

administrator

Das Magazin für professionelle System- und Netzwerkadministration

**Im Test:
Sterling Commerce
Connect:Direct 4.4**

14

**Im Test:
NetApp FAS 2020**

20

**Workshop:
Microsoft SQL Server für
das VirtualCenter einrichten**

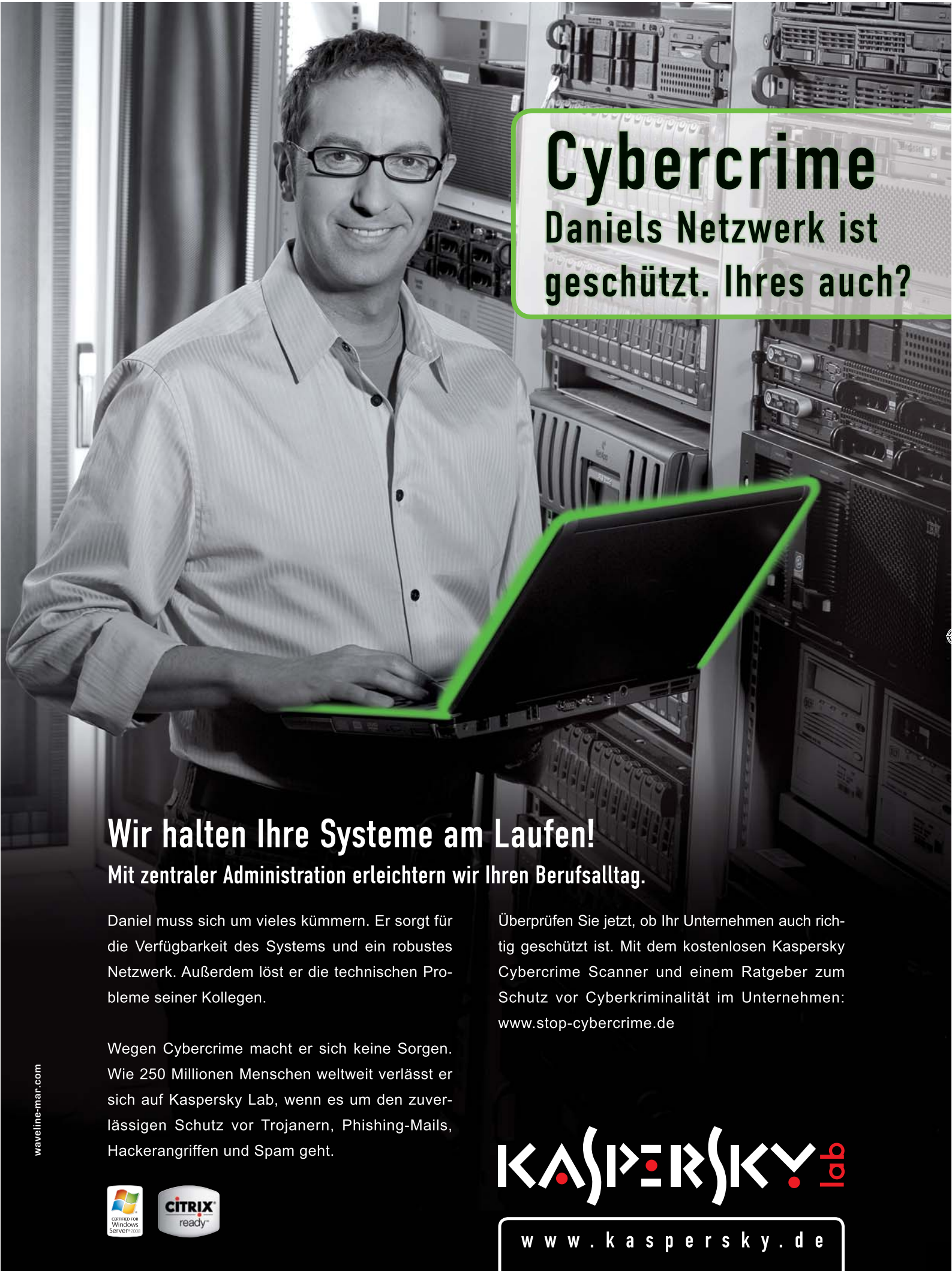
28

**Systeme:
Neuerungen im Dateisystem ext4**

39

Datei- und Datenbank- administration





Cybercrime

Daniels Netzwerk ist geschützt. Ihres auch?

Wir halten Ihre Systeme am Laufen!

Mit zentraler Administration erleichtern wir Ihren Berufsalltag.

Daniel muss sich um vieles kümmern. Er sorgt für die Verfügbarkeit des Systems und ein robustes Netzwerk. Außerdem löst er die technischen Probleme seiner Kollegen.

Wegen Cybercrime macht er sich keine Sorgen. Wie 250 Millionen Menschen weltweit verlässt er sich auf Kaspersky Lab, wenn es um den zuverlässigen Schutz vor Trojanern, Phishing-Mails, Hackerangriffen und Spam geht.

Überprüfen Sie jetzt, ob Ihr Unternehmen auch richtig geschützt ist. Mit dem kostenlosen Kaspersky Cybercrime Scanner und einem Ratgeber zum Schutz vor Cyberkriminalität im Unternehmen: www.stop-cybercrime.de



KASPERSKY lab

www.kaspersky.de

Verweigerungshaltung

Liebe Leser,

es lassen sich viele Gründe dafür finden, dass die vier großen Musikverlage ihre Musik wieder “frei” – ohne Digital Rights Management (DRM) – vertreiben:

So bezeichnete etwa Richard Stallman, Präsident der Free Software Foundation, DRM als “die Funktionalität, das Funktionieren zu verweigern” und formulierte so die Vorbehalte, die viele Verbraucher teilen. Neben der sehr mäßigen Kundenakzeptanz basiert der Rückzug vom DRM ebenso auf steigenden Kosten der Komponenten oder auch ungeklärten Fragen des Datenschutzes.



Ein Blick auf die Eckpunkte dieser Technik zeigt uns als zugrunde liegende Techniken die Verschlüsselung, digitale Wasserzeichen und eine Rechtedefinition. Diese drei Techniken wiederum erlauben vier Funktionalitäten: Zugangskontrolle, Nutzungssteuerung, Rechtesteuerung, Nutzungsabrechnung. Ja, holla die Waldfee, ruft der IT-Verantwortliche, altbekannte Grundpfeiler der IT-Sicherheit! Wenn wir uns jetzt noch vor Augen führen, wie wichtig der Schutz einzelner Dokumente gegen unbefugtes Einsehen, Kopieren oder Löschen heutzutage ist, wird ein Schuh draus: DRM wandert in die Unternehmen!

Zwar scheint es dazu notwendig, das “D” durch ein “E” zu ersetzen und das Kind nun Enterprise Rights Management zu rufen, doch unter der Haube tuckert der DRM-Motor. Welches mächtige Werkzeug IT-Verantwortlichen hier zur Verfügung steht, zeigt unser Beitrag ab Seite 60. Denn mit ERM verflüchtigen sich die Sorgen um USB-Sticks der Mitarbeiter oder die Bereitstellung eines DVD-Brenners. So wird das Verschieben der neuesten Konstruktionspläne auf einen USB-Stick *endlich* zu einer Funktionalität, die das Funktionieren verweigert.

Somit haben Administratoren neue Werkzeuge an der Hand, um die unerwünschte Bewegung von Daten über die Unternehmensgrenzen hinaus zu unterbinden. Doch auch das Gegenteil kann sich durchaus als Herausforderung darstellen: Große Datenmengen, deren Ankunft beim Empfänger außerhalb des Unternehmens zeitkritisch ist und deren Transport dennoch sicher vorstattengehen muss. Mit einiger Mühe lässt sich so ein Transport absichern, doch der “unterbrechungsfreie” Transfer stellt auch heutzutage noch ein Problem dar. Wir testen ab Seite 14 ein Werkzeug, das verspricht, die Dateien sicher zu ihrem Zielort zu transportieren.

Viel Vergnügen beim Lesen, Ihr


John Pardey
Chefredakteur

1&1 Sommer-Aktion:

**3 Monate
für 0,– €/Monat***



HOSTING

**3 Monate
für 0,– €/Monat***

Danach ab
14,99 €/Monat.*



SERVER

**3 Monate
für 0,– €/Monat***

Danach ab
99,99 €/Monat.*



E-SHOPS

**3 Monate
für 0,– €/Monat***

Danach ab
29,99 €/Monat.*

*Einmalige Einrichtungsgebühr 14,90 € (bei den Servern 99,- €), 12 Monate Mindestvertragslaufzeit, Preise inkl. MwSt.



Außerdem ständig weitere Preis-Aktionen im Internet:

**z. B. .info-Domain supergünstig und
ohne Einrichtungsgebühr!**

Jetzt informieren und bestellen unter:

01805 / 001 535 14 ct/Min. dt. Festnetz,
Mobilfunkpreise ggf. abweichend

www.1und1.info



1&1

INHALT

IT-Administrator – Ausgabe Juli 2009

Datei- und Datenbank-administration

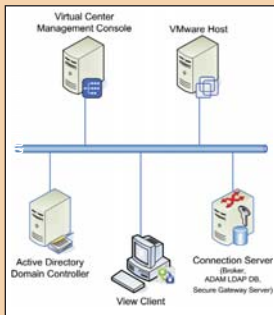
Im Test: Infowatch CryptoStorage

Geklaute Notebooks, ausspionierte PCs und entwendete Daten von Netzlaufwerken sind im Büroalltag keine Seltenheit. Einen wirksamen Schutz gegen unberechtigten Zugriff bietet eine geeignete Datenverschlüsselung. CryptoStorage von Infowatch eignet sich dabei für verschiedene Szenarien sowohl zur Absicherung des eigenen Arbeitsplatzes als auch zum Schutz gemeinsam genutzter Verzeichnisse. IT-Administrator hat das Tool für Sie getestet.



Seite 25

VDI mit VMware View einrichten (1/3)



Bislang war der Begriff Server-based Computing mit Terminalservern verbunden. Doch seit kurzem drängen Virtual Desktop Infrastructure-Lösungen der verschiedensten Hersteller in diesen Markt und hauchen dem etwas angestaubten traditionellen Ansatz mit Individualität, Innovation und Virtualisierung neues Leben ein. Wir zeigen Ihnen am Beispiel von VMware, wie Sie die komplexe neue Technik in den Griff bekommen.

Seite 44



Server- und Systemmanagement



Clientmanagement



Storage



Sicherheit



Messaging

Themenübersicht



Virtualisierung



Netzwerkmanagement



Job/Weiterbildung



Recht

AKTUELL

06 News

09 ITANet aktuell:

IT-Administrator-Workshop "Hochverfügbarkeit" am 16. Juli in Heidelberg
99,99 Prozent Workshop

10 IT-Administrator vor Ort:

2. Deutscher IPv6-Gipfel, 14. und 15. Mai 2009, Potsdam
Ideen für das neue Protokoll

12 IT-Administrator vor Ort:

11. IT-Sicherheitskongress des BSI, 12. bis 14. Mai, Bonn Bad-Godesberg
Sichere Wege zum Ziel

PRODUKTE

14  Im Test: Sterling Commerce Connect:Direct 4.4
Hochsichere Verbindung

20  Im Test: NetApp FAS2020
Storage und virtuelle Landschaft in einem

25  Im Test: Infowatch CryptoStorage
Schlanker Datentresor

PRAXIS

28  Workshop: SQL Server für das VirtualCenter von VMware einrichten
Sicherer Hafen für virtuelle Daten

34  Systeme: Microsoft EBS, SBS und Home Server im Vergleich
Ein ungleiches Trio

39  Systeme: Neuerungen im Linux-Filesystem ext4
Neue Strukturen schaffen

44  Workshopserie: Virtual Desktop Infrastructure mit VMware View einrichten (1/3)
Zentralisierung am Arbeitsplatz

50  Workshop: MySQL-Datenbankmanagement mit phpMyAdmin
Herr der Daten

55  Systeme: Exchange Server
Öffentliche Ordner migrieren

56 Tipps, Tricks & Tools

WISSEN

60  Know-how: Enterprise Rights Management
Integrierte Dokumentensicherheit im Unternehmen

63 Buchbesprechung
"Ubuntu Server" und "Security Monitoring"

64 Website & Fachartikel online

RUBRIKEN

03 Editorial

05 Inhalt

41 Seminarmarkt

65 Das letzte Wort

66 Vorschau, Impressum, Inserentenverzeichnis

Leisetreter

Mit der **Workstation 5000 Silent** bietet TAROX einen Rechner an, der durch eine hohe Grafikleistung sowie Schnelligkeit und Zuverlässigkeit überzeugen soll. Hierfür beinhaltet das Gerät einen NVIDIA Quadro FX470 Grafikkchip mit bis zu 512 MByte Cache sowie passiver Kühlung, der in das Mainboard integriert ist. Als CPU verbaut der Hersteller Intel Core2Duo E8400 Prozessoren mit 3 GHz. An Festplattenplatz stehen 320 GByte zur Verfügung. Um den Büroalltag nicht zu stören, verrichten die Rechner mit 28 dB(A) leise ihren Dienst. Die **Workstation 9500** ist daneben mit der integrierten NVIDIA-Grafikkarte Quadro FX 1800 ausgestattet, die für CAD-, DCC- und Visualisierungsanwendungen zertifiziert ist. Sie arbeitet mit der parallelen NVIDIA CUDA-Prozessorarchitektur, 30-Bit Farbgenauigkeit und automatischer Konfiguration der Anwendungs-Anzeigeoptionen für optimale Leistung. Für Rechenleistung sorgt dabei Intels Core i7-Technologie und der X58-Chipsatz. Der 6 GByte große Arbeitsspeicher arbeitet im Triple Channel-Modus, während die Festplatte 500 GByte speichert. Für 670 Euro ist das Modell 5000 Silent zu haben. Die größere Variante 9500 kostet rund 1.500 Euro. (dr)

TAROX: www.tarox.de/index.php?id=167



Soll eine hohe Grafikleistung bei niedrigem Geräuschpegel bieten: Die Workstation 5000 von TAROX

Gut gelüfteter Blade-Würfel

Fujitsu erweitert mit dem neuen **Primergy BX900**-System sein Portfolio an Blade-Servern. Durch die Vollintegration von Stromversorgung und Kühlung erreicht der Hersteller eine Platzersparnis, die in einer Standard-Server-Chassis mit zehn Höheneinheiten den Einbau von 18 statt bisher 16 Servern erlaubt. Trotz der damit erreichten Leistungssteigerung in Höhe von zwölf Prozent pro Chassis will der Hersteller durch eine besonders effiziente Umwandlung von Gleich- in Wechselstrom sowie ein ausgefeiltes Lüftungskonzept die Energiekosten insgesamt deutlich senken. An der Rückseite des Gehäuses lassen sich neben den maximal sechs Netzteilen bis zu acht Connection-Blades verbauen, die die Rechner etwa über 10-GByte-Schnittstellen oder FC-Switches mit bis zu 8 GByte mit dem Unternehmensnetzwerk verbinden. Als Servereinheit kommt das Modell "Primergy BX920 S1" zum Einsatz, das mit Intel Xeon-Prozessoren der Serie 5500 ausgestattet ist und sich laut



Insgesamt 18 Blade-Server bringt Fujitsu in der Chassis "Primergy BX900" unter

Fujitsu besonders gut für die Virtualisierung umfangreicher Infrastrukturen eignen soll. Aus Gründen der Netzwerkkonsolidierung lassen sich in dem aufgrund seines würfelförmigen Aussehens "Dynamic Cube" getauften Gehäuses auch Storage Blades unterbringen. Das System ist ab sofort zu einem Preis ab 8.500 Euro pro Chassis erhältlich. Je nach Konfiguration der Server kommen zu diesem Betrag noch Kosten ab 1.500 Euro pro Blade hinzu. (ln)

Fujitsu: <https://de.ts.fujitsu.com/rl/produkte/flash/dynamiccube/>

Die Server mit sechs Kernen

HP stellt neue Server der ProLiant G6-Reihe vor, die auf den jüngsten Sechskern-Opterons von AMD basieren. Das Portfolio umfasst die Modelle HP ProLiant DL785, DL585, DL385 sowie DL165. Sie sind für den Einsatz im Rack optimiert. Hinzu kommen mit den Modellen ProLiant BL465, BL495c und BL685c noch drei Server-Blades. Die Rechner weisen laut Hersteller zu einem **günstigen Einstiegspreis** eine hohe Performance und eine gesteigerte Energieeffizienz auf. Letztere will HP unter anderem mit einer Sensortechnologie verbessert haben, die die Temperatur eines Servers überwacht und dann entsprechend dessen Kühlung optimiert. Nach Hersteller-eigenen Messungen soll

ein G6-Server so im Vergleich zur Vorgängergeneration nur noch die **Hälfte der Energie verbrauchen**. Das kleinste Modell, DL165, verfügt über einen Prozessorsockel mit einem Opteron 2427 mit 2,2 GHz Taktfrequenz und einen Arbeitsspeicher von 4 GByte. Das Gerät soll ohne Festplatten – maximal lässt es sich mit vier SATA- oder SAS-Speichern bestücken – zu einem Preis von rund 1.700 US-Dollar zu haben sein. Der für Virtualisierungslösungen empfohlene Blade-Server BL685c kostet in der Variante mit zwei Sockeln mit Opteron 8389-Prozessoren zu je 2,9 GHz und insgesamt 8 GByte RAM knapp 11.000 US-Dollar. (ln)

Hewlett-Packard: www.hp.com/go/proliant/

Firewall für Außenstellen

Die Appliance **StoneGate FW-1030 FW/VPN** von **Stonesoft** bietet Leistungsmerkmale wie effiziente **Traffic Inspection** und **SSL-Entschlüsselung**. Sie richtet sich vor allem an kleine Unternehmen sowie entfernte Zweigstellen mit zwei- bis dreistelligen Anwenderzahlen. So setzt die Firewall mit einer Höhengrenze bis zu 650 MBit/s an Datenverkehr durch. Der VPN-Durchsatz beträgt 120 MBit/s, wobei sich bis zu 1.000 Tunnel einrichten lassen. Bei der HTTPS-Inspection fließen immerhin noch 40 MBit/s durch die Leitung. Anschluss findet die Appliance über sechs GBit-Ether-

net-Ports. Bis zu 16 Geräte lassen sich im Active/Active-Verbund clustern. So will der Hersteller für eine kontinuierliche Netzwerk-Konnektivität sorgen. Daneben sollen ein Server-Loadbalancing sowie Fallbackmöglichkeiten zu alternativen Providern zusätzliche Sicherheit bieten. Ihre Daten speichert die Firewall auf einem Solid State-Laufwerk ab. Eine Anti-Virus-Engine für Web- und E-Mailverkehr ist optional als Zusatzlizenz erhältlich. Ab 4.950 Euro ist die Firewall-Appliance ab sofort verfügbar. (dr)

Stonesoft: www.stonesoft.com/en/products_and_solutions/products/fw/appliances/



Die Firewall-Appliance StoneGate FW-1030 FW/VPN sichert das Netzwerk ab und sorgt für eine redundante Anbindung

Kleinst-NAS mit viel Speicher

Nur 135x60x90mm misst der neue NAS-Speicher **ALL6501** von **Allnet**. Das platzsparende Format kommt durch die Verwendung von zwei SATA-Festplatten im 2,5 Zoll-Format zustande, die den Anwendern insgesamt 2 TByte an Datenkapazität zur Verfügung stellen und im laufenden Betrieb ausgetauscht werden können. Um für die Redundanz der Magazinspeicher zu sorgen, hat der Hersteller das Gerät außer mit RAID 0 auch mit RAID 1 ausgestattet, was die Spiegelung der Daten in Echtzeit erlaubt. Eine GBit-Ethernet-Schnittstelle sorgt für die Anbindung ins Netzwerk, während sich über zwei USB-Ports weitere Speichermedien oder ein Netzwerkdrucker betreiben lassen. Nutzer können das lüfterlose NAS-System zudem als FTP- und Samba-Server verwenden. Die Eingliederung in eine Active Di-

rectory-Umgebung ist allerdings nicht vorgesehen. Zugriff auf das EXT3-Filesystem ist unter den Betriebssystemen Windows NT / 2000 / XP und Vista sowie unter Mac OSX möglich. Das ALL6501 ist ab sofort erhältlich und kostet ohne Festplatten 170 Euro. (ln)

Allnet: www.allnet.de



Mit dem "ALL6501" bringt Allnet einen äußerst kompakten NAS-Server auf den Markt

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

Netgear präsentiert den neuen RangeMax 150 Wireless-Router **WNR1000**. Das Gerät arbeitet sowohl in Wireless-B-, Wireless-G- als auch in Wireless-N-Netzen. Neben einem WAN-Port bietet der Router vier Fast-Ethernet-Anschlüsse. Für Sicherheit sorgen eine Überprüfung vertrauenswürdiger Nutzer, zeitbasierte Nutzungskontrollen, das Logging von Internetseiten sowie URL Content Filtering. Der Double Firewall Schutz über NAT und SPI schützt vor Angriffen von außen. Daten können über WPA2, WPA und WEP verschlüsselt werden. Für 50 Euro ist der Router erhältlich. (dr)

www.netgear.de

Citrix bringt eine neue Technologie für NetScaler auf den Markt. Mit **nCore** sollen die NetScaler-Appliances eine bessere Unterstützung von Web 2.0-Applikationen und Cloud-Services bieten. Durch die Ultra-Fast Packet Engine werden mehrere CPU-Kerne genutzt, was sich auf Skalierbarkeit und Performance positiv auswirken soll. Die Geräte sind somit in der Lage, nun mehrere komplexe Verarbeitungsprozesse verschiedener Applikationen parallel auszuführen. Die neue nCore-Technologie ist Teil der neuen NetScaler 9.1 Software, die für Citrix-Nutzer mit laufenden Wartungsverträgen kostenlos zum Download bereitsteht. (dr)

www.citrix.de

Mit **FASTRecover** stellt **BakBone** eine Software für das Echtzeit-Backup in Windows-Umgebungen vor. Das können etwa Exchange oder SQL Server sowie Fileserver sein, auf denen fortlaufend Daten auf Bytelevel gesichert werden. Dabei verspricht der Hersteller, Daten eines beliebigen Zeitpunkts innerhalb von nur 30 Sekunden wieder verfügbar zu machen. Hierfür analysiert die Software die laufenden User-Anfragen auf die Server und stellt dementsprechend die unmittelbar benötigten Daten zuerst wieder her. Ab 2.995 Euro ist die Lösung in drei Ausführungen erhältlich. (dr)

www.bakbone.com

HP erweitert sein Thin Client-Portfolio um den **4410t Mobile Thin Client**. Der Hersteller will mit dem festplattenlosen Notebook die Unternehmenssicherheit erhöhen, da sensible Dateien nicht mehr auf dem Rechner selbst, sondern auf einem zentralen Server gehostet werden. Auch der integrierte SSD-Speicher erlaubt durch einen Schreibfilter das Ablegen von Daten nur bedingt. Einer Infektion durch Malware will HP so einen Riegel vorschieben. Als Betriebssystem kommt Windows Embedded Standard (WES) mit RDP 6.1 zum Einsatz. Damit kann der Thin Client die neuesten Sicherheits- und Management-Technologien von Windows Server 2008 nutzen. Das Gerät wird ab August zu einem Preis von rund 590 Euro erhältlich sein. (ln)

www.hp.com

Kontakt nach Hause

Aruba Networks stellt im Rahmen des **Virtual Branch Network (VBN)** drei neue Remote Access Points-Reihen sowie eine neue Branch Office Controller-Serie vor, die der Vernetzung von Zweigstellen und anderen Remote-Lokationen dienen. Die VBN-Geräte verbinden Anwender außerhalb des Firmennetzes sicher und transparent mit den Unternehmensanwendungen und -ressourcen. Hierfür bauen die Remote-Komponenten eine VPN-Verbindung zu den Gateway-Appliances im Unternehmensnetzwerk auf. Der neue Access-Point RAP-2WG etwa richtet sich an Home Offices und ermöglicht die Anbindung von bis zu fünf Mitarbeitern. Das Gerät funkt in den Standards 802.11b/g und bietet zusätzlich einen Ethernet-Port zum Anschluss von kabelgebundenen Netzwerkgeräten. Das Modell RAP-5WN hingegen bedient bis zu 50 Nutzer und eignet sich damit auch für Außenstellen. Es unterstützt neben 802.11b und g auch den n-Standard. An noch größere Umgebungen richtet sich der neue 620 Branch Office Controller. Über ihn lassen sich 256 User mit der Firmenzentrale sowohl per Kabel als auch drahtlos mittels WLAN verbinden. Der Multiservicecontroller Aruba 6000 mit VBN-Software unterstützt in der Firmenzentrale dabei bis zu 8.000 Geräte der Serien RAP oder BOC 600 und bis zu 32.000 Anwender. Die neuen Modelle sind ab sofort erhältlich. Der Access Point RAP-2WG kostet 109 US-Dollar, die größere Variante RAP-5WN ist für 435 Dollar zu haben. Für den Branch Office Controller 620 fallen 1.645 Dollar an. (dr)

Aruba: www.arubanetworks.com/products/remote_access_points.php



Klein und handlich:
Der Remote Access Point
RAP-2WG von Aruba

Hochskalierbare SAN-Speicher

Infotrend stellt innerhalb seiner **G6 8Gbit/s Fibre Channel SAN-Lösungen** zwei neue Modellreihen mit jeweils zwei und vier Höheneinheiten vor. Die insgesamt vier neuen Systeme **S12F-R1840/S12F-G1840** und **S24F-R1840/S24F-G1840** basieren auf der ASIC667-RAID-Technologie des Herstellers. Somit soll sich ihre Kapazität durch das Hinzufügen von Erweiterungssystemen hochskalieren lassen. Dank des Einsatzes von zwei 8 Gbit/s FC-Hosts-Ports pro Controller sollen die Systeme zudem eine hohe Performance bieten. Die Lesegeschwindigkeit soll 2.600 MByte/s betragen, 1.200 MByte/s schreibt das SAN-System laut Hersteller. Bis zu 12 beziehungsweise 24 SAS- oder SATA-II-

Festplatten kommen dabei zum Einsatz. Um einen Datenverlust bei Stromausfall zu verhindern, schreiben "Flash Backup Module" (FBM) alle Daten aus dem Cache in ein Flash-Modul. Die Battery Backup Unit (BBU) stellt dafür automatisch den nötigen Strom bereit. Ist die Stromversorgung wieder gewährleistet, werden die Informationen vom Flash-Modul zurück ins Speichersystem geschrieben. Die Systeme unterstützen gängige Betriebssysteme wie Windows Server 2008, Solaris, Linux, IBM-AIX und HP-UX sowie Virtualisierungsplattformen wie VMware und Hyper-V. Ab 4.950 Euro sind die Modelle ohne Festplatten ab sofort erhältlich. (dr)

Infotrend: www.infotrend.com/main/2_product/productNo-host.asp



Bis zu 2.600 MByte/s Lesegeschwindigkeit
sollen die neuen SAN-Systeme von Infotrend bieten

Rechenzentrum auf dem Reißbrett

Um den Aufbau von Rechenzentren zu modellieren, bietet **Avocent** den **MeragePoint Infrastructure Explorer** an. Die Windows-Software ermöglicht das virtuelle Ausstatten von Serverräumen mit Racks sowie den darin enthaltenen Servern. Dabei lassen sich per Drag-and-Drop Geräte beliebig hin- und herschieben. An Vorlagen beinhaltet die Software mehrere tausend Servertypen und Netzwerkgeräte sowie deren typische Leistungsaufnahme und Wärmeabgabe. Damit lässt sich erkennen, wo eventuelle Hotspots liegen und wie sich die Wärmeentwicklung sowie Stromversorgung optimal im Raum verteilen lässt. Dies soll nicht zuletzt zu Einsparungen bei

der Kühlung führen. Auch die noch verfügbaren Ports kann der IT-Verantwortliche über die Software einsehen und die Verkabelung so durchplanen und bei Bedarf ändern. Der Infrastructure Explorer lässt sich zudem so konfigurieren, dass er Avocents Managementsoftware DSView 3 nutzt, die für die Steuerung eines Rechenzentrums ausgelegt ist. Sie erlaubt das Remote-Management und unter anderem die Problembehebung bei traditionellen sowie virtuellen Servern und verwaltet zudem Avocents intelligente Stromverteilungseinheiten. Für 950 Euro pro Rack ist die Software ab sofort erhältlich. (dr)

Avocent: www.avocent.com/Products/Product.aspx?id=12685

IT-Administrator-Workshop

„Hochverfügbarkeit“ am 16. Juli in Heidelberg

99,99 Prozent Workshop

von John Pardey

Eine zuverlässige Hochverfügbarkeitslösung ist nicht immer nur eine Frage des Budgets, das die Wahl zwischen dieser und jener Lösung lässt, sondern ist im besten Fall durch kluge Konzepte und Konfigurationen gekennzeichnet. In unserem Workshop „Hochverfügbarkeit“ zeigen wir anhand zweier Beispiele Maßnahmen, wie Sie hochverfügbare Dienste und Applikationen betreiben. Zum einen erfahren Sie dabei, wie Sie mit Microsofts App-V virtualisierte Anwendungen hochverfügbar zur Verfügung stellen. Im zweiten Schwerpunkt des Workshops stellen wir Ihnen vor, was Linux mit dem neuen „HA 3“ Unternehmen in Sachen Hochverfügbarkeit mitbringt. Melden Sie sich noch heute kostenlos an, die Plätze sind begrenzt.

Ab 13 Uhr bieten wir unseren Abonnenten am 16. Juli in Heidelberg den – wie gewohnt kostenlosen – Workshop „Hochverfügbarkeit für Dienste und Applikationen“. Diesmal haben wir uns entschieden, zwei ausführliche Präsentationen in die Workshopagenda aufzunehmen und diesen mit jeweils rund 90 Minuten den Raum zu geben, um die für das anspruchsvolle Thema Hochverfügbarkeit notwendigen technische Tiefe zu ermöglichen.

Virtuelle Applikationen verteilen

Zunächst erläutert Thorsten Christoffers, sepago-Berater und Community-Blogger, die virtuelle Applikationsbereitstellung und die Konfiguration der Microsoft App-V-Komponente in den SCCM 2007 R2. Er zeigt die Vereinigung virtueller und herkömmlicher Bereitstellungsszenarien in einer Plattform und legt dar, wie Sie durch die optimale Konfiguration die Verfügbarkeit Ihrer Applikationen erhöhen.

Die Teilnehmer erfahren mehr über Tipps und Tricks bei der richtigen Paketierung,

der Übergabe an den SCCM Server bis hin zur Auslieferung der virtuellen Pakete über die Verteilungsserver. Die Auswirkungen führt Christoffers exemplarisch an einem Windows XP- und einem Windows Vista-Rechner vor.

Linux HA 3

Der Vortrag von Dr. Michael Schwartzkopff, MultiNET Services GmbH, stellt die Fähigkeiten dar, die Linux-HA in Version 3 mitbringt. Die wichtigste Neuerung ist dabei sicher die eingebaute Überwachung der Ressourcen. Anhand der Grundelemente „Ressource“ und „Bedingung“ zeigt Schwartzkopff, wie sich selbst komplexe Konfigurationen abbilden lassen. Abschließend geht der Dozent noch auf die Entwicklung des Projektes Linux-HA (Stichwort: „pacemaker“) ein.

Wie üblich ist der Workshop am 16. Juli für alle Abonnenten kostenlos. Alle Informationen zur Veranstaltung und der Anmeldung finden Sie im nebenstehenden Kasten. Wir würden uns freuen, Sie begrüßen zu dürfen.

ITANet Schirmherrschaft:



ITANet
Die System und Netzwerk User Group

Die Agenda des Workshops

13 Uhr: Begrüßung

13.15 Uhr: Verteilung von Microsoft App-V-Paketen mit SCCM 2007 R2 zur Optimierung der Verfügbarkeit – wie Administratoren durch den redundanten Aufbau der Verteilungsserver des SCCM eine Hochverfügbarkeit der Zustellung von virtuellen Paketen sicherstellen.

Dozent:

Thorsten Christoffers, sepago, Köln

14.45 Uhr: Pause

15 Uhr: Partnervortrag Realtech: Hochverfügbarkeit sichern - Unternehmensweites IT-Management auf Basis einer normalisierten Configuration Management Data Base (CMDB)

Dozent:

Dr. Kürsad Gögen, Product Manager
IT Service Management, Realtech

16 Uhr: Linux HA Version 3 – wohin geht die Reise?

Dozent:

Dr. Michael Schwartzkopff,
MultiNET Services GmbH, Grasbrunn

17.30 Uhr: Ende des Workshops

Ort: Print Media Lounge,
Kurfürstenanlage 60, 69115 Heidelberg
(direkt gegenüber des Hauptbahnhofs)

Teilnahmegebühren:

Für IT-Administrator Abonnenten kostenlos.

Anmeldung bis zum 6. Juli unter

www.it-administrator.de/usergroup/termine/52193.html

Workshop
„Hochverfügbarkeit“ am 16. Juli



Zweiter Deutscher IPv6-Gipfel, 14. und 15. Mai 2009, Potsdam

Ideen für das neue Protokoll

von Dirk Srocke

Bereits kommendes Jahr soll jeder vierte Internetnutzer hierzulande IPv6 nutzen können - so zumindest die Zielstellung des deutschen IPv6-Rats. Ein entsprechender Aktionsplan wurde auf dem zweiten Deutschen IPv6-Gipfel vorgestellt. Zum ersten Mal gab es dort auch Preise für besonders pfiffige Nutzungsideen des IPv4-Nachfolgers. Die oft mobilen Anwendungen bergen jedoch auch neue Sicherheitsrisiken.

Als Rückgrat der modernen Gesellschaft müsse sich das Internet auch in Deutschland weiterentwickeln, meinte Professor Dr. Christoph Meinel anlässlich des zweiten Deutschen IPv6-Gipfels am Hasso Plattner Institut (HPI) der Universität Potsdam. Der Wissenschaftler doziert bereits seit den 90er Jahren über den Nachfolger des noch immer allgegenwärtigen Internet Protocol der Version 4. Während das Protokoll in Asien bereits stark angenommen wird und die US-Regierung bereits IPv6-konforme Gerätschaften verlangt, fehle es in Deutschland noch an dem nötigen Bewusstsein zum Wandel.

Gründe hierfür sieht der Akademiker in einem nicht akuten Adressmangel sowie in leidlich funktionierenden Behelfslösungen wie Network Address Translation (NAT). Für mobile Anwendungen sei NAT aber nicht geeignet. Zudem biete der IPv4-Nachfolger neben dem auf 128 Bit gestiegenen Adressraum zahlreiche Vorteile. Hierzu zählen eine verbesserte Dienstqualität oder eine sichere Kommunikation über direkte End-to-End-Verbindungen. Des Weiteren sollen sich Netzwerke mit IPv6 deutlich leichter verwalten lassen.

Darum will Meinel als Vorsitzender des Deutschen IPv6-Rates dem Protokoll endlich zum Durchbruch verhelfen. Den Weg dorthin beschreibt die Expertengruppe aus Industrie, Forschung, Politik und Verwaltung in einem "Nationalen IPv6-Aktions-

plan für Deutschland". Das unter [1] abrufbare Papier soll auch auf dem kommenden IT-Gipfel der Bundesregierung eingebracht werden. Der Aktionsplan skizziert IPv6 als Fundament für die Entstehung des "Internet der Dinge". Zu möglichen Einsatzszenarien zählen Fahrzeuge, die untereinander kommunizieren (Vehicle-to-X Communication), oder Sensornetzwerke.

Netbook ersetzt Server

Von den mobilen Qualitäten des überarbeiteten Internet Protocol konnten sich die Teilnehmer des Mitte Mai zum zweiten Mal veranstalteten IPv6-Gipfels live überzeugen. So demonstrierte Junaid Islam, Präsident und CTO der Videoplattform Vidder, wie sich mit einem schwachbrüstigen Netbook Liveübertragungen mit 1.000 Zuschauern realisieren lassen. Trick des Ganzen: Der mobile Rechner nahm als Mobile Node Kontakt mit Islams heimischen Router auf. Das als Home Agent agierende System wiederum fungierte als Server und bediente die Zuschauer.

IPv6 als Grundlage von Unified Communications

Bereits kommendes Jahr soll das Potenzial der vorgestellten Anwendungen auf breiter Basis verfügbar sein, fordert der IPv6-Aktionsplan. Konkret soll sich 2010 ein Viertel aller deutschen Internetanwender per IPv6 mit dem Netz verbinden und auf die wichtigsten Inhalte und Dienste zugreifen, ohne dabei signifikante Unterschiede zu be-

merken. Das Protokoll sei ausgereift und verfügbar, sagte Meinel und verwies auf moderne Betriebssysteme und aktuelle Router.

Der Aktionsplan orientiert sich am dreiphasigen Internet Transition Plan der Network Group der IETF (Internet Engineering Task Force). Diesem zufolge sollen Internet Service Provider bis 2010 ein IPv6-Angebot für Endkunden einrichten. Hierbei gebe es in Deutschland noch Probleme, gestand der Vorsitzende des IPv6-Rates ein. Zwar sei bekannt, dass es interne Projekte bei den Anbietern gebe, für marktreife Angebote fehle es aber noch immer an einer entsprechenden Nachfrage. Den von Meinel als "Henne-Ei-Problem" charakterisierten Missstand wolle der IPv6-Rat angehen und die Anbieter wettbewerbsübergreifend an einen Tisch bringen. Erste Gespräche gebe es bereits. Bis 2012 sieht die IETF dann einen zwingenden Einsatz von IPv6 vor - ein Ziel, das im IPv6-Aktionsplan zitiert wird.

Migrationsstrategien und Behelfslösungen

Als eingeschränkte Übergangslösung schlug der IPv6-Rat einerseits Protokollübersetzungs-Gateways vor. Diese ermöglichen jedoch keine transparente Interoperabilität und seien daher nicht zukunftssicher. Besser sei es, über so genannte Dual-Stacks zu migrieren. Die Methode erlaubt den parallelen Betrieb von IPv6 und IPv4 auf ein und demselben physischen Gerät im gleichen



Dr. Robert E. Kahn spricht im Museum für Kommunikation in Berlin zum "Information Management on the Future Internet"

Netzwerk. Während der mit zehn bis 20 Jahren angesetzten Übergangsphase könnten beide Standards somit koexistieren. Als dritte Lösung für eine sanfte Umstellung auf IPv6 kommen Tunneltechniken infrage. Dabei werden IPv6-Datenpakete über herkömmliche IPv4-Netze übertragen.

Weitere Migrationshilfe gab es für die Zuhörer der Expertenvorträge am Hasso Plattner Institut der Universität Potsdam. Andreas Schachtner von der afS Holding verdeutlichte dabei, wie viel Zeit bei der Umstellung auf IPv6 bereits verschenkt wurde. Kurz vor dem Ende des verfügbaren IPv4-Adressraums stehe IPv6 noch immer in den Startlöchern. Statt darüber zu resignieren, erklärte der IT-Berater, wie sich bestehende Adressräume vorübergehend spreizen lassen, um Adressengpässe kurzfristig zu überbrücken. Als praktika-

ble, wenngleich nicht einzige Lösung, böte sich hierbei ein revidiertes NAT-PT (Network Address Translation – Protocol Translation) an.

Thomas Tremml von Microsoft Deutschland erläuterte, wie die aktualisierten Betriebssysteme Windows 7 und Windows Server 2008 R2 beim Übergang auf IPv6 helfen können. Die mit den Systemen verfügbare Zugangs- lösung DirectAccess unterstützt die Verfahren ISATAP, Tere- do und 6to4.

Sicherheitsbedenken bei mobilen Diensten

In einem systemübergreifenden Tutorial beschrieb der diplomierte Informatiker und Buchautor Benedikt Stockebrand die Umstellung auf IPv6. Trotz der allgemeinen IPv6-Euphorie schlug der IT-Berater dabei auch kritische Töne an. Gerade die mobilen Dienste böten zwar spannende Funktionen, könnten aber auch Sicherheitslöcher aufreißen. Bei dem von Stockebrand geschilderten Szenario vermittelt der stationäre Home Agent die Verbindung zwischen mobilem Endgerät (Mobile Node) und Dienst im Internet (Correspondent Node).

