IT-ADMINISTRATOR.DE

04/2011

€ 12,60 ISSN 1614-2888

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

Backup & Recovery

HP ProLiant DL385 G7 Server

- Bis zu 2 Eight-Core oder Twelve-Core AMD Opteron™ Prozessoren der 6100 Serie
- Bis zu 256 GB Speicher
- Bis zu 8 Hot-Plug-fähige HP Small Form Factor SAS, SATA oder Solid State Laufwerke
- iLO 3 ermöglicht eine leistungsstarke, hardware-basierte Remote-Verwaltung und -Steuerung über einen Standard-Web-Browser und entlastet damit die IT-Mitarbeiter

HP ProLiant DL585 G7 Server

- Bis zu 4 Eight-Core oder Twelve-Core AMD Opteron™ Prozessoren der 6100 Serie
- Bis zu 512 GB Speicher
- Bis zu 8 Hot-Plug-fähige HP Small Form Factor SAS, SATA oder Solid State Laufwerke

PROFITIEREN

Sie von der neuen Effizienz.

HP ProLiant Server sind jetzt noch sparsamer.

Sie wollen Ihre IT-Kosten senken? Und dafür Ihre Server konsolidieren und den Energieverbrauch reduzieren? Mit HP ProLiant Servern basierend auf AMD Opteron™ Prozessoren der 6100 Serie erreichen Sie Ihre Ziele:

- 27-fache Leistung pro Watt als Server der letzten Generation*
- 94 % Effizienz durch Platinum-zertifizierte HP Netzteile*
- 91:1 Konsolidierung mit HP ProLiant DL585 G7*
- 4P-Leistung zum 2P-Preis mit HP ProLiant DL585 G7*

Ermitteln Sie jetzt Ihr individuelles Einsparpotenzial unter **www.hp.com/de/profitieren_a**

100 % Sicherheit

Sichern Sie Ihre IT Investition immer mit **HP Care Pack Services** ab. Sie erweitern damit die Standardgarantie Ihrer HP ProLiant Server im Leistungsumfang, in der Reaktionszeit, Ansprechzeit und Laufzeit. Mit der DMR-Option des HP Care Pack Services können Sie außerdem defekte Festplatten „im Fall der Fälle“ einbehalten und der Datenschutz bleibt in Ihren Händen.

Care Pack SERVICES

*Weitere Informationen finden Sie unter www.hp.com/de/profitieren_a

EDITORIAL

Apfel und Sündenfall

Liebe Leser,

es ist die alte Geschichte vom Chef-Gadget, das zum Abteilungsleiter-Gadget wird und das kurz darauf so gut wie jeder hat und nun sollen Sie, lieber Herr Administrator, doch bitte dafür sorgen, das so beliebte Gerät in die IT-Infrastruktur einzubinden. Nun wäre es schön, wenn Sie bei dieser "alten Geschichte" auch von den Erfahrungen der Vergangenheit profitieren könnten und die Sache einfach erledigen. Doch leider reden wir hier vom aktuellen Superstar der Gadgets – dem iPad.

Zweifellos ist Apples Topseller ein in vielen Situationen nützliches Gerät, das mit innovativer Technik die Anwender begeistert. Und für uns als Fachmagazin stehen technisch valide und umsetzbare Informationen für Ihren Job im Vordergrund. Daher betreiben wir genauso wenig Apple-Bashing wie dessen vorbehaltlose Huldigung. Doch das iPad ist so etwas wie der Sündenfall für das Client Lifecycle-Management. Dass Sie in der Beschaffung für jedes iPad jeweils eine Kreditkartennummer benötigen, ist eine reine – wenn auch nicht triviale – Sache der Organisation. Dass jedoch die Anwender unternehmensweite Sicherheitsrichtlinien – sofern Sie es schaffen, diese auf das iPad zu bringen – einfach ausschalten können, ist nicht akzeptabel.

Sie sollten sich – bevor Sie sich breitschlagen lassen, das iPad als neuen Client in das Netz aufzunehmen – genau über die Probleme informieren, die dies mit sich bringt. Einen Anfang macht da unser Beitrag ab Seite 34. Doch auch hier berichten wir lediglich über das technisch Machbare in Sachen iPad. Wer sich jedoch auf der CeBIT bei Herstellern von Client-Management-Suiten über die Möglichkeiten einer Verwaltung des iPad mit derartigen Werkzeugen informieren wollte, musste lange suchen: Nur ein Hersteller hat dazu einen Ansatz im Portfolio. Und dieser Hersteller gibt freimütig zu, wie beschränkt die Möglichkeiten des Managements sind und zieht als Fazit, dass sich jeder IT-Verantwortliche schriftlich gegen die Gefahren einer Integration des iPad ins Unternehmensnetzwerk absichern sollte!

Aber auch in anderen misslichen Lagen helfen wir Ihnen in unserem Schwerpunkt zu Backup & Recovery weiter: Ab Seite 54 finden Sie eine Anleitung zum Bare Metal Recovery eines Windows 2008-Servers. Und natürlich haben wir auch wieder spannende Tests im Gepäck.

Viel Vergnügen beim Lesen, Ihr

John Pardey
Chefredakteur

baramundi
software AG

Mit baramundi in die Arenen der Champions

Anpfiff für Matchwinner „IT-Lifecycle-Management“

baramundi Focus Tour 2011: Kommen Sie in die Arenen der Champions!

Perfekte Technik entscheidet im Fußball – und in der IT erfolgreicher Unternehmen. Automatisierte Bewegungsabläufe und optimale Kooperation im Team garantieren beste Ergebnisse.

Was erfolgreiche Sportclubs beherrschen, führt auch viele andere Unternehmen zu reduzierten IT Kosten und spürbaren Synergieeffekten. Denn Teamspiel und Doppelpass sind auch im Client Management üblich. Zum Beispiel passt baramundi Connect Daten aus der baramundi Management Suite direkt und zielsicher zu anderen Applikationen aus Helpdesk, Buchhaltung und anderen.

Wie Sie Ihre IT so zum Dream Team formen und Client Management zur Paradedisziplin machen, zeigen wir Ihnen schon bald in den schönsten Stadien Deutschlands. Spielen Sie mit – und gewinnen Sie!

Ihr Focus Tour Match im Überblick

Vom Anpfiff bis zur Matchanalyse – mit baramundi spielen Sie in der ersten Liga. Ihr Focus Tour Matchtag zeigt Ihnen, wie Ihr Unternehmen von erstklassigem Client Management profitiert. Ihre Themen:

- Automatisierte Windows 7 Migration
- Virtualisierung und Client Management
- Intelligenter Software Rollout unter Windows 7
- Kunden im Praxisdialog: Migration als Big Bang oder Step-by-Step

Ihr Spieltag mit Stadionrundgang: Anmelden - und kostenlos teilnehmen!

Wie unterstützt die baramundi Management Suite Ihr IT-Team? Antworten erhalten Sie schon bald in diesen Stadien:

12.04.2011 - SIGNAL IDUNA PARK **Dortmund**
13.04.2011 - Commerzbank Arena **Frankfurt**
04.05.2011 - Imtech Arena **Hamburg**
05.05.2011 - Olympiastadion **Berlin**

Die Teilnahme ist für Sie kostenlos.

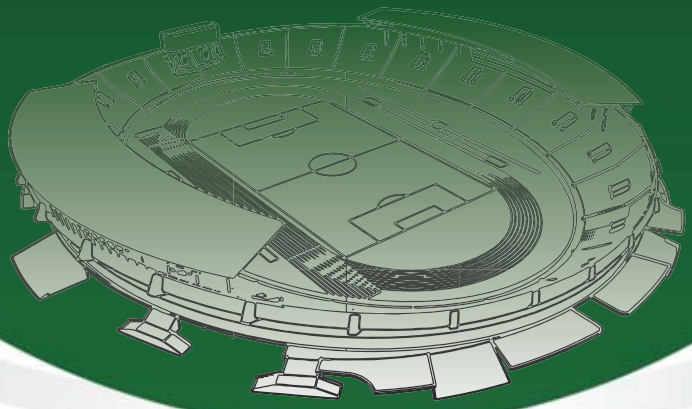
Mit der baramundi Management Suite gewinnen

Ihr Stadionbesuch bringt Ihnen sicher viele neue Erkenntnisse und Erfahrungen zum Client Management. Dazu hautnahes Stadionfeeling im VIP-Bereich. Und vielleicht auch noch viele rasante Matches auf Ihrem Bildschirm: Denn unter allen Fans der baramundi Focus Tour verlosen wir eine Playstation 3 mit FIFA 11.

Werden Sie Matchwinner im effizienten IT-Management. Mit der baramundi Focus Tour.

Weitere Informationen und die detaillierte Agenda finden Sie online:
www.baramundi.de/focus-tour

Interesse? Dann melden Sie sich zur kostenfreien Veranstaltung an:
www.baramundi.de/focustour



baramundi software AG
Beim Glaspalast 1
86153 Augsburg

Fon: +49 (821) 5 67 08 - 380
Fax: +49 (821) 5 67 08 - 19
E-Mail: focustour@baramundi.de

INHALT

IT-Administrator – Ausgabe April 2011

Backup & Recovery

Im Test: Primera Disc Publisher Pro Xi

Wer schon einmal mehr als fünf Exemplare einer identischen CD/DVD mit einem einfachen Brenner erstellen durfte, der weiß um die Dauer und die gefühlte Stupidität dieses Vorgangs. Kommt es mehrmals im Jahr zu einem solchen Szenario, beispielsweise für ein Softwareupdate, eine Datenarchivierung oder den Versand eines elektronischen Katalogs auf Scheibe, so kann sich die Anschaffung einer automatisierten Lösung schon lohnen. IT-Administrator hat sich den Primera Disc Publisher Pro Xi im Test genauer angeschaut und DVDs in Serie produziert.

