IT-ADMINISTRATOR.DE

03/2009

€ 12,60 ISSN 1614-2888

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

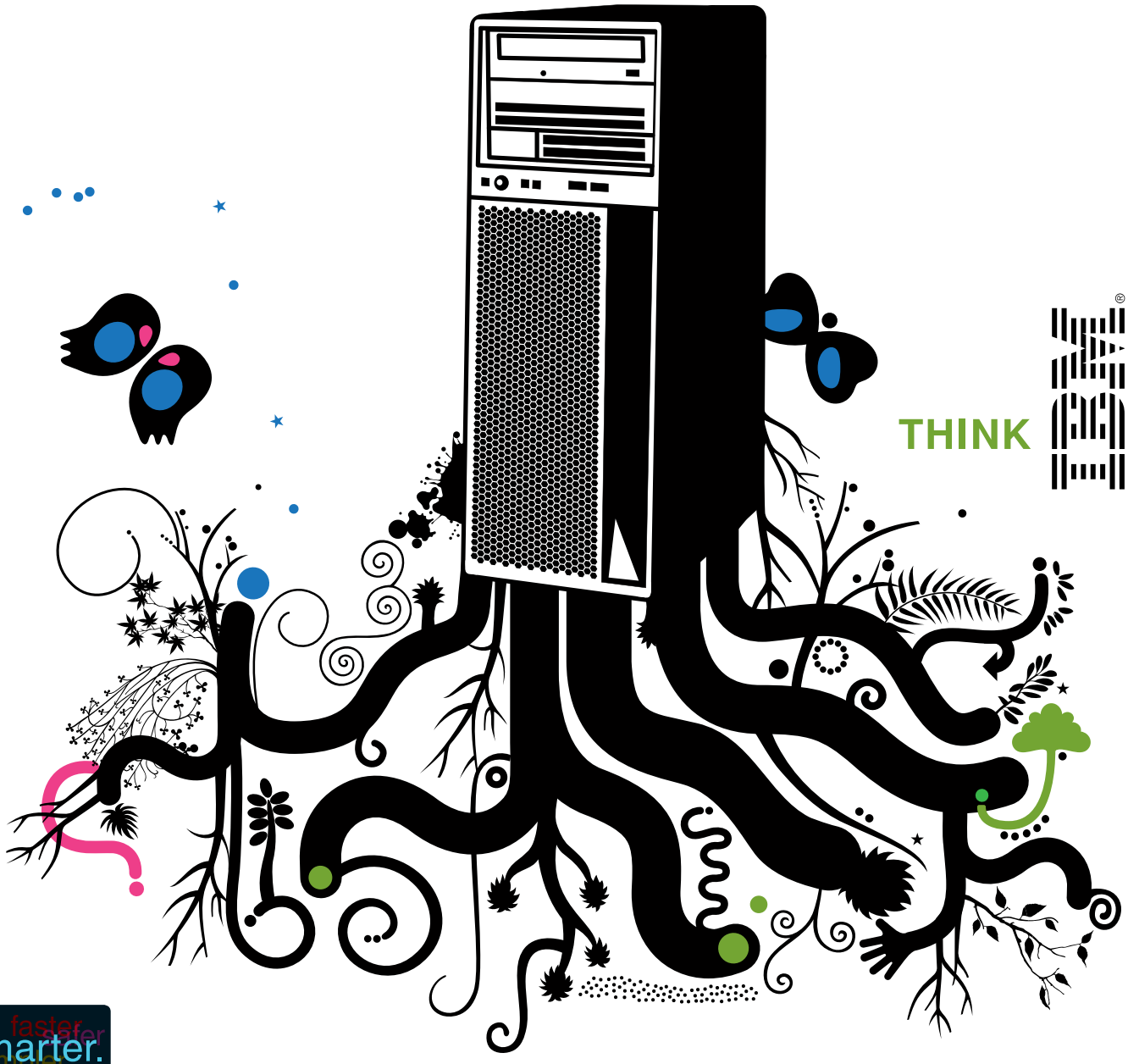
Netzwerkmanagement

4 196583 212905 03

ENERGIEKOSTEN SCHRUMPFEN – UND DIE LEISTUNG WÄCHST.

Sie möchten die Energiekosten senken – aber nicht auf Kosten der Leistung? Dann wird Ihnen IBM Dynamic Infrastructure gefallen: Es ist unsere Vorstellung davon, wie zukünftige Rechenzentren Ihr Geschäft voranbringen. Effizient, flexibel, umweltfreundlich und maßgeschneidert. Eine Vorstellung, die schon in mehr als 2.000 Unternehmen erfolgreiche Realität wurde.

Systeme, Software und Services
für einen smarten Planeten.
ibm.com/green/datacenter/de



faster smarter greener
smarter.
IBM auf der CeBIT '09, 3.– 8. März
Halle 2 & 9 ibm.com/de/cebit

O&M IBM IT 9/09

EDITORIAL

Auf los geht's los!

Liebe Leser,

wahrscheinlich ist auch in Ihrem Netzwerk die Amtssprache noch IPv4 – ein robustes und erprobtes Protokoll, dessen Funktionen und Aufbau jeder Admin im Schlaf erklären kann. Wozu dann die Mühe, sich mit neuen IP-Adressen im Stil von "ba3f:35a1:c32b:1913::1" zu befassen? Doch es gibt gute Gründe für IPv6. Der einfachste und zugleich meistgenannte: Die Adressen werden knapp.

Über vier Milliarden IP-Adressen stehen mit IPv4 zur Verfügung. Ein Pool, der angesichts immer mehr IP-fähiger Geräte langsam an seine Grenzen stößt. NAT hilft hier nur begrenzt weiter, wollen wir nicht irgendwann ein völlig fragmentiertes Internet aus etlichen Teilnetzen mit übersetzenden Routern und Gateways als Flaschenhälse und Stolpersteine. Da sind die $3{,}4 \times 10^{38}$ (oder 340 Sextillionen) möglichen IPv6-Adressen schon eine andere Zahl. Kein Wunder, ist doch eine IPv6-Adresse 128 Bit lang – ebenso wie ein derzeit noch sicherer AES-Schlüssel. Und auch verbesserte Sicherheitsstandards, effizienteres Routing und eine einfachere Administration sprechen für das neue Protokoll.

Warum tut sich also nichts, oder zumindest nicht viel? In der Tat wird der schwarze Peter im Kreis herumgereicht: Unternehmen fragen kein IPv6 nach, da es quasi keine Provider und speziellen Applikationen hierfür gibt. Provider und Softwarehersteller wiederum verzeichnen kaum eine Nachfrage und sehen daher keinen Bedarf zu investieren. Immerhin stellt – neben diversen Versuchsnetzen wie dem "6WiN" des Deutschen Forschungsnetzes (DFN) oder dem IPv6-DNS-Dienst von DynDNS – Windows Server 2008 einen größeren Schritt in Richtung IPv4-Ablösung dar. Erstmalig setzt das Betriebssystem primär auf das neue Protokoll, Version 4 ist nur noch als Fallback-Lösung mit an Bord. Und auch Windows Vista spricht bereits IPv6. Damit rückt die Migration auf Version 6 wenigstens unternehmensintern in greifbare Nähe.

Wie Sie unter Windows Server 2008 das neue Protokoll optimal nutzen, lesen Sie in unserem Sonderheft I/2009. Darin finden Sie auf 180 Seiten praxisnahe Workshops rund um das Serverbetriebssystem und dessen Einsatz im Netzwerk. In der März-Ausgabe des IT-Administrator zeigen wir zudem, wie verlässlich Ihnen Hyperic HQ bei der Netzwerküberwachung hilft und wie Sie Mac-Rechner über das LAN booten. Viel Spaß beim Lesen,

Ihr

Daniel Richey
Redakteur IT-Administrator

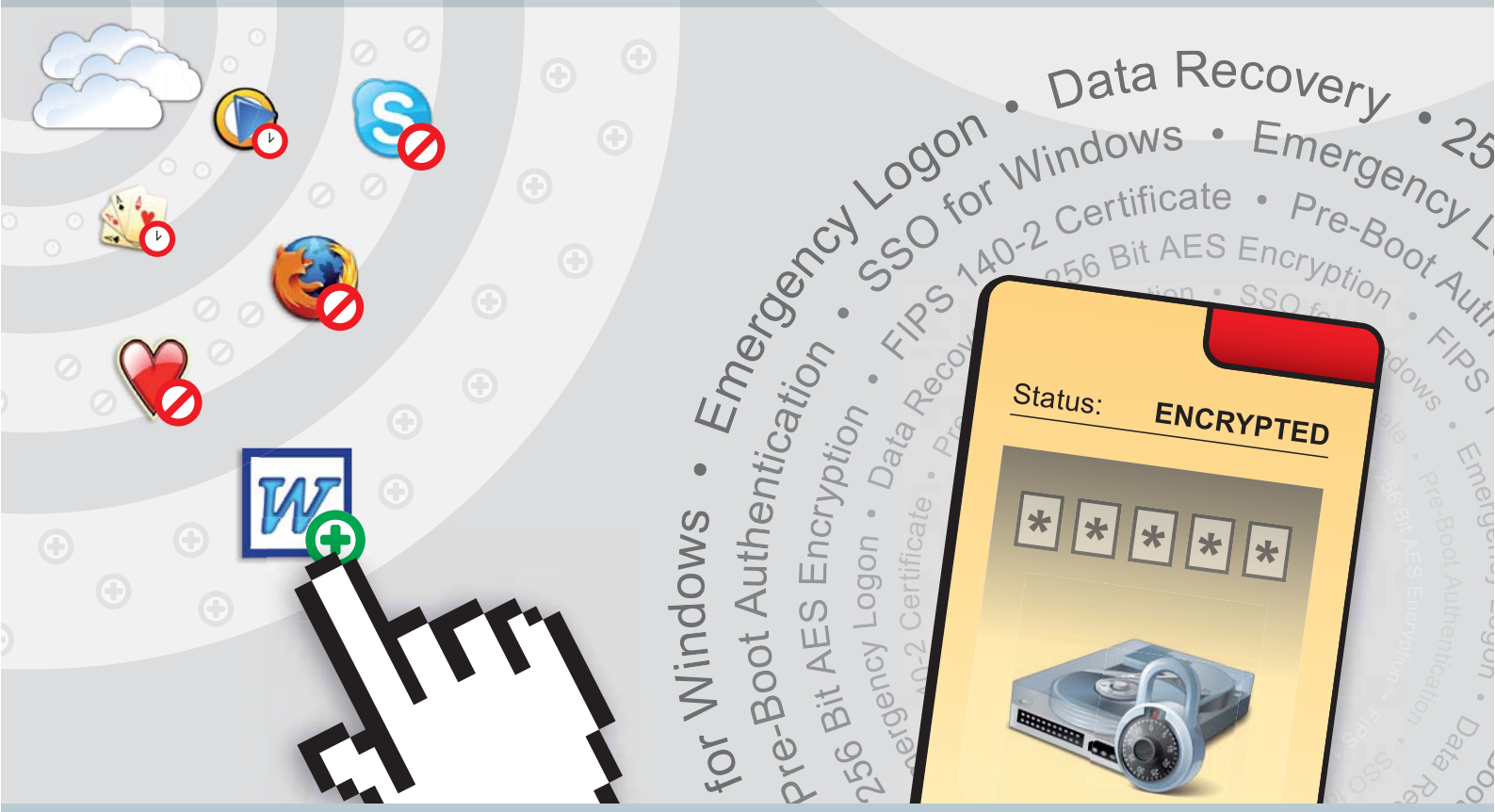
DriveLock 5.5

Intelligente Kontrolle mobiler Geräte

»DLP & DriveLock What comes next?

Live auf der CeBIT 2009 – Halle 11 Stand C27

CeBIT
HANNOVER
3.– 8. 3. 2009
cebit.com



DEN DATEN-LECKS AUF DER SPUR:
DRIVELOCK 5.5 R2 IST NOCH DICHTER UND NOCH SICHERER ALS JE ZUVOR.

Zusätzlich neu beim Application Launch Filter: Die laufend aktualisierte Online-Datenbank mit mehreren Millionen Anwendungen erleichtert die Konfiguration des Regelwerks genauso großartig wie der automatisierte Application-Scan Ihres Referenz-Arbeitsplatzes.

Testen Sie diese und weitere Neuerungen (übrigens auch zur Terminal Server Edition) live auf der CeBIT.
Und schauen Sie mit uns zusammen in die weitere Zukunft der Datensicherheit mit **DriveLock**.

Referenzen / Informationen / Testversion
» **WWW.DRIVELOCK.DE**

Ein perfektes Praxis-Tool von CenterTools. Empfohlen und getestet von Fachblättern und erfolgreich eingesetzt bei vielen großen Unternehmen Europas, Nordamerikas und Asiens.

CenterTools

INHALT

IT-Administrator – Ausgabe März 2009

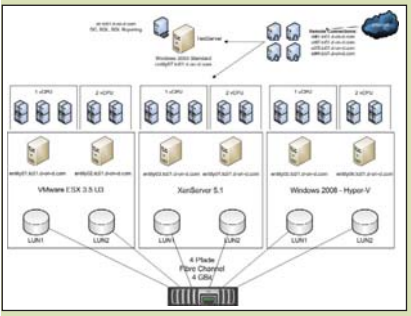
Netzwerkmanagement

Im Test: Hyperic HQ 4.01 Enterprise

Netzwerk- und Systemmonitoring ist besonders komfortabel mit grafischer Oberfläche und visualisierten Messergebnissen. So erkennt der Administrator mit einem Blick, wo Störungen auftreten. Hersteller Hyperic wollte als Firmennamen eigentlich einen aus zwei Pflanzenarten gebildeten Fantasienamen verwenden, doch ein Fehler beim Ausfüllen der Papiere ließ lediglich den ersten Teil des Antidepressivums Johanniskraut (Hypericum perforatum) stehen. Kein schlechtes Omen für eine komplexe Software, sich auch im Namen gleich auf das Wesentliche zu beschränken. Wir haben für Sie getestet, ob Hyperic HQ tatsächlich geeignet ist, möglichst nebenwirkungsarm die dunklen Wolken aus dem Gemüt eines geplagten Admins zu vertreiben.

Seite 21

Rechenzentrum auf Knopfdruck



Immer wieder sieht sich der IT-Verantwortliche mit der Anforderung konfrontiert, Software oder Hardware zu testen. Oft steht noch irgendwo ein alter Server zur Verfügung, der dann für diese Aufgabe genutzt wird. Problematisch wird es jedoch, sobald die Applikation eine größere Infrastruktur erfordert oder wenn aussagekräftige Lasttests erfolgen sollen. Als schwierig erweist sich dabei ebenfalls, dass meistens die Zeit für die Durchführung ausgiebiger Tests und deren Vorbereitung – allein der Aufbau der Hardware – fehlt. Als Alternative bietet sich die Anmietung einer kompletten Testinfrastruktur an. In diesem Beitrag zeigen wir Ihnen anhand eines realen Lasttests die Arbeit mit und in einem "Remote Rechenzentrum".

Seite 51

NAP unter Windows Server 2008 (2)

Mit dem Windows Server 2008 erhalten Administratoren auch das Feature "Network Access Protection". Im ersten Teil unserer Workshopserie haben wir die Grundlagen des Netzwerkschutzes und erste Konfigurationsschritte aufgezeigt. Im zweiten Teil befassen wir uns mit der clientseitigen Einführung von NAP und dem DHCP-basierten Schutz.

Seite 56

Mit der "GeNUCard" müssen mobile Anwender nicht auf eine Hardware-Firewall verzichten

Firewall für die Hosentasche

GeNUA will mit der **GeNUCard** auch auf mobilen Rechnern für Sicherheit sorgen. Die Karte findet Platz im **Express Card Slot** und beinhaltet drei zentrale Sicherheitssysteme: **eine Firewall, ein VPN-Gateway und eine Token-Funktion.** Sobald die Mini-Firewall in das Notebook gesteckt wird, kontrolliert sie die gesamte Datenkommunikation über die externen Schnittstellen in Richtung Firmennetz. Die Firewall prüft, ob die gewünschte Verbindung zulässig ist, und das Gateway baut dann ein verschlüsseltes Virtual Private Network (VPN) zur eingerichteten Gegenstelle auf. Über die Token-Funktion erfolgt die Authentisierung sowie das Key Handling. Ein weiteres Sicherheitsmerkmal der IPv6-fähigen Steckkarte ist die Unabhängigkeit vom gesicherten Laptop, da die Lösung mit eigenem Betriebssystem läuft. So soll das Sicherheitspaket funktionsfähig bleiben, selbst wenn der Laptop durch unvorsichtigen Umgang bereits kompromittiert sein sollte. Die Karte verfügt über einen Ethernet-Anschluss für Internet und LAN, einen USB-Port für UMTS, GPRS und den Anschluss eines Token sowie über einen Einschub für eine SD-Card. Die kompakte Sicherheitslösung ist ab sofort zu Preisen ab 375 Euro erhältlich. *(ln)*

GeNUA: www.genua.de/produkte/genucard/

99 Speicherplatten

Mit dem **MSA2300fc G2** bringt **HP** ein **Fibre Channel-basiertes Storage Array** auf den Markt, das bis zu 99 Festplatten fasst. Das Speichersystem eignet sich laut HP für die Storage-Konsolidierung in mittelständischen Unternehmen oder für Zweigstellen größerer Firmen. In dem zwei Höheneinheiten messenden Gehäuse lassen sich sowohl SAS- als auch SATA-II-Laufwerke implementieren. Maximal können mit einer Übertragungsgeschwindigkeit von 4 GBit/s **im SAN bis zu 60 TByte** bereitgestellt werden. Die Neuerscheinung unterstützt neben x86-basierten Systemen unter Windows und Linux auch HPs Integrity Server mit dem Betriebssystem HP-UX. Das MSA2300fc steht in zwei Varianten zur Verfügung. Diese unterstützen entweder 3,5-Zoll- oder 2,5-Zoll-Laufwerke. Weiterhin kann der Administrator zur Sicherung von Daten auf bis zu 255 Snapshots zurückgreifen. Die SAN-Komponente ist zu einem Listenpreis ab 6.400 Euro erhältlich. *(ln)*

Hewlett-Packard: www.hp.com

Das SAN-Modul "MSA2300fc G2" fasst bis zu 60 TByte Daten

Aktualisierungszentrale

UpdateStar veröffentlicht Version 3.2 der gleichnamigen **Aktualisierungssoftware**, die Anwender über **Updates und Patches** für auf dem Rechner installierte Windows-Programme auf dem Laufenden hält. Insgesamt soll das Tool **mehr als 135.000 Softwareprodukte** erkennen. Damit diese Zahl in Zukunft kontinuierlich wächst, setzt der Anbieter auf die Zusammenarbeit mit den Nutzern, die die Datenbank selbst aktualisieren und pflegen können. Vor der endgültigen Freigabe werden alle Aktualisierungen dann durch den Hersteller auf Richtigkeit geprüft. Neben der Update-Funktion beinhaltet das Werkzeug zudem eine Softwareverwaltung, mit der sich Anwendungen einfacher und schneller deinstallieren lassen sollen als mit Windows-Bordmitteln. Ferner besteht die Möglichkeit, komplette Software-Setups zu exportieren, um die Programme in exakt dem gleichen Versionsstand an einem anderen Rechner zur Verfügung zu stellen. Die für den gewerblichen Gebrauch benötigte Premium-Edition kostet mit einer Lizenzlaufzeit von einem Jahr rund 20 Euro. Günstiger fährt, wer das Werkzeug für mehrere PCs einkauft. Ab 50 Lizenzen reduziert sich der Preis auf knapp 10 Euro pro Rechner und Jahr. *(ln)*

Updatestar: www.updatestar.com/de/

"Updatestar" kümmert sich um Aktualisierungen für über 135.000 Programme

Der "Multichannel VPN Router 300" von Viprinet bündelt unterschiedliche WAN-Leitungen zu einem Kanal

Schneller durch Bündelung

Mit dem **Multichannel VPN Router 300** stellt **Viprinet** ein Gerät vor, mit dem sich Unternehmensstandorte per WAN-Bündelung vernetzen lassen. Dabei können beliebige unterschiedliche Leitungsarten wie DSL und UMTS sowie verschiedene Service-Provider kombiniert werden. Die Bandbreiten dieser Leitungen stehen dann in Summe im LAN zur Verfügung. Auf diese Weise ist es möglich, durch eine Bündelung von drei UMTS-Zugängen auch an weißen Flecken auf der DSL-Landkarte für einen breitbandigen Internetzugang zu sorgen. Durch die **Verteilung des Ausfallrisikos** auf mehrere ISP-Netze will der Hersteller zudem eine hohe Verfügbarkeit der Internetanbindung gewährleisten. In insgesamt drei Modulslots nimmt der Router beliebige Modemkarten auf. Die Stromversorgung erfolgt über ein externes Netzteil. Ein optional erhältliches KFZ-Netzteil erlaubt zudem den mobilen Betrieb. Die maximale Durchsatzrate beträgt 100 MBit/s, NAT und Port-Forwarding werden unterstützt. Eingerichtete VPN-Tunnel lassen sich mit SSL/AES verschlüsseln. Das 1 kg schwere und 147 x 130 x 177 mm messende Gerät ist ab sofort zu einem Preis von 890 Euro erhältlich. *(ln)*

Viprinet: www.viprinet.de

Erweiterte Abschussliste

ZyXEL setzt in den UTM-Appliances **ZyWALL USG 100** und **200** ab sofort auf einen eigenen Virenschutz. Die selbst entwickelte Engine verfügt laut Hersteller über **mehr als 15.000 Schädlingssignaturen**. Käufer des elektronischen Torwächters für kleinere Büros können auf Wunsch zwar weiterhin auf den bisher implementierten Scanner von Kaspersky zurückgreifen, dieser umfasst in seiner Datenbank laut ZyXEL jedoch lediglich 3.200 Signaturen. Neben dem Blocken von Viren soll die Appliance auch den Kampf gegen Spam übernehmen und das Unternehmen **mit einer ICSA-zertifizierten Firewall** vor DoS-Attacken bewahren. Modell 100, das für die Nutzung durch bis zu 20 User gedacht ist, verfügt über zwei WAN- und fünf LAN-Ports und erlaubt maximal 50 gleichzeitige auf IPSec basierende VPN-Verbindungen. Firewall und Virenschutz von Variante 200 erlauben höhere Durchsatzraten, außerdem stellt das Gerät bis zu 50 Anwendern eine größere Zahl an simultan möglichen VPN-Verbindungen bereit. Die Hardwarepreise betragen 495 respektive 665 Euro. Dazu kommen Nutzungslizenzen, die je nach Gerät und Vertragsdauer bei rund 100 Euro pro Jahr beginnen. *(ln)*

ZyXEL: www.zyxel.de/web/index.php

ZyXEL stattet die UTM-Appliance "ZyWALL USG 100 / 200" mit einem umfassenderen Virenschutz aus

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

Overland Storage stellt die nächste Generation seiner skalierbaren und automatisierten Tape Libraries vor. Die **NEO E-Serie** lässt sich über SCSI, FC oder SAS ins SAN einbinden und unterstützt LTO-4 HH-Bandlaufwerke und Direct-Connect-Schnittstellen. Modell 2000E verfügt über 30 bis 240 Cartridges pro Modul, während das Modell 4000E mit 60 bis 240 Bandkassetten ausgestattet ist. Beide Varianten sollen sich beliebig kombinieren und erweitern lassen. Im Gegensatz zu den Vorgängermodellen erfolgt die Partitionierung nun intern und ohne Einsatz einer speziellen VIA-Karte. Administratoren können die Systeme per Fernzugriff überwachen und eventuelle Fehler remote analysieren. Die Bandbibliotheken sind ab sofort zu einem Einstiegspreis ab 9.645 Euro erhältlich. *(ln)*

www.overlandstorage.com/german/

Von **VMware** kommt mit dem **View Open Client** der erste Open Source-Client für virtuelle Desktop-Umgebungen auf den Markt. Anwendern soll es so möglich sein, von einem unter Linux laufenden Thin Client auf einen entfernten, von VMware View bereitgestellten Windows-Desktop zuzugreifen. Das Release unterstützt sicheres Tunneling mittels SSL, Zwei-Faktoren-Authentifizierung mit RSA SecurID, ein Add-On RPM-Paket für Novells SUSE Linux Enterprise Thin Client (SLETC) und eine vollständige Kommandozeilen-Schnittstelle. Die Hardware-Anforderungen für den Thin Client sind gering: Ein i586-kompatibler Prozessor, 2 MByte Speicherplatz sowie 128 MByte RAM sollen laut Hersteller ausreichend sein. *(ln)*

http://code.google.com/p/vmware-view-open-client/

NCP bietet mit dem **Secure Entry Client** die erste VPN-Suite für Windows 7 an. Wie der neueste Streich aus dem Hause Microsoft befindet sich der VPN-Client im Betastadium und kann für 30 Tage kostenlos genutzt werden, um etwa die Einbindung von Teleworkern auch unter dem neuen Betriebssystem rechtzeitig testen zu können. Die Software soll kompatibel zu den Gateways aller namhaften VPN-Hersteller sein und bietet Leistungsmerkmale wie einen eigenen Dialer, eine dynamische Personal Firewall und die integrierte Unterstützung einer großen Anzahl von Mobile Connect Cards. Administratoren soll die Verwaltbarkeit durch Network Access Control-Funktionen (NAC), PKI-Unterstützung, die Integration von Identity- und Access-Management-Systemen sowie Verzeichnisdiensten auf LDAP-Basis wie Microsoft Active Directory besonders einfach gemacht werden. *(ln)*

www.ncp-e.com/de/downloads/software.html

Bis zu 4 TByte stellt der NAS-Speicher "NSS3000" von Cisco im Netzwerk bereit

Cisco-Storage nicht nur für Große

Auch **Cisco** nimmt kleinere **NAS-Geräte** in sein Portfolio auf und veröffentlicht mit dem **NSS3000** einen Netzwerkspeicher mit vier SATA-Festplatteneinschüben. Laut Hersteller ist das für 15 User ausgelegte Gerät für kleinere Unternehmen gedacht, die es als Fileserver betreiben oder zum Backup wichtiger Daten verwenden wollen. Das mit einem Linux-Betriebssystem ausgestattete NAS stellt dabei maximal 4 TByte an Speicherkapazität zur Verfügung. Die Magnetspeicher lassen sich im laufenden Betrieb austauschen und unter den RAID-Modi 0, 1, 5 und 10 verwalten. Außerdem ist ein Betrieb im JBOD-Modus möglich. Neben der manuellen Bestimmung von Zugriffsrechten kann der Administrator **Benutzerdaten aus dem Active Directory übernehmen**. Die 256 Bit AES-Verschlüsselung soll für die Sicherheit der abgelegten Daten sorgen. Durch eine Unterstützung der Dateisysteme von Microsoft Windows, Macintosh OS X und Linux stellt das NSS3000 die gespeicherten Dokumente auch in einer heterogenen Umgebung sämtlichen Clients zur Verfügung. Ebenso lässt sich per FTP auf die Storage-Komponente zugreifen. Der NAS-Speicher ist ab sofort verfügbar und kostet ohne Festplatten rund 1.100 US-Dollar. *(ln)*

Cisco: www.cisco.com/en/US/products/ps9965/index.html

Virtueller Backup-Server

Arkeia Software ergänzt sein Angebot an Sicherungslösungen um eine **virtuelle Backup-Appliance**. Version 8.0 von **Network Backup** steht erstmals auch als System-Image für eine virtuelle Maschine unter VMware zur Verfügung. Laut Hersteller eignet sich die Software somit besonders für den Betrieb in heterogenen Umgebungen: Ein Agent wird auf dem ESX-Hypervisor installiert und ermöglicht das Backup einer oder mehrerer virtueller Maschinen auf diesem Rechner, egal welches Betriebssystem oder welche Applikationen auf der virtuellen Maschine vorhanden sind. Das Programm **läuft unter ESX sowie ESXi** und kommt des Weiteren mit Virtual Tape Libraries (VTL) zurecht. Vorteile sieht der Anbieter neben der einfacheren Administrierbarkeit vor allem in der Konsolidierung von Netzwerken, da kein eigener Backupserver mehr benötigt wird. Der Einstiegspreis für die virtuelle Appliance mit drei Agenten liegt bei 2.000 Euro. Die neuen Features von Version 8.0 wie eine verbesserte Benutzeroberfläche und erweiterte Report-Funktionen stehen weiterhin auch auf einer Hardware-Appliance zur Verfügung. *(ln)*

Arkeia: www.arkeia.com

Thin Client-Baukasten

IGEL hat sein **Thin Client-Angebot** überarbeitet und bietet fünf neue Serien an. Charakteristisch für das **Universal Desktop-Konzept** ist dabei die bedarfsgerechte, modulare Auswahl aus fünf Hardwareplattformen, drei Betriebssystemen und drei Firmwarepaketen. Die Einstiegsserie UD2 ersetzt die bisherige "Smart"-Reihe und ist mit einem Via Eden 400 MHz-Chipsatz ausgestattet. Die UD3-Serie folgt der kompakten Allroundserie "Compact" nach und besitzt einen Via Eden-Chipsatz mit 800 MHz. Beide Modellreihen sind VESA-montierbar, also beispielsweise auf der Monitorrückseite. Das Highend-Modell UD5 fasst die bisherigen Modellreihen "Winestra" und "Premium" zusammen und wartet mit einer Via C7-CPU mit 1,5 MHz und einem freien PCI-Slot auf. Die UD7-Serie entspricht dem Quadview-Thin Client "PanaVeo" mit vier Videoausgängen und die UD9-Serie der früheren "Elegance"-Reihe. Eine wesentliche Neuerung in der Produktstrategie des Herstellers sind dabei die drei aufeinander aufbauenden Firmwarepakete "Entry", "Standard" und "Advanced". Dieses **modulare Baukastensystem** erlaubt Kunden eine bedarfsgerechte Auswahl an lokalen Softwaretools, -clients und unterstützten Protokollen, die sie für den direkten Zugriff auf ihre aktuellen und künftigen zentralen IT-Infrastrukturen benötigen. Die neuen Firmwarepakete bietet IGEL in der Regel für drei interne Betriebssysteme an: IGEL Linux, Windows Embedded CE 6.0 und Windows Embedded Standard 2009 als Nachfolger von XP Embedded. Die neuen Modelle sind ab sofort erhältlich. Die Preise beginnen bei 224 Euro. *(dr)*

IGEL: www.igel.de

Die neuen Thin Clients von IGEL sollen auch dank umweltfreundlicher Materialien und niedrigem Stromverbrauch überzeugen

Kaspersky
Open Space
Security

Optimaler Schutz für dynamische Unternehmens-Netzwerke

Kaspersky Open Space Security schützt Firmen-Netzwerke jeder Größe inklusive externer Mitarbeiter und mobiler User zuverlässig – und wächst mit allen zukünftigen Anforderungen an die Unternehmens-IT.

Ihre Vorteile:

- Optimaler Schutz vor Viren, Spyware und Hackern auf allen Netzwerk-Ebenen
- Proaktiver Schutz der Workstations vor bisher unbekannten Viren
- Echtzeit-Scan von Mails und Internet-Traffic
- Automatische Isolierung infizierter Rechner
- Zentrale Administration mit umfangreichem Berichts-System

Überzeugen Sie sich von der optimalen Skalierbarkeit und dem flexiblen Lizenzmodell unserer Produkte.

CERTIFIED FOR Windows Server 2008

CITRIX ready

Kaspersky Open Space Security hat als erste Antiviren-Software weltweit das Zertifikat „Citrix Ready“ erhalten.

Besuchen Sie uns zur CeBIT 2009!
Halle 11, Stand D37.

KASPERSKY lab

www.kaspersky.de

IT-Administrator-Workshop am 1. April in Eschborn/Frankfurt am Main

Ein Schritt aus der Unsicherheit

ITANet
Die System und Netzwerk User Group

ITANet Schirmherrschaft:
REALTECH

IT-Administrator Trainings-Partner
fast lane

von John Pardey

In Sachen Sicherheit der IT muss der Administrator stets Augen und Ohren offenhalten. Überlegungen zur Sicherheit neuer Applikationen und wie diese zum Schutz des Unternehmens beitragen können, gehören ebenso wie Fragen des IT-Rechts – Stichwort Compliance – zu den Aufgaben der IT-Security. Daher bieten wir unseren Abonnenten am 1. April einen Workshop, der ausgewählte Security-Themen adressiert.

Ein Nachmittag reicht selbstverständlich nicht, die ganze Bandbreite sicherheitsrelevanter Fragestellungen auch nur annähernd zu behandeln. So entschieden wir uns, eine Auswahl aktueller Themen aufzubereiten und eingehend zu beleuchten. Die Agenda umfasst somit Vorträge zur Security von Windows 7, zu wichtigen Rechtsfragen und der immer wichtiger werdenden Storage-Security.

Den Workshop eröffnen wird Michael Kranawetter, Chief Security Advisor Microsoft Deutschland, den wir für die Vorstellung der Security von Windows 7 gewinnen konnten. Kranawetter wird aufzeigen, ob und wie die Securityfeatures des neuen Client-Betriebssytems seit Windows Vista weiterentwickelt wurden. Da Windows 7 sich aktuell noch in der Betaphase befindet, stellt der Workshop sicher auch eine hervorragende Gelegenheit für die Teilnehmer dar, einen "Insider" intensiv zu dem neuen Client zu befragen.

Der zweite Vortrag des Tages ersetzt sicher kein Jurastudium, obwohl es vor dem Hintergrund der Compliance mit Themen wie GDPdU oder Basel II manchmal den Eindruck macht, der Administrator von heute brauche ein ebensolches. Vielmehr bieten wir Ihnen einen schnellen Ritt durch wichtige rechtliche Themen, die Ihren Arbeitsalltag betreffen – anschnallen, bitte!

Dazu befassen sich Thorsten Logemann, Geschäftsführer der intersoft consulting services GmbH aus Hamburg, und seine Kollegin Faezeh Shokrian, Consultant und Rechtsanwältin, selbstverständlich auch mit der schier allgegenwärtigen Compliance.

Den Abschluss des Workshops bildet ein Vortrag zur Sicherheit von Speichersystemen. Ein Thema, das, insbesondere vor dem Hintergrund der Virtualisierung, immer wichtiger wird.

Wie gewohnt ist der Workshop am 1. April für alle Abonnenten kostenlos. Alle Informationen zur Veranstaltung und Anmeldung finden Sie im nebenstehenden Kasten. Wir würden uns freuen, Sie in Eschborn bei Frankfurt begrüßen zu dürfen.

Agenda und Dozenten des Workshops

"Windows 7 Security"

Michael Kranawetter ist Chief Information Security Advisor für Microsoft und in dieser Funktion Ansprechpartner für Chief Information Security Officers, unter anderem für die Themen Governance, Risk and Compliance und für die Microsoft-Informationssicherheitsstrategie. Er konnte seine Erfahrung in der Informationssicherheit durch drei internationale Zertifizierungen (CISM, CISA, CIPP) bestätigen.

Michael Kranawetter, Microsoft

"Der Admin und akuelle Fragen des IT-Rechts"

Thorsten Logemann ist Geschäftsführer der intersoft consulting services GmbH und entwickelt Strategien für die von ihm konzipierten Beratungssparten IT-Sicherheit, Datenschutz und IT-Compliance. Logemann sammelte zuvor umfangreiche Erfahrungen in den Bereichen Systemadministration, insbesondere auf den Gebiet Sicherheitslösungen und Risikomanagement.

Thorsten Logemann, intersoft consulting services GmbH

Faezeh Shokrian ist Rechtsanwältin und Consultant für Datenschutz. Sie ist externe betriebliche Datenschutzbeauftragte für Unternehmen, erstellt Datenschutzdokumente/-konzepte und berät zu Fragen derIT-Compliance. Sie verfügt über bereichsübergreifende juristische Kompetenzen und Erfahrung in unterschiedlichen Projekten.

"Storage-Security"

Der Dozent war zum Redaktionsschluss dieser Ausgabe noch in Absprache

Vortrag unseres Workshop-Partners:
Netzwerksicherheit durch Transparenz:
Welchen Beitrag Business Process Management und Business Service Management leisten können

Referent: Dr. Kürsad Goegen, Product Manager IT Service Management Realtech

Ort: Fast Lane Institute for Knowledge Transfer, Ludwig-Erhard-Straße 3, 65760 Eschborn

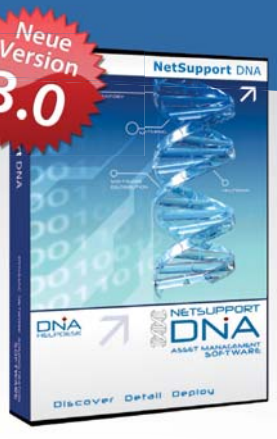
Teilnahmegebühren:
Für IT-Administrator-Abonnenten kostenlos.

Anmeldung bis zum 23. März unter
https://www.it-administrator.de/usergroup/termine/51980.html

Workshop "Netzwerksicherheit" am 1. April 2009

Vista Kompatibel

Komplettes Asset Management



Umfassendes Asset Management - Jederzeit und Überall

Für Sie ist es nichts Neues: Eine vollständige Inventarisierung von PC- und Serversystemen ist wichtig, die Steuerung der Nutzung von Anwendungen und Internet ist notwendig und eine Verteilung von Software-Anwendungen über das Netzwerk ist definitiv zeitsparend!

Und Sie wissen, dass die Anforderungen in modernen Unternehmen inzwischen viel größer sind: Es geht um die zentrale Wartung und Verwaltung beliebig vieler Netzwerke über das Internet – und dies ist die Domäne von NetSupport DNA.

NetSupport DNA ist ein vollständig modular aufgebautes System zur Lizenzverwaltung und Inventarisierung von umfangreichen Hard- und Software-Installationen. Neben frei konfigurierbaren Benachrichtigungs- und Alarmfunktionen bietet es ein umfassendes Überwachungs-System für die Nutzung des Internet und der installierten Software.

NetSupport DNA bietet darüber hinaus auch eine vollständige AD-Integration, marktführende Fernwartungsfunktionen und optional einen ITIL-basierenden Helpdesk. Und selbstverständlich lassen sich Software-Anwendungen und Daten mittels Push & Pull-Funktionen komfortabel über Internet und LAN im Netzwerk verteilen.

Und NetSupport DNA leistet jetzt noch mehr: Dank des neuen integrierten Communication Gateways ist die sichere Interaktion zwischen den einzelnen Komponenten im Netzwerk ein Kinderspiel – und das ganz ohne den Einsatz eines VPN oder die umständliche Anpassung von Firewalls und Netzwerkfunktionen.

Viele gute Gründe, um noch heute zu testen, wie NetSupport DNA auch in Ihrem Unternehmen Zeit und Geld einsparen kann. Laden Sie einfach die kostenlose Testversion für 50 User herunter.

Network Computing AWARDS 2008 FINALIST

PC PRO RECOMMENDED

Best of CeBIT america Winner

PCPlus

Hier finden Sie weitere Informationen und können downloaden

www.netsupportdna.com

PCIS

sales@pci-software.de +49 (0)89 550 508 -10 www.pci-software.de

Kooperation mit dem "Datacenter on Demand"

Redaktion und Rechenzentrum

von John Pardey

Das Schweizer IT-Systemhaus Kybernetica und das IT-Administrator-Magazin haben eine umfangreiche Kooperation vereinbart, von der die Leser gleich in doppelter Hinsicht profitieren. Kybernetica ist der Betreiber des "Datacenter on Demand", eines Dienstleistungsanbots, welches IT-Abteilungen erlaubt, modernstes Equipment anzumieten und dieses komfortabel und remote für Schulungen oder Tests zu nutzen. Für das IT-Administrator-Magazin ergeben sich durch die Nutzung des Datacenter on Demand für Produkttests ganz neue Möglichkeiten, Soft- und Hardware noch praxisnäher als bisher zu testen. Zudem erhalten alle ITANet-Mitglieder einen Rabatt bei der Nutzung des Datacenter on Demand.

Es ist für ein IT-Magazin nicht unüblich, seine Testlabore durch Leihstellungen führender Hersteller zu bestücken oder Produkttests, wie sie jeden Monat im IT-Administrator erscheinen, über externe Tester und deren Labore abzuwickeln. Doch selbst die großzügigste Dauerleihstellung – die immer auch Fragen nach der Herstellerunabhängigkeit aufwirft – ist nicht zu vergleichen mit der Ausstattung, die der Redaktion des IT-Administrator nunmehr für Produkttests zur Verfügung steht.

Cluster und mehr lassen sich über das Internet mieten

Unschlagbare Ausstattung

Überhaupt war die umfassende Ausstattung im Datacenter-on-Demand (D-on-D) ein treibender Faktor hinter den Anstrengungen der IT-Administrator-Redaktion, diese Kooperation zu realisieren. Die Ausstatterliste des D-on-D liest sich denn auch wie das Who's Who der IT: Cisco, HP, VMware, Net-App und viele mehr bestücken das Rechenzentrum mit State-of-the-art-Equipment.

Aktuell können Nutzer unter 37 physikalischen Servern sowie zwölf Speichersystemen wählen. Als Standardserver verwendet das D-on-D primär 2U Rackserver der Firma Hewlett-Packard [1]. Rackserver sind für diese Zwecke besser als Bladeserver geeignet, da neueste Technologien, wie zum Beispiel FCoE (Fibre-Channel over Ethernet) einen CNA (Converged Network Adapter) benötigen. Die erhältlichen Formate liegen zuerst auf Basis von PCIe und in der Größe von Steckkarten im Vollformat vor. Solche Komponenten können Blades leider nicht aufnehmen. Nur Rackserver bieten in dieser Hinsicht die geforderte Flexibilität. Einen Überblick über die verfügbaren Speichersysteme finden Sie unter [2].

Entwicklung des D-on-D

D-on-D wurde 2004 als kleines IT-Labor von Urs Stephan Alder ins Leben gerufen. Was als Infrastruktur für den Selbstbedarf begann, hat sich mittlerweile zum modernsten und größten herstellerunabhängigen IT-Labor der Schweiz gemausert. Urs Stephan Alder hatte primär das Eigeninteresse, sich solide und kontinuierlich in seinem Berufsfeld (IT- Training und Consulting) weiterzubilden. Anfang 2004 war die Server-Virtualisierung die neue Verheißung eines zukünftigen IT-Eldorados für IT-Dienstleister. Alder war von der Technologie begeistert und wollte sich dieses Berufsfeld unbedingt erschließen.