Bewegt sich ein Nutzer samt mobilem Endgerät, läuft der Datenverkehr zwischen Mobile Node und Correspondent Node weiter über den Home Agent. Das bedeutet in der Praxis ein höheres Datenvolumen sowie steigende Latenzzeiten. Alternativ könne der Home Agent die IP-Adresse des Mobile Node auch weitervermitteln, um einen direkten Kontakt zu ermöglichen. Hierbei sind zum einen Angriffe durch einen Man-in-the-Middle möglich. Zudem ermögli-

che das als "Route Optimization" bekannte Verfahren das Erstellen detaillierter Bewegungsprofile: Die Subnetze, in die sich der Mobile Node einbucht, sind geographisch lokalisierbar.

Ideenwettbewerb für IPv6

Mit einem internationalen Wettbewerb wollte der IPv6-Rat zeigen, welche weiteren Anwendungen heute schon mit IPv6 realisierbar sind. Dem Aufruf folgten 41 Experten aus 19 Ländern. Zu den Anwesenden bei der Preisverleihung zählte Internet-Pionier Dr. Robert Elliot Kahn. Der Mitentwickler des Transmission Control Protocol (TCP) wurde in Berlin von Prof. Hasso Plattner zum "HPI Fellow" ernannt.

Der erste Preis in der Kategorie "IPv6-Anwendungen" ging an Mark Palkow, Geschäftsführer der Berliner Softwareschmiede Daviko. Das Unternehmen präsentierte eine flexible Unified-Communications-Lösung: Teilnehmer können mit dieser Video-konferenzen auf tragbaren Endgeräten (PDA) verfolgen und die laufende Übertragung auf ein stationäres Telepräsenz-System umschalten. Platz zwei gab es für Gilles Haiat vom französischen Softwarehersteller Vizelia für eine Umweltmonitoring-Software mit Funksensoren. Ebenfalls ausgezeichnet wurde Tobias Neumann vom Netzwerk-ausrüster Cisco: Die Anwendung Cisco Unified Communications (CUC) unterstützt Dual Stack und ermöglicht Anwendern, IPv6 schrittweise einzuführen.

Weitere Preise gab es zudem für die besten Ideenskizzen zukünftiger Applikationen. Dr. Roland Bless von der Universität Karlsruhe beschrieb, wie sich IPv6 sinnvoll für Peer-to-Peer-Netze nutzen lässt. Emanuele Goldini von der Universität Pavia umriss eine Art umgekehrtes RSS-Feed. Bei diesem werden Empfänger per Pushprinzip mit Nachrichten versorgt statt regelmäßig nach Informationen anfragen zu müssen. Ebenfalls ausgezeichnet wurde Systemadministrator Maximilian Weigmann für seinen Vorschlag, chronisch kranke Menschen mit einer IPv6-Infrastruktur ständig zu überwachen. (dr)

[1] Aktionsplan des IPv6 Council
www.ipv6council.de/aktionsplan/

Links



11. IT-Sicherheitskongress des BSI, 12. bis 14. Mai, Bonn Bad-Godesberg

Sichere Wege zum Ziel

von Daniel Richey

Das Bundesamt für Sicherheit in der Informationstechnik, kurz BSI, befasst sich in staatlichem Auftrag mit der IT-Sicherheit. Mitte Mai fand der 11. Kongress des BSI in Bonn-Bad Godesberg statt. Rund 500 Teilnehmer informierten sich über Neues in den Bereichen staatliche und privatwirtschaftliche IT-Sicherheit – mit einem bunten Strauß an Themen und hochkarätigen Teilnehmern. IT-Administrator war für Sie vor Ort.

Unter dem Motto "Sichere Wege in der vernetzten Welt" fanden vom 12. bis 14. Mai 2009 zahlreiche Vorträge und Podiumsdiskussionen rund um das Thema Informations- und IT-Sicherheit statt. Das BSI begrüßte dazu über 500 Teilnehmer aus den Bereichen Verwaltung, Industrie und Wissenschaft in der Stadthalle Bonn-Bad Godesberg. Darunter Vertreter zahlreicher Konzerne, Hochschulen und Behörden. Begleitet wurde das Kongressprogramm von einer Ausstellung, in der Unternehmen ihre Sicherheitslösungen für den IT-Bereich präsentierten.

Bundesinnenminister Schäuble stellte in seiner Eröffnungsrede die Bedeutung der IT-Sicherheit in Anbetracht der zunehmenden Vernetzung der Informationstechnik heraus. Mit der Sicherheit und Verfügbarkeit des Internets stehe und falle die Funktionsfähigkeit unserer global vernetzten Informationsgesellschaft. Zudem warnte der Minister vor einer Verschärfung der IT-Sicherheitslage. Jede Form einer IT-Krise könne zu einem erheblichen volkswirtschaftlichen Schaden führen und das Vertrauen in das Internet in Frage stellen. Um dem ständigen Wandel gerecht zu werden, sei die geplante Neuaufstellung des BSI ein wesentlicher Beitrag. Schäuble hoffte in diesem Zusammenhang auf eine baldige Verabschiedung der Novelle des BSI-Gesetzes und gab sich überzeugt davon, dass das BSI als Nukleus der IT-Sicherheitskompetenz weiter ausgebaut würde.

Sicher ins Internet – für Unternehmen

Naturgemäß befasste sich der Kongress mit zahlreichen staatlichen Aspekten der IT-Sicherheit – der elektronische Personalausweis und Bürgerportale als zwei Beispiele. Doch auch die Sicherheit in Unternehmen stand auf dem Plan, etwa mit der sicheren Internet-Anbindung oder dem Identitätsmanagement.

Dr. Helge Kreutzman vom BSI und Roman Maczkowsky von der m-privacy GmbH stellten das Prinzip "Remote Controlled Browsers System" (ReCoBS) vor. Dabei handelt es sich um ein Modell, das Mitarbeitern ein sicheres Surfen im Netz ermöglichen soll. Dabei wird der Browser nicht auf den lokalen Clients der Mitarbeiter ausgeführt, sondern auf einem gehärteten Server in einer DMZ. Die Webseiteninhalte werden dann über ein Videoprotokoll auf die Clientrechner übertragen, während aktive Inhalte auf den gesicherten Servern ausgeführt und abgespielt werden. Gelingt nun Schadcode über eine Schwachstelle in den Browser, sind lediglich die ReCoBS-Server betroffen. Diese haben jedoch keinen Zugang zu internen Daten im Netz und lassen sich über schreibgeschützte Images regelmäßig neu aufsetzen. Nichts desto trotz bleiben die besuchten Webseiten für die User interaktiv und ein – natürlich vom System kontrollierter – Datenaustausch über das Web ist möglich.

Etwas weiter gefasst hatte Cornelia Schildt vom BSI ihren Vortrag zum Thema sicheres Surfen im Internet. Sie stellte die sogenannte ISI-Reihe (Internet-Sicherheit) des Bundesamtes vor. Sie ist eine Ergänzung zu den Grundschutz-Katalogen und führt Unternehmen methodisch und modular an das Thema heran. Die Module im Rahmen der ISI-Reihe befassen sich unter anderem mit der sicheren Anbindung des lokalen Netzwerks an das Internet, dem sicheren WLAN-Betrieb, der Absicherung eines Webserver oder der sicheren Nutzung von E-Mail. Noch sind jedoch nicht alle Module durch das BSI zusammengestellt. Als praxisnahe Anwendungshilfen stehen dann Checklisten zur Internet-Sicherheit zur Verfügung, anhand derer Unternehmen die Umsetzung der Empfehlungen überprüfen können.

Fazit

So hochkarätig die Teilnehmer- und Referentenliste war – mit Peter Schaar sei nur ein prominentes Beispiel genannt – so bunt gemischt waren die Sicherheitsthemen. Für IT-Administratoren gab es besonders am zweiten sowie dritten Veranstaltungstag nützliche Infos, die durchaus die eine oder andere Anregung geliefert haben dürften. Für Schäuble sollte die Zukunft der IT-Sicherheit übrigens Züge der Straßenverkehrsordnung tragen: Jeder Teilnehmer im Netz ist neben seiner eigenen Sicherheit auch für die der anderen Nutzer verantwortlich. 

WENIGER REISEN. WENIGER EMISSIONEN. WENIGER KOSTEN.

Wie weit würden Sie gehen, um Kosten und Emissionen zu senken? Nun, dank der IBM Lotus Collaboration Software müssen Sie nirgendwohin „gehen“. Denn mit Web-Konferenzen, Instant Messaging und Social Computing lässt Lotus Software Menschen schneller und effizienter zusammenarbeiten – unabhängig davon, wo sie sich gerade aufhalten. So werden Entscheidungen wie im Flug getroffen, aber ganz ohne Jetlag, Kerosin und CO₂-Emissionen.

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





Im Test: Sterling Commerce Connect:Direct 4.4 Hochsichere Verbindung

von Jürgen Heyer

Wer regelmäßig wichtige und vertrauliche Daten absolut sicher, zuverlässig und nachvollziehbar übertragen muss, stößt bei der Suche nach geeigneter Software schnell auf den Begriff "Managed File Transfer" (MFT). Marktführer in dieser Sparte ist Sterling Commerce, dessen Produkt Connect:Direct bereits bei vielen namhaften Unternehmen zum Einsatz kommt. In einem Test hat IT-Administrator dieses spezielle Werkzeug einmal genauer unter die Lupe genommen.

Es gibt viele gute Gründe, wichtige und vertrauliche Daten sicher zu übertragen. Dies können personenbezogene Daten sein, die beispielsweise Banken verarbeiten, aber ebenso Konstruktionsdaten. Diese werden von global agierenden Unternehmen häufig an verschiedenen Standorten für die Weiterentwicklung benötigt, müssen daher über weite Strecken ausgetauscht werden und dürfen trotzdem auf keinen Fall in fremde Hände gelangen, denn Industriespionage ist ein einträgliches Geschäft und findet überall statt. Gerade der Datentransport ist als Schwachstelle bekannt, wird gerne attackiert und muss daher besonders gesichert werden.

Das zu AT&T gehörige Sterling Commerce bietet eine ganze Reihe an Programmen an, die unter den Sammelbegriff Managed File Transfer fallen. Das am häufigsten eingesetzte ist Connect:Direct (C:D), welches wir im Testlabor einmal genauer betrachtet haben. Sterling Commerce ist mit einem Markt-

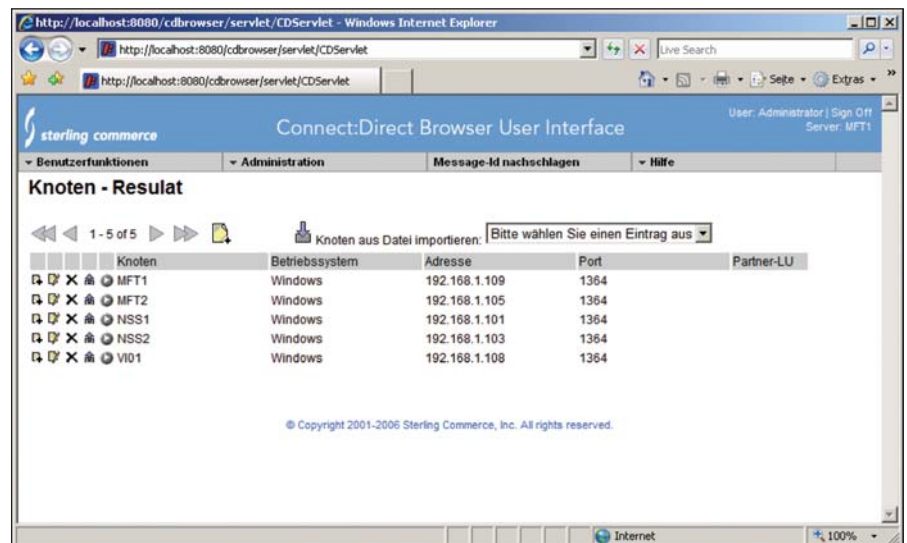


Bild 1: Neben dem Requester unter Windows lässt sich C:D über ein Webinterface administrieren

anteil von über 48 Prozent führend beim sicheren Dateitransfer.

Die meisten Leser dürften beim Datentransfer über größere Strecken sowie über das Internet an FTP, SFTP, SSH, HTTP sowie HTTPS, gegebenenfalls auch noch an WebDAV, denken oder gar ein Produkt einsetzen, welches eines dieser Protokolle verwendet. Bei durchschnittlichen Anforderungen an den Automatisierungsgrad und die Datensicherheit sowie einem geringen Datenvolumen ist es durchaus in Ordnung, mittels SFTP oder SSH zu übertragen. Falls aber eine derartige Lösung die Anforderungen nicht mehr erfüllt und vorgegebene SLAs nicht garantieren kann, dann kommt ein

MFT-Produkt wie C:D ins Spiel. Wichtig ist dabei die Tatsache, dass C:D nicht nur ein Name für ein Produkt ist, sondern tatsächlich auch ein eigens entwickeltes Protokoll aus den 70er Jahren beschreibt, welches zuerst im Mainframe-Umfeld eingesetzt wurde und heute eine sehr breite Betriebssystem- beziehungsweise Plattformunterstützung bietet, wie Windows, Unix (HP, IBM, Sun, Linux), OpenVMS, i5/OS (OS/400), Linux on z/OS, z/VM und z/VSE, HP NonStop.

Zügige Installation

Während bei herkömmlichen Transferlösungen meist eine Seite explizit als Server arbeitet, zu dem sich dann ein oder mehrere Clients verbinden, ist C:D symmetrisch

Lauffähiges System unter Windows, Unix (HP, IBM, Sun, Linux), OpenVMS, i5/OS (OS/400), Linux on z/OS, z/VM und z/VSE, HP NonStop, keine besonderen Hardwareanforderungen, unterstützte Netzwerkprotokolle: TCP/IP, SNA

Systemvoraussetzungen





aufgebaut, also mit den gleichen Modulen auf beiden Seiten. Im Kern handelt es sich um einen Dienst, der als Server fungiert und die Kommunikation abwickelt. Bei der Standardinstallation spielt es erst einmal keine Rolle, in welche Richtung übertragen werden soll und wer einen Auftrag initiiert. Die Bedienung erfolgt wahlweise über ein Windows-Programm, den so genannten Requester, einen Webbrowser oder per Kommandozeile (CLI).

Letztendlich ist an allen Endpunkten, die Daten austauschen sollen, eine identische Installation vorzunehmen, bei der nur wenige Abfragen zu beantworten sind. Der Serverdienst läuft wahlweise unter dem lokalen Systemaccount oder unter einem Domänenbenutzer. Alle benötigten Ports sind standardmäßig vorgegeben. Das erleichtert die Einrichtung, erlaubt aber ebenso individuelle Anpassungen. Optional lassen sich auch die Systems Network Architecture (SNA) konfigurieren und die Einstellungen des Requesters im Active Directory registrieren. Falls ein Unternehmen ein Netzwerkmanagement wie Tivoli oder HP Openview einsetzt, kann der Administrator zur einfachen Integration SNMP-Traps sowie ein SNMP Event Logging konfigurieren. Benachrichtigungen erfolgen außerdem wahlweise über Broadcasts oder mittels SMTP. Sofern nicht explizit ein SQL-Server angegeben wird, installiert C:D eine MySQL-Datenbank zur Verwaltung der Protokolleinträge. Um die Einrichtung vieler Knoten zu erleichtern, lassen sich Konfigurationsdateien für nachfolgend noch genauer beschriebene Netmaps und Benutzerauthorisierungen importieren.

Mit etwas Übung dauert die Installation auf einem Windows- oder Linux-Knoten etwa 15 Minuten, auf einem Mainframe sind laut Hersteller etwa zwei Stunden einzuplanen. Wer nach einer Installation unter Windows in den Menüordner schaut, dürfte anfangs angesichts der relativ vielen Einträge etwas erschrecken. Nach einer Einweisung wird aber schnell klar, dass eigentlich nur ein Tool, der Requester, regelmäßig benötigt wird.

Für eine Einarbeitung in C:D sind die mitgelieferten elektronischen Handbücher nur bedingt geeignet, der Leser wird durch viel Text mit wenigen Bildern geradezu erschlagen. Die Unterlagen sind in erster Linie als Nachschlagewerk gedacht. Auch die Online-Hilfe ist nicht Kontextsensitiv, so dass IT-Verantwortliche sich immer wieder durch die Dokumentation zum aktuellen Problem hindurchsuchen müssen. Sterling empfiehlt beim Einstieg in C:D eine etwa dreitägige Schulung, wobei wir dies aufgrund der selbst erhaltenen Einweisung für angemessen halten, um das Programm umfassend bedienen zu können.

Nur eine Handvoll Befehle

Basis von C:D ist eine geradezu minimalistische, Plattform-unabhängige Skriptsprache. Ein auf einem Windows-System erstelltes Skript kann ebenso unter Linux oder auf einem Mainframe laufen. Die Skriptsprache besteht aus den vier Hauptbefehlen *Copy*, *Run Task*, *Run Job* und *Submit*. Der *Copy*-Befehl versteht sich von selbst, mit *Run Task* werden an einem Knoten Programme aufgerufen, mit *Run Job* Batchanweisungen gestartet. *Submit* dient zum Aufrufen eines Prozesses, also eines gespeicherten Skripts, welches wiederum aus den genannten Befehlen bestehen kann. Zu den Hauptbefehlen kommen noch einige Anweisungen hinzu, um Schleifen oder Verzweigungen zu bilden. Prozesse sind letztendlich das wichtigste Instrument, um Abläufe zu programmieren. Sie werden als Datei gespeichert und dann beispielsweise per Scheduler aufgerufen. Neben den Prozessen gibt es noch Arbeitslisten (Work Lists), die wiederum

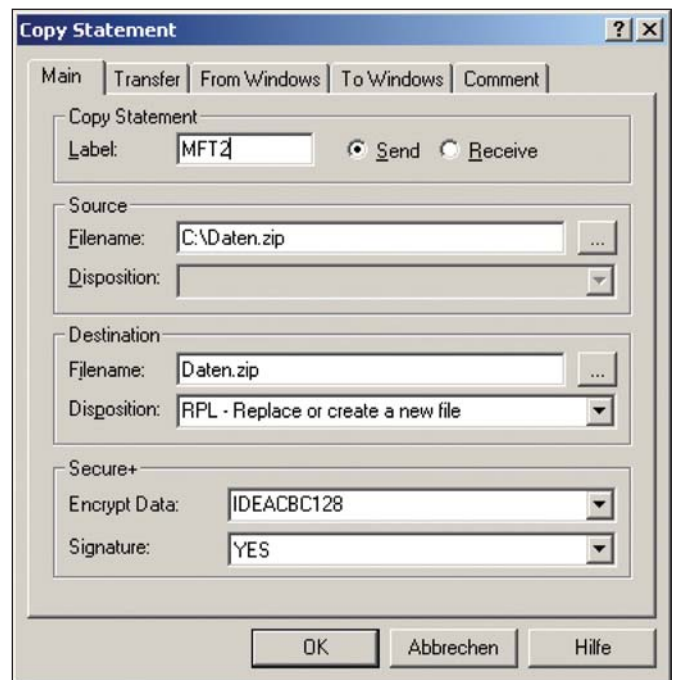


Bild 2: Mit der Option "Secure+" lassen sich die Daten symmetrisch verschlüsseln

Prozesse, aber auch Task- und Jobaufrufe sowie Sende- und Empfangsbefehle enthalten können.

Hinsichtlich der drei Steuermöglichkeiten Kommandozeileingabe, Requester und Web-Browser haben wir im Test dem Requester den Vorzug gegeben, da er aus unserer Sicht am eingängigsten zu bedienen ist. Der Web-Browser besitzt ein zusätzliches Benutzermodell und eignet sich beispielsweise für einen Helpdesk mit eingeschränkten Rechten, um einmal schnell etwas überprüfen zu können.

Der Requester macht von der Oberfläche her einen etwas altbackenen Eindruck. Trotzdem ist er übersichtlich, nur im Statistikbereich sind einige Fenster zum Anzeigen von Abläufen relativ klein geraten und besitzen zudem eine feste Größe. Für eine Nutzung auf einem Netbook mag das passend sein, bei den heute verwendeten großen Arbeitsplatz-Monitoren bleibt aber ein Großteil der Fläche ungenutzt und der Anwender ist ständig dabei, in diversen Listen hoch und runter zu scrollen.

Der Requester eignet sich ideal dazu, Aufträge aus einzelnen Statements zusam-



menzüklicken. Zur Definition eines Statements wie beispielsweise einer Kopieranweisung öffnet sich ein Fenster mit mehreren Registerblättern, in denen das gewünschte auszuwählen beziehungsweise einzutragen ist. Im Hintergrund wird daraus das Skript erstellt. Wer die Skriptsprache selbst erlernen möchte, hat die Möglichkeit, zwischen Statement- und Textanzeige umzuschalten. So lässt sich gut vergleichen, wie der Requester die Statements in Skriptbefehle umsetzt.

Automatisierung des Datentransfers

Zur Automatisierung von Abläufen gibt es mehrere Möglichkeiten. So lässt sich jeder Prozess über einen in C:D integrierten Scheduler steuern, ebenso aber auch über einen Scheduler des Systems. Sollte ein Job abbrechen, erfolgen automatische Restartversuche in unterschiedlichen Intervallen. Die Standardwerte hierzu sind in einer INI-Datei hinterlegt. Durch das Übertragen dieser Datei auf einen anderen Knoten lassen sich schnell die Einstellungen übernehmen.

Neben der Steuerung über einen Scheduler ist C:D auch durch unterschiedliche Schnittstellen gut in andere Werkzeuge integrierbar: Im Windows-/Linux-Umfeld sind dies Java APIs, VBS, C, C++, Shell-Skripte und Batch, bei z/OS können unter anderem Java APIs, Batch ISPF

und CICS verwendet werden. Eine weitere Möglichkeit zur Automatisierung stellt der C:D File Agent dar. Mit ihm lassen sich Verzeichnisse auf Vorhandensein von Dateien mit bestimmten Namen überwachen und anhand dessen Aktionen ausführen, um so Aufträge in C:D mit anderen Abläufen zu koppeln.

Sicherheit wird groß geschrieben

Bei der Standardversion von C:D erfolgt die Benutzerauthentifizierung über die Sicherheit des Betriebssystems. Optional ist zu C:D die Option "Secure+" erhältlich, die wir im Test mitinstalliert haben. Sie ist auf jeden Fall erforderlich, wenn die Daten schützenswert sind oder über eine öffentliche Leitung übertragen werden sollen. Dann erfolgen die Authentifizierung und der Schlüsselaustausch zwischen den kommunizierenden Knoten mit X.509-Zertifikaten. Für eine zusätzliche Datenverschlüsselung nutzt C:D SSL und TLS.

Ein wichtiges Instrument für die grundsätzliche Abgrenzung der möglichen Kommunikationsbeziehungen ist die Netmap. In diese müssen alle Gegenstellen eingetragen sein, mit denen ein Knoten Kontakt aufnehmen soll. Andernfalls wird die Gegenstelle gar nicht zur Auswahl angeboten. Ebenso müssen alle Gegenstellen eingetragen sein, die einen Kontakt aufnehmen dürfen, es sind also letztendlich gegenseitige

Einträge erforderlich. Bei der Aufnahme einer Gegenstelle in die Netmap werden unter anderem die Wiederholversuche und -intervalle sowie die maximale Anzahl der Sessions und der Kommunikationspfad (zum Beispiel TCP) festgelegt. Indem dies für jede Gegenstelle getrennt erfolgt, ist es möglich, individuelle Eigenheiten wie die Bandbreite und die Qualität der Strecke zu berücksichtigen.

Im Gegensatz zu FTP, wo durch den Client eine Benutzerauthentifizierung am Server erfolgt, geschieht dies bei C:D durch Benutzer-Proxies. Dabei wird ein entfernter Benutzer auf einen lokalen Benutzer gemappt. Die Rechte und Einstellungen des lokalen Benutzers allein sind für den Zugriff maßgeblich, hier sind auch die Root-Verzeichnisse für einen Up- und Download hinterlegt. Dabei ist es nicht möglich, durch irgendwelche Verzeichnisstrukturen zu browsen, was die Sicherheit erhöht. Wer also mit C:D eine Verbindung initiiert, weiß gar nicht, mit welchem Benutzer er auf der Gegenseite arbeitet.

Indem sich C:D aufgrund der breiten Betriebssystemunterstützung direkt auf dem System installieren lässt, wo die zu übertragenen Dateien entstehen beziehungsweise benötigt werden, lässt sich die Übertragung vom Start bis zum Ziel verschlüsseln, also auch auf dem Weg durch das Unternehmen, was vor einem Man-in-the-Middle-Angriff an jeder Stelle schützt. Für eine optimale Performance erfolgt die Datenverschlüsselung durch einen symmetrischen Zufallsschlüssel. Da symmetrische Schlüssel vor allem bei mehrfacher Verwendung leichter zu knacken sind als asymmetrische, wird jeder Schlüssel nur einmal benutzt. Wie schon eingangs erwähnt, ist C:D ein eigenes Protokoll. In Verbindung mit der Option Secure+ ist das Produkt nach FIPS 140-2 (NIST) und Common Criteria (NI-APP) zertifiziert.

Neben dem uneingeschränkt nutzbaren C:D gibt es die Version Connect:Direct Select, eine Java Version für unterschiedli-

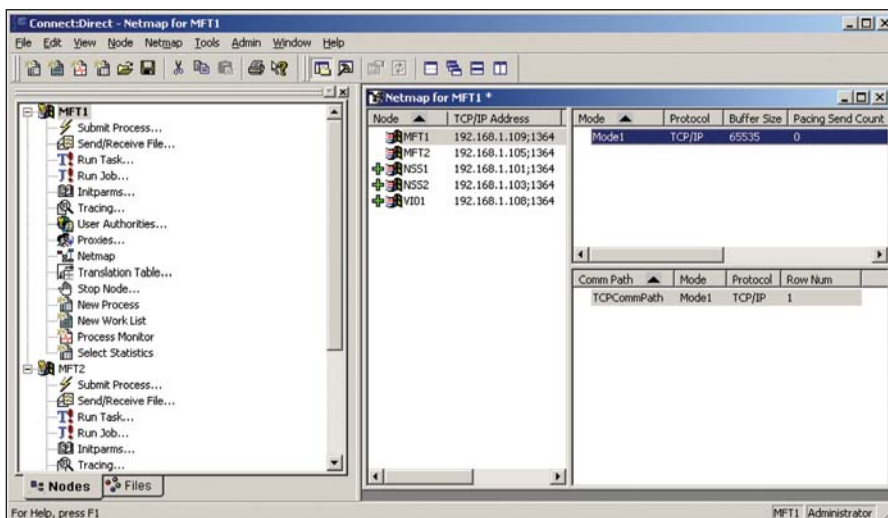


Bild 3: Bei jedem Knoten müssen die Gegenstellen in eine Netmap eingetragen werden, sonst verzweigt C:D den Verbindungsaufbau

WUT

wird

GUT

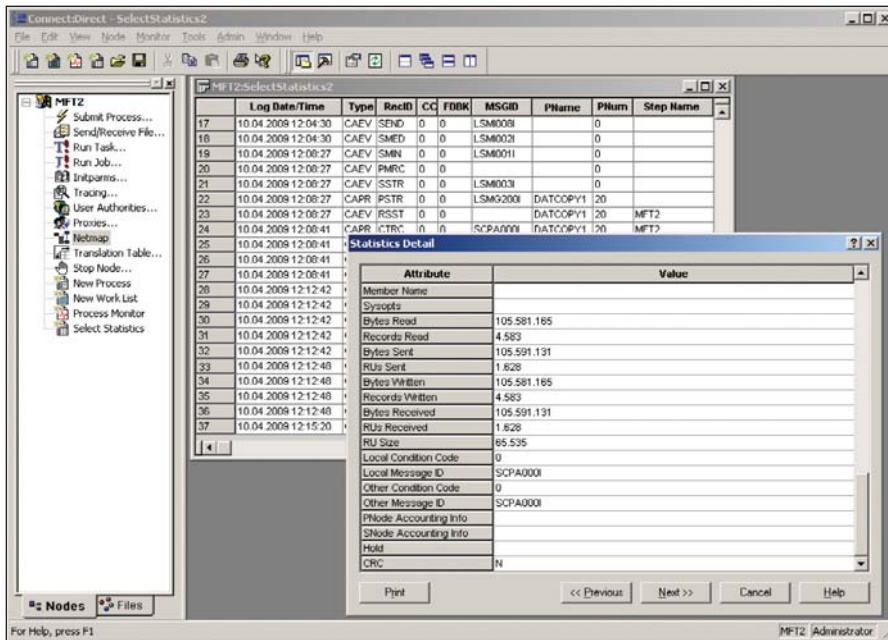


Bild 4: Detaillierte Reports erlauben eine exakte Kontrolle der durchgeführten Aktionen. Zu kleine Fenster mit fester Größe erschweren allerdings die Übersicht.

che Plattformen. Sie kommt beispielsweise dann zum Einsatz, wenn ein Unternehmen A, welches C:D nutzt, mit einem Unternehmen B, welches C:D (noch) nicht verwendet, Daten austauschen will. Dieses erhält dann die Select-Version, in der die Gegenstelle A fest hinterlegt ist. So kann das Tool nur für den Transfer zwischen A und B genutzt werden.

Effiziente Übertragung

C:D eignet sich auch für die Übertragung sehr großer Datenmengen bis hin zu mehreren TByte. Dabei wird mit einem Copy-Befehl immer nur eine Datei übertragen, ein Transfer von mehreren Dateien oder ganzen Verzeichnissen ist nicht möglich. Bei einer Übertragung wird die Datei direkt an die Zielposition geschrieben und nicht erst temporär zwischengespeichert. Das spart Zeit und der Plattenplatz muss nicht doppelt vorgehalten werden. Hervorzuheben ist der geringe Overhead, mit dem das Programm arbeitet, das heißt es werden nur wenig mehr Daten übertragen im Vergleich zur Rohdatenmenge. Bei der testweisen Übertragung einer ZIP-Datei mit 105 MByte lag die übertragene Datenmenge nur um 10 KByte höher.

Darüber hinaus unterstützt C:D optional eine Komprimierung mit verschiedenen Modi. Die Komprimierung erfolgt während des Kopierens blockweise im Puffer, es sind also keine zusätzlichen Schritte erforderlich. Um bei der Übertragung großer Datenmengen zu verhindern, dass bei einem Abbruch ganz von vorne begonnen werden muss, arbeitet C:D auf Wunsch mit Checkpoints mit variablen Abständen. Dann kann das Programm eine abgebrochene Übertragung beim letzten Checkpoint wieder aufsetzen. Weiterhin führt C:D bei Bedarf während der Übertragung eine Zeichensatzumwandlung durch, beispielsweise ANSI/ASCII zu EBCDIC. Auch unterschiedliche Satzendezeichen lassen sich bedarfsgerecht hinzufügen, tauschen oder entfernen. Der Administrator kann innerhalb von C:D Zeichensatztabellen hinterlegen, die dann verwendet werden.

Normalerweise arbeitet C:D Queue-basiert, die Aufträge werden also in eine Warteschlange gestellt und dann abgearbeitet. Dies lässt sich im Requester auch recht gut beobachten. Optional ist aber auch eine parallele Verarbeitung zu verschiedenen Gegenstellen hin möglich.

Was Manager wütend macht, ist die Ungewissheit, ob Geschäftsprozesse in höchster Performance zur Verfügung stehen.

GUT zu wissen, wo der Fehler steckt. Noch besser: wie er sich auswirkt. Unsere **Business Process Management** Software stellt sicher, dass Administratoren richtig reagieren und auch Ihr Management jederzeit über den Zustand aller Geschäftsprozesse im Bilde ist.

Mehr GUTES unter:
www.realtech.de/BPM



theGuard!

REALTECH AG | Telefon: +49.6227.837.651
E-Mail: customer-services-itsm@realtech.de



Im Test fiel positiv auf, dass sich alle oben genannten Funktionen und Optionen individuell parametrisieren lassen. Werden beispielsweise über eine Verbindung bereits komprimierte Daten übertragen, macht eine erneute Komprimierung durch C:D keinen Sinn, dies würde nur unnötig CPU-Leistung kosten und den Transfer womöglich verlangsamen. Bei einer Probe zeigte sich dieser Effekt sofort: Wurde für die Übertragung der oben erwähnten ZIP-Datei auch die Komprimierung von C:D aktiviert, wuchs der Overhead von 10 KByte auf über 2 MByte. Gleichzeitig stieg die Übertragungsdauer von drei Sekunden auf dreizehn Sekunden. Auch die Nutzung von Checkpoints sollte auf die Datenmenge und die Leitungsbandbreite abgestimmt werden, um das Optimum aus Zuverlässigkeit und Durchsatz zu erzielen.

Gespiegeltes Reporting

Ein wichtiger Aspekt beim Managed File Transfer ist die Protokollierung aller Aktionen, um geforderte SLAs nicht nur einhalten, sondern dies auch nachweisen zu können. So vergibt C:D an jede Operation eine fortlaufende, eindeutige Transaktionsnummer. Weiterhin werden die Protokolldateien zum Abschluss einer Operation zwischen den beiden Gegenstellen ausgetauscht. Dies ist quasi die Quittierung einer erfolgreichen Übertragung. Der Vorteil dieses Protokollabgleichs besteht darin, dass auf beiden Seiten die gleichen Protokolle vorliegen mit

identischen Transaktionsnummern. Somit kann jede Seite unabhängig die Übertragungen kontrollieren.

Sollten einmal Probleme aufgetreten sein, lässt sich über die Transaktionsnummer auf beiden Seiten die fragliche Aktion schnell herausuchen. Im Falle von C:D ist die Protokollierung nachweislich revisionssicher. Auch für Supportfälle sind die erzeugten Protokolle recht hilfreich. Hierbei ist anzumerken, dass Sterling Commerce im Rahmen des Wartungsvertrages nicht nur Softwareprobleme bearbeitet, sondern auch bei Problemen mit erstellten Aufträgen unterstützt, also entsprechende Kundenskripte auf Fehler hin analysiert.

Fazit

Im Test zeigte sich schnell, dass ein speziell auf einen Managed File Transfer zugeschnittenes Produkt wie Connect:Direct einer konventionellen Lösung mittels SSH oder SFTP und Standard-Tools deutlich überlegen ist. Individuell einstellbare Parameter wie Wiederholungsversuche, Verschlüsselung, diverse Komprimierungslevel und Checkpoints erlauben eine optimale Abstimmung auf die jeweilige Datenstrecke, um eine möglichst schnelle und zuverlässige Übertragung zu erzielen. Eine kurze Schulung durch den Hersteller empfiehlt sich, um bereits nach wenigen Tagen das Programm umfassend einsetzen zu können. Eine sehr breite Betriebssystemunterstützung, die auch den Einsatz an einem Mainframe vorsieht, erlaubt eine Konfiguration und Absicherung der Übertragungsstrecke von Endpunkt zu Endpunkt, was die Überwachung enorm erleichtert. Das integrierte Reporting ist revisionssicher, eine Alarmierung erfolgt

Optimierungsbedürftig erscheint uns allerdings die zentrale Benutzeroberfläche des Requesters. Hier wird zu viel mit festen Fenstergrößen gearbeitet, was vor allem Analysen erschwert. Wünschenswert sind zudem übersichtlichere Handbücher und eine effektivere, Kontext-sensitive Hilfe. (jp)



Produkt

Programm für den revisionssicheren Datentransfer (Managed File Transfer – MFT).

Hersteller

Sterling Commerce
www.sterlingcommerce.de

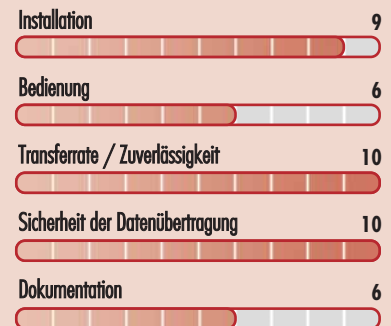
Preis

Ab 8.600 Euro für eine Vollversion unter Windows, im Detail richten sich die Preise nach Plattform, Anzahl der gleichzeitigen Sitzungen oder CPUs.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für den regelmäßigen, sicheren Transfer großer Datenmenge bei gleichzeitiger Einhaltung höchster Sicherheitsanforderungen und SLAs bezüglich der Zuverlässigkeit.

bedingt für gelegentliche Transfers bei eher mäßigen Sicherheitsanforderungen. Dann ist zu prüfen, ob die Anforderungen den Preis und den Aufwand rechtfertigen.

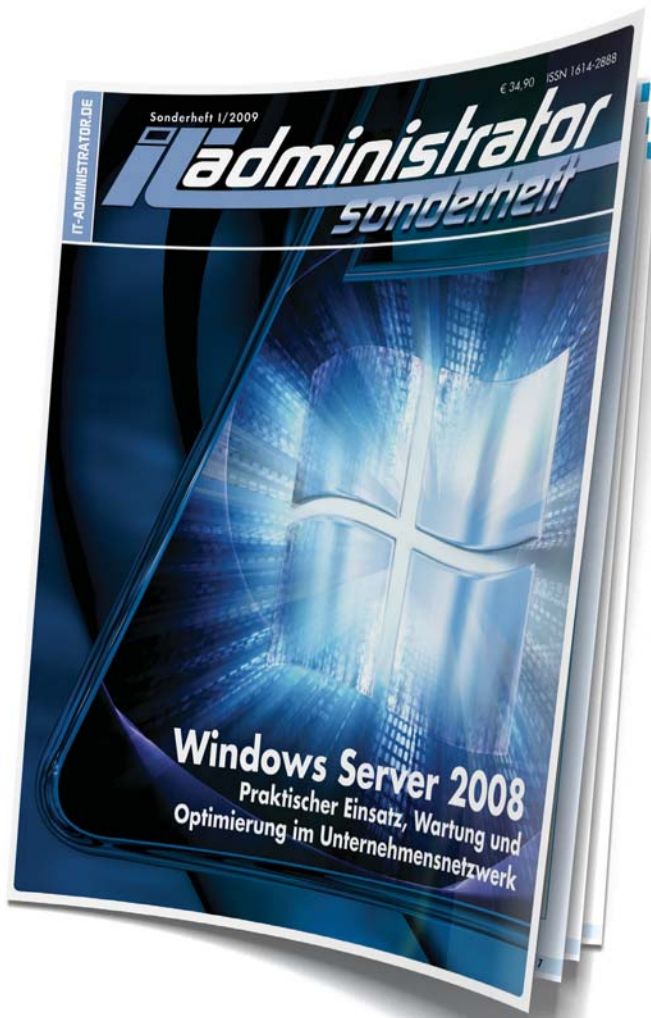
nicht für Unternehmen, die keinen Bedarf für sichere Übertragungen haben. Hier reichen preiswerte, konventionelle Lösungen, die beispielsweise auf FTP oder SFTP basieren.

Sterling Commerce Connect:Direct 4.4

Attribute	Value
Member Name	
Sysopts	
Bytes Read	105.581.165
Records Read	4.583
Bytes Sent	105.591.131
RUs Sent	1.628
Bytes Written	105.581.165
Records Written	4.583
Bytes Received	105.591.131
RUs Received	1.628
RU Size	65.535
Local Condition Code	0
Local Message ID	SCPA0001
Other Condition Code	0
Other Message ID	SCPA0001
PNode Accounting Info	
SNode Accounting Info	
Hold	
CRC	N

Bild 5: Bei optimaler Einstellung erzeugt C:D nur einen geringen Transfer-Overhead und arbeitet damit schnell

per SNMP, SMTP und Broadcast.



Bestellen Sie jetzt das IT-Administrator Sonderheft I/2009!

180 Seiten Praxis-Know-how rund um

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/



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.