Seite 26

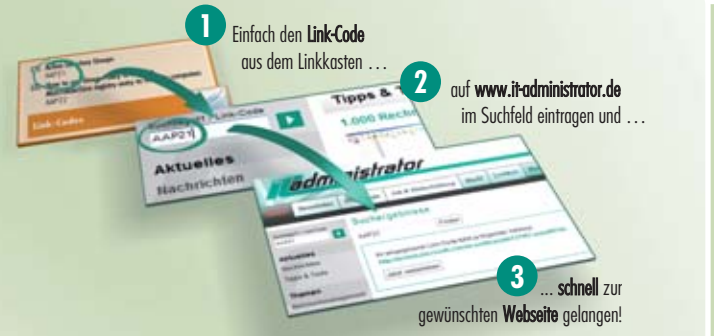
Datensicherung unter Hyper-V

Wer über Hyper-V und Windows Server 2008 (R2) virtuelle Server zur Verfügung stellt, muss sein Datensicherungskonzept an die virtuelle Umgebung anpassen. Die Sicherung des Hosts und der darauf laufenden virtuellen Server verlangt andere Herangehensweisen als die Sicherung herkömmlicher physikalischer Server. Wir zeigen Ihnen in unserem Workshop, wie Sie mit Hausmitteln Backups von Hyper-V anfertigen und was beim Einsatz von Microsofts Data Protection Manager wichtig ist. Außerdem erklären wir, wie Sie mit der PowerShell virtuelle Maschinen automatisiert exportieren können.

Seite 50

Neu im IT-Administrator: Link-Codes

Unsere neuen Link-Codes ersparen Ihnen mühsame Tipparbeit bei langen URLs



NAS mit InfiniBand

Synology stellt im Rahmen der neuen **xs (Extreme)- und Plus-Serie** neue NAS-Server vor. Die Geräte bieten Platz für maximal 36 Festplatten und damit ein Speichervolumen von über 100 TByte. Die xs-Serie besteht aus den beiden RackStations RS3411xs und RS3411RPxs für den Serverschrank sowie der DiskStation DS3611xs. Die Rack-Modelle verfügen ab Werk über zehn Festplatteneinschübe, lassen sich jedoch mittels separat erhältlicher Erweiterungseinheiten auf 34 Festplatten aufrüsten. Die DiskStation DS3611xs verfügt über zwölf Festplatten-Steckplätze, auch sie lässt sich mit der Erweiterungsstation DX1211 auf 36 Bays skalieren. Die Erweiterungsstationen werden über InfiniBand-Kabel mit 12 GBit Bandbreite angebunden. Die NAS-Server bieten zudem vier GBit-LAN-Ports mit Link Aggregation und zwei 10 GBit-Anschlüsse für zusätzliche Add-on PCIe-Karten. Ausgestattet mit einem Intel i3-Prozessor sollen diese Modelle Übertragungsgeschwindigkeiten von durchschnittlich 800 MByte pro Sekunde beim Lesen und Schreiben erreichen. Zu den Neuheiten der Plus-Serie gehören das Rack-Modell RS2211+ sowie die identische, jedoch mit redundanter Stromversorgung ausgestattete RackStation RS2211RP+. Die Modelle der plus-Serie erreichen Lese- und Schreibgeschwindigkeiten von durchschnittlich 190 MByte pro Sekunde und können mit den Erweiterungseinheiten auf 22 beziehungsweise 24 Festplatteneinschübe aufgerüstet werden. Die Plus-Serie ist ab 1.499 Euro verfügbar, die Preise für die xs-Serie lagen bei Redaktionsschluss noch nicht vor. *(jp)*

Synology: www.synology.com/de/

Mit der RS3411xs richtet Synology seinen Blick erstmals auf Speicheranwendungen in Unternehmen

WLAN-Schutz mit FortiGate

Fortinet bringt das **Major Release 3** (MR3) seines Betriebssystems **FortiOS 4.0** mit integrierter Security für kabelgebundene und kabellose Netze auf den Markt. Ausgestattet mit dem neuen Betriebssystem ermöglicht die ebenfalls neue Appliance **FortiGate-3140B** etwa, Profile für Richtlinien, die Überwachung des Webfiltering und Regelung des Datenverkehrs zu erstellen. Die Appliance bietet 10 GBit/s IPS-Durchsatz, 22 GBit/s VPN-Traffic- und 58 GBit/s Firewall-Durchsatz. Für den Anschluss an das Netzwerk verfügt das Gerät über 22 Ports. In der neuen FortiOS-Version 4.0 MR3 wurden zudem die Wireless-Controller-Funktionen erweitert, um Fortinet-WLAN Access Points automatisch bereitzustellen und Schwachstellen wie etwa Rogue Access Points zu erkennen. Diese Funktionen sollen eine verhaltens- und personenbasierte Zugangskontrolle zu geschützten Daten ermöglichen. Mit den integrierten Policy-Optionen können darüber hinaus verdächtige Bewegungen und Aktionen im Netzwerk überwacht, in Quarantäne verschoben oder blockiert werden. Management- und Reporting-Funktionen für Wireless-Verbindungen und Sicherheit sind ebenfalls integriert. Auch wird das neue FortiToken-System des Herstellers unterstützt sowie die IPv6-Unterstützung weiter ausgebaut. Verfügbar sein soll das Firmware-Upgrade ab sofort. Für Bestandskunden mit Wartungsvertrag ist das Update kostenlos. Die Appliance FortiGate-3140B kostet inklusive einjährigem Wartungsvertrag mit Antivirus-, IPS- und Anti-Spam-Pattern 76.000 Euro. *(dr)*

Fortinet: www.fortinet.com

Die Appliance FortiGate-3140B von Fortinet bietet 10 GBit/s IPS-Durchsatz

Feinjustierter Datenschutz

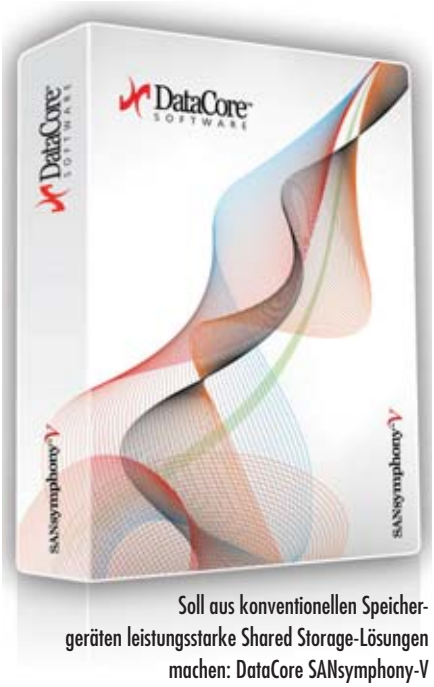
SonicWALL stellt seine nächste Produktgeneration für **Continuous Data Protection** (CDP) vor. Mit einer neu entwickelten Architektur soll das **Appliance-basierte SonicWALL CDP 6.0** eine verlässliche Lösung für Backup und Recovery im Unternehmenseinsatz bieten. Sie umfasst hierfür Funktionen für die Administration und soll es ermöglichen, geschäftskritische Informationen effizient zu verwalten, intelligent zu schützen und vollständig wiederherzustellen. CDP 6.0 bietet dabei eine vollständige Datenwiederherstellung, selbst wenn die ursprünglichen Daten fehlerhaft sind. Daneben erlaubt die neue Version das Einrichten granularer Richtlinien für Backups und ermöglicht damit laut Hersteller, geschäftskritische Daten vorzuhalten, zu filtern und dauerhaft zu sichern. Dabei kann die CDP 6.0 veraltete und unwichtige Dateien aus dem Backup-Set entfernen. Die Preise für das Produkt beginnen bei 1.990 Euro inklusive Support. *(dr)*

SonicWall: www.sonicwall.com/de/

Hochleistungs-Storage für Virtualisierung

DataCore Software bietet mit **SANsymphony-V** die achte Generation seiner Software-Plattform für die Storage-Virtualisierung an. Das Werkzeug soll konventionelle Speichergeräte in leistungsstarke **Shared Storage-Lösungen** für Infrastrukturen mit dynamischer Desktop- und Servervirtualisierung umwandeln. Die neue Generation beseitigt dabei laut Anbieter die typischen Performance-Probleme, IO-Flaschenhälse und Ausfallzeiten auch bei geschäftskritischen Applikationen wie Datenbanken oder Mailservern. Durch das DataCore-eigene Adaptive Caching sowie weitere Performance-fördernde Technologien verarbeitet SANsymphony-V eine Vielzahl unterschiedlicher Workloads simultan, ohne dass Veränderungen in der Speicherplatzzuweisung zu Ausfällen, Verzögerungen oder Geschwindigkeitsengpässen führen. Die neue Version bietet unter anderem eine intuitive, konfigurierbare GUI, Workflow-Integration und -Automation, automatische Wizards und ein aufgabenorientiertes Design. Außerdem steht Administratoren nun eine integrierte Continuous Data Protection (CDP) zur Verfügung. Eine komplett redundante Konfiguration von SANsymphony-V mit Hochverfügbarkeitsfunktion und einjährigem 24x7-Support ist ab 10.000 US-Dollar erhältlich. *(dr)*

DataCore: www.datacore.com/SANsymphony-V/



Soll aus konventionellen Speichergeräten leistungsstarke Shared Storage-Lösungen machen: DataCore SANsymphony-V

Kommunikation aus der Wolke

C4B Com For Business veröffentlicht das erste **Service Release** seiner **UC-Anwendung XPhone Unified Communications 2011**. Die UC-Plattform umfasst **CTI, Presence Management und die Unified Messaging-Dienste Fax, Voicemail und SMS**. Mit dem Service Release 1 (SR1) erweitert der Anbieter seine CTI-Lösung um Cloud-Services. Mit der aktuellen Version ist es somit möglich, neben Groupwaresystemen im Haus auch gehostete Systeme (zum Beispiel Microsoft BPOS) oder Cloud-Services um CTI- und Unified Communications-Funktionen zu erweitern und mit der lokalen Telefoninfrastruktur zu verknüpfen. Die Anwender können damit auf Kontaktdaten auch aus der Business-Anwendung Google Apps zugreifen und direkt daraus wählen. Das SR1 ist außerdem mit zusätzlichen Schnittstellen für Softwarepartner ausgestattet. Diese können über offene XML-Standards ihre externen Anwendungen um UC-Funktionen erweitern. Darüber hinaus enthält die Lösung ein Click-to-Dial-Plug-In für Webbrowser. So können User per Mausklick von einem Webbrowser aus Anrufe tätigen. Auch sehen die Anwender bei der aktuellen Version ein Bild des Anrufers aus den Outlook-Kontakten. Mit der erweiterten Hotkey-Steuerung kann aus jeder Anwendung heraus das Gespräch weiterverbunden werden. Ab sofort steht die aktuelle Version für Bestandskunden als kostenloses Update zur Verfügung. XPhone Unified Communications kostet bei 25 Usern ab 89 Euro pro Nutzer. *(dr)*