Dafür musste mehr als ein PC beschafft werden, richtige Server und ein Storage-System standen auf der Stückliste. So baute Alder seine IT-Infrastruktur [3] im Laufe der Zeit entsprechend auf. Doch Alders Steckenpferd verursachte immer mehr Kosten und er sah sich mit der Frage der zukünftigen Finanzierung konfrontiert. Nach kurzer Überlegung lag die Lösung auf der Hand: das Inventar gegen einen Obolus teilen – die Geburtsstunde des D-on-D.

Über die Jahre hat sich gezeigt, dass ein Bedarf am Mieten von professionellen IT-Laboren besteht. Dank der Vernetzung durch das Internet ist die Kundschaft global erreichbar. D-on-D entwickelte sich zu einem universellen Werkzeug für IT-Profis aller Art.

Heute nutzen Alders Kunden die Infrastruktur für Tests neuer Applikationen und Hardware, für Schulungen oder aber Lasttests – einen detaillierten Bericht über einen vergleichenden Lasttest für Windows Terminal Server finden Sie in dieser Ausgabe ab Seite 51. In diesem Lasttest untersuchte unser Autor Bertram Wöhrmann, wie sich virtualisierte Terminalserver auf verschiedenen Plattformen verhalten.

Sonderkonditionen für Abonnenten des IT-Administrator

So profitieren Sie als Leser also zukünftig von noch realitätsnäheren und somit aussagekräftigeren Produkttests im IT-Administrator. Und darüber hinaus erhalten Sie als ITANet-Mitglied beziehungsweise IT-Administrator-Abonnent bei D-on-D einen fünfprozentigen Rabatt [3] auf den Mietpreis, sollten Sie einmal kurzfristigen Bedarf an entsprechendem Equipment haben.

Dabei haben Sie die Möglichkeit, sich die benötigte Gerätschaft selbst flexibel zusammenzustellen ("à la carte") und den Mietpreis direkt zu kalkulieren oder eines von zwei vordefinierten Paketen auszuwählen, die für spezifische Aufgaben geeignet sind. Auf jeden Fall lohnt es sich bei grundsätzlichem Interesse, die Site im Auge zu behalten, denn die Entwicklung und somit der Ausbau an verfügbarer Hardware ist derzeit äußerst dynamisch.

Links

[1] Serversysteme im D-on-D
www.d-on-d.com/e-server.htm

[2] Speichersysteme im D-on-D
www.d-on-d.com/e-speicher.htm

[3] Netzwerkkomponenten im D-onD
www.d-on-d.com/e-san-netzwerk.htm

[4] Kontaktformular für IT-Administrator-Abonnenten
www.kybernetika.ch/co.htm

Im Test: Citrix XenApp 5.0

Der Hydra neue Köpfe

von Christian Knermann

Seit die Microsoft-Terminaldienste des Windows Servers unter dem damaligen Projektnamen "Hydra" das Licht der Welt erblickten, erweitern die Produkte aus dem Hause Citrix deren Funktion. Mit XenApp 5.0 als Nachfolger des Presentation Servers 4.5 hält nicht nur ein neuer Name Einzug in das Produkt, sondern auch eine Reihe von Neuerungen und Verbesserungen. Diese mussten sich in unserem Test beweisen.

Mit dem Windows Server 2008 hielten lange erwartete Funktionen ins Terminaldienste-Umfeld Einzug, die zuvor Drittanbietern vorbehalten waren:

- Die "RemoteApps" stellen einzelne Anwendungen dar, als seien sie lokal installiert.
- Der Sitzungsbroker erlaubt es, mehrere Server zu einer ausfallsicheren Farm zu verbinden.
- Terminal Services Web Access bietet den Anwendern die RemoteApps über ein Web-Interface an, was mittels Terminal Services Gateway (TSG) auch über HTTPS funktioniert und den RDP-Datenstrom per SSL verschlüsselt.

Bei einer Bewertung all dieser Neuerungen steht für viele Administratoren besonders eine Frage im Vordergrund: Reicht bereits die Basisfunktionalität des Windows Servers aus oder sind weiterhin zusätzliche Produkte von Drittanbietern erforderlich? Die Antwort lautet: Es kommt drauf an …

Kleinere Umgebungen von geringer Komplexität lassen sich bereits mit den Bordmitteln des Windows Servers versorgen, wie unser erster Test [1, 2] zeigte. Einschränkend wirkt dabei allerdings, dass dies nur für homogene Microsoft-Umgebungen mit relativ neuen Clients gilt. Denn ältere Systeme, Linux-Thin Clients und andere Linux/UNIX-Clients können viele der neuen Funktionen nicht nutzen. Sobald die Umgebung wächst, geht zudem schnell die Übersicht verloren, da es den Terminaldiensten an einer zentralen Konsole zur Administration mangelt und zu viele Handgriffe einzeln pro Server durchzuführen sind. Heterogene Landschaften mit unterschiedlichen Clientplattformen und zahlreichen Terminalservern sind also weiterhin auf Drittanbieter angewiesen.

Alles Xen

So schickt denn auch Citrix eine neue Version seiner Lösung für die Anwendungsbereitstellung ins Rennen und stiftet bei dem ein oder anderen altgedienten Administrator zunächst einmal Verwirrung. Denn das Produkt, welches ehedem als "MetaFrame" bekannt war und dann zum "Presentation Server" wurde, erhält nun abermals einen neuen Namen: XenApp (in der Version 5.0) tritt die Nachfolge des Presentation Server 4.5 an. Dabei bezieht sich die Namensgebung unter Verwendung von "Xen" nicht unbedingt auf den gleichnamigen Hypervisor, sondern wird von Citrix weiter gefasst als Synonym für Virtualisierung verstanden. So dient der XenServer der Virtualisierung von Server-Betriebssystemen, XenDesktop der Virtualisierung von Desktops und eben XenApp der Virtualisierung von Anwendungen.

Der grundlegende Ansatz hat sich dabei gegenüber früheren Versionen nicht verändert. XenApp setzt auf den Windows-Terminaldiensten auf und erweitert deren Funktionalität. Sowohl die Terminaldienste-Lizenzierung als auch ein oder mehrere Terminalserver müssen also bereits installiert sein. Der Sitzungsbroker wird dagegen nicht benötigt und die Lastverteilung bringt XenApp bereits mit. Das Citrix Web-Interface ersetzt den Rollendienst "Terminaldienste-Webzugriff". Statt des Terminal Services Gateway kann wahlweise die Software Citrix Secure Gateway oder das Access Gateway, eine Hardware-Appliance aus dem Hause Citrix, zum Einsatz kommen. Die erstgenannte Lösung ist im Umfang von XenApp bereits enthalten.

Architektur mit Single Point of Failure

Das grundlegende Funktionsprinzip zur Erweiterung der Terminaldienste ist aber

für alle Editionen identisch (Bild 1). Mehrere Terminalserver werden zu einer Verwaltungseinheit, der "Server Farm", zusammengefasst. Die Farm-Konfiguration, das heißt beispielsweise, welche veröffentlichten Anwendungen auf welchen Servern für welche Benutzer freigegeben sind, wird zentral im Datenspeicher der sogenannten "Independent Management Architecture" (IMA) abgelegt. Über den IMA-Port 2512 (TCP) kommunizieren die Server einer Farm untereinander.

Im einfachsten Fall hält der erste XenApp-Server einer Farm den Datenspeicher in Form einer lokalen Access-Datenbank, die Sie im Laufe der Installation anlegen können. Alle Terminalserver führen den Citrix XML-Dienst aus, über den das Web-Interface Informationen zur Konfiguration der Farm abfragen kann. Standardmäßig läuft der XML-Dienst auf Port 80 (TCP). Während der Installation besteht jedoch die Möglichkeit, einen alternativen Port anzugeben.

Das Web-Interface bietet zwei verschiedene Typen Websites zum Zugriff auf veröffentlichte Applikationen an. Zum einen lässt sich über eine Website vom Typ "XenApp Services" eine Konfigurationsdatei im XML-Format bereitstellen. In diesem Fall ist auf dem Client das XenApp-Plug-in für gehostete Anwendungen erforderlich, das vormals als "Citrix Program Neighborhood Agent" bekannt war. Das Plug-in verankert sich auf dem Client im Systemtray und ermöglicht dem Anwender direkt, die für ihn freigegebenen Applikationen von den Terminalservern zu starten (Bild 2).

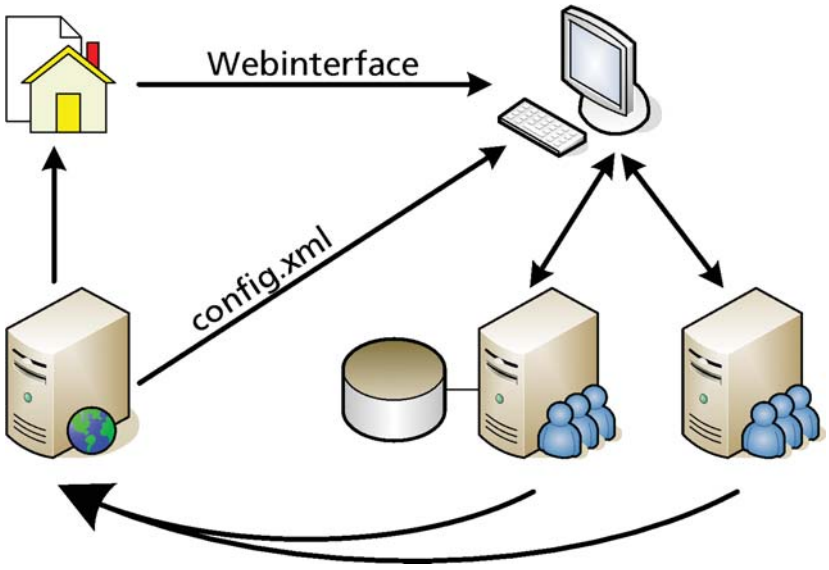


Bild 1: In der XenApp-Architektur veröffentlichen mehrere Server ihre Anwendungen über ein Web-Interface

Zum anderen bietet eine Website vom Typ "XenApp Web" Anwendern die Möglichkeit, sich über einen Browser interaktiv anzumelden und auf veröffentlichte Anwendungen zuzugreifen. Für diese Variante kann das XenApp Web-Plug-in eingesetzt werden. In beiden Fällen wird beim eigentlichen Start einer veröffentlichten Anwendung eine direkte Verbindung zwischen Client und einem der Terminalserver über das Protokoll "Independent Computing Architecture" (ICA) aufgebaut.

Der Vorteil dieser Architektur ist nun, dass die veröffentlichten Applikationen auch über mehrere Server hinweg an einer zentralen Stelle administrierbar sind. Über den XML-Dienst und das Web-Interface werden Änderungen sofort für alle Clients verfügbar. Entsprechend wichtig ist allerdings der Datenspeicher. Fällt dieser aus, funktionieren die übrigen Terminalserver zwar weiter, da sie die Konfiguration im Local Host Cache (LHC) lokal zwischenspeichern. Dieser Cache erlaubt aber nur lesenden Zugriff, sodass im Falle einer Störung keine Konfigurationsänderungen mehr möglich sind, bis der Datenspeicher wieder verfügbar ist. Der Server, der die lokale Access-Datenbank hält, wird somit zum Single Point of Failure. Unsere Empfehlung lautet daher, im produktiven Einsatz einen separaten Datenbankserver zu verwenden. XenApp unterstützt hier Microsoft SQL Server, Oracle sowie IBM DB2.

Lizenzierung einrichten

Für unsere Testinstallation wählten wir ein heterogenes Szenario, bestehend aus einem Domain Controller unter Windows

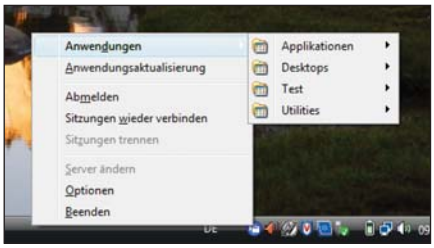


Bild 2: Das XenApp-Plug-in stellt die Verbindung zu den serverseitigen Anwendungen her

Produktvarianten im Überblick

XenApp 5.0 ist in den Editionen "Advanced", "Enterprise" und "Platinum" erhältlich [3]. Bereits das Einstiegmodell umfasst mit Load Balancing und der Möglichkeit, einzelne Anwendungen zu veröffentlichen, die nötigen Funktionen zum Aufbau einer Terminalserver-Farm. In der von uns getesteten Enterprise Edition kommt das Anwendungsstreaming hinzu, das Applikationen in Paketen isoliert und zur Offline-Nutzung an Clients ausliefert. Die Platinum-Edition beinhaltet darüber hinaus die erforderlichen Lizenzen zur Nutzung weiterer Citrix-Produkte, wie die Single Sign-On-Lösung "Password Manager", die VPN-Lösung "Access Gateway" oder den "WANScaler" zur Beschleunigung der Datenübertragung im WAN. Im Falle von Access Gateway und WANScaler entstehen allerdings zusätzliche Kosten, da beide Lösungen eine entsprechende Hardware-Appliance voraussetzen. Lediglich Zugriffslizenzen für diese Appliances sind mit der Platinum Edition bereits abgegolten.

Server 2003 SP2, einem weiteren unter Windows Server 2008 sowie drei Terminalservern. Der erste Terminalserver unter Windows Server 2003 SP2 war bereits als Citrix Presentation Server 4.5 Enterprise Edition vorinstalliert. Die übrigen Terminalserver unter Windows Server 2008 waren jeweils mit einer Installation der Microsoft-Terminaldienste vorbereitet. Der Windows Server 2003 DC dient gleichzeitig als Dateiserver für die servergespeicherten Profile und führt zudem die Microsoft Terminaldienste-Lizenzierung sowie den Citrix Lizenzmanager aus.

Letzteren setzt XenApp 5.0 in der Version 11.5 voraus, der auf dem XenApp-Medium zu finden ist. Die grundlegende Funktionalität hat sich gegenüber der Vorgängerversion nicht geändert. Bestandteile sind der auf dem Lizenzmanager FlexLM basierende Dienst "Citrix Licensing" sowie die als JSP-Webseite realisierte "License Management Console". Im Internet [4] lassen sich passend zu den erworbenen Lizenzen eine an den Namen des Lizenzservers gebundene Datei erzeugen, die über die Konsole auf den Server hochladen wird, sowie aktuelle und historische Daten zu deren Nutzung anzeigen. Die XenApp-Lizenzen werden nach dem "Concurrent User"-Modell vergeben. Relevant sind lediglich die gleichzeitigen Zugriffe unabhängig von namentlich benannten Benutzern. Nach dem Ende einer Benutzersitzung wird die von ihr belegte Lizenz wieder im Pool verfügbar.

Nach dem Versuch, die neue Lizenzierung einfach als Upgrade über unsere bestehende Instanz zu installieren, fand der Dienst zunächst die Lizenzdateien nicht. Ursache war, dass die Dateien sich im Pfad *C:\Programme\Citrix\Licensing\MeineDateien* befanden, der Dienst nach dem Upgrade aber im Pfad *C:\Programme\Citrix\Licensing\MyFiles* suchte. Durch Verschieben der Dateien ließ sich diese Klippe umschiffen. Um ähnliche Probleme zu vermeiden, lautet unsere Empfehlung, im Rahmen einer Migration zunächst die Lizenzen zu sichern, dann Citrix Licensing zu deinstallieren und anschließend die neue Version zu installieren. In diesem Fall lässt sich während der Installation der Pfad zu den Lizenzdateien angeben.

Web-Interface auf dem Terminalserver installieren

Möchten Sie das Web-Interface mit auf dem Terminalserver installieren, konfigurieren Sie den XML-Dienst auf Port 8080 (TCP). Der Port 80 (TCP) steht dann dem für das Web-Interface erforderlichen IIS exklusiv zur Verfügung.

Installation und Upgrade

Der Verlauf einer Neuinstallation präsentiert sich gegenüber dem Presentation Server 4.5 ohne wesentliche Änderungen [5]. Denn trotz des Versionssprungs auf 5.0 stellt die neue Ausgabe für den Windows Server 2003 eher ein Minor Release dar. Da der Kern von XenApp sich gegenüber dem Presentation Server nicht geändert hat, gestaltet sich eine Aktualisierung einfach. Es genügt ein Upgrade der Komponenten und Clients, um in den Genuss der neuen Funktionen zu kommen. Ein solches Upgrade ist allerdings nur vom Presentation Server 4.5 direkt möglich. Ältere Versionen müssen zunächst in einem Zwischenschritt auf Version 4.5 aktualisiert werden. Verschiedene Migrationsszenarien behandelt ein Leitfaden von Citrix [6].

In unserer Testumgebung installierten wir zunächst das XenApp Plugin 11.0 auf den Clients und führten dann auf dem Presentation Server ein Upgrade der Managamentkonsolen durch. Die Installationsroutine aktualisierte die Access Management Console (AMC) auf die neueste Version. Weiterhin stand die "Erweiterte XenApp-Konfiguration" zur Auswahl, hinter der sich Altbekanntes verbirgt. Es handelt sich um den Nachfolger der in Java realisierten Presentation Server Console, was leider bedeutet, dass auch unter XenApp 5.0 die Administration einer Terminalserver-Farm noch nicht vollständig über die AMC möglich ist.

Die Konfiguration einiger Features wie der Citrix-eigenen Richtlinien oder der Druckerverwaltung findet sich in der "Erweiterten XenApp-Konfiguration", während fast alle übrigen Funktionen in die AMC umgezogen sind. Die aktualisierte AMC ist Voraussetzung für ein Upgrade auf das neue Web Interface 5.0.1, welches sowohl XenApp als auch XenDesktop integrieren kann. Beim Upgrade wurde unsere vorhandene Konfiguration automatisch in das neue Web-Interface übernommen. Anschließend war das WI weiter unter der vom Presentation Server 4.5 bekannten Adresse *http://{servername}/Citrix/AccessPlatform* erreichbar, präsentierte sich aber in komplett erneuerter Optik.

Single Sign-On konfigurieren

Statt einer "Site für Program Neighborhood-Dienste" versorgen nun die "XenApp Services" die Clients mit einer Konfiguration. Eine solche Site konfigurierten wir analog zu unserem Windows Server 2003. Als Authentifizierungsmethode richteten wir auch hier "Passthrough" ein, sodass Anwender nach der Anmeldung an einem Desktop transparent Applikationen von anderen Terminalservern starten können, ohne erneut nach Logon-Informationen gefragt zu werden. Als wir nun aber im XenApp Plug-in die Serveradresse auf den neuen Web-Interface-Server änderten, mussten wir feststellen, dass der Single Sign-On mittels Passthrough nicht funktionierte und zu einer Fehlermeldung führte (Bild 3).

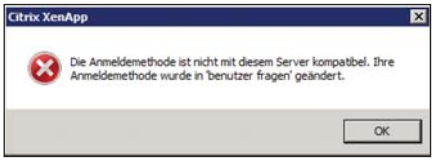


Bild 3: Ohne Kerberos funktioniert Single Sign-On nicht

Dies lag darin begründet, dass unter Windows Server 2008 für die Passthrough-Authentifizierung das Kerberos-Protokoll Voraussetzung ist. Wir aktivierten in der AMC in den Eigenschaften der Authentifizierungsmethode entsprechend die Option "Nur Kerberos verwenden". Darauf-

hin war es möglich, sich transparent am XenApp-Plug-in anzumelden. Beim Versuch, Anwendungen vom zweiten Windows Server 2008-System zu starten, funktionierte der Single Sign-On dennoch nicht. Stattdessen forderte eine Anmeldemaske zur Eingabe von Benutzername und Passwort auf. Eine Recherche im Citrix Knowledge Center ergab zwei weitere Schritte, um Kerberos nutzen zu können. So aktivierten wir in der AMC in den Eigenschaften unserer Farm auf der Seite "Farmweit\XenApp\Allgemein" die Option "DNS-Adressauflösung für XML-Dienst aktivieren".

Weiterhin riefen wir auf dem Domaincontroller in der MMC "Active Directory-Benutzer und -Computer" die Eigenschaften der Accounts unserer Terminalserver auf. Nachdem wir auf der Registerkarte "Delegierung" jeweils die Option "Computer bei Delegierung aller Dienste vertrauen (nur Kerberos)" (Bild 4) gewählt hatten, starteten wir die Systeme neu. Anschließend war es von den Clients aus möglich, sowohl unter Windows Server 2003 als auch 2008 Terminalserver-Desktops zu starten und von dort per Single Sign-On weitere Applikationen von den übrigen Terminalservern zu beziehen.

XenApp 5.0 ermöglicht somit den transparenten Zugriff auf heterogene Farmen, was insbesondere während einer Migration von Windows Server 2003 auf 2008 den Anwendern den Zugang zu Ressourcen erleichtert. Mit entsprechend konfigurierten Benutzerprofilen können sich die Anwender darauf konzentrieren, was sie tun möchten, ohne darauf achten zu müssen, auf welchem Betriebssystem oder Server die gewünschte Applikation läuft.

Oberfläche anpassen

Für den Fall, dass das neue, schwarze Design nicht gefällt, stellt Citrix unter dem Slogan "Pimp My XenApp" [7] Ressourcen bereit, um auf einfache Weise zu einem weißen Design zu gelangen oder das Aussehen anderweitig anzupassen. Auf der Seite finden sich zusätzlich einige weitere Designs sowie das Web-Interface SDK als Grundlage für umfangreichere Anpassungen des WI zum Download.

Damit waren die Voraussetzungen geschaffen, um weitere Terminalserver unter Windows Server 2008 in unsere Farm aufzu-

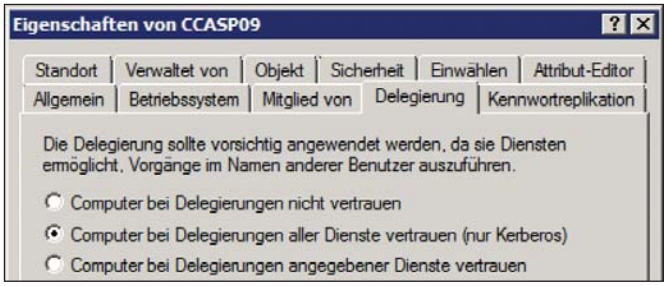


Bild 4: Damit der Single Sign-On funktioniert, müssen die Systeme einander vertrauen

nehmen. Auf unserem Windows Server 2008-System installierten wir zunächst zwei Microsoft-Hotfixes [8], um zum einen die Kompatibilität zu älteren Citrix-Clients zu gewährleisten und zum anderen einen möglichen Stop-Fehler zu adressieren. Hinzu kamen das .NET Framework 3.5, Visual J# 2.0 und Visual C++2005 SP1 aus dem Support-Verzeichnis des XenApp-Mediums sowie die aktuelle SUN Java-Laufzeitumgebung Version 6 Update 11. Weiterhin ergänzten wir über den Server-Manager die Rolle "Webserver (IIS)" und aktivierten die zusätzlichen Rollendienste "ASP.NET", "Windows-Authentifizierung" sowie die "IIS 6-Metabasiskompatibilität" als Voraussetzung für das Web-Interface.

So gerüstet konnten wir mit der Installation von XenApp 5.0 beginnen. Wir entschieden uns im ersten Schritt für die "Enterprise Edition". Im folgenden Dialog wählten wir die "Anwendungsvirtualisierung", mit der automatisch sowohl XenApp selbst als auch alle benötigten Komponenten selektiert wurden. Die übrigen Konfigurationsschritte verliefen auch unter Windows Server 2008 wie vom Presentation Server 4.5 gewohnt, und nach einem obligatorischen Neustart bootete das System als XenApp Server. Analog verfuhren wir mit dem zweiten Terminalserver und veröffentlichten von den Servern jeweils sowohl einen Desktop als auch ein zuvor installiertes Word 2007, was sich ebenso einfach gestaltete, wie vom Vorgänger-Produkt unter Windows Server 2003 bekannt.

Auch unter Windows Server 2008 wollten wir nun ein Web-Interface zur Konfiguration der Clients konfigurieren, was sich von früheren Versionen lediglich durch geänderte Begriffe unterscheidet. Aus der "Access Platform-Site" wurde eine Site vom Typ "XenApp Web". Für ein neu installiertes Web-Interface lautet die Adresse entsprechend *http://{servername}/Citrix/XenApp*.

Schriftartenglättung

Eine der neuen Funktionen ist dabei die Unterstützung der Schriftartenglättung. Diese lässt sich sowohl in "XenApp Services" als auch in "XenApp Web" jeweils auf der Seite "Anzeige" der Sitzungsoptionen über die Checkbox "Schriftartenglättung zulassen" aktivieren. Anschließend wird in Desktop-Sessions die Kantenglättung verfügbar. Zu finden ist die Option in den Eigenschaften der Anzeige auf der Registerkarte "Darstellung" über die Schaltfläche "Effekte…".

Ebenso lassen sich die Einstellungen direkt über den Registrierungseintrag HKCU\Control Panel\Desktop\FontSmoothingType vom Typ "DWORD" vornehmen. Der Wert "0" deaktiviert die Kantenglättung. Wert "1" aktiviert die für Röhrenmonitore empfohlene Methode "Standard" und "2" die für TFT-Monitore gedachte Methode "ClearType". Auf Windows Server 2003-Systemen müssen ein Microsoft-Hotfix und das Citrix Hotfix Rollup Pack 3 installiert sein, damit die Kantenglättung funktioniert [9].

Bild 5: Profile lassen sich verknüpfen, um die Kommunikation zwischen isolierten Anwendung zu ermöglichen

Streaming erlaubt Interaktion gekapselter Anwendungen

Auch XenApp 5.0 adressiert mit dem integrierten Anwendungsstreaming die Kapselung und Offline-Nutzung von Applikationen. Aufseiten des Servers ist dazu mindestens die Enterprise-Edition erforderlich. Der Client benötigt zusätzlich das XenApp-Plug-in für gestreamte Anwendungen. Weitere Komponenten sind mindestens eine Workstation als "Profiler" zur Paketierung von Anwendungen sowie eine Dateifreigabe zur Bereitstellung der Applikationen. Auch die Funktionsweise des Streaming Profiler 1.2 hat sich gegenüber der Vorgängerversion nicht wesentlich verändert, jedoch einige Verbesserungen erfahren. Allem voran ist sicher zu nennen, dass das Anwendungsstreaming nun Windows Vista und Windows Server 2008 als Zielplattformen unterstützt. Diese stehen im Dialog zur Zielplattform in der 32- und 64-Bit-Variante zur Auswahl.

Eine der Beschränkungen der Anwendungsisolierung unter Presentation Server 4.5 war, dass Applikationen in unterschiedlichen Paketen nicht direkt miteinander kommunizieren konnten. Dieser Effekt lässt sich auch in der aktuellen Version noch nachvollziehen. So erstellten wir mit dem Streaming Profiler jeweils ein Profil für Word 2003 und ein weiteres für CorelDRAW 12.

Werden diese Profile nun einzeln über die AMC veröffentlicht, wissen die bei-

Links und Ressourcen

[1] **"Neuer Lastesel im Netz: Terminaldienste unter Windows Server 2008 (1)"**
in IT-Administrator 9/2008

[2] **"Unsere kleine Farm: Terminaldienste unter Windows Server 2008 (2)"**
in IT-Administrator 10/2008

[3] **Editionen von XenApp 5.0**
www.citrix.de/produkte/schnellsuche/xenapp/produktuebersicht/editionen/

[4] **Citrix-Portal zum Erzeugen der Lizenzdatei**
www.mycitrix.com

[5] **"Modellpflege: Citrix Presentation Server 4.5"**
in IT-Administrator 11/2007

[6] **Leitfaden zu Migrationsszenarien**
http://community.citrix.com/blogs/citrite/gusp/2008/09/07/The+Ultimate+XenApp+5+Migration+Guide/

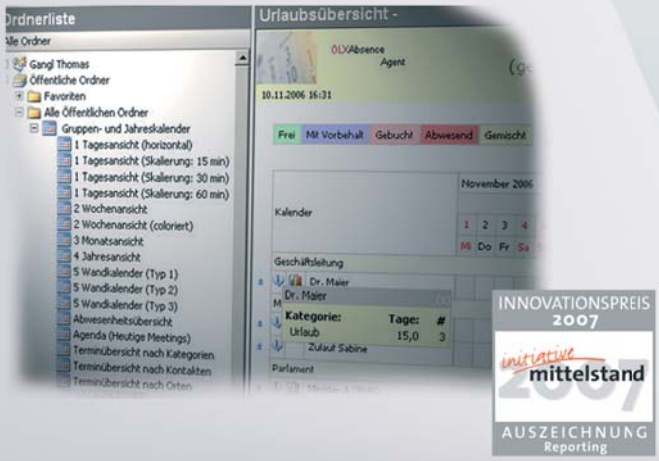
[7] **Oberflächendesigns für XenApp**
www.pimpmyxenapp.com

[8] **Windows Server 2008 Hotfixes**
http://support.microsoft.com/kb/949914/en-us
http://support.microsoft.com/kb/951149/en-us

[9] **Microsoft Hotfix und Citrix Hotfix Rollup Pack 3 für Kantenglättung**
http://support.microsoft.com/kb/946633/en-us
http://support.citrix.com/article/CTX117461/

Wer liefert Ihnen das fehlende Puzzleteil zu Outlook© und Exchange©?

Gruppenkalender
Terminmanagement



INNOVATIONSPREIS 2007 – initiative mittelstand – AUSZEICHNUNG Reporting

Mobiler Zugriff
auch für Öffentliche Ordner

INNOVATIONSPREIS 2007 – initiative mittelstand – AUSZEICHNUNG Mobile Business

Unternehmensweite
Signaturen & Disclaimer

Individualentwicklung
Vertrauen in Erfahrung

www.gangl.de

Ihr Partner für praxisorientierte Outlook© und Exchange© Lösungen!

Ihre Ansprüche sind unser Ansporn!

✉ info@gangl.de ☎ +49 7173 9290 53

den Applikationen nicht voneinander. Ein Word-Dokument mit einer eingebetteten CorelDRAW-Grafik ließ sich zwar öffnen. Es war aber nicht möglich, die Grafik direkt aus Word heraus zu bearbeiten, da sie nur als "Unknown Object" erkannt wurde. Mit der früheren Version des Streaming Profilers bestand der einzige Ausweg darin, ein neues Profil zu erstellen, um darin Word und CorelDRAW gemeinsam zu installieren. Bei einer größeren Zahl an Anwendungen und Abhängigkeiten zwischen diesen würde ein solches Vorgehen aber in sehr großen Profilen oder einer Unzahl verschiedener Profile gipfeln, um alle möglichen Abhängigkeiten zu berücksichtigen.

XenApp 5.0 adressiert das Problem mit der neuen "Interisolierungs-Kommunikation". So ist es über den Assistenten des Profilers möglich, direkt bei der Erstellung eines neuen Profils Abhängigkeiten zu anderen Profilen zu definieren. Weiterhin können Profile als reine Verknüpfung weiterer Profile erstellt werden, ohne selbst Anwendungen zu enthalten. Wir testeten diesen Weg, um Word und CorelDRAW zu integrieren, indem wir ein neues Profil erzeugten und die beiden Applikationen als verknüpfte Profile auswählten. Im nächsten Dialogschritt aktivierten wir die Option "Erstellen Sie ein Profil, das nur auf andere Profile verweist (keine Installation erforderlich) …".

Das Ergebnis war entsprechend eine Verknüpfung der beiden Anwendungen (Bild 5). Anschließend änderten wir die veröffentlichten Applikationen in der AMC derart, dass diese nicht mehr auf die separaten Profile, sondern auf das neue verknüpfte Profil "Word + CorelDRAW" verwiesen. Als Ergebnis wurde damit die Interaktion zwischen den gekapselten Anwendungen möglich. Wir konnten das CorelDRAW-Objekt direkt aus Word heraus bearbeiten. Somit offeriert XenApp 5.0 größere Flexibilität beim Streaming bei reduziertem Speicherplatzbedarf. Hinzu kommen differenzielle Updates, die bei Änderungen von Profilen nur noch das Delta der Änderungen übertragen und somit auch die Ladezeit verringern. Weiterhin besteht nun die Möglichkeit, Applikationen via HTTP/HTTPS zu streamen, was die sichere Anwendungsbereitstellung im WAN erleichtert.

Fazit

XenApp 5.0 bringt die lange erwartete Unterstützung für Windows Server 2008, was insbesondere heterogene Farmen und somit Migrationswege ermöglicht. Angesichts zahlreicher Detailverbesserungen, beispielsweise im Bereich des Streamings, profitieren auch Anwender von Windows Server 2003. Soweit wir neue Funktionen, insbesondere der Platinum-Edition, nicht im Rahmen dieses Tests abdecken konnten, seien die Präsentationen im Citrix Webinar-Archiv als Quelle weiterer Informationen empfohlen.

Kritisch anzumerken ist, dass genau die Punkte offen bleiben, die bereits beim Test des Presentation Server 4.5 das ansonsten stimmige Bild trübten. So ist die vollständige Migration der Administrationstools auch in XenApp 5.0 noch nicht konsequent abgeschlossen. Einige Optionen sind weiterhin nur in der Java-Konsole zu finden. Es bleibt der Wunsch, dass spätestens in der nächsten Version die Administration aller Funktionen zentral über die AMC möglich ist. Ein weiterer Wunsch betrifft wiederum granularere Ablauffristen für Offline-Applikationen, sodass Lizenzen nach definierbaren Zeiträumen wieder verfügbar werden. Dies sollte auf Basis einzelner Applikationen und Benutzergruppen steuerbar sein.

Insgesamt stellt XenApp 5.0 dennoch gegenüber den reinen Microsoft-Terminaldiensten eine signifikante Erweiterung der Funktionen bereit und kann die Verwaltung einer Farm wesentlich vereinfachen, sobald mehr als ein bis zwei Terminalserver zu administrieren sind. *(jp)*

Der Autor dieses Artikels, Dipl.-Inform. (FH) Christian Knermann, ist stellvertretender Leiter des IT-Managements am Fraunhofer Institut für Umwelt-, Sicherheits- und Energietechnik UMSICHT in Oberhausen. Zugleich leitet er das Projekt "Competence Center Application Service Providing" der Fraunhofer Gesellschaft.

Produkt
Funktionserweiterung der Microsoft-Terminaldienste.

Hersteller
Citrix Systems
www.citrix.de

Listenpreise
Advanced Edition etwa 250 Euro pro User
Enterprise Edition etwa 360 Euro pro User
Platinum Edition etwa 560 Euro pro User

Lizenzierung pro gleichzeitigem Benutzer (Concurrent Use). Die Preise sind an den Dollarkurs gekoppelt und können daher schwanken.

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

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

Installation und Inbetriebnahme	7
Funktionsumfang	9
Unterstützung verschiedener Clientplattformen	9
Lizenzverwaltung	6
Anwendungsstreaming	8

Dieses Produkt eignet sich

optimal für heterogene Umgebungen, in denen Windows-Applikationen unter Windows Server 2003 und 2008 von vielen verschiedenen Plattformen aus genutzt werden sollen.

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

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

Citrix XenApp 5.0

Hyperic HQ 4.01 Enterprise

Unbeschwertes Monitoring

von Ronald Wölfel und Thomas Drilling

Quelle: Lianem - Fotolia.com

Netzwerk- und Systemmonitoring ist besonders komfortabel mit grafischer Oberfläche und visualisierten Messergebnissen. So erkennt der Administrator mit einem Blick, wo Störungen auftreten. Hersteller Hyperic wollte als Firmennamen eigentlich einen aus zwei Pflanzenarten gebildeten Fantasienamen verwenden, doch ein Fehler beim Ausfüllen der Papiere ließ lediglich den ersten Teil des Antidepressivums Johanniskraut (Hypericum perforatum) stehen. Kein schlechtes Omen für eine komplexe Software, sich auch im Namen gleich auf das Wesentliche zu beschränken. Wir haben für Sie getestet, ob Hyperic HQ tatsächlich geeignet ist, möglichst nebenwirkungsarm die dunklen Wolken aus dem Gemüt eines geplagten Admins zu vertreiben.

Bei Hyperic HQ handelt es sich um eine fast vollständig in Java geschriebene webbasierte Monitoring-Lösung für gehobene Ansprüche. Das wird nicht zuletzt auch daran deutlich, dass die seit Herbst letzten Jahres gültige Version 4.0x sogar Amazons Cloud Computing unterstützt. Seit 2006 steht auch eine GPL-Version zur Verfügung, die allerdings in puncto Applikationsüberwachung, SNMP und Alarmierung stark eingeschränkt ist.

Zunächst interessierte uns der Funktionsumfang und wie hoch die Hürden bei Installation und Einrichtung sind. Auch Hyperic basiert auf dem Zusammenspiel eines Servers mit seinen Agenten, die sich – Java sei Dank – in Hinblick auf die Plattformen beliebig gemischt einsetzen lassen. Der Server speichert und verdichtet die Informationen, die er von den Agenten erhält, in einer Datenbank. Dabei ist er auf "seine" Informationszuträger angewiesen und kann selbst nicht tätig werden. Er lauscht auf Port 7080, der gleichermaßen als Webinterface-Port wie auch als offenes Ohr für die Mitteilungen seiner Agenten dient.

Autonome Agenten

Auch bei den Agenten handelt es sich um J2EE-Anwendungen, die Betriebszustände, Dienstinformationen, Ping-Zeiten et cetera ermitteln. Die so erhaltenen Messwerte (Metriken) müssen sich jedoch keineswegs auf den gleichen PC beziehen. Als Außenhorchposten des Hyperic-Netzwerks können Agenten auch zur Überwachung der Netzwerkdienste von Internetservern eingesetzt werden. Sowohl die Agenten als auch der Server benötigen jeweils einen offenen Port. Eventuell vorhandene Firewalls müssen also gleich doppelt "gepierct" werden. Nur die Enterprise Edition verfügt über einen bidirektionalen Modus, sodass hier ein Port genügt.

Die Agenten sind plattformunabhängig einsetzbar und arbeiten nach Instruktion auch weitgehend autonom. Das bedeutet, sie setzen ihre Arbeit auch dann fort, wenn gerade keine Netzwerkverbindung zum Server besteht. Steht die Verbindung wieder, werden die Statistiken und Graphen mit den gepufferten Daten ergänzt und fortgeführt. Selbstverständlich können IT-Verantwortliche einen Agenten auch auf dem HQ-Server-Rechner installieren. Doch zur Überwachung des Servers selbst ist dies nicht erforderlich, das bereits mitgelieferte Plug-in "HQ-Health" liefert in der GUI bereits ein Minimal-Monitoring über die Vitalfunktionen der einzelnen Komponenten.

Hardware-Anforderungen

Für den Server:

- 2.400 MHz Dual-Pentium Xeon
- 4 GByte RAM (Minimum 1 GByte)
- 1-5 GByte Festplattenplatz

Für den Agent:

- 500 MHz Celeron
- 256 MByte RAM
- 0,5 GByte Festplattenplatz

Vorbereitung der Installation

In der Testphase kam es immer wieder zu Problemen mit leicht differierenden Uhrzeiten zwischen Agent und Server, insbesondere beim Einsatz des Servers in virtualisierten Umgebungen. Die Zeit der beteiligten Rechner sollten Administratoren daher aktiv mit dem NTP-Daemon kontrollieren.

Noch vor der eigentlichen Installation ist die Umgebung festzulegen. Schließlich sind Netzwerke so vielfältig wie das Leben selbst, was sich zunächst in den Hyperic-Versionen für die unterschiedlichsten Plattformen (Linux, Solaris 10, Mac OS X, MS-Windows) widerspiegelt. Naturgemäß ist die Agentenvielfalt noch etwas größer. Hier werden zusätzlich Pakete für die Plattformen FreeBSD, AIX und HP-UX angeboten. Schließlich gibt es jedes Paket in einer Variante mit oder ohne enthaltener JRE. Außerdem stehen in der GPL-Version auch noch die Paketquellen zur Verfügung. Als weitere Konzession an die unterschiedlichsten Installationsszenarien ist der Einsatz alternativer DBMS wie Oracle oder MySQL zur integrierten PostgreSQL-Engine zu nennen. Außerdem können Agenten vorkonfiguriert und damit automatisiert installiert werden. Darüber hinaus lässt sich die Windows MSI-Version des Agenten automatisiert bequem via Push-Technik gleichzeitig auf mehrere Rechner installieren.

Server-Installation

Eine Installation als root-Benutzer ist nicht gestattet. Empfohlen wird das Anlegen eines Hyperic-Nutzers mit

```
useradd hyperic -m -G users -s
  /bin/bash
```

Auf das Setzen des Passworts kann verzichtet werden, stattdessen nimmt der Adminstrator als root mit *su - hyperic* die Hyperic-Identität an.

Die Installationsdatei *hyperic-hq-installer-4.0.2-EE-940-x86-linux.tgz* kopierten wir in das Heimatverzeichnis und entpackten sie. In dem entstandenen Verzeichnis *hyperic-hq-installer* starteten wir mit *./setup.sh* die Installationsroutine.

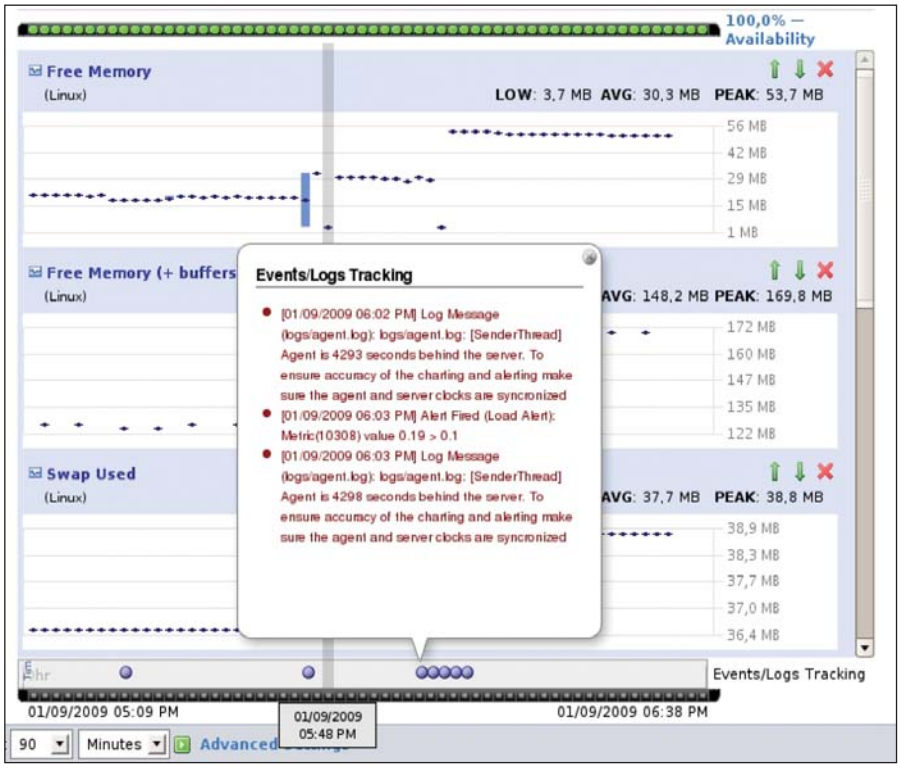


Bild 1: In den Indikator-Diagrammen des Monitor-Reiters sind Zeitdifferenzen zwischen Server und Agent als blauer Punkt zu erkennen

Die Software fragte nun, ob Server, Agent oder beides installiert werden soll. Außerdem mussten wir den vorgegebenen Pfad */home/hyperic* bestätigen. Sagen dem Skript die Shared-Memory-Einstellungen nicht zu, so unterbricht es die Installation kurz und bittet den Administrator, auf einer anderen Konsole das *tune-os.sh*-Skript auszuführen, das die erforderlichen Änderungen an der */etc/sysctl.conf* vornimmt. Im Anschluss setzten wir das *setup.sh*-Skript fort.