So erreichen Sie unseren
Vertrieb, Abo- und
Leserservice:

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

Tel: 06123/9238-251

Fax: 06123/9238-252

leserservice@it-administrator.de

Diese und weitere Aboangebote
finden Sie auch im Internet
unter www.it-administrator.de



Heinemann Verlag

Leopoldstraße 85

D-80802 München

Tel: 089-4445408-0

Fax: 089-4445408-99

Geschäftsführung:

Anne Kathrin Heinemann

Matthias Heinemann

Amtsgericht München HRB 151585

ITA 0709

**Im Test: NetApp FAS2020**

Storage und virtuelle Landschaft in einem

von Dennis Zimmer

Die Storage-Systeme von NetApp gehören zu den beliebtesten in der Servervirtualisierung und vor allem in der Desktopvirtualisierung. IT-Administrator hat das Einstiegssystem FAS 2020 näher in Augenschein genommen. Dieses Storage-System steht etwa in Konkurrenz zu einer HP MSA2000 und kann zum Betrieb kleinerer Virtualisierungsumgebungen genutzt werden. Besonders beim Funktionsumfang überraschte die Speicherlösung.

Vor der Anschaffung eines Storage-Systems muss der Administrator erst einmal wissen, welche Datenmenge und Performance er für den späteren Betrieb benötigt. Aufgrund dieser Daten kann bei NetApp dann der betreuende Partner eine Planung der Storage-Lösung durchführen. Wie bereits erwähnt, ist das NetApp FAS2020 ein Einstiegsmodell für kleinere Umgebungen – kann aber prinzipiell von der Datenmenge auch in mittlere Bereiche wachsen (bis zu 68 Festplatten). Dabei sollten vor allem die Performanceanforderungen an den Controller des Storage-Systems nicht unterschätzt werden. Doch immerhin lassen sich die Köpfe eines NetApp-Systems tauschen, ohne dass es zu einem Datenverlust kommt. Damit besteht die Möglichkeit, langsam zu wachsen. Die grundsätzliche Verwaltung passiert unabhängig von der Größe mit dem NetApp-eigenen Betriebssystem ONTAP (derzeit in Version 7.3 verfügbar).

Weiterhin muss der IT-Verantwortliche bei der Ersteinrichtung des NetApp-Filers beachten, dass das ONTAP-Betriebssystem die ersten drei Festplatten nutzt. Dazu wird die Basiseinheit, ein sogenanntes "Aggregat", angelegt. Diesem werden die physikalischen Festplatten zugewiesen und es ist verantwortlich für den RAID-Level. Kommt etwa RAID 4 zum Einsatz, geht



Bild 1: Das NetApp-Interface gibt eine Übersicht zu den Volume-Einstellungen und erlaubt das Resizing

dadurch eine Festplatte im Aggregat für die Parität verloren. Bei dem auf höhere Datensicherheit ausgelegten RAID DP (Double Parity – zwei Festplatten im Verbund können ausfallen, im Gegensatz dazu ist es bei RAID 4 nur eine Festplatte), gehen folglich zwei Festplatten in diesem RAID-Level an die Parität verloren.

RAID4 versus Double Parity

Damit das Storage-System auf einen Plattenausfall schnell reagiert werden kann, ist mindestens eine Spare-Festplatte notwendig (RAID DP – zwei Spares). Da-

mit wird auch schnell klar, dass bei der Anlage mehrerer Aggregate eine sorgfältige Planung nötig ist. Die Maximalgröße eines Aggregats liegt ab ONTAP-Version 7.3 bei 16 TByte. Außerdem sollten immer nur gleiche Festplatten in einem Aggregat betrieben werden, also etwa SAS 300 GByte für das Aggregat 0; SATA 500 GByte im Aggregat 1. In einer kurzen Beispielrechnung möchten wir die Unterschiede im Speicherbedarf verdeutlichen. Dabei nutzen wir 14 SAS-Festplatten mit jeweils 300 GByte Kapazität. In jedem Fall sind 3 Festplatten für ONTAP

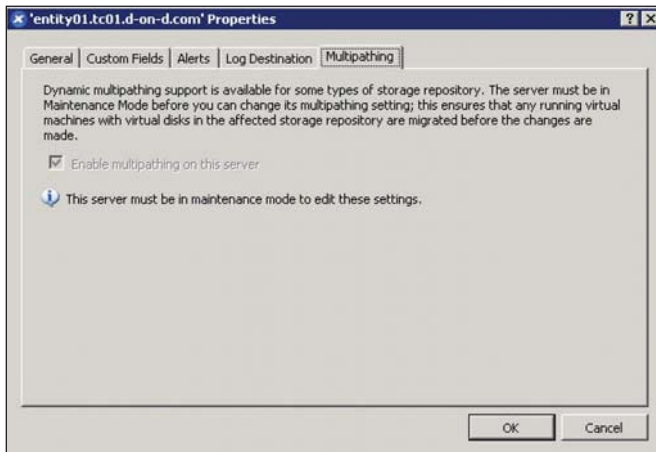


Bild 2: Das Multipathing erlaubt es einem Server, über mehrere Pfade dasselbe Festplattensubsystem anzusprechen

reserviert, damit sind nur noch 11 Platten wirklich verfügbar:

- Ein Aggregat, RAID DP:
 - 1 x Parity
 - 1 x Double Parity
 - 2 x Spare
 - 7 x 300 GByte SAS Rest = 2,1 TByte
- Zwei Aggregate, RAID DP:
 - 2 x Parity
 - 2 x Double Parity
 - 4 Spare
 - 3 x 300 GByte SAS Rest = 900 GByte

Dieses Beispiel verdeutlicht, weshalb ein Verständnis der NetApp-Architektur so wichtig ist, um nicht sinnlos Festplattenkapazität zu verschwenden. Im Gegensatz dazu gilt es zu beachten, dass die Zeit für ein RAID-Rebuild im Falle eines Plattenfehlers mit der Größe der verwendeten Festplatten steigt. Daher sollten die Vor- und Nachteile abgewägt werden.

Auf dem Aggregat kommt übrigens das NetApp-eigene Dateisystem WAFL (Write Anywhere File Layout) zum Einsatz, das unter anderem die Basis für die Snapshot-Fähigkeiten bildet. Die verwendeten RAID-Gruppen kommen außerdem sehr gut mit Größenerweiterungen klar, wodurch es möglich ist, dem RAID nachträglich und im laufenden Betrieb zusätzliche Festplatten zuzuordnen und damit den Plattenplatz zu vergrößern. Eine Ver-

kleinerung ist jedoch nicht möglich. Die Aggregate bilden die Basis zur Anlage von Volumes, die sich später als Freigaben für Linux, VMware ESX, Citrix XenServer (NFS) oder Windows (CIFS) sowie LUNs (iSCSI, FC) nutzen lassen. Sämtliche Snapshot-Aktivitäten werden auf Volumes oder LUNs und nicht auf Aggregaten oder

Shares angewandt. Dies sollten Administratoren ebenfalls im Hinterkopf behalten, bevor sie die Volumes mit zu vielen LUNs oder Freigaben belegen. Auch Volumes können jederzeit vergrößert werden.

Für unseren Test haben wir folgende Konfiguration aufgesetzt:

- 1 Aggregat mit 12 zugeordneten Festplatten
- 6 Volumes à 300 GByte
- 2 LUNs à 250 GByte iSCSI (jeweils 1 LUN VMware ESX, Citrix XenServer)
- 2 LUNs à 250 GByte FC (jeweils 1 LUN VMware ESX, Citrix XenServer)
- 2 NFS-Freigaben (jeweils eine Freigabe VMware ESX, Citrix XenServer)
- 2 Netzwerkanschlüsse für die iSCSI-Nutzung
- 2 Netzwerkanschlüsse für die NFS-Nutzung
- 2 Anschlüsse für die FC-Nutzung

Folgende Funktionen haben wir dabei lizenziert: FC, CIFS, NFS, FlexClone. Kostenfrei waren iSCSI, Thin Provisioning und Deduplikation.

Konfiguration NetApp FAS2020

Nach der Initialeinrichtung unseres Speichersystems über das Managementinterface wechselten wir auf die Weboberfläche, um die komplette Konfiguration durchzuführen. Das GUI ist über https://{NetApp-IP-Adresse}/na_admin und dem root-Benutzer erreichbar. Ob-

wohl die Verwaltung sehr gut gegliedert ist, finden sich NetApp-Anfänger nicht direkt zurecht. Hintergrund dafür ist allerdings weniger die Bedienbarkeit, sondern eher das fehlende Grundverständnis für die Architektur des NetApp-Fileers. Daher sollte bei der Ersteinrichtung ein erfahrener Techniker zur Seite stehen.

Alle Funktionen der Weboberfläche und noch einige darüber hinaus können über die Kommandozeile des NetApp-Systems genutzt werden. Dabei ist das CLI über den Managementadapter oder über einen Standardethernet-Adapter und SSH verfügbar. Natürlich lässt sich auch aus der Webverwaltung direkt auf die Konsole zugreifen.

Der Testaufbau bestand aus einem Storage-System FAS2020 mit vier GBit-Anschlüssen (NFS + iSCSI) und zwei 4-Gbit-Fiber Channel-Anschlüssen. Daher sind als Protokolle zu den HP DL385 G5 Servern NFS, iSCSI und Fiber Channel möglich. Die Netzwerke wurden über Cisco Catalyst 2950 (48 Ports) und Brocade SilkWorm angebunden und sind jeweils redundant ausgelegt. Auf jeweils einem Serverpaar haben wir VMware ESX 3.5 und Citrix XenServer 5 installiert und mit der NetApp Integration getestet. Wir verbanden uns hierzu über das Microsoft Remote Desktop Protocol (RDP) auf einen Windows 2003-Client, von dem aus der weitere Zugriff auf die Server und Storage-systeme, sowie Netzwerkkomponenten erfolgte.

Komponenten NetApp FAS2020

- Hersteller: Network Appliance
- Typ: FAS2020, Single Head
- OS: ONTAP v. 7.2
- Netzwerk: Zwei Ethernet Anschlüsse à 1 Gbit
- Fiber Channel: Zwei Ports à 4 Gbit
- Festplatten: Zwölf 300 GByte SATA
- Konfiguration: Ein Aggregat à 12 Festplatten, RAID DP Protokoll: NFS, iSCSI, FC

Komponenten HP DL385 G5

- Prozessor: 2 Sockel, Intel 5420 QuadCore, 2,5 GHz
- RAM: 8 GByte RAM
- Festplatten: RAID1 mit zwei 72 GByte SAS
- Netzwerkanschlüsse: Zwei Anschlüsse Gbit Ethernet on Board, 4 Ports Intel E1000 Serveradapter
- FC: 4-Gbit-FC DualHBA FC-1242SR

Unsere Testumgebung



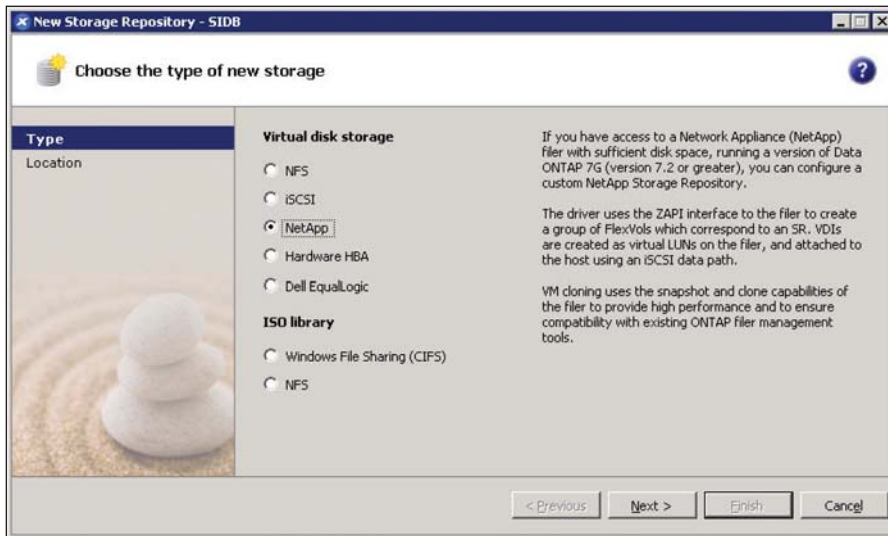


Bild 3: Storage Repositories lassen sich über einen Wizard hinzufügen

Anschluss und Konfiguration VMware ESX 3.5

Die Verbindung des NetApp-Systems mit den ESX-Servern unterscheidet sich nicht vom Standardvorgehen bei der Storage-Anbindung. Es existieren selbstverständlich Best Practices Dokumente [1], welche bei der Einrichtung helfen. Allerdings sollte zur Verbesserung der Cluster Failover Performance und der Diagnosemöglichkeiten die Host Utilities in der Service Console der ESX-Server installiert werden. Diese Host Utils werden auf der NetApp-Webseite (NOW Account) bereitgestellt.

Da der VMware ESX-Server die Pfade nicht aus der Sicht des Storage, sondern nur aus der Sicht des Servers konfiguriert, wird nicht auf Individueleinstellungen des Speichersystems eingegangen. NetApp reagiert auf diesen Zustand mit den "VMware Host Utils", die auf der Service Console des ESX-Servers installiert werden. Neben den Pfadeinstellungen optimieren diese Tools auch die HBA-Einstellungen (Host Bus Adapter, FC oder iSCSI, Emulex oder QLogic), was den Port Timeout angeht. Derzeit existieren keine Host Utils für ESXi. Diese werden erst mit vSphere verfügbar.

Auch unter XenServer besteht die Möglichkeit das NetApp-System standardmäßig zu verbinden und zu konfigurieren. Allerdings existiert auch die Möglichkeit

einer intelligenten Storageverwaltung durch XenServer direkt. Durch diese Funktionalität verwaltet der XenServer die Stagesysteme und erstellt, löscht und konfiguriert Volumes und LUNs selbstständig bei der normalen Verwaltung der virtuellen Maschinen.

Betrieb mit XenServer

Citrix XenServer unterstützt im Gegensatz zu VMware ESX die vollständige Integration der NetApp und deren Verwaltung. Zur Vollständigkeit: gleiches gilt für Dell EqualLogic Storage. Diese Funktionalität richtet sich vor allem an kleinere Unternehmen, in denen Storage- und Server-Teams aus den gleichen Administratoren bestehen. Die NetApp-Integration nimmt dem Administrator die SAN-Verwaltung, was Bereitstellung, Löschung und Pfadverwaltung angeht komplett ab. Dies bedeutet, dass der Anwender eine neue virtuelle Maschine erstellt und XenServer im Hintergrund automatisch die LUN und die Zuordnung erledigt. Die geht soweit, dass bei Verwendung der Volclone / LUN clone-Funktionalität die virtuellen Maschinen mit XenServer-Mitteln in Sekunden geklont und bereitgestellt werden können. Selbst Thin Provisioning und Deduplikation wird mittels XenServer konfiguriert.

Doch hat dieses Szenario auch einige Nachteile: Der XenServer legt im Standard acht

600 GByte große Volumes mit Thin Provisioning und Deduplikation an. Auf diesen Volumes wird für jede virtuelle Maschine und deren Festplatte eine eigene LUN angelegt und mit dem XenServer verbunden. Bei der Namensgebung kommen dann die kryptischen UUIDs zum Einsatz. Dies hat zur Folge, dass auf dem XenServer zwar alles richtig und übersichtlich aussieht, die Verwaltung über das NetApp-Management aber sehr unübersichtlich wird. Daher eignet sich diese Funktionalität nur für kleinere Infrastrukturen und der Administrator sollte ein wenig üben, bevor er diese Funktion produktiv nutzt.

Übrigens stellt der XenServer die LUN/Host-Zuordnungen selbstständig und stetig korrekt ein, was bei Live-Migrationen beziehungsweise Neustarts von virtuellen Systemen in unserem Test zu Multipathing-Fehlern im XenCenter-Protokoll führte. Diese können zwar ignoriert werden, lästig ist es trotzdem.

Plattenanschluss

Natürlich lässt sich das NetApp-System auch ohne die zusätzlichen Verwaltungsfunktionen des XenServer einsetzen und die LUNs direkt über iSCSI verbinden. Dazu muss beim Hinzufügen des SR iSCSI statt NetApp ausgewählt werden. Da die Clusterfunktion (von Marathon lizenziert) die Heartbeat LUN nicht über die NetApp Integration nutzen kann, muss in diesem

Im Rahmen der Kooperation des Schweizer IT-Systemhauses Kybernetika und des IT-Administrator Magazins fand dieser Produkttest im Datacenter on Demand statt. Kybernetika ist der Betreiber des "Datacenter on Demand" (www.d-on-d.com), einem Dienstleistungsangebot, welches IT-Abteilungen erlaubt, modernstes Equipment anzumieten und dies komfortabel und remote über das Internet für Schulungen oder Tests zu nutzen.

Die Ausstattung des Datacenter on Demand besteht aus Enterprise-Class Hardware (Server, Speicher-Systeme, SAN- und Netzwerk-Komponenten) von Herstellern wie Cisco, HP, VMware, NetApp und viele mehr. Aktuell können Nutzer unter 37 physikalischen Servern sowie 12 Speichersystemen wählen.

**Getestet im
Datacenter on Demand**



Fall sogar zwingend eine iSCSI-LUN direkt zum XenServer verbunden werden.

Die FC SRs (Storage Repositories) fügten wir im Test über die Funktion "Hardware HBA" im Storage Repository-Wizard hinzu. Dabei hat das System zuerst nach dem Target (Storage System) gescannt und anschließend nach den verfügbaren LUNs. Ansonsten ist der Ablauf mit dem Vorgehen bei iSCSI-Disks identisch. Allerdings sollte der Administrator in jedem Fall vor der ersten Verbindung mit dem SAN das Multipathing in den Eigenschaften des Hosts aktivieren, während dieser sich im Maintenance-Modus befindet.

Die NFS-Unterstützung seitens des XenServer läuft über den Wizard zum Hinzufügen neuer SRs, der die IP/DNS-Adresse des Storage-Adapters anfordert und nach der Freigabe fragt. Dabei ist zu beachten, dass ISO-Repositories und normale SRs bei XenServer existieren, die sich durch die Zugriffsart und die Nutzung unterscheiden. ISO SRs werden immer als Read-Only verbunden, SRs sind dagegen beschreibbar. Genau wie unter VMware ESX müssen die NFS-Freigaben mit Root Access freigegeben werden, also die Option "no_root_squash" aktiviert sein.

Partition Alignment

Das Partition Alignment ist in jeder Infrastruktur mit Blockzugriff (SCSI, iSCSI, FC,

nicht jedoch NFS) ein Thema, verursacht durch die Verschiebung der Sektoren (MBR – Master Boot Record). Je mehr Schichten sich zwischen der physikalischen Festplatte und dem Betriebssystem befinden, desto größer sind die Folgen des Partition Alignment. Beim Einsatz von NetApp und VMware/Citrix existieren drei Schichten oberhalb der physikalischen Festplatte: Das WAFL-Dateisystem, das VMFS/LVM und NTFS/EXT3 – also vom Storage über das Virtualisierungssystem zum Dateisystem des Gastbetriebssystems.

Aus diesem Grund sollten bereits bei der Installation der virtuellen Maschine die Partitionen mit einem korrekten Layout versehen werden. Da dieses Thema erst in den letzten Monaten öffentlich diskutiert wurde, sind jedoch bereits viele bestehenden virtuellen Maschinen falsch eingerichtet. NetApp hat sich dem Partition Alignment angenommen und sowohl ein Tool zum Scannen der Partitionen, als auch ein Tool zum Korrigieren des Alignments erstellt und gibt dieses an anfragende Kunden weiter. Limitiert werden diese Werkzeuge nur durch die Anzahl der Partitionen innerhalb des VMDKs, welche korrigiert werden können [2].

Eindrucksvolle Deduplizierung

NetApp bietet einige sinnvolle Zusatzfunktionen. Im Normalfall werden bei Nutzung von blockorientiertem Zugriff

(iSCSI, FC) beispielsweise die virtuellen Festplattendateien immer mit voller Größe erstellt, also 20 GByte belegen auf dem Storage 20 GByte – selbst wenn nur 5 GByte wirklich genutzt werden. Das "Thin Provisioning" umgeht dieses Verhalten und optimiert so den genutzten Speicherplatz. Ein Server erhält so zwar 20 GByte, im Storage



Bild 4: Über einen Wizard lassen sich die NFS-Einstellungen vornehmen



**Jetzt kostenlose
Basic-Edition
anfordern!**

www.rent-a-mind.de/basic-edition

- » **Unified Messaging:** Die Alternative zu Lotus Notes, Exchange, etc.
- » **Nachrichten:** E-Mail, Telefax, Brief
- » **Organisation:** Aufgabenübersicht, Kalender, Projektplanung inklusive.
- » **Dokumentenmanagement,** Automation, RSS-Reader, Kamera-Aufzeichnung, Video-Recorder, uvm.
- » **Mobiles Arbeiten** Client-/Server-Zugriff über IP: Notebook, PDA, Web-Frontend und das iPhone.
- » **Integriertes Backup** inklusive externer Datenspeicher-Lösung.
- » **Bis zu 50% Upgrade-Rabatt.**

Wir beraten Sie gerne und erstellen ein individuelles Angebot. Rufen Sie uns an!



rent a mind
Dienstleistungs- und Verlags GmbH
Memeler Str. 30 | 42781 Haan bei Düsseldorf
Telefon 02129 3457-0
kontakt@rent-a-mind.de | www.rent-a-mind.de



werden allerdings nur die belegten 5 GByte verbraucht.

Außerdem lässt sich Thin Provisioning zur Überbelegung nutzen. Obwohl physikalisch nur 2 TByte im Storage verfügbar sind, können 4 TByte nach außen vergeben werden. Natürlich darf die reale Datennutzung dann die 2 TByte nie übersteigen. Bezüglich Planung und Verwaltung auf Serverseite vereinfacht Thin Provisioning die Situation dadurch wesentlich, da sich Festplattenvergrößerungen vermeiden lassen, wenn die Festplatte von Beginn an größer dimensioniert wird. Gefahr droht eher im Storage-Management, denn hier muss der Administrator den real verfügbaren Platz immer im Auge behalten.

Ein weiteres Feature zur Speicheroptimierung stellt die Deduplikation dar. Das Verfahren läuft bei NetApp nachts durch und scannt die Daten per Checksummen. Redundante Dateien werden anschließend zusammenfasst und damit dedupliziert. Vor allem bei Infrastrukturen mit vielen gleichartigen Systemen ist Deduplikation ein wahres Allheilmittel, das bis zu 80 Prozent des Datenaufkommens einsparen kann. Technisch bedeutet dies, dass die Daten nur einmal vorgehalten werden und Redundanzen als Verlinkung existieren. Die NetApp-Deduplikation lief in unserem Test mit NFS besser als im SAN und spielte die maximalen Möglichkeiten bei sich möglichst wenig verändernden Daten voll aus.

Snapshots und Replikation

Snapshots sind eine der herausragenden Funktionen von NetApp. Allerdings soll-

te der Snapshot-Einsatz nicht übertrieben werden, da darunter der Plattenplatzverbrauch und die Übersichtlichkeit leiden. Snapshots bieten nichts desto trotz sehr große Vorteile im NetApp-Umfeld, da das Verfahren "Copy-on-First Write" genutzt wird. Damit kann jeder Snapshot unabhängig der Reihenfolge gelöscht werden, ohne dass es zum Daten- oder Zugriffsverlust anderer Snapshots oder des Originalvolumes kommt. Weiterhin sind die Snapshots keine 1:1-Kopien der LUNs, wodurch nur die Änderungsdaten nach seit Erstellung des Snapshots Plattenplatz belegen.

Mittels der "FlexClone"-Funktion ist es außerdem möglich, Volumes als Ganzes zu kopieren. Dieser Klonen können einem Server zusätzlich zugeordnet werden, beispielsweise um Dateien oder virtuelle Maschinen wiederherzustellen.

Unter "SnapMirror" schließlich ist eine Datenreplikation beziehungsweise ein Datenspiegel zwischen zwei NetApp-Systemen zu verstehen. Diese Lösung ist auch zwischen unterschiedlichen NetApp-Filemodellen möglich. Etwa wird häufig zwischen einem leistungsfähigeren NetApp-System im Hauptstandort und einem kleineren System im Backupstandort der Datenbestand repliziert. Fällt der Hauptstandort aus, kann der Administrator sehr schnell den Betrieb am Backupstandort wieder aufnehmen. Allerdings ist dabei auf die Datenkonsistenz zu achten.

Fazit

Unser Test hat gezeigt, dass NetApp mit der FAS2020 einen leistungsfähigen und dennoch preislich günstigen Storage für kleinere Infrastrukturen anbietet. Aufgrund der Flexibilität dank Snapshots, Thin Provisioning und Deduplikation liegt der Funktionsumfang in den meisten Fällen weit vor der Konkurrenzshardware. Allerdings ist die FAS2020 sehr skalierbar und kann mehrere TByte Storage verwalten. Wird die Last zu groß für den Kopf, lässt sich dieser problem-

los einen größeren tauschen, ohne dass es zum Datenverlust kommt. Weiterhin ist es möglich die FAS2020 mit weiteren Netzwerkadaptern – wenn auch begrenzt – auszustatten oder mit einem zweiten Kopf zu Clustern. (dr)

Produkt

Storage-System

Hersteller

NetApp
www.netapp.com

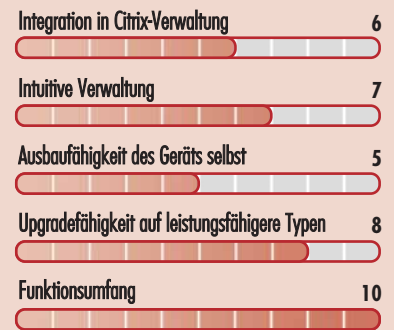
Preis

Ein FAS2020-System mit sechs SATA-Platten à 500 GByte inklusive CIFS und NFS liegt bei rund 15.000 Euro. Ohne CIFS und NFS beläuft sich der Listenpreis auf rund 10.000 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für kleine virtualisierte Landschaften (etwa auch Außenstellen), Mischumgebung virtuell/physikalisch, Windows Fileservice mittels NetApp FAS2020 nativ, Infrastrukturserver als VM mittels iSCSI, FC- oder NFS-Anbindung.

teilweise für Mischumgebung oder für die Spiegelung zwischen FAS2020 und FAS2050, wobei die FAS2050 als zentraler Storage dient und die FAS2020 als Failoversystem genutzt wird.

nicht für größere Virtualisierungsprojekte (30 Server-VMs und mehr) – abhängig des Leistungsbedarfs der VM, Infrastrukturen mit hoher Last auf dem Storagesystem oder Infrastrukturen mit schnellem Datenwachstum.

NetApp FAS2020

[1] Best Practices zu NetApp und VMware VI 3
www.netapp.com/us/library/technical-reports/tr-3428.html

[2] Blog-Beitrag zur Partitionszuteilung
http://blogs.netapp.com/storage_nuts_n_bolts/2009/01/mbrscanmbralign.html

Links





Im Test: Infowatch CryptoStorage Schlanker Datentresor

von Jürgen Heyer



Geklaute Notebooks, ausspionierte PCs und entwendete Daten von Netzlaufwerken sind im Büroalltag keine Seltenheit. Einen wirksamen Schutz gegen unberechtigten Zugriff bietet eine geeignete Datenverschlüsselung. CryptoStorage von Infowatch eignet sich dabei für verschiedene Szenarien sowohl zur Absicherung des eigenen Arbeitsplatzes als auch zum Schutz gemeinsam genutzter Verzeichnisse. IT-Administrator hat das Tool für Sie getestet.

CryptoStorage-Editionen

Infowatch bietet CryptoStorage in einer Personal-Version an, die wir zum Test zur Verfügung gestellt bekommen haben. Darüber hinaus gibt es eine Enterprise-Version, die in Europa vorerst nur als Beta-Version erhältlich sein wird. Der größte Nachteil der Personal-Version bei der Administration vieler Benutzer ist das Fehlen einer zentralen Benutzerverwaltung. Diese kommt mit der Enterprise-Version, die sich aber noch im Betastatus befindet, so dass uns ein Test nicht sehr sinnvoll erschien. Dennoch gehen wir auch auf die Funktionen dieser Variante ein.

Während die Personal-Version den Austausch verschlüsselter Daten auf Wechselträgern erlaubt – es werden hier nur Benutzer und Passwort zur Eingabe benötigt – können die Daten bei der Enterprise-Version das Netzwerk in verschlüsselter Form nicht verlassen. Vorgesehen ist allerdings ein Offline-Betrieb, zu dem ein Benutzer für eine bestimmte Zeit freigeschaltet werden kann, damit er beispielsweise auch am Notebook bei fehlendem Netzwerkzugang auf lokal abgelegte verschlüsselte Daten zugreifen kann. Andernfalls ist der

Zugriff gesperrt. Alle Benutzer, die mit der Enterprise-Version arbeiten, müssen sich auf einem zentralen Sicherheitsserver authentisieren. Die Authentisierung erfolgt entweder per Passwort, Private Key oder Zertifikat, wobei die Standards X.509 und PKCS unterstützt werden. Dabei ermöglicht die Enterprise-Version auch den Einsatz von Aladdins eToken, ruToken und Zertifikaten auf Datenträgern (USB-Stick, Festplatte), um so eine Zweifaktoraauthentisierung zu realisieren.

Bei der Enterprise-Version erfolgt die komplette Administration durch eine zentrale Konsole, von der aus auf entfernten Systemen die Benutzerlisten geändert werden können. Weiterhin lassen sich sehr individuelle Zugriffsrechte vergeben, wobei sich Infowatch an praxisnahen Szenarien orientiert hat. Beispielsweise kann ein Administrator bei Bedarf zwar verschlüsselte Objekte einrichten und die Zugriffsrechte der anderen Benutzer ändern, aber selbst nicht auf den Inhalt der Container zugreifen.

Die zum russischen Antivirus-Hersteller Kaspersky Lab gehörende Firma Infowatch deckt mit CryptoStorage unterschiedliche Anforderungen an eine Datenverschlüsselung ab. Diese beginnen bei einer Container-Datei, die der Anwender als zusätzliches Laufwerk sieht. Alle Dateien, die er hier ablegt, werden verschlüsselt gespeichert. Der Zugriff auf den Container ist erst nach einer Anmeldung möglich. Weiterhin lassen sich bereits bestehende Verzeichnisse verschlüsseln, so dass dann keine Änderung der Datenablagestruktur erforderlich ist. Die dritte Möglichkeit besteht in der Verschlüsselung ganzer Partitionen, was auch mit Bootlaufwerken gelingt. Dann kann das System erst nach einer Anmeldung überhaupt gestartet werden. Eine Besonderheit des Tools ist, dass verschlüsselte Verzeichnisse und Container auch auf Netzwerkfreigaben angelegt werden können, kombiniert mit einer Benutzerverwaltung, so dass auch mehrere Anwender gemeinsam in verschlüsselten Bereichen arbeiten können.



Bild 1: Die Verschlüsselung ganzer Festplatten kann durchaus einige Stunden dauern



Die Betaversion bietet weder eine Integration in das Active Directory noch einen Abgleich mittels LDAP, vielmehr ist eine eigene Benutzerdatenbank zu pflegen. Es gibt aber wohl Überlegungen des Herstellers, eine derartige Integration in die endgültige Version für den europäischen Markt einzubauen. CryptoStorage Enterprise ermöglicht ein zentrales Logging aller Benutzeraktivitäten, welches sich an die jeweiligen Erfordernisse anpassen lässt. Bezüglich der Ablage der Daten auf Netzlaufwerken unterstützt die Enterprise-Version auch Microsoft DFS (Distributed File System).

Daneben besteht eine spezielle Möglichkeit, verlorene Schlüssel wiederzuerlangen. Das macht Sinn, wenn ein Schlüssel tatsächlich vergessen wurde oder ein Mitarbeiter im Streit die Firma verlässt und den Schlüssel nicht mehr verraten will. Dann muss eine so genannte Erneuerungskommission tätig werden, die durch bestimmte Eingaben an einem zentralen Server gemeinsam eine Erneuerung eines unbekannten Schlüssels veranlassen kann.

Schlank und einfach

Die Personal-Version von CryptoStorage 1.0 ist nur rund 3,7 MByte groß und in wenigen Sekunden installiert. Eine zusätzliche Konfiguration ist normalerweise nicht erforderlich. Es gibt zwar ein kleines Konfigurationstool, das aber nur den Status von drei Diensten steuert. Diese sind für die drei eingangs aufgeführten Verschlüsselungsarten Container, Verzeichnis und Partition zuständig. Ein weiteres kleines Tool ermöglicht das sichere Löschen von verschlüsselten Partitionen, falls diese nicht mehr benötigt werden.

Voraussetzung für den Betrieb von CryptoStorage ist ein System unter Windows 2000 Server SP4, Windows 2003 Server, Windows 2000 Professional SP4, Windows XP, Vista SP1

Systemvoraussetzungen



Die eigentliche Bedienung erfolgt über einen zusätzlichen Eintrag im Kontextmenü, welches sich im Explorer beim Klick mit der rechten Maustaste auf ein Verzeichnis oder Laufwerk öffnet. Eine Verschlüsselung läuft grundsätzlich so ab, dass der Anwender das zu verschlüsselnde Objekt (Partition, Dateibereich) anwählt und aus dem Kontextmenü die Option aufruft. Daraufhin fragt CryptoStorage nach einem Benutzer sowie Passwort, außerdem lässt sich noch eine Beschreibung angeben. Anschließend verschlüsselt CryptoStorage den Bereich mit AES 128 Bit. Der erste Benutzer, der letztendlich die Verschlüsselung initiiert hat, wird als Eigentümer behandelt. Öffnet er erneut das Kontextmenü, kann er nun weitere Benutzer als Mitbenutzer hinzufügen, wodurch der Multi-User-Zugriff realisiert wird. Wenig komfortabel zeigte sich im Test, dass der Zugriff mehrerer Benutzer für jeden Bereich eigens zu definieren ist. Es gibt dabei keine zentrale Benutzerverwaltung, jede Neueinrichtung ist daher mühevoll und individuell. Weiterhin ist es nicht möglich, die Rechte zu staffeln oder anderweitig individueller festzulegen.

Alle Benutzer haben die gleichen, vollen Zugriffsrechte – sprich, jeder kann lesen und schreiben. Außerdem kann jeder Benutzer das komplette Objekt sicher löschen (Wipe-Funktion). Dabei werden die Daten überschrieben, um eine spätere Wiederherstellung zu verhindern. Nur der Besitzer hat ergänzende Möglichkeiten zur Verwaltung, indem er jederzeit die zusätzlichen Benutzer ändern kann. Außerdem kann er einen verschlüsselten Dateibereich wieder entschlüsseln oder auch neu verschlüsseln. Eine neue Verschlüsselung ist dann angeraten, wenn beispielsweise ein anderer Benutzer aus der Zugriffsliste gelöscht wurde. Hintergrund

ist, dass sich dieser Benutzer während des erlaubten Zugriffs Informationen über den benutzten Schlüssel besorgt haben könnte, die er dann nutzen kann, um sich wieder einen Zugriff zu verschaffen. Durch eine Neuverschlüsselung wird dies vermieden. Bezüglich anderer eingetragener Benutzer ändert sich dadurch nichts, sie bleiben auch eingetragen. Nur ist während der Neuverschlüsselung kein Zugriff möglich.

Für ein häufiges Öffnen und Schließen von geschützten Verzeichnissen ist die Arbeitsweise von CryptoStorage recht unkomfortabel. So erscheint beim Anklicken eines verschlüsselten und noch nicht geöffneten Verzeichnisses eine Standardfehlerausgabe, wie sie Windows bei fehlenden Zugriffsrechten einblendet. Nun ist der Ordner erst über das Kontextmenü mit Benutzer- und Passwortangabe zu öffnen (Object Attach). Besser wäre es, beim Öffnungsversuch käme gleich die Anmeldemaske. Das Schließen eines Ordners (Object Detach) gelingt dagegen mit einem Mausklick.

Bezüglich des Multi-User-Zugriffs ist CryptoStorage tatsächlich mehrbenutzerfähig, denn ein auf einer Freigabe verschlüsseltes Objekt kann problemlos von mehreren Benutzern, die über unterschiedliche Clients zugreifen, gleichzeitig geöffnet werden. Innerhalb des Objekts greifen für die einzelnen Dateien wieder die normalen Sperren beim Zugriff.

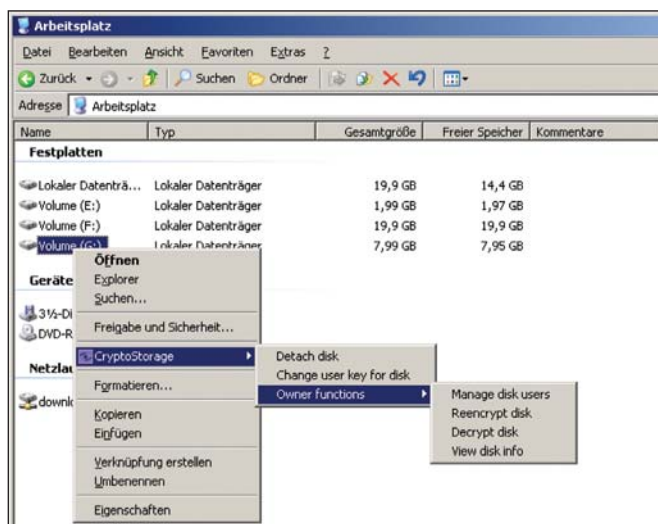


Bild 2: Die gesamte Bedienung von CryptoStorage ist in das Windows-Kontextmenü integriert

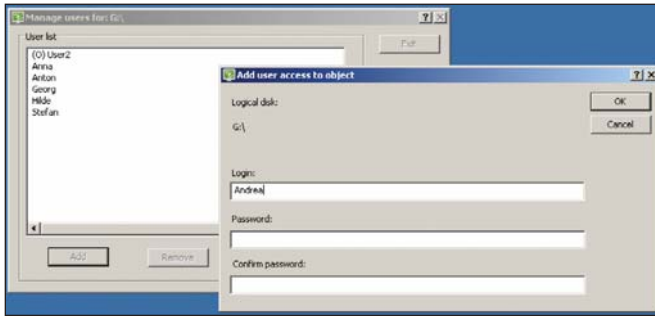


Bild 3: Jedem verschlüsselten Objekt lassen sich neben dem Besitzer weitere Benutzer mit Kennung und Passwort hinzufügen

Diverse Einschränkungen

Vor allem beim Verschlüsseln von ganzen Laufwerken und Wechseldatenträgern gibt es einige Einschränkungen, die unbedingt zu beachten sind. So lassen sich ganze Laufwerke nur verschlüsseln, wenn sie die Standardsektorgröße von 512 Byte besitzen. Nicht unterstützt wird die komplette Verschlüsselung dynamischer Laufwerke. Verschlüsseln lassen sich nur lokale Festplatten, keine Netzlaufwerke. Dass sich auf einem Netzlaufwerk einzelne Verzeichnisbäume verschlüsseln lassen, ist davon unabhängig. Sicher kann direkt auf dem Server auch eine Partition verschlüsselt werden, letztendlich macht das aber wenig Sinn: Ist am Server ein Benutzer angemeldet, der die Partition für den Zugriff öffnet, können alle anderen Benutzer auch über darauf angelegte Freigaben zugreifen, ist die Partition am Server nicht angehängt, kann niemand über eine Freigabe zugreifen und diesen Zustand auch nicht ändern.

Befinden sich auf einem logischen Laufwerk mehrere Partitionen, können diese einzeln ver- und entschlüsselt werden, allerdings lässt sich solch ein Vorgang immer nur für eine Partition zur gleichen Zeit anstoßen. Um ganze Partitionen abzusichern, muss der Nutzer darauf achten, wo er CryptoStorage installiert. Die Partition, auf der CryptoStorage liegt, lässt sich nur dann verschlüsseln, wenn es sich um das Systembeziehungsweise Bootlaufwerk handelt. Der Grund hierfür ist einfach: Im Falle der System-/Bootpartition muss das Aufsperrn bereits vor dem Booten des Betriebssystems erfolgen, so dass dann auch auf die Installation zugegriffen werden kann.