C4B: www.c4b.de

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

Riverbed gibt die Verfügbarkeit von **RiOS 6.5** bekannt, das als Betriebssystem auf den WAN-Optimierungslösungen des Herstellers zum Einsatz kommt. Zu den aktualisierten Funktionen gehört eine neue Klassifizierungs-Engine, die mit Application-Signature-Matching und der Zergliederung von Protokollen Anwendungen noch effizienter einstufen soll. Auch an den QoS-Funktionen will Riverbed gearbeitet haben: Einzelne Applikationen lassen sich nun entsprechend ihrer Latenz-Empfindlichkeit priorisieren, zudem will der Hersteller das Management der QoS-Einstellungen über die zentrale Konsole vereinfacht haben. Neu ist außerdem eine Unterstützung des SMB v2-Protokolls, das unter Windows 7 Verwendung findet. *(ln)*
www.riverbed.com/de/

Acer bietet die **Business-LCDs B243HLC** und **B273HL** an. Um Anwendern auch bei nicht direkt frontaler Ansicht eine hohe Bildqualität zu liefern, verfügen die Modelle über Vertical Alignment Panels (VA-Panels). Damit erlauben die Bildschirme einen Betrachtungswinkel von 178 Grad bei CR 10:1. Zudem können die neuen LCDs um 110 mm in der Höhe verstellt werden. Für die Einstellung der Betrachtungsposition lässt sich der Bildschirm um 15 Grad aufwärts und um fünf Grad abwärts neigen sowie um jeweils 35 Grad nach rechts oder links schwenken. Zusätzlich ermöglicht die Pivot-Funktion des Acer B243HL eine Drehung um 90 Grad. Die Widescreen-Displays sind in den Größen 24 Zoll beim B243HLC und 27 Zoll (Acer B273HL) erhältlich und bieten eine Full HD-Auflösung von 1.920 x 1.080. Ab 209 beziehungsweise 335 Euro sind die Bildschirme erhältlich. *(dr)*
www.acer.de

RES Software hat den **RES Virtual Desktop Extender** (VDX) als eigenständiges Produkt veröffentlicht, das Mitarbeitern innerhalb einer virtuellen Umgebung den gleichzeitigen Zugriff auf lokale und virtuelle Applikationen erlaubt. Die Lösung ist kompatibel mit den Desktop-Virtualisierungslösungen Citrix XenApp, Citrix XenDesktop, VMwareView und Microsoft Remote Desktop Services sowie Produkten für Profilmanagement wie AppSense Environment Manager. Anwender, die unterschiedliche Technologien und Software-Versionen in ihren Terminal-Server- und Virtual-Desktop-Umgebungen einsetzen, können lokale Anwendungen nahtlos in virtuelle Desktop-Sessions einbinden. VDX steht ab sofort zur Verfügung und kostet 15 Euro pro Arbeitsplatz. *(dr)*
www.reverseseamless.com

M86 stellt die **SMB Security Suite** vor. Diese besteht aus M86 MailMarshal Secure Email Gateway, M86 WebMarshal, M86 Filter List sowie M86 Marshal Reporting Console und bietet eine Auswahl an Virenschutz-Lösungen. Die Suite richtet sich an Unternehmen mit bis zu 500 Usern und liefert Features für das User-Management sowie für die Kontrolle von Content und Policys. Mit Tools wie Quota Management und Content Inspection erlaubt die Lösung zudem, Richtlinien für eine akzeptable Web 2.0-Nutzung zu implementieren, ohne den Zugang komplett zu sperren. Die Preise starten bei rund 25 US-Dollar pro Nutzer. *(dr)*
www.m86security.com

Katastrophenschutz für den Admin

FalconStor kündigt die Verfügbarkeit des Disaster Recovery-Automationstools **RecoverTrac** an. Das Tool ist als Standardfunktion unter anderem in dem FalconStor **Continuous Data Protector** (CDP) integriert. RecoverTrac soll als **Disaster Recovery-Automationslösung** eine serviceorientierte Wiederherstellung sowohl für physikalische als auch virtuelle Server-Infrastrukturen ermöglichen. Es automatisiert hierfür komplexe und fehleranfällige Sicherungs- und Ausfallssicherungs-Aufgaben für Systeme, Anwendungen und Dienste sowie für das gesamte Rechenzentrum. Das Disaster Recovery-Tool repliziert dabei nicht nur Daten, sondern richtet die Wiederherstellung kompletter Dienste durch eine serviceorientierte Data Protection (SODP) aus. Es automatisiert die Fortführung von Servern, Speichern, Netzwerken und Anwendungen in einem vorgegebenen, koordinierten Prozess. Die Lösung arbeitet dabei laut Hersteller mit fast allen Betriebssystemen, virtuellen Maschinen und Netzwerken. Sie unterstützt die Wiederherstellung in physical-to-physical, physical-to-virtual und virtual-to-virtual Umgebungen. RecoverTrac steht ab sofort als Standardfunktion für FalconStor CDP und FalconStor Network Storage Server (NSS) ohne Preisaufschlag zur Verfügung. *(dr)*

FalconStor: www.falconstor.com

Dezentrale Software-Lager

Aagon erweitert mit **AutoMATE** und der **ACMP-Version 3.8** sein Produktportfolio. Bei AutoMATE handelt es sich um eine **Rekorder-Software**, die alle Eingaben und Einstellungen einer Softwareinstallation und Deinstallation auf einem Testsystem aufzeichnet und daraus ein automatisch ablaufendes Paket erstellt. Dieses Paket lässt sich im Anschluss direkt in das Clientmanagement-System ACMP 3.8 importieren und per Mausklick an beliebige Benutzergruppen verteilen. Dabei kann der Administrator mit Hilfe von AutoMATE auch Menüs, Schaltflächen und sonstige Steuerelemente auf Client-Rechnern bedienen, Listeneinträge lokalisieren und selektieren sowie Programme starten, bedienen und überwachen. **ACMP 3.8** bietet zudem neue **File-Repositories**. Diese lokalen Depot-Server für Installationspakete setzen pro Standort lediglich ein Netzwerklaufwerk voraus und synchronisieren ihre Daten automatisch mit einem zentralen Verteilungs-Repository. Administratoren können die Replikation der Pakete zwischen Depot-Server und Repository manuell und zeitgesteuert anstoßen. Eine weitere Neuerung von ACMP 3.8 ist ein Freigabeprozess für die sogenannten Client Commands. Dabei handelt es sich um Aufgabenskripte, die Administratoren zentral erstellen und über den ACMP-Agenten auf allen Arbeitsstationen im Unternehmen ausführen können. AutoMATE und ACMP 3.8 sind ab sofort verfügbar. Die Preise richten sich jeweils nach der Zahl der Arbeitsstationen. AutoMATE kostet beispielsweise für 100 bis 249 PCs 9,83 Euro pro Arbeitsplatz. Bei ACMP 3.8 liegen die Preise zwischen 39 und 65 Euro pro PC – einschließlich einem Jahr Upgrade-Insurance. *(dr)*

Aagon: www.aagon.de

ACMP 3.8 von Aagon ermöglicht lokale Depot-Server zur Softwareverteilung

Einblick ins Web 2.0

Astaro stellt mit **Application Control, Log Management und Endpoint Security** drei neue IT-Sicherheitslösungen vor. **Application Control** bietet Next Generation Firewall-Funktionen, mit deren Hilfe IT-Administratoren einen besseren Einblick in die allgemeine Internetnutzung erhalten, unerwünschte Anwendungen wie zum Beispiel Facebook blockieren sowie die Internet-Bandbreitennutzung priorisieren können. Administratoren können mit Astaro Application Control kontrollieren, wer welche Anwendungen nutzt, und den Einsatz von nicht arbeitsrelevanten Applikationen einschränken. Das **Log Management** ermöglicht es Nutzern des Astaro Security Gateways, Logdaten von sämtlichen Systemen und Anwendungen zentral zu speichern und zu analysieren. Unternehmen können mit Hilfe von Funktionen zur Fehlerverfolgung und automatischen Benachrichtigungen ihre Fehlerbehebungsdauer laut Hersteller um 80 Prozent reduzieren und Standards wie etwas PCI besser einhalten. **Endpoint Security** schließlich ermöglicht durch Data Leakage Prevention-Funktionen die vollständige Überwachung von USB-Schnittstellen, DVD-Laufwerken und sonstigen Peripheriegeräten. Security Agents werden im lokalen Netzwerk wie auch standortübergreifend verteilt und von einem zentralen Astaro Security Gateway verwaltet. Astaro Endpoint Security bietet umfangreiche Funktionen für das Reporting, mit denen IT-Administratoren jederzeit eine Nutzungsanalyse und Standortbestimmung für sämtliche Geräte durchführen können. Application Control ist als Teil der Astaro Web Security Subscription kostenfrei verfügbar. Zum Log Management und zur Endpoint Security konnte der Hersteller noch keine Preise nennen. Eine ASG 220 für 75 bis 300 User kostet mit Web Security Subscription und Standard-Support 1.430 Euro pro Jahr. *(dr)*

Astaro: www.astaro.com

Pimp your RAID

Drobo erweitert sein Portfolio an **Netzwerkspeichern** für den KMU-Bereich um die **Modelle b800fs, b800i und b1200i.** Die 800er-Variante fasst bis zu acht SATA-Festplatten, während sich das b1200i mit maximal zwölf SATA-, SAS- oder auch SSD-Speicherelementen bestücken lässt. Die Sicherung der Daten erfolgt mit der Technologie "BeyondRAID", die laut Hersteller auf traditionellem RAID basiert, den Festplattenverbund aber um einige neue Funktionalitäten erweitert. So soll es damit zum Beispiel möglich sein, den RAID-Level im laufenden Betrieb ohne Datenverlust beziehungsweise -migration zu ändern oder neue Platten zu einem bestehenden Festplatten-Pool hinzuzufügen. Über eine Thin Provisioning-Funktion kann der Nutzer ferner bis zu 255 Volumes mit einer nominellen Kapazität von 16 TByte bereitstellen. Zu den weiteren Features der Storage-Lösung gehören das Herunterfahren von Festplatten bei Nichtbenutzung sowie die Unterstützung von Jumbo Frames. Während sich das Modell b800fs nur mit den gängigen Dateiprotokollen (CIFS, SMB, AFP) ins Netzwerk einbinden lässt, fungieren die beiden anderen Versionen zusätzlich als iSCSI-Zielserver. Zwei LAN-Anschlüsse mit automatischem Failover sollen für Redundanz sorgen. Die beiden 8-Bay-Varianten sind zu Preisen ab 1.650 Euro ab sofort erhältlich, der NAS-Speicher mit zwölf Einschüben soll im zweiten Quartal 2011 folgen. *(ln)*