In */home/hyperic/* wurde nun ein Verzeichnis nach der Namenskonvention server-Versionsnummer-Version angelegt (zum Beispiel server-4.0.2-EE). Das Shellskript *hq-server.sh* zum Start des Servers befindet sich im Verzeichnis "bin" dieses Programmverzeichnisses:

```
/home/hyperic/server-4.0.2-
  EE/bin/hq-server.sh start
```

Schon nach wenigen Augenblicken konnten wir uns unter der entsprechenden IP-Adresse und Portnummer (7080) in das Web-Interface einloggen.

Allerdings sollte der Hyperic-Server auch mit jedem Neustart des Systems automatisch starten. Ein Diensteskript musste also her, doch es fehlt leider im Paket. Unter den Stichworten "Debian Init Scripts" wurden wir auf den Hyperic-Seiten [1] fündig. Das entsprechende Skript *hq-server* speicherten wir unter */etc/init.d/* und machten es ausführbar. Unter dem gleichen Namen ist dort eine default-Datei mit Einstellungen zum Installationspfad des Hyperic-Benutzers verfügbar. Diese Textdatei speicherten wir in */etc/default/* und passten den darin konfigurierten Pfad an.

Nachdem wir alle Änderungen vollzogen hatten, funktionierte das Stoppen und Starten von Hyperic mit dem Init-Skript. Die Verlinkung des Init-Skriptes mit den entsprechenden Runlevel-Verzeichnissen erledigten wir schließlich mit dem Befehl

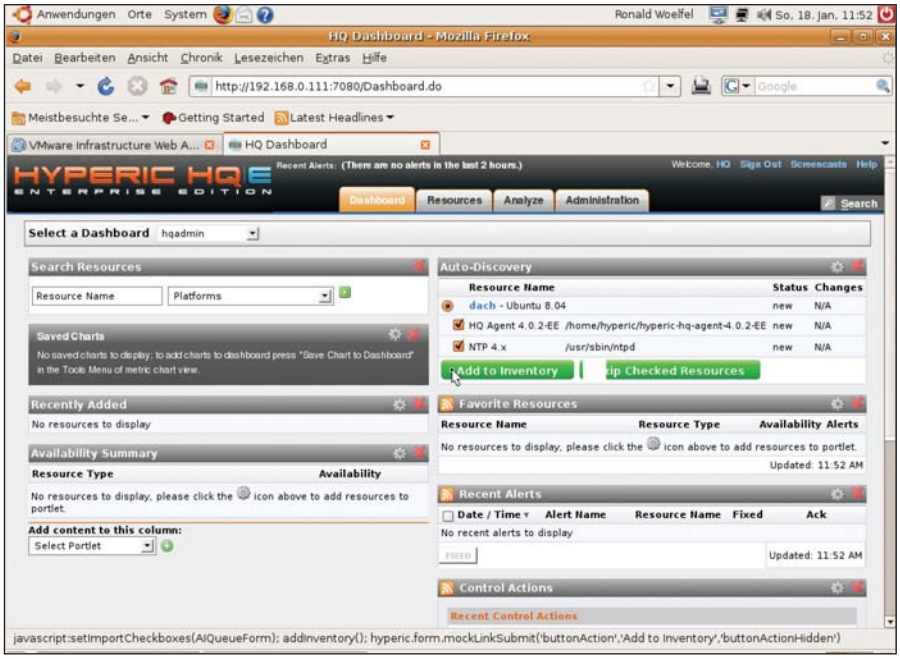


Bild 2: Nach der Installation des Agenten ist es notwendig, die neuen Ressourcen mit "Add to Inventory" zu übernehmen

```
update-rc.d hq-server defaults
```

Die GUI, die zu diesem Zeitpunkt schon zur Verfügung steht, macht ein Editieren von Konfigurationsdateien fast gänzlich überflüssig. Nur grundsätzliche Servereinstellungen wie Portnummern, Datenbankoptionen oder Mailserver-Einstellungen müssen in */conf/hq-server.conf* konfiguriert werden. Mitunter ist auch das Editieren der Template-Dateien notwendig, so muss etwa in der Datei *jboss-service-event.xml* SMTP-Auth konfiguriert werden, falls kein lokaler SMTP-Server vorliegt.

Hyperic als GPL-Version

Wer lieber auf freie Software setzt, wird schnell erkennen, dass bei der GPL-Version von Hyperic manche Vorteile freier Software einfach fehlen. Nicht allein die Funktionsbeschränkungen sind lästig, auch die unübersehbaren Bemühungen der Firma, letztlich doch die Kontrolle über die GPL-Version zu behalten, stehen einer freien Weiterentwicklung durch die Community entgegen. Schließlich wurde der Quellcode erst im Nachhinein veröffentlicht und in der GPL-Software ist keine Dokumentation [2] enthalten, sodass Anwender auf die Anleitung der Hersteller-Homepage angewiesen sind. Dort ist aber auf jeden Fall eine Registrierung notwendig – selbst für kleine Lern-Videos [3]. Im Falle eines Konkurses steht die Community-Edition damit ohne eine Zeile Dokumentation da.

Installation des Agenten

Die Installation des Agenten unter Debian-Systemen verlief fast analog zur Server-Installation. Hinsichtlich der Benutzerrechte gilt allerdings die Einschränkung, dass der empfohlene Weg, minderprivilegierte Benutzerrechte zu verwenden, in vielen Fällen zum Scheitern verurteilt ist. Damit fehlt nämlich zum Beispiel dem Agenten das Recht [4], nach Fehlermeldungen in Logdateien zu suchen. Außerdem benötigt schon der einfache PING-Test in Java aufgrund des selbstgenerierten ICMP-Pakets root-Rechte. Dennoch bot sich die Installation als Hyperic-Benutzer an. Damit der Agent trotzdem root-Rechte erhält, mussten wir in */etc/default/hq-agent* "HYPERIC_USER=root" setzen.

Agent unter XP

Nun installierten wir einen Agent auf einem Windows XP-Rechner: Nach dem Entpacken der rund 70 MByte großen Datei *hyperic-hq-agent-4.0.2-EE-940-win32.zip* in "Programme" fand sich im dort neu entstandenen Verzeichnis wieder ein bin-Verzeichnis mit einer Batchdatei zur Installation. Genau diese Datei starteten wir von der Kommandozeile aus:

```
hq-agent.bat install
```

Nach einem kurzem Augenblick erreichte uns die Meldung "wrapper | Hyperic HQ Agent installed". Unter "Verwaltung/Dienste" war nun der entsprechende Dienst eingetragen. Wichtig ist jedoch nicht zu vergessen, diesen Dienst im Anschluss noch zu starten:

```
hq-agent.bat start
```

Ein vom Server registrierter Rechner wird anhand der Prozesstabelle durch den auto-discovery-Prozess automatisch inventarisiert. Die entsprechenden Ressourcen, zum Beispiel ein SSH-Dienst, fanden sich in der GUI, sobald wir die Ressourcen des neuen Agenten mit "Add to Inventory" übernahmen. Bei Ausfällen werden allerdings keine Alarmmeldungen generiert, diese sind anhand individueller Schwellenwerte selbst zu definieren.

Plattformen, Server und Services

Hyperic legt zur Verwaltung des Inventars eines Rechners das folgende hierarchische Modell zugrunde:

- Die Basis bildet die "Plattform". Hyperic kennt hier nicht nur Linux, Win32 et cetera, sondern auch virtuelle Plattformen wie Xen oder VMware-Hosts. Plattformen beinhalten CPUs, Netzwerk-Interfaces und Dateisysteme.
- Server und Services benötigen eine Plattform. Ein "Server" ist in der Hyperic-Sprachregelung ein Serverdienst wie beispielsweise Apache, der die Grundlage für weitere Software, etwa eine PHP-Anwendung, ist.
- Diese auf dem Server basierende Software heißt im Hyperic-Kontext "Service". Die meisten Dienste, wie etwa SSH oder POP3, benötigen keinen zugrunde liegenden Server. Sie setzen direkt auf der Plattform auf und werden daher als Plattform-Services bezeichnet.

Diese Ressourcen (Plattform, Server und Services) eines Rechners werden bei der Installation des Agenten oder bei den Auto-Scans (alle 15 Minuten) automatisch erkannt. Anders dagegen verhält es sich mit der "Inventar-Typ"-Applikation. Die (Hyperic-)Applikation ist ein Zusammenspiel unterschiedlicher Server und Services, die gemeinsam für die Erfüllung einer Aufgabe benötigt werden – die Einrichtung von Applikationen erfolgt händisch.

Die Informationen, die Hyperic über Plattformen, Server und Services zentral in der Datenbank speichert, werden "Metrics" genannt und nach nach Verfügbarkeit- (Availability), Durchsatz- (Throughput), Auslastungs- (Utilization) und Performance-Metrics unterschieden.

Arbeiten mit Hyperic

Das Hauptmenü bilden

- das Kennzahlencockpit (Dashboard),
- die Ressourcen-Übersicht (Resources),
- das Analysewerkzeug (Analyze) und
- der Bereich der Administration.

Das Dashboard glänzt mit vielen Ajax-Effekten: Ähnlich einem gewöhnlichen Desktop lassen sich die scheinbar autonomen Javascript-Boxen (Portlets) hin- und herschieben. So können Administratoren sich das Dashboard individuell einrichten, um die optimale Übersicht über den aktuellen Gesundheitszustand ihrer Ressourcen zu gewährleisten.

Die Verwaltung der Ressourcen selbst erfolgt über den gleichnamigen Reiter. Ein Klick auf die kleinen Icons "M" (Monitor), "I" (Inventory) und "A" (Alert) führen in den zugehörigen Bereich der angewählten Plattform. Im dann sichtbaren Reiter-Menü ist zusätzlich zu den Bereichen "Monitoring", "Inventory" und "Alert" noch die Option "Views" anwählbar. Hier können sich IT-Verantwortliche mittels sogenannter "Live-Execs" in Echtzeit über den Systemstatus informieren (who, top, df, netstat et cetera).

Im Monitorbereich sind im linken Fenster tabellarisch die Server und Services aufgeführt. Der größere rechte Bereich ist den Graphen (Charts) vorbehalten. Über den zweiten Reiter im rechten Feld (Metric Data) können die Zeitabstände einzelner Messungen festgelegt oder geändert werden. Gelistet werden dort nur Statistiken zu den gemessenen Metrics. Erst der Klick auf das kleine grüne Dreieck hinter "Show all Metrics" zeigt alle auswählbaren Datenquellen zu einer Ressource. Damit eine dort aufgeführte Datenquelle angezapft wird, müssen IT-Verantwortliche nur den Haken entsprechend setzen und unter "Collection Interval for Selected" einen Zeitabstand für die Messung eingeben.

Der Bereich "Analyze" erstellt vor allem Berichte (reports). Die beeindruckend große Bandbreite reicht von tabellarischen Events (etwa Logins) bis hin zu gut skalierten Graphen über die Entwicklung

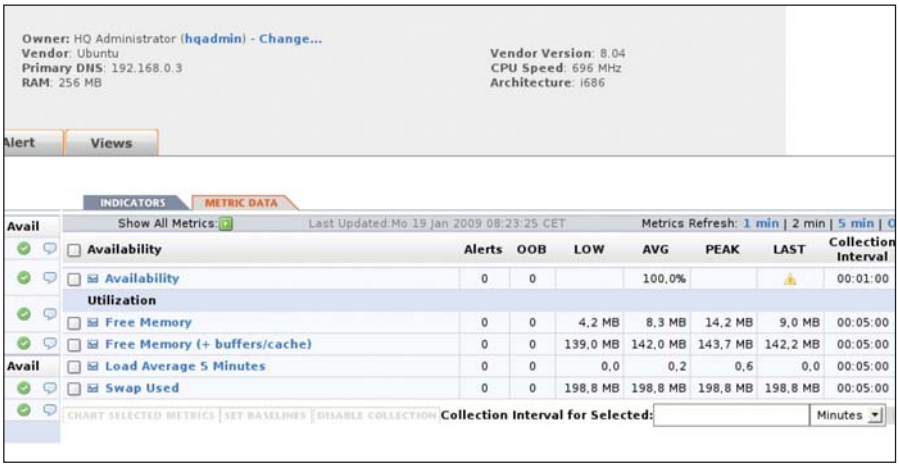


Bild 3: Im "Metric-Data"-Reiter lassen sich über "Show all Metrics" die für angewählte Ressourcen möglichen Checks einblenden und aktivieren

von Festplattenplatz. In jedem Fall sind der gewünschte Zeitbereich und die Ausgabeart festzulegen. Möglich ist hier die Darstellung im Browser (HTML), als PDF sowie Excel- und CSV-Exporte.

Im Administrationsbereich schließlich finden Anwender die Benutzerverwaltung, unter den Server-Einstellungen unter anderem auch die Konfiguration der Standard-Metrics und einen Abschnitt mit den bereits mitgelieferten Plug-ins wie dem bereits erwähnten HQ-Health.

Produkt
Java-basierte Monitoring-Software mit umfangreichen Reporting-Funktionen.

Hersteller
Hyperic Inc.
www.hyperic.com

Preis
Die Startpreise von Hyperic HQ berechnen sich wie folgt: Produktivsysteme/Server kosten 300 Euro pro CPU-Einheit inklusive einem Jahr für Support und Maintenance. Netzwerk-Devices und Nicht-Produktivsysteme schlagen mit 200 Euro pro Device und Support-Jahr zu Buche. Lizenzgebühren fallen nicht an.

Als Produktivsysteme gelten physikalische CPU-Einheiten und virtuelle Maschinen. Nicht-Produktivsysteme sind Netzwerk-Devices und Test- oder Entwicklungssysteme.

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

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

Bedienung	7
Einbinden neuer Clients	8
Automatische Diensteerkennung	10
Überwachung von Logfiles	8
Dokumentation	8

Dieses Produkt eignet sich

optimal für das Monitoring von heterogenen Serverfarmen und die Visualisierung unterschiedlichster Messwerte.

teilweise für die Überwachung von Arbeitsplatzrechnern in KMUs.

nicht für die Überwachung in Minilinux-Systemen und gemieteten virtuellen Servern.

Hyperic HQ 4.01 Enterprise

Einrichten eines Plattform-Service

Als Erstes testeten wir das Seitenausliefern (HTTP-Request) eines Webservers im Internet. Über den Resources-Reiter wählten wir die entsprechende Plattform aus, die den Test ausführen sollte. Ein Klick auf das Tools-Menü stellte uns unter anderem die Option "New Platform Service" zur Auswahl. Zunächst legten wir Service-Name und Service-Typ (HTTP) fest. Erst im zweiten Schritt bestimmten wir die Details über den Link "Configuration Properties". Zwingend notwendig war hier das Eintragen des Rechnernamens (Hostname).

Da der Zugriff über einen Proxy erfolgen sollte, gaben wir diesen ebenfalls hier an. Login und Passwort sind in der Regel nicht erforderlich, die voreingestellten Werte entfernten wir daher. Im "Monitoring"-Reiter erscheint der neue Service zunächst mit einem grauen Fragezeichen. Dies signalisiert, dass noch kein Zugriff erfolgt ist und daher kein Zustand angegeben werden kann. Nach wenigen Minuten erscheinen beim Anklicken des vorher gewählten Service-Namens die Charts zu Response-Code und Response-Time.

Alarmierung

Als Zweites sollte nun ein Alarm ausgelöst werden, wenn ein bestimmter Prozess aus der Prozesstabelle verschwindet. Als Prozess diente der "vino-VNC-Server", wie er beispielsweise unter Ubuntu zum Einsatz kommt. Zunächst war wieder ein Plattformtest mit dem Namen vino-Prozesscheck anzulegen, der Service-Typ war diesmal "Process".

In der Detailkonfiguration kam die "Process-Table-Query-Language" (PTQL) zum Einsatz, die eine weitgehend plattformunabhängige Abfragesyntax der Prozesstabelle ermöglicht. Der Prozessname

lautet "vino-server", der entsprechende Ausdruck (einzutragen unter "process.query") lautet "State.Name.eq =vino-server". Allerdings war es eher mühsam, sich mit der PTQL-Syntax durch das Anlegen von (Test-)Services vertraut zu machen. Besser geeignet als Übungsfeld ist die "Sigar"-Shell, die wir – ergänzt um die jeweiligen Pfadangaben – mit

```
java -jar sigar.jar
```

aufriefen. Schon nach wenigen Minuten fand sich unter den "Ressourcen" der entsprechenden Plattform der "Auto-Group"-Process, in dem neben dem neu definierten vino-server-Check auch der in der Regel vorhandene sshd-Check zu finden ist.

Zur Orientierung gerade im Bereich der Ressourcen ist der oben links eingeblendete "Breadcrum"-Pfad hilfreich. Er spiegelt auch die jeweilige hierarchische Gliederung wider. So ändert er sich von "Platforms / Linux / Plattformname" bei dem Klick auf das als Verzeichnis gekennzeichnete "Process" in "Auto-Grous / Process / Plattformname". Schalteten wir nun mittels des "Metric Data"-Reiters und Klick auf "Availability" auf das Verfügbarkeits-Diagramm um, so konnten wir dort direkt mit "Define New Alert" die gewünschten Kriterien für den Alarm beim Fehlen dieses Prozesses auswählen.

In der "Metric Availability" wählten wir als Bedingung "< (less than)" und trugen im nächsten Feld noch die 1 (für 100 Prozent) ein. Die übrigen Optionen akzeptierten wir mit "OK". Stoppte nun der entsprechende Prozess, erschien sowohl auf dem Dashboard selbst als auch auf jeder anderen Seite am oberen Bildschirmrand bald der Alarmhinweis, der auch per Mail zugestellt wurde.

Leider blieb es jedoch nicht bei diesem einen Hinweis: Solange das Problem fortbestand, folgten im konfigurierten Intervall fortlaufend weitere Meldungen. Dies ließ sich nur verhindern, indem wir einen sogenannten "Recovery Alert" definieren [5, 6] (ein Feature, das der Enterprise-Version vorbehalten ist).

Fazit

Hyperic glänzt in vielen Punkten und trägt seinen vom Johanniskraut abgeleiteten Namen zu Recht. Statt den Administrator mit komplizierten Konfigurationsdateien und -optionen zu plagen, erkennt Hyperic viele Serverdienste automatisch und übernimmt auch gleich deren Konfiguration. Für die individuellen Konfigurationen genügen oft wenige Klicks. Nach einer geringen Einarbeitungszeit erhält der Anwender übersichtliche und aussagekräftige Graphen über wichtige Indikatoren wie etwa Ressourcenverbrauch oder Anbindungsgeschwindigkeit. Dabei bleibt die Bedienung trotz der vielfältigen Möglichkeiten in Sachen Monitoring und Alarmierung einfach.

Der konsequente Einsatz von Java ermöglicht zudem die Unterstützung sehr unterschiedlicher Plattformen. Andererseits führt der Speicher- und CPU-Hunger der J2EE-Applikation dazu, dass an einen Einsatz auf kleineren Systemen, zum Beispiel auf gemieteten virtuellen Servern oder gar im embedded-Bereich, nicht zu denken ist. *(jp)*

Links

[1] **Skript zum Start von Hyperic beim Hochfahren des Servers**
http://support.hyperic.com/display/hypcomm/Debian+Init+Scripts/

[2] **Hyperic-Dokumentation**
http://support.hyperic.com/display/DOC/HQ+Documentation/

[3] **Tutorials und Live-Seminare**
www.hyperic.com/demo/

[4] **Agenten vorkonfigurieren**
http://support.hyperic.com/display/DOC/Agent+Properties/

[5] **Alarmflut mit Recovery Alerts stoppen**
http://support.hyperic.com/display/DOC/Recovery+Alerts/

[6] **MTP-Auth für Alarmmails konfigurieren**
http://support.hyperic.com/display/DOC/Configuring+HQ+Server+for+SMTP+Server/

Im Test: Linux SME Server

Tausendsassa zum kleinen Preis

von Thomas Joos

Neben herkömmlichen Serverlösungen gibt es gerade unter Linux Alternativen, um für kleine und mittelständische Unternehmen diverse Dienste bereitzustellen. Die wohl ausgereifteste Alternative zu kommerziellen Serverlösungen ist der kostenlose Linux SME Server. Die aktuelle Version 7.4 basiert auf CentOS 4.7, einem Klon des RedHat Enterprise Servers 4. SME stellt neben einem Datei- und Druckserver eine Internet-Firewall mit DSL-Funktionalität, einen Webserver auf Basis von Apache 2, eine MySQL-Datenbank, die Sprachen Python und PHP sowie einen vollwertigen Mailserver bereit. IT-Administrator hat sich das Betriebssystem in einem Praxistest genauer angesehen.

SME Server ist modular aufgebaut und durch einen Paketmanager wie RPM nahezu beliebig erweiterbar. Bereits ab Werk kommt die Serverlösung mit einer komfortablen Ausstattung daher. So unterstützt etwa der Mailserver neben POP3 und IMAP4 auch den Zugriff per Webmail. Viren und Spam lassen sich mit einem integrierbaren Scanner bekämpfen, der zudem den Schutz des lokalen Dateisystems unterstützt. Außerdem kann der Server zum Proxy (Squid)-, Telefon-, VPN-, DHCP- und Faxserver ausgebaut werden. Der Telefonserver spielt auf Wunsch den Anrufbeantworter. Praktischerweise ist die Open Source-Distribution nicht auf eine bestimmte Anzahl von Benutzern und Computern begrenzt, sondern kann theoretisch mehrere hundert Anwender anbinden.

Bild 1: Der auf Linux basierende SME Server muss sich in seiner Funktionsvielfalt nicht hinter kommerziellen Produkten verstecken

Einfache Installation und Erstkonfiguration

Die Installation erfolgt am besten über eine bootfähige Installations-CD, die unter [1] als ISO-Datei zur Verfügung steht. Nachdem wir das Image auf CD gebrannt hatten, ließ sich diese zum Booten des Servers und Installieren von SME verwenden. Zu Testzwecken kann die Installation auf einer virtuellen Maschine, zum Beispiel über die kostenlos erhältliche "VirtualBox" oder "VMware Workstation" erfolgen. Letzteren Weg haben wir auch für diesen Test gewählt. Nach dem Erstellen der virtuellen Maschine begrüßte nach deren Bootvorgang die typische Installationsoberfläche von Linux den Tester. Bevor die Installation begann, überprüfte ein Assistent zunächst, ob die CD komplett lesbar war. Dieser Vorgang soll Fehlern während der Installation vorbeugen und stellt sicher, dass sich keine Probleme aufgrund eines fehlerhaften Datenträgers einschleichen.

Treiberlücken bei der Festplattenauswahl

Auch in der aktuellen Version erkannte SME nicht alle Treiber, besonders was Festplatten betraf. Die einzige Möglichkeit bestand darin, die fehlenden Treiber manuell einzubinden, was allerdings einen Linux-versierten Admin voraussetzt. Zwar tauchte dieses Problem bei IDE- oder SATA-Platten seltener auf, aber die meisten Unternehmen setzen bei Servern nun einmal die etwas stabileren SCSI-Datenträger ein. In einer virtuellen Maschine sollte die Festplatte also am besten als IDE-Laufwerk verbunden sein, da SME sonst teilweise Schwierigkeiten mit dem SCSI-Treiber von VMware hat.

Nachdem SME letztendlich den Datenträger erkannt hatte, zeigte der Installationsassistent ein neues Fenster an, in dem sich die Sprache und das Tastaturlayout des Servers auswählen ließen. Während der Installation formatierte SME alle Festplatten.

Aus diesem Grund ist es ratsam, ein Testsystem oder eine virtuelle Maschine zu verwenden, auf der keine Daten gespeichert sind, die Sie später noch benötigen.

Nach der Auswahl der Zeitzone startete schließlich der eigentliche Installationsvorgang. Im Gegensatz zu Windows Server 2008 und Vista läuft dieser nicht imagebasiert ab, sondern wie bei Windows Server 2003 und älteren Versionen durch das Kopieren von Dateien. Abhängig von der Geschwindigkeit des Testsystems kann diese Phase natürlich etwas länger dauern. Danach war ein Neustart nötig und die Grundkonfiguration des Servers konnte beginnen. Der erste Schritt bei der Einrichtung war das Festlegen des Administrator-Kennworts. Dieses benötigen Sie später für die Anmeldung an der Verwaltungs-Webseite. Lobenswert ist, dass der Assistent die Sicherheit des Kennworts überprüft und Verbesserungsvorschläge macht. Ähnlich wie beim Assistenten zur Installation von Active Directory gaben wir auf der nächsten Seite einen Domänennamen ein. SME verwendet diesen Namen dann auch als E-Maildomäne. In der Verwaltungsoberfläche lassen sich jederzeit zusätzliche Domänen eingeben oder die Standarddomäne ändern. Schließlich legten wir noch den Servernamen und die IP-Adresse fest.

Die Auswahl des Arbeitsmodus

Nach den Grundangaben ging es ans Eingemachte. Es stand die Entscheidung an, wie der Server verwendet werden soll. Generell stehen drei Optionen zur Auswahl, nach denen sich der Server konfigurieren lässt: Wollen Sie das Gerät als Internetgateway verwenden, müssen Sie diesen Arbeitsmodus auswählen. Auch lässt sich der Server ohne Internetzugang betreiben beziehungsweise als Server hinter einem DSL-Router oder einer weiteren Firewall. Dieser Betrieb ist der von uns empfohlene Weg. Zwar bietet SME die Möglichkeit, sich direkt per DSL mit dem Internet zu verbinden. Angesichts der Tatsache, dass DSL-Router und kleinere Firewalls sehr günstig sind, sollten Sie diese Konstellation aus Sicherheitsgründen aber nicht in Erwägung ziehen.

Mit der Option "Server und Gateway" ist die Maschine also aus dem Internet erreichbar, zum Beispiel für den Betrieb als Web- und Mailserver. Bei der Auswahl "Privater Server und Gateway" ist der Server quasi nur als Client mit dem Internet verbunden. Von außerhalb lassen sich keine Verbindungen aufbauen. Dazu ist in SME eine Firewall integriert, die zwischen internen und externen Paketen unterscheiden kann. Im Standardumfang sind die Steuerungsmöglichkeiten der Firewall sehr minimal, dafür ist diese aber sicher eingestellt. Mit Erweiterungen lässt sich die Firewall ausbauen, sodass Sie mehr Möglichkeiten zur Freigabe von Datenströmen konfigurieren können.

Aber selbst wenn der Server lediglich im Modus "Nur Server" betrieben werden soll, lassen sich Maildienste und Webserver auf dem lokalen Server erreichen. Dafür mussten wir einfach auf der Firewall oder dem DSL-Router eine Port-Weiterleitung eintragen. Die nächsten Installationsfenster unterschieden sich in den Auswahlmöglichkeiten abhängig von der Option, die wir bei der Internetanbindung gewählt hatten. Im "Server und Gateway"-Modus hatten wir die Möglichkeit, die Verbindung zu spezifizieren. Auf der folgenden Seite wählten wir aus, ob eine DSL- oder Kabelverbindung vorliegt oder ob eine Einwahl per ISDN oder Modem erfolgt. Im Modus "Nur Server" ließ sich im entsprechenden Fenster die IP-Adresse des Internet-Gateways eingeben.

Waren im Server mehrere Netzwerkkarten verbaut, erkannte dies der Installationsassistent und schlug den Aufbau eines Netzwerkkartenverbundes vor. Dieser ließ sich fehlertolerant und für besseren Datendurchsatz konfigurieren. An dieser Stelle offenbarte sich aber eines der Probleme von Linux-Installationen: Bei unseren Tests ließ sich der Installationsassistent bei der Auswahl des Netzwerkkartenverbundes nicht fortführen, sondern sprang ohne Fehler- oder Hinweisfenster immer wieder zurück. Nach einigen Versuchen erbarmte sich der Installationsassistent aber und setzte seine Arbeit fort. In SME integriert ist ein eigener DHCP-Server. Ist im Netzwerk kein anderer DHCP-Server in Betrieb, lässt sich dieser verwenden.

Verwaltung des Servers

Nach der Installation steht die Web-Oberfläche über die Adresse *http://{Servername}/server-manager* zur Verfügung. Der Ver-

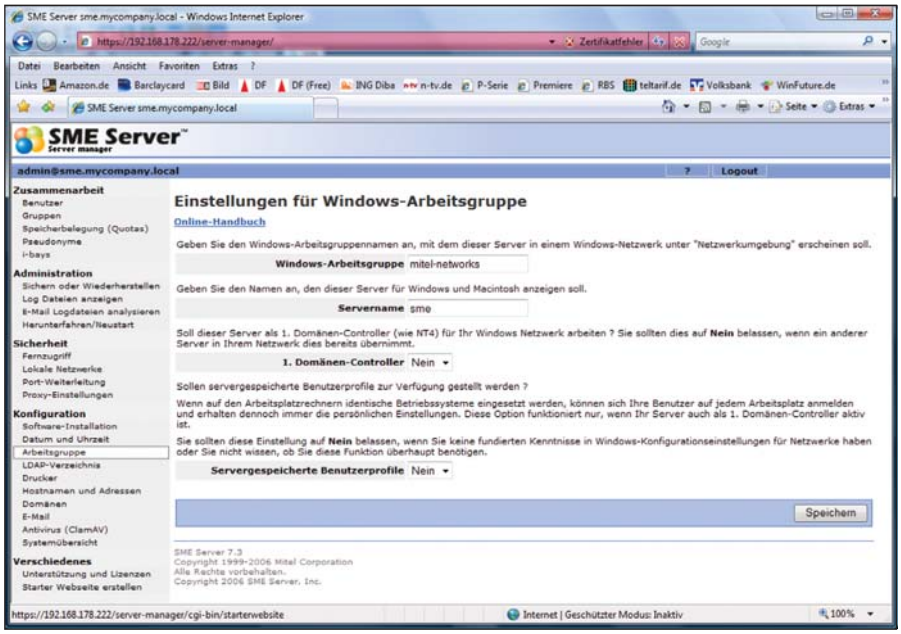


Bild 2: Die Konfiguration von SME erfolgt über ein Web-Interface, was Linux-Neulingen die Arbeit erleichtert

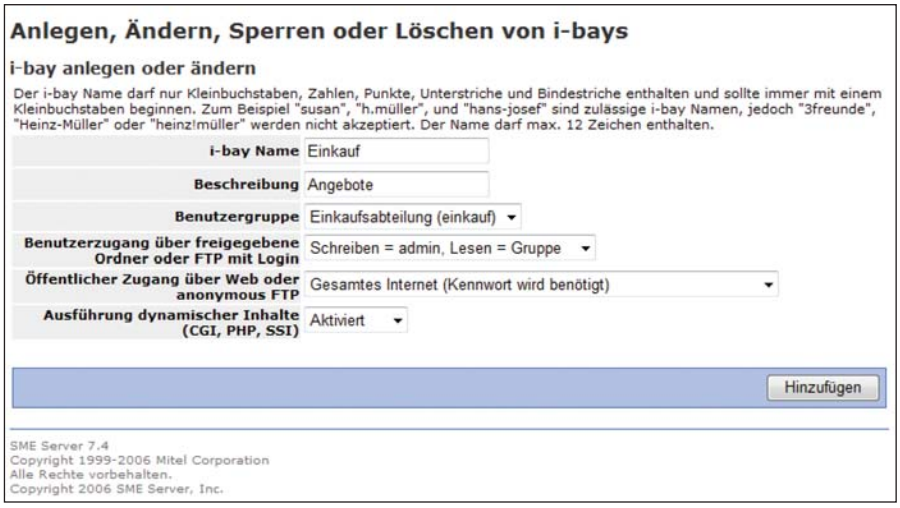


Bild 3: Sogenannte "i-bays" regeln die Rechte von Benutzergruppen. Dazu zählt auch der Fernzugriff auf den Server.

bindungsaufbau findet über eine SSL-verschlüsselte Seite statt. Als Anmeldenamen verwenden Sie "admin" mit dem Kennwort, das Sie bei der Installation festgelegt haben. Auf dieser Oberfläche lassen sich viele Möglichkeiten einstellen, allerdings nicht tiefgehende Administrationsaufgaben. Der Vorteil dieses Szenarios ist, dass die Web-Oberfläche nicht überladen wirkt. Allerdings lassen sich wichtige Einstellungen aus diesem Grund nur in der Konsole festlegen. Daher sollten Sie sich bei der Einrichtung und Verwaltung des Servers mit Linux auskennen.

Erste Konfigurationsschritte

Die Verwaltungswebseite lässt sich über jeden Webbrowser und von jedem Arbeitsplatz aus aufrufen. Die Seite macht einen aufgeräumten Eindruck und Administratoren finden sich schnell zurecht. Über den Link "Benutzer" auf der linken Seite des Verwaltungsfensters werden neue Benutzer konfiguriert und bestehende verwaltet. An dieser Stelle lassen sich auch allgemeine Daten eingeben, Kennwörter zurücksetzen, der VPN-Zugang konfigurieren und eine Weiterleitungsadresse konfigurieren, wenn der Server E-Mails nicht lokal zustellen kann. Benutzer lassen sich zu Gruppen zusammenfassen, um Berechtigungen für Verzeichnisse besser festzulegen. Auch diese Verwaltung ist sehr einfach und intuitiv zu bewerkstelligen. Wer will, kann hier Grenzwerte für zu speichernde Dateien festlegen. Über den Link "Speicherbelegung" ist sehr leicht zu konfigurieren, welche Benutzer wie viel Speicherplatz belegen dürfen. Die Möglichkeiten an dieser Stelle sind jedoch sehr begrenzt: Weder lassen sich Gruppen einbinden noch detailliertere Konfigurationen vornehmen, zum Beispiel welche Dateitypen Anwender speichern dürfen. Im Gegensatz zu Windows bietet Linux SME keine Möglichkeit zu bestimmen, wie der Server beim Erreichen des Grenzwertes vorgehen soll, also ob er das Speichern weiterer Dateien verhindern oder den Anwender nur warnen soll.

Eine Besonderheit von Linux SME sind die sogenannten "i-bays". Hierbei handelt es sich um die Möglichkeit, spezielle Verzeichnisse auf dem Dateisystem zu erstellen, "Information-Bays" genannt. Im Rahmen der Einrichtung wird festgelegt, welche Benutzergruppe Zugriff auf das Verzeichnis erhalten soll. Eine Besonderheit der i-bays ist die Möglichkeit, schon bei der Erstellung den Zugriff über das Internet zu konfigurieren. Aktivieren Sie den Internetzugriff, lässt sich über das Internet per Webbrowser oder FTP auf das Verzeichnis zugreifen. Auch hier bietet SME einige Eingriffs- und Kontrollmöglichkeiten. Über den Bereich "Administration" legen Sie die Datensicherung des Servers fest. Leider hat die Software "flexbackup", welche die Datensicherung steuert, standardmäßig nicht die Möglichkeit, Daten auf Netzlaufwerke oder DVD-Brenner zu sichern. Im Standardumfang der SME-Distribution unterstützt die Datensicherung nur Bandlaufwerke. Mit einigen Tricks, Recherche im Internet und etwas Linux-Wissen lassen sich die Konfigurationsdateien der Software aber so anpassen, dass andere Sicherungsmethoden möglich sind.

Zur Fehlerbehebung oder zur Überwachung bietet der Server über den Link "Log Dateien anzeigen" die Möglichkeit, alle aktuellen Aktionen des Servers und der laufenden Prozesse zu überwachen. Hier gibt es einige Filter- und Einstellungsmöglichkeiten. Über die Webseite lässt sich der Server übrigens über das Netzwerk herunterfahren und neu starten. Das erspart Laufarbeit und die Verwendung der Konsole erübrigt sich. Leider bietet der Assistent für den Neustart nicht die Möglichkeit, eine Uhrzeit einzugeben, zu der der Server neu starten soll. Auch eine Warnung an die angebundenen Anwender lässt sich leider nicht erstellen.

Der Fernzugriff erspart unnötige Wege

Im Bereich "Sicherheit" lässt sich über den Link "Fernzugriff" der VPN-Zugang des Servers steuern. Als Protokoll für VPN verwendet Linux SME standardmäßig das PPTP-Protokoll. Dabei werden einzelne PTP-Pakete (Point-To-Point) in sogenannte GRE-Pakete (Generic Routing Encapsulation) verpackt und verschickt. Viele Experten stufen PPTP mittlerweile als sicher ein, auch wenn die Verschlüsselung nicht so stark ist wie die von L2TP. PPTP ermöglicht die verschlüsselte Einkapselung von verschiedenen Netzwerkprotokollen und unterstützt Schlüssellängen bis zu 128 Bit. Nachdem die Authentifizierung durchgeführt wurde, wird die Verbindung verschlüsselt. Die Verschlüsselung baut auf dem Kennwort der Authentifizierung auf. Je komplexer das Kennwort ist, desto besser ist die Verschlüsselung. Da die Verschlüsselung und der Transport der einzelnen IP-Pakete durch das GRE-Protokoll durchgeführt wird, ist darauf zu

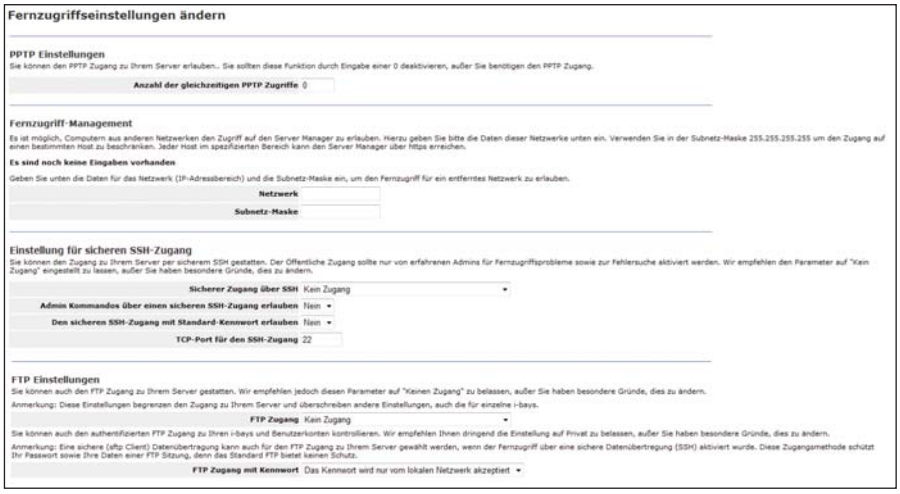


Bild 4: Der Remote-Zugriff auf den SME Server lässt sich auf mehrere Arten realisieren

achten, dass die Hardwarefirewall beziehungsweise der DSL-Router, der vor dem ISA-Server im Internet platziert wird, dieses Protokoll beherrscht.

Im gleichen Bereich erfolgt der Zugriff auf die Verwaltungswebseite des SME Servers. Diese ist standardmäßig auf das lokale Netzwerk beschränkt. Auch der SSH- und der FTP-Zugang lassen sich an dieser Stelle steuern. Ferner kann hier die Konfiguration des lokalen Proxyservers für den Internetzugriff der Anwender sowie die Steuerung der Port-Weiterleitung vorgenommen werden, wenn der Server als Linux-Gateway zum Einsatz kommt.

SME kann auch mit Windows

Die Entwickler von SME erweitern und verbessern das System ständig. Sicherheits-Patches und neue Programmversionen sollten daher genauso eingepflegt werden wie unter Windows. Um die Aktualisierung zu erleichtern ist über den Link "Software-Installation" die Update-Seite von SME zu erreichen. Dieser überprüft, ob es im Internet neue Versionen und Patches gibt und installiert diese auf dem Server. Die Installation lässt sich problemlos über die Webseite anstoßen. Windows-Arbeitsstationen lassen sich außerdem an Linux SME wie an einen Domänencontroller anbinden. Standardmäßig simuliert SME zwar keinen Domänencontroller, aber über den Link "Arbeitsgruppe" können Sie alle notwendigen Konfigurationen steuern. An dieser Stelle lässt sich der Name des Servers, der Windows-Domäne und die Emulation als Domänencontroller aktivieren. Außerdem werden an dieser Stelle servergespeicherte Benutzerprofile aktiviert. Die Benutzerkonten und -daten speichert Linux SME in ein LDAP-Verzeichnis, ähnlich wie das Active Directory von Windows Server 2000/ 2003/2008. Zwar lassen sich an dieser Stelle keine spezifischen Einstellungen ändern, aber über den Link "LDAP-Verzeichnis" wird bestimmt, ob und wie andere Server und Programme auf das Verzeichnis zugreifen dürfen.

Weitere interessante Möglichkeiten sind die Steuerung des E-Mailservers und des dazugehörigen Virenschutzes. Dieser baut auf ClamAV auf. Über die Links "E-Mail" und "Antivirus" steuern Sie über den Webbrowser den Zugriff und die Konfiguration. Allerdings lassen sich an dieser Stelle nur sehr rudimentäre Einstellungen vornehmen. Gerade hier würden sich viele Systemverwalter etwas mehr Einstellungsmöglichkeiten wünschen. Für kleinere Unternehmen sollten die Einstellungen an dieser Stelle jedoch ausreichen. Systemverwalter, die mehr Einstellungsmöglichkeiten verlangen, können entweder in die Konfigurationsdateien eingreifen oder zusätzliche Pakete installieren.