Innerhalb einer verschlüsselten Partition können übrigens unabhängige Verzeichnisse wieder zusätzlich mit eigener Benutzerverwaltung und eigenen Passwörtern verschlüsselt werden, eine Verschachtelung ist hier zulässig. Beim

Start einer Partitionsverschlüsselung darf sich keine Datei im Zugriff befinden, sondern erst, wenn die Verschlüsselung läuft. Eine Verschlüsselung von CDs/DVDs ist nicht möglich, allerdings können CDs und DVDs verwendet werden, um verschlüsselte Container zu speichern. Der Hersteller empfiehlt, CryptoStorage nicht auf Rechnern einzusetzen, auf denen mehrere Betriebssysteme installiert sind.

Bei verschlüsselten Partitionen werden alle für CryptoStorage notwendigen Informationen in einer versteckten Datei auf der ersten Partition des Laufwerks gehalten. Im Normalbetrieb sorgt CryptoStorage dafür, dass diese Datei nicht gelöscht wird. Wird allerdings die ganze Partition neu formatiert, muss der Nutzer erst die anderen Partitionen entschlüsseln, sonst ist anschließend kein Zugriff mehr möglich. Tools zur Veränderung der Partitionsgröße dürfen übrigens bei verschlüsselten Partitionen nicht verwendet werden. Hier ist die Wahrscheinlichkeit eines Datenverlusts groß. In diesem Fall sollte das Laufwerk erst entschlüsselt, dann die Größe verändert und anschließend wieder verschlüsselt werden.

Fazit

CryptoStorage Personal ist am Arbeitsplatz vielseitig einsetzbar, da es die drei üblichen Verschlüsselungsarten für ganze Partitionen, Verzeichnisse und Container in einem Produkt vereint. Aufgrund seiner Multi-User-Fähigkeit ist es auch für die Verschlüsselung gemeinsam genutzter Ordner geeignet, allerdings nur, wenn

nicht zu viele Benutzer berechtigt werden müssen und nur wenige Änderungen stattfinden. Sind viele Benutzer zu administrieren, lohnt sich vielmehr ein Blick auf die Enterprise-Version. Von der Bedienung her ist CryptoStorage recht einfach und übersichtlich gehalten, das Öffnen eines noch geschlossenen Objekts könnte aber etwas komfortabler gestaltet sein. Zu beachten sind diverse Einschränkungen bei der Verschlüsselung ganzer Partitionen. (dr)

IT

Produkt

Programm zur Datenverschlüsselung.

Hersteller

Infowatch
www.infowatch.com

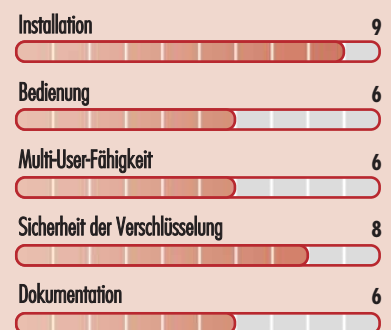
Preis

Infowatch Personal kostet 30 Euro, die Enterprise-Version ist ab 32 Euro erhältlich. Eine Preisstaffelung beginnt bei 250 Lizenzen.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für kleinere Unternehmen bei einer überschaubaren Anzahl an Systemen und Benutzern.

bedingt für größere Unternehmen, wenn viele Benutzer berechtigt werden sollen. Hier empfiehlt sich der Einsatz der Enterprise-Version mit einer zentralen Benutzerverwaltung.

nicht für Fälle, in denen kein Windows als Betriebssystem zum Einsatz kommt.

Infowatch CryptoStorage Personal 1.0



Quelle: Pixello.de

Auch das VirtualCenter will seine Daten ordentlich verwaltet wissen

Microsoft SQL Server für das VirtualCenter von VMware einrichten

Sicherer Hafen für virtuelle Daten

von Bertram Wöhrmann

Für den Administrator ist die unter dem VirtualCenter liegende Datenbank nur ein Mittel zum Zweck. Sie soll ihren Dienst verrichten und erreichbar sein. Damit es aber kein böses Erwachen gibt, muss der IT-Verantwortliche seinen Job gewissenhaft erledigen. In diesem Workshop zeigen wir Ihnen die Punkte auf, die für ein harmonisches Funktionieren beider Systemwelten relevant sind. Zudem erfahren Sie, welche Daten in der Datenbank abgelegt werden.

Jeder Administrator kann dem Problem begegnen, dass das VirtualCenter nicht mehr startet. Nach kurzer Fehlersuche steht schnell fest: Der Datenbankserver hat ein Problem und die Datenbankinstanz fährt nicht mehr hoch. Damit steht auch das VirtualCenter still und die virtuelle Umgebung ist nur noch eingeschränkt verwaltbar. Die Dokumentation von VMware beschreibt zwar sehr detailliert die Installation von Applikation und Datenbank. Auch die Anbindung einer externen Datenbank an das VirtualCenter findet sich darin genau dargelegt. Aber nicht jeder VMware-Administrator kennt sich auch in den Tiefen der verschiedenen Datenbankserver aus.

Grundsätzlich gilt: Wer das VirtualCenter von VMware einsetzt, hat die Wahl, welche Datenbank er verwenden möchte. Unterstützung finden Datenbanken von Oracle sowie Microsoft. Am einfachsten arbeitet es sich mit der mitgelieferten freien Version, dem Microsoft SQL Express Server. Die Express-Version sollten Sie aber

nur in Testumgebungen einsetzen. Der Unterschied zwischen der freien und der kostenpflichtigen Variante ist zum einen die maximal mögliche Datenbankgröße und zum anderen die Möglichkeit, Aufträge für Wartung und Alarmierungen einzurichten. Die einzige Alternative für produktive Umgebungen sollte das Vollprodukt von Oracle oder von Microsoft sein. Eine Rolle bei der Auswahl spielt sicherlich auch die Erfahrung, die bereits im Unternehmen mit der einen oder anderen Datenbank vorliegt.

Auswahl der geeigneten DB-Lizenz

Auf Basis des Microsoft SQL 2005 Server gehen wir nun auf die Schritte ein, mit denen Sie im Fehlerfall das VirtualCenter möglichst schnell wieder in Betrieb nehmen. Vor der Installation sollten Sie zunächst abwägen, ob Sie nur eine zusätzliche Datenbank auf einem vorhandenen Server oder eine eigene Instanz für das Management der virtuellen Umgebung anlegen. Grundsätzlich ist zu empfehlen, eine eigene Datenbankinstanz zu nutzen und die Datenbank nicht auf einen bereits vor-

handenen Server mitanzulegen. Anders sieht es aus, wenn Sie auf einem vorhandenen Datenbankserver eine neue Instanz für das Management der virtuellen Umgebung anlegen.

Legen Sie einen Datenbankserver nur für das VirtualCenter an, reicht der Microsoft SQL Server in der Standardversion vollkommen aus. Soll dagegen eine eigene Instanz auf einem bereits vorhandenen oder auch neuen Datenbankserver installiert werden, kann es notwendig sein, die Enterprise-Lizenz des SQL-Servers zu nutzen. Dies ist der Fall, wenn Sie mehr als 16 Instanzen auf einem Server installieren möchten. Der große Vorteil eines eigenen Servers oder einer Instanz liegt übrigens darin, dass Sie in beiden Fällen auf demselben Server mehrere von einander unabhängige Datenbank-Patchlevel betreiben können. Sie müssen sich in diesem Fall beim Patchen nicht darum kümmern, ob die unterschiedlichen Datenbanken alle mit dem neuen Patchlevel kompatibel sind oder nicht. Jede Umgebung ist somit unabhängig und kann isoliert betrachtet werden.

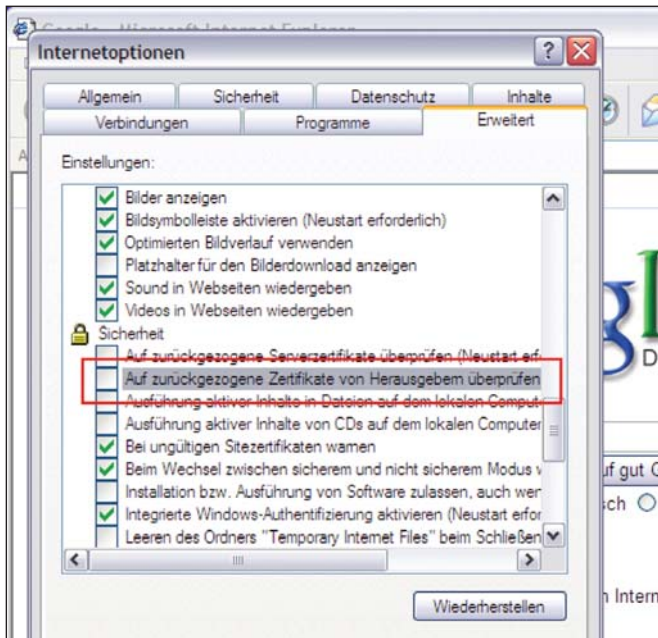


Bild 1: Die Zertifikatsprüfung in den Internet Explorer-Einstellungen muss deaktiviert sein

Installation der SQL-Datenbank

Für den Start der SQL-Server-Dienste benötigen Sie zunächst einen User mit den passenden Rechten im Active Directory (AD). Damit Informationen, die der SQL-Server verschicken möchte, beim richtigen Personenkreis ankommen, ist zudem ein gültiges E-Mailkonto oder eine Verteilerliste nötig. Der sa-User ist der Hauptadministrator einer Datenbankinstanz. Das Passwort sollte nach den geltenden Firmenrichtlinien vergeben werden. Nach der erfolgreichen Installation des Datenbankservers oder der Datenbankinstanz folgt das aktuelle von VMware freigegebene Servicepack für den SQL-Server. Auch die Onlinehilfe sollten Sie auf den aktuellen Stand bringen.

Bevor es nun an die Konfiguration des SQL-Servers geht, ist unter Umständen eine Konfigurationsanpassung im Internet Explorer vorzunehmen. Die Anpassung ist notwendig, wenn das ManagementStudio beim Start sehr lange Zeit benötigt. Es gibt eine Möglichkeit den Aufruf zu beschleunigen: Deaktivieren Sie im Internet Explorer die Option "Auf zurückgezogene Zertifikate von Herausgebern überprüfen" (siehe Bild 1).

Die Verzögerung beim Start des ManagementStudio hat ihre Ursache darin, dass alle .NET-Zertifikate auf Gültigkeit überprüft werden. Hat der Computer, auf dem die Managementoberfläche gestartet wird, keinen Zugang zum Internet, muss jedes Zertifikat auf den Standardtimeout von 15 Sekunden warten, bis das nächste Zertifikat geprüft wird. Je mehr Zertifikate im System vorhanden sind, desto länger dauert der Aufruf. Die Deaktivierung der genannten Option unterbindet diese Abfrage.

Haben Sie alle Grundinstallationsarbeiten durchgeführt, folgt das Anlegen der Datenbanken für das VirtualCenter und den Updatemanager. Mit der rechten Maustaste wählen Sie hierfür das Kontextmenü bei "Databases" aus und die beiden benötigten Datenbanken werden angelegt. Die wichtigsten Parameter sind dabei die Initialgröße und die maximale Größe beziehungsweise die Art des Wachstums der Datenbanken. Der Speicherort der Datenbanken und der Log-Dateien lässt sich ebenfalls anpassen. Somit besteht die Möglichkeit, Datenbank und Logs voneinander zu trennen. Allgemein ist zu empfehlen, die Datenbanken nicht automatisch mitwachsen zu lassen. Im Dialog "Eigenschaften" passen Sie für

diesen Fall die Parameter entsprechend an. Die Datenbankinstanzen für VMware stellen sich in der Managementkonsole des SQL Servers dar, wie in Bild 2 zu sehen.

Aufgrund von Änderungen vom SQL Server 2000 zur Version 2005 fallen nun einige zusätzliche Konfigurationsarbeiten an. Das Ziel ist es, den Administrator in seiner Arbeit zu unterstützen und von rudimentären Überwachungsaufgaben zu entlasten. Das Hauptaugenmerk liegt hierbei auf einem hohen Automatisierungsgrad. Zuerst einmal sollten Sie den SQL-Server so konfigurieren, dass die Serverdienste beim unerwarteten Beenden automatisch neu gestartet werden. Bild 3 zeigt das entsprechende Kontextmenü des SQL-Agenten.

Achten Sie darauf, dass die beiden Punkte, die mit "Auto restart ..." beginnen, aktiviert sind. Wichtig ist an der Stelle, dass diese Einstellung für jede Datenbank-Instanz gesondert durchgeführt werden muss. Als Nächstes schaffen Sie die Basis dafür, dass E-Mailbenachrichtigungen vom Server verschickt werden können. Für eine automatische Benachrichtigung per E-Mail und damit einhergehend einer kurzen Reaktionszeit im Fehlerfall richten Sie un-

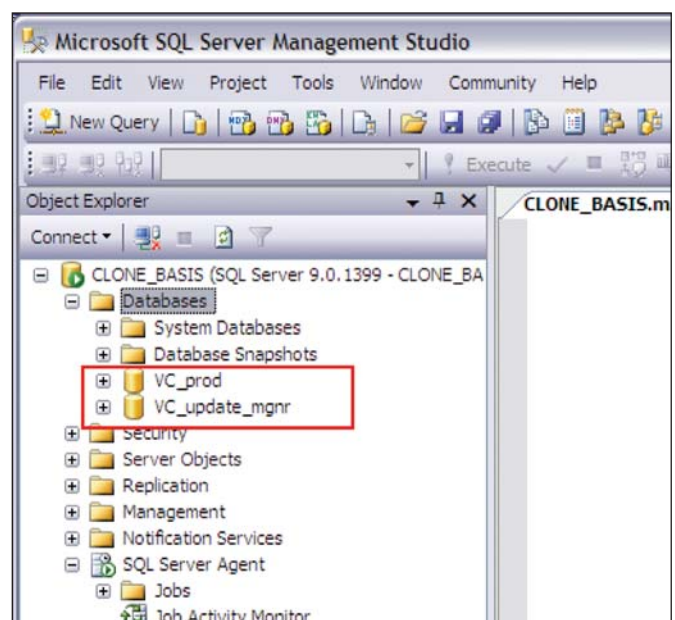


Bild 2: Die Datenbanken für das VirtualCenter und den Updatemanager

ter dem Punkt “{DB Instanz}/Management/Database Mail” eine E-Mail-adresse oder eine Verteilerliste ein. Achten Sie jedoch darauf, dass stets mehr als nur eine Person, am besten ein definierter Personenkreis die entsprechenden Nachrichten erhält. Es wäre fatal, wenn der Mitarbeiter, der gerade im Urlaub verweilt, als einziger die Fehlermeldung erhält.

Für alle, die sich nicht so im MS SQL-Umfeld auskennen, sei gesagt, dass es grundsätzlich zwei Möglichkeiten gibt, um Aktionen am SQL-Server und an den Datenbanken durchzuführen. Zum Einen kann die Maus das Mittel der Wahl sein – mit verschiedenen Wizards lassen sich Aktionen konfigurieren und ausführen. Alternativ steht die direkte Eingabeoberfläche für die SQL-Syntax in der Managementoberfläche zur Verfügung. In diesem Fall wird die gewünschte Aktion mit SQL-Befehlen durchgeführt. Der Aufruf der Eingabeoberfläche geschieht über “New Query”. Auf der rechten Seite des Managementfensters öffnet sich ein Bereich, in dem Sie die Syntax eingeben und ausführen können.

Die Übersichtlichkeit im Texteditor des SQL Servers lässt sich verbessern, indem Sie im ManagementStudio, unter “Tools / Options / Texteditor / All Languages / Line Numbers”, die Zeilennummern aktivieren. Die Ziffer “1” im Syntax-Fenster zeigt dabei die Aktivierung der Zeilennummernfunktion an. Nach der Ausführung der oben beschriebenen Aktionen sind noch weitere Anpassungen notwendig.

SQL-Scripting für die Automatisierung

Um die Überwachung der VMware-Datenbanken zu automatisieren, legen Sie am besten einen Operator an. Dabei hilft das folgende Skript weiter:

```

--- Operator anlegen
--- Beginn ---
USE [msdb]
GO
EXEC msdb.dbo.sp_add_operator

```

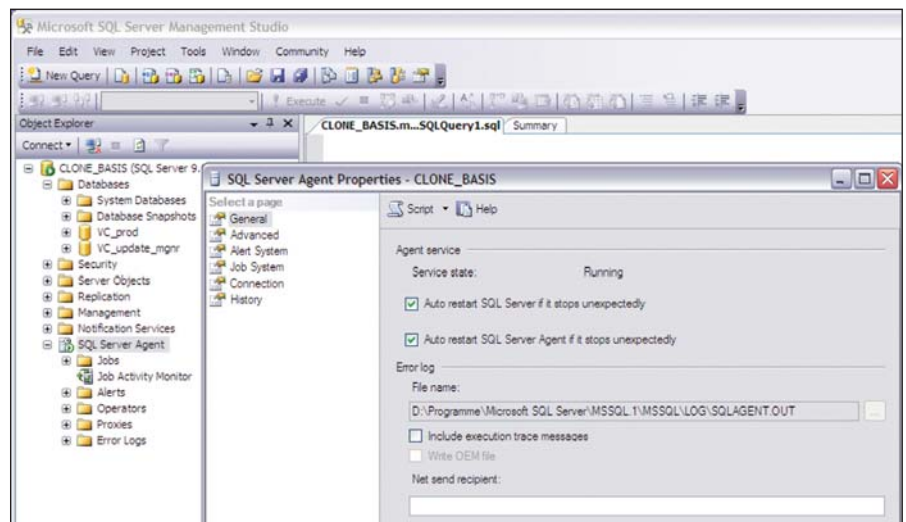


Bild 3: Die SQL-Server-Agenten mit aktivierter Auto Restart-Funktion

```

@name=N'Admin, SQL',
@enabled=1,
@pager_days=0,

@email_address=N'sql.admin@mail-
host.de',
@pager_address=N'',
@netsend_address=N''

```

GO

--- Ende ---

Der Operator ist das Bindeglied zwischen dem SQL-Server-Agenten und dem Administrator. Der Name des Operators muss innerhalb einer SQL-Instanz eindeutig sein und darf maximal 128 Zeichen lang sein. Benötigen Sie mehrere Operatoren, können Sie den Code mehrfach nutzen, dabei den Operatornamen austauschen und das Skript erneut starten. Häufig genutzte Codesegmente lassen sich auch als Datei abspeichern und später wieder nutzen. Wie in unserem Skript zu erkennen ist, werden User in der msdb-Datenbank abgespeichert. Des Weiteren sind alle Einstellungen in

der msdb zu finden, die mit dem SQL-Server-Agent zusammenhängen, wie etwa auch die Warnungen. Die Warnungen für die kritischen Schweregradfehler 19 bis 25 wurden in der Vorgängerversion des SQL Server 2005 automatisch eingerichtet. In der neueren Version ist der Administrator dafür zuständig, die Warnungen selbst anzulegen. Aus diesem Grund sollten sie überwacht werden. In unserem Beispiel fangen wir den Schweregrad 19 ab. Bei der Anlage der weiteren Fehler gilt es lediglich, den Fehlertext und die Schwere mit der entsprechenden Fehlernummer anzupassen.

```

--- Schwere Fehler als
Warnungen anlegen
--- Beginn ---
USE [msdb]

```

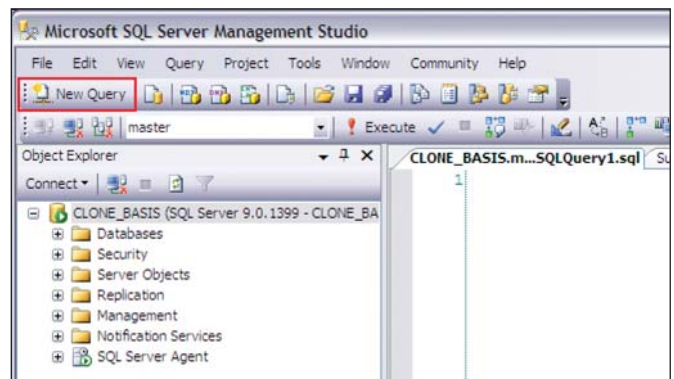


Bild 4: Aufruf des SQL Query-Fensters zur Eingabe der gewünschten Syntax über den Punkt “New Query”



```
GO
EXEC msdb.dbo.sp_add_alert
    @name=N'Schwerer Fehler 019',
    @message_id=0,
    @severity=19,
    @enabled=1,
    @delay_between_responses=0,

    @include_event_description_in=0
GO

--- Ende ---
```

```
--- Transaktionslog msdb DB voll
--- Beginn ---

USE [msdb]
GO
EXEC msdb.dbo.sp_add_alert
    @name=N'Transaktionslog msdb DB
voll',
    @message_id=9002,
    @severity=0,
    @enabled=1,
    @delay_between_responses=0,
```

Eine der möglichen kritischen Situationen bei Datenbankservern ist der Füllgrad der Log-Dateien. Die Überwachung der Log-Dateien ist aus diesem Grund extrem wichtig. Zur Kontrolle der tempdb- beziehungsweise der msdb-Datenbank bietet sich hierfür das folgende Skript an. Der Fehlercode für ein volles Transaktionslog lautet übrigens "9002". Für die Überwachung weiterer Log-Dateien passen Sie das Skript einfach entsprechend an:

```
@include_event_description_in=0,
@database_name=N'msdb'
GO

--- Transaktionslog master DB voll

USE [msdb]
GO
EXEC msdb.dbo.sp_add_alert
    @name=N'Transaktionslog tempdb DB
voll',
    @message_id=9002,
```

```
@severity=0,
@enabled=1,
@delay_between_responses=0,

@include_event_description_in=0,
@database_name=N'tempdb'
GO
--- Ende ---
```

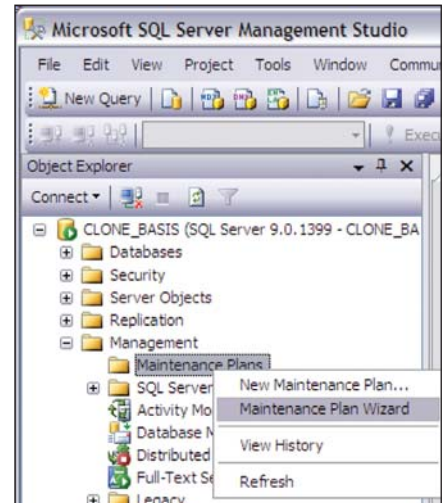


Bild 5: Der Maintenance Plan Wizard – zu erreichen per Rechtsklick auf "Maintenance Plans"



Der Weg zu einer sicheren IT

Erleben Sie mit der it-sa in Nürnberg vom 13.-15. Oktober 2009 eine Messe, die sich exklusiv auf das Thema IT-Sicherheit konzentriert!

it-sa 2009: Mehr Themen - mehr Service

- Lösungen zu Informations-Sicherheit, Storage- und Netzwerksicherheit, Datenschutz, Hardware-Sicherung, Security-Awareness
- Non-Stop-Vortragsprogramm auf 2 großen Foren mit Kurzreferaten, Podiumsdiskussionen und Live-Demos
- Guided Tours von unabhängigen Consultants
- Topic-Routen zu Trendthemen, Basis-Lösungen
- Seminare, Security-Tagungen, Workshops



→ Jetzt informieren: www.it-sa.de

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

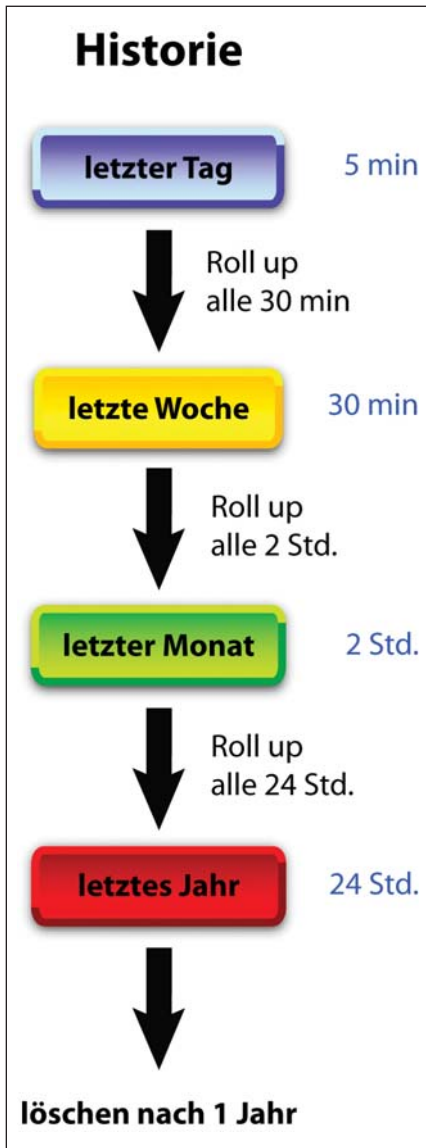


Bild 6: Historie der Performance-Daten mit Aktualisierungsintervallen von fünf Minuten bis 24 Stunden

Die so erstellten Operatoren und Warnmeldungen lassen sich nun über das Kommando `Update_Alert` miteinander verknüpfen. Für jeden Operator und jeden Fehler müssen Sie dazu eine Verbindung einrichten (siehe Listing).

Sicherungsjobs als Rettungsring

Für den Fall, dass ein sehr schwerwiegender Fehler auftritt, sollten Sie Vorsorge treffen. Dazu lassen sich in der Management-Konsole passende Sicherungsjobs einrichten. Wichtig ist an der Stelle, dass nicht nur die Applikationsdatenbanken gesichert werden, sondern

auch die Datenbanken master und msdb. Beide sind für die Funktion des Datenbankservers und der Applikationen sehr wichtig. Auf die msdb sind wir bereits eingegangen. In der master-Datenbank stehen alle für die zugehörigen Instanzen relevanten Daten. Ist diese zerstört und liegt keine aktuelle Sicherung vor, wird die ungeplante Ausfallzeit mit Sicherheit länger dauern. Für die Sicherung von Datenbanken können Sie einen Job über einen Wizard aufsetzen. Der Aufruf erfolgt über das entsprechende Kontextmenü.

Die Sicherung der Daten kann auch auf der Festplatte des Servers erfolgen. In einem solchen Fall werden die Backupfiles dann dateibasiert gesichert. Sichern Sie die Daten nie auf der selben Festplatte, auf der auch die Datenbanken liegen. Die Originaldaten und deren Sicherungen sollten Sie immer voneinander getrennt aufbewahren.

Die Daten des VirtualCenter

Die Daten in der VirtualCenter-Datenbank gliedern sich in drei Teile: Zum Einen wird das Inventar in der Datenbank abgelegt. Alle Konfigurationsparameter der ESX-Hosts finden sich dabei in der Datenbank. Ebenso sind die Parameter für das High Availability (HA) und den Distributed Resource Scheduler (DRS) zentral gespeichert. Die Konfigurationsdaten der Ressourcenpools befinden sich auch dort, ebenso wie alle Angaben der virtuellen Maschinen. Schließlich gehört das Thema Rechteverwaltung ebenfalls dazu. Alle Benutzerrollen sind Teil des Inhalts, ebenso wie die Benutzerrechte und deren Verknüpfung untereinander.

Der zweite Block in der Datenbank betrifft das Thema Ereignisse und Alarme. Diese gehören zum Inhalt der Instanz genauso wie die dazugehörigen Schwellwerte. Im letzten und dritten Teil wird der weitaus größte Block an Daten gespeichert. Es handelt sich um die Performance Daten, sie nehmen bis zu 90 Prozent des Platzes in Anspruch.

Informationsübersicht

Die Performance Informationen gliedern sich in vier Zeitabschnitte: letzter Tag, letzte Woche, letzter Monat und letztes

```

--- Warnungen mit Operatoren verknüpfen
--- Beginn ---

USE [msdb]
GO
EXEC msdb.dbo.sp_update_alert @name='Schwerer Fehler 019',
    @message_id=0,
    @severity=19,
    @enabled=1,
    @delay_between_responses=0,
    @include_event_description_in=0
GO
EXEC msdb.dbo.sp_add_notification
    @alert_name='Schwerer Fehler 019',
    @operator_name='SQL Admin',
    @notification_method = 1
GO

.
.
.

--- Bis Schweregrad 25 ergänzen

--- Transaktionslog msdb DB Vo11

USE [msdb]
GO
EXEC msdb.dbo.sp_update_alert @name='Transaktionslog msdb DB Vo11',
    @message_id=9002,
    @severity=0,
    @enabled=1,
    @delay_between_responses=0,
    @include_event_description_in=0,
    @database_name='msdb'
GO
EXEC msdb.dbo.sp_add_notification
    @alert_name= 'Transaktionslog msdb DB Vo11',
    @operator_name='SQL Admin',
    @notification_method = 1
GO

--- Transaktionslog Tempdb DB Vo11

USE [msdb]
GO
EXEC msdb.dbo.sp_update_alert @name='Transaktionslog tempdb DB Vo11',
    @message_id=9002,
    @severity=0,
    @enabled=1,
    @delay_between_responses=0,
    @include_event_description_in=0,
    @database_name='master'
GO
EXEC msdb.dbo.sp_add_notification @alert_name='N'Transaktionslog tempdb DB Vo11',
    @operator_name='SQL Admin',
    @notification_method = 1
GO

--- Ende ---
  
```

Listing: Verbindungen für Operatoren und Fehler





Jahr. Alle fünf Minuten werden vom VirtualCenter die Performance Daten in die Datenbank eingefügt. Damit dieser Datensatz nicht ausufert, findet eine regelmäßige Konsolidierung der Daten statt. In Bild 6 sehen Sie den Ablauf der Konsolidierung der Informationen. Regelmäßig startende Jobs fassen die Daten zusammen. Am aktuellen Tag schreibt das System die Daten alle fünf Minuten in die Datenbank. Die Informationen der letzten Woche werden im 30-Minuten-Rhythmus zusammengefasst. Der letzte Monat wird auf ein Zwei-Stunden-Intervall reduziert. Alle 24 Stunden findet die Konsolidierung der Daten der letzten elf Monate statt. Die maximale Aufbewahrungsdauer von Performance Daten beträgt zwölf Monate. Nach Ablauf des Zeitraumes von einem Jahr werden die Daten gelöscht.

Die Statistikläufe können Sie aber auch auf die eigenen Bedürfnisse anpassen. Sollten die Performance Daten in ande-

ren Zeitintervallen gesammelt werden, so haben Sie im VirtualCenter die Möglichkeit, die Zeitspannen anzupassen. Im Menüpunkt "Administration / VirtualCenter Management Server / Configuration / Statistics" konfigurieren Sie die Intervalle. Weitere Hinweise zu dem Thema finden sich im Basis Administrationshandbuch für den VirtualCenter Server [1] ab Seite 281. Aufgrund der Tatsache, dass Reorganisationsläufe auch parallel starten können, ist es wichtig, den Datenbankserver mit viel Arbeitsspeicher auszustatten. Reicht die Leistungsfähigkeit der Festplatte nicht aus, so besteht die Möglichkeit, die Datenbank-Dateien und die Log-Dateien voneinander zu trennen.

Fazit

Bei einer sorgfältigen Konfiguration der Datenbank und dank der Automatisierung sollten keine Probleme im VirtualCenter-Betrieb zu erwarten sein. Bei der Größenbestimmung des Datenbankservers bietet

die Empfehlung, die VMware im Kalkulations-Sheet [2] vorgibt, eine passende Grundlage. Bei der Auswahl des Betriebssystems und der Version des Datenbankservers sollte auf jeden Fall berücksichtigt werden, wie viel Arbeitsspeicher adressiert werden muss. Informationen für die Arbeitsspeicher- und CPU-Ausstattung des Datenbankservers sind im VirtualCenter Database Performance Guide [3] zu finden. (dr)



- [1] Basic System Administration
www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_admin_guide.pdf
- [2] VirtualCenter Database Sizing Calculator
www.vmware.com/support/vi3/doc/vc_db_calculator.xls
- [3] VirtualCenter Database Performance for Microsoft SQL 2005
www.vmware.com/files/pdf/vc_database_performance.pdf

Links



Am 27. und 28.08.2009 veranstaltet der Just Community e.V. zum 5. mal das größte Developer und IT-Pro Community Event.

Unter dem Motto „Check-In zum Wissensvorsprung“ stehen zahlreiche nationale und internationale Speaker bereit und werden Sie mit auf die Reise durch die neuesten Technologien und Informationen aus der IT nehmen.

Neben den Vorträgen haben Sie natürlich auch dieses Jahr wieder viel Zeit für das Networking mit anderen ITlern aus Nah und Fern.

Anmeldung und Informationen unter:

[HTTP://WWW.NRWCONF.DE/](http://www.nrwconf.de/)

Sponsored by:

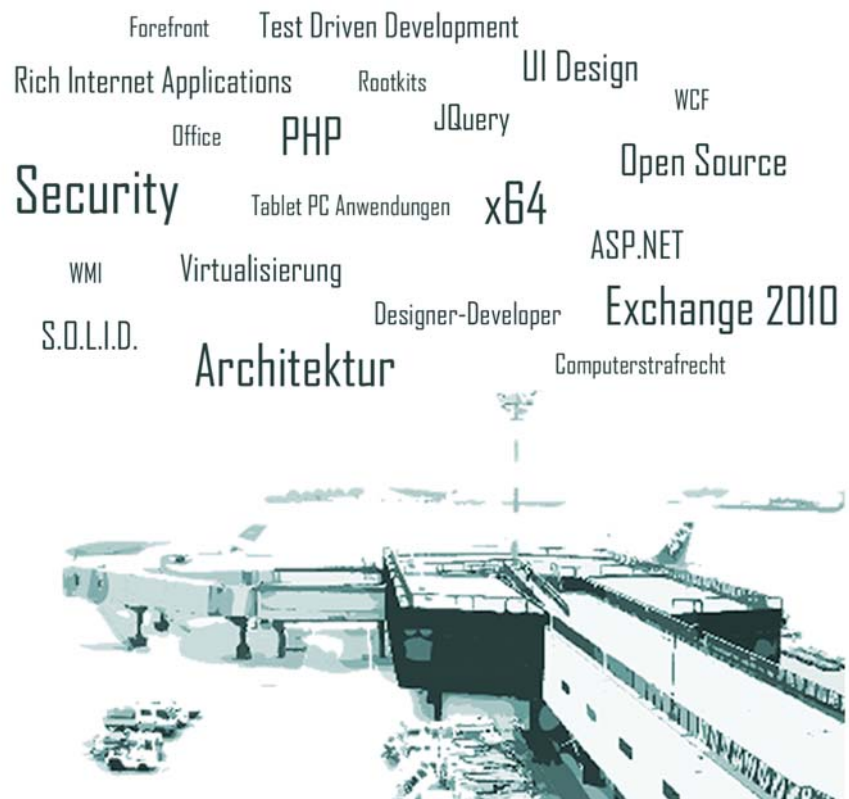


invent

devcoach®
SOFTWARE // DEVELOPMENT • ARCHITECTURE • CONSULTING

Microsoft

BROCKHAUS AG
SOFTWARE & CONSULTING





Microsoft Essential Business Server, Small Business Server und Home Server im Vergleich *Ein ungleiches Trio*

von Thomas Joos

Die Anforderungen an die IT sind in mittelständischen und kleinen Unternehmen mittlerweile nahezu identisch. Remotefähigkeiten, Verfügbarkeit und Stabilität sind nur einige Beispiele für solche Anforderungen. Microsoft bietet mit dem neuen Windows Essential Business Server 2008 und dem Small Business Server zwei Lösungen für mittelständische Unternehmen an. Doch auch der Home Server kann eine Alternative sein.

Mit dem Windows Essential Business Server (EBS) 2008 bietet Microsoft eine integrierte Multiserverlösung an, die über den Windows Small Business Server (SBS) 2008 hinausgeht. Sie richtet sich an Unternehmen mit bis zu 300 Rechnern, denen die kleinere Serverlösung von Microsoft nicht mehr genügt. Ein großer Vorteil beim EBS – vor allem im Vergleich zur Planung, Installation und der Verwaltung von Einzellösungen – ist die automatische und angepasste Konfiguration. Auch die nahtlose Migration von SBS zum Essential Business Server sowie die günstigere Lizenzierung sind Vorteile des EBS. Wie Small Business Server 2008, erscheint auch der Windows Essential Business Server 2008 in den beiden Versionen “Standard” und “Premium”.

Essential Business Server 2008

Im Gegensatz zu SBS dürfen Sie die verschiedenen Serverlösungen von Windows Essential Business Server 2008 auf bis zu vier unterschiedliche Server verteilen. Außerdem steht EBS ausschließlich in einer 64-Bit-Version zur Verfügung, einschließlich aller integrierten Produkte. Dadurch erhöhen sich im Vergleich zur 32-Bit-Software die Stabilität und die Geschwindigkeit. Da alle enthaltenen Funktionen auf 64-Bit ausgelegt sind und mit Windows Server 2008 x64 auch das entsprechende Betriebssystem zur Verfügung steht, erhalten Sie eine skalierbare Infrastruktur. Die

Standard-Edition enthält Lizenzen für bis zu drei Server. EBS unterscheidet dabei zwischen Verwaltungsserver, Messagingserver und Sicherheitsserver.

Verwaltungsserver SCE

Auf dem Verwaltungsserver integrieren Sie Windows Server 2008 Standard Edition mit Microsoft System Center Essential (SCE) 2007. Zusätzlich dient dieser Server als Domänencontroller für das Active Directory. SCE basiert auf der Serverüberwachungslösung “System Center Operations Manager” 2007 (SCOM) und unterstützt die Überwachung von maximal 30 Servern. Das Produkt behält die Server im Netzwerk mit speziellen Agenten im Auge und unterstützt die Systemadministratoren beim Finden von Fehlern sowie deren Behebung. Sie erhalten auf einer grafischen Oberfläche den Status aller Server angezeigt und können sofort die Probleme lösen, wenn bestimmte Fehler auftauchen. Ohne eine automatisierte Überwachung fallen viele Fehler erst dann auf, wenn zum Beispiel die Verbindung zum Server fehlschlägt. Die konsequente Überwachung ist einer der Bausteine, welche die Stabilität und Ausfallsicherheit eines Netzwerks gewährleisten und die Arbeitsfähigkeit der Anwender sicherstellen. Neben der reinen Verfügbarkeit der Server überwacht SCE auch Serverfunktionen bis ins Detail.

Messagingserver

Beim zweiten Server handelt es sich um den Messagingserver. Auch auf diesem installieren Sie Windows Server 2008 in der Standard Edition. Hauptbestandteil des Servers ist Exchange Server 2007 Standard Edition sowie Forefront Security for Exchange Server. Im Preis enthalten sind Updates für den Virenschutz für ein Jahr – Sie erhalten also einen vollwertigen Mailserver mit integriertem Virenschutz. Exchange Server 2007 bietet eine Unified Messaging Plattform, die E-Mail, Fax und Voicemail in einem Postfach integriert. Dabei will Microsoft die Grenzen zwischen den verschiedenen Kommunikationskanälen abbauen. Jedes Exchange-Postfach fungiert jetzt quasi auch als ein Anrufbeantworter, jeder Anwender hat eine eigene Durchwahl.

Eine weitere Funktion in Exchange Server 2007 ist die Möglichkeit, Telefonmenüs für Kunden und Lieferanten aufzubauen, die wie ein Callcenter funktionieren. Ruft ein Kunde bei einer Durchwahl an, bietet ihm der Server ein Telefonmenü an, das über die Weiterleitung von Anrufen, der Möglichkeit Sprachnachrichten zu hinterlassen bis hin zu geschäftszeitabhängigen Ansagen alle Möglichkeiten einer echten Telefonzentrale bietet. Neben der Möglichkeit, E-Mails per Telefon abzurufen (Outlook Voice Access), können Nutzer mit Smartphones oder anderen kom-



patiblen Geräten ihre E-Mails weltweit über das Internet synchronisieren, bearbeiten und beantworten.