Drobo: www.drobo.com

Drobo will bei seinen Netzwerkspeichern, hier das b800fs, die Möglichkeiten traditioneller RAID-Verbünde erweitern

Viele Wege führen zum Server

ATEN bietet mit dem **KN4140v KVM Over the NET** einen **IP-fähigen 40-Port-Switch** an. Der KN4140v ist ein **Cat 5 KVM-Switch** mit Over-IP-Funktionalität, der bis zu fünf simultane Bus-Sessions unterstützt. Über das Login an der lokalen Konsole sowie vier weiteren per LAN, WAN oder eine Internetverbindung können Administratoren zeitgleich auf unterschiedliche Ports dezentraler Netzwerke zugreifen. Per Fernzugriff ist so die Überwachung und Steuerung von bis zu 40 Servern einer Managementebene (inklusive Blade-Server) oder 640 Geräten in einer zweistufigen Kaskadeninstallation möglich. Insgesamt können 64 User-Accounts eingerichtet werden, wobei maximal 32 simultane Logins möglich sind. Durch die redundante Stromzuführung ist die Verfügbarkeit des KN4140v und damit der Zugriff auf das System auch bei Ausfall einer Leitung gewährleistet. "Power Association" ermöglicht die Kopplung mit PDUs (Power Distribution Units) und Powermanagement, so dass angeschlossene Server zentral über die Switch-Schnittstelle ein- und ausgeschaltet werden können. Darüber hinaus können Administratoren die Server mit den Out-of-Band-Verwaltungstools des KN4140v selbst bei einem totalen Netzwerkausfall kontrollieren. Über das CC2000 Control Center Over the NET kann der KN4140v mit anderen IP-fähigen KVM-Switches, seriellen Gerätekonsolen und PDUs in Aggregate Devices (Portgruppen) gebündelt und konsolidiert werden. Der Preis für den Switch beträgt rund 5.580 Euro. *(dr)*

ATEN: www.aten.be

Der KN4140v von ATEN bietet In- und Out-of-Band-Zugriff

Doppelte Speicher-Kontrolle

Ein neues **Doppel-Controller iSCSI-Speicher-Gerät** stellt **American Megatrend International** mit dem **StorTrends 3400i** vor. StorTrends 3400i bietet mit 16 hot-swappable SAS-Festplatten eine Speicher-Kapazität von bis zu 32 TByte. An Bord hat das Gerät die Version 2.8 der StorTrends iTX-Software, die die Ausfallsicherheit des Doppel-Controller-Desings in vollem Umfang unterstützen soll. Die Appliance verbraucht drei Höheneinheiten im Serverrack und ist mit bis zu vier Prozessoren und 8 GByte eigenem Arbeitsspeicher ausgestattet. Durch den doppelten Controller bietet die 3400i echte aktiv/aktiv-Hochverfügbarkeit, die beim Ausfall eines System-Controllers sofort auf den zweiten Controller umschaltet und so Datenverlust vermeiden sowie hohe Verfügbarkeit gewährleisten soll. Besonders interessant gerade in Virtualisierungs-Umgebungen ist die Fähigkeit der Appliance, bis zu 8.048 (read only oder writable) Snapshots zu erzeugen. Dies soll insbesondere die Kosten für Desktopvirtualisierung deutlich senken. Verfügbar ist die StorTrends 3400i ab 20.000 Euro. *(jp)*

American Megatrends International: www.ami.de

Dicke Firewalls für großen Traffic

SonicWALL stellt neben dem bereits genannten CDP 6.0 die **Firewall-Serie SuperMassive E10000** vor. Die Firewalls bieten laut Hersteller eine **hochskalierbare Multicore-Architektur** mit bis zu **96 Cores**. Die SuperMassive-Appliances erzielen bis zu 40 GBit/s Datendurchsatz und mehr als 30 GBit/s für Application Control und Intrusion Prevention. SuperMassive E10100 ist die hoch skalierbare Next Generation Firewall, die als Erste verfügbar sein wird. Die Appliance bietet zwölf Prozessorkerne und weitere zwölf Cores in der integrierten High-Availability-Variante. Das Gerät leistet Deep Paket Inspection, Application Intelligence, Control & Visualization sowie Intrusion Prevention bei einem Durchsatz von 3 GBit/s. Die Appliance SonicWALL SuperMassive E10200 verfügt über 24 Prozessorkerne und erzielt einen Durchsatz von 7,5 GBit/s für Application Control und IPS. Das Modell SuperMassive E10400 verfügt über 48 Prozessorkerne, die einen Durchsatz von bis zu 15 GBit/s für Application Intelligence, Control & Visualization und IPS erreicht. Durch höchste Leistung und maximalen Durchsatz soll sich schließlich das Flagg-schiff der SuperMassive-Serie auszeichnen: die Appliance SonicWALL SuperMassive E10800 mit 96 Cores. Das Gerät bietet bei einem Durchsatz von 30 GBit/s Application Intelligence, Control & Visualization, soll dabei mehrere tausend Anwendungen erkennen und gleichzeitig Intrusion Prevention leisten. Dabei lassen sich die sechs 10 GBit/s-SFP+-Ports und die 16 GBit/s-SFP-Ports je nach Anforderung kombinieren. SonicWALL SuperMassive E10100 ist ab dem zweiten Quartal 2011 erhältlich. Die Produkte SuperMassive E10200, E10400 und E10800 stehen ab dem dritten Quartal 2011 zur Verfügung. Das Modell E10100 ist ab 140.000 Euro verfügbar. *(dr)*

SonicWALL: www.sonicwall.com/de

Die Firewall-Appliance SuperMassive E10800 von SonicWALL verfügt über 96 CPU-Kerne

Virtuelles Auge

Mit **vCenter Operations** stellt VMware ein Tool zur **Leistungs-, Kapazitäts- und Konfigurationsanalyse** in virtualisierten Umgebungen vor. Integrierbar in VMware vSphere-Umgebungen, erkennt und analysiert vCenter Operations die Daten der zugrundeliegenden physikalischen Komponenten (Server, Storage, Netzwerk) und anderer Management-Tools. Die daraus resultierenden Informationen sollen anschließend dem Nutzer in Form von konkreten Handlungsweisungen auf Anzeigetafeln anschaulich dargestellt werden. So will der Hersteller gewährleisten, dass Service Level in Cloud-Umgebungen durch die Abbildung der Performance und des Gesundheitszustands der IT-Umgebung in Echtzeit eingehalten werden. Zudem verspricht das Werkzeug eine schnellere Problemfindung in der Virtualisierungs-Infrastruktur. Durch die Performance- und Kapazitätsanalyse soll das IT-Personal jederzeit über die Auslastung und Bedarfsanforderungen der Systeme informiert sein und so bei Bedarf sofort Entscheidungen über neue, notwendige Installationen treffen können. Und auch die Einhaltung von Compliance bei veränderten Rahmenbedingungen soll vCenter Operations durch die automatische Erkennung von Konfigurationsänderungen gewährleisten. Die Software ist ab 50 US-Dollar pro virtueller Maschine zu haben. *(jp)*

