anzeigendisposition
Lightrays: Lorenz Mueller, Andreas Skrzypnik
dispo@it-administrator.de
Tel.: 089/452196-90
Fax: 089/452196-89

Druck
Ceská Unigrafie, a.s.
U Stavoservisu 1
CZ - 100 40 Prag 10

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 Beilagen von Galileo Computing und DatacenterDynamics, außerdem eine Zangenbanderole von IBM.

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

1&1 WEBHOSTING

HOMEPAGE

MIT BESTEN AUSSICHTEN FÜR 2010!

WEBHOSTING

Komplett-Lösungen für den perfekten Internet-Auftritt

z. B. 1&1 Homepage Business:
- 3 Inklusiv-Domains
- Neu: 5 GB Webspace
- UNLIMITED Traffic

3 Monate für 0,–*

~~14,99 €/Monat*~~

Nach 3 Monaten zahlen Sie günstige 14,99 €/Monat.*

0,– €/Monat in den ersten 3 Monaten*

SERVER

Hochleistungs-Server für gehobene Ansprüche

z. B. 1&1 Dedicated Server Dual-Core XL:
- AMD Opteron™ 1218
- 2 x 2,6 GHz
- UNLIMITED Traffic

3 Monate für 0,–*

~~99,99 €/Monat*~~

Nach 3 Monaten zahlen Sie günstige 99,99 €/Monat.*

0,– €/Monat in den ersten 3 Monaten*

.de-Domain ein ganzes Jahr lang für 0,– €/Monat!*

Viele weitere attraktive Angebote im Internet!

*Einmalige Einrichtungsgebühr 9,60 € (bei 1&1 Homepage Business 14,90 € und bei 1&1 Dedicated Server 99 €). 12 Monate Mindestvertragslaufzeit. Preise inkl. MwSt

MEMBER OF united internet

0180 5 / 001 535 14 ct/Min. dt. Festnetz, Mobilfunkpreise ggf. abweichend.

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

www.1und1.info

1&1