SME unterstützt ferner eine Ordnerduplizierung, um Datenverlust vorzubeugen. Gut gefallen hat uns, dass SME dazu ein echtes RAID 1 verwendet, wenn der Computer kein Hardware-RAID bietet. Negativ in Erscheinung trat hingegen, dass SME keine speziellen Konnektoren bietet, um Computer an den Server anzubinden. Auch die komplette Datensicherung der Arbeitsstationen auf den Server ist nur über Zusatz-Tools möglich. Geübte und bastelfreudige Anwender können diese Funktionen kostenlos nachrüsten, hier ist aber deutlich mehr Arbeit notwendig als zum Beispiel beim Small Business Server von Microsoft.

Zusatzmodule für jeden Zweck

Bereits im Standardpaket sind alle wichtigen Serverfunktionen integriert. In den meisten Fällen ist eine Erweiterung des Servers mit weiteren Paketen nicht notwendig. Einige Zusatzfunktionen sind aber durchaus erwähnenswert.

Fetchmail und SpamAssassin

Der Mailserver arbeitet mit dem Multidrop-System, das heißt der Server holt die Mails per POP3 ab und verteilt diese intern an die einzelnen Postfächer. Wer sich etwas mit Linux auskennt, kann die Erweiterung "Fetchmail" installieren. Diese baut den Server um weitere Mailfunktionen aus, beispielsweise ein besseres Webfrontend. Die Installation dieser Software lässt sich allerdings nur über die Shell durchführen. Die Konfiguration ist dann wieder über die Web-Oberfläche möglich. Unter [2] finden Sie die neueste Version der Distribution sowie Informationen zu deren Installation und Konfiguration.

Was beim SME Server etwas negativ auffällt, ist die Behandlung der Datensicherung. Die Konfiguration des Backups lässt sich zwar in der Web-Oberfläche durchführen, allerdings sind die Möglichkeiten begrenzt. Wie erwähnt ist vor allem die Sicherung auf Festplatten oder Freigaben im Netzwerk nicht optimal bis gar nicht integriert. Linux-versierte Administratoren können die Konfigurationsdatei aber so abändern, dass eine Sicherung auf eine Festplatte möglich ist. Wer Linux SME ein-

setzt, sollte außerdem auf notwendige Sicherheitserweiterungen achten. In diesem Bereich stellen viele Entwickler kostenlose Möglichkeiten zur Verfügung. Unter [3] finden Sie Pakete für Antivirenschutz auf Basis von Clam Antivirus. Auch Antispam-Pakete auf der Grundlage von Spam-Assassin finden Sie auf dieser Seite.

Produkt
Auf Linux basierendes Serverbetriebssystem, das verschiedene Dienste bereitstellt.

Hersteller
Open Source
www.contribs.org

Preis
Kostenlos, da das Paket unter der GNU General Public License (GPL) vertrieben wird.

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

Konfiguration	7
Laufender Administrationsaufwand	8
Zuverlässigkeit	8
Funktionsumfang	9
Skalierbarkeit	8

Dieses Produkt eignet sich

optimal für kleinere Unternehmen, die eine einfache und kostenlose Serverlösung suchen und offen für Linux sind.

teilweise für mittlere Unternehmen, die Server für kleinere Niederlassungen suchen und wenig investieren wollen.

nicht für große Unternehmen mit Microsoft-Netzwerken oder Firmen, die mehrere Server einsetzen.

SME Server

[1] Deutsche SME Server-Community
www.smeserver.de

[2] SME Server Dokumentation
www.contribs.org

[3] Security-Module für SME
http://sme.swerts-knudsen.dk

[4] Erweiterungen für den SME Server
http://sudemo.info/wiki/

Links

Wer mehr Erweiterungen will, muss Linux-Wissen mitbringen

Es ist zu beachten, dass die Einbindung zusätzlicher Pakete deutlich mehr Linux-Wissen erfordert als die Grundinstallation und -konfiguration des Servers. Auch die Verwaltung des Servers verkompliziert sich mit steigender Anzahl an Add-ons. Auch bei der Erweiterung des Servers kann es vorkommen, dass nicht alle Pakete kompatibel zu den neuen Versionen von Linux SME sind. Viele Pakete, die kompatibel zu den Versionen 6.x sind, funktionieren bei den Versionen 7.x nicht mehr. Als Telefonserver-Erweiterung unterstützt SME die bekannte Serversoftware "Asterisk". Diese erweitert den Server zu einer vollwertigen Telefonanlage mit VoIP-Fähigkeit. Auch hier ist wieder Hintergrundwissen für Linux und die Konfiguration von Telefonanlagen notwendig. Allerdings sind die Möglichkeiten dann schier unendlich. Viele Zusatzmodule finden Sie im Internet unter [4].

Fazit

SME bietet einen großen Funktionsumfang, der für kleine und mittelständische Unternehmen durchaus interessant sein kann. Selbst Linux-Muffel, die aber gerne an Servern basteln, sollten sich SME zumindest in einer virtuellen Umgebung einmal ansehen. Die Konfiguration ist nicht kompliziert, die Verwaltung erfolgt zum größten Teil über eine Web-Oberfläche, und auch der Großteil aktueller Hardware unterstützt die Lösung. Alle Funktionen von SME wird wohl kaum ein Unternehmen nutzen, aber wer will, findet mit SME Server schier unbegrenzte Erweiterungsmöglichkeiten für sein Netzwerk mit hochprofessionellen Tools wie Joomla und MySQL. Standardmäßig ist die Oberfläche sehr einfach gehalten, und auf der Web-Oberfläche lassen sich alle wichtigen Einstellungen vornehmen. Aktuell in der Entwicklung befindet sich die neue Version 8.0, die sich als Betaversion bereits aus dem Internet herunterladen lässt. *(ln)*

Quelle: Pixelio.de

Mit ZFS von Sun steht ein umfangreiches, aber dennoch einfach zu bedienendes Filesystem zur Verfügung

Erste Schritte im Dateisystem ZFS

Ordnung mit nur zwei Kommandos

von Thomas Weyergraf

Will ein modernes Dateisystem schnell sein, muss es ausgefeilte Cache-Strategien implementieren, die jedoch nicht dazu führen dürfen, dass die Hauptanforderung verletzt wird: die Datensicherheit. Im Regelbetrieb darf ein Dateisystem gar keine Daten verlieren und im Fall eines Ausfalls oder Absturzes sollte es so wenig Daten wie möglich einbüßen und dabei schnell reparierbar sein. Sun hat für die Entwicklung seines Filesystems Jahre gebraucht und das Ergebnis, ZFS, erstmals im Sommer 2006 zusammen mit dem hauseigenen Unix-Derivat Solaris ausgeliefert. In diesem Workshop zeigen wir Ihnen die Grundlagen von ZFS auf und geben Ihnen anhand von Beispielen eine praktische Einführung in dessen Administration.

Drei Kriterien stehen bei ZFS im Vordergrund: Es ist einfach zu administrieren, es gibt praktisch keine Grenzen hinsichtlich Größe und Anzahl von Dateisystemen und Dateien, und ZFS bietet ein Maximum an Datensicherheit. Wie unsere Praxisbeispiele zeigen werden, ist die Administration in der Tat sehr einfach – lediglich zwei Kommandos werden benötigt. Oft reicht eine einzige Kommandozeile aus, um einen RAID-Verbund zu erzeugen und ein betriebsbereites Filesystem darauf anzulegen. Um zukünftige Grenzen von vornherein zu vermeiden, hat Sun ZFS als 128-Bit-Dateisystem ausgelegt, wodurch ein Adressraum zur Verfügung steht, der für alle theoretisch denkbaren Speichersysteme ausreicht.

Auch in Sachen Datensicherheit hat Sun tief in die Trickkiste gegriffen. Im Normalbetrieb funktionieren heutige Dateisysteme problemlos – Fehler sind ausgesprochen selten und die Datensicherheit ist gegeben. Interessant wird das Thema, wenn Dateisysteme nicht sauber heruntergefahren werden – etwa im Fall eines Systemabsturzes. Unter Unix müssen die betroffenen Dateisysteme überprüft und gegebenenfalls repariert werden. Das Problem dabei: Der Vorgang dauert abhängig von der Größe der Dateisysteme sehr lange – unter Umständen sogar Stunden. Sun umgeht das Problem durch eine geschickte Strategie zum Schreiben von Daten in ZFS. Anders als in herkömmlichen Dateisystemen überschreibt ZFS Daten niemals. Wird eine Datei modifiziert, werden die bestehenden Datenblöcke nicht verändert – vielmehr allokiert ZFS neue Blöcke, in denen die aktualisierten Daten geschrieben werden. Anschließend lassen sich die Blöcke mit den alten Daten freigeben.

Schnappschüsse gegen Datenverlust

Das gleiche Verfahren wendet ZFS auch auf die Verwaltungsdaten an. Mit diesem Vorgehen wird das Dateisystem praktisch unzerstörbar. Stürzt ein ZFS-basiertes System ab, sind stets die bereits vorhandenen Daten vollständig intakt – lediglich gerade zum Zeitpunkt des Absturzes im Schreiben befindliche Daten sind verloren. Der zeitaufwendige fsck-Lauf entfällt. Sun wendet dieses Verfahren auch im ZFS-eigenen RAID-Subsystem an. Das Filesystem bietet mit RAID-Z und RAID-Z2 zwei an RAID-5 angelehnte Verfahren, bei denen Daten und Parity-Informationen ebenfalls in neuen Blöcken abgelegt werden, statt bestehende Daten direkt zu überschreiben. Ganz ohne Nachteil ist dieses Verfahren allerdings nicht: Wird in einem ZFS-Dateisystem eine sehr große Zahl hinreichend großer Dateien sehr oft modifiziert, verteilen sich die Datenblöcke der Dateien zusehends auf den Platten. Das kann die durchschnittlichen Seek-Zeiten beim Datenzugriff in die Höhe treiben. Sun hat an dieser Stelle viel optimiert und vor allem die gegenwärtige Hardware-Entwicklung auf seiner Seite. Server verfügen heutzutage über sehr viel RAM, was effektives Caching selbst großer Datenmengen erlaubt, und mit der Verbreitung von SSDs in performancekritischen Serveranwendungen erledigt sich das Seek-Problem quasi von selbst.

Auf der anderen Seite bietet das Verfahren aber ungeahnte Vorteile: Es erlaubt, Snapshots eines Dateisystems ohne nennenswerten Aufwand zu erzeugen. Ein Snapshot ist quasi ein Foto des Dateisystems unter Beibehaltung des aktuellen Datenbestands. Änderungen finden zwar statt,

aber der Zustand zum Zeitpunkt des Snapshots wird beibehalten und nicht freigegeben. Der Administrator kann später jederzeit auf den Datenbestand zum Zeitpunkt des Snapshots zugreifen. Unter ZFS sind diese Schnappschüsse sehr einfach und vor allem schnell realisiert. Im Prinzip wird nur der Zeitpunkt vermerkt – alle zukünftigen Änderungen überschreiben bestehende Daten ohnehin nicht.

Damit gestaltet sich der Umgang mit Snapshots sehr einfach und verleitet dazu, diese Technik intensiver als bislang einzusetzen. Tägliche oder gar stündliche Schnappschüsse sind unter ZFS im Handumdrehen erzeugt und administrativer Alltag. Backups können im laufenden Betrieb bequem von Snapshots gezogen werden, die zu definierten Zeitpunkten erzeugt wurden – etwa nachdem laufende Dienste auf dem Server kurz angehalten wurden. Zudem können Snapshots unabhängig vom Orginal-Dateisystem beschrieben werden, in diesem Fall heißen die Snapshots "Clones". Orginal und Clone teilen sich alle gemeinsamen unmodifizierten Datenblöcke, lediglich die Änderungen an beiden Dateisystemen werden unabhängig voneinander verwaltet. Das Anlegen eines Snapshots oder eines Clones erfordert somit keinerlei aufwendige Kopiervorgänge bestehender Daten, und die "Kosten" hinsichtlich Speicherkapazität und Serverrechenzeit sind praktisch null.

Wie eingangs erwähnt, fasst ZFS Storagemanagement, Volumemanagement und Dateisysteme aus klassischer Sicht zusammen. Das Filesystem bildet dabei Storage-Pools (Zpools). In diesen Pools werden Blockdevices wie Platten zusammengefasst und mittels eines ZFS-Dateisystems gemountet. Als Blockdevices – die unter ZFS als Virtual Devices (Vdev) bezeichnet werden – sind Festplatten, Partitions und Dateien erlaubt. Wenn nicht anders angegeben, werden Vdevs in einem Zpool als Stripe (RAID-0) betrieben. Alternativ bietet ZFS die Möglichkeit, Vdevs zu spiegeln (Mirror, RAID-1) oder als die bereits erwähnten RAID-Z oder RAID-Z2-Arrays zu konfigurieren. Ein eingerichteter Zpool steht automatisch samt darauf angelegtem ZFS-Dateisystem sofort zur Verfügung.

Der Administrator kann auf einem Zpool weitere ZFS-Dateisysteme anlegen – eine statische Zuteilung von Speicher zu Dateisystemen, wie etwa bei LVM unter Linux, entfällt. Standardmäßig steht jedem ZFS-Dateisystem der gesamte Speicherplatz des Zpools zur Verfügung. ZFS erlaubt allerdings, die Speicherkapazität pro ZFS-Dateisystem mittels Quotas zu limitieren. Diese Quotas lassen sich zur Laufzeit ändern, wodurch aufwendige Resize-Aktionen auf RAIDs, Logical Volumes und Dateisystemen entfallen.

Administration mit zwei Kommandos

Die gesamte praktische Administration läuft unter ZFS mit lediglich zwei Kommandos ab: *zpool* und *zfs*. Dabei wickeln Sie mit *zpool* den Löwenanteil des eigentlichen Storagemanagements ab, während *zfs* vornehmlich dazu dient, auf bereits eingerichteten und aktiven Zpools ZFS-Dateisysteme zu administrieren.

Anlegen eines Zpools

Zunächst legen wir in unserem Beispiel einen Zpool an. Nutzen Sie hierfür

```
zpool create itatest /dev/dsk/c1t1d0
  /dev/dsk/c1t2d0
```

Damit erzeugen Sie einen Zpool mit zwei Festplatten als Vdevs. Ohne Angabe eines RAID-Levels legen Sie so die beiden Platten als Stripe (Raid-0) an. Mit dem Kommando *zpool list* lassen sich nun alle im System vorhandenen Zpools anzeigen (Listing 1). In unserem Beispiel existiert nur der Zpool "itatest", der zuvor angelegt wurde. Eine detaillierte Übersicht zu einem Zpool erhalten Sie mit dem Befehl *zpool status {zpool-name}* (Listing 2).

In unserem Beispiel werden komplette Festplatten verwendet, ein Vorgehen, das von Sun ausdrücklich empfohlen wird, da ZFS damit die höchste Performance erreicht. Alternativ können Sie hier auch Partitions oder gar Dateien verwenden.

Alle Kommandos, selbst das Erzeugen des Zpools, sind übrigens extrem schnell ausgeführt. Lange Wartezeiten, wie unter klassischen Unix-Dateisystemen etwa beim *mkfs*, entfallen. Nach lediglich wenigen Sekunden ist der Zpool anlegt und auch zerstört. Letzteres erreichen Sie mit

```
zpool destroy itatest
```

Ohne Angabe eines Mountpoints wird der Zpool in unserem Beispiel automatisch unter "/itatest" gemountet und kann sofort verwendet werden. Ebenfalls abweichend von klassischen Unix-Dateisystemen sind Zpool-Änderungen automatisch und dauerhaft gültig: Ein angelegter Zpool steht auch nach einem Reboot wie gewohnt zur Verfügung, ohne dass weitere Konfigurationsschritte wie das Eintragen in */etc/fstab* nötig wären. Für ZFS gelten hinsichtlich der Datensicherheit bei der Verwendung von RAID die üblichen Einschränkungen. Der Zpool in unserem Beispiel bietet mit RAID-0 zwar die höchstmögliche Performance, aber die geringste Datensicherheit. Der Ausfall einer Platte führt zum Datenverlust.

```
zpool list
NAME     SIZE   USED  AVAIL   CAP  HEALTH  ALTROOT
itatest  68G    95.5K  68.0G   0%  ONLINE  -
```

Listing 1

```
zpool status itatest
pool: itatest
state: ONLINE
scrub: none requested
config:

NAME        STATE     READ      WRITE     CKSUM
Itatest     ONLINE    0         0         0
c1t1d0      ONLINE    0         0         0
c1t2d0      ONLINE    0         0         0

errors: No known data errors
```

Listing 2

1. Erzeugen eines Zpools als Mirror mit zwei Dateien als Vdev:

```
# zpool create itatest mirror /usr/testhd1 /usr/testhd2
```

2. Anlegen einer 40 MByte großen Testdatei auf dem Zpool:

```
# mkfile 40m /itatest/test1
```

3. Simulation des Ausfalls eines Vdev:

```
# rm /usr/testhd2
```

4. Erzwingen eines Checks des Zpools:

```
# zpool scrub itatest
```

5. Status zeigt Zpool als defekt:

```
# zpool status
pool: itatest
state: DEGRADED
status: One or more devices could not be opened.
      Sufficient replicas exist for the pool
      to continue functioning in a degraded state.
action: Attach the missing device and online it using
   'zpool online'.
see: http://www.sun.com/msg/ZFS-8000-2Q
scrub: scrub completed after 0h0m with 0 errors on Wed Dec
   17 08:40:28 2008
config:

NAME          STATE       READ        WRITE       CKSUM
Itatest       DEGRADED    0           0           0
Mirror        DEGRADED    0           0           0
/usr/testhd1  ONLINE      0           0           0
/usr/testhd2  UNAVAIL     0           0           0
   cannot open

errors: No known data errors
```

6. Entfernen des "defekten" Vdevs aus dem Zpool:

```
# zpool detach itatest /usr/testhd2
```

7. Hinzufügen eines Ersatz-Vdev zum Zpool:

```
zpool attach itatest /usr/testhd1 /usr/testhd3
```

8. "Resilver"-Lauf:

```
root@drdeng:/# zpool status
pool: itatest
state: ONLINE
scrub: resilver completed after 0h0m with 0 errors on Wed
   Dec 17 09:05:53 2008
config:
[...]
```

Umgang mit Vdev-Ausfällen

```
NAME        STATE     READ      WRITE     CKSUM
Itatest     ONLINE    0         0         0
raidz1      ONLINE    0         0         0
c1t1d0      ONLINE    0         0         0
c1t2d0      ONLINE    0         0         0
c1t3d0      ONLINE    0         0         0

errors: No known data errors
```

Listing 3

```
zfs list
NAME          USED   AVAIL   REFER   MOUNTPOINT
Itatest       132K   66.9G   24.0K   /home2
```

Listing 4

Zpool mit RAID-Z

Nun wollen wir einen Zpool erzeugen, der mit RAID-Z arbeitet. Lediglich die Angabe des RAID-Levels, also der Parameter 'raidz', reicht aus, um den Zpool als RAID anzulegen:

```
zpool create itatest raidz
  /dev/dsk/c1t1d0 /dev/dsk/c1t2d0
  /dev/dsk/c1t3d0
```

Anschließend zeigt der Status des Zpools, dass dieser als RAID-Z arbeitet (Listing 3). Die weiteren im Kasten "Umgang mit Vdev-Ausfällen" gezeigten Schritte demonstrieren den Umgang von ZFS mit Vdev-Ausfällen. Zunächst legt Schritt 1 einen Zpool als Mirror (RAID-1) an, der als Vdevs zwei Dateien verwendet. Anschließend wird der Zpool mit Testdaten beschrieben (Schritt 2) und der Ausfall eines Vdev durch Löschen der entsprechenden Datei (Schritt 3) simuliert. In Schritt 4 schließlich folgt die Konsistenzprüfung – dieser Vorgang heißt im ZFS-Kontext "Scrubbing" (Schrubben). Der anschließende *zpool status* zeigt, dass der Zpool beschädigt (DEGRADED) ist und gibt in den Zeilen "status:" und "action:" klar verständliche Hinweise, was passiert ist und was zu tun ist (Schritt 5). Zunächst entfernt Schritt 6 das defekte Vdev aus dem Zpool. Würde es sich um eine physikalische Platte handeln, könnten Sie diese nach dem Detach physikalisch entfernen. In Schritt 7 wird nun ein Ersatz-Vdev hinzugefügt. ZFS fängt automatisch an, im Hintergrund das Zpool-RAID wieder aufzubauen – im ZFS-Kontext als "Resilvering" bezeichnet. Schritt 8 zeigt schließlich den Status des Zpools nach vollendetem Resilvering. An dieser Stelle sind die Reparaturarbeiten bereits abgeschlossen.

Wie Sie sehen, fällt der Umgang mit Zpools denkbar einfach – ein Kommandozeilen-Tool, wenige und klare Optionen und vor allem kurze Kommandolaufzeiten erleichtern den Umgang mit Zpools ungemein. Der einzige Vorgang, der mitunter eine längere Laufzeit erfordert, ist der Resilver-Lauf. Da dieser vollkommen transparent im Hintergrund abgewickelt wird, fällt eine Beeinträchtigung des Regelbetriebs minimal aus, von leichten Leistungseinbußen des Zpools während des Resilvering einmal abgesehen.

Alle vorangegangenen Beispiele haben lediglich ein ZFS-Dateisystem pro Zpool verwendet. Dies entspricht der traditionellen Vorgehensweise, nach der auf RAIDs logical Volumes eingerichtet werden, die ihrerseits mit Dateisystemen zugänglich gemacht werden. Mit dem zweiten ZFS-Befehl *zfs* lassen sich Zpools sehr viel flexibler verwalten.

Zpools verwalten

Nachfolgend gehen wir auf die Verwaltung der Zpools über *zfs* ein. Zunächst können Sie mit

```
zfs set mountpoint=/home2 itatest
```

den Mountpoint des Zpools "itatest" vom Default-Wert "/itatest" auf "/home2" ändern. Analog zum Kommando *zpool* bietet auch *zfs* die Möglichkeit, mittels der Option "list" Informationen zu den verfügbaren ZFS-Dateisystemen auszugeben: (Listing 4).

Anschließend erzeugen Sie mit

```
zfs create itatest/bill
zfs create itatest/bob
zfs create itatest/alice
```

drei ZFS-Dateisysteme im Zpool "itatest". Die Syntax "itatest/bill" bezeichnet nicht den tatsächlichen Dateipfad, sondern lediglich die Zugehörigkeit zum Zpool – erreichbar ist etwa "itatest/bill" über den Pfad "/home2/bill", da dieser zuvor geändert wurde. Die erzeugten Dateisysteme "bill", "bob" und "alice" erben alle Optionen, die im übergeordneten ZFS "itatest" gesetzt wurden, darunter auch die verfügbare Kapazität. Nun können Sie mit

```
zfs set quota=5G itatest/bill
zfs set quota=10G itatest/bob
```

die Quotas für die Dateisysteme bill und bob setzen. Bill darf 5 GByte Speicherplatz benutzen, während bob 10 GByte zugewiesen werden. Doch anders als unter Unix üblich, kennt ZFS an sich keine Quotas per User. Üblicherweise haben Administratoren unter Unix etwa die Home-Verzeichnisse der Benutzer unter "/home" als Verzeichnisse abgelegt und die verfügbare Kapazität pro Benutzer mit den klassischen Quotas angepasst. Unter ZFS gehen Sie nun anders vor: Pro User legen Sie ein ZFS an (etwa bill, bob und alice), deren Mountpoints vom übergeordneten ZFS geerbt werden. Speicherplatz wird pro User anschließend explizit auf dem User-ZFS gesetzt – genauso wie im vorliegenden Beispiel.

Mit dem Kommando *zfs list* können Sie nun wieder die Dateisysteme unter "itatest" anzeigen lassen (Listing 5). Um die Optionen anzuzeigen, die für das Dateisystem "itatest/bill" gesetzt sind, nutzen Sie den Befehl *zfs get all itatest/bill*: Neben den eigentlichen Optionen in der Spalte "Properties" ist die Spalte "Source" wichtig. Ein "-" in dieser Spalte bedeutet, dass die Option nicht verändert werden kann. Ein "local" zeigt, dass die Option explizit für dieses ZFS gesetzt wurde, während "default" die Standardeinstellung anzeigt. Das zuvor angesprochene Vererben von Eigenschaften durch übergeordnete ZFS' wird anhand der Option "mountpoint" sichtbar: Der Mountpoint wurde für itatest gesetzt und an "itatest/bill" vererbt. Entsprechend der Ausführung von Zpool-Kommandos gilt auch für *zfs*, dass die Laufzeit selten mehr als Sekunden benötigt. Möchten Sie viele ZFS-Dateisysteme für entsprechend zahlreiche Benutzer anlegen, geht das sehr schnell.

```
zfs list
NAME            USED  AVAIL  REFER  MOUNTPOINT
itatest         235K  66.9G  29.3K  /home2
itatest/alice  24.0K  66.9G  24.0K  /home2/alice
itatest/bill   24.0K  5.00G  24.0K  /home2/bill
itatest/bob    24.0K  10.0G  24.0K  /home2/bob
```

Listing 5

Fazit

Bei ZFS handelt es sich um ein sehr mächtiges Dateisystem. Es hat seit seiner Markteinführung zu Recht für Furore gesorgt und zeigt, in welche Richtung die Entwicklung von Dateisystemen und Storage-Management geht. Bereits jetzt arbeiten viele Betriebssystementwickler an der Integration von ZFS in andere Systeme als Solaris. FreeBSD unterstützt schon ZFS, NetBSD wird folgen und Mac OS soll augenscheinlich komplett auf ZFS umsteigen. Die von Sun gewählte Open Source-Lizenz zusammen mit zahlreichen Patenten auf grundlegende ZFS-Technologien machen eine Integration in Linux dagegen unwahrscheinlich. Wenn Sie praktische Erfahrungen mit ZFS im Administrationsalltag sammeln, werden Sie garantiert nur noch unwillig auf die klassischen Filesysteme zurückgreifen wollen. Es bleibt zu hoffen, dass Sun ZFS weiter öffnet – als Standarddateisystem unter UNIX wäre es mehr als nur willkommen. *(dr)*

[1] Informationen zu ZFS
http://docs.sun.com

Links

```
zfs get all itatest/bill
NAME          PROPERTY       VALUE                  SOURCE
itatest/bill  type           filesystem             -
itatest/bill  creation       Wed Dec 17 10:26 2008  -
itatest/bill  used           24.0K                  -
itatest/bill  available      5.00G                  -
itatest/bill  referenced     24.0K                  -
itatest/bill  compressratio  1.00x                  -
itatest/bill  mounted        yes                    -
itatest/bill  quota          5G                     local
itatest/bill  reservation    none                   default
itatest/bill  recordsize     128K                   default
itatest/bill  mountpoint     /home2/bill            inherited from itatest
[...]
```

Listing 6

VMware VirtualCenter durch Plug-ins erweitern

Echte Erweiterungen für künstliche Umgebungen

von Bertram Wöhrmann

Bild: Adem Percem - Fotolia.com

VMware sieht das VirtualCenter als die zentrale Managementkonsole in virtualisierten Umgebungen. Bisher war es jedoch vor allem in größeren Infrastrukturen recht mühsam, sich für bestimmte Aufgaben wie etwa die Migration von Storage durch diverse Menüstrukturen zu hangeln. Version 2.5 des VirtualCenter erlaubt jetzt erstmals die Integration externer Plug-ins, sodass sich stets wiederkehrende Arbeitsschritte erheblich vereinfachen lassen. IT-Administrator stellt Ihnen in diesem Workshop die besten Plug-ins vor und hilft bei deren optimaler Verwendung.

In seinen Anfangszeiten war das VirtualCenter von VMware nicht viel mehr als eine schöne Zugabe und kam vor allem beim Management sehr großer Umgebungen zum Einsatz. Auch bei der Nutzung von VMotion hatte die Verwaltungskonsole durchaus ihren Nutzen. Die Funktionen waren aber für die meisten Aufgaben sehr rudimentär. Für den Administrator bestand zwar die Möglichkeit, die Konsole an die eigenen Bedürfnisse anzupassen, der Hersteller ließ hier allerdings nicht viel zu. Eine offene Schnittstelle für eigene Erweiterungen gab es nicht. So musste der Administrator mit unterschiedlichen Konsolen vorlieb nehmen. Für die Administration der Hosts etwa wurde der Anwender auf die Managementkonsole des ESX Servers umgeleitet.

Die aktuelle Version 2.5 der Verwaltungszentrale beschreitet jedoch neue Wege: Tools, die früher parallel zum VirtualCenter gelaufen sind, wie etwa der VMware Converter, sind nun voll in die Konsole integriert. Diese Einbindung geschieht über eine neu implementierte Plug-in-Schnittstelle. Diese gibt dem Administrator die Möglichkeit, dem VirtualCenter zusätzliche Funktionen zur Verfügung zu stellen. Hierbei ist es unerheblich, ob die Erweiterungen das Management der virtuellen Maschinen (VM), der Hosts oder der Cluster betreffen.

Der Vorteil liegt auf der Hand: Zum einen kann sich der Programmierer neuer Features voll auf die eigentlichen Funktionen konzentrieren, ohne eine eigene Oberfläche erdenken zu müssen. Zum anderen können sämtliche Mechanismen, wie etwa die Rechtevergabe, einmalig im VirtualCenter erfolgen und müssen nicht mehrfach in unterschiedlichen Applikationen durchgeführt werden. Auch das Abgreifen der Informationen der virtuellen Landschaft erfolgt nun ausschließlich über die VMware-eigenen Möglichkeiten der Management-Applikation.

Versionskonflikte vermeiden

Eigentlich handelt es sich nicht um eine, sondern um zwei Schnittstellen. Nennen wir sie einfach serverbasierte und clientbasierte Plug-ins. Ein serverbasiertes Plug-in wird direkt über das VirtualCenter installiert. Grundsätzlich hat damit jeder VirtualCenter Client-Benutzer die Möglichkeit, diese Erweiterungen zu installieren und zu nutzen. Der Anwender greift über den Client auf das VirtualCenter zu und findet die serverbasierten Plug-ins unter dem Menüpunkt "Plug-ins \ Manage Plugins". Aus diesem Menü heraus lassen sich die serverbasierten Plug-ins installieren. Die Installationsquellen eines Plug-ins werden vor der Installation automatisch auf das Endgerät kopiert. Anschließend findet die lokale Installation statt.

Leider hat VMware an dieser Stelle nur halbe Arbeit geleistet. Zwar ist mit diesem Mechanismus gewährleistet, dass jeder Administrator, der ein serverbasiertes Plug-in installieren möchte, dieselbe Installationsbasis hat, es findet allerdings keine Ver-

Bild 1: In einem eigenen Menü lassen sich ab Version 2.5 des VirtualCenter Plug-ins aktivieren und verwalten

sionskontrolle statt. Das bedeutet in der Praxis, dass es nach einem Update des VirtualCenter nicht automatisch zu einem Update auf installierte Plug-ins kommt. Auch auf eine Warnung, dass es eine neuere Version der Erweiterung gibt, wartet der Nutzer vergeblich. Hier besteht auf jeden Fall noch Nachholbedarf, denn der Client erfährt eine automatische Aktualisierung. So ist es nicht unwahrscheinlich, dass die Kombination Client zu Plug-in Versionskonflikte aufweist.

Um dies zu vermeiden, müssen Sie lokal auf dem entsprechenden Computer das Plug-in über "Systemsteuerung \ Software" deinstallieren. Erst dann lässt sich anschließend die neue Version des Plug-ins über den VI-Client installieren. Unter dem Menüpunkt "Plugins \ Manage Plugins" im VirtualCenter lassen sich die installierten Module aktivieren. Führen Sie diese Aktion nicht durch, dann ist die Software zwar ordnungsgemäß installiert, Sie können sie aber nicht nutzen.

Die clientbasierten Plug-ins sind Softwarepakete, die sich lediglich lokal auf dem Endgerät installieren lassen. Die Quellen werden nicht zentral vom VirtualCenter-Server zur Verfügung gestellt. In diesem Fall kann es schnell passieren, dass mehrere Administratoren mit unterschiedlichen Softwarerelease-Ständen arbeiten. Unter Umständen kann es dadurch zu unerklärlichen Fehlern kommen. clientbasierte Plug-ins müssen Sie vor der Nutzung ebenfalls aktivieren.

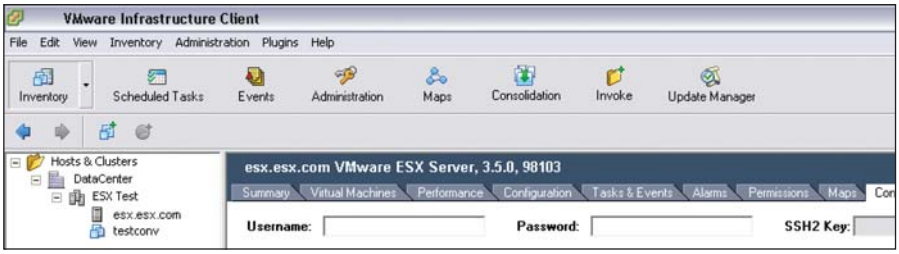


Bild 2: Das "ConsoleClient-Plug-in" erweitert das VirtualCenter um eine SSH-Konsole

Plug-ins von VMware

Die ersten prominenten Mitglieder, die zur Fraktion der Plug-ins gehören, kommen von VMware selbst. Es handelt sich um den "VMware UpdateManager" und den "VMware Converter". Der UpdateManager kam mit der Version 2.5 neu zum VirtualCenter hinzu und übernimmt das Patchen von VMs und Hosts. Das Modul installieren Sie auf einem zentralen Server, es kann auch der VirtualCenter Server selbst sein. Über eine Internetfreischaltung wird es dem Patchserver ermöglicht, automatisch Patches für die Betriebssysteme Linux, Microsoft Windows und VMware ESX Server herunterzuladen. Die benötigte Größe für die zugehörige Patch-Datenbank können Sie über ein Excel-Sheet berechnen, das VMware auf seiner Website zur Verfügung [1] stellt. Der VI-Client verbindet sich über das Plug-in mit dem Patchserver. Das Patchen wird dann über den Client konfiguriert und durchgeführt.

Der VMware Converter dient zur Virtualisierung von physikalischen Servern auf einen einzelnen ESX-Server oder eine Serverfarm. Bei der Übernahme physischer Systeme kopiert das Modul die angeschlossenen Dateisysteme um und kreiert eine neue virtuelle Maschine. Dabei konfiguriert das Tool auch neue einheitliche Treiber.

Wenn Sie eigene Plug-ins programmieren möchten, finden Sie unter [2] eine umfangreiche Anleitung. Ausreichende Programmier- und Englischkenntnisse vorausgesetzt, können Sie sich mit dieser Anleitung oder mit dem VMware-eigenen Leitfaden [3] Ihre persönlichen Erweiterungen maßschneidern.

Eigene Plug-ins erstellen

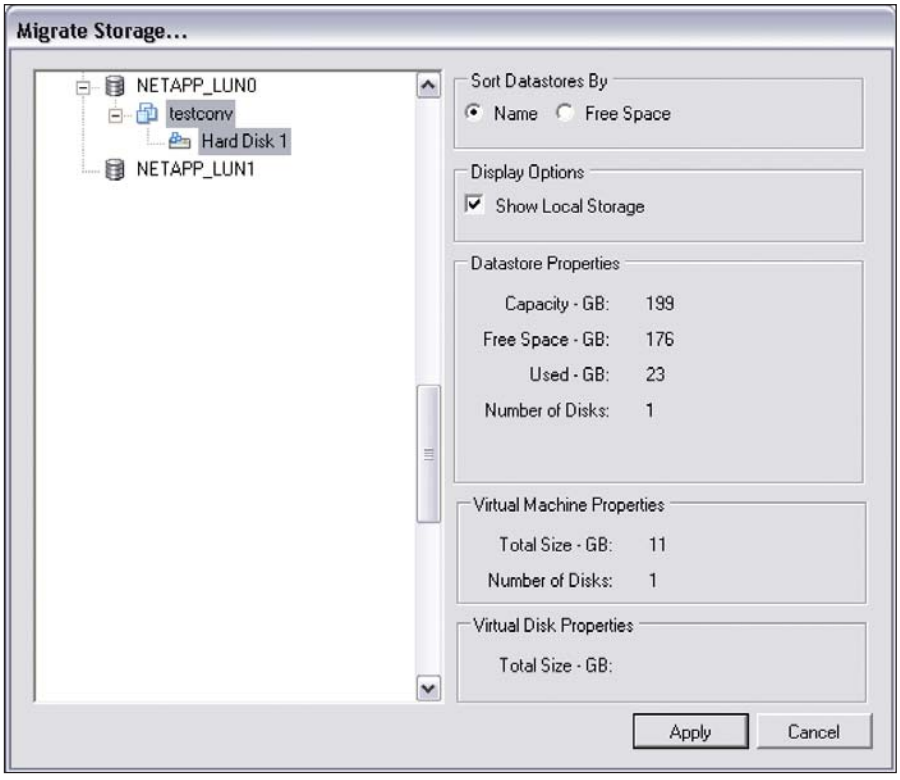


Bild 3: Mit dem "SVMotion-Plug-in" lässt sich Storage einfach und übersichtlich verschieben

Eine Vielzahl kleiner und nützlicher Helfer

Nicht lange nachdem die finale Version des VirtualCenter 2.5 erhältlich war, haben die ersten Programmierer Plug-ins zur Verfügung gestellt, um die Administration von VMware-Komponenten zu erleichtern. Diese nicht von VMware programmierten Plug-ins wollen wir Ihnen näher vorstellen. Einerseits gibt es kleinere Helferlein, die Administrationswege einfach und gut verkürzen. Andererseits existieren auch Erweiterungen, die aufgrund ihrer Komplexität sehr mächtig sind. Allen gemein ist der Gedanke, dass sämtliche Aktionen, die ein Objekt der virtuellen Infrastruktur betreffen, sich im VirtualCenter anstoßen und anzeigen lassen. Alle im Folgenden betrachteten Plug-ins benötigen das .NET Framework 2.0.

SSH-Sitzungen mit dem Console-Plug-in

Viele Konfigurationsanpassungen lassen sich natürlich per Maus in der grafischen Oberfläche des VirtualCenter vornehmen. Rückmeldungen, die Sie beim Absetzen der verschiedenen Konfigurationsbefehle in der Kommandozeile erhalten, erleichtern aber die Fehlersuche. Deshalb pflegen viele Administratoren die ESX-Hosts zusätzlich zum VirtualCenter noch in ein SSH-Tool wie etwa "Putty" ein. Mit noch mehr Komfort arbeiten Sie im VirtualCenter nach Installation und Aktivierung des "ConsoleClient-Plug-ins" von Andrew Kutz. Bei dieser Erweiterung handelt es sich um eine SSH-Konsole, welche die Administration extrem erleichtert. Für die Installation starten Sie einfach die MSI-Datei. Weitere Einstellungen sind nicht notwendig. Das Plug-in ist als freier Download erhältlich [4].

Klicken Sie nun auf einen ESX-Host, zeigt die Verwaltungskonsole in der Übersicht einen zusätzlichen Reiter an. Über "Console" können Sie direkt eine SSH Sitzung auf dem zugehörigen ESX-Host öffnen, um Befehle abzusetzen oder Logs auszuwerten. In die entsprechenden Eingabefelder sind Username und Passwort einzutragen. Über "Connect" öffnen Sie die Sitzung auf dem Host.

Einfaches Storage-Management mit SVMotion

Sicher kennen Sie folgende Situation: Eine VMware-LUN ist aufgrund des starken Wachstums einer VM fast vollgelaufen. Beim Server, der nun verlagert werden soll, sind die Ausfallzeiten so gering wie möglich zu halten. ESX 3.5 hat neben verschiedenen Sicherheits-Patches auch eine neue Funktion namens "Storage VMotion" mitgebracht. Damit lassen sich im laufenden Betrieb die Festplatten einer VM von einer LUN auf eine andere LUN verschieben. Das Interface, das VMware an dieser Stelle mitliefert, ist allerdings mehr als rudimentär. Die Länge des einzugebenden Strings mit den passenden Parametern ist nicht von schlechten Eltern.

Genau an diesem Punkt greift das ebenfalls von Andrew Kutz entwickelte "SVMotionClient-Plug-in" [5]: Es stellt Ihnen eine grafische Oberfläche zur Verlagerung einer virtuellen Maschine im laufenden Betrieb auf eine andere LUN zur Verfügung. Durch ein neues Kontextmenü lässt sich diese Funktion auf sehr einfache Art und Weise aufrufen und das Verschieben der Daten einer VM anstoßen. Die Funktionen sind simpel und verständlich benannt.

Die Installation ist genauso unspektakulär wie die des Console-Plug-ins. Die Voraussetzung für die Nutzung des Erweiterung ist allerdings, dass neben dem .NET Framework auch das Paket "VMware VI Remote CLI" installiert ist [6]. Dieses ermöglicht Ihnen, remote ohne Terminalsitzung Befehle auf einem ESX-Server abzusetzen. Es handelt sich um in Perl geschriebene Skripte, die eine Konfiguration der Hosts vom Admin-Arbeitsplatz zulassen. Eine Befehlsliste mit den zugehörigen Informationen befindet sich unter dem passenden Link in der Linkliste.

An sich sind die einzelnen Konfigurationspunkte des Plug-ins selbsterklärend. Klicken Sie mit der rechten Maustaste auf das Kontextmenü einer VM, dann erhalten Sie den zusätzlichen Menüpunkt "Storage-VMotion". Nach dem Aufruf zeigt die

Bestellen Sie jetzt

das IT-Administrator

Sonderheft II/2008!

180 Seiten Praxis-Know-how

rund um

Exchange 2003/2007

+ Tools-CD

zum Abonnenten-Vorzugspreis* von

nur € 29,90

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

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

administrator
Das Magazin für professionelle System- und Netzwerkadministration

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

☐ **Ja**, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand)_____
und bestelle das IT-Administrator Sonderheft II/2008 inklusive CD zum **Abonnenten-Vorzugspreis** von nur **€ 29,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft II/2008 inklusive CD zum Preis von **€ 34,90** inkl. Versand und 7% MwSt.

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

Ich zahle ☐ per Bankeinzug

Geldinstitut:

Kto.: BLZ:

oder ☐ per Rechnung

Datum:

Unterschrift:

Firma:

Name, Vorname:

Straße:

Land, PLZ, Ort:

Tel:

E-Mail:

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

ITA 0309

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

Administrations-Suite sofort die angewählte VM mit der zugehörigen LUN an. Es besteht die Möglichkeit, die lokalen VMFS-Filesysteme nicht anzeigen zu lassen. Die Liste der LUNs können Sie nach Plattenplatz oder alphabetisch sortieren. Nach dem Markieren der VM samt VMDK-Files und Konfigurationsdatei können Sie das System mit der Maus einfach auf eine andere LUN verschieben. Nach dem Betätigen des "OK"-Buttons beginnt der Transfer der gesamten VM-Konfiguration auf die neue Ziel-LUN und Sie können den Vorgang im Statusfenster verfolgen.