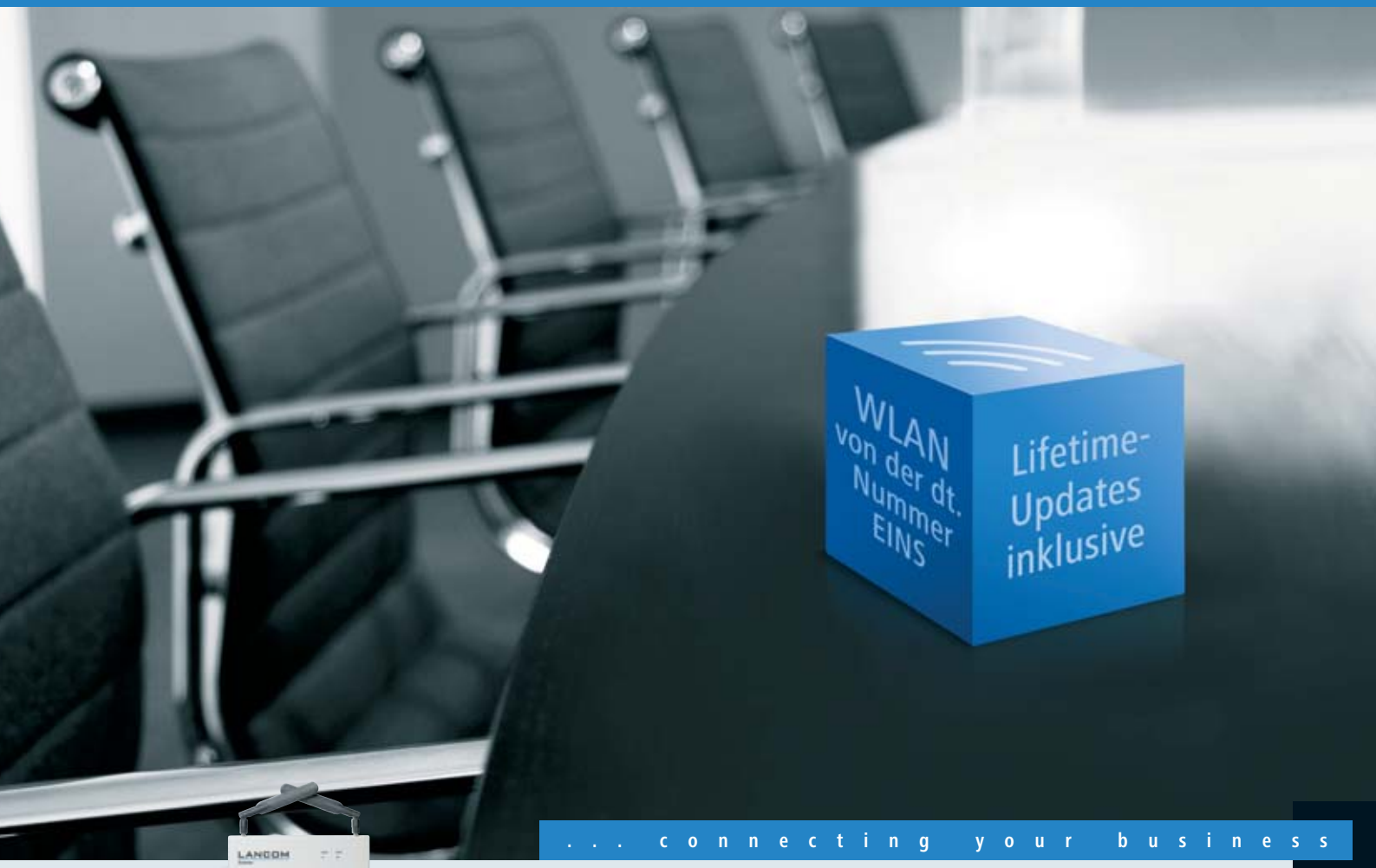
VMware: www.vmware.de

Schlanke Schnellstarter

IGEL Technology präsentiert eine neue Gerätegeneration seiner Einstiegs- und Allroundmodelle **IGEL UD2** und **UD3**. Dank neuer **VIA-Prozessoren** booten die Universal Desktop Thin Clients (UD) schneller und sollen bis zu 44 Prozent mehr Leistung als die Vorgängermodelle bieten. Der IGEL UD3 mit dem VIA Nano-Prozessor VX 855 unterstützt GBit-LAN und weist einen geringeren Stromverbrauch auf. So soll das Gerät 10 Watt im Betrieb (Idle) beziehungsweise 1 Watt im Standby (Sleep) verbrauchen. Für die Videowiedergabe bietet das Modell UD3 einen DVI-I-Anschluss mit einer maximalen Bildschirmauflösung von 1.920 x 1.200 Punkten. Über ein optionales Y-Kabel ist ein zweiter VGA-Monitor anschließbar. Für den Anschluss von Peripheriegeräten besitzt der UD3 insgesamt fünf USB 2.0-Ports, je eine PS2- und eine serielle Schnittstelle sowie Audio-In und Audio-Out. Beide Thin Client-Modelle sind mit unterschiedlichen Betriebssystemen und Firmware-Paketen erhältlich. Die Linux-basierten Modelle unterstützen dabei die neue Protokollerweiterung RemoteFX für Microsoft VDI. Der UD3 ist je nach Betriebssystem und Firmwarepaket ab 353 Euro zu haben, der IGEL UD2 ab 237 Euro. Das Modell UD3 bietet IGEL dabei wahlweise mit IGEL Linux oder Windows Embedded Standard an. Der IGEL UD2 ist zudem mit Windows CE erhältlich. *(dr)*

IGEL: www.igel.com

Der Thin Client UD3 von IGEL soll nur 1 Watt Strom im Schlafmodus verbrauchen



. . . connecting your business

Made
in
Germany

WLAN mit Hochverfügbar-keitsgarantie? Von LANCOM!

Mit der LANCOM Smart Controller-Architektur sorgen wir für maximale Ausfallsicherheit im WLAN: was immer passiert, das Funknetz steht weiter zur Verfügung.

Davon profitieren kleine WLANs genauso wie Netze mit Tausenden von Access Points, der Hotspot genauso wie die Installation im Freien. Und: Wireless LANs von LANCOM skalieren perfekt – so wächst Ihr Netz ganz einfach mit Ihren Bedürfnissen.

Setzen auch Sie auf WLAN von der deutschen Nummer EINS! Exzellenter Service, kostenlose Updates & Investitionsschutz inklusive.

LANCOM
Systems

IT-Administrator Workshop "Update Virtualisierung 2011"

ITANet Workshop-Partner:

IT-Administrator Trainings-Partner:

Global Knowledge

Dranbleiben!

von John Pardey

Die Server-Virtualisierung tritt nach großen Erfolgen bei der Konsolidierung der Rechenzentren in eine neue Phase: Management, Monitoring und Netzwerkanbindung rücken in den Fokus der IT-Verantwortlichen. Gleichzeitig sind die Entwicklungen in der Desktop-Virtualisierung so rasant vorangeschritten, dass sich diese Technologie aufmacht, ihre Nische zu verlassen. Unsere Workshops im Frühsommer in Frankfurt und Leipzig bringen Sie auf den aktuellen Stand der Virtualisierung.

Das Versprechen der ersten Welle der Server-Virtualisierung, die Hardware-Infrastruktur zu konsolidieren und so erheblich die Kosten zu reduzieren, setzten viele IT-Verantwortliche erfolgreich in die Praxis um. Parallel dazu entwickelten zahllose Hersteller neue Produkte, um Storage, Netzwerk oder auch Clients mit ähnlichen Resultaten zu virtualisieren.

Aktuelle Herausforderungen der Virtualisierung

Vielfach übersehen wird dabei, dass die Virtualisierung von x86-Servern noch eine sehr junge Technologie ist. Mit wachsender Komplexität zeigten sich erste Kinderkrankheiten. So ist das Monitoring solcher Server oft unvollständig und die Verwendung von virtuellen Switchen birgt Sicherheitsrisiken. In unserem Workshop greift Dozent Nico Lüdemann diese Themen auf und stellt dar, in welche Richtung aktuelle Lösungsansätze für diese Probleme gehen. Dabei thematisiert er auch den weit verbreiteten parallelen Betrieb physikalischer und virtueller Server und dessen spezielle Herausforderungen.

Besonders verlockend scheint die Virtualisierung in Sachen Desktop, denn die schlichte Masse an Rechnern an den Arbeitsplätzen lässt auf besonders hohe Einsparpotentiale schließen. Zudem eröffnen sich Wege, um die ärgerlichen Dauerbrenner Patchmanagement, Softwareverteilung oder Geräteunabhängigkeit in den Griff zu bekommen. Der Workshop stellt den Teilnehmern den aktuellen Stand der Technologie dar und will aufzeigen, welche Wege der Client-Virtualisierung sich für welchen Einsatzzweck eignet. Außerdem stellt er den potentiellen Einsparungen die zu erwartenden Kosten gegenüber. Abschließend werfen wir noch einen Blick auf den aktuellen Stand des Client-Managements in diesem Umfeld.

Zwei Termine zur Auswahl

Für alle IT-Verantwortlichen, die Virtualisierung am Server oder Client betreuen, bietet unser Workshop ein Update neuer Erkenntnisse und Möglichkeiten. Neu ist ab 2011 auch, dass wir jeden Workshop an zwei Terminen anbieten. Die beiden inhaltlich identischen Workshops finden diesmal am 8. Juni in Frankfurt und am 7. Juli in Leipzig statt. Alle Informationen zur Anmeldung und zum Workshop finden Sie im Kasten "Workshop Update Virtualisierung 2011". Die Anmeldung ist jeweils bis eine Woche vor dem Workshop-Termin möglich. Wir würden uns freuen, Sie begrüßen zu dürfen.

ITANet
Die System und Netzwerk User Group

Die Agenda des Workshops

13.00 Uhr: Begrüßung

13.15 Uhr: Server-Virtualisierung aktuell

- Herausforderung Management: Blinde Flecken des Monitorings und neue Werkzeuge für die Verwaltung virtualisierter Server
- Abschied vom virtuellen Switch: Neue Wege der Anbindung virtueller Maschinen an das Netzwerk
- Gemeinsame Verwaltung physikalischer und virtueller Server: Stolperfallen, Methoden, Tools

Dozent: Nico Lüdemann

14.45 Uhr: Pause

15.00 Uhr: Partnervortrag:
Veeam Backup – mehr als nur Backup

Dozent: Dirk Hannemann (Frankfurt)
Matthias Frühauf (Leipzig)

15.45 Uhr: Pause

16.00 Uhr: Desktop-Virtualisierung aktuell

- Virtuelle Applikationen versus gehosteter Desktop
- Lokale Virtualisierung für mobile Anwender
- Vor- und Nachteile, Kosten
- Wie passt das alles ins Client-Management?

Dozent: Nico Lüdemann

17.30 Uhr: Ende der Veranstaltung

Ort

8.Juni 2011, Frankfurt/M.:
Global Knowledge Germany Training GmbH,
Hungener Straße 6, 60389 Frankfurt

7. Juli 2011, Leipzig:
Commundo Tagungshotel Leipzig,
Zschochersche Straße 69, 04229 Leipzig

Teilnahmegebühren

Für IT-Administrator-Abonnenten kostenlos. Haben Sie ein Abonnement des IT-Administrator und möchten einen Kollegen mitbringen, erheben wir für den zweiten Teilnehmer eine Schutzgebühr von Euro 75,- (zzgl. 19% MwSt.). Verfügt Ihr Unternehmen über kein Abonnement, wird eine Schutzgebühr von Euro 145,- (zzgl. 19% MwSt.) fällig.

Anmeldung bis zum 1. Juni (Frankfurt/M.) beziehungsweise 1. Juli (Leipzig) unter
www.it-administrator.de/workshops/

Workshop Update Virtualisierung 2011

Überarbeitete Punktevergabe in den Produkttests

Mehr Klarheit

von John Pardey

Seit der Einführung unserer Bewertungskästen für die Produkttests kommen immer wieder Leser mit Fragen bezüglich der Punktevergabe auf uns zu: Was bedeuten eigentlich sieben Punkte? Wie kommt die Höhe der Punktvergabe zustande? Wie sieht es mit der Vergleichbarkeit aus? Und woraus ergeben sich eigentlich die fünf Kategorien, nach denen bewertet wird? So verdichtete sich in der Redaktion im Laufe der Zeit der Verdacht, dass die Bewertungen für den Leser transparenter und einheitlicher gestaltet werden müssen. Gemeinsam mit unseren externen Testlabors überarbeiteten wir die Bewertungsmaßstäbe für noch mehr Klarheit bei unseren Testergebnissen.