Exchange 2007 Standard Edition unterstützt maximal fünf Speichergruppen mit fünf Postfachspeichern. Eine Beschränkung der Datenbankgröße gibt es auch in der Standard-Edition nicht mehr. Forefront Security for Exchange hat seinen Ursprung im Produkt "Antigen" von Sybari, die Microsoft nach einer längeren Kooperation im Juni 2005 übernommen hat. Forefront Security hat die Aufgabe, E-Mails bei der Zustellung nach Viren oder Spams zu prüfen. Die Lösung setzt auf die von Microsoft lizenzierten Engines der Unternehmen AhnLab, Authentium, CA (VET und Innoculate), Kaspersky Labs, Norman Data Defense, Sophos und VirusBuster. Eingehende E-Mails können von bis zu fünf Engines gleichzeitig gescannt werden. Forefront Security überprüft standardmäßig nicht immer eine E-Mail mit allen verfügbaren Engines, sondern basiert auf einem intelligenten Mechanismus, dem "Multiple Engine Manager" (MEM), um den Server nicht zu stark zu belasten. Dieser steuert, mit wie vielen und welchen Engines eine E-Mail gescannt werden soll.

Sicherheitsserver

Bei der dritten Variante handelt es sich um den Sicherheitsserver, der auch die Verbindung zum Internet darstellt. Auf diesem Server stehen Exchange 2007 Standard Edition und das Forefront Threat Management Gateway Medium Business Edition zur Verfügung. Hierbei handelt es sich um den Nachfolger des Internet Security & Acceleration-Server 2006 (ISA). Neben einer Firewall und einem Proxy-Server enthält der Sicherheitsserver Filter und Funktionen, um das Netzwerk sicher mit dem Internet zu verbinden. So lassen sich von unterwegs Daten abrufen oder E-Mails abfragen und zwar fast vollkommen unabhängig vom Endgerät. Beim Betriebssystem handelt es sich ebenfalls um Windows Server 2008 Standard Edition.

Premium-Edition mit SQL-Datenbank

Trotz dieses mehrstufigen Konzepts ist die Verwaltung nicht sehr kompliziert, da die Einrichtung, ähnlich wie beim Small Business Server, automatisiert und auf die Produkte hin optimiert erfolgt. Die Premium Edition des Windows Essential Business Server 2008 enthält noch einen Datenbankserver mit SQL Server 2008 Standard Edition, den Sie ebenfalls auf getrennter Hardware installieren dürfen. Auch hier dient als Betriebssystem wieder Windows Server 2008 in der Standard Edition. Die Vorteile von Windows Essential Business Server 2008 liegen auf der Hand: Zum Einen erhalten Unternehmen eine integrierte Serverlösung, bei der die Produkte aufeinander abgestimmt sind. Die Verwaltung ist im Vergleich zu den Einzelprodukten erheblich erleichtert. Auch die Lizenzierung ist wesentlich einfacher und kostengünstiger. Da die Produkte auf bis zu vier Servern verteilt sind, laufen Unternehmen nicht Gefahr, dass ein einzelner Server überlastet sein könnte.

Im Vergleich zum Small Business Server, der die Installation aller Produkte nur auf einem einzelnen Server vorsieht, erhalten mittelständische Unternehmen mit dem EBS ein hervorragendes Mittel an die Hand, um ihre Serverstruktur zu konsolidieren, zu vereinheitlichen und die Verwaltung zu verbessern. Vor allem Unternehmen, die bereits auf Small Business Server setzen, aber über das Produkt hinausgewachsen sind, erhalten mit dem EBS die beste Lösung, Ihre IT-Infrastruktur zu erweitern. Durch die Vorkonfiguration der Komponenten hält sich auch der Aufwand für die Integration der Produkte in Grenzen. Da Windows Essential Business Server komplett auf x64-Software ausgelegt ist, kann der Betrieb auch nur auf Servern erfolgen, die mit x64-Prozessoren ausgestattet sind. Der Verwaltungsserver und der Messagingserver müssen über mindestens 4 GByte, der Sicherheitsserver über mindestens 2 GByte Arbeitsspeicher verfügen. Darüber hinaus sollten alle Ser-

ver über ausreichend Festplattenplatz verfügen und idealerweise über RAID-Datenträger abgesichert sein.

Windows Small Business Server 2008

Die neue Version des Small Business Server enthält zusammengefasst alle aktuellen und überarbeiteten Produkte, die für Unternehmen zum Aufbau einer Infrastruktur maßgeblich sind. Dennoch enthält SBS 2008 nach wie vor viele Einschränkungen, zum Beispiel die auf einen Server begrenzte Installation. Die wichtigste Einschränkung für den Small Business Server 2008 sind die maximal 75 Arbeitsplätze, die sich an den Server anbinden lassen.

Neu ist, dass nun die kleine Server-Edition von Microsoft als 64-Bit-Version zur Verfügung steht. Microsoft stellt den SBS in den Versionen Standard und Premium zur Verfügung. Windows Small Business Server 2008 Standard muss auf einem einzelnen Server installiert werden. Basis des Produkts sind Windows Server 2008 Standard Edition, Exchange Server 2007 Standard Edition, Windows SharePoint Services 3.0 und Windows Server Update Services 3.0. Außerdem liefert der Hersteller mit dem Server noch 120-Tage-Testversionen von Windows Live OneCare für Server sowie Forefront Security für Exchange Server. Unternehmen, die auf die Premium Edition setzen, erhalten darüber hinaus noch den Datenbank-Server Microsoft Small Business Server 2008 Standard Edition für Small Business sowie eine weitere Lizenz für Windows Server 2008 dazu. Der Datenbank-Server darf und soll auf einer zweiten Servermaschine installiert werden. Die Lizenzierung erfolgt sehr einfach: Für jeden verbundenen Benutzer oder PC müssen Sie eine CAL erwerben, die dann für alle enthaltenen Produkte gültig ist.

Lizenzierung für Nutzer und Geräte

Microsoft bietet Standard-CALs sowie Premium-CALs an, die zusätzlich eine Anbindung an den zweiten Server und SQL Server 2008 erlauben. Als Voraussetzung für den

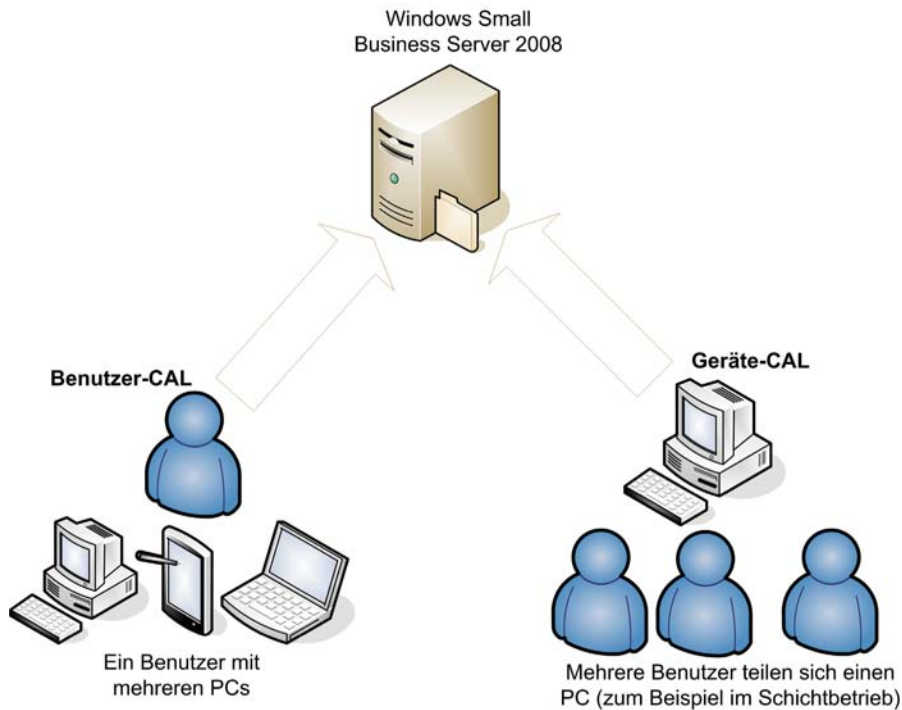


Bild 1: Die Lizenzierung des SBS kann über Benutzer- oder Geräte-CALs erfolgen

Small Business Server muss die Hardware mindestens 4 GByte RAM bieten, bis maximal 32 GByte sind möglich. Im Lieferumfang der Lösung sind bereits fünf Benutzerlizenzen enthalten, der Rest lässt sich leicht nachinstallieren. Microsoft bietet die beiden Lizenzvarianten Geräte-Lizenzen und Benutzer-Lizenzen an. Die beiden Lizenzen unterscheiden sich nicht preislich voneinander. Sie müssen bereits bei der Bestellung Ihrer Lizenzen im Voraus planen, welchen Lizenztyp Sie einsetzen wollen. Sie können auf einem Small Business Server auch die verschiedenen Lizenzen miteinander mischen, je nach optimaler Lizenzierung. Es ist jedoch nicht erlaubt, die einzelnen erhältlichen Lizenzpacks in Geräte- und Benutzer-Lizenzen aufzusplitten. Sie dürfen also ein Fünfer-Pack Geräte-Lizenzen und ein Fünfer-Pack Benutzerlizenzen kaufen und lizenzieren. Es ist aber nicht erlaubt, dass Sie diese Pakete aufsplitten und zum Beispiel als Zweier-Geräte-Lizenz und Achter-Benutzerlizenz verwenden.

Lizenzieren Sie mit Geräte-CALs, müssen Sie für jeden PC, der auf diesen Server zugreift, eine Lizenz kaufen, unabhängig davon, wie viele Benutzer an diesem PC ar-

beiten. Betreiben Sie PCs zum Beispiel im Schichtbetrieb, an denen zu unterschiedlichen Zeiten unterschiedliche Benutzer arbeiten, benötigen Sie für diese PCs nur jeweils eine Geräte-CAL. Im umgekehrten Fall, wenn also ein Benutzer mit mehreren PCs, Notebooks oder Smartphones auf den Server zugreift, benötigen Sie für diesen Benutzer mehrere Geräte-CALs, da dieser Benutzer mit mehreren PCs auf den Server zugreift. Auch PCs, auf denen Sie per Outlook Web Access oder Remote Web Workplace auf den Small Business Server 2008 zugreifen, müssen lizenziert werden. Alternativ können Sie auch eine Benutzer-CAL kaufen. Jeder Benutzer mit einer Benutzer-CAL kann an beliebig vielen PCs eine Verbindung mit einem Server aufbauen.

Grundsätzlich gilt also, Sie müssen die Gesamtzahl Ihrer Arbeitsstationen, Pocket-PCs und sonstiger Geräte lizenzieren, wenn Sie Geräte-Lizenzen kaufen. Bei Benutzer-Lizenzen müssen Sie diese genau der Anzahl der Benutzer zuweisen, die insgesamt mit dem Small Business Server 2003 R2 arbeiten. Gehen wir in einem Beispiel von einer IT-Firma aus, in der 40 Mitarbeiter be-

schäftigt sind. Von diesen 40 Mitarbeitern arbeiten 25 mit der Windows-Domäne. Jeder dieser Mitarbeiter hat einen PC und ein Notebook, mit denen er am Small Business Server arbeitet, um Dateien auszutauschen oder auf sein Postfach zurückzugreifen. Obwohl in diesem Unternehmen nur 40 Mitarbeiter beschäftigt sind, verbinden sich 50 PCs mit dem Server. Es müssen in diesem Beispiel daher 50 Geräte-Lizenzen erworben werden. Erwirbt das Unternehmen seine Lizenzen jedoch als Benutzer-Lizenz, sind lediglich 25 Lizenzen nötig, da nur 25 Benutzer mit dem Small Business Server 2003 R2 arbeiten.

Auch für Heimarbeitsplätze gibt es entsprechende Beispiele. In einem Unternehmen gibt es zum Beispiel 45 PCs. Von diesen 45 PCs werden 30 PCs im Schichtbetrieb von jeweils zwei Mitarbeitern geteilt. Zusätzlich gibt es 15 Mitarbeiter, die berechtigt sind, sich zu Hause ins Netzwerk einzuwählen und auf den Small Business Server zugreifen, um E-Mails abzurufen oder Dateien zu öffnen. Diese Mitarbeiter können auch mit Smartphones über das Internet auf den Exchange Server zugreifen. Diese 15 Mitarbeiter arbeiten jeweils an einem der 45 PCs des Unternehmens. Die beste Lizenzierung in diesem Beispiel sieht folgendermaßen aus: Das Unternehmen deklariert die enthaltenen fünf Lizenzen des Small Business Server als Benutzer-Lizenzen für fünf der Heimarbeitsplatz-Benutzer. Zusätzlich werden weitere zehn Benutzerlizenzen erworben und den Heimarbeitsplätzen zugewiesen. Mit diesen Lizenzen dürfen jetzt diese Heimarbeitsplatz-Benutzer sowohl von zu Hause mit Ihrem PC als auch mit dem Smartphone und dem PC am Arbeitsplatz auf den Server zugreifen. Für die restlichen 30 PCs werden Geräte-Lizenzen erworben, die es einer beliebigen Anzahl Benutzern erlaubt, von den 30 fest definierten PCs auf den Small Business Server 2003 R2 zuzugreifen.

Windows Home Server

Auch wenn es der Name nicht vermuten lässt, bietet sich der Windows Home Server auch für kleinere Unternehmen an.



Bild 2: Die klar gegliederte Startseite des Home Server

Der Server soll eine zentrale Datenablage, Sicherungsplattform und einen Zugriffspunkt darstellen, auf die alle Anwender im Haushalt oder kleinem Büro Zugriff erhalten. Auch die Nutzung des Internets ist möglich. Insgesamt lassen sich bis zu zehn Computer im Netzwerk zusammen mit dem Windows Home Server betreiben. Windows Home Server baut auf der 32-Bit-Version von Windows Server 2003 mit installiertem Service Pack 2 auf. Dadurch läuft das System auch in diesem frühen Entwicklungszustand schon sehr stabil. Generell ist die Bedienung von Windows Home Server sehr einfach gehalten. So eignet sich der Server auch für kleinere Unternehmen, die nicht über geschultes IT-Personal verfügen – Assistenten und einzelne Schaltflächen sind oft selbsterklärend. Geübte Anwender können zusätzlich zu den Standardfeatures Funktionen von Windows Server 2003 einsetzen, sodass von Anfängern bis Profis jeder seinen Server auf seine Bedürfnisse einrichten kann. Die primäre Funktion des Home Servers ist die Möglichkeit, alle Daten, Dokumente, Fotos und Bilder an einem zentralen Ort zu speichern, sodass diese Dokumente überall verfügbar sind. Da die

se Technologie dabei auf Sicherheitsmechanismen beruht, die auch in größeren Unternehmen zum Einsatz kommen, bietet sie einen guten Schutz. Auf dem Home Server wird der Sicherheitsstatus, die aktivierte Firewall und der Virenschutz aller Computer überwacht. Stellt ein Computer im Netzwerk ein Sicherheitsrisiko dar, warnt der Server den Administrator.

Mit dem Windows Home Server können externe Mitarbeiter über eine spezielle interne Webseite auch sicher über das Internet auf die Daten zugreifen. Die Kommunikation erfolgt dabei über einen Webbrowser und wird verschlüsselt. Wechselnde IP-Adressen im Internet stellen dabei kein Hindernis dar – Microsoft bietet hierfür einen kostenlosen dynamischen DNS-Dienst an. Der Zugriff aus dem Internet beschränkt sich aber nicht nur auf die Dateien und Freigaben, sondern bietet auch die Möglichkeit, via Remote Desktop auf Rechner im Unternehmen zuzugreifen. Eine weitere wichtige Funktion ist die automatische Datensicherung der angebundenen Client-Computer. Neben der zentralen Datenblage speichert der Server auch au-



Bild 3: Die Add-Ins finden sich übersichtlich in der Home Server-Konsole wieder

Worüber Administratoren morgen reden

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

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

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

Jetzt einfach und kostenlos
bestellen unter:





tomatisch die Daten der Clientcomputer. Diese Sicherung lässt sich auch auf dem jeweiligen Client-Computer einzeln konfigurieren. Alle angeschlossenen Client-Computer lassen sich komplett auf dem Server sichern und auch wiederherstellen. Dazu ist nur genügend Festplattenplatz auf dem Server erforderlich. Daten, die auf mehreren Computer identisch vorhanden sind, speichert der Sicherungsassistent automatisch nur einmal, was den unnötigen Plattenverbrauch des Servers reduziert. Zum Lieferumfang des Servers gehört auch eine Wiederherstellungs-CD.

Add-ins und Voraussetzungen

Microsoft stellt für den Windows Home Server ebenfalls ein Entwicklungssset kostenlos zur Verfügung. Der Server verfügt über eine Programmierschnittstelle, über die freie Entwickler die Funktion des Servers erweitern und neue Komponenten integrieren können. So gibt es bereits Erweiterungen, mit denen Sie die Webseite Ihres Servers anpassen können, damit diese grafisch ansprechender aussieht. Die Installation der Add-Ins ist bewusst einfach gehalten: Alle Zusatzmodule integrieren sich in die Home Server-Konsole.

Windows Essential Business Server 2008

www.microsoft.com/germany/server/essential/ebs/

Windows Essential Server Solutions

www.microsoft.com/germany/server/essential/default.mspx

Windows Hardware Logo Program for Systems

www.microsoft.com/whdc/winlogo/hwrequirements.mspx

Microsoft-Portal für den Mittelstand

www.microsoft.com/germany/mittelstand/

Windows Home Server-Webseite

www.microsoft.com/germany/windows/products/winfamily/windowshomeserver/

Deutsche Windows Home Server Community

www.home-server-blog.de

Add-Ins für den Home Server

www.whsaddins.net

Microsoft Home Server-Forum

<http://forums.microsoft.com/windowshomeserver/>

Links



Haben Sie Windows Home Server zusammen mit entsprechend lizenzierter Hardware gekauft, müssen Sie sich keine Gedanken über die Systemvoraussetzungen machen. Folgende Bedingungen gelten für die Installation: Der Computer muss mindestens über einen 1 GHz Pentium III oder vergleichbaren AMD-Prozessor verfügen. An Arbeitsspeicher erwartet die Software mindestens 512 MByte RAM, ansonsten bricht die Installation mit einem Fehler ab. Bei Windows Home Server handelt es sich um ein 32-Bit-Betriebssystem, das aber auch 64-Bit-Prozessoren unterstützt. Die Größe der Festplatte sollte mindestens 70 GByte betragen. Achten Sie darauf, dass herkömmliche IDE- oder SATA-Festplatten nicht für den Dauerbetrieb geschaffen sind und deutlich leichter defekt gehen als SCSI-Festplatten.

Der Home Server kann zwar ohne weiteres auch mit IDE-Festplatten entsprechend der Größe betrieben werden, allerdings wird empfohlen, SCSI-Platten zu verwenden, die aber deutlich teurer sind. Eine WLAN-Anbindung unterstützt Windows Home Server nicht. Die Clientcomputer im Windows Home Server-Netzwerk müssen mit einem der folgenden Betriebssysteme ausgestattet sein: Windows Vista Home Basic, Home Premium, Ultimate, Business oder Enterprise, Windows XP Home, Professional, Media Center, Tablet PC-Edition SP2. Manche Hersteller bieten Windows Home Server mit nur einer physikalischen Festplatte an. Diese Konfiguration ergibt allerdings keinerlei Sinn. Da auf dem Server alle Daten Ihres Netzwerkes gespeichert werden sollen, würden diese Daten verloren gehen, wenn nur eine Festplatte im Server eingebaut ist und die Festplatte defekt ist.

Sichere Datenablage

Sobald mehrere physikalische Festplatten im Server eingebaut sind, können Sie diese entweder durch ein Hardware-RAID auf dem Server, ein Software-RAID unter Windows Home Server oder einer Ordnerduplizierung absichern. Auch bei der Größe des Datenspeichers sollten Sie darauf achten, dass auf dem Server alle Daten

gespeichert werden, die bereits auf den vorhandenen Computern gespeichert sind. Aktivieren Sie die Ordnerduplizierung, verdoppelt sich dieser Speicherverbrauch. Lassen Sie sich noch die Computer im Netzwerk auf den Home Server sichern, was durchaus sinnvoll ist, benötigen auch diese Sicherungen Platz. Auch das Wachstum Ihrer Daten sollten Sie vorausplanen: Da Festplattenplatz sehr günstig ist, bietet es sich an, den Server mindestens mit zwei 500 GByte-Platten auszustatten, besser mehr. Auch wenn sich der Datenspeicher jederzeit vergrößern lässt, bedeuten zusätzliche Festplatten stets mehr Stromverbrauch. Nicht vergessen sollten Sie auch den Speicherverbrauch des Betriebssystems selbst, da auch dieses auf dem Home Server gesichert werden kann. Hinzu kommen noch bis zu 15 Prozent des Speicherplatzes für die Schattenkopien, die bei der Wiederherstellung des Servers eine große Rolle spielen. Lagern Sie Ihre Daten auf den Home Server regelmäßig per Datensicherung aus, sollten Sie den zusätzlichen Kauf einer externen Festplatte in Erwägung ziehen.

Da alle Daten auf dem Server abgelegt werden und auch der Zugriff über das Internet denkbar ist, installieren Sie auf dem Server eine Antiviren-Software. Achten Sie darauf, dass ansonsten keine beliebige Software installierbar ist, sondern nur Antiviren-Programme – entweder kompatibel zu Windows Server 2003 oder sogar speziell hierfür entwickelt. Die meisten Hersteller von Antiviren-Software bieten Versionen für Windows Home Server an. Der Betrieb und die Verwaltung von Windows Home Server stellen Anwender vor immer neue Herausforderungen. Das liegt zum einen daran, dass der Server ständig erweitert werden kann, zum anderen aber auch daran, dass die Verwaltung, vor allem im Fehlerfall, schnell Probleme bereiten kann. Aus diesem Grund haben wir für Sie im Kasten "Links" die wichtigsten Webseiten für Windows Home Server aufgelistet. Auf diesen Seiten erhalten Sie neue Informationen, zusätzliche Software, zahlreiche Anleitungen und oft auch rege Communities mit vielen Teilnehmern. (dr)





Neuerungen im Linux-Filesystem ext4

Neue Strukturen schaffen

von Thomas Drilling

Unter Linux gilt das seit Jahrzehnten ausgereifte Standard-Dateisystem ext3 als schnell und robust. Da ext3 jedoch bei LVM- und RAID-Systemen seit geraumer Zeit an seiner Kapazitätsgrenze kratzt, war eine Neuentwicklung unumgänglich. IT-Administrator zeigt auf, wie das seit der Kernel-Version 2.6-28 als stabil geltende ext4 mit neuen Features modernen Speicheranforderungen in Sachen Geschwindigkeit und Speicherplatz gerecht wird.

Das Dateisystem ext3 bringt für den Einsatz auf Server-Systemen mit komplexen RAID- und LVM-Konfigurationen zwei Probleme mit sich: Zum einen stößt es mit einer Maximalgröße für Dateien von 2 TByte und einer maximalen Gesamtgröße von 16 TByte massiv an eine Kapazitätsgrenze. Weiterhin bedingen Volumes in der genannten Größenordnung auch ein nicht mehr tolerierbares "Trägheitsproblem" bei Prüf- und Reparaturvorgängen, weil ext3 mit Zeitstempeln von einer Sekunde arbeitet.

Dazu muss erwähnt werden, dass sich ext3 technisch nicht von der Jahrzehnte alten Entwicklung ext2 unterscheidet. Die ext-Entwickler erweiterten ext3 lediglich um ein Journal, das jederzeit ein konsistentes Dateisystem garantiert und damit die Zeit zur Überprüfung eines möglicherweise korrupten oder nicht sauber gemounteten Volumes von Stunden auf Minuten reduzierte. Das galt allerdings zu der Zeit, als Volumes von einigen Hundert MByte noch als gigantisch galten. Auf heutigen Server-Systemen sind Größen von 16 TByte Festplattenspeicher – gerade in LVM-Verbünden – ziemlich alltäglich und wer mehr braucht, geht bei ext3 leer aus. Darüber hinaus sind die durch das Journal bedingten "rasanten" Reparaturzeiten gegenüber ext2 bei solchen Größenordnungen durchaus nicht mehrasant. Ansonsten erbt ext4 aber selbstverständlich alle positiven Eigen-

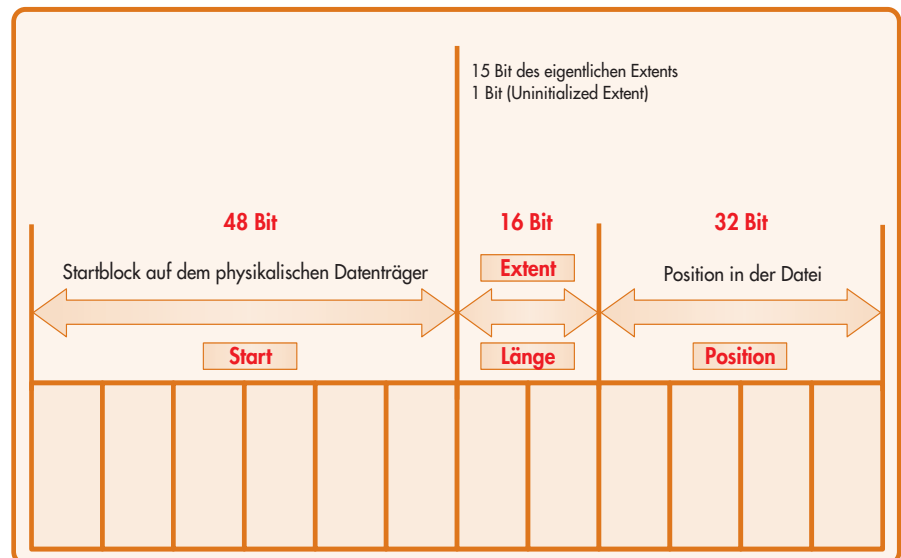


Bild 1: Die Datenstruktur zur Beschreibung eines Extents umfasst 96Bit (12Byte), wobei der eigentliche Extent 15 Bit groß ist.

schaften von ext3 und garantiert außerdem eine problemloses Upgrade.

Zu den unverkennbaren Vorteilen von ext3 gehört – etwa gegenüber anderen ehemaligen Neuentwicklungen wie ReiserFS oder XFS – dessen Robustheit aufgrund der ausgeklügelten Meta-Datenstrukturen. Damit sind alle ext-Dateisysteme so stabil, dass sich sogar von einer defekten Festplatte meist noch alle Daten retten lassen, auch wenn diese schon nicht mehr lesbar ist. Eine große Rolle bei Reparaturvorgängen spielen auch die ausgereiften ext-Tools aus dem Paket "e2fsprogs", wie etwa *fsck* oder *tune2fs*.

ext4 behebt Schwachstellen seiner Vorgänger

Die eigentliche Entwicklung von ext4 begann mit zwei relativ unspektakulären Patches für ext3, die testweise erstmals im Entwickler-Kernel 2.6-19 Einzug hielten. Zum einen erweiterten die Entwickler die Blocknummern, mit denen das Dateisystem die logischen Blöcke auf dem physikalischen Datenträger zählt, auf 48 Bit, was auf Anhieb für eine maximale Dateisystemgröße von 1 EByte (Exabyte = 1.024 TByte) sorgt. Dateien können prinzipiell 16 TByte groß werden, seit der Kernel-Version 2.6-25 sogar ebenfalls 1 EByte.

Die zweite große Neuerung bestand im Ersetzen der bisherigen "Indirekten Blockadressierung" durch so genannte "Extents", wie sie bei anderen modernen Dateisystemen längst gang und gäbe sind. Dies kommt vor allem dem effizienteren Umgang mit großen Dateien und damit indirekt der Performance zugute. Insbesondere die Einführung von Extents dürfte die wichtigste Neuerung von ext4 sein, galt allerdings bis zum Kernel 2.6-27 als experimentell. Seit der Kernel-Version 2.6-23 unterstützt ext4 bis zu 32.000 Unterverzeichnisse pro Directory. Mit der offiziellen Vorstellung von ext4 im stabilen Kernel 2.6-28 Ende 2008 gilt ext4 als fertig und einsatzbereit (und findet seitdem nach und nach Einzug in die Distributionen).

Hierbei wurde unter anderem auch ein wesentlicher Schwachpunkt von ext3 beseitigt, die maximal mögliche Auflösung bei Zeitstempeln von einer Sekunde. Diese führte – wie erwähnt – zu inakzeptabel langsamen Prüf- und Reparaturvorgängen bei sehr großen Volumes. Die Einführung

von Zeitstempeln auf Nanosekunden-Basis in ext4 beseitigt diese Schwachstelle. Verbleibende Probleme werden mit der aktuellen Kernel-Version 2.6-30 – aktuell war zum Redaktionsschluss der fünfte Release Candidate RC5 vom 9. Mai 2009 – behoben. Dem "0-Byte-Problem" wenden wir uns später in diesem Beitrag zu. Aktuell unterstützt bisher nur Ubuntu 9.04 ext4 vollständig. Hier steht das neue Dateisystem beim Partitionieren als Option zur Verfügung. OpenSUSE und Fedora werden ext4 erst mit ihren kommenden Versionen (openSUSE 11.2 und Fedora 11) unterstützen, dann aber bereits als Default-Dateisystem.

Neuerungen in ext4

Ext4 kann nicht nur größere Datenträger und Dateien verwalten, sondern bringt noch weitere interessante Neuerungen mit. Zwar gab es schon vorher Patches für ext3, die das eine oder andere Problem lösten, aber die ext-Entwickler wollten keine durch Patches bedingte Probleme riskieren und programmierten ext4 daher völlig neu. Dabei haben die Entwickler ext4 zahlreiche Verbesserungen spendiert, die gegenüber ext3 im Wesentlichen der Geschwindigkeit und Skalierbarkeit zugutekommen. Ist beispielsweise ein Dateisystem-Check erforderlich, geht das bei ext4 nicht nur aufgrund der Zeitstempel deutlich fixer, sondern auch deshalb, weil ext4 lediglich Blockgruppen prüfen muss, die auch allokiert sind.

Weiter haben die Entwickler ext4 mit einer neuen Version des "Journaling Block Device" (jdb2) ausgestattet und Dateien werden im I-Node jetzt endlich über "Extents" adressiert und nicht mit Hilfe der bei großen Dateien von einem gewaltigen Verwaltungs-Overhead überschatteten indirekten Blockadressierung. Die Zusammenfassung von zusammenhängenden Blöcken mit 48-Bit-Blocknummern trägt zudem zu einer Reduzierung des Zusatzaufwands bei der Adressierungslogik bei (RAM, E/A-Zugriffe und Transaktionen). Weiter ermöglicht ext4 eine so genannte "Online-Defragmentierung", also eine

Bild 2: Ubuntu9 unterstützt ext4 bereits vollständig

Defragmentierung während die Partition noch eingehängt ist. Eine weitere Neuerung namens "persistente Preallokation" ermöglicht das Reservieren von Speicherplatz für eine Datei im Voraus, der dann reserviert bleibt und mit hoher Wahrscheinlichkeit zusammenhängt, wovon vor allem Datenbanken und Media-Streams profitieren. Weitere Features der stabilen ext4-Version sind die Verwendung von Prüfsummen für das Journal oder das Reservieren von Verzeichnis-I-Nodes.

Extents organisieren die Datenflut

Alle UNIX- und Linux-Dateisysteme wie etwa die ext-Familie, aber auch XFS oder ReiserFS, arbeiten mit den drei wichtigen Datenstrukturen "Verzeichnisse", "Inodes" und "Datenblöcke". Datenblöcke fassen physikalische Festplattensektoren von je 512 Byte zu logischen Verwaltungseinheiten von 1, 2 oder 4 KByte zusammen. Über die Größe der logischen Datenblöcke entscheidet ein Parameter ("-b" beim Linux-Kommando *mke2fs*) beim Formatieren. Per Default passt *mke2fs* die Blockgröße übrigens automatisch an die Größe der Partition an. Bei der Größe heutiger Festplatten kommen aber ausschließlich 4-KByte-Blöcke zum Einsatz. Zwar vereinfachen möglichst große Blöcke das Verwalten großer Datenbereiche – ext3 und ext2 benutzen 32-Bit-Zahlen zum "Durchnummerieren" der Blöcke (das reicht bei 4-KByte-Blöcken für maximal 16 TByte) – allerdings kommt es bei großen Blöcken und kleinen Dateien mitunter zur Platzverschwendung (interne Fragmentierung), weil Dateien immer mindestens ganze Blöcke belegen müssen.

Bei allen UNIX-ähnlichen Dateisystemen übernehmen I-Nodes die Funktion eines Inhaltsverzeichnisses (I-Node-Liste oder auch Index-Tabelle) des gesamten Dateisystems. Der I-Node (I-Node für "Index node") ist eine spezielle Datenstruktur von 128 Byte, die Metadaten jeweils einer Datei enthält, wie deren exakten Speicherort auf der Festplatte sowie Größe und Dateiattribute. Im Gegensatz zu Windows-Dateisystemen verwalten zwar auch UNIX-Dateisysteme nicht unmittelbar physikalische Sektoren der Festplattenpartition, sondern logische Zuordnungseinheiten, allerdings spricht man bei UNIX von Blöcken und nicht von Clustern.

Beim Partitionieren lässt sich bestimmen, wie viel physikalischen Speicher (Festplattensektoren von je 512 Byte) ein Block enthalten soll, also etwa 1, 2, 4 oder 8 KByte. Davon hängt beispielsweise die maximale Dateigröße für das resultierende Dateisystem ab sowie die maximale Gesamtgröße des Dateisystems, die etwa für ext3 bei 2 TByte für eine Datei und 16 TByte für das gesamte Dateisystem liegt und eine Beschränkung darstellt, die maßgeblich für die längst überfällige Neuentwicklung ext4 verantwortlich war.

I-Nodes





Außerdem belegen die Verwaltungsstrukturen des Dateisystems bei kleinen Dateien anteilig mehr Platz zuungunsten der Datenblöcke. Große Dateien dagegen verursachen mehr Verwaltungs-Overhead im I-Node. Insbesondere die Ineffizienz der indirekten Blockadressierung beim Umgang mit großen Dateien hat mit ext4 zur Einführung von so genannten "Extents" geführt. Zwar gibt es selbstverständlich auch bei ext4 Datenblöcke, Verzeichnisse und I-Nodes. Ein ext4-I-Node adressiert allerdings überhaupt keine einzelnen Blöcke mehr, sondern "mappt" stattdessen einen (möglichst großen) "Bereich" einer Datei auf einen Bereich zusammenhängender physikalischer Datenblöcke auf der Festplatte.

Eines der wichtigsten Ziele bei der Entwicklung von ext4 bestand in der Kompatibilität. So ist ext4 in der Lage, ein bestehendes ext3-Dateisystem direkt zu mounten und in ein ext4-Dateisystem zu überführen. Somit lassen sich ext3-Dateisysteme ohne ein Backup mit Rücksicherung unmittelbar in ext4 konvertieren. Eine Rückwärts-Konvertierung ist allerdings nicht möglich. Zum Anlegen eines ext4-Dateisystems steht auch bei ext4 das Kommando:

```
mkfs -T ext4 {Devicename}
```

zur Verfügung. Mit

```
tune2fs -O extents {Devicename}
```

lässt sich ein ext3- in ein ext4-Dateisystem konvertieren. Linux speichert dann ab sofort sämtliche neuen Dateien im Extent-Format. Bestehende Dateien bleiben jedoch unangetastet. Außerdem versteht es sich von selbst, dass sich das neue Dateisystem ab jetzt nicht mehr als ext3 mounten lässt, weil der Vorgang irreversibel ist. Nach dem Anlegen des Dateisystems lässt sich dieses mit

```
mount {Devicename} {Einhängepunkt}
```

mounten. Zwar lässt sich das Dateisystem beim Mounten mit "-t ext4" angeben, die meisten Distributionen sind jedoch so konfiguriert, dass mount das Dateisystem automatisch erkennt. Ein existentes ext3-Dateisystem lässt sich übrigens auch als ext4 mounten, bleibt dabei aber natürlich bis zum endgültigen Konvertieren ein ext3-System.

Upgrade und Umgang mit ext4



te. Der Clou dabei: ein ext4-I-Node benötigt dazu nur noch drei Verwaltungs-Informationen statt einer ganzen Reihe davon, wie in ext3. Dazu gehören der "Beginn" (Position) sowie die Größe des Bereichs innerhalb der Datei und die Nummer des ersten physikalischen Datenblocks auf der Festplatte.

Der Datenbereich im I-Node zur Beschreibung eines Extents hat eine Größe von 12 Byte. Von diesen 96 Bit entfallen 48 Bit (48-Bit-Blocknummern) auf die physikalische Startadresse des korrespondierenden Blockbereichs auf der Festplatte, 32 Bit auf die "Position" innerhalb der Datei und 16 Bit auf die "Größe" des Extents selbst. Allerdings nutzt ext4 von diesen 16 Bit tatsächlich nur 15 Bit für die Größe des Extents. Das zusätzliche Bit ist ein Status-Bit, welches kennzeichnet, ob der Extent bereits Daten enthält oder nicht. Die Reduzierung der Extent-Größe auf 15 Bit hat übrigens zwei Gründe. Zum einen ist das übrige Bit für die Realisierung der bei den Neuerungen beschriebenen Funktion "persistent preallocation" verantwortlich, zum anderen kommt die Reduzierung auf 15 Bit der Tatsache entgegen, dass ein einzelner Extent damit maximal 2^{15} , also 128 MByte groß werden kann, weil ja bekanntlich alle Linux-Dateisysteme die Datenbereiche der Festplatte in 128-MByte-Blöcke aufteilen.

Jeder solchen "Blockgruppe" ist dann jeweils eine "Kopie des Superblocks", ein "Blockgruppen-Deskriptor" sowie ein Ausschnitt der I-Node-Bitmap, der Block-Bitmap und der eigentlichen I-Node-Tabelle vorangestellt.

Bei größeren Dateien kommt auch bei der Verwendung von Extents ein indirektes Verfahren zum Einsatz, so genannte "Extent-Bäume". Dabei kommt mit dem "Extent-Index" eine weitere Datenstruktur ins Spiel. Dieser enthält nur die Start-Position des Extents innerhalb der Datei sowie eine physikalische Blocknummer auf der Festplatte. Dieser Datenblock enthält dann entweder weitere Extents, die auf Datenblöcke zeigen, oder wieder einen Extent-Index. Auch hier beginnt jeder Block mit einem Extent-Header und der gesamte Extent-Baum hat seine Wurzel im ersten Extent-Index direkt im I-Node.

Maximale Volume-Größe

Ext4 erweitert die 32-Bit-Blocknummern auf dem physikalischen Datenträger von ext3 auf 48 Bit. Allerdings "zählt" auch ext4 die Blöcke innerhalb einer Datei mit 32 Bit – was grundsätzlich zu unterscheiden ist und für die maximale Dateigröße von 2^{32} (16 TByte) verantwortlich ist. Die Standard-Blockgröße bleibt unverändert bei 4 KByte. Aus diesen Eckdaten ergibt sich eine rechneri-

SEMINARMARKT

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

www.it-administrator.de/seminarmarkt

**Mit Wissen
zum Erfolg**



Die ADN Akademie bietet bundesweit Seminare und Zertifizierungen als autorisiertes Schulungszentrum für:

CITRIX

DataCore

IGEL

Microsoft

SONICWALL

SWH

Buchen Sie noch heute!

02327.9912-425

www.adn.de/training





sche Gesamtgröße für das gesamte Dateisystem von 2^{48} (1 EByte), was für die nächsten Jahre und Jahrzehnte auch ohne eine weitere Vergrößerung der Blocknummern ausreichend sein sollte, wenn gleich eine Vergrößerung der Blocknummern auf etwa 64 Bit in Zukunft durchaus denkbar ist.