Dieses Modul bietet auf einfache Weise die Möglichkeit, LUNs zu bereinigen oder Systeme zu verschieben, weil eine VM zu stark gewachsen ist und der zur Verfügung stehende freie Plattenplatz nicht mehr ausreicht. Es kann allerdings beim Aufruf des VirtualCenter die Fehlermeldung erscheinen, dass das SVMotion-Plug-in nicht aktiviert werden kann. Dieses Problem tritt dann auf, wenn im Internet Explorer ein Proxy eingestellt ist. Nach dessen Deaktivierung funktioniert alles einwandfrei. Auch diese Erweiterung steht kostenfrei zur Verfügung.

Rescan auf den HostBus-Adapter automatisieren

Stellen Sie einer VMware-Farm eine neue LUN zur Verfügung, geht die Handarbeit unmittelbar danach erst richtig los. Mit dem SSH-Client muss auf allen betroffenen ESX-Hosts ein Rescan auf die HostBus Adapter (HBA) durchgeführt werden. Die Firma icomasoft stellt zur Automatisierung dieses Vorgangs das kleine, aber feine Plug-in "VI Rescan" [7] zur Verfügung, das dem Administrator viel Arbeit abnimmt.

Durch den Aufruf des Tools über das Kontextmenü kommt es automatisch zu einem Rescan auf die HostBus-Adapter der betroffenen Hosts. Der Administrator muss sich so beim Einbinden oder Abmelden von LUNs nicht durch die Managementkonsole oder die Kommandozeile der Service Console der einzelnen ESX-Server wühlen, um den Rescan auf allen Systemen durchzuführen. Die Aktion lässt sich auf einen Host oder eine Gruppe von Hosts anwenden.

Nach dem freien Download der Software folgt die sehr einfache Installation. Während des Installationsdialogs gibt es die Möglichkeit, das Plug-in direkt zu aktivieren, sodass Sie es sofort nutzen können. Der VI-Client sollte geschlossen sein beziehungsweise nach der Installation neu gestartet werden. Die Software selbst wird in das Standardverzeichnis für Plug-ins unter "{ProgramFiles} \ VMware \ Infrastructure \ Virtual Infrastructure Client \ Plugins" installiert. Das Plug-in ist clientbasiert und steht daher nicht über den VirtualCenter Server zur Verfügung.

Arbeitstier VI PowerScripter

Von allen hier vorgestellten Plug-ins ist "VI PowerScripter" [8] von icomasoft die mit Abstand umfangreichste Erweiterung. Der Administrator hat – PowerShell Kenntnisse vorausgesetzt – hier die Möglichkeit, selbst Module für das VirtualCenter zu programmieren, wenn ihm der Umfang der mitgelieferten Skripte nicht ausreicht, egal ob das Management angepasst werden soll oder ob Aufgaben zu automatisieren sind. Auch Auswertungen über die Auslastung der virtuellen Infrastruktur sind ohne Probleme möglich. Muss der Administrator Daten für das Billing zur Verfügung stellen, dann ist dies mit einem passenden Shell-Skript überhaupt kein Problem. Alle Daten, die in der VirtualCenter-Datenbank liegen, sind für den Administrator zugänglich. Beim Reporting sind Sie nicht auf die eingeschränkten Ausgaben des VirtualCenter angewiesen.

Grundsätzlich haben Sie mit diesem Plug-in die Möglichkeit, PowerShell-Skripte für die Administration von Komponenten der virtuellen Infrastruktur zu nutzen. Die Skripte lassen sich nicht nur auf ein Objekt, sondern gleichzeitig auf mehrere Objekte anwenden. Unterschieden wird zwischen Skripten für die Administration von Host- und DataCenter-Objekten beziehungsweise für die Administration von virtuellen Maschinen.

Wenn Sie etwa kontrollieren möchten, welche VMs in einer Farm ein verbundenes CD-ROM Laufwerk haben, können Sie dies mit dem Aufruf des passenden Skripts ohne Probleme mit wenig Aufwand durchführen. Auch zur Erstellung eines neuen VLANs in einer Serverfarm ist nur noch ein Aufruf nötig. Mit einem einfachen PowerShell-Skript richten Sie das Netzwerk auf allen betroffenen Hosts ein. Die Anwendungsmöglichkeiten sind nur durch die Fantasie und die Programmierfähigkeiten des Administrators eingeschränkt.

Der VI PowerScripter Professional ist zum Preis von 285 Euro beim Hersteller icomasoft erhältlich. Eine auf 15 Tage begrenzte Vollversion lässt sich auf der Hersteller-Website herunterladen.

Installation richtig durchführen

Die Installation des PowerScripter-Plug-ins läuft nur dann einwandfrei durch, wenn alle Software-Voraussetzungen erfüllt sind. Diese werden durch die Setuproutine überprüft. Zur Erfüllung dieser Vorgaben benötigen Sie die Microsoft PowerShell V1. Bei Windows 2008 Server ist sie bereits Bestandteil des Betriebssystems. Kommt

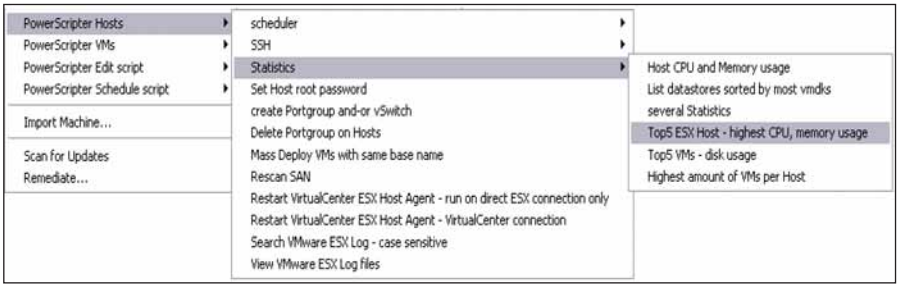


Bild 4: Das Kontextmenü des "PowerScripter" ermöglicht das Erstellen umfangreicher Statistiken

eine andere Windows-Version zum Einsatz, sollten Sie die passende PowerShell-Version bei Microsoft herunterladen [9]. Weiterhin müssen Sie Microsofts .NET Framework 2.0 aufspielen [10] und das VMware Infrastructure Toolkit 1.0 [11] darf ebenso nicht fehlen.

Abschließend benötigen Sie noch die PowerGUI [12], falls Sie die Skripte direkt im VI-Client editieren möchten. Bei der PowerGUI handelt es sich um eine grafische Oberfläche zur Erstellung von PowerShell-Skripten. All diese Bestandteile sind kostenfrei verfügbar. Wollen Sie grafische Auswertungen erstellen, wie etwa Auslastungs-Diagramme oder die Verteilung von Plattenplatz, können Sie diese ganz simpel mit dem kostenpflichtigen Zusatz "PowerGadgets" [13] in die Skripte einarbeiten.

Der VI-Client muss mindestens in Version 2.5 oder höher installiert sein. Auf die Installation der benötigten Softwarepakete gehen wir an dieser Stelle nicht weiter ein. Der aktuelle VI-Client lässt sich direkt vom VirtualCenter Server herunterladen. Ein Aufruf von "http://{VirtualCenter Servername}" zeigt eine Webseite an, über die sich der Download durchführen lässt. Ist der Webservice des VirtualCenter deaktiviert, können Sie sich den Client direkt vom ESX-Server herunterladen. Dazu rufen Sie die URL "http://{ESX Servername}" auf oder Sie greifen direkt auf die VirtualCenter-Installations-CD zurück.

Wie schon beim SVMotion-Plug-in funktioniert der PowerScripter nur, wenn der Proxy-Eintrag im Internet Explorer deaktiviert ist. Dies ist eine Einschränkung, die in einer der nächsten VI Toolkit-Versionen behoben werden soll. Nach der Installation der PowerShell müssen Sie die Execution Policy der PowerShell auf "Remote-Signed" setzen.

Vor der Installation des Plug-ins sollte der VI-Client geschlossen werden. Alle Voraussetzungen für die Installation werden dann sorgfältig geprüft. Während der Installation haben Sie die Möglichkeit, die sofortige Aktivierung der Erweiterung zu veranlassen. Andere Einstellungen lassen sich nicht vornehmen. Auch hier gilt es vorher, den Client zu schließen oder ihn nach der Installation neu zu starten. Wurde die automatische Aktivierung des Plug-ins deaktiviert, ist dies nachträglich unter dem Menüpunkt "Plugins \ ManagePlug-ins \ Installed" möglich.

Die Installation des Schedulers erfordert etwas mehr Konfigurationsaufwand. Sie müssen entscheiden, in welchem Pfad Sie die Software installieren wollen und ob alle lokalen Anwender die Software nutzen dürfen oder nur ein Nutzer. Das folgende Eingabefenster fordert Sie dazu auf, den FQDN beziehungsweise die IP-Adresse des VirtualCenter-Servers einzugeben. Der Standardwert für den Timeout steht auf 60 Sekunden und sollte so belassen werden. Nach der Bestätigung müssen Sie einen gültigen Account für das VirtualCenter eingeben. Nach der Verifikation durch die Installationsroutine wird eine Erfolgsmeldung für diesen Vorgang angezeigt. Abschließend legen Sie noch einen Account fest, mit dem der Scheduler-Service gestartet werden soll. Die Rechte des eingetragenen Users legen fest, in welchem Kontext die Tasks im VirtualCenter ausgeführt werden, unabhängig davon, mit welchem Account Sie am VirtualCenter angemeldet sind.

Nach dem Abschluss der Installationsarbeiten ist auf dem Administrations-PC ein neuer Dienst installiert, der mit dem VirtualCenter kommuniziert und die erstellten Tasks dort platziert.

PowerScripter individuell konfigurieren

Damit Sie ein Gefühl für den Aufwand der Erstellung von Skripten bekommen, listen wir im Folgenden ein Beispielskript, das bei dem Plug-in dabei ist. Für den Rescan der HostBusAdapter aller ausgewählten ESX-Server genügt folgendes Skript:

```
$_ | Get-VMHostStorage -RescanAllHBA
$_ | Get-VMHostStorage -Refresh
```

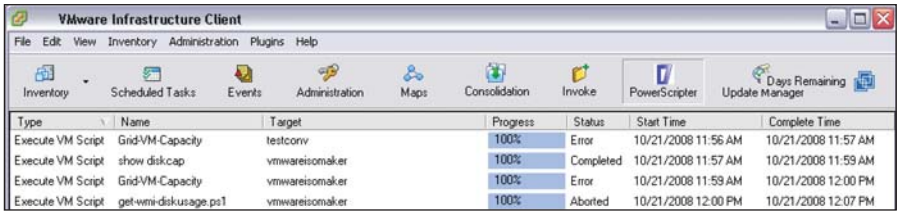


Bild 5: Eine Statusanzeige informiert über die mit dem "PowerScripter" gestarteten Skripte

Ein um ein Vielfaches geringerer Aufwand, als wenn Sie diese Aktion über die Service Console oder etwa über das VirtualCenter vornehmen würden. Somit gibt es nun eine einzige Umgebung, in der Sie die Administration der Landschaft für sämtliche Routineaufgaben vornehmen können. Es ist nicht mehr notwendig, zur Verwaltung der Hosts oder VMs Befehle in der Service Console abzusetzen.

Die PowerShell nutzt Librarys, die die verschiedenen Befehle zur Verfügung stellen. In der Sprache der PowerShell werden diese Dateien "Cmdlets" genannt. Das VMware VI Toolkit enthält die Befehle, die Sie in den Skripten zur Administration der virtuellen Umgebung nutzen können. Zwischen Groß- und Kleinschreibung wird dabei nicht unterschieden. Starten Sie die Ausführung eines Skripts, so wird dieses im Kontext des angemeldeten VI Client-Anwenders ausgeführt.

Das Menü des PowerScripters ist weitestgehend selbsterklärend, außer dem Handbuch findet sich dort der "Tip of the day" und die Möglichkeit, nach aktuellen Updates suchen zu lassen. Der erste Punkt gibt Ihnen die Möglichkeit, Ihre Skripte menügesteuert zu verwalten. Das Löschen von Skripten aus dem Repository ist hier ebenso möglich wie ein Import von neuen Dateien. Sollten Sie nicht das Kontextmenü direkt in der Oberfläche des VI-Clients nutzen, dann besteht die Möglichkeit, über diesen Menüpunkt einen Scheduled Job aufzusetzen. Dazu jedoch später mehr.

In Abhängigkeit der Ablage der Skriptdateien kommt es zu einer Anpassung des Kontextmenüs. Grundsätzlich liegen die Skripte unter "{ProgramFiles} \VMware\ Infrastructure \Virtual Infrastructure Client\ Plugins \ icomasoft PowerScripter \". Es existieren hier zwei Unterverzeichnisse, eines für Host-Skripte ("HostScripts") und eines für Skripte für virtuelle Maschinen ("VmScripts"). Ist in einem der genannten Unterordner ein Verzeichnis angelegt, wird dieses als Untermenüpunkt im Kontextmenü dargestellt. Sie können so auf einfache Art und Weise Ihr eigenes Repository anlegen.

Besteht der Bedarf, dass alle Admins auf identische Skripte zugreifen sollen, gibt es die Möglichkeit, das Skript-Verzeichnis vom lokalen Standardpfad auf ein Netzlaufwerk zu verlegen. Dies geschieht über eine Anpassung in der Konfigurationsdatei des Plug-ins. Die Datei *PowerScripter.dll.config* müssen Sie im Abschnitt "paths" auf den neuen Pfad anpassen. Die Übernahme der Konfiguration erfolgt über das Deaktivieren und das erneute Aktivieren des PowerScripter-Plug-ins. Diese Aktion ist bei jeder Konfigurationsänderung vorzunehmen.

Viele Administratoren nutzen die PowerGUI von Quest. Auch deren Dateiformat PowerPack wird hier unterstützt. Die Powerpack-Dateien werden automatisch als Unterverzeichnis dargestellt. Somit lassen sich die Menüs strukturiert und übersichtlich aufbauen. Das Plug-in bringt von Haus aus schon eine Reihe von Skripten mit.

Aufrufen der Skripte

Es gibt verschiedene Möglichkeiten, die Skripte aufzurufen. Entweder Sie wählen ein Objekt direkt aus oder Sie nehmen eine Mehrfachauswahl vor und wenden anschließend das PowerShell-Skript auf die markierten Objekte an. Selbstverständlich können Sie Skripte zudem auf übergeordnete Objekte anwenden. Diese Auswahl schließt natürlich die untergeordneten Host- beziehungsweise VM-Objekte bei der Ausführung mit ein.

Nachdem Sie die Elemente markiert haben, öffnen Sie mit der Maustaste das Kontextmenü und wählen den passenden Menüpunkt aus. Die direkte Ausführung der Skripte stoßen Sie über die ersten beiden Menüpunkte an. Unterschieden wird hier, wie bereits beschrieben, zwischen hostbasierten und VM-basierten Skripten. Wählen Sie den Editierungsmodus, dann öffnet sich automatisch die PowerGUI und bietet die Möglichkeit der Änderung des ausgewählten Skripts. Der letzte PowerScripter-Menüpunkt erzeugt einen zeitgesteuerten Task für die Ausführung des angewählten Skripts. Zu sehen ist der Task dann in dem Reiter des Hosts oder der VM im VirtualCenter.

Ist ein Skript manuell gestartet, werden die Skriptläufe angezeigt. Dazu klicken Sie in der "Main Toolbar" des Clients auf das Icon für den PowerScripter. Es öffnet sich ein Übersichtsfenster, in dem dessen Aktionen dargestellt werden. Alle Skriptläufe werden hier dokumentiert, zusätzlich gibt es die Möglichkeit, laufende Skripte abzubrechen. Zeitgesteuerte Skripte werden als Scheduled Tasks in den Events angezeigt.

Die Anwendungsmöglichkeiten zur Erstellung von Skripten sind nur durch die Funktionen beschränkt, die das VI Toolkit von VMware zur Verfügung stellt. Der VI PowerScripter Professional bringt einen Scheduler mit zur zeitgesteuerten Ausführung von Skripten. Alles bindet sich nahtlos in das VirtualCenter ein. Im Softwarepaket sind bereits eine Reihe von vorgefertigten Skripten und SSH-Cmdlets für die Interaktion mit SSH-fähigen Applikationen enthalten. Die Pflege der Berechtigungen für den PowerScripter wird an bekannter Stelle im VirtualCenter vorgenommen. Damit erhöht sich die Sicherheit, weil getrennte Anmeldungen entfallen.

Fazit

Mit der Plug-in-Schnittstelle, die im VirtualCenter Server ab Version 2.5 enthalten ist, hat VMware einen riesigen Schritt zur individuellen Anpassung und Individualisierung des VI-Clients gemacht. Die bis jetzt erhältlichen Plug-ins lassen nur erahnen, welche Möglichkeiten sich dem Admin bieten, um Aufgaben schneller und effektiver durchführen zu können. Vor allem mit dem VI PowerScripter Plug-in können Sie selbst eigene Anpassungen durchführen, ohne ein begnadeter Programmierer zu sein. Wie immer ist aber Vorsicht geboten, bevor Sie die selbst erstellten Skripte auf Produktivumgebungen loslassen. Entsprechende Testläufe ersparen Ihnen hier böse Anrufe und kurze Nächte. *(ln)*

Links

[1] Excelsheet DB Größe UpdateMananger
www.vmware.com/support/vi3/doc/vi3_vum_10_sizing_estimator.xls

[2] Programmieranweisung Plug-ins fürs VirtualCenter von Andrew Kutz
http://akutz.files.wordpress.com/2008/05/vi3progplugin-rev13.pdf

[3] Programmieranweisung Plug-ins fürs VirtualCenter von VMware
www.vmware.com/support/developer/vc-sdk/vcplugin-exp/

[4] Console Plug-in von Andrew Kutz
http://akutz.googlecode.com/files/ConsoleClientSetup-0.1.5.msi

[5] SVMotion Plug-in von Andrew Kutz
http://akutz.wordpress.com/tag/svmotion/

[6] VMware VI Remote CLI
www.vmware.com/go/remotecli

[7] VI Rescan Plug-in
www.icomasoft.com/de/produkte/rescan-plugin.html

[8] VI PowerScripter Plug-in
http://www.icomasoft.com/de/produkte/vi-powerscripter.html

[9] Microsoft PowerShell
www.microsoft.com/windowsserver2003/technologies/management/powershell/download.mspx

[10] Microsoft .NET Framework
www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5

[11] Vmware VI Toolkit
http://blogs.vmware.com/vipowershell/

[12] PowerGUI
http://powergui.org/downloads.jspa

[13] PowerGadgets
www.softwarefx.com/sfxSqlProducts/powergadgets/

Apple-Systeme vom Netz booten

So zähmen Sie Panther und Tiger

von Andreas Roscher

Quelle: Eric Isselée / Sean Gladwell - Fotolia.com

Die Installation eines Apple-Systems ist einfach. Wer mehr als ein System zu managen hat, kann sich auf Tools aus dem Apple-Umfeld einlassen. Hinter den Kulissen agiert aber ein fast normales Unix, welches sich auch ohne Spezialwerkzeuge und sogar mithilfe eines Linux-Servers sicher vom Netz booten lässt. Wie das geht und welche Kniffe Sie dabei beachten müssen, zeigen wir Ihnen in diesem Workshop.

Warum das Booten vom Netz zum guten Ton eines jeden Betriebssystems gehören sollte, ist einleuchtend. Es verursacht schlicht wesentlich weniger Aufwand, wenn ein Computer vom Netz bootet und Sie ihn aus der Ferne sicher bespielen, reparieren oder administrieren können. Nicht ganz einfach macht dies allerdings die Tatsache, dass Apple mittlerweile mehr als eine Prozessorsorte im Angebot hat und zudem die Verwendung verschiedener Versionen von Mac OS X erzwingt. Ältere Computer wie etwa das iBookG4 haben gar keine Chance, auf das "Leopard" genannte aktuelle Mac OS X 10.5 zurückzugreifen. Im Kasten "Verwendete Macs" haben wir die für diesen Workshop verwendeten Rechner aufgeführt.

Beim Netzwerk-Boot in Apple-Umgebungen kommen diverse Dateien zum Einsatz. Damit alle Experimente gefahrlos ablaufen, erstellen wir die Bootdateien mithilfe einer externen Firewire-Festplatte. Dadurch stehen immer zwei Installationen zur Verfügung. Eine Installation befindet sich auf der internen Festplatte und hat das System zum Inhalt, wie es die Installationsprozedur von Mac OS X hervorbringt. Auf diese interne Installation soll nach dem anvisierten Booten vom Netz der Fernzugriff möglich sein.

Die Installation auf der externen Festplatte dient der Erstellung der notwendigen Bootdateien und wird minimalistisch ausgelegt. Aufgrund der unterschiedlichen Partitionierungs-Schemata zwischen Intel- und Power-PC-Macs können Sie entweder Leopard oder Tiger auf der externen Festplatte installieren. Beides nebeneinander geht nicht. Um den Fernzugriff abzusichern, müssen wir uns am Anfang ein wenig damit befassen, wie die Installation auf der externen Festplatte aussehen sollte. Diese Regeln lassen sich auch für die Installation auf der internen Festplatte anwenden, um maximale Unix-Administrationserfolge zu erzielen.

Doppelt gemoppelt: Interne und externe OS-Installation

Um Mac OS X als Unix-System zu begreifen, ist der erste Schritt nach der Installation die Freigabe der Kennung "root" zum Login und die Aktivierung des Login-Fensters. Funktioniert das Login des lokalen Benutzers einmal nicht, können Sie sofort auf die Kennung Root ausweichen, um den Schaden zu beheben. Im Finder erreichen Sie über "Programme / Dienstprogramme" die Anwendung "Terminal" und kommen so auf den Unix-Prompt. Zuerst bekommt die Kennung Root ein Passwort:

```
sudo passwd Root
```

Wollen Sie sich direkt als Root anmelden, muss es nach dem Booten ein Anmeldefenster geben. Über "Systemeinstellungen/ Benutzer / Anmeldeoptionen" stellen Sie das Anmeldefenster auf "Name / Kennwort" und der Haken bei "Automatisch anmelden als" entfällt beziehungsweise wird beim Leopard auf "Deaktiviert" umgestellt. Möchten Sie im Terminalfenster nur schnell mal Root werden, erfolgt das mit dem Kommando "su" unter dem Leopard sofort, da der beim Installieren ange-

Mac OS	Version	Prozessor	Computer
Panther	Mac OS 10.3	PowerPC	iBookG4
Tiger	Mac OS 10.4	PowerPC	iBookG4
Leopard	Mac OS 10.5.4	Intel	Mac mini

Verwendete Macs

Bild 1: Die Minimalinstallation auf der externen Platte wird nur zum Booten des Systems verwendet

legte Benutzer ein Mitglied der Gruppe "admin" ist. Unter Tiger ist das Kommando "su" nur für Mitglieder der Gruppe "wheels" zugänglich. Wir nennen unseren Benutzer "oma". Mit dem folgenden Kommando kommt die Oma auch bei Tiger und Panther noch unter die Räder – erhält also Root-Rechte:

```
sudo niutil -createprop .
  /groups/wheel root oma
```

Nun kann der Anwender nach dem nächsten Systemstart direkt auf den Root-Prompt wechseln und das nervende "sudo" vor jedem Systemkommando entfällt.

```
su -
```

Bei der Installation auf der internen Platte sollten Sie keine Abstriche machen. Da ein Unix ohne C-Compiler kein Unix ist, kommt das Paket *Developer.mpkg* von der Xcode Tools-CD in jedem Fall noch dazu und auch das X-Window-System sollte sich im Boot finden. Um das Booten vom Netz zu lernen, wird die Installation in minimaler Form auf einem 10 GByte umfassenden Plattenstück auf einer externen Firewire-Platte wiederholt. Minimalistisch bedeutet, alles abzuwählen, was sich abwählen lässt (Sprachen, Drucker, X-Window und so weiter). So lässt sich der Platzbedarf einer Tiger-Installation wenigstens auf 2 GByte begrenzen. Beim Leopard erfordert die Minimalinstallation 6 GByte Plattenplatz. Über "Systemeinstellungen / Startvolume" legen Sie die Installation auf der externen Platte als Startvolume fest (Bild 1). Als Ergebnis bootet der Computer von der externen Platte, wenn diese beim Booten bereits eingeschaltet ist. Ist dies nicht der Fall, bootet der Mac von der internen Platte. Das funktioniert für den iBookG4 und für den Mac mini gleichermaßen. Damit alle Bootvorgänge auch sichtbar werden, stellen Sie final noch den Verbose-Modus für das Booten ein:

```
nvram boot-args="-v"
```

Nun haben Sie zwei bootbare Systeme, die sich von außen nicht erreichen lassen, da alle Netzwerkdienste abgeschaltet sind. Das ändert sich nach dem Einschalten des SSH-Serverdienstes. Dazu müssen Sie Root sein:

```
service ssh start
```

Nun sollten Sie sich auch von außerhalb mit der Kennung Root per SSH anmelden können. Für den Fall späterer Irrtümer ist dieser SSH-Zugang überlebenswichtig.

Bootdateien erstellen

Das Booten eines Macs vom Netz erfordert immer vier Dateien:
- Loader-Datei
- Kernel-Datei
- Kernel-Extensions-Datei
- Root-Image-Datei

Die Regeln für die Dateinamen sind unterschiedlich. Nur bei der Loader- und der Root-Image-Datei haben Sie die freie Wahl des Dateinamens, da Sie beide Namen beim DHCP-Serverdienst hinterlegen können. Die Namen der Kernel-Datei und der Kernel-Extensions-Datei sind in der Loader-Datei fest verdrahtet. Loader-, Kernel- und Kernel-Extensions-Datei müssen im Datenverzeichnis des TFTP-Serverdienstes (Trivial File Transfer Protocol) vorhanden sein. Im Fall unseres Linux-Systems ist es das Verzeichnis "tftpboot". Um das iBookG4 mit Tiger zu booten, sind folgende Dateien erforderlich:
- */tftpboot/macosx.tiger.ppc*
- */tftpboot/mach.macosx* und
- */tftpboot/mach.macosx.mkext*

Die Dateien zum Booten des iBookG4 lassen sich mithilfe des Tiger-Systems auf der internen Platte erstellen:

```
mkdir /tftpboot
cd /tftpboot
cp /usr/standalone/ppc/bootx.bootin-
  fo macosx.tiger.ppc
cp /mach_kernel mach.macosx
kextcache -a ppc -s -l -n -z -m
  mach.macosx.mkext/System/Library/
  Extensions
```

Um den Mac mini mit dem Leopard zu booten, sind die folgenden Dateien erforderlich:
- */tftpboot/macosx.leopard.i386*
- */tftpboot/mach.macosx* und
- */tftpboot/mach.macosx.mkext*

Die Dateien zum Booten des Mac mini lassen sich mithilfe des Leopard-Systems auf der internen Platte erstellen:

```
mkdir /tftpboot
cd /tftpboot
cp /usr/standalone/i386/boot.efi
  macosx.leopard.i386
cp /mach_kernel mach.macosx
kextcache -a i386 -s -l -n -z -m
  i386.macosx.mkext/System/Library/
  Extensions
```

Die Dateien *mach.macosx* und *mach.macosx.mkext* sind namentlich bei Panther, Tiger oder Leopard immer gleich, müssen aber je nachdem, welcher Kernel gebootet werden soll, völlig verschiedene Inhalte haben. Aktuell können Sie somit immer nur eine Reihe von Macs mit einer Mac-Version vom Netz booten. Ein Mischbetrieb wür-

de von Apple die Intelligenz erfordern, in den Loader-Programmen abweichende Dateinamen für die Kernel-Datei und die Kernel-Extensions-Datei zu verwenden. Schlaue Lösungen zum automatisierten Booten der Macs tauschen die Bootdateien dynamisch aus. So können Sie einmal einen Schulungsraum mit Intel-Macs booten und bespielen, während zu einem anderen Zeitpunkt ein Schulungsraum mit Power-PC-Macs an der Reihe ist.

Bootserver einrichten

Auf dem Linux-Bootserver kommen die Dateien in das Verzeichnis "tftpboot" und erhalten die passenden Rechte:

```
chmod 755 /tftpboot
chmod 444 /tftpboot/*
```

In diesem Zusammenhang sollten Sie auch wissen, wie Sie Linux dazu bringen, die Rolle eines TFTP- und eines DHCP-Servers zu spielen. Dazu ist die Datei */etc/dhcp3/dhcpd.conf* mit den richtigen Einträgen zu füttern, damit das Booten per DHCP vom Netz funktioniert. Für den Client "ibookg4" sieht der passende Eintrag folgendermaßen aus:

```
host ibookg4 {
hardware ethernet 00:0a:95:bc:f9:40
  ;
fixed-address ibookg4 ;
option host-name "ibookg4" ;
option subnet-mask 255.0.0.0 ;
option routers 10.1.1.31 ;
option root-path
  "nfs:10.1.1.31:/home/img.nfsroot/
  macosx.tiger.ppc:macosx.dmg" ;
filename "macosx.tiger.ppc" ; }
```

Der Eintrag root-path verweist auf die Datei *macosx.dmg*, die sich laut DHCP-Eintrag im Verzeichnis */home/img.nfsroot/macosx.tiger.ppc* befinden muss. Damit Sie auf diese noch zu erzeugende Datei zugreifen können, muss das verwendete Verzeichnis auch beim NFS-Serverdienst (Network File System) freigegeben sein. In unserem Fall hat die Datei */etc/exports* den passenden Eintrag:

```
/home/img.nfsroot
  *(rw,no_root_squash,no_all_squash,
  insecure)
```

Für den Mac mini weicht der Eintrag im DHCP-Server nur geringfügig ab:

```
host macmini {
hardware ethernet 00:1f:f3:46:4a:9d
  ;
fixed-address macmini ;
option host-name "macmini" ;
option subnet-mask 255.0.0.0 ;
option routers 10.1.1.31 ;
option root-path
  "nfs:10.1.1.31:/home/img.nfsroot/
  macosx.leopard.i386:macosx.dmg" ;
filename "macosx.leopard.i386" ; }
```

Die Verwendung einer IP-Adresse für den NFS-Server ist im DHCP-Eintrag bei der Option "root-path" Pflicht. Stimmen alle Einträge und laufen die Dienste DHCP, TFTP und NFS, können wir uns der Erstellung der Datei *macosx.dmg* zuwenden. Benötigt wird eine Datei *macosx.dmg*, die auf das Tiger-OS zugeschnitten ist, und eine Datei *macosx.dmg*, mit der Leopard zurechtkommt. Wenn Sie das Booten vom Netz versuchen und es gibt noch keine Datei *macosx.dmg*, endet Mac OS X in einer Kernel Panic. Das Erstellen der Datei *macosx.dmg* erfolgt mit dem Kommando "hdiutil". Dazu booten Sie den Mac bei ausgeschalteter externer Festplatte. Das Mac OS X von der internen Festplatte fährt hoch. Nach einer Anmeldung als Root schalten Sie die externe Festplatte ein. Das Einhängen der Partitionen der externen Platte erfolgt automatisch. Da in unserem Fall die Mac OS X-Installationen auf der externen Platte immer unter dem Verzeichnis "/Volumes/OMAmpartition" auftauchen und wir unter "/var" auf dem iBookG4 und dem Mac mini noch genug Platz für die Datei *macosx.dmg* haben, ist das folgende Kommando zum Erstellen der Datei korrekt:

```
hdiutil create -fs HFS+ -srcfolder
  /Volumes/OMAmpartition /var/
  macosx.dmg
```

Die Datei für den Tiger kommt auf 1 GByte. Die Datei für den Leopard bringt es auf 3 GByte. Das Programm "hdiutil" formatiert in der Datei *macosx.dmg* das gewünschte Dateisystem (HFS+), um alle Daten aus dem Verzeichnis "/Volumes/OMAmpartition" dort abzulegen. Da der Mac OS X-Kernel beim späteren Zugriff auf die Datei *macosx.dmg* nur ausgewählte Dateisysteme akzeptiert, ist auch klar, warum die Dateien nicht ausgepackt auf dem NFS-Server liegen dürfen. Mit der Datei *macosx.dmg* steht ein root-Dateisystem zur Verfügung, auf das der Kernel nach dem Booten vom Netz per NFS-Protokoll zugreifen kann, sobald Sie die Datei auf dem Linux-Server richtig platziert haben. Ist etwas am Inhalt der Datei faul, kommt es beim Booten vom Netz zu den im Kasten "Kernel Panic" beschriebenen Fehlermeldungen.

Mit der Datei *macosx.dmg* für den Leopard haben wir uns die beschriebene Kernel Panic eingehandelt. Um sicher zu sein, dass es nur an dieser Datei liegt, schieben wir dem Mac mini einfach die gleichnamige Datei des Tiger-Systems unter. Wie erwartet, kann der Leopard-Kernel in die nur 1 GByte große Datei des Tigers hineingreifen und hängt sich erst dann mit der folgenden Fehlermeldung auf, wenn es zum Aufruf des nicht

```
netboot: retrieving IP information from DHCP
   response
netboot: IP address 10.1.1.225 netmask 255.0.0.0
   router 10.1.1.3
netboot: retrieving root path from BSDP response
Server 10.1.1.31
Mount /home/img.nfsroot/macosx.leopard.i386
Image /macosx.dmg
root on 10.1.1.31:/home/img.nfsroot/
   macosx.leopard.i386
netboot_setup: calling di_root_image
IOHDIXController: NOTE: administrator is creating
   non-ejectable disk image
IOHDIXController::setProperty(di-root-image, /
   macosx.dmg) failed
netboot_setup: di_root_image: failed 107
panic(): bsd_init: NetBoot could not find root,
   107:
panic(): /SourceCache/xnu/xnu-
   1228.5/bsd/kern/bsd_init.c:820
```

Kernel Panic

Schmidt's LoginInventory

keep IT simple

www.loginventory.com

für den Intel-Mac kompilierten Programms */sbin/launchd* kommt:

```
netboot_setup: calling di_root_image
IOHDIXController: NOTE: administra-
  tor is creating non-ejectable disk
  image
netboot: root device 0xe000005
panic(): "Process 1 exec of
  /sbin/launchd failed,
panic(): /SourceCache/xnu/xnu-
  1228.5.20/bsd/kern/kern_exec.c:
  2885
```

Es gilt also zu prüfen, was an der Datei *macosx.dmg* für den Leopard nicht stimmt. Niemals sollten Sie vergessen, die verwendete NFS-Freigabe zu überprüfen. So stellt sich hier schnell heraus, dass der etwas ältere NFS-Server auf dem Linux-System der Schuldige ist:

```
mount -t nfs
  anne:/home/img.nfsroot/macosx.
  leopard.i386 /mnt
dd if=/mnt/macosx.dmg of=/dev/null
dd: opening `/mnt/macosx.dmg': In-
  put/output error
dd if=/home/img.nfsroot/macosx.
  leopard.i386/macosx.dmg
  of=/dev/null
6609587+1 records in
6609587+1 records out
```

Wenn wir die Datei *macosx.dmg* durch die NFS-Brille betrachten, scheint es ein Größenproblem zu geben. Also verlegen wir die Datei kurzerhand auf einen PC unter Solaris 10 x86 (und befassen uns später mit der Suche nach einem aktuelleren Linux):

```
mount -t nfs
  book2:/home/img.nfsroot/macosx.
  leopard.i386 /mnt
dd if=/mnt/macosx.dmg of=/dev/null
6609587+1 records in
6609587+1 records out
```

Nun klappt die Sache offensichtlich. Die erstellte Datei *macosx.dmg* für den Leopard ist wie erwartet fehlerfrei. Sie darf nur nicht unter einem veralteten NFS-Server abgelegt werden. Gut zu wissen, dass selbst bei neuen Linux-Systemen nur der im Kernel platzierte NFS-Server die großen Dateien wirklich mit an Bord hat. Ein falscher Kernel, ein fehlendes Modul oder die Installation des im User-Space laufenden NFS-Servers drücken ein aktuelles Linux beim NFS wieder unter die 2-GByte-Grenze.

Booten vom Netz

Das Booten vom Netz müssen Sie einmalig auf den Mac-Clients einschalten. Um das Booten vom Netz beim Mac mini einzuschalten, müssen Sie mithilfe des installierten Systems das Netzwerk als Startvolume festlegen. Gibt es die beim DHCP-Server eingetragene Loader-Datei *macosx.leopard.i386*, wird das Booten vom Netz ausgeführt. Existiert diese Datei nicht, erfolgt der Startvorgang von einer eventuell eingelegten bootbaren DVD oder von Festplatte. Wer den Netzwerkstart nicht mit einem Mausklick aktivieren will, kann mit dem Kommando "nvram" zuschlagen. Der einzeilige Kommandoaufruf für den Mac mini ist nachfolgend der Übersicht halber mehrzeilig dargestellt. Um alles zu sehen, aktivieren Sie auch hier noch einmal den Verbose-Modus:

```
nvram efi-boot-device=
"<array>
<dict>
<key>BLMACAddress</key>
<data>AB/zRkqd</data>
<key>IOMatch</key>
<dict>
<key>IOProviderClass</key>
<string>IONetworkInterface</string>
<key>BSD Name</key>
<string>en0</string>
</dict>
</dict>
</array>
"
nvram boot-args="-v"
```

Die bei Macs nach dem Einschalten übliche Taste zum Einleiten eines Netzwerk-Boots funktioniert mit einer PC-Tastatur am Mac mini leider nicht. Beim iBookG4 können Sie ebenfalls per Mausklick das Booten vom Netz erzwingen. Sie erreichen dies aber auch hier mit dem Kommando:

```
nvram boot-device="enet:bootp"
nvram boot-args="-v"
```

Um den iBookG4 per Tastendruck vom Netz zu booten, müssen Sie nach dem Einschalten die Tasten drücken, bis ein blinkender blauer Globus erscheint. Ist der blaue Globus verschwunden, ist das Laden der Loader-Datei, etwa */tftpboot/macosx.tiger.ppc,* abgeschlossen und der Loader meldet sich mit einem grauen Apple-Symbol und einem grauen Globus. Ist der graue Globus verschwunden, ist das Laden der Kernel-Datei und der Kernel-Extensions-Datei abgeschlossen. Der Kernel meldet sich nun wegen des eingeschalteten Verbose-Modus mit weißen Texten auf schwarzem Grund und versucht, an die Datei *macosx.dmg* zu gelangen. Mithilfe des Programms "dmesg" können Sie das nach einem erfolgreichen Booten nachlesen, wann immer Sie wollen:

```
dmesg
netboot: retrieving IP information
  from DHCP response
netboot: IP address 10.1.1.223
  netmask 255.0.0.0 router 10.1.1.3
netboot: retrieving root path from
  BSDP response
Server 10.1.1.31
Mount /home/img.nfsroot/macosx.
  tiger.ppc
Image /macosx.dmg
```

Die Meldungen beim Mac mini sagen de facto das Gleiche. Nur holt sich der Mac mini die Datei *macosx.dmg* vom Solaris 10-Server an der IP-Adresse 10.1.1.198:

```
dmesg
netboot: retrieving IP information
  from DHCP response
netboot: IP address 10.1.1.225
```

```
  netmask 255.0.0.0 router 10.1.1.3
netboot: retrieving root path from
  BSDP response
Server 10.1.1.198
Mount /home/img.nfsroot/macosx.
  leopard.i386
Image /macosx.dmg
```

Der aufgeführte BSDP-Response ist ein DHCP-Response. BSDP ist eine nur von Apple verwendete Variante eines DHCP-Servers, die eigentlich nicht nötig ist. Das Mac-System nimmt die Antwort auch vom ganz normalen DHCP-Server des Linux-Systems entgegen. Die erstellte Datei *macosx.dmg* bootet den Mac auf die gleiche Art und Weise, wie es beim Booten von Festplatte der Fall ist. Nur der Kernel kommt vom Netz, und als Root-Dateisystem kommt der Inhalt der besagten Datei zum Einsatz. Der Mac hängt sich daraufhin alle lokalen Datenträger ein, deren er habhaft werden kann, und erinnert vom Erscheinungsbild her an eine "Diskless Workstation" (Bild 2). An der Ausgabe des Programms "df" ist gut zu erkennen, dass die Datei *macosx.dmg* als Platte "/dev/disk1" angenommen wurde und die interne Platte "/dev/disk0" unter "/private/var/netboot" eingehängt ist. Das vorbereitete Remote Login als Root funktioniert problemlos.

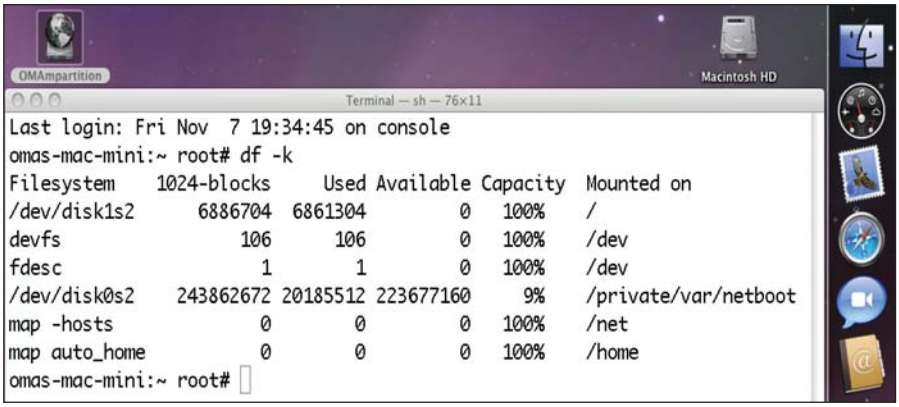


Bild 2: Der sichtbar gemachte Bootvorgang enthüllt, dass der Kernel vom Netz gestartet wurde

```
ssh -l root ibookg4
ssh -l root imacmini
```

Unerwünschte Features abschalten

Das gewünschte Booten von Mac OS X vom Netzwerk funktioniert, aber es ist ein üppig ausgestattetes Mac OS X mit allen – für uns in diesem Fall unerwünschten – Facetten einer grafischen Oberfläche. Ganz zu schweigen von den Powermanagement-Funktionen und anderen Formen künstlicher Intelligenz, die im schlimmsten Fall den Mac ausgerech-

net dann schlafen legt, wenn Sie aus der Distanz gerade mit der Fernwartung beschäftigt sind. Wollen Sie sich an dieser Stelle nicht den vielen Varianten des Bootvorgangs hingeben, die bei Panther, Tiger und Leopard unterschiedlicher nicht sein können, packen Sie das Problem am besten gleich an der Wurzel an. Auf dem Mac OS X der externen Festplatte erstellen Sie dafür die Datei */etc/rc.local.oma* mit dem in Listing "Grafische Oberflächen ausschalten" angegeben Inhalt.