Den Abschluss eines jeden Tests im IT-Administrator bildet der Bewertungskasten, der dem Leser auf einen Blick die Leistungsfähigkeit, aber auch Einsatzgebiete und – nie zu vernachlässigen – die zu erwartenden Kosten einer Beschaffung auf einen Blick darstellen soll.

Was die fünf Bewertungskriterien bedeuten

Während die Informationen zu Produktart, Hersteller und Preis in der Regel völlig eindeutig sind, variieren unsere Bewertungs-Kästen zunächst bei den jeweils fünf Produkteigenschaften. Hier legen wir Wert darauf – und dies gilt nach wie vor –, dass das Testlabor die fünf Features des getesteten Produkts auswählt, die für die Funktionalität des Produkts entscheidend sind. Als einfaches Beispiel lässt sich hier anführen, dass bei einer Backup-Software ganz gewiss die Handhabung und die Umsetzung der Sicherungs- und Rücksicherungsfunktion in der Bewertung zu berücksichtigen sind. Verallgemeinernd ausgedrückt, bewertet das Testlabor die fünf Produkteigenschaften, die ein potentieller Käufer als zentral betrachtet.

Dies war in der Vergangenheit so und wird von der Redaktion und den Testlabors auch zukünftig so gehandhabt werden. Einzig Kriterien wie etwa "Installation" oder "Dokumentation" – die in der Vergangenheit des Öfteren ihren Weg in die fünf Bewertungen fanden – werden zukünftig dort nur noch auftauchen, wenn ihre Umsetzung entscheidenden Einfluss auf die Funktionalität des getesteten Produkts hat. So werden Sie etwa den Punkt "Dokumentation" dort nur noch finden, wenn es sich um ein außergewöhnlich komplexes Produkt handelt, bei dem der Benutzer ohne eine Dokumentation mehr oder weniger aufgeschmissen ist.

Was die Höhe der Punktevergabe bedeutet

Etwas weniger einheitlich war bisher zugegebenermaßen die Höhe der vergebenen Punkte in den fünf Kategorien. Wie eingangs erwähnt, haben wir hier zusammen mit unseren Testlabors nun eine einheitliche Skala entwickelt, die ab dieser Ausgabe zum Einsatz kommt und für alle Produkttester verbindlich ist. Diese neue Skala entnehmen Sie der Tabelle auf dieser Seite. Wichtig für Sie als Leser ist dabei, dass mit der Einführung der neuen Skala die durchschnittlichen Bewertungen zukünftig niedriger ausfallen. An die Top-Bewertungen 9 und 10 legen wir ab sofort deutlich höhere Maßstäbe an und die Bewertung eines Features, das einwandfrei funktioniert, ist ab sofort eine 6, während dies in der Vergangenheit eher eine 7 oder 8 war. Wir hoffen, dass die Tests für Sie so eindeutiger und nachvollziehbarer werden. Bei Fragen senden Sie uns gern eine E-Mail an redaktion@it-administrator.de.

Bedeutung der Punkte in den Tests

Punkte	Bedeutung
0	Feature nicht vorhanden
1	Feature nur rudimentär vorhanden beziehungsweise Feature funktioniert nicht
2	Feature entspricht nicht dem aktuellen Standard und/oder funktioniert mangelhaft
3	Feature entspricht deutlich nicht dem aktuellen Standard, funktioniert aber
4	Feature entspricht dem Standard, hat aber deutliche Mängel in der Umsetzung
5	Feature entspricht dem Standard, hat aber leichte Mängel in der Umsetzung
6	Feature entspricht dem Standard vergleichbarer Produkte und funktioniert einwandfrei
7	Feature ist dem Standard leicht überlegen
8	Feature ist dem Standard deutlich überlegen
9	Feature ist vollkommen neu / technologisch vergleichbaren Produkten weit überlegen – funktioniert aber nur mit leichten Einschränkungen
10	Feature ist vollkommen neu / technologisch vergleichbaren Produkten weit überlegen und funktioniert einwandfrei

Im Test: Veeam Backup & Replication 5.0

Backup mit Funktions-Check

von Jürgen Heyer

Routinierte Administratoren wissen, dass eine Datensicherung, bei der nie die zugehörige Wiederherstellung getestet wurde, womöglich nicht viel wert ist. Zeigt sich erst im Ernstfall, dass die gesicherten Daten unvollständig oder inkonsistent sind oder unter Umständen die Rücksicherung gar nicht funktioniert, ist großer Ärger programmiert. Was liegt also näher, als eine Funktionsprüfung gleich in den Sicherungsjob zu integrieren? IT-Administrator hat sich genauer angesehen, wie dies beim neuen Backup & Replication 5.0 von Veeam funktioniert.

Unter Administratoren kursieren immer wieder Geschichten von mehr oder weniger unerfahrenen Kollegen, die jahrelang ihrer Datensicherung vertrauten und erst bei einem größeren Datenverlust schmerzhaft erfahren mussten, dass ihre Backups unvollständig oder anderweitig nicht konsistent waren. Umso schwerer wiegt, dass der Hauptgrund oftmals darin bestand, dass zwar die Ausführung des Sicherungsjobs kontrolliert, aber die Rücksicherung und deren Ergebnis nie auf Funktionstüchtigkeit getestet wurde. Tatsächlich ist es sehr wichtig, auf eine korrekte Vorgehensweise zu achten, wenn nicht nur normale Datenbestände, sondern Datenbanken, E-Mailsysteme wie ein Exchange-Server oder auch Domänencontroller gesichert werden.

Zur Backup-Software gehörige Agenten auf den zu sichernden Systemen helfen hier, die Datenbestände konsistent zu sichern. Etwas komplizierter wird es, wenn Applikationen in virtuellen Maschinen laufen und die Daten nicht über eine auf der VM installierten Backup-Software gesichert werden sollen, sondern Ressourcen-sparender über einen externen Backup-Server, der die virtuelle Landschaft im Zugriff hat. Dann kommen bei der Sicherung noch mehr Komponenten ins Spiel, die korrekt miteinander agieren müssen.

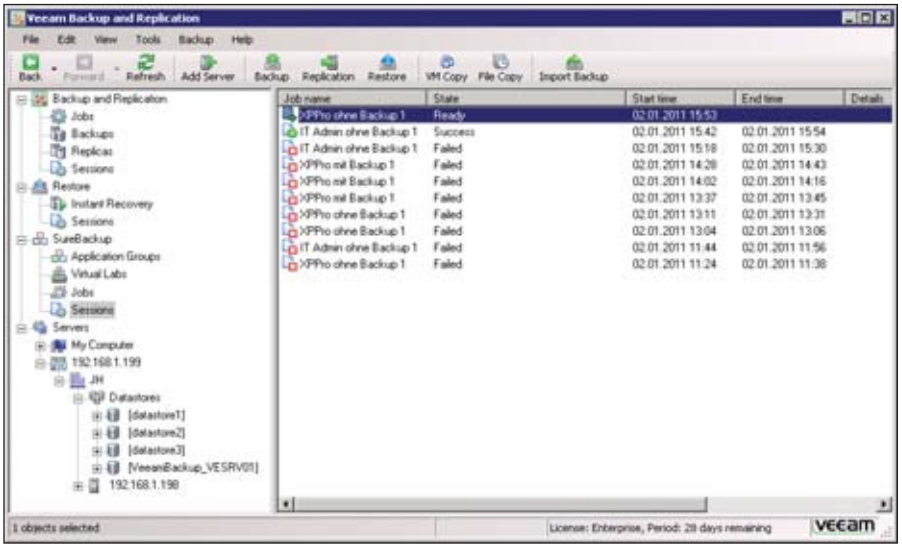


Bild 1: Die Hauptansicht der B&R-Administrationskonsole ist sehr übersichtlich aufgebaut und intuitiv bedienbar

Um zu prüfen, ob die erstellten Backups brauchbar sind, ist es letztendlich die beste Lösung, die Ergebnisse regelmäßig durch Tests zu verifizieren, was allerdings manuell recht aufwändig ist. Um beispielsweise komplette, gesicherte VMs zu testen, ist eine entsprechend vorbereitete Umgebung notwendig, da ein Einspielen in die Produktion Namens- und IP-Adresskonflikte erzeugen würde. Der auf Datensicherung und Management virtueller Umgebungen unter VMware spezialisierte Softwarehersteller Veeam bietet nun mit der neuen Version Backup & Replication 5.0 (im Weiteren B&R genannt) genau hierfür eine Lösung an.

Direkter Start von Backup-Dateien

Mit einer speziellen, zum Patent angemeldeten Technik namens vPower startet die Software eine oder auch mehrere VMs direkt aus den Backup-Dateien in einer isolierten Umgebung (Sandbox-Verfahren), um so die Funktionsfähigkeit automatisch zu verifizieren oder auch dem Administrator die Möglichkeit zu geben, manuell eigene Tests durchzuführen. Die Sicherungsdateien werden dabei nur gelesen und somit durch diesen Test nicht verändert. Weiterhin ist es möglich, eine gesicherte VM nicht nur isoliert laufen zu lassen, sondern optional auch mit dem Produktionsnetz zu verbinden. Und falls eine produktive VM

komplett ausfällt, kann B&R mittels vPower eine vorhandene Sicherungsdatei ohne vorherigen Restore als VM registrieren und starten, damit diese in kürzester Zeit die Aufgabe der ausgefallenen VM übernimmt. Auf diese Weise wird der Backup-Pool quasi zu einem weiteren Standort für VMs.

Ausreichend Rechenleistung ist gefragt

Veeam empfiehlt für den Backup-Server eine Hardware mit mindestens vier Cores und 1 GByte RAM beziehungsweise 2 GByte, wenn die SQL-Verwaltungsdatenbank mit auf dem System installiert wird. Im Test wurde schnell sichtbar, dass die Performance mit der Prozessorleistung steigt und fällt, so dass der Server vor allem beim gleichzeitigen Sichern mehrerer Systeme großzügig bemessen werden sollte. Für die Netzwerkanbindung ist mindestens GBit-Ethernet erforderlich, besser noch ist eine komplette SAN-Integration. Bei den Betriebssystemen können wahlweise 32- und 64-Bit-Versionen von Windows XP, Vista, 7, 2003, 2008 und 2008 R2 verwendet werden. Es ist durchaus möglich, den Sicherungsserver zu virtualisieren, die genannten Leistungsdaten sollten aber auch dann berücksichtigt werden.