Vorteile der Extents

Die Vorteile der Extents sind zum einen eine Verkleinerung des Verwaltungs-Overheads bei sehr großen Dateien. So benötigt eine relativ große Datei (< 512 MByte) zum „Aufgefunden werden“ bei ext4 nur drei Extent-Strukturen von je 12 Byte, während eine ext3-I-Node dazu mehrere hundert KByte wahllos verteilter 32-Bit-Blocknummern zusammensuchen muss, was nicht nur mehr Verwaltungsspeicher kostet, sondern auch länger dauert. Weiter vermindern Extents dank der damit einhergehenden Neuerung der „persistenten Preallokation“ von Speicher auch den Grad einer etwaigen „externen“ (im Gegensatz zur beschriebenen „inter-

nen“) Fragmentierung. Dies zahlt sich vor allem bei Streaming-Daten oder einer mit der Zeit anwachsenden Image-Datei von VMware aus. Im Übrigen ist „interne Fragmentierung“ bei jedem Dateisystem „normal“ und kostet allenfalls Speicherplatz, während die externe Fragmentierung im Einzelfall durchaus zu Lasten der Performance gehen kann.

Das 0-Byte-Problem

Bei der Einführung von ext4 allerdings berichteten Nutzer von mysteriösen Datenverlusten, die bei genauerer Betrachtung gar nicht mysteriös sind. So speichert ext4 Dateien nach Möglichkeit stets zusammenhängend, wozu auch das Prinzip der Blockgruppen – eine Art interne Partitionierung des Dateisystems – beiträgt. Da ext4 Schreibzugriffe nicht direkt ausführt, sondern gepuffert, muss der „Block Allocator“ nicht jeden einzelnen Block sofort aufrufen, sondern kann stets mehrere Datenblöcke am Stück allokalieren (delayed allocation). Im Idealfall lässt sich so ein kompletter Extent am Stück reservieren (multiblock allocation).

Unter dem Strich stellt jedoch die beschriebene delayed-allocation-Funktion eine so genannte „aggressive“ Cache-Strategie dar, bei der das Risiko eines Datenverlustes bei Stromausfall oder Systemabsturz steigt, weil Daten einerseits länger im Cache verbleiben und außerdem das Schreiben von Meta-Informationen und Daten immer nacheinander mit einem gewissen zeitlichen Abstand erfolgt. So kann eine neu angelegte Datei beispielsweise im Dateisystem auftauchen, noch „bevor“ die eigentlichen Daten geschrieben sind, dann allerdings mit der Größe 0 Byte, weil die zugeordneten Datenblöcke noch nicht geschrieben wurden.

Dieses Verhalten ist durchaus regelkonform, hat aber einen unschönen Nebeneffekt. So greifen etwa vorsichtige Programmierer beim Schreiben einer neuen Version einer Datei zu dem Trick, zunächst in eine neue temporäre Datei zu schreiben und diese erst in einem zweiten

Schritt auf den alten Namen umzubenennen. Auf diese Weise bleibt die Original-Datei so lange wie möglich erhalten, sollte es beim Schreiben der neuen Datei zu einem Systemabsturz kommen. Im Zusammenhang mit „delayed allocation“ allerdings kann es in einem solchen Fall passieren, dass die überschriebene Datei nach einem Absturz keine Daten enthält, weil der zugehörige I-Node-Eintrag schon auf die neu angelegte Datei zeigt, die Funktion „rename ()“ aber ebenfalls eine reine Meta-Operation ist und die Daten noch nicht geschrieben sind.

Da es seit der Einführung von ext4 in dieser Hinsicht mehrfach zu Unmut bei betroffenen Anwendern kam, was eine hitzige Diskussion bei den Kernel-Entwicklern nach sich zog, hat Linus Torvalds ab der Kernel-Version 2.6-30 für eine Änderung gesorgt. Ext4 versucht jetzt derartige „problematische Situationen“ selbsttätig zu erkennen und schaltet im Bedarfsfall in das beschriebene Verhalten von ext3 zurück, schreibt also immer erst Daten, bevor es Meta-Informationen ändert.

Fazit

Für Arbeitsplatz-Anwender besteht angesichts der Stabilität und Ausgereiftheit von ext3 derzeit kein zwingender Bedarf, auf ext4 umzusteigen, zumindest solange nicht, bis die kommenden Versionen der großen Distributionen ext4 als Standard mitbringen. Der Geschwindigkeitsvorteil zählt aber auch hier schon jetzt, insbesondere dann, wenn es um Anwendungen mit sehr großen Dateien (Datenbanken, Mediastreaming, Virtual Computing) oder sehr vielen Dateien geht, wie etwa Mail-/IMAP-Server, allesamt aber eher Server-Anwendungen. Bei Servern ist ein Wechsel jedoch vielfach schon jetzt von Nöten, weil ext3 auf RAID- und LVM-Systemen an seine Grenzen stößt. Mit ext4 dagegen lassen sich Dateisysteme mit bis zu 1 Exabyte anlegen und verwalten. In dieser Hinsicht wird ext4 in erster Linie einem Vergleich mit XFS standhalten müssen, da ReiserFS nicht mehr weiterentwickelt wird und bisher nicht im Kernel enthalten ist. (jp)

Informationen zu ext4 allgemein

http://wiki.ubuntuusers.de/Jaunty_Jackalope#ext4-Dateisystem/
<http://ext4.wiki.kernel.org/index.php>
<http://kerneltrap.org>

Design von ext4 / Extents

http://ext4.wiki.kernel.org/index.php/Ext4_Design7
<http://lwn.net/Articles/187321/>
<http://kernelnewbies.org/Ext4/>

Information zum 0-Byte-Problem in Zusammenhang mit der Cache-Strategie Delayed Allocation

www.linux-community.de/Internal/Nachrichten/Ext4-soll-Datenverlust-verursachen/
<http://thunk.org/tytso/blog/2009/03/12/delayed-allocation-and-the-zero-length-file-problem/>
<http://ldn.linuxfoundation.org/blog-entry/delayed-allocation-and-zero-length-file-problem/>

Links



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 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 Dozenten: Thomas Weyergraf und Nico Lüdemann 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 Dozenten: Thorsten Christoffers, Dr. Michael Schwartzkopff 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

iläNet
Die System und Netzwerk User Group

IT-Administrator Trainings-Partner

fast lane

ITANet Schirmherrschaft:


REALTECH

Mehr Infos und Anmeldeformulare zu den Veranstaltungen unter

<http://www.it-administrator.de/usergroup/termine/>
oder per E-Mail an info@itanet.de



Virtual Desktop Infrastructure mit VMware View einrichten (1/3)

Zentralisierung am Arbeitsplatz

von Andreas Badur und Dr. Jürgen Fechter

Bislang war der Begriff Server-based Computing mit Terminalservern verbunden. Doch seit kurzem drängen Virtual Desktop Infrastructure-Lösungen der verschiedensten Hersteller in diesen Markt und hauchen dem etwas angestaubten traditionellen Ansatz mit Individualität, Innovation und Virtualisierung neues Leben ein. Wir zeigen Ihnen am Beispiel von VMware View, wie Sie die komplexe neue Technik in den Griff bekommen.

Die Virtual Desktop Infrastructure (VDI) ergänzt die bisherige Virtualisierungs- und IT-Landschaft. Besonders bei zentral verwalteten, aber dennoch individuellen Clients spielt VDI seine Stärke aus: Die Benutzer greifen mit ihren Rechnern auf ein virtuelles Gastsystem zu. Diese zusätzliche Virtualisierungsschicht vereinfacht Installationen, Upgrades, Patches, Backups und Restores. Auch andere durch die Virtualisierung geschätzte Vorteile wie die Live-Migration von VM-Gastsystemen, Suspend und Resume sowie Snapshots machen VDI interessant. Das Konzept ersetzt jedoch Terminalserver-Umgebungen oder standardisierte lokale Desktopumgebungen auch aus Kostengründen in nächster Zeit nicht. Die Präsenz der zahlreichen namhaften VDI-Produktanbieter offenbart dennoch eindrucksvoll das mögliche zukünftige Potenzial dieser Technik.

VMware View

Bei VMware heißt die entsprechende VDI-Technologie "VMware View". Sie reiht sich nahtlos in bestehende VMware Infrastructure 3-Umgebungen ein. Ein Virtual Center (VC) ist dabei Pflicht, Cluster und Data Stores auf SAN-/NAS-Servern Kür. Ob Sie ESX- oder ESXi-Hosts einsetzen, spielt keine Rolle. VMware View kommt außerdem ohne VMotion und High Availability (HA) aus, lebt aber

mit diesen Optionen erst richtig auf. Der VMware View Manager besteht aus mehreren Komponenten: View Connection Server (VCS), View Agent, View Client, View Client with Offline Desktop, View Portal, View Administrator, View Composer und ThinApp. Den View Composer, ThinApp und die – momentan noch experimentelle – Offline Desktop-Unterstützung gibt es nur in der teureren Premier-Version.

Eine minimale Testumgebung setzt sich aus dem VCS, VC mit ESX(i)-Server, einem Active Directory (AD)-Domänencontroller und Desktop Clients mit View Client zusammen. Das VC muss mit den Sysprep-Ergänzungen ausgestattet sein. Auch sollte grundlegendes Know-how über VMware Infrastructure 3 vorhanden sein. Das AD von Windows 2000 und Windows 2003 wird unterstützt, Schemaänderungen sind keine notwendig.

Architektur und Protokolle

Die Kernkomponenten einer View-Umgebung sind der View Client, View Agent und der VCS. Als View Client dient entweder ein Thin Client, der mit VMware View kompatibel sein muss, oder ein Standard Windows-, Linux- oder Mac-Client. Auf diesen wird dann die View Client-Software installiert. Während der View Client unter Windows als eine native Ap-

plikation realisiert ist, basiert er für Linux- und Mac-Rechner auf Java. Bei Letzteren erfolgt der Zugriff über einen Browser auf ein Web-Portal. VMware bezeichnet deshalb den Client als View Portal. Dieser Zugriff geht bei Windowssystemen op-

Zu den Vorteilen von SBC zählen

- Zentrales Management
- Fernzugriff kann von jedem Ort aus erfolgen.
- Sicherheit durch zentrale Haltung der Daten im Rechenzentrum. Dadurch ist eine leichte Einhaltung der gesetzlichen Vorgaben möglich.
- Bessere Performance, einfache Erweiterung der Ressourcen
- Thin Clients senken die mit Administration, Installation, Wartung, Stromverbrauch und Support verbundenen Betriebskosten weiter.

Zu den Nachteilen von SBC zählen

- Der Netzwerkzugriff muss gewährleistet sein.
- Restriktionen der Desktopzugriffs-Protokolle wie RDP oder ICA
- Eingeschränkte Applikationskompatibilität: Manche Programme laufen nicht auf SBC-Basis. Dies hat programmtechnische Gründe wie hart codierte Verzeichnisse oder Zugriff auf lokale Geräte (etwa Dongle an USB- oder COM-Schnittstelle).
- Die Desktop-Protokolle unterstützen keine hardwareunterstützte 3D-Darstellung auf Clientseite. Auch Media Streaming, beispielsweise für Videobearbeitung, ist eine Herausforderung und funktioniert nicht mit jedem Client.

Vor- und Nachteile von Serverbased Computing





tional auch durch Installation eines ActiveX Controls. Die Aufgaben des VCS sind vielfältig. Er erlaubt beispielsweise einen sicheren serverseitigen Verbindungsaufbau durch die Komponente View Secure Gateway Server. Die andere Schlüsselkomponente ist der View Broker Admin Server. Diese enthält zwei Portalserver: einen für die Benutzer, die auf ihre Desktops zugreifen wollen und einen für die Administratoren zur Verwaltung ihrer VMware View-Umgebung. Die Authentifizierung der View Clients erfolgt über den VCS durch das AD. Er holt Benutzer- und Gruppen-Informationen aus dem AD und ordnet sie den virtuellen Desktops oder Desktop-Pools zu.

Diese Informationen zusammen mit zusätzlichen Konfigurationsdaten werden in einer ADAM-Datenbankinstanz (Active Directory Application Mode) gespeichert. Das Minimum sind drei Einträge: das VM-Gastsystem selbst, die Beschreibung des Pools mit den dazugehörigen Gastsystemen und ein Desktop-Applikationseintrag je Pool. Betrachten können Sie die Einträge mit dem lokal installierten Programm ADAM ADSIEdit. Damit kann der VCS seine Brokerrolle erfüllen und die richtigen Zielsysteme anbieten. Darüber hinaus korrespondiert der VCS auch mit dem VC, um virtuelle Maschinen (VM) bereitzustellen. Zusammenfassend dient der Connection Server also dazu, Konfigurationseinstellungen vorzunehmen, virtuelle Desktops und Pools zu verwalten, Berechtigungen für Desktopzugriffe für Anwender oder Gruppen festzulegen sowie zum Aufbau und Koordination der Client-Verbindungen, zur Authentifizierung und als Portal. Ist dieser von einer Störung betroffen, verlieren die Clients ihre Verbindung, weshalb der Aufbau eines Replica-Servers in einer Produktivumgebung ratsam ist. Damit umgehen Sie diesen "Single Point of Failure".

Der View Agent läuft als Dienst auf den Zielmaschinen und stellt die Kommunikation zwischen View Client und VCS sicher. Der Agent muss also auf sämtlichen

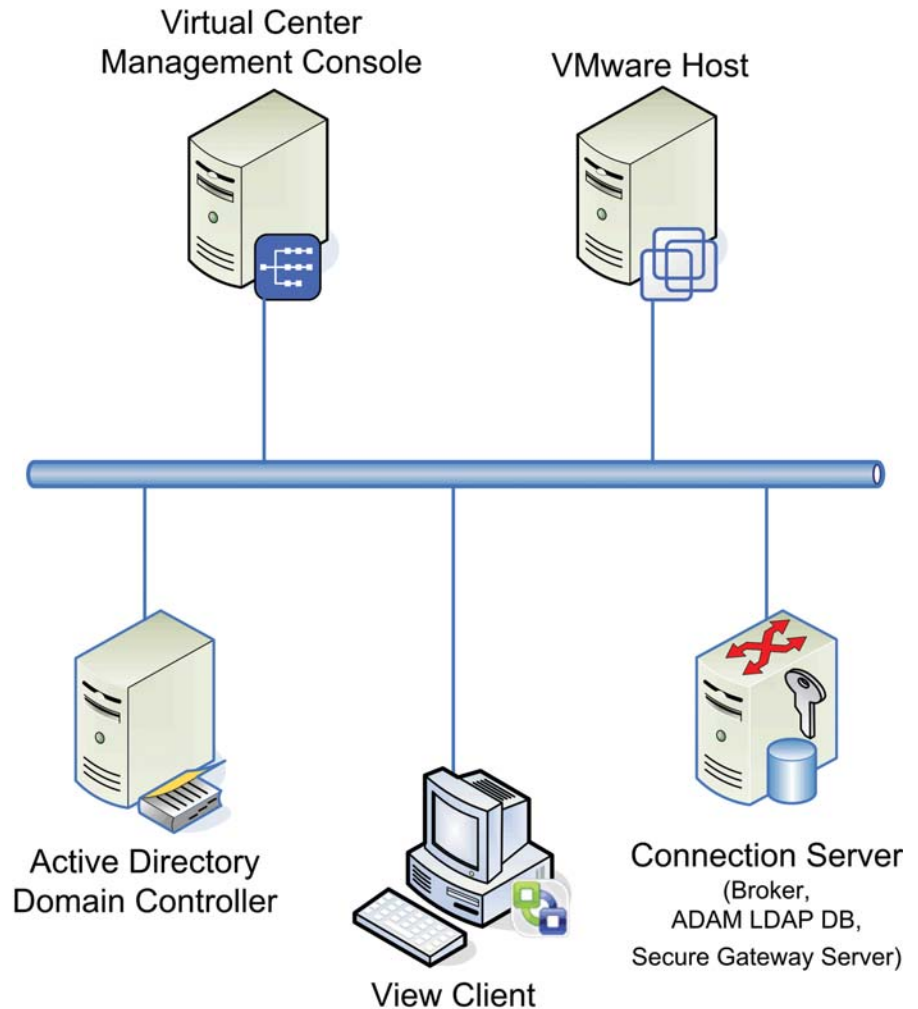


Bild 1: Unsere Workshop-Umgebung für den View Client:
Der Connection Server, das Virtual Center und ein AD-DC sind Pflicht

Zielsystemen, egal ob virtuell oder physikalisch, installiert sein und dient zum Aufbau und Monitoring der Verbindung. Er beinhaltet Komponenten für virtuelles Drucken, vormals ThinPrint, Remote USB-Unterstützung und SingleSignOn. Zusätzlich verrichtet er Aufgaben, wie den Namen des View Clients an das Gastsystem zu geben.

Kommunikation der drei Kernkomponenten

Beim erstmaligen Verbindungsaufbau stellt der Benutzer mit seiner View Client-Software oder dem Portal eine Verbindung zum Desktopsystem her. Allerdings geschieht dies nicht direkt, sondern über den vermittelnden VCS. Dieser nimmt die Anfrage des View Clients an. Er sucht die

entsprechenden Zielsysteme aus seiner ADAM Datenbank zusammen mit dem Benutzernamen heraus. Dies kann ein ganzes individuelles Gastsystem, ein (noch) nicht personalisiertes Image im Pool oder aber eine physikalische Maschine wie ein Desktop-Client oder Terminalserver sein. Im nächsten Schritt erscheint eine Liste der Zielsysteme auf dem View Client.

Der Benutzer wählt einen der Einträge aus; dieser Schritt kann auch automatisiert werden. Die Auswahl wird über eine neu aufgebaute zweite Verbindung zum VCS zurückgemeldet. Im Falle eines Pools wird nun die konkrete (virtuelle) Maschine festgelegt. Der VCS nimmt Kontakt zum VC auf und fragt den Status des Zielsystems ab. Gegebenenfalls ist ein Auf-

wecken, Neustart oder eine automatische Bereitstellung einer neuen Maschine notwendig. Als abschließender Schritt stellt der VCS eine RDP-Verbindung über den View Agent des Zielsystems her, tunnelt diesen mit dem HTTP/HTTPS Protokoll und reicht ihn unter der bestehenden zweiten Verbindung an den View Client weiter. Bei Nutzung eines Thin Clients entfällt der Tunnel, da dieser nur direkt über das RDP-Protokoll auf Clients zugreifen kann.

Unterstützte Systeme

Die Liste der unterstützten Betriebssysteme ist nicht besonders lang, reicht aber für den Unternehmenseinsatz aus. Der View Connection Server muss auf einem Windows 2003 Server mit AD-Anbindung installiert werden. Die Minimalanforderung ist ein 32-Bit-Windows Server 2003 Standard mit SP2. R2, Enterprise Edition und 64 Bit werden ebenfalls unterstützt. Die von View Agent, View Client und Offline Desktop unterstützten Betriebssysteme finden Sie in Tabelle 1. Generell gilt, dass 64-Bit-Systeme nicht unterstützt werden. Das ist aber normalerweise nicht weiter tragisch, da typischerweise bei virtuellen Desktops kein großer Arbeitsspeicher benötigt wird.

Unterstützte Client-Betriebssysteme				
Betriebssystem	View Agent		View Client	Offline Desktop
	virtuell	physikalisch		
Windows 2000 Prof. SP4	–	–	✓	–
Windows XP Prof. SP 1	✓	✓	✓	–
Windows XP Prof. SP 2/3	✓	✓	✓	✓
Windows XP Home SP 2	–	–	✓	–
Windows XP embedded	–	–	✓	–
Windows Vista Home/ Home Premium	–	–	✓	–
Windows Vista Business/ Business SP 1	✓	✓	✓	–
Windows Vista Enterprise SP 1	✓	✓	–	–

VMware unterstützt im webbasierten Umfeld auch nur 32-Bit-Betriebssysteme, aber die Zugriffe sollten auch mit 64-Bit-Betriebssystemen möglich sein. Wir konnten dies erfolgreich mit einem CentOS 5.2 64 Bit, Firefox 3.0.6 32 Bit und rdesktop1.6 testen. Der Zugriff auf den Webadministrator funktioniert auch von

Windows Server 2003 und 2003 R2 aus. Der Zugriff auf das Webportal funktioniert nur mit Windows Server 2003 und nicht mit dem 2003 R2. Da VMware dies nicht offiziell unterstützt, wurde es nicht in der Tabelle aufgeführt.

Installation des VMware View Connection Server

Der VCS ist das Herzstück von VMware View. Er verrichtet seine Arbeit als Verbindungsbroker und stellt gleichzeitig das administrative Interface, den View Administrator, und das Webportal "View Portal" für den Zugriff auf die virtuellen Desktops zur Verfügung. Sie können den VCS in drei Varianten installieren: Standard, Replica oder Security. Letztere dient dazu, einen Broker in der DMZ zu betreiben, ähnlich dem Edge-Server von Exchange 2007. Die Hardware-Anforderungen für einen VCS sind sehr niedrig: Ein Pentium IV 2-GHz-Prozessor oder höher, wobei Dual-Prozessoren empfohlen werden, mindestens 2 GByte RAM, wobei ab 50 Desktops mehr als 3 GByte empfohlen werden, und eine 10/100 MBit-Netzwerkkarte (Gbit empfohlen). Die Anforderungen sind für alle Varianten gleich. Gerne darf der VCS auch in einer VM laufen.

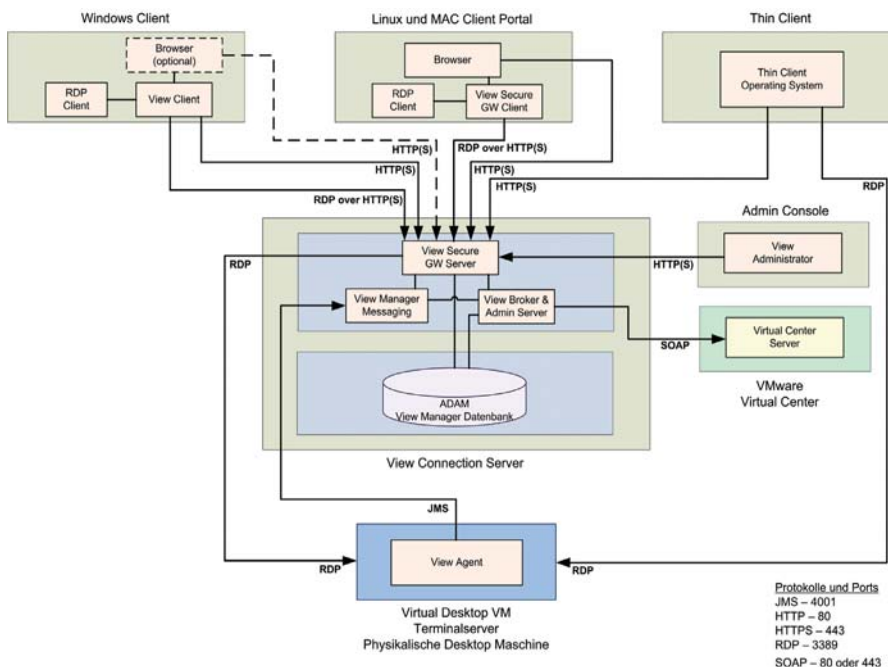


Bild 2: In der Systemarchitektur von View dominieren die Protokolle HTTP/S und RDP

Während der Installation wird automatisch Microsofts LDAP-Server ADAM auf der Maschine eingerichtet. In ADAM sind die Konfigurationen von VMware View gespeichert. Möchten Sie eine Ausfallsicherheit oder Loadbalancing der Verbindungsbroker erreichen, installieren Sie neben dem Standard- weitere Replica-Server. Da ADAM dieselbe Replikationstechnik wie das AD benutzt, kann nun jeder beliebige VCS-Server ausfallen, ohne dass es zu Datenverlusten oder Konnektivitätsproblemen kommt. Leider bringt der VCS kein eigenes Loadbalancing mit, so dass Sie auf Drittherstellertools ausweichen müssen.

Die Installation selbst ist sehr einfach: Starten Sie *VMware-viewconnectionserver-{xxx}.exe*, akzeptieren die Lizenzbedingungen und wählen einen Installationsordner aus. Fertig. Wenn Sie ein verteiltes Administrationskonzept haben, können Sie auch für die VMware View-Administration eine eigene Rolle definieren. Werfen Sie dazu einen Blick auf den Kasten "Eigene Rolle im VC definieren". Die initiale View Manager Konfiguration erfolgt dann über die Weboberfläche. Hier dürfen sich alle lokalen Administratoren des VCS anmelden. Da ein self-signed Zertifikat mitinstalliert wurde, erscheint eine Warnung, die Sie jedoch ignorieren können. Sie können dieses Zertifikat natürlich auch durch eines der eigenen oder einer öffentlichen Public Key Infrastructure (PKI) austauschen.

Austausch des Zertifikats

Führen Sie folgende Schritte aus, um den VCS mit einem anderem Zertifikat zu versehen: Um den VCS mit einem ande-

Voraussetzungen für webbasierte Komponenten

Betriebssystem	View Portal	View Administrator
Windows 2000 Prof. SP4	keine Unterstützung	
Windows XP Prof. SP 1/2/3, SP2	Internet Explorer 6 SP2 / Internet Explorer 7	
Windows Vista Home/Home Premium		
Windows Vista Business/Business SP 1	Internet Explorer 7	Internet Explorer 6 Internet Explorer 7 Firefox 2.0 Firefox 3.0
Windows Vista Ultimate/Ultimate SP 1		
RedHat Enterprise Linux 5.0, Update 1	Firefox 2.0 / 3.0 Java JRE 1.5.0 oder 1.6.0 rdesktop ab 1.4.1	
Suse Linux Enterprise 10 SP1		
Ubuntu 8.04		
Mac OS X 10.4 und 10.5	Safari Java JRE 1.5.0 RDC 2.0	

Kostenlos für
IT-Administrator-Abonnenten

iläNet

Workshop in Heidelberg

Hochverfügbarkeit

am 16. Juli 2009

Die Agenda:

- > Verteilung von Microsoft App-V-Paketen mit SCCM 2007 R2 zur Optimierung der Verfügbarkeit – wie Administratoren durch den redundanten Aufbau der Verteilungsserver des SCCM eine Hochverfügbarkeit der Zustellung von virtuellen Paketen sicherstellen.

Referent: Thorsten Christoffers, sepago, Köln

- > Linux HA Version 3 – wohin geht die Reise?

Referent: Dr. Michael Schwartzkopff,
MultiNET Services GmbH, Grasbrunn

Workshop-Partner:

- > Hochverfügbarkeit sichern – Unternehmensweites IT-Management auf Basis einer normalisierten CMDB

ITANet Workshop-Partner:



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

Termin: 16. Juli 2009

Ort: Print Media Lounge, Kurfürstenanlage 60,
69115 Heidelberg

Uhrzeit: 13.00 bis ca. 17.30 Uhr

Teilnahmegebühren:

Für ITANet-Mitglieder beziehungsweise
IT-Administrator-Abonnenten kostenlos.

ITANet Schirmherrschaft:



Anmeldeschluss: 06.07.2009

Mehr Infos und Anmeldeformulare unter
<http://www.it-administrator.de/usergroup/termine/>



Bei Bedarf kann im VC eine eigene Rolle "View Administrator" definiert werden. Dafür werden folgende Rechte benötigt:

- Folder: Create Folder, Delete Folder
- Virtual Machine — Inventory: Create, Remove
- Virtual Machine — Interaction: Power On, Power Off, Suspend, Reset
- Virtual Machine — Configuration: Add new disk, Add or Remove Device, Modify Device Settings, Advanced
- Provisioning: Customize, Deploy Template, Read Customization Specifications
- Resource: Assign Virtual Machine to Resource Pool

Eigene Rollen im VC definieren



ren Zertifikat zu versehen, stellen Sie sicher, dass das Javatool "keytool" sich im Suchpfad befindet. Erweitern Sie dazu die Umgebungsvariable "PATH" um C:\Program Files\VMware\View Manager\Server\jre\bin. Öffnen Sie anschließend eine Konsole und wechseln Sie in das Verzeichnis "C:\Program Files\VMware\View Manager\Server\sslgateway\conf". Mit

```
keytool -genkey -keyalg "RSA"
-keystore keys.p12
-storetype pkcs12 -validity 360
```

erstellen Sie dort einen neuen Keystore. Füllen Sie alle angeforderten Werte aus. Wenn nach dem Vor- und Zuname gefragt wird, geben Sie den FQDN des VCS ein. Das Länderkürzel muss zweistellig erfasst werden, also DE für Deutschland. Erstellen Sie nun ein neues Certificat Signing Request (CSR). Geben Sie hierzu auf der Konsole ein:

```
keytool -certreq -keyalg "RSA"
-file certificate.csr
-keystore keys.p12 -storetype
pkcs12 -storepass
{secret}
```

Wobei {secret} für das Passwort des Keystores "keys.p12" steht. Hierbei wurde ein CSR in der Datei *certificate.csr* abgelegt. Dieses reichen Sie bei Ihrer lokalen oder

externen PKI wie VeriSign ein. Fordern Sie auf jeden Fall ein PKCS#7-Zertifikat an. Bei Thawte gibt es zum Testen kostenlos ein 21 Tage gültiges SSL-Zertifikat [2]. Speichern Sie das erhaltene Zertifikat auf dem VCS in einer Datei *certificate.p7* ab und rufen dann folgenden Befehl

```
keytool -import -keystore keys.p12
-storetype pkcs12 -storepass
-keyalg "RSA" -trustcacerts
-file certificate.p7
```

auf. Nun müssen Sie dem VCS noch mitteilen, dass er das neue Zertifikat in dem Store *keys.p12* verwenden soll. Stellen Sie sicher, dass die Datei *keys.p12* in "C:\Program Files\VMware\View Manager\Server\sslgateway\conf" liegt. Erstellen Sie in demselben Verzeichnis eine Datei *locked.properties* und tragen folgende Werte ein:

```
keyfile=keys.p12
keypass={secret}
```

Starten Sie den Dienst "VMWare View Connection Server neu". Melden Sie sich am View Administrator an und überprüfen Sie, ob in den Events folgende Meldung auftaucht "The Secure Gateway Server is using SSL certificate store keys.p12 with password of 6 characters".

Die Verwaltungsoberfläche

Der View Administrator gliedert sich in vier große Bereiche, die Sie über entsprechend benannte Knöpfe erreichen. Unter "Desktops and Pools" sehen Sie im linken Teil alle definierten Pools und im rechten Teil alle dazugehörigen Einstellungen. Unter "User and Groups" ist es ähnlich. Links sehen Sie nur die Benutzer und Gruppen des ADs, für die Konfigurationen vorgenommen wurden und rechts die jeweiligen Werte. Diese beiden Bereiche enthalten auch eine Suchfunktion, um bei vielen Pools oder Gruppen leichter den Überblick zu behalten. Den Bereich "Events" können Sie benutzen, um Ereignisse und Probleme des VCS zu beobachten und analysieren.

Unter "Configuration" nehmen Sie die globalen Einstellungen von VMware View vor. Hier tragen Sie nun den Lizenzschlüssel und die VC-Server mit Benutzernamen und Passwort ein. Für den Zugriff auf das VC empfiehlt es sich, einen eigenen Benutzer im AD anzulegen. Die Checkbox "Connect using SSL" und die Einstellungen zum View Composer bleiben aktiviert beziehungsweise unverändert. Unter "Advanced" können Sie nun noch global festlegen, wie viele Maschinen maximal gleichzeitig erstellt werden (Maximum number of concurrent provisioning operations) und bei wie vielen Maschinen maximal gleichzeitig der Powerstatus geändert werden darf (Maximum number of concurrent power operations). Verändern Sie die Werte je nach Leistungsfähigkeit Ihrer Hostsysteme. Damit ist die initiale Installation und Konfiguration abgeschlossen.

Ein Backup der Konfiguration können Sie leicht mit dem mitgelieferten Tool erzeugen. Öffnen Sie ein Konsolenfenster und wechseln Sie in das Verzeichnis "C:\Program Files\VMware\View Manager\Server\bin\". Dort führen Sie den Befehl *vdmexport > vdmconfig.ldf* aus. Damit werden die LDAP Informationen des ADAM in die Datei *vdmconfig.ldf* ausgegeben. Um einen Restore der Daten durchzuführen, benötigt Sie das Tool LDIFDE. Mit *LDIFDE -i -f vdmconfig.ldf -s 127.0.0.1* auf dem VMC werden die Daten aus der Datei zurück ins LDAP gespielt.

Installation VMware View Agent

Die Agentensoftware muss auf allen Rechnern installiert werden, die über den VCS gemanagt und auf die zuge-

Sie sollten im AD eine Gruppe der Benutzer definieren, die auf diese Maschine Zugriff per RDP haben dürfen. Standardmäßig ist das nur den Administratoren erlaubt. Diese Gruppe wird in die lokale Gruppe "Remotedesktopbenutzer" aufgenommen.

Tipp



griffen werden soll. Dies kann etwa auch eine VM auf einem VMware Server oder eine physikalische Maschine sein. Dies macht Sinn, wenn Sie zum Beispiel die dedizierte Maschine eines Anwenders physikalisch absichern und diese in den Serverraum verlagern möchten, aber eine Virtualisierung des Desktops aus Performancegründen nicht in Frage kommt.

Die Installation gestaltet sich ebenfalls sehr einfach: *VMware-viewagent-{xxx}.exe* ausführen und die Lizenzbestimmungen akzeptieren, Optionen auswählen und "Install" anklicken. Die Optionen selbst haben folgende Bedeutung:

- VDM Secure Authentication: Ermöglicht Single-Sign-On, das heißt sobald man sich am View Client angemeldet und einen Desktop Pool ausgewählt hat, wird man automatisch am System angemeldet. Beachten Sie, dass dabei die Datei *gina.dll* des Betriebssystems durch eine eigene ersetzt wird. Unter "HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows NT \ CurrentVersion \ Winlogon \ Gina" können Sie sehen, welche DLL verwendet wird.
- USB Redirection: Diese Funktion wird benötigt, wenn Sie lokal angeschlossene Geräte am Remote Desktop benutzen möchten. Dies können Sie mit Hilfe einer Policy auch wieder verbieten, so dass eine Installation nicht schadet. Unter Windows 2000 wird USB-Redirection nicht unterstützt.
- Virtual Printing: Erleichtert das Drucken der Clients auf lokal angeschlossenen Druckern, da nur ein genereller Treiber benötigt wird.

Falls auf der Maschine noch kein Remote Desktop aktiviert ist, fragt der Installer nach, ob er es aktivieren soll. Dies müssen Sie mit "JA" beantworten. Sofern nichts dagegen spricht, sollten Sie alle Optionen installieren, besonders wenn später die Maschine in ein Template für die automatische Desktoperstellung kopiert wird. Sonst müssen Sie später alle Schritte zur Erstellung einer Maschine und Generierung eines Templates wiederholen.

Besitzt die Maschine mehrere Netzwerkkarten, müssen Sie in der Registry noch unter "HKEY_LOCAL_MACHINE \ Software \ VMware, Inc. \ VMwareVDM \ Node Manager \ subnet = {n.n.n.n/m}" (REG_SZ) eintragen, wobei {n.n.n.n} der TCP/IP-Maske entspricht und Sie für "m" die Subnetzmaske einfügen, die der Agent an den VCS für die RDP Verbindung melden soll.

Damit beenden wir unseren ersten Teil. Im zweiten Teil erfahren Sie, wie Sie das Portal und den View Client installieren und Desktop-Pools erstellen. (dr) 

Andreas Badur und Dr. Jürgen Fechter arbeiten für den IT-Dienstleister science + computing ag.

Intensivseminar IT-SECURITY in München

27. bis 29. November 2009

In dem 3-tägigen Workshop demonstrieren wir Ihnen die Verwundbarkeiten von IT-Systemen und die Methoden der Hacker. Dabei liegt der Schwerpunkt auf der Praxis – Sie werden richtig hacken.

Diese Hacker-Techniken werden behandelt:

- > Sniffing-Techniken zum Abhören von Datenströmen
- > Knacken von Passwörtern
- > Scanning, das Ausspionieren offener und nutzbarer Ressourcen
- > Denial of Service-Attacken
- > Ausnützen von Puffer-Überläufen
- > Angriffe über manipulierte www-Seiten
- > Installieren von Rootkits

Anhand dieser Angriffe, die alle in einem abgeschotteten Testnetzwerk stattfinden, werden effektive Sicherheitsmaßnahmen entwickelt.

Der Workshop wendet sich an Netzwerkadministratoren und IT-Sicherheitsverantwortliche in Unternehmen.

Das Training ist keine Anleitung zum Hacken, sondern dient allein der Aufklärung und dem Schutz firmeninterner Netzwerke.

Termin: 27. bis 29.11.2009

Ort: GeNUA, Domagkstraße 7,
85551 Kirchheim bei München

Uhrzeit: jeweils 9.00 bis ca. 17.00 Uhr

IT-Administrator Trainings-Partner

GeNUA

Teilnahmegebühren:

Für ITANet-Mitglieder bzw.

IT-Administrator-Abonnenten: € 1.245,- zzgl. 19 % MwSt.

Für Nichtabonnenten: € 1.395,- zzgl. 19 % MwSt.

Anmeldeschluss: 16.10.2009

 **Bei Anmeldung bis 14. August erhalten Sie einen Frühbucher-Preisnachlass von € 100**

Mehr Infos und ein Bestellformular finden Sie unter
www.it-administrator.de/workshops/



MySQL-Datenbankmanagement mit phpMyAdmin

Herr der Daten

von Dr. Holger Reibold

MySQL ist zwar kostenlos, aber in der Regel alles andere als ein benutzerfreundlicher Datenbankserver. Beim täglichen Umgang mit MySQL-Datenbanken ist es lästig, auf die Server-eigenen Tools zurückzugreifen. Dank phpMyAdmin vereinfacht sich die Arbeit deutlich. Das Werkzeug ermöglicht die Datenbankverwaltung via Browser. IT-Administrator zeigt in diesem Workshop, wie Sie das Tool optimal einsetzen.

Das mit Abstand benutzerfreundlichste und leistungsfähigste Werkzeug für die Verwaltung von MySQL-Servern ist phpMyAdmin [1]. Nicht nur, wenn Sie lokal mit MySQL-Datenbanken hantieren, sondern gerade beim Betrieb einer typischen Web-Anwendung macht phpMyAdmin eine hervorragende Figur. Mit dem Werkzeug lassen sich MySQL-Datenbanken einfach und schnell per HTTP mit einem Browser ansprechen, ohne auf komplizierte SQL-Befehle zurückgreifen zu müssen. Das Tool unterstützt Sie etwa beim Erzeugen und Löschen von Datenbanken sowie beim Erstellen und Bearbeiten von Tabellen. Dabei führen Sie über phpMyAdmin bequem SQL-Statements aus – auch im Batch-Modus. Eine integrierte Benutzerverwaltung erlaubt zudem eine detaillierte Zugriffssteuerung. Weitere Highlights sind die umfangreichen Exportfunktionen: Sie können Ihre Daten in die Formate CSV, Word, Excel, XML und PDF exportieren. Inzwischen hat phpMyAdmin einen derart hohen Reifegrad erreicht, dass es von Version zu Version fast nur noch kleinere Verbesserungen gibt.

phpMyAdmin in Betrieb nehmen

Die wenigen Systemvoraussetzungen erfüllt in der Regel jede Standardumgebung. Um mit der deutschsprachigen Variante der Lösung zu arbeiten, laden Sie sich die Version mit dem Zusatz “all-languages” von der Projekt-Site herunter, entpacken das Archiv und kopieren es in das Dokumentenverzeichnis Ihres Webservers. So-



Bild 1: Ein erster Blick auf die aktuelle phpMyAdmin-3.1.3-Installation

fern Sie über eine fertige Umgebung wie XAMPP verfügen, können Sie direkt mit der Arbeit an Ihren Tabellen loslegen. Falls nicht, müssen Sie phpMyAdmin erst für das Zusammenspiel mit dem Datenbankserver konfigurieren. Dazu können Sie zwei Wege einschlagen:

- Sie bearbeiten die Konfigurationsdatei `config.inc.php` manuell.
- Sie greifen zum Setup-Assistenten, der Sie bei der Konfiguration unterstützt.