So läuft auf jeden Fall der SSH-Serverdienst und ein Remote-Login ist möglich. Wer sich seiner Sache sicher ist, lässt in der While-Schleife gar kein Login zu oder verfolgt, wie es beim Leopard zu sehen sein wird, eine noch härtere Gangart. Um beim Booten in der Datei */etc/rc.local.oma* zu landen, ändern Sie auf der externen Festplatte unter Tiger und Panther die Datei */etc/rc*. Am Ende dieser Datei steht beim Panther der SystemStarter, der den restlichen Bootvorgang steuert:

```
# Datei /etc/rc (Auszug)
export LANGUAGE
SystemStarter -gr ${VerboseFlag}
  ${SafeBoot}
exit 0
```

Da ist der Schwenk auf die Datei */etc/rc.local.oma* ganz einfach:

```
/usr/sbin/sshd
HOME=/private/var/root
export HOME
cd $HOME
while echo ""
do
echo Login:
read REPLY
case $REPLY in
root)
cd $HOME
echo /bin/bash
echo "   stty intr 'AC'" > .bashrc
echo `pwd`
echo $PATH
/bin/bash
;;
esac
done
```

Grafische Oberfläche ausschalten

```
# Datei /etc/rc (Auszug)
export LANGUAGE
# SystemStarter -gr ${VerboseFlag}
  ${SafeBoot}
sh /etc/rc.local.oma
exit 0
```

Unter Tiger ist der Eingriff ähnlich. Nur müssen Sie hier den SystemStarter an anderer Stelle abschalten:

```
# Datei /etc/rc (Auszug)
if [ "${SafeBoot}" = "-x" ]; then
launchctl load
  /System/Library/LaunchDaemons
else
launchctl load
  /System/Library/LaunchDaemons
# SystemStarter ${VerboseFlag}
fi
```

Am Ende der Datei */etc/rc* wird wieder die Datei /etc/rc.local.oma aufgerufen:

```
# Datei /etc/rc (Auszug)
if [ -f /etc/rc.local.oma ]; then
sh /etc/rc.local.oma
fi
exit 0
```

Für Leopard ist die Datei */etc/rc* abgeschafft. Der Kernel geht gleich auf das binäre Programm */sbin/launchd*. Das macht die Sache etwas komplizierter, aber nicht unmöglich. Die Datei */System / Library / LaunchDaemons / com.apple.loginwindow.plist* schafft den Aufruf des Programms "loginwindow" ab. Dann haben Sie Ruhe vor der grafischen Oberfläche. Stattdessen wird die Datei */etc/rc.local.oma* aufgerufen:

```
<dict>
<key>Label</key>
<string>com.apple.loginwindow
  </string>
<key>ProgramArguments</key>
<array>
<string>/etc/rc.local.oma</string>
</array>
<key>KeepAlive</key>
<true/>
</dict>
```

Die Datei */ etc / rc.local.oma* für Leopard ist auch nur eine kleine Dauerschleife. Ein Login an der Konsole von Leopard ist trotzdem nicht möglich, da */ dev / console* vom Programm */sbin/launchd* blockiert ist.

```
#!/bin/sh
while echo ""
do
/usr/libexec/getty std.57600 console
read REPLY < /dev/console
echo > /dev/console
done
```

Das Ergebnis ist ein Leopard in Schwarz-Weiß. Der Fernzugriff per SSH funktioniert trotzdem einwandfrei. So können Sie jederzeit Daten über das Netz sichern oder zurückspielen. Durch den Eingriff in das Skript */etc/rc* beziehungsweise in die Datei *com.apple.loginwindow.plist* geht das Booten mit der neu erstellten Datei *macosx.dmg* viel schneller. Ist der Mac erst einmal vom Netz gebootet, geht alles, was sich per Kommando regeln lässt [1].

Fazit

Suchen Sie im Web nach Informationen zum Booten eines Macs über das Netz, finden sich jede Menge widersprüchliche Aussagen. In der Realität ist es allerdings nur das übliche Zusammenspiel von DHCP, TFTP- und NFS-Server unter Verwendung der richtigen Bootdateien. Die Bootdateien sind nur mit etwas Cleverness zu erstellen. Lohn der Mühe ist die Option, aus der Ferne mit einem Mac jederzeit das zu tun, was ein Mac OS X per Kommando ermöglicht – und das ist so gut wie alles. Und mit der hier beschriebenen Methode müssen Sie nicht auf einen Apple-Server zurückgreifen, um endlich einen Mac vom Netz zu booten. *(ln)*

[1] IT-Administrator 03/2007
"Weck das Unix in Dir", auch online unter www.it-administrator.de/themen/server_client/fachartikel/51937.html

Ressourcen

Ausgelagerte Server als Testlandschaft

Rechenzentrum auf Knopfdruck

von Bertram Wöhrmann

Immer wieder sieht sich der IT-Verantwortliche mit der Anforderung konfrontiert, Software oder Hardware zu testen. Oft steht noch irgendwo ein alter Server zur Verfügung, der dann für diese Aufgabe genutzt wird. Problematisch wird es jedoch, sobald die Applikation eine größere Infrastruktur erfordert oder wenn aussagekräftige Lasttests erfolgen sollen. Als schwierig erweist sich dabei ebenfalls, dass meistens die Zeit für die Durchführung ausgiebiger Tests und deren Vorbereitung – allein der Aufbau der Hardware – fehlt. Als Alternative bietet sich die Anmietung einer kompletten Testinfrastruktur an. In diesem Beitrag zeigen wir Ihnen anhand eines realen Lasttests die Arbeit mit und in einem "Remote Rechenzentrum".

In dem hier beschriebenen Fall ergab sich die Anforderung, Windows Terminal Server (WTS) einem Lasttest zu unterziehen, um die zu erwartende Leistung zu messen. Diese Tests sollten auf WTS-Servern stattfinden, die auf unterschiedlichen virtuellen Plattformen betrieben werden, um eine möglichst umfangreiche und zukunftssichere Aussage zu ermöglichen. Die Erarbeitung der Ergebnisse sollte dabei in recht kurzer Zeit erfolgen. Das damit einhergehende Problem war zum einen die kurzfristige Bereitstellung von Hardwareressourcen in der benötigten Anzahl und zum anderen die erforderliche Manpower.

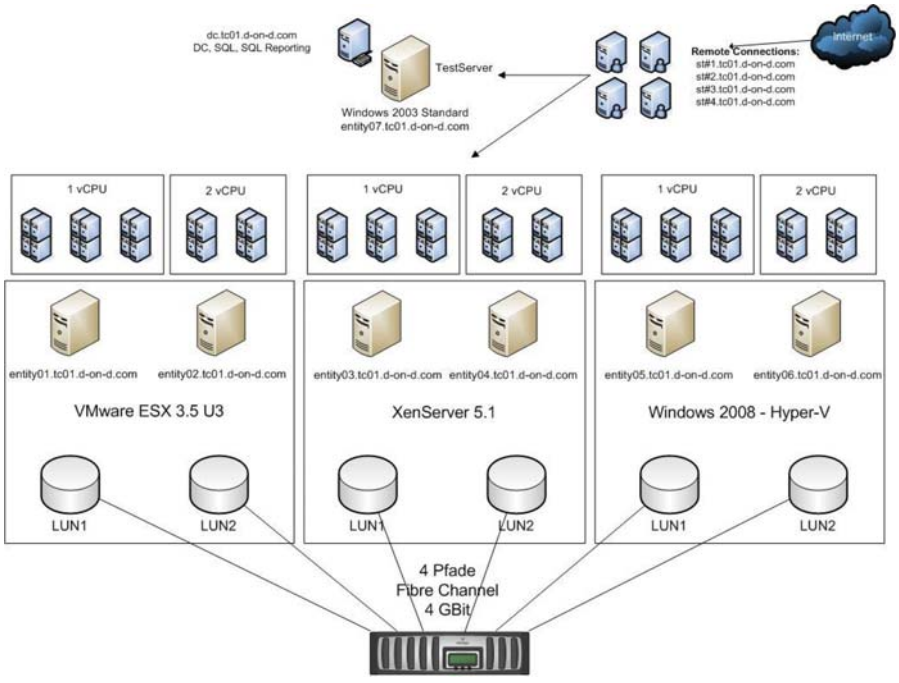


Bild 1: Der Aufbau der Infrastruktur zum Test auf drei Virtualisierungsplattformen

Massive Hardware-Anforderungen

Für die parallele Durchführung der Tests benötigten wir sieben physikalische Server: Jeweils zwei Server mit VMware ESX 3.5 U3, XenServer 5.1 und Microsoft Hyper-V. Das siebte System diente zur Ausführung der Lasttests mittels Citrix Edgesight. Zur einwandfreien Durchführung der Tests benötigten wir zusätzlich einen Domänencontroller und einen MS SQL-Server mit Reporting Services, welcher unter VMware-Server auf dem siebten System zusätzlich lief. Wichtig war hierbei, immer gleiche Voraussetzungen bei den Zielsystemen zu schaffen, ohne die Kosten aus den Augen zu verlieren.

Auf jeder Virtualisierungsplattform legten wir jeweils drei virtuelle Server mit einer vCPU und 4 GByte Arbeitsspeicher an sowie zwei virtuelle Server mit zwei vCPUs und 4 GByte RAM. Die Systeme wurden mit der Windows 2003 Standard- und Enterprise-Edition getestet, um auch dort Unterschiede direkt festzustellen. Diese traten aber erwartungsgemäß erst bei Systemen mit mehr als 4 GByte Hauptspeicher auf.

Die Durchführung der Tests fand immer isoliert auf einer Gruppe von identischen virtuellen Servern statt. Alle nicht für den Test relevanten Systeme, die ebenfalls auf der entsprechenden Virtualisierungsplattform liefen, wurden ausge-

schaltet. Auf den virtuellen Systemen installierten wir Microsoft Office 2003 SP3, da der Lasttest die Nutzung der Office-Komponenten simuliert. Im Ergebnis sollte sich damit widerspiegeln, wie viel Last eine definierte Anzahl von Anwendern, die mit den Systemen arbeiten, erzeugt.

Faktoren, die Messergebnisse beeinflussen oder verfälschen

In unserem speziellen Fall musste gewährleistet sein, dass die Zugriffe auf den Storage über das Fibre Channel-Netzwerk und die Zugriffe über das IP-Netzwerk nicht von anderen Computern beeinflusst werden. Somit benötigten wir für einen aussagekräftigen Test separaten Storage und ein isoliertes Netzwerk. Diese Faktoren sprechen für die Nutzung eines Mietrechenzentrums. Der Aufwand für das Mieten von Hardware samt zugehöriger Peripherie und deren Aufbau und Abbau im eigenen Rechenzentrum ist weit höher als die Kosten für die Nutzung von Fremdhardware in einem anderen RZ.

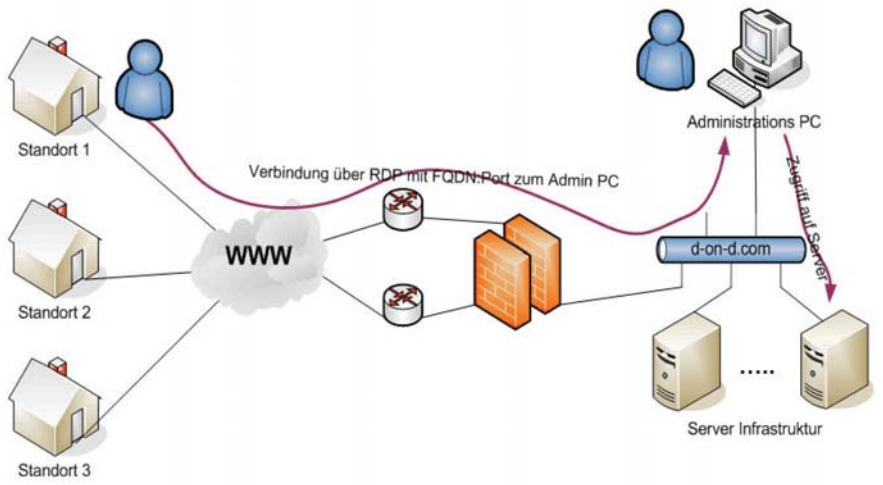


Bild 2: Der Zugriff über das Internet erfolgt zunächst auf eine Arbeitsstation und erst von dort auf die Testinfrastruktur

Ein nicht zu unterschätzender Vorteil einer gemieteten Umgebung liegt in der zeitlichen Einschränkung, da die Systeme eben nur für einen gewissen Zeitraum zur Verfügung stehen. Im Normalfall wird den Administratoren die benötigte Zeit für die Tests auch zugebilligt, wenn die Testlandschaft nur begrenzt zur Verfügung steht. Finden Tests auf "übrig gebliebenem" Blech im eigenen RZ statt, dann passiert es oft, dass die Aufgaben nach einer gewissen Zeit im Tagesgeschäft untergehen.

Daher realisierten wir unseren Lasttest im "Datacenter on Demand (siehe Kasten). Für unseren speziellen Fall wurde nur die Infrastruktur vorbereitet. Des Weiteren setzten wir einen externen Virtualisierungsspezialisten ein, der die Basisinstallation der Server nach den bekannten Best Practices durchführte. Dies entlastete die beteiligten Kollegen enorm und führte zu einer zeitnahen Durchführung der Tests.

Lasttest per Fernzugriff

Für den Zugriff auf unsere Testlandschaft benötigten wir lediglich einen Internetzugang mit den zusätzlichen Ports für die getunnelten RDP-Sessions. Diese Sitzung endet auf einem Computer, der als Einstiegspunkt in die gemietete Umgebung dient. Von hier aus hatten wir die Möglichkeit, alle anderen Server und auch die Peripherie zu erreichen und zu konfigurieren. Von dem Einstiegspunkt aus nutzten wir die Funktion der "Remote Management Boards" der Server (in diesem Fall HP iLO). Alternativ ist ein Zugriff via SSH beziehungsweise RDP auf die Systeme möglich.

Ist das Konzept des Fernzugriffs auf das RZ einmal verstanden, lässt sich mit der Infrastruktur sehr einfach und effizient arbeiten. Der Nutzer muss sich darüber im Klaren sein, dass er in einem "fremden" Rechenzentrum arbeitet, das heißt idealerweise legt er vor der Nutzung einen Plan über die benötigte Software und die Konfiguration an.

Für den clientseitigen Zugriff auf das Rechenzentrum benötigen Sie lediglich eine 64-KBit-Verbindung, um performant per RDP arbeiten zu können. Der Zugang stellt somit kein Problem dar, selbst wenn nur eine UMTS-Karte zum Einsatz kommt. Die Möglichkeit des Internetzugriffs half uns weiterhin wesentlich bei der Verteilung der

Datacenter on Demand

Die im "Datacenter on Demand" – www.d-on-d.com – des Schweizer Systemhauses Kybernetika eingesetzten Server-, Netzwerk-, Fibre Channel- und Storage-Komponenten sind "state of the art". Alle Komponenten sind für die Virtualisierungsprodukte – insbesondere VMware – zertifiziert, was Probleme bei den Tests beziehungsweise der Installation minimiert. Testlizenzen für die zum Einsatz kommende Software stellt das d-on-d kostenfrei zur Verfügung.

Die Anbindung an das Internet erfolgt mit 10 MBit/s über eine redundante Firewall von zwei unterschiedlichen Herstellern. Dies gewährleistet einen zügigen Down- beziehungsweise Upload der benötigten Daten von und zu den Testservern. Die Systeme werden hardwareseitig fertig in die Infrastruktur integriert übergeben, sodass sich sofort mit der Installation der Komponenten beginnen lässt. Die Kunden können sich aber auch alle Systeme vorinstalliert übergeben lassen.

Die Netzwerkstruktur gestaltet sich relativ einfach: Die Administration erfolgt über einen (oder mehrere) Remote Desktop (RDP) über das Internet. Alle dahinterliegenden Komponenten haben private IP-Adressen. Über diesen Weg kann der Anwender alle gemieteten Komponenten administrieren. Zur Sicherheit wird nicht mit den bekannten Ports für RDP gearbeitet. Die zu nutzenden Ports werden mit der Dokumentation bekannt gegeben, die der Dienstleister bei der Übergabe zur Verfügung stellt.

Aufgaben: Während die komplette Datacenter-Konfiguration sowie -Installation durch den externen Berater erfolgte, installierten wir die Terminalserver-Umgebung selbst. Die beiden zugreifenden Personen waren örtlich etwa 500 Kilometer voneinander getrennt, was aber für unseren Lasttest absolut kein Problem darstellte.

Aufbau der Testlandschaft

Wie eingangs erwähnt, benötigten wir für unseren Test sechs Server (Zwei-Sockel-QuadCore, 16 GByte RAM, FC-Adapter), zudem ein Volumen von 450 GByte an Fibre Channel SAN-Storage mit einer 4 GBit-Anbindung und 28 GBit-Ethernet Verbindungen. Außerdem mussten wir ein weiteres dediziertes System (4 GByte RAM) zum Ausführen der Tests einplanen, damit keine Unschärfen durch Zusatzbelastungen entstehen konnten. Auf diesem System sollte später auch mittels VMware-Server eine Windows 2003-VM (Domänencontroller mit SQL 2005-Datenbank und Reporting Server, Citrix XenApp-Lizenzserver) zur Verfügung gestellt werden.

Als Speicherplattform entschieden wir uns für die Nutzung eines NetApp FAS 3020-Metroclusters, welcher über zwei Ports mit jeweils 4 GBit über Brocade Fibre Channel-Switches angebunden war. Die Serversysteme verfügten ebenfalls über jeweils zwei Fibre Channel-Ports à 4 GBit. Das genutzte Plattenaggregat bestand aus 56 FC-Festplatten zu je 146 GByte. Als Nutzkapazität stellten wir den jeweiligen Serversystemen sechs LUNs zu je 75 GByte bereit. Die für den Terminalserver-Test benötigte Software luden wir über das Internet ins Test-RZ.

Die HP-Server installierten und verwalteten wir ferngesteuert mittels des Remote Management Adapters (iLo – integrated Lights out). Dank der Virtual Media-Funktion ist es dabei möglich, das Installationsmedium als ISO-Image über das Netzwerk dem Server zuzuordnen. Die Installation der Server ging bei der VMware- und Citrix-Variante sehr zügig vonstatten. Die Microsoft Hyper-V-Installation benötigte deutlich mehr Zeit, da die Hardwaretreiber halbautomatisch (HP Smartstart) oder manuell (Intel NIC Teaming-Treiber plus NetApp Multipathing-Treiber) installiert werden mussten. Weiterhin kam es während der Installation direkt zum Bluescreen, was durch ein

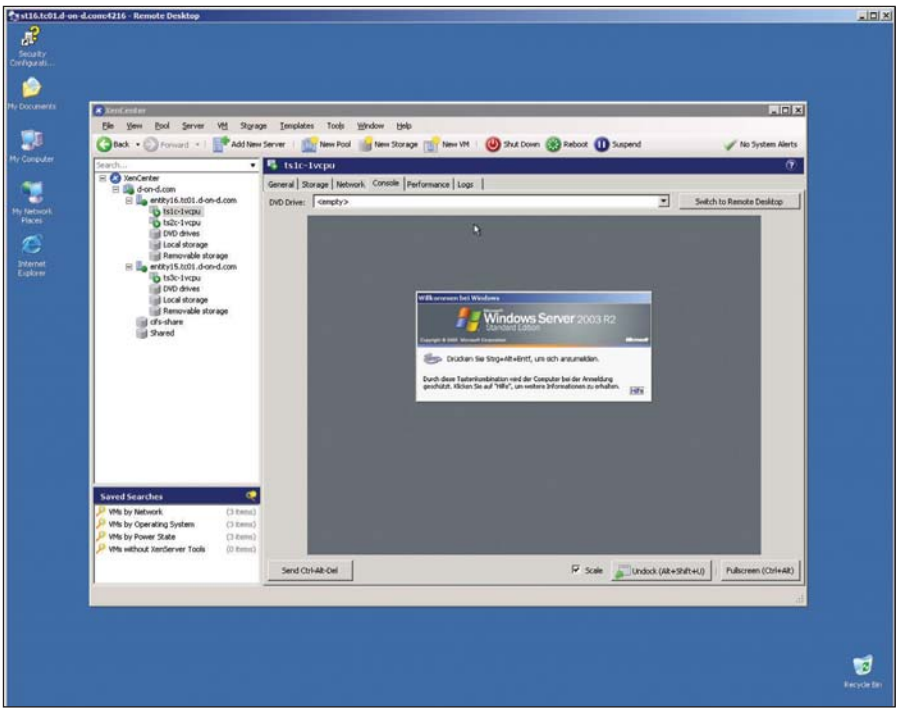


Bild 3: Die Administration von XenServer mittels RDP

Firmware-Upgrade der Server schnell gelöst werden konnte. Die virtuellen Maschinen installierten wir danach auf jedem System komplett neu und bespielten sie mit allen aktuellen Patches und dem Citrix XenApp Server.

Messen was das Zeug hält

Die Messungen selbst wurden mit der Citrix Edgesight durchgeführt, die eine genaue Analyse der vorhandenen und möglichen Performance bei unterschiedlicher Anzahl von Nutzern auf dem Terminalserver ermöglicht. Da die Basiskonfiguration bezüglich Hardware und Software immer identisch war und niemals zwei Tests gleichzeitig durchgeführt wurden, war sichergestellt, dass die Tests immer authentisch waren. Das Nutzerverhalten wurde anhand von Microsoft Office-Produkten (Word, Excel, PowerPoint) und dem Internet Explorer vollautomatisch nachgestellt.

Mit EdgeSight for Load Testing lassen sich typische Anwenderaktionen wiederholt ausführen, wie etwas das Öffnen einer Datei, Bearbeiten, Abspeichern et cetera. Kombiniert der Tester unterschiedliche Verhaltensweisen miteinander, entsteht ein komplexes Userprofile. Dieses Profil startet der Tester nun mehrfach. Beginnend mit einem simulierten User wird die Anzahl stetig erhöht. Die Lastdaten der WTS-Server werden in einer Datei abgelegt. Als Ergebnis zeigt sich, wie viele Anwender mit den getesteten Applikationen gleichzeitig arbeiten können. Es wird auch sichtbar, ob die Server sich linear verhalten, wenn die Anwenderzahl steigt.

Die Ergebnisgraphen zeigten deutlich, wie die Belastung des Servers mit der Anzahl der User ansteigt. Ein abschließender Vergleich der Messergebnisse zeigte, wie unterschiedlich sich die drei Virtualisierungsprodukte beim WTS-Einsatz verhielten.

Blieb nur eine Frage offen: Wie aussagekräftig sind die Tests und wie können die Ergebnisse in Relation zu unserer Infrastruktur gestellt werden? Daher beschlossen wir nach Abschluss der Tests und den abgenommenen Ergebnissen, dass die installierten virtuellen Systeme nicht verloren gehen dürfen. Aufgrund der hohen Datenmenge (mehrere Dutzend GByte) wurde entschieden, die virtuellen Maschinen auf USB-Platten zu sichern und auf dem Postweg zu versenden. Somit besteht die Möglichkeit, die Konfiguration in unserem RZ nachzustellen und die Ergebnisse dort mit denen aus dem Lasttest zu vergleichen.

Testkosten im Vergleich

	Gemietetes RZ	Eigenes RZ
Investition Hardware	keine	Kauf oder Miete von HW
Aufbau der Infrastruktur	durch Dienstleister	durch eigenes Personal
Reisekosten	keine	12 Übernachtungen plus Anreise
Testaufwand	6 Tage	6 Tage
Rückbau der Infrastruktur	durch Dienstleister	durch eigenes Personal
Weiterverwendung der HW	nicht relevant	nicht gewährleistet

Fazit

Der Lasttest lieferte aussagekräftige Ergebnisse hinsichtlich der Performance der verschiedenen Plattformen für virtuelle WTS-Server. Wichtig ist aber auch, das Management und die technischen Möglichkeiten ebenfalls zu betrachten. Es nützt nichts, wenn schnelle virtuelle Maschinen nicht optimal zu betreiben sind. Auch wenn unsere Ergebnisse Verschlusssache des Kunden sind, möchten wir Sie doch auf die Resultate eines wesentlich ausführlicheren Tests der Firma Login Consultant B.V. aus den Niederlanden hinweisen, deren Ergebnisse sich mit den unsrigen decken. Auf dem XenServer von Citrix sind die WTS-Server am performantesten, dann folgt mit Abstand VMware und auf dem letzten Platz findet sich Microsofts Hyper-V. Es wird sicher spannend zu beobachten, ob und wie sich das Verhältnis mit der neuen Version VI4 von VMware ändert.

Das Anmieten eines externen Rechenzentrums lohnt sich für IT-Verantwortliche unter bestimmten Rahmenbedingungen: Es ist keine Investition in eigene Komponenten notwendig, die unter Umständen nur wenige Tage benötigt werden. Die Isolation der gemieteten Serverlandschaft gewährleistet zudem ein unverfälschtes Ergebnis. Einer der größten Vorteile ist aber, dass sich von überall auf die Systeme zugreifen lässt und sich so auch mit externen Dienstleistern oder Mitarbeiter in unterschiedlichen Lokationen sehr gut zusammenarbeiten lässt.

Auch die Gegenüberstellung der beiden möglichen Varianten aus rein kostentechnischer Sicht (siehe Tabelle) zeigt, dass die Miete für unseren Test die preiswertere Alternative ist. Es fallen keine Reisekosten an und die Kosten für die Bereitstellung und den Rückbau der Server und Netzwerke übernimmt der Dienstleister. Außerdem muss sich der IT-Verantwortliche keine Gedanken über die Weiterverwendung des Testequipments machen, da er mit letztmaliger Beendigung der RDP-Sitzung auch sprichwörtlich die Tür hinter sich zu macht. Aus technischer Sicht stellt sich die Frage ebenfalls nicht: Es kommt aktuellste Hardware zum Einsatz, die Daten sind sicher und keinerlei Fremdsysteme verfälschen das Ergebnis. Auch wird die eigene produktive Umgebung in keinster Weise belastet oder gar beeinträchtigt. *(jp)*

Ergebnisse eines vergleichbaren Lasttests:
www.projectvrc.nl/index.php?option=com_docman&task=cat_view&gid=39

Links

iladministrator

Live-Workshops 2009

Jetzt Plätze sichern und anmelden!

1 München

Exchange 2007

ITANet-Workshop (kostenlos für Abonnenten)
am 05. Februar 2009, 13.00-17.30 Uhr
Dozent: Thomas Joos
Workshop-Partner: IronPort
Anmeldeschluss: 28. Januar 2009

2 Frankfurt/Eschborn

Netzwerksicherheit

ITANet-Workshop (kostenlos für Abonnenten)
am 01. April 2009, 13.00-17.30 Uhr
Dozent: wird noch bekannt gegeben
Workshop-Partner: Realtech
Anmeldeschluss: 23. März 2009

jetzt anmelden

anschließend, am 02. und 03. April 2009:

Data Center Security

Intensivseminar in Kooperation mit Fast Lane
Preis: Euro 1.190,- zzgl. 19% MwSt.
Sonderpreis für IT-Administrator-Abonnenten: Euro 1.071,- zzgl. 19% MwSt.
Anmeldeschluss: 13. März 2009

3 Berlin

Storage-Lösungen für virtualisierte Server

ITANet-Workshop (kostenlos für Abonnenten)
am 28. Mai 2009, 13.00-17.30 Uhr
Dozent: wird noch bekannt gegeben
Workshop-Partner: wird noch bekannt gegeben
Anmeldeschluss: 18. Mai 2009

am darauffolgenden Tag, dem 29. Mai 2009:

Storage-Virtualisierung

Intensivseminar in Kooperation mit Fast Lane
Preis: Euro 700,- zzgl. 19% MwSt.
Sonderpreis für IT-Administrator-Abonnenten: Euro 630,- zzgl. 19% MwSt.
Anmeldeschluss: 08. Mai 2009

4 Heidelberg

Hochverfügbarkeit von Diensten und Applikationen

ITANet-Workshop (kostenlos für Abonnenten)
am 16. Juli 2009, 13.00-17.30 Uhr
Dozent: wird noch bekannt gegeben
Workshop-Partner: Realtech
Anmeldeschluss: 06. Juli 2009

5 Hamburg

E-Mail-Management

ITANet-Workshop (kostenlos für Abonnenten)
am 30. September 2009, 13.00-17.30 Uhr
Dozent: wird noch bekannt gegeben
Workshop-Partner: Gingcom
Anmeldeschluss: 21. September 2009

anschließend, am 01. und 02. Oktober 2009:

SPAM

Intensivseminar in Kooperation mit Fast Lane
Preis: Euro 1.090.- zzgl. 19% MwSt.
Sonderpreis für IT-Administrator-Abonnenten: Euro 981,- zzgl. 19% MwSt.
Anmeldeschluss: 11. September 2009

6 Böblingen

Virtualisierte Infrastrukturen

ITANet-Workshop (kostenlos für Abonnenten)
am 29. Oktober 2009, 13.00-17.30 Uhr
Dozent: wird noch bekannt gegeben
Workshop-Partner: Kroll Ontrack
Anmeldeschluss: 19. Oktober 2009

7 München

Open Source im Mittelstand

ITANet-Workshop (kostenlos für Abonnenten)
am 24. November 2009, 13.00-17.30 Uhr
Dozent: wird noch bekannt gegeben
Workshop-Partner: GeNUA

anschließend, vom 25. bis 27. November 2009:

IT-Security-Workshop

Intensivseminar in Kooperation mit GeNUA
Preis: Euro 1.395,- zzgl. 19% MwSt.
Sonderpreis für IT-Administrator-Abonnenten: Euro 1.245,- zzgl. 19% MwSt.

IT-Administrator Trainings-Partner: GeNUA

IT-Administrator Trainings-Partner: fast lane

ITANet Schirmherrschaft: REALTECH

ITANet – Die System und Netzwerk User Group

Mehr Infos und Anmeldeformulare zu den Veranstaltungen unter

http://www.it-administrator.de/usergroup/termine/

oder per E-Mail an info@itanet.de

Netzwerkrichtlinien mit Windows Server 2008 (2)

Schutz für die Clients

von Thomas Joos

Mit dem Windows Server 2008 erhalten Administratoren auch das Feature "Network Access Protection". Im ersten Teil unserer Workshopserie haben wir die Grundlagen des Netzwerkschutzes und erste Konfigurationsschritte aufgezeigt. Im zweiten Teil befassen wir uns mit der clientseitigen Einführung von NAP und dem DHCP-basierten Schutz.

Die clientseitige Konfiguration von NAP führen Sie am besten über Gruppenrichtlinien durch. Die Einstellungen hierfür finden Sie in der Gruppenrichtlinienverwaltung unter "Computerkonfiguration / Windows-Einstellungen/ Sicherheitseinstellungen / Network Access Protection". Dort legen Sie das Verhalten der Clientcomputer fest. Die Servereinstellungen richten Sie dagegen im Server-Manager ein. Sie finden die Konfiguration des Netzwerkrichtlinienservers über "Rollen / Netzwerkrichtlinien- und Zugriffsdienste". Alternativ können Sie diese Konfiguration auch über "Start / Verwaltung / Netzwerkrichtlinienserver" aufrufen oder – noch schneller – über "Start / Ausführen / nps.msc".

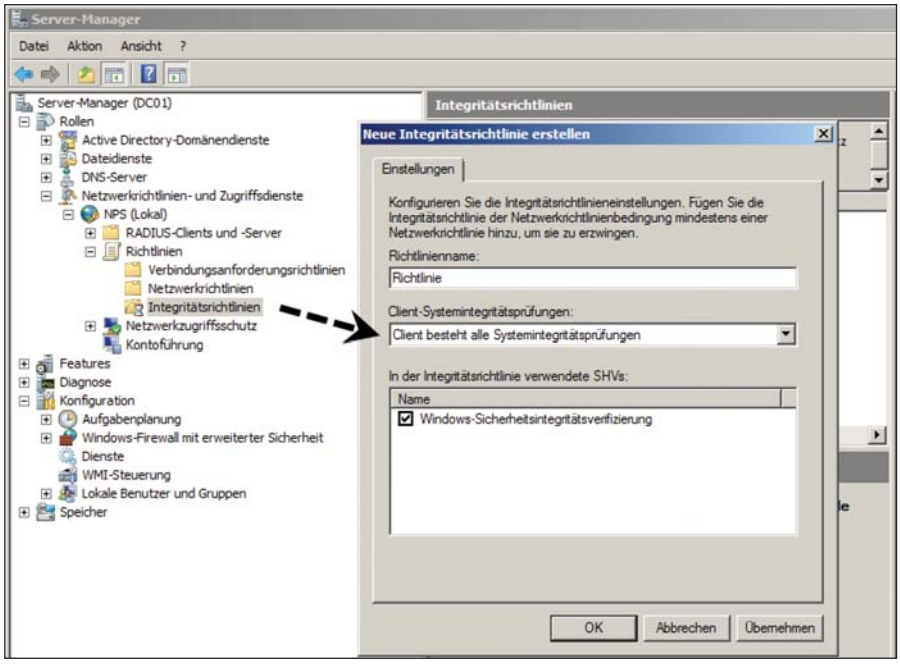


Bild 1: Anhand der Systemintegritätsprüfung lassen sich Richtlinien anwenden

Die Zugriffskontrolle baut zunächst auf der Sicherheitsintegritätsprüfung auf, die von den Clients das Statement of Health (SoH) abfragt. Die Einstellungen hierzu finden Sie in der Verwaltungskonsole über "NPS / Netzwerkzugriffsschutz / Systemintegritätsprüfungen". Rufen Sie im nächsten Schritt die Eigenschaften der Verifizierungsmethode auf, zum Beispiel die der standardmäßig vorhandenen "Windows-Sicherheitsintegritätsverifizierung". Hier können Sie über die Schaltfläche "Konfigurieren" festlegen, welche Anforderungen die Clients erfüllen müssen, um mit NAP in Ihrem Netzwerk konform zu sein. Diese Systemintegritätsprüfungen bezeichnet Microsoft auch als "Security Health Agents" (SHA). Diese Agents werden unter Windows Vista durch den "Windows Security Health Validator" (SHV) verbunden. Hauptsächlich überprüfen die SHAs den Zustand des Windows-Sicherheitscenters in Windows Vista und XP.

Über den Menüpunkt "Wartungsservergruppen" hinterlegen Sie nun die DNS-Namen oder IP-Adressen von Servern, über die nicht konforme Clients mit Updates versorgt werden können. Unter "NPS / Richtlinien / Integritätsrichtlinien" legen Sie schließlich Richtlinien dazu fest, was mit Clients passieren soll, die konform sind oder nicht. So stellen Sie etwa ein, wann die Richtlinie angewendet werden soll, also ob der Client eine vorher festgelegte Systemintegritätsüberprüfung besteht oder nicht. Zusätzlich legen Sie hier fest, welche Systemintegritätsprüfung Sie als Basis für die Integritätsrichtlinie verwenden. Sinn dieser Einstellung ist es, eine Richtlinie für konforme und eine Richtlinie für nicht konforme PCs festzulegen und auf welcher Basis diese Konformität überprüft werden soll.

Nachdem Sie über die Systemintegritätsprüfungen definiert haben, welche Sicherheitsaspekte auf einem Computer geprüft werden, legen Sie eine Integritätsrichtlinie fest. Diese entscheidet, anhand welcher Systemintegritätsüberprüfung festgemacht wird, ob ein Client konform oder nicht konform ist. Zusätzlich macht es vor allem während einer Übergangszeit Sinn, eine weitere Integritätsrichtlinie festzulegen, in die Clients aufgenommen werden, die NAP nicht unterstützen.

Als Nächstes erstellen Sie eine Netzwerkrichtlinie, die auf der Integritätsrichtlinie basiert. In dieser Policy steuern Sie, was mit den konformen beziehungsweise nicht konformen Clients passieren soll. Die Konfiguration der Richtlinien wird als XML-Datei abgespeichert. Sie finden diese Konfiguration in der Datei *ias.xml* im Verzeichnis "Windows \ System32 \ ias". Diese Datei können Sie im Fehlerfall zum Beispiel zu einem Microsoft-Experten schicken, der die Fehler dann effizienter auswerten kann. Die Logdateien für NAP-Clients finden Sie unter "Windows \ Tracing".

Netzwerkzugriffsschutz über DHCP als Kompromiss

Microsoft empfiehlt, den grundlegenden NAP-Schutz in einem Unternehmen über den DHCP-Server zu nutzen. Damit genießen Unternehmen den Vorteil der NAP ohne größere Änderungen in der Infrastruktur. Der Zugangsschutz über DHCP ist zwar die unsicherste Variante der NAP (Clients können sich schließlich auch manuell eine IP-Adresse zuteilen), dafür aber auch die am schnellsten einführbare. Damit Sie NAP mit DHCP einsetzen können, müssen Sie nicht unbedingt gleich die ganze Domäne auf Windows Server 2008 umstellen. Die Domänencontroller können ohne Weiteres noch unter Windows Server 2003 laufen. Nur der DHCP- und der Netzwerkrichtlinienserver (NPS) müssen unter Windows Server 2008 laufen.

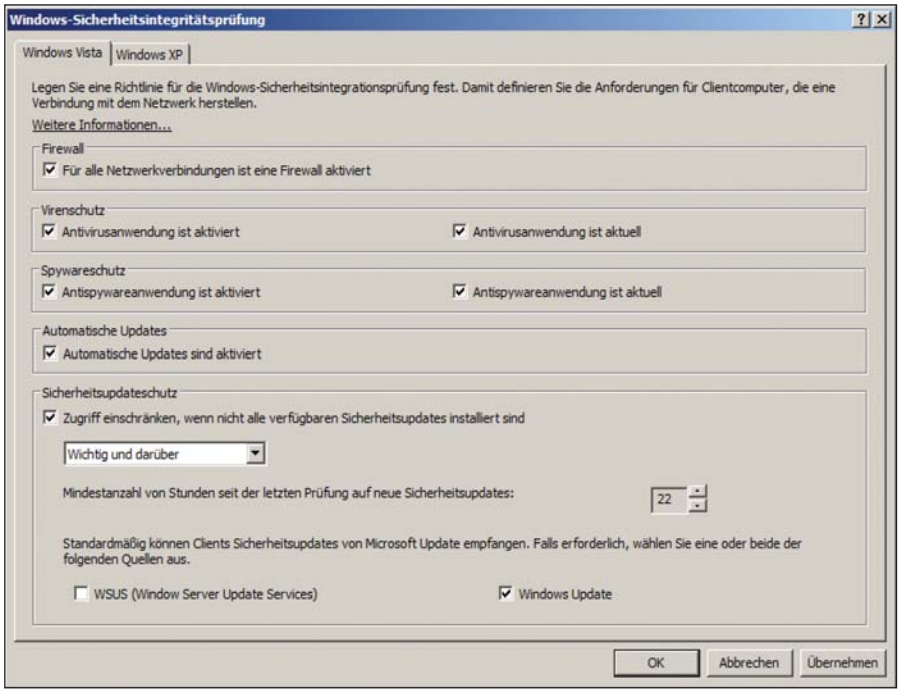


Bild 2: Sieben entscheidende Häkchen für ein sicheres System: Die Konfiguration der Sicherheitsintegritätsverifizierung

Installieren Sie auf dem Windows-Server die DHCP- sowie die Netzwerkrichtlinien und -Zugriffsdienste-Rolle. Als Clients kommen Windows Vista und Windows XP SP3 in Frage. Nachdem Sie DHCP auf dem Server installiert haben, können Sie als Nächstes einen neuen DHCP-Bereich erstellen. Der folgende Schritt besteht darin, dass Sie die Systemintegritätsprüfungen (System Health Validators, SHVs) konfigurieren. Klicken Sie dazu in der NAP-Konsole auf "Netzwerkzugriffsschutz / Systemintegritätsprüfungen" und rufen Sie die Eigenschaften der Windows-Sicherheitsintegritätsverifizierung auf. Klicken Sie jetzt im Fenster auf die Schaltfläche "Konfigurieren". Damit können Sie festlegen, welche Bedingungen eine Arbeitsstation erfüllen muss, damit diese mit dem Netzwerk kommunizieren darf. Anschließend deaktivieren Sie für einen Test zum Beispiel alle Kontrollkästchen außer "Für alle Netzwerkverbindungen ist eine Firewall aktiviert". Das Kontrollkästchen "Automatische Updates" können Sie ebenfalls aktiviert lassen. Hierüber wird konfiguriert, ob der Client seine Patches von einem WSUS-Server erhält oder direkt aus dem Internet.

Bei den Wartungsservern tragen Sie wieder die DNS-Namen oder IP-Adressen von Servern ein, mit denen nicht konforme Clients kommunizieren dürfen. Das können entweder WSUS- oder FTP-Server sein, auf denen Sie Virensignaturen bereitstellen. In diesem Beispiel können Sie den Domänencontroller als Wartungsserver festlegen, damit nicht konforme NAP-Clients Zugriff auf DNS haben. Erstellen Sie dabei zu Testzwecken eine neue Gruppe und hinterlegen Sie den Domänencontroller, der auch den DNS-Dienst bereitstellt. Klicken Sie hierfür mit der rechten Maustaste auf den Menüpunkt "Wartungsservergruppen", rufen Sie den Kontextmenübefehl "Neu" auf und tragen Sie die Daten des DNS-Servers ein.

Der nächste Schritt besteht darin, dass Sie eine Integritätsrichtlinie (Health Policy) erstellen, die als Grundlage die Systemintegritätsprüfung (SHV) verwendet. Anhand dieser Richtlinie werden die Clients später bei bestandener Systemintegritätsprüfung als konform erklärt. Die zweite Richtlinie erklärt Clients nicht konform, wenn sie die Systemintegritätsprüfung nicht bestanden haben.