Für den Test installierten wir B&R in der Enterprise-Version in einer VM unter Windows 2008 R2 und nutzten als Datenbank Microsoft SQL Server 2005 Express, die automatisch mit eingerichtet wird, wenn der Administrator keine schon vorhandene Datenbank angibt. Zusätzlich installierten wir den optionalen Backup Enterprise-Manager, eine Web-Anwendung, die als gemeinsame Verwaltungskonsole dient, wenn mehrere B&R-Sicherungsserver betrieben werden sollen. Außerdem sind über diesen Manager sogenannte AIR-Rücksicherungen, auf die wir weiter unten eingehen werden, zu genehmigen.

Neben der Sicherung und Wiederherstellung ganzer VMs oder zumindest kompletter VMDK-Dateien ermöglicht B&R auch eine Wiederherstellung einzelner Dateien aus einem Backup. Falls dies in größerem Maße genutzt werden sollte, ist es sinnvoll, den Veeam Backup Search Server zur Dateiindizierung einzusetzen. Dieser setzt auf dem Microsoft Search Server auf und erfordert als Basis einen Search Server 2008/2010, wahlweise auch in der Express-Edition. Hinsichtlich der ESX-Plattform werden vSphere 4 und VM ware Infrastructure 3 mit ESX(i)3.x/4.x unterstützt. Für den Test nutzten wir einen Host unter ESX4i in Verbindung mit einem vCenter Server 4.x.

Reibungslose Installation

Die Installation von B&R inklusive Enterprise Manager verlief problemlos. Im Test nutzten wir die mitgelieferte SQL 2005 Express-Datenbank, die samt der benötigten Datenbankinstanz automatisch mit eingerichtet wurde. Im Laufe der Installation fragte B&R die zu nutzenden Ports ab, wobei wir die Standardvorgaben übernahmen. Weiterhin benötigte die Backup-Software die Anmeldeinformationen, um auf den SQL-Server und das so genannte "VBR Catalog"-Verzeichnis mit den Indexdateien zugreifen zu können. Wichtig ist zudem, dass eine geeignete Lizenzdatei vorhanden ist, sonst ist die Installation nicht möglich. Für Tests bietet Veeam Trial-Lizenzen für 30 Tage an, auf Nachfrage auch 90-Tage-Lizenzen.

Nach Abschluss der Installation standen uns zwei Benutzeroberflächen zur Verfügung, die Administrationskonsole für die lokale Installation sowie die Web-GUI des Enterprise Manager. Zu beachten ist, dass der Enterprise Manager in erster Linie eine übergreifende Verwaltungsaufgabe hat, aber nicht dazu gedacht ist, beispielsweise einzelne Aufträge anzulegen. Dies erfolgt stets über die Administrationskonsole der jeweiligen B&R-Installation. Hier sind zur weiteren Einrichtung auch die Server anzugeben, mit denen B&R kommunizieren soll. Ist ein vCenter Server im Einsatz, empfiehlt Veeam, dessen Adresse und Credentials aufzunehmen, statt die einzelnen ESX(i)-Hosts einzutragen. Handelt es sich um ESX-Server, fragt B&R optional auch die SSH-Einstellungen der Service-Konsole ab. Außerdem sind die Daten der Linux-Server anzugeben, die eventuell für Sicherungs- oder Replizierungsjobs genutzt werden sollen.

Ist dies erledigt, sind in der Konsole alle erfassten Systeme, die darin befindlichen Datastores sowie die Zuordnung zu einem vCenter aufgelistet. Die Administrationskonsole ist ähnlich wie der Windows Explorer zweispaltig aufgebaut mit einer hierarchischen Menüansicht in der linken Spalte. Der Administrator kann hier die Datastores durchsuchen und sich deren Inhalte ansehen. Es lassen sich auch einzelne Dateien öffnen, um beispielsweise via Editor die Log-Informationen einzusehen. Insgesamt ist die Konsole sehr übersichtlich aufgebaut und intuitiv bedienbar.

Sicherungskonzepte in Hülle und Fülle

Beim ersten Studium der Datenblätter und der Dokumentation wird der Administrator mit einer Vielzahl an mehr oder weniger neuen Begriffen und Namenskreationen wie Surebackup, Replication, AIR, Instant Recovery, VM Copy, File Copy, Virtual Lab, Reverse Incremental und Full Synthetic Backup konfrontiert, die letztendlich auf unterschiedlichste Sicherungs- und Wiederherstellungsverfahren schließen lassen. Doch nach anfänglicher Ver-

Systemvoraussetzungen

VMware vSphere 4.x oder Infrastructure 3.x (VI3) mit Hosts unter ESX(i) 3.x/4.x als Umgebung für zu sichernde virtuelle Maschinen.

Veeam Backup-Server: Quad-Core CPU, 2 GByte Hauptspeicher, GBit-Netzwerkkarte, Windows XP SP3/Vista SP2/7/2003 SP2/2008 SP2, 2008 R2, MS SQL Server 2005/2008 inklusive Express-Version, .NET-Framework 2.0 SP1, PowerShell 2.0.

Mögliche Speicherziele für Sicherungen: SAN via HBA oder iSCSI, direkt angebunden an den Backup-Server, NAS-Systeme mit CIFS (direkt) oder NFS-Freigabe (gemountet an einem ESX-Host oder Linux Server), DAS (Direct Attached Storage) inklusive USB-Platten am Backup-Server, Server unter Windows (via CIFS), Linux, ESX 3.x/4.x (via Agent).

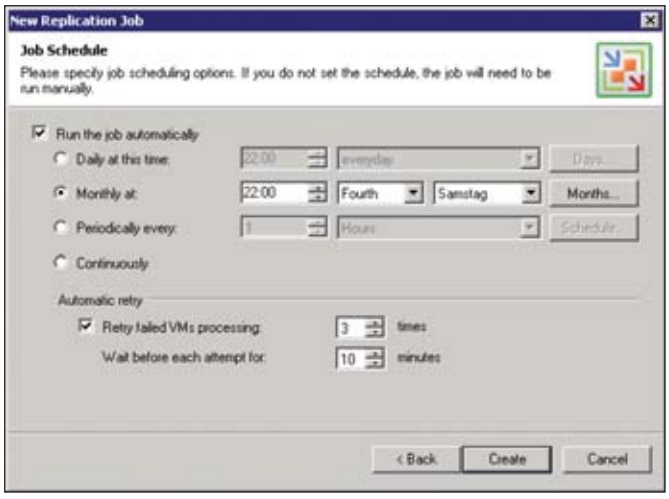


Bild 2: Ein komfortabler Zeitplaner ermöglicht eine gute Automatisierung von Sicherungs- und Replikationsaufträgen

wirrung und daraus resultierender eingehender Beschäftigung mit den Funktionen stellte sich zumindest in unserem Test der erlösende Aha-Effekt ein. So ergeben alle Features durchaus einen Sinn. Bereits bei der Datensicherung wird die Vielfalt ersichtlich: Hier stehen insgesamt vier Möglichkeiten zur Verfügung, genannt Backup, File Copy, VM Copy und Replication.

Backup

Die am häufigsten genutzte Funktion dürfte das normale Backup sein, um letzten Endes virtuelle Maschinen zu sichern. B&R unterstützt hierfür drei verschiedene Sicherungswege, wobei deren Nutzung davon abhängt, in welcher Umgebung der Backup-Server konfiguriert ist. Bei "Direct SAN Access" müssen die VMs auf SAN-Speicher laufen und auch der Backup-Server benötigt eine SAN-Anbindung. Dies ermöglicht Sicherungen mittels vStorage-API, ohne das LAN zu belasten (LAN-less Backup). Im Test verwendeten wir den Modus "Virtual Appliance". Dieser setzt voraus, dass B&R selbst auf einer VM installiert ist, damit die Software den ESX I/O Stack nutzen kann. Die Option "Network" letztendlich ist dann zu wählen, wenn nur das LAN als Transportweg genutzt werden kann. Hierbei nutzt Veeam das NBD-(Network Block Device)-Protokoll. B&R versucht übrigens stets, den vom Administrator vorgegebenen Weg zu nutzen, führt aber standardmäßig einen Failover auf den Netzwerkmodus durch, falls die anderen Modi fehlschlagen. Auf Wunsch lässt sich der Datenverkehr im Netzwerk auch verschlüsseln.

Ein Backup-Job kann gleichzeitig unterschiedliche Objekte sichern, also VMs, Ressourcen-Pools, Datastores oder auch ein komplettes vCenter, wobei sich innerhalb der Objekte zusätzlich Ausschlüsse definieren lassen. Ein Administrator kann beispielsweise einen Ressourcen-Pool sichern, aber darin wiederum eine VM oder auch innerhalb einer VM einzelne Platten ausklammern. Insgesamt haben uns die sehr flexiblen Auswahlmöglichkeiten gut gefallen. Von Vorteil ist auch, dass B&R bei jeder Änderung sofort berechnet, wie groß die resultierende, zu sichernde Datenmenge ist.

Als Ziel können alle Geräte genutzt werden, die in der Konsole erfasst wurden – allerdings keine ESXi-Server. Eine Schaltfläche zur Kapazitätsprüfung verrät dem Administrator sofort, ob auf dem Ziel ausreichend Platz für die ausgewählte Datenmenge vorhanden ist. Innerhalb der erweiterten Funktionen hat der Administrator noch diverse Anpassungsmöglichkeiten hinsichtlich Sicherungsverfahren und Platzsparmaßnahmen, die wir weiter unten beschreiben.

Sofern VMs der Hardware-Version 7 zum Einsatz kommen (Standard ab ESX 4 und Workstation 6.5), wird per Default die CBT-Funktion (Changed Block Tracking) von vSphere genutzt, wodurch sich die inkrementell zu sichernden Blöcke schneller ermitteln lassen. Bei Windows-VMs kann der Administrator VSS aktivieren und das Dateisystem innerhalb der VM indizieren lassen, um darin nach Dateien suchen zu können. Diese Funktion ist aber rein optional und nicht notwendig, um einzelne Dateien aus einer VM-Sicherung wiederherzustellen. Falls in bestimmten Konstellationen bei Windows-Systemen VSS nicht möglich ist oder es anderweitig notwendig wird, lässt sich auch das VMware-Tool Quiescence nutzen. Weiterhin hat der Administrator die Möglichkeit, zum Abschluss einer Sicherung einen Post-Job zu starten und sich per SNMP benachrichtigen zu lassen.