Die Konfigurationsdatei sucht phpMyAdmin standardmäßig im gleichen Ordner, in dem Sie auch die Index-Seite `index.php` finden. Darüber hinaus gibt es noch eine weitere wichtige Datei: `layout.inc.php`. Mit dieser bestimmen Sie das Layout von phpMyAdmin. Um das Zusammenspiel mit dem MySQL-Server einzurichten, rufen Sie den Setup-Assistenten auf. Dazu star-

ten Sie Ihren Standardbrowser und öffnen die URL `http://{Hostname oder IP-Adresse des Servers}/phpmyadmin/setup/`. Der Setup-Assistent begleitet Sie dann durch die verschiedenen Schritte. Im linken Bereich sehen Sie die notwendigen Punkte “Overview”, “Features”, “Navigation frame”, “Main frame”, “Importieren” und “Exportieren”.

Zunächst müssen Sie sich vermutlich mit einigen Fehlermeldungen herumschlagen. Im Kopfbereich der ersten Seite finden Sie ein Auswahlménü, das Ihnen die Anpassung der Sprache erlaubt. Verwenden Sie der Einfachheit halber am besten die deutschsprachige Benutzerführung. Außerdem werden Sie – immer abhängig von der jeweiligen Umgebung – mit weiteren Fehlermeldungen konfrontiert: So mahnt das Setup womöglich das Fehlen einer Kompressions-



Bild 2: Der phpMyAdmin-Setup-Assistent greift Ihnen beim Einrichten der Umgebung unter die Arme

komponente, eine unsichere Verbindung und das Erzwingen einer SSL-gesicherten Verbindung an. In jedem Fall müssen Sie sich mit folgender Fehlermeldung auseinandersetzen: “Cannot load and save configuration”. Das Setupskript sichert die neue Konfigurationsdatei `config.inc.php` im Verzeichnis `config` der phpMyAdmin-Installation. Mit hoher Wahrscheinlichkeit existiert dieses Verzeichnis noch nicht in Ihrer Umgebung und muss erst angelegt werden. Erzeugen Sie das Verzeichnis und versehen Sie es mit den notwendigen Lese- und Schreibrechten. Unter Linux führen Sie dazu folgende Kommandos aus:

```
cd phpMyAdmin
mkdir config
chmod 777 config
```

Damit ist die Umgebung für das Erstellen eines neuen Servers vorbereitet. Wenn Sie die Rechte des config-Verzeichnisses mit einem FTP-Client anpassen, so weisen Sie ihm vollen Lese- und Schreibzugriff zu.

Basiskonfiguration

Als Nächstes gilt es, verschiedene allgemeine Eigenschaften der Konfigurationsdatei festzulegen. Dazu stehen Ihnen drei Auswahlmenüs zur Verfügung:

- “Default language”: Hier bestimmen Sie die Standardsprache.
- “Default server”: Hier legen Sie den Standardserver fest.

- “End of line”: Bestimmen Sie, mit welchen Zeichen der Zeilenumbruch gesteuert wird. Bei Linux-Systemen ist das “\n”, bei Windows-Rechnern “\r\n”.

Mit einem Klick auf die Schaltfläche “New Server” erzeugen Sie nun eine neue Konfiguration. Konkret stehen Ihnen auf der zugehörigen Seite vier Register für die Konfiguration des Zusammenspiels von phpMyAdmin und MySQL zur Verfügung: “Basic settings”, “Signon login options”, “Server configuration” und “PMA database”. Sie landen automatisch auf dem Register “Basic settings”, auf dem eine Fülle an

Einstellungen auf Sie warten. Zu jeder Konfiguration finden Sie am Ende der Konfigurationsbeschreibung einen Fragezeichen- und einen Info-Button. Ein Klick auf das Fragezeichen öffnet die Beschreibung der offiziellen Dokumentation, ein Klick auf den Info-Button den zugehörigen Wiki-Eintrag.

Auf dem Register “Basic settings” nehmen Sie die allgemeinen Verbindungseinstellungen zum MySQL-Server vor. Die erste wichtige Einstellung fällt im Eingabefeld “Server hostname” an. Hier geben Sie den Hostnamen oder die IP-Adresse an, unter welcher der MySQL-Server zu erreichen ist. Wenn Sie MySQL und phpMyAdmin auf dem gleichen System ausführen, können Sie den Eintrag “localhost” beibehalten. Sie sollten außerdem die Option “Use SSL” aktivieren, um die Verbindung zwischen phpMyAdmin und dem MySQL-Server zu schützen. Das empfiehlt sich zumindest dann, wenn Sie beide auf unterschiedlichen Rechnern ausführen und der Datenverkehr prinzipiell abgehört werden könnte. Als Authentifizierungstyp empfiehlt sich im Auswahlménü “Authentication type” die Verwendung der Option “Cookie”. Regeln sollten Sie außerdem den Benutzernamen und das Passwort für den Zugriff in den beiden dafür vorgesehenen Eingabefeldern.

Bild 3: Die Datenbankliste in der sogenannten Server-Ansicht



Auf dem Register "Signon session name" können Sie eine Session-Bezeichnung sowie die URL für das Ein- und Ausloggen angeben. Über diese beiden Felder geben Sie etwa alternative URLs an, zu der User beim Einloggen sowie nach dem Logout umgeleitet werden. Wichtig dabei ist die Verwendung einer absoluten URL und des Protokolls. Sie können das Login beispielsweise auf http://www.mein_mysql-server.de/userlogin/login.php umleiten.

Wenn Sie phpMyAdmin produktiv einsetzen wollen, so gilt es, alle möglichen Sicherheitsmechanismen auszuloten und gegebenenfalls zu aktivieren. Es bieten sich mehrere Schutzmechanismen an. Neben Apache-spezifischen Funktionen können Sie die Sicherheit auch mit phpMyAdmin-Einstellungen optimieren.

Die phpMyAdmin-Konfigurationsdatei bietet Möglichkeiten, den Zugriff zu beschränken. Hierfür verwenden Sie den Konfigurationsabschnitt

```
$cfg['Servers'][$i]['AllowDeny'] = 'rules'
```

Mit der Standardkonfiguration wird keine Einschränkung definiert. Wenn Sie den Zugriff für Benutzer und IP-Adressen steuern wollen, bedienen Sie bestimmte Regeln, die in `array()` zusammengefasst werden. Hier ein Beispiel:

```
$cfg['Servers'][$i]['AllowDeny'] = 'rules' =
array('allow Peter from 192.168.0.11',
      'allow Klaus from all');
```

Bei voranstehender Beispielkonfiguration wird dem Benutzer Peter der Zugriff vom System mit der IP-Adresse 192.168.0.11 und dem Benutzer Klaus von allen beliebigen Systemen erlaubt. Ein "deny" verhindert den Zugriff dagegen. Es gibt zwei weitere Schutzmechanismen. So können Sie eine Datenbank gezielt in der Datenbankliste der Web-Schnittstelle ausblenden. Dazu nutzen Sie den Parameter "only_db":

```
$cfg['Servers'][$i]['only_db'] = '';
```

Soll lediglich die Datenbank1 in der Liste aufgeführt werden, so verwenden Sie folgende Konfiguration:

```
$cfg['Servers'][$i]['only_db'] = 'datenbank1';
```

Auch die Verwendung von Platzhaltern ist möglich. Die Einstellungen gelten übrigens für alle Benutzer einer Server-spezifischen Konfiguration.

Mehr Sicherheit für phpMyAdmin



Das Register "Server Configuration" erlaubt die Anpassung verschiedener erweiterter Einstellungen. Sie können beispielsweise die Ansicht auf Seiten von phpMyAdmin auf bestimmte Datenbanken beschränken. Dazu tragen Sie diese einfach in das Textfeld "Show only listed databases" ein. Über das Eingabefeld "Hide databases" verstecken Sie sogar bestimmte Datenbanken. Mit dem Register PMA database konfigurieren Sie schließlich die phpMyAdmin-Datenbank, über die Sie Zugriff auf weitere Funktionen haben. Das Tolle an der phpMyAdmin-Konfiguration: Sie können quasi beliebig viele Server-Konfigurationen anlegen, wenn Sie nicht nur für einen, sondern für mehrere Server zuständig sind.

Mit phpMyAdmin arbeiten

Nachdem Sie phpMyAdmin für das Zusammenspiel mit einem oder auch mehreren MySQL-Servern konfiguriert haben, können Sie sich an die Arbeit mit Ihren Datenbanken machen. phpMyAdmin besitzt eine übersichtlich strukturierte Schnittstelle, über die Sie alle typischen Aktionen beim Umgang mit Datenbanken steuern. Die Web-Schnittstelle des Datenbankmanagers ist zweigeteilt: Links die Navigationsleiste, rechts die dazugehörigen Einstellungen und Funktionen.

phpMyAdmin stellt Ihnen verschiedene Ansichten für das Arbeiten mit Ihren Daten zur Verfügung. Zwei wichtige Ansichten sind die Datenbank- und die Tabellenansicht. Die Datenbanksicht öffnen Sie, indem Sie in der Navigationsleiste eine Datenbank auswählen. Diese Ansicht weist die typischen Details und Funktionen von Datenbanken auf. Sie können beispielsweise die bestehenden Tabellen einsehen, die Struktursicht öffnen, Tabellen erstellen, SQL-Befehle auf die Datenbank anwenden oder Inhalte gezielt exportieren. Die sogenannte Tabellenansicht öffnen Sie, indem Sie eine Datenbank und eine Tabelle in der Navigationsleiste auswählen. Alternativ wählen Sie in der Datenbanksicht eine Tabelle auf dem Register Struktur aus und klicken auf die Schaltfläche Ansicht in der gewünschten Tabellenzeile.

In der Spalte "Aktion" führen Sie typische Tabellenaktionen durch. phpMyAdmin stellt Ihnen außerdem die sogenannte Server-Ansicht zur Verfügung. Diese öffnen Sie, indem Sie auf der Homepage der lokalen phpMyAdmin-Installation auf "Datenbanken" klicken. Hier finden Sie die verschiedenen Datenbanken aufgeführt. Am Ende jeder Datenbankspalte sehen Sie ein Icon, über das Sie die Rechte für die jeweilige Ablage überprüfen können. Ein

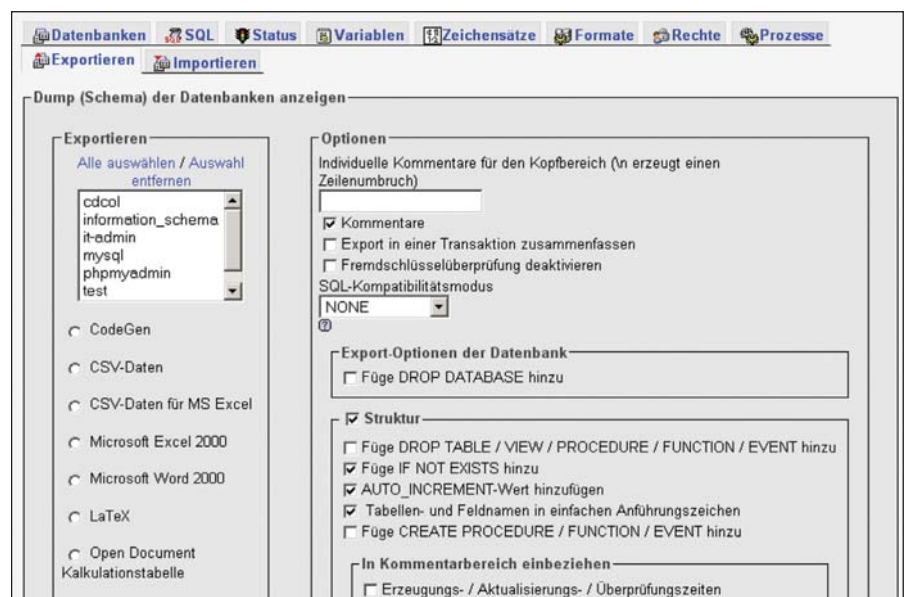


Bild 4: Die Exportfunktionen von phpMyAdmin haben es in sich: Besonders für den Export nach SQL stehen Ihnen vielfältige Optionen zur Verfügung



Neuen Benutzer hinzufügen

Anmelde-Informationen

Benutzername: Textfeld verwenden: admin

Host: Textfeld verwenden: testserver

Passwort: Textfeld verwenden:

Wiederholen:

Passwort generieren:

Datenbank für Benutzer

☒ Keine

☐ Erstelle eine Datenbank mit gleichem Namen und gewähre alle Rechte

☐ Gewähre alle Rechte auf Datenbanken die mit dem Benutzernamen beginnen (username_%)

Globale Rechte (Alle auswählen / Auswahl entfernen)

MySQL-Rechte werden auf Englisch angegeben.

Daten	Struktur	Administration
☒ SELECT	☒ CREATE	☒ GRANT
☒ INSERT	☒ ALTER	☒ SUPER
☒ UPDATE	☒ INDEX	☒ PROCESS
☒ DELETE	☒ DROP	☒ RELOAD
☒ FILE	☒ CREATE TEMPORARY TABLES	☒ SHUTDOWN

Bild 5: Die Benutzerverwaltung des Datenbankmanagers erlaubt die exakte Steuerung der Benutzerrechte

Klick prüft die Rechte und die Benutzer, deren Rechte und erlaubt das Bearbeiten der Einstellungen. Die Server-Ansicht führt die einzelnen Datenbanken auf und erlaubt das Prüfen – und auch Bearbeiten – der Datenbankberechtigungen.

Datenbanken anlegen und verwalten

Zu den typischen Aufgaben im Umgang mit MySQL-Datenbanken gehört das Erstellen und Bearbeiten von Datenbanken und Tabellen. Aber auch Aktionen wie

das Bearbeiten der Datenbankstruktur und das Importieren von Datenbeständen gehören zu den gängigen Aktionen. Um eine neue Datenbank anzulegen, müssen Sie normalerweise den SQL-Befehl `CREATE DATABASE {Datenbankbezeichnung}` ausführen. Mit phpMyAdmin ist das deutlich einfacher: Hier geben Sie auf der phpMyAdmin-Startseite im Bereich "Actions" in das Eingabefeld "Neue Datenbank anlegen" die Datenbankbezeichnung ein und bestätigen mit

"Anlegen". Sie landen automatisch auf dem Dialog für das Anlegen von Tabellen. Dort weisen Sie der ersten Tabelle ebenfalls eine Bezeichnung und die Anzahl der Felder zu. Um die zuvor erzeugte Tabelle mit Daten zu füllen, wechseln Sie zum Register "Einfügen". Dort stehen standardmäßig zwei Eingabeblocks zur Verfügung, über die Sie die Datenbank manuell mit Daten füttern können. Dass es sich um zwei Blöcke handelt, liegt an der Standardeinstellung der Konfigurationsdatei. Die Option "`$cfg['InsertRow']`" ist für diese Einstellung zuständig und ist standardmäßig auf "2" gesetzt.

Auch die Bearbeitung der Datenbankstruktur, genauer der Tabellenstruktur, wird mit phpMyAdmin fast zum Kinderspiel. Hierfür greifen Sie zur Strukturansicht. Um eine oder auch mehrere neue Zeilen einzufügen, geben Sie unter Felder hinzufügen die gewünschte Anzahl an. phpMyAdmin geht standardmäßig davon aus, dass die neuen Zeilen am Ende der Tabelle angefügt werden. Daher ist auch die Option "An das Ende der Tabelle" aktiv. Möchten Sie die neue Zeile an den Anfang setzen, aktivieren Sie die Option "An den Anfang der Tabelle". Die neue Zeile erzeugen Sie nun durch einen Klick auf "OK", sie landet anschließend an der gewünschten Position. Sollen die neuen Felder nicht untereinander, sondern nebeneinander angeordnet werden, müssen Sie einmal mehr die phpMyAdmin-Konfigurationsdatei anpassen. Dort finden Sie zwei relevante Einstellungen:



Lesen Sie den IT-Administrator als E-Paper

Testen Sie kostenlos und unverbindlich die elektronische IT-Administrator Leseprobe auf www.it-administrator.de.

Wann immer Sie möchten und wo immer Sie sich gerade befinden – Volltextsuche, Zoomfunktion und alle Verlinkungen inklusive. Klicken Sie sich ab heute mit dem IT-Administrator einfach von Seite zu Seite, von Rubrik zu Rubrik!

Infos zu E-Abos, E-Einzelheften und Kombiangeboten finden Sie auf:

www.it-administrator.de/magazin/epaper





```
$cfg['DefaultDisplay'] = 'horizontal'
$cfg['DefaultPropDisplay'] = 'horizontal'
```

Import und Export mit phpMyAdmin

phpMyAdmin ist sowohl für den Import wie auch den Export von Daten und Strukturen gerüstet. Sie können mithilfe des Datenbankmanagers erstellte Datenbanken bequem auf anderen Rechnern sichern, diese mit anderen Anwendern austauschen oder auch bestehende Datensätze

phpMyAdmin speichert die Einstellungen des Setups in der Datei `config.inc.php` des neu angelegten config-Verzeichnisses. Diese sieht bei einer ganz einfachen Konfiguration beispielsweise wie folgt aus:

```
<?php
/*
 * Generated configuration file
 * Generated by: phpMyAdmin 3.1.3 setup script by
 * Piotr Przybylski <piotrprz@gmail.com>
 * Date: Sun, 26 Apr 2009 12:00:00 +0200
 */

/* Servers configuration */
$i = 0;

/* Server: localhost1 [1] */
$i++;
$cfg['Servers'][$i]['verbose'] = '';
$cfg['Servers'][$i]['host'] = 'localhost';
$cfg['Servers'][$i]['port'] = '';
$cfg['Servers'][$i]['socket'] = '';
$cfg['Servers'][$i]['connect_type'] = 'tcp';
$cfg['Servers'][$i]['extension'] = 'mysqli';
$cfg['Servers'][$i]['auth_type'] = 'cookie';
$cfg['Servers'][$i]['user'] = 'root';
$cfg['Servers'][$i]['password'] = '';

/* Server: localhost2 [2] */
$i++;
$cfg['Servers'][$i]['verbose'] = '';
$cfg['Servers'][$i]['host'] = 'localhost2';
$cfg['Servers'][$i]['port'] = '';
$cfg['Servers'][$i]['socket'] = '';
$cfg['Servers'][$i]['connect_type'] = 'tcp';
$cfg['Servers'][$i]['extension'] = 'mysqli';
$cfg['Servers'][$i]['auth_type'] = 'cookie';
$cfg['Servers'][$i]['user'] = 'root';
$cfg['Servers'][$i]['password'] = '';

/* End of servers configuration */

$cfg['blowfish_secret'] =
    '49d865d5cdf93.43199824';
$cfg['defaultlang'] = 'en-utf-8';
$cfg['serverdefault'] = 0;
$cfg['upload_dir'] = '';
$cfg['save_dir'] = '';
?>
```

Wenn Sie mit den Eigenheiten der phpMyAdmin-Konfigurationsdatei vertraut sind, können Sie hier eine Vielzahl an Einstellungen anpassen.

Listing: Die phpMyAdmin-Konfigurationsdatei



nutzbar machen. Und dank der umfangreichen Import- und Exportfunktionen sind MySQL und phpMyAdmin bestens für das Zusammenspiel mit anderen Anwendungen gerüstet. Insbesondere die Exportfunktionen haben es in sich.

Die Importfunktionen sind recht beschränkt. Mithilfe von phpMyAdmin können Sie zwei Formate in eine MySQL-Datenbank importieren: SQL- und CSV-Dateien. Um bestehende SQL-Daten in eine bestehende oder auch leere Datenbank zu importieren, öffnen Sie die gewünschte Datenbank, wechseln zum Register "Importieren", wählen die Datei aus, bestimmen das Format und führen den Import mit einem Klick auf "OK" aus.

Weitaus umfangreicher sind die Exportfunktionen. Diese sind über das Register "Exportieren" zugänglich, das in allen Ansichten verfügbar ist. Bevor Sie sich an den Export von Daten machen, sollten Sie zunächst verschiedene Punkte klären:

- Soll die gesamte Datenbank oder nur bestimmte Tabellen exportiert werden?
- Soll lediglich die Struktur, nur die Daten oder doch beides exportiert werden oder ist lediglich ein Daten-Subset gefragt?

Die Handhabung der Exportfunktion ist ansonsten einfach. Bestimmen Sie im Bereich "Exportieren" die zu exportierende Datenbank und unterhalb des Auswahlmenüs das Zielformat. Rechts finden Sie – abhängig vom gewählten Exportformat – die Optionen. Beim Export nach SQL können Sie beispielsweise die Zielstruktur anpassen.

Benutzerverwaltung

Die wichtigste administrative Aufgabe ist die Benutzerverwaltung, die über den Link "Rechte" verfügbar ist. Dabei übernimmt das MySQL-Berechtigungssystem eine zentrale Aufgabe: Es stellt sicher, dass alle Benutzer nur genau die Aktionen durchführen dürfen, zu denen sie berechtigt sind. Stellen Sie mit phpMyAdmin die Verbindung mit einem MySQL-Server her, wird die Benutzeridentität durch den Host, von

dem aus der Zugriff erfolgt, sowie dem angegebenen Benutzernamen festgelegt. Das System gewährt Berechtigungen gemäß dieser Informationen. Dabei zieht MySQL sowohl Hostnamen als auch Benutzernamen heran, um den Anwender zu identifizieren. Die MySQL-Zugriffskontrolle läuft in zwei Phasen ab:

- Phase 1: Der Server prüft, ob der Anwender das Recht besitzt, sich mit diesem verbinden zu können.
- Phase 2: Verfügt der Anwender über das Recht, sich zu verbinden, überprüft der Server jede Anfrage, die man durchführt, um festzustellen, ob man die erforderliche Rechte besitzt, um diese auszuführen. Will der Anwender beispielsweise eine Tabelle in einer Datenbank löschen, stellt der Server sicher, dass der Anwender die SELECT-Berechtigung für die Tabelle bzw. die DROP-TABLE-Berechtigung für die Datenbank besitzt.

Die Benutzerverwaltung führt in der so genannten Benutzerübersicht zunächst einmal die bestehenden User samt Host, Kennwort, globalen Rechten sowie die Vererbung auf. Über das Stiftsymbol am Ende einer jeden Benutzerzeile können Sie die Einträge bearbeiten und exakt steuern, auf welche Daten und Strukturen der Zugriff möglich ist und welche administrativen Berechtigungen für einen Benutzer gelten.

Fazit

Mit phpMyAdmin wird die Verwaltung von MySQL-Servern und -Datenbanken zum Kinderspiel. Kein Wunder, denn das Tool kann auf eine lange Entwicklungsphase zurückblicken. phpMyAdmin bietet alles, was Sie für die tägliche Arbeit benötigen. Einfach zu handhaben ist es zudem. Damit ist pnpMyAdmin ein Must-have-Werkzeug für jeden Datenbankadministrator. (dr)

[1] Projektseite von phpMyAdmin
www.phpmyadmin.net

Links



Exchange Server

Öffentliche Ordner migrieren

von Robert Lindermeier

Mit der Einführung einer neuen Version des Exchange Servers nutzen viele Administratoren die Möglichkeit, "Altlasten" über Bord zu werfen und eine vollständig neue, an die aktuellen Erfordernisse angepasste Active Directory Domäne einzuführen. Damit einher geht natürlich ein gewisser Mehraufwand, denn nun müssen neben den Postfächern und sonstigen Einstellungen die vielfach immer noch gerne genutzten Öffentlichen Ordner in die neue Exchange-Organisation migriert werden. Insbesondere das Migrieren der Berechtigungen stellt oftmals einen enormen Aufwand dar. Zwei Tools von Microsoft bieten jedoch entscheidende Dienste hierfür an: Das InterOrg-Replikation-Tool [1] zur Replikation der Inhalte der Öffentlichen Ordner und PFDAdmin [2], um die Berechtigungen in der Altdomäne zu exportieren und zu migrieren. Auch wenn es nicht explizit angegeben ist, so können Sie doch beide Tools auch mit Exchange Server 2007 verwenden.

Im ersten Schritt richten Sie nun die Replikation der Öffentlichen Ordner aus der bestehenden Exchange-Organisation hin zur neuen Organisation ein. Nachdem Sie das Tool auf dem Zielsystem entpackt haben, finden Sie zwei ausführbare Dateien vor. Das ist einmal die *exscfg.exe*, mit der Sie die Interorg-Replikation konfigurieren und zum anderen die *exsrv.exe*, mit der die eigentliche Replikation gestartet wird. Wir starten im ersten Schritt die Konfiguration mit *exscfg.exe*. Über "Session / Add" fügen Sie die Public Folder Replication hinzu (siehe Bild 1).

Die meisten Angaben sind relativ logisch. Sie sollten allerdings darauf achten, dass das angegebene Postfach auch entspre-

chende Zugriffsrechte auf die Öffentlichen Ordner hat. Am besten benutzen Sie das Tool PFDAdmin, um einen speziellen Benutzer (hier PFDAdmin) Besitzerrechte an allen Öffentlichen Ordner einzuräumen. Über den Schalter "Advanced" geben Sie die Logindaten des PFDAdmin jeder Domäne an, damit sich das Tool auch korrekt anmelden kann. Sie können jederzeit auf beiden Servern unterschiedliche Konten verwenden, auch wenn die Domänen per Trust verbunden sind.

Im nächsten Schritt konfigurieren Sie nun die zu replizierenden Ordner. Dazu öffnen Sie die "Folder List" und tragen nach dem erfolgreichen Login auf beiden beteiligten Exchange Server (Schaltfläche "Logon") alle gewünschten Quell-Ordner (Publisher) und Zielordner (Subscriber) ein. Bitte beachten Sie, dass das Tool nur in der Lage ist, ab der obersten Ordner-Ebene rekursiv nach unten zu arbeiten und weitere Unterordner anzulegen. Daher müssen Sie im Zielsystem eventuell die benötigten Ordner zuvor erzeugen. Nachdem die Konfiguration abgespeichert ist, können Sie die Replikation mit *exsrv* starten und kontrollieren. Als geübter IT-Administrator kommen Sie damit sicher relativ leicht zurecht.

Um nun die Berechtigungen zu übertra-

Beim Hinzufügen der Public Folder Replication müssen auch die Zugriffsrechte im Hintergrund stimmen

gen, gehen Sie wie folgt vor: Exportieren Sie in der Quellumgebung mit PFDAdmin alle Berechtigungen (NT-Konten) in eine Datei. Bearbeiten Sie nun diese Datei und passen Sie sie auf die migrierten Konten an (NetBIOS-Name der Zieldomäne). Importieren Sie schließlich die neuen Berechtigungen in die neue Umgebung. Wurden zuvor alle Konten und Gruppen/Verteilerlisten per ADMT migriert, steht der Nutzung nun nichts mehr Wege. (dr)

[1] InterOrg Replikation

www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=e7a951d7-1559-4f8fb400-488b0c52430e

[2] PFDAdmin

www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=635be792-d8ad-49e3-ada4-e2422c0ab424

Links





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.



Zur **Verteilung von Updates** auf die Clients verwenden wir in unserem Netzwerk die Windows Server Update Services (WSUS). Nachdem sich am Server selbst ja konfigurieren lässt, in welchen Intervallen der Update-Dienst von Microsoft über das Internet kontaktiert werden soll, ist mir nicht so ganz klar, wann und wie häufig sich denn nun die einzelnen **Clients mit WSUS in Verbindung setzen**, um die für sie passenden Updates abzuholen. Gibt es denn irgendeine Möglichkeit, das Aufspielen sämtlicher erforderlicher Updates auf einem Client zu erzwingen?

Wann ein Client sich im lokalen Netzwerk mit WSUS verbindet, kann tatsächlich schlecht vorhergesagt oder gar fest eingestellt werden. Unter anderem sorgt der auf dem Client laufende Dienst "BITS" (Background Intelligent Transfer Service) dafür, dass nur dann Aktualisierungen übertragen werden, wenn die Bandbreite des Netzwerks es zulässt. Es gibt jedoch eine Möglichkeit, auf dem Client die sofortige Versorgung mit allen nötigen Updates zu erzwingen. Geben Sie dazu in der Kommandozeile `wuauclt.exe /detectnow`

ein. Der Rechner setzt sich nun sofort mit WSUS in Verbindung und überprüft den derzeitigen Aktualisierungsstand und lädt eventuelle Updates herunter. In seltenen Fällen führt jedoch auch dieser Befehl nicht zum Erfolg. Fügen Sie dem Kommando dann ein weiteres Attribut hinzu. Mit `wuauclt.exe /resetauthorization /detectnow`

löschen Sie ein eventuell auf dem Client vorhandenes Cookie, das nach dem letzten Update vom WSUS gesetzt wurde. Spätestens jetzt sollte das sofortige Update funktionieren. Der beschriebene Befehl lässt sich auf allen Windows-Rechnern ab Windows 2000 SP3 einsetzen. (In)

Bei Wartungsarbeiten an Clients und Servern ist es mir sehr wichtig, im **Windows-Explorer** sowohl die versteckten Dateien als auch die **vollständige Dateieindung angezeigt** zu bekommen. Das langwierige Hangeln durch das entsprechende Menü empfinde ich aber als sehr umständlich. Kann ich diese Grundeinstellungen nicht irgendwo schneller ändern?

Sie haben die Möglichkeit, durch Änderungen in der Registry auch ohne langwierige Menüeingaben zum gewünschten Ergebnis zu kommen. Nach der Eingabe von `regedit` bewegen Sie sich in der Registrierungsda-

tenbank zum Verzeichnis `HKEY_CURRENT_USER / Software / Microsoft / Windows / CurrentVersion / Explorer / Advanced` und klicken dort auf den Eintrag "Hidden". Ändern Sie dessen Wert auf "1", zeigt der Explorer in Zukunft stets die versteckten Dateien an. Um auch verborgene Systemdateien immer sichtbar zu machen, setzen Sie den Wert des Parameters "ShowSuperHidden" auf "1". Für die standardmäßige Anzeige der vollständigen Dateieindung verändern Sie den Eintrag "Hide FileExt", hier muss dessen Wert allerdings auf "0" gesetzt werden. Beachten Sie, dass Sie den Windows Explorer nach sämtlichen Änderungen neu starten beziehungsweise aktualisieren müssen, damit die Änderungen sichtbar werden. (In)

Einige unserer Mitarbeiter müssen ab und zu auf einen **Telnet-Server zugreifen**. Zumindest unter Windows XP können sich aber **nur als Administrator** angemeldete Nutzer mit einem Telnet-Server verbinden. Wie kann ich für normale Anwender einen **Telnet-Zugang einrichten**?

Außer Administratoren gestattet Windows XP nur den Mitgliedern der Benutzergruppe "TelnetClients", sich mit einem Telnet-Server zu verbinden. Da diese Gruppe standardmäßig nicht vor-

handen ist, müssen Sie diese in der Systemsteuerung unter "Verwaltung / Computer" erst anlegen. Alle Benutzer, die Sie nun über die Benutzerverwaltung dieser Gruppe hinzufügen, können ab sofort von ihrem Rechner aus einen Telnet-Server kontaktieren. Bitte beachten Sie, dass Sie die Benutzergruppe mit der genauen Bezeichnung, wie oben angegeben, hinterlegen müssen, auch was die Groß- und Kleinschreibung betrifft. (ln)



Apple

Per AFP verbinde ich mich des Öfteren als Administrator auf einen Dateiserver. Dieser zeigt mir allerdings nur die eingerichteten Share Points an. Lieber wäre es mir, wenn ich stattdessen Zugriff auf die tatsächlichen Volumes hätte. Gibt es hier einen Weg, um die Ansicht anzupassen?

Seit OS X 10.3 werden bei einer AFP-Verbindung zu einem Server nur noch die Share Points dargestellt. Um dies zu ändern und die wirklichen Volumes angezeigt zu bekommen, geben Sie im Terminal-Modus das Kommando

```
sudo serveradmin settings afp:admin31GetSp = no
```

und bestätigen Sie die Änderung mit Ihrem Admin-Passwort. Sollten Sie es sich wieder einmal anders überlegen, können Sie die Einstellung mit dem Wert "yes" statt "no" am Ende der Befehlskette auch wieder rückgängig machen. Nach jeder Änderung ist ein Neustart von AFP nötig. (ln)

Ich will mir auf einem Apple unter Mac OS X sämtliche offenen Ports anzeigen lassen, dabei aber nicht auf irgendwelche Tools zurückgreifen. Kann ich alle auf das Internet zugreifenden Programme mit Bordmitteln aufspüren?

Auch ohne zusätzliche Werkzeuge können Sie sich auf Apple-Rechnern alle offenen Verbindungen anzeigen lassen. Geben Sie dazu im Terminal den Befehl

```
sudo lsof -n | grep TCP
```

ein und bestätigen Sie diesen mit Ihrem Admin-Kennwort. Sie erhalten daraufhin eine Aufstellung, die Aufschluss über die geöffneten TCP-Verbindungen gibt. Die gleiche Information können Sie sich auch für alle UDP-Übertragungen geben lassen. Ersetzen Sie in der Befehlssyntax dazu einfach "TCP" durch "UDP". (ln)



Google Chrome

Seit einiger Zeit benutze ich Google Chrome als Browser-Alternative. Was ich in den Optionen allerdings vermisste, ist die Möglichkeit, sich eine Liste aller auf dem System installierten Plug-Ins anzeigen zu lassen, die für die Darstellung von Webseiten nötig sind. Verfügt der Browser über eine Möglichkeit, eine dementsprechende Liste auszugeben?

Google Chrome verfügt über einige versteckte Funktionen, die hauptsächlich Informationen über den Systemstatus und den Browser selbst bereitstellen. Um auf diese Aufstellungen zuzugreifen, geben Sie in der Adresszeile von Chrome "about:" ein, unmittelbar gefolgt von einem weiteren Parameter: Mit "plugins" teilt Ihnen der Browser im aktuellen Tab sämtliche installierten Internet-Plug-Ins mit. Dies betrifft auch die für die Konkurrenzprodukte Firefox und Internet Explorer installierten Erweiterungen wie Shockwave Flash oder Silverlight. Mit dem Zusatz "cache" bringen Sie eine Liste aller von Chrome im Cache gelagerten Seiten auf den Schirm. Da der Browser über keine Option verfügt, die Größe des Cache-Speichers zu begrenzen, empfiehlt es sich, diesen von Zeit zu Zeit von Hand zu leeren. Mit "memory" vergleichen Sie den Speicherverbrauch aller aktuell gestarteten Browser und mit "dns" erfahren Sie mehr über die letzten zehn DNS-Vorabrufe, die der Browser zum schnellsten Seitenaufruf getätigt hat. (ln)

Google Chrome verfügt ja über die sogenannte Incognito-Funktion, die weder den Browserverlauf noch beim Surfen abgelegte Cookies speichert. Wie kann ich den Browser so einstellen, dass er automatisch bei jedem Start in diesem Vernebelungs-Modus startet?

Normalerweise können Sie einen neuen Tab, unter dem Sie inkognito surfen können, nach einem Klick auf das durch den Schraubenschlüssel dargestellte Einstellungs-Symbol aktivieren. Schneller geht dies mit der Tastenkombination "Strg+Umschalten+N". Wollen Sie standardmäßig im Incognito-Modus starten, können Sie der Desktop-Verknüpfung zu Google Chrome einfach den Parameter "-incognito" hinzufügen. Der vollständige Verknüpfungs-Pfad muss also "C:\Dokumente und Einstellungen\{Benutzer}\Lokale Einstellungen\Anwendungsdaten\Google\Chrome\Application\chrome.exe" -incognito

lauten. Alternativ können Sie den Browser natürlich auch aus der Kommandozeile heraus mit diesem Zusatz starten, um das Speichern persönlicher Informationen zu verhindern. (ln)



Windows Server ermöglicht die Installation mehrsprachiger Systeme. Lässt sich Citrix XenApp auch in einer mehrsprachigen Windows-Umgebung installieren? Citrix bietet keine mehrsprachige XenApp-Benutzeroberfläche über ein

Viele weitere Tipps & Tricks sowie konkrete Hilfe bei akuten Problemen bekommen Sie auch im Internet bei unserem exklusiven Foren-Partner administrator.de. Fast 50.000 registrierte Benutzer tauschen dort in über 100 Kategorien ihre Erfahrungen aus und leisten Hilfestellung. So wie der IT-Administrator das praxisnahe Fachmagazin für Administratoren ist administrator.de die Internetplattform für alle System- und Netzwerkadministratoren.

www.administrator.de



ADMINISTRATOR | IT-FORUM

zentrales System, wie es spezielle Multisprach-Versionen der Windows Server tun. Diese ermöglichen die Konfiguration mehrerer Sprachen auf der Benutzeroberfläche über ein einziges System. So kann zum Beispiel ein Unternehmen, das die Benutzeroberfläche auf Deutsch, Französisch und Italienisch anbieten möchte, diese drei Sprachen über einen Server bereitstellen. Citrix XenApp 5.0, Presentation Server 4.x, MetaFrame Presentation Server 3.0, MetaFrame XP und MetaFrame 1.8 sind in den fünf Sprachversionen Englisch, Spanisch, Deutsch, Französisch und Japanisch verfügbar. Citrix Presentation Server 4.x und XenApp 5.0 können aber in mehrsprachigen Windows-Umgebung installiert werden und ermöglichen es damit unterschiedlichen Nutzern, sich jeweils mit ihrer Sprache anzumelden – hierfür gibt es auch Support. Citrix unterstützt darüber hinaus die Installation von entsprechenden Produkt-Sprachversionen auf gleichsprachigen Microsoft Betriebssystemen, also beispielsweise ein deutsches XenApp 5 auf einem deutschen Windows Server 2008. (Citrix/ln)



Tools

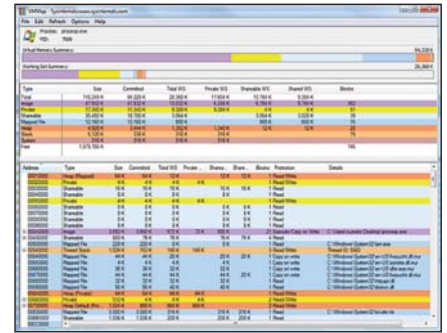
Oft plagen sich Administratoren mit dem Problem, dass sie unter HKEY_USER den **Registry Hive eines bestimmten Benutzers** suchen, ihn aber nicht sofort finden. Ähnlich sieht es bei Fehlermeldungen aus, die lediglich eine SID (Security ID) enthält, aber keinen Hinweis auf den Benutzer, den der Fehler betrifft. Besonders im Terminalserverumfeld, in dem sich viele Benutzer ein System teilen, sind dies zwei häufig anzutreffende Problemstellungen. Denn bei einem Terminal Server können unter HKEY_USER viele Hives existieren, die als Schlüsselnamen nur die SID besitzen. Das Werkzeug **SID2Username** erzeugt auf Knopfdruck den zur SID gehörigen Benutzernamen.