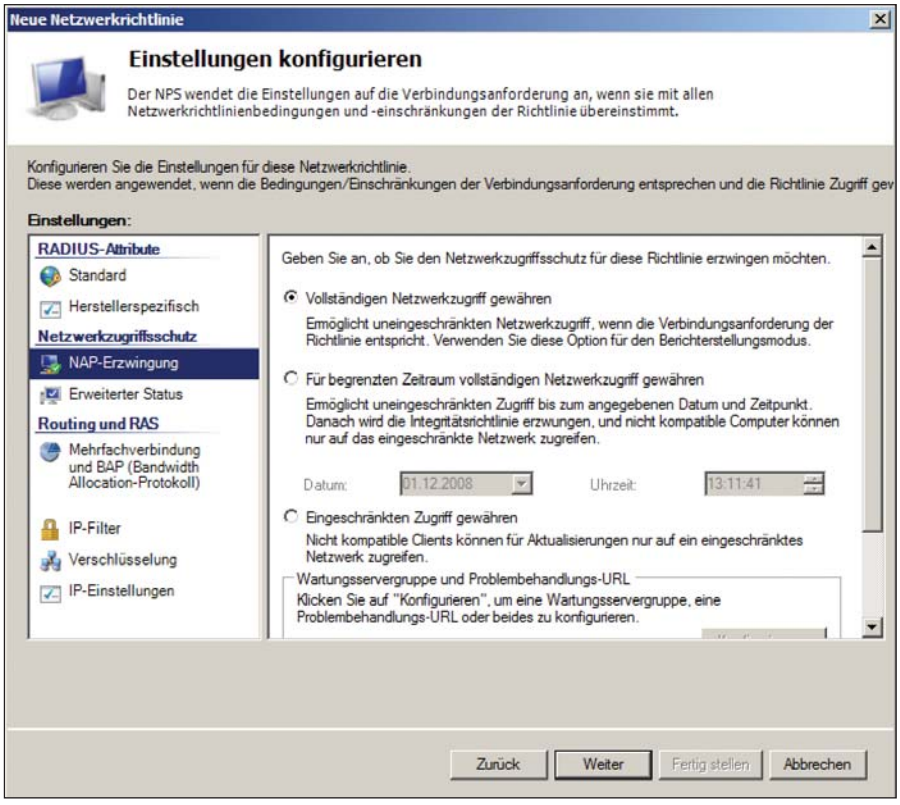


Bild 3: Über die NAP-Erzwingung für Clients gewähren Sie den Netzwerkzugriff oder schränken diesen ein

Klicken Sie zum Erstellen einer Integritätsrichtlinie mit der rechten Maustaste auf "Richtlinien / Integritätsrichtlinien" und wählen Sie im Kontextmenü den Befehl "Neu". Geben Sie der Richtlinie die Bezeichnung "NAP-konform". Stellen Sie sicher, dass im Listenfeld "Client-Systemintegrität prüfen" der Eintrag "Client besteht alle Systemintegritätsprüfungen" ausgewählt ist. Aktivieren Sie das Kontrollkästchen "Windows-Sicherheitsintegritätsverifizierung".

Erstellen Sie anschließend eine weitere Integritätsrichtlinie mit der Bezeichnung "Nicht-NAP-konform". Wählen Sie im Listenfeld den Eintrag "Client besteht mindestens eine Systemintegritätsprüfung nicht" aus und aktivieren Sie wiederum das Kontrollkästchen "Windows-Sicherheitsintegritätsverifizierung". Netzwerkrichtlinien (Network Policies) steuern wie bereits geschildert den Netzwerkzugriff von Clients basierend auf Integritätsrichtlinien (Health Policies), die wiederum auf den Systemintegritätsprüfungen (System Health Validators, SHVs) aufbauen.

Bevor Sie neue Richtlinien erstellen, sollten Sie zunächst die standardmäßig angelegten Richtlinien deaktivieren. Klicken Sie diese dazu mit der rechten Maustaste an und wählen Sie im Kontextmenü den Eintrag "Deaktivieren" aus.

Umgang mit gesunden Clients

Im Anschluss erstellen Sie die Netzwerkrichtlinie für konforme Clients: Klicken Sie dazu mit der rechten Maustaste auf den Konsoleneintrag "Richtlinien / Netzwerkrichtlinien" und wählen Sie im Kontextmenü den Befehl "Neu" aus. Geben Sie der Richtlinie eine Bezeichnung in der Form "Vollzugriff für NAP-konforme Clients" und klicken Sie auf "Weiter". Klicken auf der nächsten Seite "Bedingungen angeben" auf den Punkt "Hinzufügen" und wählen Sie als Option "Integritätsrichtlinien" aus. Klicken Sie nun auf "Hinzufügen". Wählen Sie die Richtlinie "NAP-konform" aus.

Auf der nächsten Seite des Fensters legen Sie den Netzwerkzugriff der Richtlinie fest. Wählen Sie hier "Zugriff gewährt" aus. Klicken Sie auf "Weiter", um zum Fenster "Authentifizierungsmethoden konfigurieren" zu gelangen. Deaktivieren Sie die Standardeinstellungen und aktivieren Sie noch die Option "Nur Integritätsprüfung für Computer durchführen". Klicken Sie auf "Weiter" und belassen Sie im nächsten Fenster alle Einstellungen wie sie sind. Klicken Sie nun im Fenster "Einschränkungen konfigurieren" ebenfalls auf "Weiter", wodurch Sie in das Fenster "Einstellungen konfigurieren" gelangen. Wählen Sie hier "NAP-Erzwingung" und stellen Sie sicher, dass die Option "Vollständigen Netzwerkzugriff gewähren" aktiviert ist. Schließen Sie nun die Erstellung der Richtlinie ab.

Ungesunde Clients aussperren

Nachdem Sie die Richtlinie für konforme NAP-Clients angelegt haben, sollten Sie eine Netzwerkrichtlinie erstellen, die den Netzwerkzugriff für nicht konforme Clients steuert. Gehen Sie dazu analog wie eben vor und weisen Sie der Richtlinie eine passende Bezeichnung zu. Wählen Sie diesmal als Integritätsrichtlinie die Richtlinie "Nicht-NAP-konform" aus. Auf der Seite "Zugriffsberechtigungen angeben" wählen Sie auch hier "Zugriff gewähren". Der Zugriff wird später noch eingeschränkt. Natürlich könnten Sie für sich auch die Option "Zugriff verweigert" auswählen, um den Clients die komplette Kommunikation zu untersagen. Allerdings sperren Sie in diesem Fall die Clients komplett aus dem Netzwerk aus.

Klicken Sie auf "Weiter", um zum Fenster "Authentifizierungsmethoden konfigurieren" zu gelangen. Deaktivieren Sie dort die Standardeinstellungen und aktivieren Sie noch das Kontrollkästchen "Nur Integritätsprüfung für Computer durchführen". Klicken Sie zweimal auf "Weiter", um zur Seite "Einschränkungen konfigurieren" und anschließend zur Seite "Einstellungen konfigurieren" zu gelangen. Dort klicken Sie auf "NAP-Erzwingung". Aktivieren Sie die Option

"Eingeschränkten Zugriff gewähren". Aktivieren Sie das Kontrollkästchen "Automatische Wartung von Clientcomputern aktivieren". Schließen Sie nun die Erstellung der Netzwerkrichtlinien ab. Damit sind die NAP-Einstellungen erledigt. Jetzt folgt die Konfiguration des DHCP-Servers unter Windows Server 2008 für die Network Access Protection.

Konfigurieren des DHCP-Servers für NAP

Im nächsten Schritt konfigurieren Sie den DHCP-Server unter Windows Server 2008, damit dieser NAP nutzen kann. Rufen Sie dazu über "Start / Verwaltung / DHCP" oder im Server-Manager die Verwaltungskonsole des DHCP-Servers auf. Auch über "Start / Ausführen / dhcpmgmt.msc" ist die Konsole erreichbar. Um DHCP für NAP zu konfigurieren, rufen Sie im Anschluss noch die Eigenschaften des Bereiches auf, den Sie zuvor erstellt haben. Wechseln Sie dann auf die Registerkarte "Netzwerkzugriffsschutz" und aktivieren Sie die Option "Für diesen Bereich aktivieren". Aktivieren Sie nun die Option "Netzwerkzugriffsschutz-Standardprofil" verwenden.

Anschließend können Sie den DHCP-Server so konfigurieren, dass NAP-konforme Clients eine IP-Adresse vom Server erhalten. Klicken Sie mit der rechten Maustaste auf den Konsoleneintrag "Bereichsoptionen" unterhalb des von Ihnen erstellten Bereiches und wählen Sie "Optionen konfigurieren" aus. Wechseln Sie nun auf die Registerkarte "Erweitert" und wählen Sie im Dropdown-Listenfeld "Benutzerklasse" die Option "Standardbenutzerklasse" aus. Jetzt können Sie die Optionen auswählen, die Ihren standardmäßigen NAP-konformen Clients zugewiesen werden sollen, zum Beispiel DNS-Server, WINS und DNS-Domäne.

Im folgenden Schritt müssen Sie den DHCP-Server so einrichten, dass nicht konforme NAP-Clients entsprechende IP-Adressen erhalten, damit sich diese mit den Wartungsservern verbinden oder nur teilweise mit dem Netzwerk kommunizieren können. Klicken Sie hierfür mit der rechten Maustaste auf den Konsoleneintrag "Bereichsoptionen" unterhalb des von Ihnen erstellten Bereichs und wählen Sie "Optionen konfigurieren" aus. Wechseln Sie auf die Registerkarte "Erweitert" und wählen Sie im Dropdown-Listenfeld "Benutzerklasse"

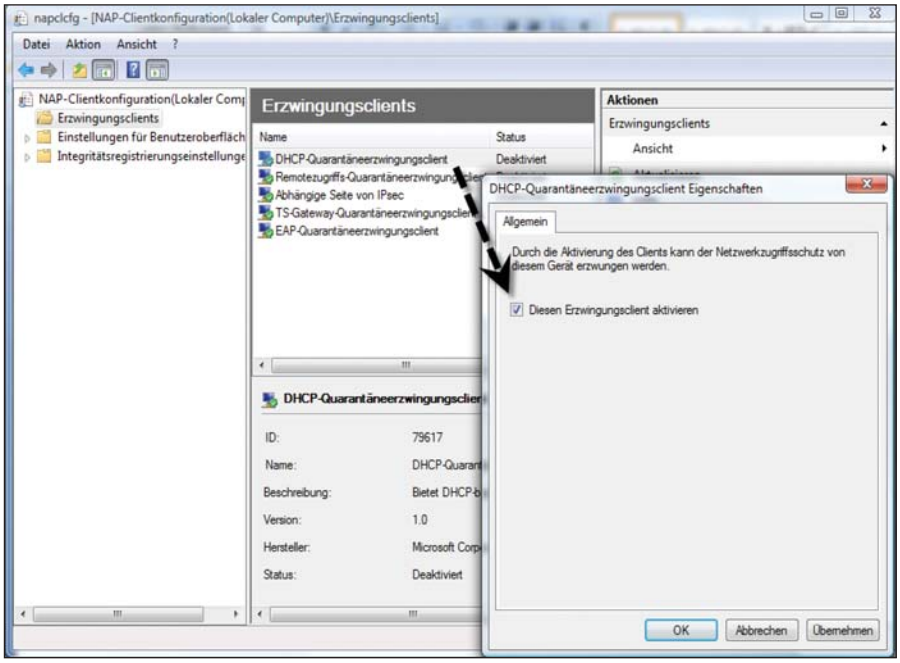


Bild 4: Aktivieren des DHCP-Quarantäneerzwingungsclients unter Windows Vista

die Option "Standardmäßige Netzwerkzugriffsschutz-Klasse" . Wählen Sie nun die Option "006 DNS-Server" aus und hinterlegen Sie die IP-Adresse Ihres DNS-Servers. Unter der Option "015 DNS-Domänenname" hinterlegen Sie jetzt als Namen einen DNS-Namen, zum Beispiel "restricted.contoso.com". Durch diese Konfiguration haben Sie sichergestellt, dass die konformen NAP-Clients eine vollständige Anbindung an das Netzwerk erhalten und die nicht konformen eingeschränkten Zugriff.

Sicherheitseinstellungen auf den Clients

Damit die Windows-Sicherheitsintegritätsverifizierung unter Server 2008 Daten empfangen kann, muss auf dem PC das Sicherheitscenter aktiviert sein. Das Center fragt die entsprechenden Daten auf dem PC ab und sendet diese zum NPS-Server. Auf Windows Vista-PCs, die Mitglied einer Domäne sind, wird das Sicherheitscenter deaktiviert. Um NAP unter Windows Vista zu testen, müssen Sie dieses daher aktivieren. Der beste Weg dazu in einer Testumgebung ist die Aktivierung über lokale Richtlinien.

Sie finden die Einstellung auch über Gruppenrichtlinien unter "Computerkonfiguration / Administrative Vorlagen / Windows-Komponenten / Sicherheitscenter". Aktivieren Sie die Richtlinie "Sicherheitscenter aktivieren (nur Domänencomputer)". Nun folgt die Aktivierung der DHCP-NAP-Unterstützung: Starten Sie dazu auf dem Vista-PC über "Start / Ausführen / napclcfg.msc" die Verwaltungskonsole des NAP-Clients. Klicken Sie in der Konsolenstruktur auf den Eintrag "Erzwingungsclients". Aktivieren Sie den "DHCP-Quarantäneerzwingungsclient".

Alternativ können Sie Erzwingungsclients für den Netzwerkzugriffsschutz auch über Gruppenrichtlinien aktivieren. Diese Einstellung finden Sie unter "Computerkonfiguration / Windows-Einstellungen / Sicherheitseinstellungen / Network Access Protection / NAP-Clientkonfiguration / Erzwingungsclients". Der nächste Schritt zur Anbindung von Windows an eine NAP-Infrastruktur ist die Aktivierung des Systemdienstes "NAP-Agent" (Network Access Protection). Setzen Sie nach Aufruf der Dienstekonsole über *Services.msc* den Starttyp dieses Dienstes auf "Automatisch" und starten Sie diesen. Durch die Einstellung in der Netzwerkrichtlinie, dass sich die angebundenen PCs automatisch warten sollen, wenn diese nicht NAP-konform sind, wird die Windows-Firewall immer wieder in Echtzeit automatisch aktiviert, wenn Sie diese deaktivieren. Dadurch ist sichergestellt, dass auch auf PCs, an denen Benutzer mit Administratorrechten sitzen, die Firewall immer aktiv ist. In regelmäßigen Abständen, vor allem bei der Anmeldung, erscheint im Infobereich der Taskleiste ein Hinweis, ob der Client den Netzwerkrichtlinien entspricht. Klicken Sie doppelt auf die Meldung oder das dazugehörige Symbol, erhalten Sie eine ausführliche Statusangabe anzeigt.

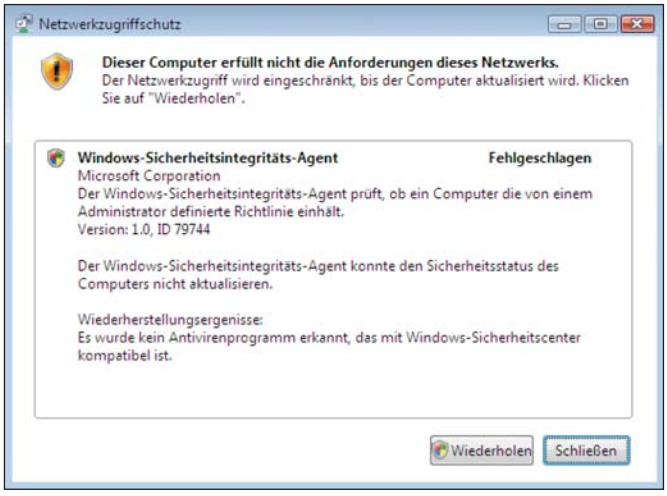


Bild 5: Überprüfung des Netzwerkzugriffsschutzes mit ausführlicher Statusmeldung

Da die Firewall immer wieder automatisch aktiviert wird, müssen Sie auf einem anderen Weg testen, ob auch die Konfiguration des DHCP-Servers funktioniert, der nicht konformen Clients den eingeschränkten Zugriff zur Verfügung stellt. Der einfachste Weg dazu ist, dass Sie die Systemintegritätsüberprüfung so abändern, dass der Client die Prüfung nicht mehr besteht. Mit dieser Änderung wird der Client durch die Integritätsrichtlinie zum nicht konformen Client erklärt und die Netzwerkrichtlinie schränkt den Zugriff ein. Rufen Sie zum Beispiel die Windows-Sicherheitsintegritätsüberprüfung auf und lassen Sie auf einem Test-PC noch den Virenschutz kontrollieren. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie in der NAP-Konsole auf "Netzwerkzugriffsschutz/Systemintegritätsprüfungen".
2. Öffnen Sie die Eigenschaften der Windows-Sicherheitsintegritätsverifizierung.
3. Klicken Sie im Fenster auf die Schaltfläche "Konfigurieren". Jetzt können Sie einstellen, welche Bedingungen eine Arbeitsstation erfüllen muss, damit diese mit dem Netzwerk kommunizieren darf.
4. Aktivieren Sie für diesen Test die Option "Antivirusanwendung ist aktiviert".
5. Klicken Sie auf "OK". Sie müssen keine weiteren Änderungen vornehmen. Die Einstellungen werden automatisch von den Integritätsrichtlinien und auch den Netzwerkrichtlinien übernommen.

Sie können den NAP-Status eines PCs in der Befehlszeile über den Befehl *netsh nap client show state* anzeigen lassen. Alle weiteren Ereignisse der NAP-Konfiguration finden Sie in der Ereignisanzeige. Die Ereignisse auf dem Client finden Sie in der Ereignisanzeige über "Anwendungs- und Dienstprotokolle / Microsoft / Windows / Network Access Protection / Operational". Auf dem Server finden Sie die Fehler im Systemprotokoll.

Netzwerkzugriffsschutz mit VPN

NAP macht vor allem für Clients Sinn, die sich per VPN einwählen. Bei diesen Rechnern können Administratoren standardmäßig nicht sicherstellen, ob ein Vi-

renschutz installiert oder die Firewall aktiviert ist. Mit NAP verhindern Sie so gezielt, dass sich unsichere Clients aus dem Internet mit Ihrem sicheren internen Netzwerk verbinden. Ähnlich wie bei NAP über DHCP können Sie auch bei NAP über VPN einen Netzwerkrichtlinienserver einsetzen, um Ihr Netzwerk effizient zu schützen. Die Domänencontroller lassen sich dabei noch unter Windows Server 2003 betreiben – nur der VPN- und der Netzwerkrichtlinienserver müssen unter Windows Server 2008 laufen. Bei der Einwahl verbindet sich der Client aus dem Internet mit dem RAS-VPN-Server. Dieser fordert, wie bei DHCP, ein Statement of Health (SoH) vom Client und gibt dieses an den Netzwerkrichtlinienserver weiter.

Auf Basis dieser Richtlinien erklärt der Server den Client dann entweder zum konformen oder zum nicht konformen NAP-Client und wendet die Richtlinien an. Auf dem Client sollte idealerweise Windows Vista oder mindestens Windows XP mit SP3 installiert sein. Optimal wäre auch der Einsatz einer internen Windows-CA. Die sichere Einwahl über VPN realisieren Sie am besten auch geschützt durch entsprechende Zertifikate, die Sie durch eine interne Windows-CA ausstellen lassen können. Für eine Testumgebung sollten Sie ein Beispielkonto anlegen und diesem Konto entsprechende Einwahlberechtigungen erteilen. Aktivieren Sie auf der Registerkarte "Einwählen" im Bereich "Netzwerkzugriffsberechtigung" die Option "Zugriff gestatten".

In einer produktiven Umgebung können Sie auch die Option "Zugriff über NPS-Netzwerkrichtlinien steuern" wählen. In diesem Fall erstellen Sie eine Gruppe im Active Directory, zum Beispiel mit der Bezeichnung "VPN-Zugriff", und nehmen die Benutzerkonten in die Gruppe mit auf, denen Sie VPN-Zugriff gestatten wollen. Auf dem NPS-Server können Sie dann dieser Gruppe die Einwahl gestatten. Dies hat den Vorteil, dass Sie nicht die einzelnen Benutzerkonten konfigurieren müssen, sondern über Gruppenmitgliedschaft die Einwahl steuern. Im nächsten Schritt sollten Sie dem NPS-Server ein Zertifikat zuweisen. Öffnen Sie hierfür über "Start / Ausführen / mmc" eine neue Konsole. Fügen Sie nun das Snap-in "Zertifikate" zu dieser Konsole hinzu und wählen Sie als Option für den Zertifikatespeicher des Snap-ins "Computerkonto" aus.

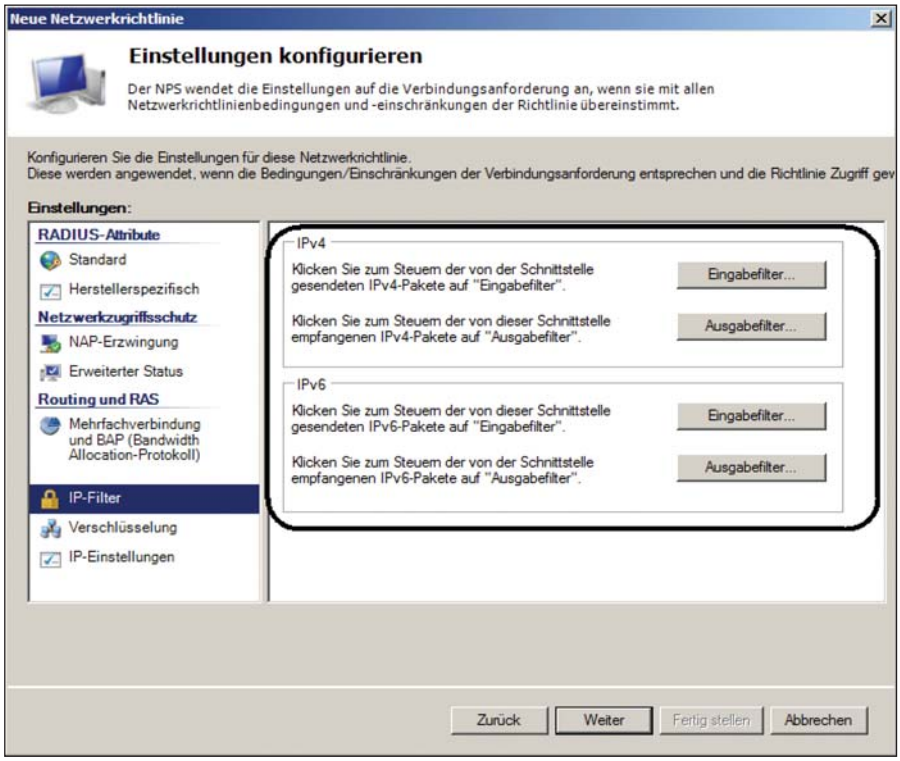


Bild 6: Das Erstellen von IP-Filtern für VPN-Clients zur NAP-Überprüfung ist für IPv4 und IPv6 möglich

Wählen Sie im nächsten Schritt den lokalen Computer aus und klicken Sie im Snap-in mit der rechten Maustaste auf "Eigene Zertifikate". Dort gehen Sie im Kontextmenü auf den Eintrag "Alle Aufgaben / Neues Zertifikat anfordern". Wählen Sie nun als Zertifikattyp "Computer". Haben Sie den NPS-Server auf einem Domänencontroller installiert, können Sie als Zertifikattyp auch "Domänencontroller" auswählen. Dieses Zertifikat verfügt über die gleichen Möglichkeiten, die ein Computer-Zertifikat beherrscht. Allerdings sollten Sie den NPS- und VPN-Server am besten auf einem getrennten Server installieren. Klicken Sie auf "Registrieren", um das Zertifikat anzufordern. Nach wenigen Sekunden sollte das Zertifikat als erfolgreich ausgestellt angezeigt werden.

Im Anschluss können Sie den NPS-Server konfigurieren. Starten Sie dazu die Verwaltungskonsole für die Netzwerkrichtlinien. Als Nächstes konfigurieren Sie die Systemintegritätsprüfungen exakt so, wie weiter vorne für NAP über DHCP. Im Anschluss erstellen Sie die gleichen Integritätsrichtlinien. Die Konfiguration der Systemintegritätsprüfungen und der Integritätsrichtlinien erfolgt komplett identisch. Wichtig an dieser Stelle ist die Konfiguration der Windows-Sicherheitsintegritätsverifizierung (Statement of Health, SoH). Diese wird vom Client durch das Sicherheitscenter an den Server übermittelt.

Damit sind die Konfigurationen des DHCP-Servers und der Windows-Clients abgeschlossen. Im dritten und abschließenden Teil unserer Workshopserie zeigen wir Ihnen, wie Sie unter Windows Server 2008 ein IPSec-VPN in Ihrer NAP-Umgebung einrichten. *(dr)*

Exchange Server 2003

Mailbox-Retter für den Verzeichnisdienst

von Robert Lindermeier

Die Hoffung, dass jeder Exchange-Administrator seine Umgebung vorschriftsmäßig sichert, wird in aller Regel erfüllt. Zu wichtig sind die Daten der E-Mailpostfächer für ein Unternehmen. Doch was geschieht, wenn zwar die Exchange-Datenbanken sauber und erfolgreich gesichert wurden, aber das Active Directory (AD) mit allen Benutzerkonten verloren geht? Üblicherweise wären die folgenden Schritte der Weg, um einem Active Directory-Ausfall in Umgebungen mit wenigen Postfächern zu begegnen:

- Active Directory neu aufsetzen und Konten neu anlegen
- Exchange-Server neu installieren
- Postfachspeicher-Datenbank aus Sicherung einspielen
- Jedes Postfach mit einem Benutzerkonto wieder verbinden

Gehen wir nun aber davon aus, dass Sie die Benutzerkonten nicht alle kennen und Sie sich die viele Handarbeit schenken wollen. Exchange 2003 speichert zu den Postfächern auch Daten über die zugeordneten Benutzerkonten aus dem AD. Diese Tatsache machen wir uns in diesem Workshop zunutze und zeigen auf, wie Sie aus einer Postfachdatenbank eines Exchange Server 2003 die zu den Postfächern gehörenden Benutzerkonten restaurieren – ohne die Konten von Hand neu anlegen zu müssen.

Hilfe von Microsoft

Für diese Art der Wiederherstellung bietet Microsoft Support ein Tool an, das bis Exchange 2000 auch auf der CD unter "Support \ Tools" mitgeliefert wurde: MBConn (*mbconn.exe*). Leider wurde das Werkzeug nicht mehr mit Exchange 2003 ausgeliefert, obwohl es auch in dieser Version prima funktioniert. Sie können es unter [1] direkt herunterladen.

Store mit verwaisten Postfächern bereitstellen

Der erste Schritt für die erfolgreiche Wiederherstellung der verwaisten Postfächer ist, die Postfachdatenbank aus der Datensicherung wiederherzustellen und auf einem neuen Exchange-Server bereitzustellen. Eine Exchange Server-Datenbank kann jederzeit auf einem anderen Exchange-Server bereitgestellt werden, sofern der Name der Organisation und der administrativen Gruppe identisch sind. Sollten Sie nicht oder nicht mehr wissen, wie die genaue Bezeichnung der Exchange-Organisation und der entsprechenden administrativen Gruppe war, können Sie dies mit dem nachfolgenden Befehl direkt aus der Datenbank extrahieren:

```
find "/ou=" priv2.edb
```

Nun erhalten Sie eine lange Liste der LegacyExchangeDN, aus der Sie eindeutig den Org- und Admingroup-Namen erkennen können, etwa

```
/o=YOUR-ADMIN/ou=Erste
  administrative Gruppe/cn=Reci-
  pients/cn=Hans.Meier
```

Mit diesen Angaben installieren Sie nun im neuen Active Directory eine neue Exchange-Organisation sowie Exchange-Server, die den betreffenden Namen entsprechen. Abschließend zeigt ein Blick mit dem Systemmanager unter "Postfachspeicher / Postfächer" alle Postfächer dieser Datenbank an, natürlich versehen mit einem roten Kreuz für "abgehängtes Postfach".

Benutzerdaten mit MBConn exportieren

Diese Daten der abgehängten Benutzer in dem betreffenden Postfachspeicher machen Sie sich nun mithilfe des Tools *Mbconn.exe* zunutze. Dazu starten Sie das Tool und verbinden sich im ersten Dialog mit dem betroffenen Exchange-Server und einem erreichbaren globalen Katalog.

Im nächsten Schritt wählen Sie den betreffenden Postfachspeicher aus – das Tool listet nun alle abgehängten Postfächer dieses Stores auf. Über den Menüpunkt "Actions / Export Users" erstellen Sie eine LDF-Datei, mit deren Hilfe Sie die benötigten Benutzerkonten per LDIF-

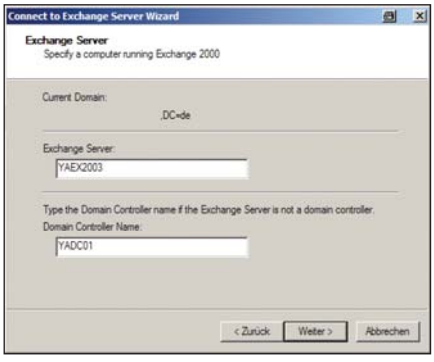


Bild 1: Über einen Wizard können Sie sich auf den Exchange-Server verbinden

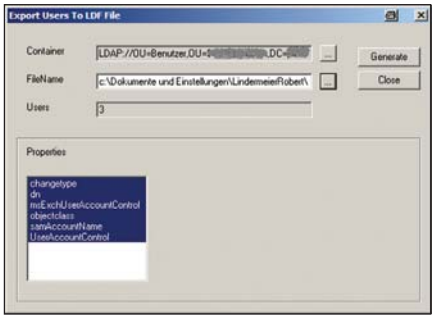


Bild 2: Ein Export in eine LDF-Datei ermöglicht es, die Benutzerkonten im Active Directory wieder anzulegen

DE im Active Directory anlegen. Dabei muss zwingend eine OU des Active Directory als Ziel für die zu erzeugenden Benutzerkonten angegeben werden. Durch einen Klick auf die Schaltfläche "Generate" erzeugen Sie nun im angegebenen Verzeichnis eine LDF-Datei, deren Inhalt per Editor bei Bedarf auch noch nachbearbeitet werden kann:

```
dn: CN=Lindermeier\, Robert,OU=
  Benutzer,DC=Your-Admin,DC=intern
changetype: add
UserAccountControl: 66048
msExchUserAccountControl: 0
displayName: Lindermeier, Robert
objectclass: user
samAccountName: RLINDERMEIER
```

Benutzerkonten mit LDIFDE anlegen

Die zuvor angelegte LDF-Datei wird nun als Vorlage für den Benutzerimport verwendet. Der nachfolgende Befehl erzeugt daraufhin in der angegebenen OU die benötigten Konten:

```
ldifde -i -f c:\temp\Users-to-
  recreate.ldf
```

Sollte der Fehler "Fehler in Zeile 1: Ausführung verweigert – Serverseitiger Fehler: 1325" auftreten, löschen Sie bei dem Benutzerkonto die Zeile "UserAccountControl: xxxxx".

Postfächer wieder verbinden

Der abschließende Schritt besteht darin, die verwaisten Postfächer mit den neu erzeugten Benutzerkonten zu verbinden. Dazu können Sie das Tool MBConn verwenden. Im Tool "Mailbox Reconnect" klicken Sie im Menü "Actions / Preview All" an, um für alle Postfächer das zugeordnete Konto zu finden. Alle Konten werden nun den Postfächern zugeordnet und im Active Directory wieder verbunden. Dazu wählen Sie das Kommando "Actions / Apply". Eine abschließende Meldung gibt Aufschluss über den Erfolg der Aktion. Natürlich könnte man auch die Postfächer über den Exchange System Manager einzeln zuordnen, aber das Tool macht die Angelegenheit natürlich einfacher, vor allem lässt sich damit in einem Zug eine ganze Liste an Postfächern wieder verbinden.

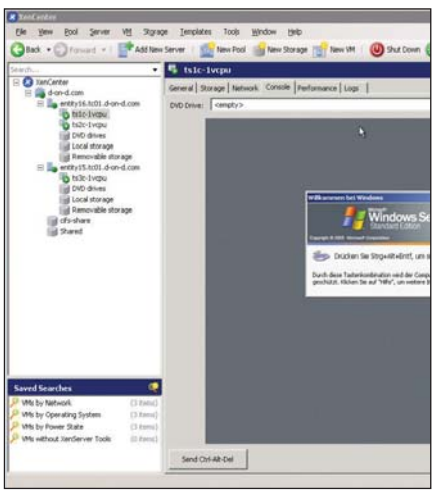


Bild 3: Über den Punkt "Preview All" sind alle Postfächer für das zugeordnete Konto sichtbar

Das Tool kann sowohl in Exchange 2000- als auch Exchange 2003-Umgebungen verwendet werden, jedoch nicht mehr unter 2007. Wie Sie Ihre Postfächer unter der neuen Exchange-Version wiederherstellen, beschreiben wir im nächsten Workshop. *(dr)*

Robert Lindermeier ist Inhaber und Geschäftsführer bei YOUR-ADMIN.

Links

[1] FTP-Download von MBConn
ftp://ftp.microsoft.com/PSS/Tools/Exchange%20Support%20Tools/MBConn/

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

In **Outlook 2007** habe ich mir mithilfe des Menüs **Ansicht** eine individuelle Konfiguration der verschiedensten Fenster zusammengestellt. Nun würde ich gerne wieder die Grundeinstellung herstellen, was mir aber auch nach längerem Herumspielen nicht gelungen ist. Habe ich eine Chance, Outlook von der Ansicht her zurückzusetzen?

Sie können Outlook 2007 mit einigen zusätzlichen Optionen starten. Schließen Sie das E-Mailprogramm und wählen Sie mit der Maus "Start / Ausführen" an. Geben Sie dann

```
outlook /cleanviews
```

ein. Outlook wird nun neu gestartet und die Standardansichten werden wiederhergestellt. Beachten Sie aber, dass sämtliche von Ihnen erstellten benutzerdefinierten Ansichten dabei verloren gehen. *(ln)*

Leider hat sich auch in unserem Netzwerk ein Server den mittlerweile weit verbreiteten Wurm **Conficker** eingefangen. Wie ich gehört habe, verbreitet sich der Schädling auch über eine Autostart-Datei, die von Windows beim Anschließen von Speichermedien wie USB-Sticks oder externen Festplatten ohne Zutun des Nutzers ausgeführt wird. Ist es irgendwie möglich, das Autostart-Feature zu deaktivieren, um wenigstens diesen **Verbreitungsweg zu stoppen**?

Es gibt eine relativ einfache Möglichkeit, um die Autostart-Funktion von externen Speichermedien abzuschalten. Öffnen Sie einen Texteditor und geben Sie folgende Anweisung ein:

```
REGEDIT4 [HKEY_LOCAL_MACHINE\SOFT-
  WARE\Microsoft\Windows NT\
  CurrentVersion\IniFileMapping\
  Autorun.inf]
```

Speichern Sie diese Datei unter dem Namen *autorun.reg* ab. Anschließend starten Sie diese Datei mit einem Doppelklick. Damit wird der Registrierungsdatenbank ein Eintrag hinzugefügt, welcher das Autostart-Feature unterbindet. Da Windows die Informationen aus der Autostart-Datei allerdings auch in einem Cache speichert, sollten Sie den Rechner nach der Durchführung der Registry-Änderung sofort neu starten. Steht Ihnen diese Möglichkeit nicht zur Verfügung, etwa weil es sich bei dem Rechner um einen produktives System handelt, können Sie auch den Eintrag in der Registry

```
HKEY_CURRENT_USER\Software\Micro-
  soft\Windows\CurrentVersion\Explo-
  rer\MountPoints2
```

löschen. *(ln)*

Gibt es eine Möglichkeit, mit einem einfachen Befehl alle auf einem Windows-System installierten **Treiber auszugeben**, ohne dass ich mich umständlich durch den Gerätemanager klicken muss?

Ab Windows 2000 können Sie sich mit dem Befehl *driverquery* alle auf dem Rechner vorhandenen Treiber anzeigen lassen. Dabei ermöglichen diverse Parameter, den Befehl nach Ihren Wünschen zu gestalten. Mit dem Zusatz "/s" und der Angabe der IP-Adresse eines Remote-Computers ist die Auflistung auch für einen entfernten Rechner kein Problem. "/v" liefert detaillierte Angaben über jeden installierten Treiber. Wer die Zusammenstellung auch später noch verwenden möchte, kann die Ergebnisse mit "/fo" und der Angabe eines entsprechenden Dateinamens auch exportieren. Der Befehl

```
driverquery /s 192.168.115.55 /v /fo
  csv > alldrivers.csv
```

gibt somit eine detaillierte Liste aller auf dem Gerät mit der obigen IP-Adresse vorhandenen Treiber aus und speichert diese in der genannten CSV-Datei, die Sie zur weiteren Verwendung beispielsweise mit Excel bearbeiten können. *(ln)*

Auf einem Rechner unter Windows XP funktioniert der **Internetzugriff** nicht mehr. Ich habe schon alles Mögliche ausprobiert, kriege den Zugang aber nicht mehr zum Laufen. Ich habe den Verdacht, dass

das TCP/IP-Protokoll beschädigt ist. Kann ich dieses irgendwie neu installieren?
Da TCP/IP eine Kernkomponente von Windows ist, können Sie dieses nicht entfernen. Sie können TCP/IP jedoch auf den Originalzustand zurücksetzen, indem Sie das NetShell-Dienstprogramm verwenden. Öffnen Sie die Eingabeaufforderung und geben Sie folgendes Kommando ein:

```
netsh int ip reset resetlog.txt
```

Der Befehl schreibt zwei Registrierungsschlüssel und gaukelt Windows so eine Neuinstallation von TCP/IP vor. Die Textdatei, in die das Tool die Ergebnisse des Resets loggt, ist zur Ausführung des Kommandos zwingend notwendig. *(ln)*

Linux

Vor kurzer Zeit habe ich das erste Mal erlebt, dass sich ein Linux-Server mit einer **Kernel Panic** aufgehängt hat. Leider musste ich mich dann vor Ort zum entfernten System begeben, um den Rechner neu zu starten. Hätte ich mir diesen Weg ersparen können? Besteht vielleicht eine Möglichkeit, den Server in so einem Fall **automatisch neu zu starten**?
Mit den entsprechenden Einstellungen bootet ein betroffener Linux-Rechner nach einer Kernel Panic automatisch neu. Fügen Sie dazu der Datei */etc/sysctl.conf* folgenden Eintrag hinzu:

```
kernel.panic = 15
```

Die Ziffer steht für die Anzahl der Sekunden, nach denen der PC nach einer aufgetretenen Kernel Panic neu startet. Beim Wert "0" findet kein automatischer Reboot statt. Wenn sie diesen jedoch verwenden, sollten Sie sicherstellen, dass ein Logging-Tool die Ursachen des Systemabsturzes aufzeichnet. *(ln)*

Ich möchte mir alle **Rechner in einem Netzwerk anzeigen** lassen, die schon einmal Datenpakete gesendet haben, will dazu aber keinen komplizierten Portscanner oder ähnliche Tools bemühen. Gibt es nicht einen einfachen Befehl, um **alle aktiven Computer samt MAC-Adresse** anzuzeigen?
Der entsprechende Befehl lautet *arp -a*. Als Resultat erhalten Sie eine Aufstellung, die die IP- und MAC-Adressen der aktiven PCs anzeigt. Ist Ihnen die IP eines Rechners bekannt, können Sie sich mit dem Befehl

```
arp -a {IP-Adresse}
```

nur die MAC-Adresse des einen gewünschten Netzwerkteilnehmers ausgeben lassen. *(ln)*

Apple

Auch wenn ich unter Max OS X einen **User aus dem System gelöscht** habe, bleibt dessen ehemaliges **Home-Verzeichnis** (/Users/Username) zurück, allerdings versehen mit dem Zusatz "gelöscht". Wie werde ich dieses Verzeichnis endgültig los? Ein manuelles Löschen funktioniert nämlich nicht.
Die in dem Verzeichnis befindlichen Daten bleiben deshalb erhalten, damit der Administrator bei Bedarf auch auf Dateien von bereits entfernten Usern zugreifen kann. Haben Sie für diesen Ordner absolut keinen Bedarf mehr, können Sie ihn löschen, indem Sie sich als Administrator anmelden, das Terminal öffnen und das Kommando

```
sudo rm -rf /Users/{Username} gelöscht
```

eingeben. Nach Eingabe des Admin-Kennworts sollte das Verzeichnis nun verschwunden sein. Falls es bei der Eingabe von "Gelöscht" Probleme mit der Tastatur geben sollte, tippen Sie einfach "gel??scht". Bei englischen Versionen von Mac erhalten die alten User-Verzeichnisse den Zusatz "deleted", dementsprechend müssen Sie beim obigen Befehl das deutsche durch das englische Wort ersetzen. *(ln)*

Über die Option "Archivieren und installieren" habe ich ein frisches **Mac OS X-System** installiert. Als ich die alten Benutzerdaten aus dem Verzeichnis "Previous Systems" von Hand in den neuen Privatordner schieben wollte, wurde dies mit dem Hinweis auf mangelnde Benutzerrechte abgelehnt. Wie bekomme ich **die alten Daten in den neuen Ordner**?
Um Probleme mit den Benutzerrechten auszuschließen, erstellen Sie von dem Benutzerordner, aus dem Sie Daten übernehmen möchten, einfach ein Disk-Image. Dies funktioniert mithilfe des Festplatten-Dienstprogramms über den Menüpunkt "Ablage / Neu / Image von Ordner". Das so erstellte Image öffnen Sie per Doppelklick und kopieren die Inhalte in den neuen Benutzerordner. Das System behandelt das Disk-Image wie eine externe Festplatte, auf der die Benutzerrechte ignoriert werden. Die Daten auf dem Image haben deshalb automatisch die Benutzerrechte des momentan aktiven Users. *(ln)*

CITRIX

Einer unserer **Citrix-Server** tut sich besonders durch **fortlaufende Performance-Probleme** hervor. Wir vermuten, dass dies irgendwie in Zusammenhang mit der auf dem Server installierten Symantec-Software für Endgeräte-Schutz zusammenhängt. Der betroffene Server wird deutlich langsamer oder antwortet gar nicht. Neben einer hohen Prozessorauslastung ist uns außerdem aufgefallen, dass die Prozesse *SmcGui.exe* und *ccApp.exe* wiederholt ausgeführt werden. Wo liegt hier das Problem?
Wie Sie richtig erkannt haben, wird das Performance-Problem dadurch verursacht, dass die Symantec-Software für

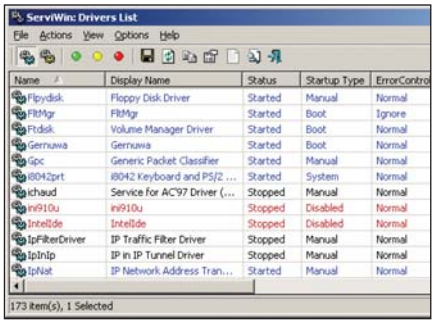
Endgeräte-Schutz wiederholt die oben genannten Prozesse ausführt – bei 64-Bit-Systemen betrifft dies zudem noch *ProtectionUtilSurrogate.exe*. Durch die Kombination dieser Prozesse vermindern sich die Server-Ressourcen deutlich. Der Hersteller hat im Upgrade "Symantec Endpoint Protection 11.0 Maintenance Release 3" den Fehler behoben. Deshalb sollten Sie unbedingt ein Upgrade auf diese oder eine höhere Version vornehmen. Der Citrix-Server sollte dann wieder mit gewohnter Leistung seinen Dienst verrichten. *(citrix/ln)*

Tools

Welcher **Treiber** verursacht die Probleme mit der Netzwerkkarte? Was ist das eigentlich für ein **Dienst**, der da auf dem Datenbankserver läuft? Welcher Treiber fehlt auf dem Notebook des Geschäftsführers? Diese und ähnliche Fragen gehören zum Supportalltag von Netzwerkverantwortlichen. Die Antworten zu finden ist jedoch häufig nicht gerade trivial. Und oft werfen die Antworten neue Fragen auf, etwa danach, wie sich der – unnötige –Dienst auf dem Datenbankserver denn nun stoppen lässt. **ServiWin** ist ein Tool, das die Antworten kennt.

ServiWin ist ein praktisches Tool, das eine Liste aller installierten Treiber und vorhandenen Dienste erstellt. Es stellt in einer Tabelle Produktnamen, Herstellerfirma, Versionsnummer und Kurzbeschreibungen für Dienste und Treiber bereit. Diese lassen sich einfach per Mausklick stoppen, starten, unterbrechen und fortsetzen. Das funktioniert nicht nur lokal, sondern auch über das Netzwerk. Darüber hinaus stehen dem Anwender Starteinstellungen wie "automatisch", "manuell" oder "nie" zur Verfügung. Ausgewählte oder auch alle Einträge lassen sich in die Zwischenablage kopieren oder als HTML-Datei exportieren. *(jp)*

Quelle:
www.nirsoft.net/utils/serviwin.html



Der Überblick über aktuelle Treiber und Dienste in ServiWin erleichtert das Trouble-shooting

Anwenderprofile unter Windows neigen dazu, im Laufe der Zeit beispielsweise durch Applikationseinträge zu wachsen. Und diese Daten verbleiben oftmals auch dann im Profil, wenn der Anwender sie längst nicht mehr benötigt oder nutzt. Besonders Einträge in der Registry widersetzen sich dabei oft hartnäckig allen Löschversuchen. Gerade in Unternehmensnetzen, in denen Profile typischerweise nicht an einen einzelnen Computer gebunden, sondern "roaming" sind, kann die Anhäufung von Daten in den Profilen den Systemadministrator vor massive Probleme stellen. Sepago stellt hier die Freeware **Profile Nurse** zur Lösung bereit.

Gerade wenn die Anzahl der Profile in die Hunderte oder gar Tausende geht, stellt schon die kleinste Anpassung der Profile eine Herausforderung dar, die der Admin oft mit aufwendigen eigenen Skripten realisieren muss. Profile Nurse erlaubt es nun, die Arbeit mit den Profilen zu automatisieren. Das Tool ermöglicht es, nicht mehr benötigte Dateien oder Registryeinträge zu löschen und somit auch Speicherplatz im "Lager" der Profile freizuräumen. Die genauen Aufgaben der Profil-Krankenschwester legt der Administrator in einem einfachen Konfigurationsfile fest und lässt diese Aufgaben dann auf die von ihm festgelegten Profile los.

So wird etwa die normalerweise enorm zeitintensive Aufgabe, ein neues Icon in alle Userprofile einzufügen, im Aufwand deutlich reduziert. Das Tool findet sich mit einer erfreulich umfangreichen Anleitung im Internet. *(jp)*

Quelle: http://blogs.sepago.de/tools/.

Der freie Hypervisor **XEN** bietet in seiner aktuellen Version Leistungsdaten, die es durchaus mit kommerziellen Lösungen aufnehmen können. Doch neben den nötigen Kenntnissen von Linux und XEN schreckt viele Administratoren der Mangel an **Verwaltbarkeit und Automatisierung** ab. Typische Aufgaben wie RAM-Anpassung, Speicher- und Netzverwaltung oder auch LVM-Snapshots deckt **Enomalism** über eine grafische Oberfläche ab und bietet darüber hinaus einen hohen Grad an Automatisierung.

Enomalism ist ein auf der Virtualisierungs-Engine Xen basierender Virtualisierungsserver mit komfortabler webbasierter Verwaltungsoberfläche. Virtuelle Maschinen können schnell erstellt und auf verschiedene Serversysteme verteilt werden. Ab Version 2.1. bietet das Werkzeug eine Importfunktion für existierende Xen-VMs und auch für KVMs (Kernel-based Virtual Machines). Ebenfalls neu ist der Umgang mit dem Autostart bei virtuellen Maschinen. Enomalism überwacht nun den Zustand der VMs und stellt ihn nach einem Neustart, der zum Beispiel durch einen Stromausfall verursacht wurde, wieder her.

Dabei stellt das "Control Center" die Zentrale der Verwaltungsplattform dar. Weitere Module lassen sich zum Teil auch einzeln betreiben. *(jp)*

Quelle: http://sourceforge.net/projects/Enomalism

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

Hochverfügbarkeit durch asynchrone Replikation bei CLS

Ausfallsichere Geldtransfers

von Joachim Brebeck

Gerade wenn es ums Geld geht, ist Hochverfügbarkeit in der IT unabdingbar. Bei der Cash Logistik Security AG (CLS) in Düsseldorf wacht permanente asynchrone Replikation über die hochsensiblen Daten. Diese Methode eignet sich für Server in kleinen Betrieben wie auch in Großunternehmen.

Zwischen 9 und 11 Uhr morgens wird es besonders kritisch: In diesem Zeitraum laufen bei der Cash Logistik Security AG (CLS) in Düsseldorf die meisten Aufträge ein. Und die sind nicht nur wichtig, sondern auch eilig, denn die schnelle und effiziente Umwandlung von Bar- in Buchgeld ist Geschäftszweck und Markenzeichen von CLS.

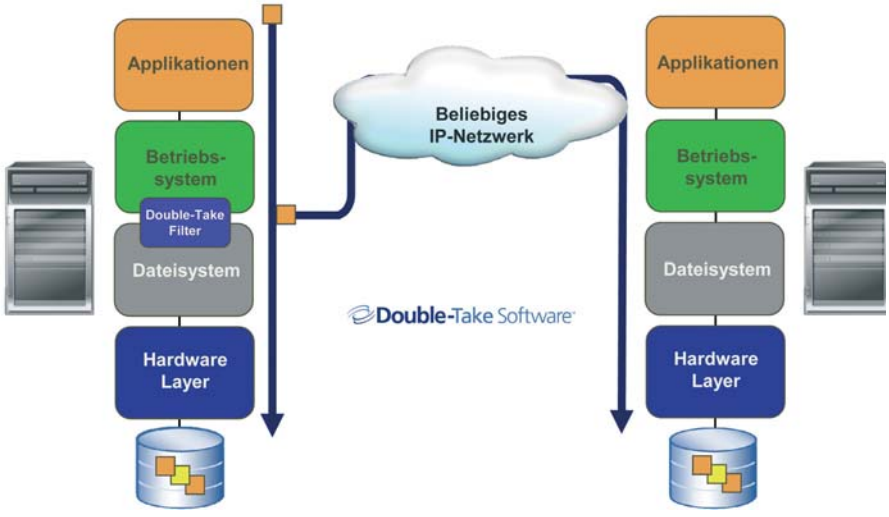


Bild 1: Die asynchrone Replikation fängt geänderte Daten zwischen Betriebssystem- und Dateisystemebene ab und leitet sie sofort an das Zielsystem weiter, ohne dass das Programm auf eine Bestätigung wartet

Keine Pause um halb zehn

Morgens um halb zehn herrscht bei CLS bereits Hochbetrieb. Nicht nur für die Mitarbeiter – auch die IT-Systeme dürfen sich jetzt keinesfalls eine Auszeit erlauben. Erhebliche Verzögerungen in den ausgefeilten Logistikprozessen oder bei Buchungsvorgängen wären die unvermeidliche Folge.

Der IT-Verantwortliche vor Ort, Marcus Brandt, Leiter EDV Organisation/Entwicklung bei CLS, stellt fest: "Natürlich sind Ausfälle oder gar Datenverluste immer ein großes Problem, aber in unserer Hauptzeit am Vormittag wären sie ganz besonders gravierend". Einige kritische Anwendungen laufen deshalb von vornherein im bestens gesicherten Rechenzentrum der Partnerbank, doch auch für den zentralen Windows-Server im eigenen Haus wurde bei stetig zunehmendem Daten- und Transaktionsvolumen eine Hochverfügbarkeitslösung immer wichtiger.

Vor der Einführung einer Hochverfügbarkeitslösung sicherte CLS seine Daten lediglich in einem Dualserverbetrieb ab, wobei Brandt beim Ausfall des primären SBS auf die Rücksicherung angewiesen war und somit einen möglichen Datenverlust in Kauf nehmen musste.

Auch Cluster bieten keine vollständige Sicherheit

Um den Schutz und die Verfügbarkeit von Daten zu verbessern, gibt es zahlreiche Ansätze. Einerseits lassen sich Systemarchitekturen natürlich von Grund auf redundant auslegen. Doch auch das schützt nicht vor Ausfällen, die durch Systemüberlastung, Benutzer, Applikationen oder lokale Katastrophen verursacht werden, und gerade das sind die häufigsten Gefahren. Zudem sprengen vollständig redundante Umgebungen fast jedes IT-Budget.

Auch lokale Microsoft-Cluster erhöhen die Verfügbarkeit, erfordern aber identische Serverkonfigurationen und Enterprise- oder Datacenter-Versionen von Windows Server. Und das geht ordentlich ins Geld. Zudem sind solche Cluster nicht für echtes Disaster Recovery geeignet, da sie sich am selben Ort befinden. Brennt es dort, sind alle Daten verloren. Das gemeinsam genutzte Plattensubsystem ist außerdem ein "Single Point of Failure". Selbst wenn sie also für mehr Sicherheit sorgen, sind Microsoft-Cluster also kein Allheilmittel.

Daten physikalisch auslagern

Die Überlegungen bei CLS führten daher zu der Einschätzung, dass das Backupsystem räumlich getrennt vom produktiven

Server zu installieren ist, etwa in einem sicheren Rechenzentrum oder einer anderen Niederlassung. Dann ist mit geeigneten Replikationstechniken eine schnelle Wiederherstellung der aktuellen Datenbestände oder der Ersatz des ausgefallenen Produktiv-Servers durch das Replikat möglich. Auch wer sich "nur" gegen Hardwaredefekte absichern will, sollte besser vorsorgen als mit den oft unzuverlässigen und nicht aktuellen Tape-Backups.

Bei der Replikation wird einmalig der gesamte Datenbestand auf einem entfernten Array gespiegelt; anschließend wird diese Kopie immer dann aktualisiert, wenn sich im Original etwas ändert. Da auch hier auf Platten gesichert wird, ist Replikation ein sehr zuverlässiges Verfahren, das zudem eine sehr schnelle und praktisch simultane Datensicherung zulässt.

Synchrone Replikation

Bei der synchronen Replikation fängt die Software Schreibzugriffe ab und sendet sie gleichzeitig an das primäre und sekundäre Array. Erst wenn beide den Empfang bestätigt haben, akzeptiert das Programm den nächsten Write Request. Beide Speicher haben also immer exakt denselben Stand, Datenverluste sind somit praktisch ausgeschlossen. Allerdings können die erforderlichen Bestätigungen zu deutlichen Performance-Verlusten führen, besonders wenn viele Transaktionen auf einmal stattfinden. Auf ein normales Büro übertragen hieße synchrone Übertragung: Wer einen Brief oder eine Mail verschickt, ruft jedes Mal beim Empfänger an und fragt, ob die Nachricht auch wirklich angekommen ist.

Synchrone Replikation lässt den Traffic im Netz stark ansteigen und erfordert daher oft schnelle und teure Fibre Channel-Verbindungen, die sich nur bis zu einer Entfernung von etwa 16 Kilometern sinnvoll einsetzen lassen. Die synchrone Replikation eignet sich daher eher für lokale Backups – und für üppige Budgets.

Asynchrone Replikation

Bei der asynchronen Replikation werden Write Requests des Betriebssystems zunächst an das lokale Array weitergereicht und erst nach dem Schreibvorgang auf das sekundäre entfernte Array kopiert. Dabei wartet die Anwendung nicht auf Bestätigungen, sondern fährt unmittelbar mit den nächsten Daten fort. Die Auswirkungen auf die Performance sind dabei minimal. Daher kann asynchrone Replikation effektiv und wirtschaftlich auch über vergleichsweise langsame WAN-Verbindungen betrieben werden.

Asynchrone Replikation ist natürlich nicht ganz so verlustfrei wie die synchrone Variante. Für eine Recovery Point Objective im Bereich weniger Minuten und eine Wiederherstellungszeit im Sekundenbereich reicht sie aber allemal. Für die meisten Unternehmen ist das völlig akzeptabel, und für diese ist die asynchrone Replikation die Lösung mit dem besten Preis-Leistungs-Verhältnis. Das gilt auch für CLS.

Datenübertragung und Failover

Wichtig ist dabei natürlich, dass nicht auf File-Ebene repliziert wird. Sonst würden umfangreiche Dateien auch nach minimalen Änderungen jedes Mal komplett übers Netz geschaufelt. Die Performance-Vorteile des asynchronen Verfahrens wären dann schnell dahin. Moderne Hochverfügbarkeitslösungen schicken daher – nach der einmaligen Vollsicherung zu Beginn – nur noch geänderte Daten über die WAN-Verbindung. Übertragen werden tatsächlich nur diejenigen Bytes, die auf dem Primärsystem modifiziert wurden. Je nach Umgebung ist damit eine Replikation sogar über Standard-Internetverbindungen wie SDSL oder gar ADSL möglich, wobei IT-Verantwortliche die Daten via VPN-Tunnel vor unbefugten Zugriffen schützen können. So kann die Recovery-Struktur ohne großen Aufwand mitwachsen, wenn neue Filialen hinzukommen.

Bild 2: Marcus Brandt, Leiter EDV Organisation/Entwicklung bei CLS

Da die generische Replikation lediglich I/O-Requests abfängt und übermittelt, ist sie auch völlig unabhängig von Applikationen und Hardware. Das Zielsystem muss in keiner Weise mit dem produktiven System identisch sein. Zudem werden durch Replikation auch offene Dateien wirkungsvoll gesichert, was etwa bei Exchange-Servern oder SQL-Datenbanken zwingend erforderlich ist.

Mit asynchroner Technik lassen sich sowohl mehrere Systeme auf eines replizieren als auch umgekehrt. Die Failover-Zeiten im Falle einer lokalen Störung sind dabei sehr kurz. Da alle Daten einschließlich offener Dateien in Echtzeit auf das Zielsystem übertragen werden, kann dieses sofort an die Stelle des ausgefallenen Servers treten. Dazu muss es nur dessen Namen und IP-Adresse übernehmen.

Voraussetzung ist natürlich, dass auf dem Zielsystem die gleichen Applikationen laufen wie auf dem zu sichernden. Zudem muss das Zielsystem überhaupt Client-Anfragen unter der vom Quellserver übernommenen IP-Adresse entgegennehmen können. Subnetze und Namensauflösung müssen daher entsprechend konfiguriert sein.

Replikation im Praxistest

Die klaren Vorteile der asynchronen Replikation erkannte auch Marcus Brandt schnell. Nach einigen Vorgesprächen nahm er Anfang 2008 das Angebot an, unverbindlich eine speziell auf den SBS-Server abgestimmte Version der Hochverfügbarkeitslösung Double-Take zu testen. Dazu installierte Brandt die Software sowohl auf seinem Produktiv-Server als auch auf einem Standby-System. Die Konfiguration war mit wenigen Mausklicks und in etwa fünf Minuten erledigt. Anschließend wurden noch die zu sichernden Daten auf das Zielsystem kopiert, und die Lösung konnte in Betrieb genommen werden.

Da Double-Take vollkommen anwendungsunabhängig arbeitet und auch offene Dateien zuverlässig sichert, waren nicht einmal Agenten für Exchange, SQL oder SharePoint vonnöten. Brandt prüfte auch andere Lösungen am Markt, doch hinsichtlich des Preises für eine SBS-Lösung fielen ähnliche Produkte von Symantec oder CA aus der Auswahl.

Recovery in Minuten

"Es stellte sich schnell heraus, dass dies unsere Lösung sein würde", so Brandt über seine ersten Erfahrungen mit Double-Take. "Die Replikation erfolgt praktisch in Echtzeit, sodass selbst bei einem Platten-Crash keine Datenverluste zu erwarten sind." Zudem ergab der Test der Failover-Funktionalität, dass der Zielserver sofort sämtliche Aufgaben des produktiven Systems übernimmt, nachdem die erforderlichen Services gestartet wurden. Selbst nach Abziehen des Netzwerkkabels vom produktiven Server konnten die Anwender innerhalb weniger Minuten weiterarbeiten. Doch nicht nur die Funktionalität überzeugte Brand: "Wichtig war uns auch die einfache Konfiguration und Verwaltung. Es ist gut zu wissen, dass man in wenigen Minuten einen Failover durchführen kann, wenn es einmal erforderlich ist."

Ebenfalls für Double-Take sprach die Tatsache, dass das Zielsystem, anders als bei einer Cluster-Lösung, nicht identisch mit dem zu sichernden System sein muss, sondern eine völlig andere Konfiguration haben kann. So musste CLS nicht gleich zwei komplett neue Server anschaffen, sondern konnte das vorhandene System weiter nutzen. Ein neuer Server dient nun als Produktivsystem, während die ältere Maschine auf "standby" steht, um im Falle eines Falles ihre frühere Tätigkeit wieder aufzunehmen. Damit dies nicht bei jedem kleinen Netzwerkproblem automatisch passiert, nutzt CLS dabei die Option, den Failover nach einer Alarmierung manuell einzuleiten.

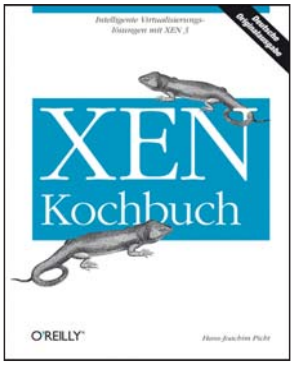
Nach dem erfolgreichen Test entschied sich CLS für die Übernahme von Double-Take in den produktiven Betrieb. Heute sichert CLS ein Volumen von etwa 500 GByte strukturierter (SQL) und unstrukturierter Daten sowie den Inhalt aller Exchange-Mailboxen auf den Backupserver. Dabei werden an einem normalen Arbeitstag tatsächlich nur etwa 4 bis 5 GByte repliziert, da ja nur die Änderungen im Datenbestand übertragen werden. Für das GBit-Ethernet des Unternehmens bedeutet dies eine sehr geringe Belastung; dennoch plant die CLS eine dedizierte Verbindung zwischen den beiden Servern, um auch bei steigendem Datenvolumen die Netzwerklast zu minimieren.

Fazit

Ein gutes halbes Jahr nach der Erstinstallation ist Marcus Brandt vollauf zufrieden mit Double-Take für SBS: "Nach ein paar anfänglichen Problemen, die letztlich durch einen Patch gelöst werden konnten, läuft die Replikation vollkommen problemlos und ressourcenschonend. Und wenn es doch einmal ein Problem gibt, werden wir schnell und kompetent unterstützt, und das Ganze im Rahmen unseres normalen Wartungsvertrages." Abgesehen von der Testphase ist bei CLS der Ernstfall noch nicht eingetreten. "Aber sollte er eines Tages kommen, werden wir innerhalb weniger Minuten wieder produktiv sein", so Brandt. *(jp)*

Joachim Brebeck ist Marketingmanager bei DoubleTake.

Xen Kochbuch



Nun kommen sie langsam auf den Markt, die Xen-Bücher. Höchste Zeit, der Hypervisor gilt als ausgereift und stabil, dem Unternehmenseinsatz steht eigentlich nichts im Weg. Außer vielleicht eine solide Anleitung für den Administrator, der sich lieber mit einem Buch in den Händen als mit ausschweifender Internet-Recherche ans Werk machen will. O'Reillys Kochbücher handeln normalerweise auf wenigen Seiten spezifische Problemstellungen ab, die sich aus der praktischen Anwendung ergeben. Hans-Joachim Pichl zweckentfremdet das Konzept hier kurzerhand. Soll Xen aus den Sourcen kompiliert und installiert werden, erklärt er das einfach zum Problem und präsentiert die Lösung als Fließtext dahinter. Das Ergebnis ist zwar mehr Buch als Kochbuch, aber am Inhalt gibt es nichts auszusetzen. Erfreulicherweise hält er den Theorieteil mit Historie und Grundlagen sehr kurz. Danach geht es sofort mit der Installation von Host und Gästen los. Kein Zweifel, das ist ein Praxisbuch par excellence. Der technische Level ist hinsichtlich Linux einigermaßen anspruchsvoll, am Anfang reichen geringe Kenntnisse aus, später, bei Kapiteln wie Hochverfügbarkeit, sollte man schon sehr sicher im Linux-Sattel sitzen.

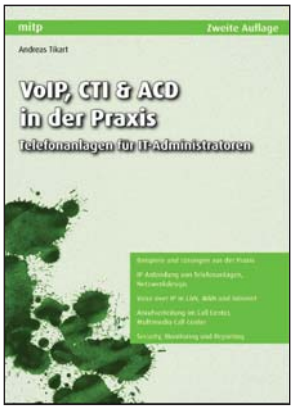
Die Mühe, die sich Picht mit der Vorarbeit gemacht hat, kann man nur loben. So sind die Kochrezepte fast durchgehend für vier Distributionen – Ubuntu, Debian, OpenSuse und Fedora – beschrieben, natürlich immer samt Erklärung der Differenzen. Auch der Umfang ist richtig gewählt. Gerade wer mehr mit Xen machen will als mal ein Windows unter Fedora zu starten, für den sind Themen wie Backup, automatisierte Installation und Migration wichtig. Denen widmet der Autor jeweils ein eigenes Kapitel. Wenn ein Bereich mehr Aufmerksamkeit vertragen könnte, dann sind es die grafischen Oberflächen zur Xen-Verwaltung.

Fazit: Praxisgerecht und umfassend, mehr kann man von einem Buch für Administratoren nicht erwarten – ein Standardwerk für angehende Xen-Admins.

Elmar Török

Autor:	Hans-Joachim Picht
Verlag:	O'Reilly
Preis:	39,90 Euro
ISBN:	978-3-89721-729-4
Bewertung:	★★★★☆

VoIP, CTI & ACD in der Praxis



Wenn Ihnen die Abkürzungen des Buchtitels mit Ausnahme von VoIP nichts sagen, gehören Sie ziemlich sicher zur angedachten Zielgruppe. Andreas Tikart möchte Administratoren aus der Netzwerkwelt helfen, mit Konzepten und Terminologie der Telekommunikationsbranche zurechtzukommen. Das ist eine gute Idee, denn trotz des Einzugs der IP-Technik in die Welt von ISDN und TAE stehen sich beide Seiten mit einem gewissen Unverständnis gegenüber. In größeren Unternehmen sind die entsprechenden Abteilungen streng getrennt, in kleinen Firmen kommt der IT-Admin oft in die Verlegenheit, auch TK-Wartungs- und Konfigurationsarbeiten durchzuführen. Gut, wenn er sich vorher mit diesem Buch beschäftigt hat. Mit dem kompakten, etwa 250 Seiten starken Werk erhält er eine kompetente und vor allem sehr auf das Relevante beschränkte Kurzanleitung. Insgesamt geht es hier um die grundlegenden Begriffe und Prinzipien, Details im Sinne der Umsetzung lässt der Autor weitgehend aus. Lediglich bei den Themen Callcenter und automatischer Rufverteilung (ACD) gibt es einige Skripte zu sehen. Ob IT-Administratoren allerdings etwas mit der Programmierung von Anrufverteilung und Queue-Management im Callcenter zu tun haben (wollen), ist fraglich.

Abgesehen von diesem Bereich sind in Tikarts Buch aber fast durchgehend relevante Dinge zu finden. Ob das Feature Access Codes sind oder verschiedene TK-Infrastrukturen, der Autor führt mit viel Fachwissen und einer flotten Schreibe durch die Kapitel. Weil die Themen nicht zu sehr ins Detail gehen, lässt sich das Buch in einem Sitz durchlesen, allerdings gibt es ein paar Anhänge mit Pinbelegungen und Feature Access Code-Listen, die auch als Nachschlagewerk eine gute Figur abgeben. Leider hat der Verlag auf ein Stichwortverzeichnis verzichtet – das macht die Suche nach einzelnen Begriffen unnötig schwer. Und auch wo es um VoIP geht, könnten die Kapitel etwas ausführlicher sein. So gibt es zwar eigene Abschnitte zu SIP und H.323, Erläuterungen zu Jitter oder Latency und die Ursachen dafür fehlen jedoch fast vollständig.

Fazit: Ein ideales Buch für IT-Admins, die sich in Telefonanlagen und TK-Konzepte einlesen wollen. Für die praktische Umsetzung geht der Text nicht tief genug, aber der Überblick wird mustergültig vermittelt. *Elmar Török*

Autor:	Andreas Tikart
Verlag:	mitp
Preis:	34,95 Euro
ISBN:	978-3-8266-5901-0
Bewertung:	★★★★☆

www.regedit.com

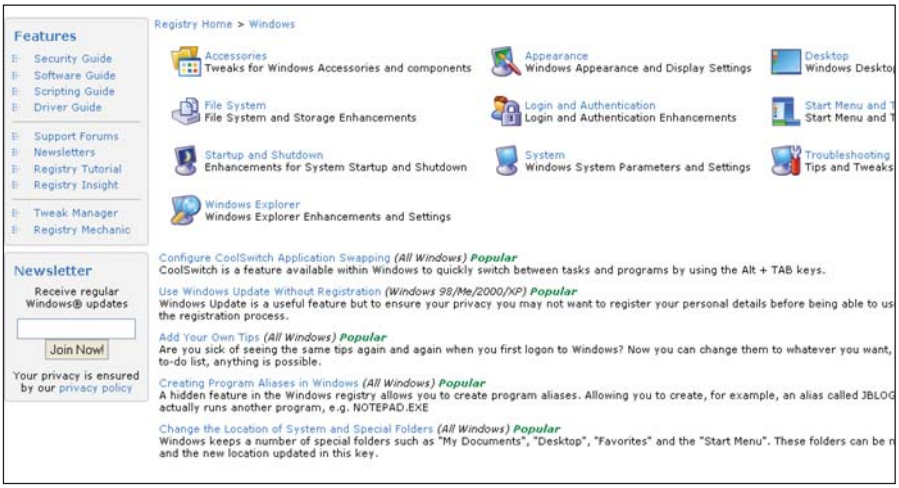
Windows Insider

Trotz aller Weiterentwicklungen, die Windows-Betriebssysteme im Laufe der Jahre erfahren haben, bleibt die Registrierdatendank – Registry – das alles entscheidende Konfigurationsverzeichnis. Darin finden sich alle Einstellungen zur Systemsteuerung und somit ist die Registry ein wichtiger Anlaufpunkt für Systemadministratoren, die Windows-Systeme optimieren oder troubleshooten. Doch gleichzeitig kommt die Registry ohne Netz und doppelten Boden daher und der Administrator ist gut beraten, genau zu wissen, was dieser oder jeder Eintrag bewirkt.

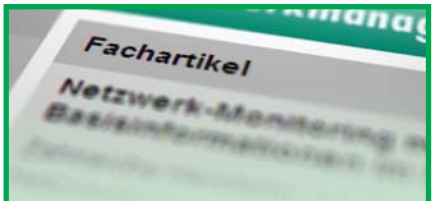
Das bekannte Entwicklungshaus für Sicherheits- und Supportwerkzeuge "PC Tools" bietet auf seiner Website einen Leitfaden zum Arbeiten mit der Windows-Registry. Nach Angaben der Site beziehen sich die dargebotenen Informationen auf die Windows-Versionen NT, 2000, XP sowie Vista. Den Einstieg findet der interessierte Netzwerkverwalter dabei – sofern notwendig – in der grundlegenden Erklärung zur Struktur der Konfigurationsdatei. Hier erklärt die Site zunächst den Aufbau und das Editieren der Registry, den Im- und Export einzelner Schlüssel sowie Backup und Restore.

Nach dem Studium des kurz gehaltenen Einsteigerleitfadens hat der Administrator dann die Wahl zwischen sechs Themengebieten: Hard- und Software, Netzwerk, Security, Windows OS und Tipps & Tricks. Innerhalb dieser Themen finden sich Unterverzeichnisse, die die Suche nach dem gewünschten Thema deutlich erleichtern. Denn die Suche, die die Site ebenfalls anbietet, scheint uns – vorsichtig ausgedrückt – optimierungsbedürftig. Auf der untersten Ebene eines jeden Themenbereichs findet sich dann eine Liste der zugehörigen "Registry-Tweaks". Diese erklären in aller Kürze, was der zugehörige Eintrag der Registrierdatenbank bewirkt und innerhalb welcher Parameter er sich sinnvoll modifizieren lässt. Hervorzuheben ist der Bereich "Software", weil sich auch Registry-Einträge finden, die über das reine Windows hinausgehen und beispielsweise den Internet Explorer und das Office-Paket behandeln.

Als Wermutstropfen bleibt abschließend nur festzustellen, dass der "Registry Guide" ausschließlich auf Englisch verfügbar ist (sollte er auf der deutschen Seite von PC Tools in übersetzter Form enthalten sein, ist die Redaktion dankbar für Hinweise – gefunden haben wir ihn dort leider nicht). Dafür finden sich in direkter Nachbarschaft aber zusätzliche Guides zu den Themen Security, Scripting, Software und Treiber. *(jp)*



Die gute thematische Gliederung erleichtert das Auffinden des richtigen Registry-Tipps enorm



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. **Im März erfahren Sie auf unserer Webseite mehr zu diesen Themen:**

Cloud Computing: Die Wolke hebt ab

Der klassische Arbeitsplatz-PC mit lokal gespeicherten und ausgeführten Anwendungen ist ein Auslaufmodell. Cloud Computing eröffnet die Chance, Anwendungen oder gar das Betriebssystem komplett ins Internet auszulagern. Im Online-Artikel zeigen wir Ihnen, welche Vorzüge die Wolke konkret bietet und was Unternehmen bedenken sollten, wenn sie diesen On Demand-Zugriff nutzen wollen.

www.it-administrator.de/themen/server_client/fachartikel/52002.html

Exchange Server 2007: POP3 und IMAP4 für den mobilen Verbindungsaufbau nutzen

Neben dem gängigen Zugriff auf das Postfach mit Outlook bietet Exchange Server 2007 auch die Möglichkeit, Nutzer per POP3 oder IMAP anzubinden. Dadurch lassen sich auch Programme wie Mozilla Thunderbird oder andere E-Mailtools zusammen mit Exchange betreiben. In diesem Online-Workshop zeigen wir Ihnen, wie Sie diese Verbindungsvariante reibungslos zum Laufen bekommen.

www.it-administrator.de/themen/kommunikation/fachartikel/52003.html

Job und Weiterbildung: Berufsschüler fit für die Märkte von morgen

Das Oberstufenzentrum Informations- und Medizintechnik in Berlin-Neukölln hat maßgeschneiderte Lehr- und Lernangebote der Cisco Networking Academy fest in sein Ausbildungsprogramm integriert. Lesen Sie in unserem Online-Beitrag, wie angehende IT-Fachkräfte in täglicher Praxiserfahrung dort Schlüsselkompetenzen erwerben können, die der Arbeitsmarkt dringend sucht.

www.it-administrator.de/themen/netzwerkmanagement/fachartikel/52005.html

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

»Trotz Komplexität immer Herr der Lage bleiben«

Arwed Kubisch (29) verstärkt seit einigen Monaten das Administratorenteam von Nordex. Das Unternehmen mit Sitz in Norderstedt und Rostock stellt Windenergieanlagen her. 1985 gegründet, ist der internationale Hersteller heute in 34 Ländern mit mehr als 3.600 Anlagen vertreten.

Welche Ausbildung haben Sie gemacht?

Ich habe eine abgeschlossene Ausbildung zum IT-Systemkaufmann.

Warum sind Sie IT-Administrator geworden?

Mich hat die IT mit ihren unterschiedlichen Facetten schon seit meiner Jugend interessiert. Und das Arbeitsgebiet des IT-Administrators ist in meinen Augen besonders interessant und vielseitig.

Welche IT-Umgebung betreuen Sie?

Als IT-Administrator bin ich in unserem Team für den lokalen Support verantwortlich. Darüber hinaus gehört das User-Management zu meinem Arbeitsbereich. Mit rund 25 Personen betreuen wir die gesamte IT-Landschaft der Nordex, die für etwa 2.000 Mitarbeiter im In- und Ausland benötigt wird. Dazu gehören auch die Mail- und Blackberry-Betreuung sowie die Administration von SAP oder der Local Support. Unsere IT-Landschaft umfasst weltweit etwa 75 Server, darunter File-, Exchange-, Backup- und DataBase-Server. Diese werden hauptsächlich durch Windows Server 2003 verwaltet.

Welches Netzwerk- und Systemmanagement setzen Sie ein?

Wir nutzen in unserem Netzwerk System Center Configuration Manager 2007 R2. Für das Server- und Komponenten-Monitoring setzen wir Whatsup Gold ein.

Welches Archivierungssystem nutzen Sie bei Nordex?

Das Unternehmen setzt zur Katalogisierung und Inventarisierung das Produkt Omnitracker von Omninet ein.

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

Es zeitlich allen recht zu machen, dabei auch einmal freundlich, aber bestimmt "Nein, das geht jetzt nicht, denn andere sind vor Ihnen dran!" zu sagen und nach Prioritäten zu differenzieren.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Derzeit arbeiten wir an der Migration des MS Project Server von der Version 2003 auf 2007. Hinzu kommt die rechtzeitige Fertigstellung und Lieferung größerer Mengen an IT-Equipment für die Kollegen im Ausland. Der Rest ist geheim.

Geburtstag:	08.12.1979
Familienstand:	ledig
Hobbys:	Freunde, Kraftsport, Langlauf, englische Literatur

Arwed Kubisch, IT-Administrator

Was macht Ihnen an Ihrem Job am meisten Spaß?

Mir gefällt der direkte persönliche Kontakt mit allen Ebenen des Unternehmens. Besonders schön sind die dankbaren Gesichter, wenn nach einem Zwischenfall die Technik wieder reibungslos läuft.

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

Die Fertigstellung und Lieferung des IT-Equipments gehört nicht zu meinen bevorzugten Aufgaben. Immerhin aber lernt man so fast jeden neuen Mitarbeiter persönlich kennen.

Was tun Sie für Ihre Fort- und Weiterbildung?

Ich informiere mich primär über das Internet auf den einschlägigen Seiten der Fachpresse. Darüber hinaus tausche ich mich mit Freunden und Kollegen aus, die wie ich Augen und Ohren offen halten. Pflichttermin ist seit elf Jahren einmal jährlich die CeBIT in Hannover. Ab 2009 stehen dann auch themenbezogene Schulungen auf der Agenda.

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

Ich habe einmal die fast zwei Jahre umfassenden geschäftliche E-Mail-Korrespondenz einer Person durch falsches Archivieren scheinbar dauerhaft gelöscht. Glücklicherweise stellte sich heraus, dass die Daten lediglich falsch abgelegt wurden.

Was war Ihr größter Erfolg als IT-Administrator?

Ich bin ja noch nicht allzu lange als IT-Administrator tätig, weshalb sich die richtig großen Erfolge hoffentlich noch einstellen werden.

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

Ein Klassiker war das scheinbar nicht funktionierende WLAN, wobei lediglich der Schalter am Notebook nicht umgelegt war.

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

Eine der größten Herausforderungen wird es sein, generell die immer komplexer werdende Software schnell zu verstehen und anwenden zu können. Dann müssen wir dafür sorgen, dass Unternehmen gut vor Hackern, Spam und Sabotage geschützt werden. Die Herausforderung für mich persönlich ist, bei der Komplexität der stetig neu hinzukommenden Programme immer Herr der Lage zu sein und trotz der wachsenden Zahl der Mitarbeiter für alle zeitlich erreichbar zu bleiben.

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 4/09 erscheint am 3. April 2009

Schwerpunktthema:

E-Mailmanagement

Im Test: Kerio Mailserver 6

Einkaufsführer: E-Mailumgebungen

Workshop: E-Mails unter Linux verwalten und archivieren

Workshop: Zarafa als Exchange-Alternative nutzen

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

Im **Mai** befassen wir uns mit dem Thema **Virtualisierung und Server-based Computing**. Dabei lesen Sie unter anderem, wie Sie Performance-Engpässe vermeiden und alte PCs in Thin Clients umwandeln. Außerdem beweisen der Thin Client CP20 sowie das Blade HC10 von IBM, was in ihnen steckt.

Als Schwerpunkt im **Juni** folgt dann das Thema **Clients – Sicherheit und Virtualisierung**.

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), *Volontär*
lars.nitsch@it-administrator.de

Birgit Lachmann, *Schlussredakteurin*
bi.lachmann@web.de

Autoren dieser Ausgabe
Petra Adamik, Joachim Brebeck, Thomas Drilling, Thomas Joos, Christian Knermann, Robert Lindermeier, Andreas Roscher, Elmar Török, Thomas Weyergraf, Bertram Wöhrmann, Ronald Wölfel

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

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

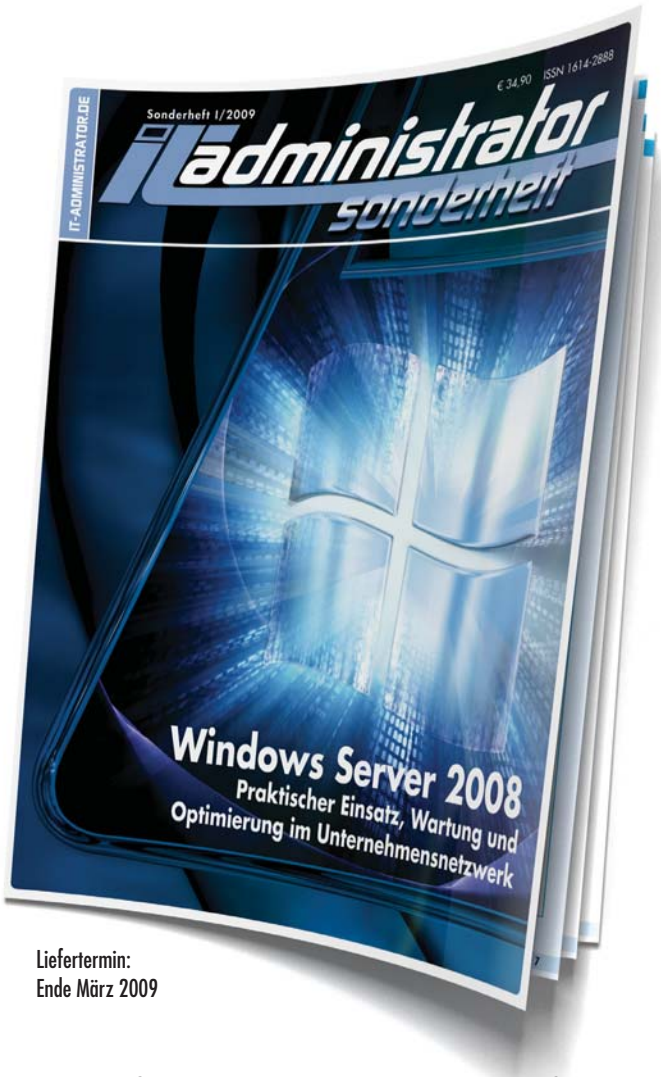
Bankverbindung für Abonnenten
Konto 174 966 462 bei der
Postbank Dortmund, BLZ 440 100 46
Kontoinhaber: Vertriebsunion Meynen

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



Liefertermin:
Ende März 2009

Bestellen Sie jetzt

das IT-Administrator

Sonderheft I/2009!

180 Seiten Praxis-Know-how rund um den

Windows Server 2008

zum Abonnenten-Vorzugspreis* von

nur € 29,90!

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

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

administrator
Das Magazin für professionelle System- und Netzwerkadministration

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

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

☐ **Ja**, ich bestelle das IT-Administrator-Sonderheft I/2009 zum Preis von **€ 34,90** inkl. Versand und 7% MwSt.

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

Ich zahle ☐ per Bankeinzug

Geldinstitut:

Kto.: BLZ:

oder ☐ per Rechnung

Datum:

Unterschrift:

Firma:

Name, Vorname:

Straße:

Land, PLZ, Ort:

Tel:

E-Mail:

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

ITA 0309

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

LANCOM

. . . connecting your business

Made
in
Germany

Das beste WLAN aller Zeiten!

Wireless LAN-Lösungen von LANCOM bereiten den Weg für eine neue Netzwerkdimension. Modernste Technologien, höchste Sicherheitslevels und herausragende Performance bieten Ihnen eine standortunabhängige Kommunikation mit ungeahnten Möglichkeiten. Drinnen wie draußen, in großen und in kleinen Netzen. Mit LANCOM vernetzen Sie Büros, Gebäude und mobile Mitarbeiter, leuchten Außengelände und Produktionsstätten aus. Kinderleicht, leistungsstark und sicher. Mit Bruttodatenraten bis 300 Mbit/s – bei voller Kompatibilität zu den gängigen 54 Mbit/s-Standards.

CeBIT
HANNOVER
3.–8.3.2009
HALLE 13
STAND C34

Professionelle **WLAN Access Points, Clients** und **Controller** vom deutschen Marktführer. Exzellenter Service, kostenlose Updates und Investitionsschutz inklusive.

LANCOM
Systems

www.lancom.de