Dieses Tool bestimmt auf komfortable Weise die SID zu einem bestimmten Benutzernamen und umgekehrt. Wenn der Administrator das Programm startet, liest es die Zwischenablage aus und zeigt sofort die gewünschte Information an. Beispielsweise ermöglicht das Werkzeug über einen Rechtsklick in der Registry auf den entsprechenden Schlüssel über den Menüpunkt "Schlüsselnamen kopieren", den entsprechenden Benutzernamen sofort anzuzeigen. Voraussetzung für das Tool ist das .NET Framework 2.0 – administrative Privilegien sind nicht nötig. (jp)



Der Download und zusätzliche Informationen unter <http://blogs.sepago.de/tools/2009/03/11/sid2username/>

IT-Verantwortliche sehen sich oft der Frage gegenüber, welche Anwendungen wie viel RAM verbraucht, um die speicherhungrigen Applikationen oder Dienste zu identifizieren, die beispielsweise gerade den Server in die Knie zwingen. Neben dem Windows-eigenen Task Manager und dem bekannten Process Explorer steht hierfür nun ein weiteres Sysinternals-Tool bereit: VMMap 1.1. Um bei dieser Art der Fehlersuche die richtige Ursache zu ermitteln, erlaubt das kostenlose Werkzeug, für einzelne Prozesse exakt zu analysieren, wie viel physikalischer und virtueller Speicher diese beanspruchen. Mit VMMap lässt sich der physikalische und virtuelle Speicherbedarf von Anwendungen detailliert analysieren und die erfassten Daten als csv- beziehungsweise txt-Datei speichern. Administratoren haben nun über "Show changes" die Möglichkeit, den Speicherbedarf einer Anwendung zu beobachten, etwa vor und nachdem eine bestimmte Funktion ausgeführt wurde. VMMap zeigt dabei die Speichernutzung des beobachteten Programms grafisch an: In einer Balken-



VMMap von Sysinternals kommt Speicherfressern auf die Spur

darstellung verdeutlicht das Tool, wie sich die unterschiedlichen Speicherkategorien im Gesamtspeicher verteilen. Die Darstellung zeigt zudem tabellarisch die Kategorien einzeln auf und ergänzt diese um die detaillierte Speicherbelegung innerhalb der Kategorie. VMMap lässt sich auch über die Kommandozeile starten und so bereits mit dem zu analysierenden Prozess aufrufen. Das Werkzeug steht als 300 KByte kleiner Download zur Verfügung und muss nicht installiert werden. VMMap läuft auf Clients ab Windows XP und auf Servern ab Windows Server 2003. (jp)

Quelle:

<http://download.sysinternals.com/files/vmmap.zip>

Auf der Homepage des IT-Administrator-Magazins stellen wir jede Woche für Sie ein praktisches Tool zum Download bereit. Neben einer Kurzbeschreibung finden Sie Systemvoraussetzungen und alle weiteren wichtigen Informationen auf einen Blick. Und können so gezielt Werkzeuge für Ihren täglichen Administrationsbedarf herunterladen.

www.it-administrator.de/downloads/software/

Download der Woche

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



Enterprise Rights Management Integrierte Dokumenten- sicherheit im Unternehmen

von Dr. Willi Kafitz und Dirk Weissenbacher

Die Zusammenarbeit über Unternehmensgrenzen hinaus kann die Integrität elektronischer Dokumente gefährden. Um solche Informationen vor unbefugter Nutzung zu schützen, ist eine Technologie nützlich, die eigentlich erfunden wurde, um digitale Raubkopien zu verhindern: das Enterprise Rights Management. IT-Administrator zeigt auf, wie Unternehmen Dateien und E-Mails vor unbefugter Weitergabe schützen können.

Die Möglichkeit, Informationen und Texte, die in elektronischer Form vorliegen, ungehindert zu reproduzieren, macht den Umgang mit dem geschriebenen Wort unter Umständen zu einem Sicherheitsproblem. Wenn Mitarbeiter vertraulich gemeinte E-Mails weiterleiten oder Informationen aus sensiblen elektronischen Dokumenten an anderer Stelle veröffentlichen, ist das im harmlosesten Fall ärgerlich. Handelt es sich allerdings um eigene Erfindungen, die plötzlich von der Konkurrenz zum Patent angemeldet werden, wird schnell deutlich, dass unter Umständen der wirtschaftliche Erfolg davon abhängen kann, wie sorgsam mit solchen Dokumenten umgegangen wird.

Organisatorische Maßnahmen mit Technologie unterstützen

Natürlich gibt es organisatorische Maßnahmen und Arbeitsanweisungen für den Umgang mit solchen Dateien – etwa Schutzklassen wie “Nur zum internen Gebrauch”, “Vertraulich” oder “Streng vertraulich”. Falls die Mitarbeiter sich nicht daran halten, erfolgen Appelle an das Sicherheitsbewusstsein oder, auf der nächsten Stufe, arbeitsrechtliche Konsequenzen. Doch damit sind die organisatorischen Mittel zum Schutz von Dokumenten bereits ausgeschöpft.



DRM sollte Musikunternehmen den Kopierschutz digitaler Musik ermöglichen – heute schützt es die Vertraulichkeit von Unternehmensinternas

Deshalb wird auch in technischer Hinsicht einiges für die Datensicherheit unternommen. Virtual Private Networks (VPNs), symmetrische und asymmetrische Verschlüsselung, elektronische Signaturen mit Zertifikaten sind hier nur einige Stichworte, wenn es um sichere Transportwege, codierte E-Mails oder Dokumentenverschlüsselung geht. Aber wie können Unternehmen sich davor schützen, wenn der Empfänger eines Dokumentes die darin enthaltenen In-

formationen nicht im Sinne des Absenders verwendet?

Es gibt tatsächlich eine Technologie, die diese Sicherheitslücke schließen kann: das Digital Rights Management (DRM) wurde zunächst entwickelt, um geistiges Eigentum an Audio- und Videodateien zu schützen und digitale Raubkopien zu verhindern. Doch die Verbraucher, die die gekauften und mit DRM versehenen Produkte nicht nach



ihren Wünschen verwenden konnten und sich deshalb bevormundet fühlten, machten den großen Film- und Musikkonzernen einen Strich durch die Rechnung. Mittlerweile gilt das DRM-Verfahren deshalb als gescheitert.

Neu aufgelegt: der Kopierschutz

Doch die zugrunde liegende Technologie ist viel zu interessant, um sie künftig ungenutzt zu lassen. DRM beginnt deshalb eine neue Karriere in der IT-Sicherheit als Enterprise Rights Management (ERM). Hierbei geht es nun nicht mehr um MP3-Musikstücke oder Hollywood-Filme, die vor unbefugter Nutzung geschützt werden sollen. Stattdessen wird das DRM-Konzept auf Unternehmensdaten angewendet. Die Zielgruppen sind die Beteiligten an einem digitalen Workflow – also Mitarbeiter oder Geschäftspartner, die auf diese Informationen zugreifen oder eben nicht zugreifen dürfen.

Die Funktionsweise ist grundsätzlich folgende: Der Verfasser oder Sender eines Dokuments verknüpft eine Information, die als Datei oder E-Mail vorliegt, mit einer Arbeitsanweisung (Policy). Darin ist festgelegt, wie der berechtigte Empfänger sie verwenden darf. Unberechtigte Benutzer hingegen können die mit ERM geschützten E-Mails oder Dateien nicht lesen, selbst wenn diese über Dritte in deren Besitz gelangen. Zudem lässt sich auch das Drucken, Kopieren oder Weiterleiten verhindern. Auch zeitabhängige Zustände sind möglich, mit denen sich Verfallsdaten oder Versionswechsel erzwingen lassen.

Damit ist eine Information erstmals nicht nur auf dem Transportweg geschützt, sondern es lässt sich darüber hinaus ihre Weiterverarbeitung kontrollieren. Dabei sind natürlich auch hier noch Szenarien denkbar, wie Personen mit krimineller Energie diesen Schutz zu umgehen versuchen. Beispielsweise, indem ein lediglich leseberechtigter Empfänger die Inhalte vom Bildschirm

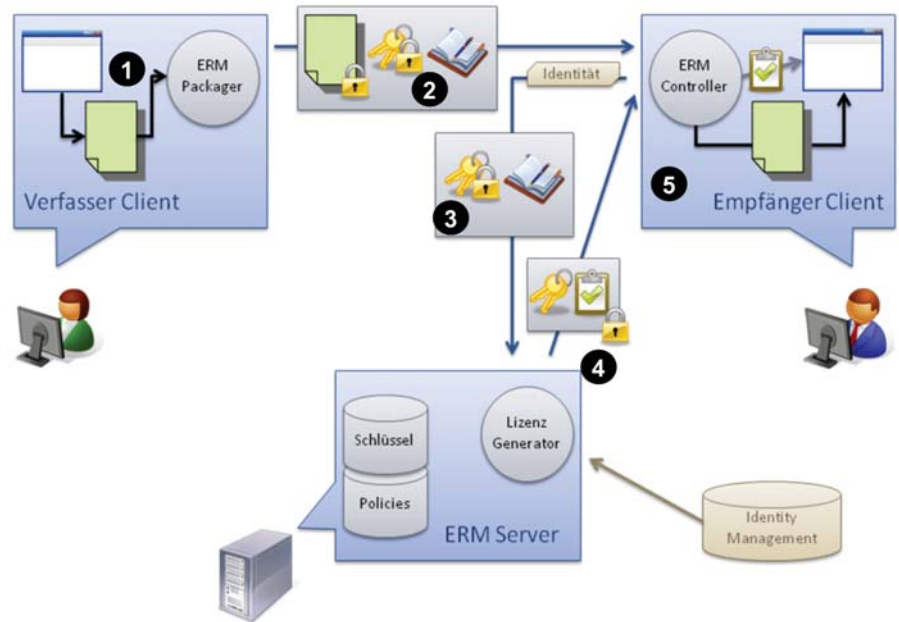


Bild 1: Die fünf Schritte des Enterprise Rights Management sichern Dateien und E-Mails

abschreibt oder abfotografiert. Trotzdem werden die technischen Möglichkeiten, mit denen Informationen unkontrolliert an Dritte weitergegeben werden können, mit ERM stark eingeschränkt.

Fünf Schritte zur sicheren Kollaboration

Technisch erfolgt Enterprise Rights Management in fünf Schritten: Um eine Information, die als Datei oder E-Mail gespeichert ist, zu schützen, benötigt der Verfasser eine Softwarekomponente – ERM-Packager genannt. Er verschlüsselt die Datei oder E-Mail mit einem symmetrischen Verfahren (Schritt 1). Außerdem erzeugt der ERM-Packager eine Policy, die festlegt, wer eine Information ansehen und wie er sie verwenden darf. Der erzeugte symmetrische Schlüssel (Dokumentenschlüssel) und die Policy werden mittels eines asymmetrischen Kryptoverfahrens geschützt, sodass beide ausschließlich für einen ERM-Server lesbar sind. Derart codiert, werden der Dokumentenschlüssel und die Policy an die geschützte Datei oder E-Mail angehängt (Schritt 2).

Wenn ein Empfänger nun auf die Information zugreifen will, benötigt er

den Dokumentenschlüssel. Da dieser codiert ist, muss der Empfänger ihn zunächst beim ERM-Server erfragen. Dies geschieht automatisch durch eine weitere Softwarekomponente, den so genannten ERM-Controller. Die Anfrage enthält den verschlüsselten Dokumentenschlüssel und die Policy sowie einen Identitätsnachweis des Empfängers. Um einen möglichst hohen Sicherheitsstandard zu erreichen, werden für diesen Nachweis die Zertifikate einer Public Key Infrastructure (PKI) verwendet (Schritt 3).

Der ERM-Server überprüft die Identität sowie die erhaltene Policy und erstellt im positiven Fall eine Lizenz (Schritt 4). Sie enthält den lesbar gemachten Dokumentenschlüssel und eine Richtlinie, die bestimmt, wie der Empfänger die Datei oder E-Mail verwenden darf. Um den Dokumentenschlüssel auch beim Transport zu schützen, wird die Lizenz ebenfalls verschlüsselt an den Empfänger übertragen. Bei ihm sorgt der ERM-Controller nun dafür, dass erstens der Dokumentenschlüssel nicht aus der Lizenz extrahiert werden kann und dass zweitens die Nutzungsrechte stets eingehalten werden (Schritt 5).



Funktionales Umfeld betrachten

Damit ERM-Systeme einen sinnvollen und sicheren Schutz von Informationen gewährleisten können, müssen sie verschiedenen Sicherheits- sowie funktionalen Anforderungen gerecht werden. Erfahrungen beim Schutz von elektronischen Medien mit dem Digital Rights Management haben gezeigt, dass ERM-Systeme vor allem durch folgende Angriffe bedroht werden:

- Ausnutzen mangelhafter Architektur
- Extrahieren des Dokumentenschlüssels
- Abgreifen der ungeschützten Daten zwischen der Entschlüsselung und der Darstellung
- Ausnutzen unsicherer Kryptographie.

Bevor ein ERM-System in einem Unternehmen zum Einsatz kommt, müssen IT-Verantwortliche es also hinsichtlich bestimmter Fragestellungen betrachten. Dabei sollte das Augenmerk zunächst auf der Sicherheit der ERM-Architektur und ihrer Softwarekomponenten liegen. Als zentraler Bestandteil ist besonders der ERM-Server durch Angriffe bedroht. Hinzu kommt, dass die Softwarekomponenten und Anwendungen gegen das Extrahieren des Dokumentenschlüssels oder der codierten Daten abgesichert werden müssen. Vor allem Clientanwendungen dürfen keine Si-

cherheitslücken haben, durch die die ERM-Kontrolle umgangen werden kann. Und schließlich sind auch die verwendeten kryptografischen Verfahren von vitalem Interesse und sollten dem aktuellen Stand der Technik entsprechen. Darüber hinaus muss ein ERM-System vollständig in die bereits bestehende IT-Landschaft eines Unternehmens integriert werden. Dies wird beispielsweise bei der Vergabe von Nutzungsrechten für eine Datei oder eine E-Mail deutlich: In Organisationen ist es keine Seltenheit, dass mehrere Mitarbeiter aus verschiedenen Abteilungen die gleichen Dateien verwenden. Sie sollen die Informationen unter Umständen aber nicht alle in der gleichen Art einsetzen dürfen. Die Vergabe von Nutzungsrechten per Hand für jeden Mitarbeiter wäre dabei mühselig und wenig effizient. Daher muss ein ERM-System in der Lage sein, die Identitäten, Rollen und Rechte eines vorhandenen Identitäts- und Zugangsmanagementsystems zu verwenden.

Rechtmanagement berücksichtigen

Um die Vergabe der Nutzungsrechte weiter zu vereinfachen, helfen so genannte "Policy Templates" – Vorlagen, die das ERM-System erstellen und verwalten können muss. Zudem kann es nach der initialen Vergabe von Nutzungsrechten

nötig werden, die Rechte eines Mitarbeiters nachträglich zu erweitern, beschränken oder auch komplett zu entziehen. Ein ERM-System sollte dafür ein entsprechendes Rechtemanagement zur Verfügung stellen.

Möchte ein Benutzer auf eine geschützte Datei zugreifen, muss er zunächst eine Lizenz anfordern, was eine eindeutige Identifizierung erfordert. Eine sichere Methode hierfür ist der Einsatz von PKI-Zertifikaten. Um die Kosten und den Verwaltungsaufwand zu minimieren, sollte ein ERM-System die Zertifikate einer bestehenden Unternehmens-PKI verwenden. Wenn ein ERM-System außerdem die Lizenzanfragen protokolliert, kann ein Unternehmen nachvollziehen, wer wann versucht, auf ein geschütztes Dokument zuzugreifen. Diese Möglichkeit des ERM bietet eine zusätzliche Ebene an Sicherheit.

Fazit

Gerade der letzte Punkt – der Zugriff des ERM-Systems auf die vorhandenen Identitäten, Rollen und Rechte – macht deutlich, dass auch das Enterprise Rights Management Bestandteil einer Sicherheitslösung aus einem Guss sein sollte. Im gleichen Maß, wie die Zusammenarbeit in digitalen Arbeitsprozessen ausgebaut wird, steigt das Sicherheitsbedürfnis eines Unternehmens und damit auch die Notwendigkeit, Dokumente und Informationen vor unbefugtem Zugriff zu schützen. Eine ganzheitliche Lösung sollte ERM deshalb einerseits mit dem Identitätsmanagement im Unternehmen verknüpfen. Andererseits können durch den Einsatz von Zertifikaten organisationsübergreifende Kollaborations- und Geschäftsprozesse nachhaltig gesichert werden. (jp)

Dr. Willi Kafitz ist Sicherheitsexperte und Lead Consultant bei Siemens Enterprise Communications in Frankfurt.

Dirk Weissenbacher ist Consultant im Center of Competence Trusted Identity von Siemens Enterprise Communications in Essen.

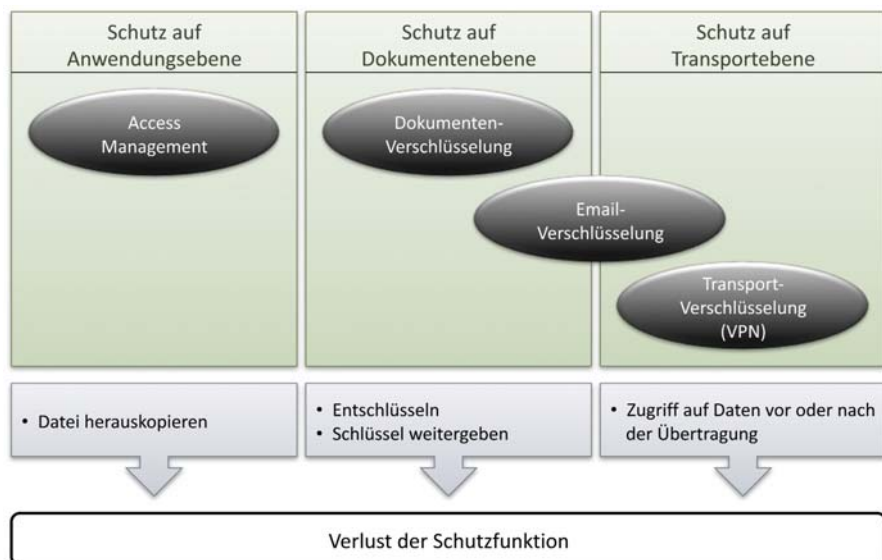
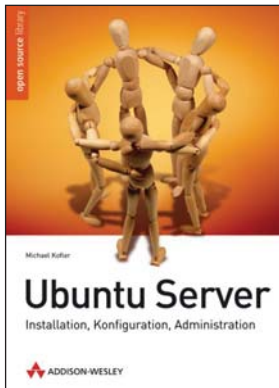


Bild 2: Notwendige Sicherungsmaßnahmen für Dateien und E-Mails – und deren Schwachstellen

Ubuntu Server



Auch wenn die meisten Ubuntu als Betriebssystem für den Client kennen, gibt es eine Server-Variante der Linux-Distribution. Der Ubuntu-Server unterscheidet sich durch die Art der vorkonfigurierten Dienste und An-

wendungen deutlich von der Client-Version. Und auch wenn die Entwickler bei Ubuntu viel Wert auf die einfache Benutzung gelegt haben, ein Serverbetriebssystem aufzusetzen ist nun mal keine einfache Aufgabe, vor allem, wenn der Server produktiv genutzt werden soll. Michael Kofler, Autor der Standardwerks "Linux", nimmt den Anwender in seinem Buch "Ubuntu Server" beim richtigen Umgang mit dem Betriebssystem an die Hand. Als Erstes sticht dabei der Start mit dem Ka-

pitel "RAID und LVM" ins Auge. Normalerweise setzen ähnliche Bücher zu nächst ein Linux auf, damit der Leser sein erstes, schnelles Erfolgserlebnis hat. Das weiß auch Kofler, doch er findet es wichtiger, die Grundlagen zu vermitteln, die zu im Nachhinein nicht mehr leicht änderbaren Konsequenzen führen. Falsche Partitions- und Dateisystementscheidungen sind dann meist nur noch durch eine Neuinstallation behebbar. Die zwei Stunden, die man mit dem ersten Kapitel verbringt, können sich später auszahlen. Und für den Fall der Fälle gibt es weiter hinten im Buch eine Anleitung zum nachträglichen Einrichten von RAID und LVM.

Für den Linux-Profi sind das natürlich keine bahnbrechenden Neuigkeiten. Die will Kofler aber auch nicht ansprechen. Ihm geht es darum, einem halbwegs mit Linux vertrauten Admin zu einem robusten und korrekt aufgesetzten Server zu verhelfen. Die Aufteilung des Buchs passt exakt dazu. Im ersten Teil geht es um die Grundinstallation, danach werden die beiden Ein-

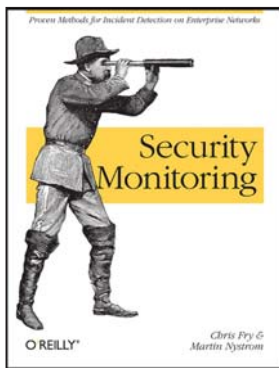
satzfälle LAN-Server und Root-Server bei einem Hosting-Provider beschrieben, jeweils mit den dort sinnvollen Diensten. Im LAN geht es um LDAP, Samba und CUPS, der Root-Server bekommt SSH, Apache, MySQL und einen Mailserver aufgesetzt. Die Anleitungen sind immer kurz und knackig, der Autor kann durch die Beschränkung auf Ubuntu Unterschiede zu anderen Distributionen außer Acht lassen.

Fazit: Wer bei seinem Ubuntu-Server alles richtig machen will, sollte dieses Buch neben die Tastatur legen. Es ist umfassend, gut geschrieben und hat genau den richtigen Tiefgang, um von ambitionierten Einsteigern bis hin zu Semi-Profis alle zu informieren.

Elmar Török

Autor:	Michael Kofler
Verlag:	Addison-Wesley
Preis:	39,95 Euro
ISBN:	978-3-8273-2774-1
Bewertung:	★★★★★

Security Monitoring



Security-Produkte schützen nur, wenn Admins sorgfältig auf die Meldungen der Software achten und entsprechende Schritte einleiten. Das kann schon in kleinen Netzen schwierig sein, große Unternehmen,

die Dutzende Subnetze und ein paar Hundert Server in Betrieb haben, haben ohne klare Struktur keine Chance. Von daher ist das Buch "Security Monitoring" nicht unbedingt notwendig. Schließlich können sich Sicherheitsbeauftragte und Administratoren auch bei anderen Vorlagen orientieren, in Deutschland beispielsweise an den Grundschutzkatalogen des BSI. Trotzdem könnte das Buch für Praktiker sinnvoll sein. "Security Monitoring" ist

kein How-To Titel, jedenfalls nicht, was die Arbeit mit Snort und Firewalls betrifft. Doch die Autoren beschreiben einen deutlich technischeren Ansatz, wie man Netzwerke hinsichtlich Sicherheitsvorfälle überwachen kann. COBIT und Sox werden angesprochen, es geht aber in der Hauptsache darum, ein Konzept zu entwickeln, wie Sicherheitsprobleme schnell erkannt und aufgeklärt werden können.

Fry und Nystrom geben dem Leser im Schnelldurchlauf praktische Methoden an die Hand, um Sicherheit begreifbar zu machen. So sollen als Erstes Regeln und Definitionen erarbeitet werden, was eigentlich überwacht wird und mit welchem Zweck. Je weiter sich der Leser vorarbeitet, desto technischer wird es. Die Autoren nutzen vor allem Netflow, um Daten zu sammeln und aufzubereiten. Das ist in Cisco-Umgebungen Standard, aber auch die meisten anderen Switch-Hersteller haben Netflow im Angebot. Immer wieder erzählen die

beiden kleine Geschichten aus ihrer langjährigen Praxis, die dem Admin zeigen, wo trotz bester Absicht Fehler und Lücken in der Überwachung entstehen können. Das letzte Kapitel konzentriert sich sogar vollständig auf die Beschreibung von Sicherheitskonzepten großer Unternehmen.

Fazit: Wer in seiner Firma IT-Sicherheit ernst nimmt, ist vermutlich schon dank der BSI-Grundschutzkataloge mit einem strukturierten Sicherheitsansatz vertraut. Eine gute Ergänzung kann "Security Monitoring" trotzdem sein, vor allem, wenn bislang Netflow noch nicht oder nur zurückhaltend eingesetzt wurde.

Elmar Török

Autoren:	Chris Fry, Martin Nystrom
Verlag:	O'Reilly
Preis:	36,99 Euro
ISBN:	978-0-596-51816-5
Bewertung:	★★★★★

www.freiesmagazin.de Alles frei

Diesen Monat möchten wir Ihnen in unserer Rubrik "Webseite" einen eher unspektakulären Vertreter dieser Gattung nahelegen, der aber nichtsdestotrotz einen zweiten Blick wert ist. Denn auf den ersten Blick bietet freiesmagazin.de nicht viel mehr als einmal im Monat den Download eines PDFs. Wie uns die Site mitteilt, berichtet das Magazin im PDF-Format über Wissenswertes und Neues zu Freier Software, Open Source und Linux. Was 2005 als unregelmäßiger Newsletter begann, reifte mit der Zeit durch Akzeptanz und Teilnahme der Linux-Community zum regelmäßig erscheinenden Magazin.

Zum Redaktionsschluss lag aktuell die Ausgabe "Mai" mit 52 Seiten vor, die sich einiger spannender Themen für den Administrator annimmt. Etwa dem "Zustand der Distribution" von Debian 5 ("Lenny"): Dieser Artikel stellt Debian 5.0 mit einem Fokus auf die Neuheiten dieser Version vor und nimmt sich dafür satte 10 Seiten Zeit. Sehr aktuell und sicher für viele IT-Verantwortliche interessant dürfte auch der Beitrag "Virtualisierung im Allgemeinen und KVM unter Proxmox VE im Speziell-

len" sein, der beleuchtet, wie sich mit Open-Source-Programmen in Firmen oder zu Hause schnell virtuelle Maschinen einrichten lassen. Darüber hinaus finden sich in dem PDF-Magazin zahlreiche weitere Fachartikel, aber auch eine Diskussion rund um die Lizenzierung, die die Macher des Magazins aus der Community in das Heft tragen und dort zusammenfassen. Sicher ein ungewöhnlicher Ansatz.

"Macher" kann im Übrigen jeder sein: die Website stellt Autorenrichtlinien bereit, anhand derer sich potenzielle Autoren orientieren und ihre Beiträge entsprechend verfassen können. Und es steht sogar eine Artikelwunschlise bereit, die von den Lesern des Magazins zusammengetragen wurde und nun auf Abarbeitung wartet.

Wie eingangs erwähnt, steht das PDF-Magazin im Zentrum dieser Website. Darüber hinaus findet sich – neben den Hinweisen zum Mitmachen – lediglich ein Archiv vergangener Ausgaben. Schön gemacht ist hier aber, dass dem Interessierten vor dem eigentlichen Download noch eine Übersicht der Schwerpunktthemen präsentiert wird. Und auch die Suche ist sicher hilfreich, um gezielt Themen zu finden, denn sie schaut auch in die PDFs. (jp)


freiesMagazin
Mai 2009

Topthemen dieser Ausgabe

Debian GNU/Linux 5.0 „Lenny“ – Der Zustand der Distribution

Dieser Artikel stellt Debian 5.0 „Lenny“ mit einem Fokus auf den Neuheiten dieser Version vor. Die größte unabhängig von Firmen entwickelte Linux-Distribution hat wie immer lange für ihre neue Version gebraucht. Ob sie ihren Qualitätsanspruch erfüllen kann, soll ein wenig untersucht werden. [weiterlesen](#)



Seite 4

Virtualisierung im Allgemeinen und KVM unter Proxmox VE im Speziellen

Wie können mit Open-Source-Programmen in Firmen oder zu Hause schnell virtuelle Maschinen eingerichtet gebracht werden? Dieser Bericht soll Virtualisierung mit KVM etwas beleuchten und einen gewissen Überblick verschaffen. Vor allem auf das Programm Proxmox VE wird dabei näher eingegangen. [weiterlesen](#)



Seite 25

Das Netbook-Touchpad: Ein ergonomisches Desaster

Der regelrechte Hype um die kleinen Helfer Netbooks muss in letzter Zeit viele Nutzer in seinen Bann gezogen haben, glaubt man den Verkaufszahlen prominenter Hersteller. In diesem Artikel wird das Acer Aspire One [A 110L] mit seinem nicht immer leicht zu bedienendem Touchpad vorgestellt und alternativen Bedienungsmethoden mit Anlehnung an Vim aufgezeigt. [weiterlesen](#)



Seite 42

Das PDF der Maiausgabe des "freiesMagazin"



Fachartikel

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

Anwenderbericht:
Moderne IT im Krankenhaus
 Mit der Einführung eines neuen Informationssystems war es nötig, im Diakonie-Krankenhaus Bremen die IT-Infrastruktur auf den neuesten Stand zu bringen. Dabei ging es um den Neubau eines Rechenzentrums nach aktueller Technik mit einer hochverfügbaren Server- und Storage-Umgebung, die den Anforderungen der neuen Krankenhausapplikationen hinsichtlich Stabilität und Performance gerecht werden sollte. Lesen Sie in unserem Anwenderbericht, wie sich diese Punkte mit einer Clusterlösung und Servervirtualisierung optimal umsetzen ließen.
www.it-administrator.de/themen/server_client/fachartikel/57830.html

10 Mythen rund um Hochverfügbarkeit
 Während die einen der Meinung sind, Hochverfügbarkeit würde sie überhaupt nicht betreffen, erkennen andere zwar grundsätzlich die Gefahr, sehen aber nicht, wie sie sich mit den Möglichkeiten kleinerer und mittlerer Unternehmen dagegen wappnen könnten. Beides ist für uns Anlass genug, einmal mit den Mythen, die rund um das Thema Hochverfügbarkeit entstanden sind, aufzuräumen.
www.it-administrator.de/themen/server_client/fachartikel/57831.html

Anwenderbericht: Migration auf SBS 2008
 Das IT-Systemhaus LemonTec in Schleswig-Holstein hat sich auf die Anforderungen von KMUs spezialisiert. Ende 2008 erfolgte auf Serverseite ein Upgrade von Small Business Server 2003 auf die aktuelle Version 2008 Premium. In unserer Case Study erfahren Sie, welche Vorteile sich das Unternehmen vom Systemsprung versprochen und wie sich die praktische Umsetzung gestaltete.
www.it-administrator.de/themen/server_client/fachartikel/57832.html

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

»Die Arbeit mit Menschen und Technik macht einfach Spaß«

Thomas Barsties (29) hat bei der alpha Personal-Service GmbH, einem Zeitarbeitsunternehmen im Rhein-Main-Gebiet, als IT-Administrator sein Hobby zum Beruf gemacht. Als IT-Leiter ist er in einer virtualisierten Umgebung Herr über rund 25 Server und zahlreiche Komponenten. Darüber hinaus zeichnet Barsties für die Entwicklung der neuen IT-Systeme des Dienstleisters verantwortlich.

Welche Ausbildung haben Sie gemacht?

2004 schloss ich meine Ausbildung zum Fachinformatiker der Fachrichtung Systemintegration ab. Nebenbei habe ich Schulungen unter anderem bei Intel, HP und Verizon besucht und bin als MCSA+M sowie MCSE zertifiziert.

Warum sind Sie IT-Administrator geworden?

Mir hat das Zusammenspiel von Hard- und Softwarekomponenten von Anfang an viel Spaß gemacht. Als ich 14 war, habe ich in der Firma eines Bekannten bei der IT gelegentlich nach dem Rechten gesehen, mit 18 betreute ich bereits eine Handvoll mittelständischer Unternehmen. Spätestens ab da hat mich der Spruch "Du kennst dich doch so gut mit Computern aus..." verfolgt und daran hat sich bis heute nichts geändert. Die Arbeit mit Menschen und Technik macht einfach Spaß.

Welche IT-Umgebung betreuen Sie aktuell?

Wir verfügen über knapp 25 Server, die zum Großteil über Hyper-V virtualisiert sind. Den gut 40 Clients stehen noch ein Dutzend Drucker und einige Home Offices sowie eine VoIP-Telefonanlage zur Seite. Neben Exchange 2007 setzen wir Terminal Server, Internet Information Server für verschiedene Aufgaben, Sharepoint Server sowie Microsoft und Firebird SQL ein. Als Leiter der IT muss ich dabei die Fäden in der Hand halten.

Welches Netzwerk- und Systemmanagement setzen Sie ein?

Derzeit befindet sich unser Nagios-System noch in der Testphase. An den Servern nutzen wir momentan noch das integrierte Servermanagement der Hersteller.

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

Zum einen sind es die Benutzer, die mit jeder Verbesserung und Automatisierung verwöhnter werden und diesen Komfort natürlich nicht mehr missen möchten. Zum anderen sind es neue Entwicklungen.



Geburstag: 17.09.1979
Familienstand: verheiratet
Hobbys: Laufen, Elektrotechnik, Heimkino

Thomas Barsties, IT-Administrator

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Die Großbaustelle ist derzeit der Relaunch unserer Webseite, in die auch unser überarbeitetes Corporate Design einfließen wird. Hier heißt es nicht nur den Webserver bereitzustellen, sondern auch Design und Funktion zu koordinieren.

Was macht Ihnen an Ihrem Job am meisten Spaß?

Nur von wenigen Dingen ist ein Unternehmen heute so abhängig wie von der IT. Es macht mir Spaß, tagtäglich die großen und kleinen Probleme zu meistern, damit alles flüssig weiterläuft.

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

Routinearbeiten sind meistens eine Qual. Alles genau zu dokumentieren, gehört aber natürlich auch zu den täglichen Pflichten.

Was tun Sie für Ihre Fort- und Weiterbildung?

Die einfachste Quelle ist das Internet mit seinen IT-Newsseiten. Für die Fortbildung nehme ich regelmäßig an Zertifizierungen

der jeweiligen Hersteller teil. Wenn man sich selbst technisch nicht verbessert, kommt der nächste BSOD (Blue Screen of Death) früher, als einem lieb ist.

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

Vor gut fünf Jahren habe ich einem damaligen Kunden das Notebook aus Versehen so eingestellt, dass das WLAN stets auf sich selbst verbunden hat. Es war die erste Version des Treibers, der auch als WLAN-Basis fungieren konnte. Bis ich den richtigen Haken im Treiber gefunden hatte, verging einige Zeit.

Was war Ihr größter Erfolg als IT-Administrator?

Seit mehr als fünf Jahren vergrößern wir unsere Räumlichkeiten rund einmal im Jahr. Aufgrund meiner IT-Planung gab es bisher noch nie einen Ressourcenengpass oder einen ungeplanten Ausfall des Systems. Darauf bin ich stolz.

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

Letztens hat mich eine Anwenderin tagelang mehrmals angerufen und gleich wieder aufgelegt. Auf Nachfrage stellt sich dann heraus, dass sie den Hörer abhebt und dann so langsam wählt, dass sie auf meiner Nebenstelle herauskommt.

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

Die größte Herausforderung ist immer die Frage, ob man wirklich gleich auf den neusten technischen Zug aufspringt und mitfährt oder noch etwas wartet.

Das Interview führte Petra Adamik,
 Freie Journalistin, München.

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 8/09 erscheint am 3. August 2009

Schwerpunktthema:

Hochverfügbarkeit

Im Test: Double Take for HyperV

Im Test: Linux-Hochverfügbarkeit mit OSCAR

Workshop: Best Practices zur Active Directory-Replikation

Systeme: Windows Server 2008 R2 im Cluster

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

Unsere Ausgabe im September dreht sich um das **Drucker- und Peripherienmanagement**. In einem Test muss die Drucklösung "PaperCut" ihr Können unter Beweis stellen. Daneben lesen Sie in unseren Workshops, wie das Drucken über Essential Business Server und Small Business Server optimal funktioniert.

Als Schwerpunkt im Oktober folgt dann das Thema **Storage**.

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

Redaktion

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

Daniel Richey (dr), *Redakteur*
daniel.richey@it-administrator.de

Lars Nitsch (ln), *Volantär*
lars.nitsch@it-administrator.de

Markus Heinemann, *Schlussredakteur*
markus.heinemann@email.de

Autoren dieser Ausgabe

Petra Adamik, Andreas Badur, Thomas Drilling,
Dr. Jürgen Fechter, Jürgen Heyer, Thomas Joos,
Dr. Willi Kalfitz, Robert Lindemeier, Uwe Mauere,
Dr. Holger Reibold, Dirk Srocke, Elmar Török,
Dirk Weissenbacher, Bertram Wöhrmann, Dennis Zimmer

Anzeigen

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

Es gilt die Anzeigenpreisliste
Nr. 6 vom 01.01.2009

LAC/2008



Produktion / Anzeigendisposition

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

Druck

Ceska Unigrafie, a.s.
U Stávovservisu 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

Urheberrecht

Alle in IT-Administrator erschienenen Beiträge sind urheberrechtlich geschützt. Alle Rechte, einschließlich Übersetzung, Zweitverwertung, Lizenzierung vorbehalten. Reproduktionen und Verbreitung, gleich welcher Art, ob auf digitalen oder analogen Medien, nur mit schriftlicher Genehmigung des Verlags. Aus der Veröffentlichung kann nicht geschlossen werden, dass die beschriebenen Lösungen oder verwendeten Bezeichnungen frei von gewerblichen Schutzrechten sind.

Haftung

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

Manuskriptensendungen

Die Redaktion nimmt gerne Manuskripte an. Diese müssen frei von Rechten Dritter sein. Mit der Einsendung gibt der Verfasser die Zustimmung zur Verwertung durch die Heinemann Verlag GmbH. Sollten die Manuskripte Dritten ebenfalls zur Verwertung angeboten worden sein, so ist dies anzugeben. Die Redaktion behält sich vor, die Manuskripte nach eigenem Ermessen zu bearbeiten. Honorare nach Vereinbarung.

So erreichen Sie den Leserservice

Leserservice IT-Administrator
Stephan Orgel
65341 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

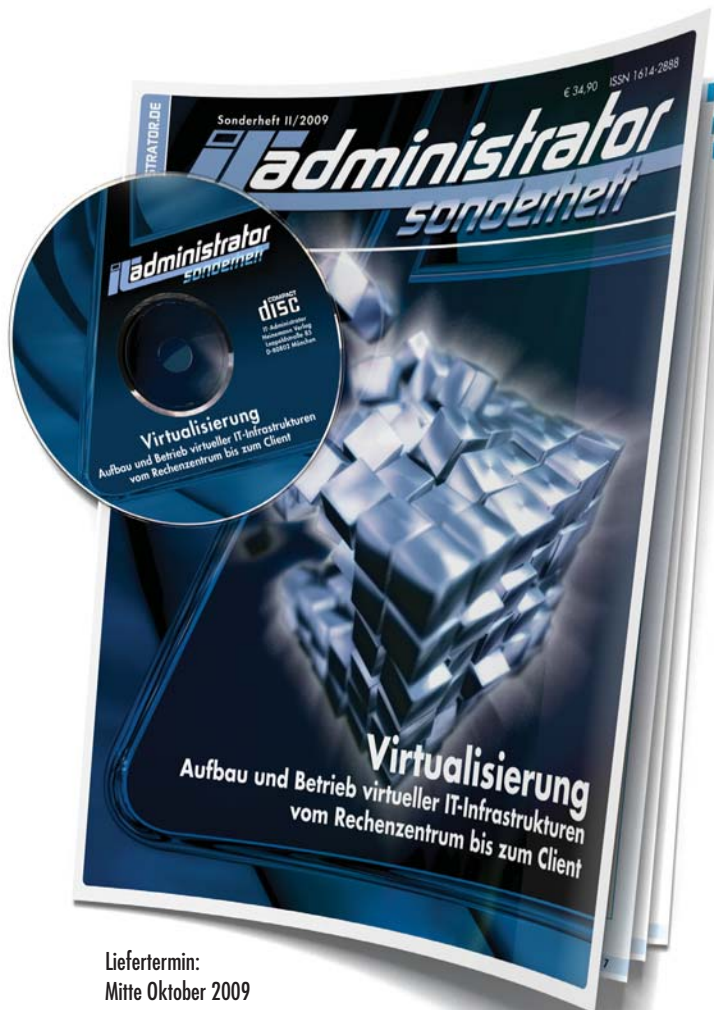
So erreichen Sie die Anzeigenabteilung

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

1 und 1 S. 04
ADN S. 41
IBM S. 13, S. 68
itsa S. 31

Kaspersky Lab S. 02
NRW Conf 09 S. 33
REALTECH S. 17
rent a mind S. 23

INSERENTENVERZEICHNIS



Liefertermin:
Mitte Oktober 2009

Bestellen Sie jetzt das IT-Administrator Sonderheft II/2009!

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

Virtualisierung

zum Abonnenten-Vorzugspreis* von

nur € 29,90!

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

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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



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

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

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

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____

BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

So erreichen Sie unseren
Vertrieb, Abo- und
Leserservice:

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

Tel: 06123/9238-251

Fax: 06123/9238-252

leserservice@it-administrator.de

Diese und weitere Aboangebote
finden Sie auch im Internet
unter www.it-administrator.de



Heinemann Verlag

Leopoldstraße 85

D-80802 München

Tel: 089-4445408-0

Fax: 089-4445408-99

Geschäftsführung:

Anne Kathrin Heinemann

Matthias Heinemann

Amtsgericht München HRB 151585

ITA 0709

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