VM Copy

Mit dieser Funktion wird der Inhalt nicht in eine Backup-Datei geschrieben, sondern Kopien erzeugt. Ansonsten stehen die gleichen Optionen zur Verfügung wie beim Backup. Außerdem lässt sich als Ziel auch ein ESXi-Server angeben.

File Copy

Über File Copy lassen sich komplette Verzeichnisse kopieren. Als Quelle und Ziel können alle Systeme angegeben werden, die in der Konsole erfasst wurden. Die Funktion greift auf Datastores ebenso zu wie auf andere Laufwerke der erfassten Server. Damit ist es beispielsweise ein Leichtes, vorbereitete ISO-Dateien für etwaige Installationen von einer Freigabe, die vom Backup-Server aus erreichbar ist, auf einen Datastore eines ESX-Servers zu übertragen. Alle beschriebenen Jobs können über einen integrierten Zeitplaner täglich, monatlich an einem bestimmten Tag, periodisch oder auch kontinuierlich wiederholt werden. Bei einem Fehler lässt sich ein Job mit einer definierbaren Anzahl an Versuchen in bestimmbaren Abständen wiederholen. In diesem Zusammenhang kann der Administrator auch vorgeben, wie viele Versionen gespeichert werden sollen, damit der Platzbedarf nicht kontinuierlich wächst, sondern der Job auch selbst aufräumt.

Doppelte Sicherheit durch Replizierung

Ein besonderes Sicherungsverfahren ist die Replizierung, bei der eine oder mehrere VMs von einem ESX-Server auf einen anderen kopiert werden. Der Job ist weitgehend identisch zur Aufgabe "VM Copy",

nur wird als Ziel zwingend ein Datastore auf einem ESX(i)-Server verlangt. Ziel der Replizierung ist das Vorhalten von Kopien produktiver VMs auf einem anderen ESX-Server, um bei einem Ausfall der primären Seite möglichst schnell die Replik in Betrieb nehmen zu können. Aus diesem Grund bekommt die Replik einen anderen Namen, standardmäßig wird "_replica" angehängt. Außerdem wird diese Kopie auf dem Ziel-ESX-Server automatisch registriert, damit sie sich jederzeit starten lässt. Bei "VM Copy" wird weder umbenannt noch registriert.

Es ist möglich, die erste Replizierung über ein anderes Medium wie einen Wechseldatenträger durchzuführen (sinnvoll bei einer Replizierung über eine langsame WAN-Strecke). Indem der Scheduler auf kontinuierliche Replizierung eingestellt ist, werden alle Änderungen möglichst zeitnah übertragen und die Kopie entspricht fast dem Original. Veeam spricht hier von Near-CDP (Continuous Data Protection) beziehungsweise SmartCDP. Mit der Replizierung stellt Veeam letztendlich ein sehr sinnvolles Werkzeug zur Verfügung, um eine Disaster Recovery-taugliche Umgebung zu schaffen, falls nicht andere Mechanismen wie Echtzeit-Replikation oder Hardware-basierende Snapshots zum Einsatz kommen, so dass auch größere Ausfälle die Produktion nicht übermäßig beeinträchtigen.

Virtuelle Sandkastenspiele

Zum Patent angemeldet hat Veeam unter anderem die beiden ähnlich funktionierenden Verfahren Surebackup und Instant VM Recovery. Surebackup adressiert das generelle Problem der Konsistenzprüfung durchgeführter Sicherungen. Was liegt bei einer virtuellen Maschine näher, als aus den Sicherungsdaten heraus die VM zu starten und zu testen, ob alle Funktionen korrekt arbeiten? Genau diesen Prozess hat Veeam in B&R mit Surebackup automatisiert. Damit dies funktioniert, sind allerdings einige vorbereitende Maßnahmen erforderlich, denn es muss eine Sandbox in Form eines virtuellen Labors (Virtual Lab) als isolierte Arbeitsumgebung für den Start der VMs gebaut werden. Diese Sandbox schottet die darin laufenden VMs vor der Produktionsumgebung ab, damit es zu keinen Konflikten kommt. Zugleich simuliert sie nach innen die Produktionsumgebung, damit die darin gestarteten VMs mit ihren ursprünglichen IP-Adressen laufen können und letztendlich keinen Unterschied sehen. Da es oft nicht möglich ist, nur eine VM für sich funktionsmäßig zu prüfen, ist zuerst eine Applikationsgruppe anzulegen, die auch aus mehreren VMs bestehen kann, um beispielsweise eine kleine Umgebung mit Domänencontroller, DNS- und Datenbankserver sowie den eigentlichen Applikationsservern nachzubilden. Die Funktionsprüfung kann mittels entsprechender Testskripte automatisiert werden, wobei B&R vorbereitete Skripte für DNS-, Mail-, SQL- und Webserver sowie Domain Controller und Global Catalog mitliefert. Der Administrator kann innerhalb der Applikationsgruppe die Startreihenfolge festlegen und auch eine Startverzögerung vorgeben, um Abhängigkeiten zu berücksichtigen.

Als Nächstes ist ein Virtual Lab zu definieren, das als Ressourcen-Pool abgebildet wird. Standardmäßig legt B&R darin eine Proxy-Appliance an, eine kleine, automatisch konfigurierte Linux-VM. Sie er-

möglicht es B&R, mit den in der Sandbox laufenden VMs zu kommunizieren und die Skripte zu starten. Dadurch sind die VMs per NAT vom Backup-Server aus erreichbar, bei Eintragungen entsprechender Routen auch von anderen Systemen im Produktionsnetz. Für spezielle Zwecke ist es zudem möglich, eine VM in der Sandbox über ein statisches Mapping in der Produktion auch ohne das Eintragen von Routen erreichbar zu machen. Beim Austesten dieser Funktion stellten wir allerdings in der Proxy-Konfiguration einen kleinen Fehler fest. Dieser führte dazu, dass die interne Prüfung beim Starten der VMs in der Sandbox auf einen Fehler lief, weil der Ping-Test nicht klappte. Obwohl wir im Test ein Class-C-Netz verwendeten, wurde bei der automatischen Konfiguration eine Class-B-Maske eingetragen. Indem wir die virtuelle Netzwerkkarte der Proxy-Appliance manuell konfigurierten, konnten wir diesen Bug umgehen.

Wichtig ist in diesem Zusammenhang auch, dass die VMs vor allem bei Verwendung von Windows 2008 als Gastbetriebssystem mit VMXNET2-Netzwerkkarten konfiguriert sein müssen, damit die Adapter auch im Virtual Lab richtig arbeiten. Bei einer VM, die wir in unserem Test mit einem E1000-Adapter konfigurierten, mussten wir feststellen, dass beim Hochfahren im Virtual Lab die Netzwerkerkennung deaktiviert war, obwohl wir diese in der Produktions-VM aktiviert hatten. Das führte wiederum dazu, dass der Ping-Test nicht klappte und das Virtual Lab aufgrund dieses Fehlers gestoppt wurde. Bei Verwendung eines VMXNET3-Adapters läuft die VM im Virtual Lab mit einer anderen IP-Adresse, was natürlich auch nicht gewünscht ist und beim Austesten einer Applikationsgruppe mit mehreren VMs sicher zu Schwierigkeiten führt. Die genannten Probleme sind übrigens bei Veeam sehr wohl bekannt und auch in der Liste der Einschränkungen zu finden. Der Hersteller hat aber keinen Einfluss darauf, da das Verhalten letztendlich durch VMware vorgegeben ist. Nachdem Veeam B&R für die Verwendung mit VMXNET2 getestet hat, ist es am besten, auch diese Adapter zu verwenden.

Sind die Applikationsgruppe und das Virtual Lab definiert, fehlt nur noch ein Job für die Zeitplanung. Dieser kann, wenn gewünscht, alle beteiligten VMs starten, die Testskripte ausführen und die Umgebung anschließend wieder herunterfahren, um so einen vollautomatischen Check zu realisieren. Für weitere manuelle Schritte oder einen temporären Zugriff aus der Produktion kann die Sandbox aber auch in Betrieb bleiben, bis der Administrator sie wieder per Hand stoppt.

Etwas abgewandelt arbeitet Instant VM Recovery, indem eine VM netzwerkseitig nicht in einer Sandbox landet, sondern direkt im ursprünglichen Netz. Das setzt natürlich voraus, dass die originale Produktionsmaschine gestoppt ist. So hat der Administrator die Möglichkeit, beim Ausfall einer Produktions-VM mittels B&R direkt aus der Sicherung einen etwas älteren, aber funktionierenden Stand zu starten, um mit möglichst geringem Zeitverzug weiterarbeiten zu können. Instant VM Recovery spart hier die Zeit für die sonst notwendige Wiederherstellung.

Wichtig ist zu wissen, dass Surebackup und Instant VM Recovery die Sicherungsdateien nicht verändern, da beide Funktionen diese nur lesend öffnen. Alle notwendigen Änderungen während der Laufzeit werden in temporäre Dateien geschrieben. Zu beachten ist auch, dass der Start einer VM aus der Sicherung heraus immer den Veeam Backup-Server benötigt, dort als Job läuft und einen vom Backup-Server angelegten und verwalteten Datastore nutzt. Veeam nennt diesen Mechanismus vPower. Wurde also beispielsweise eine VM mit Instant VM Recovery ersetzt und wird diese auf Dauer benötigt, so muss sie mit Storage vMotion oder den in B&R integrierten Funktionen Replication beziehungsweise VM Copy wieder auf den Produktions-Datastore verschoben oder kopiert werden. Erst dann arbeitet sie wieder unabhängig vom Backup-Server. Im Test konnten wir sowohl Surebackup als auch Instant VM Recovery mehrfach erfolgreich durchführen.

Wiederherstellung nach Maß

Neben Instant VM Recovery beherrscht B&R noch weitere Verfahren zur Datenwiederherstellung. Recht unspektakulär gestaltete sich im Test eine komplette VM-Wiederherstellung. Hierzu löschten wir eine vorher gesicherte VM über das vCenter und starteten dann deren Recovery. Gut gefiel uns, dass B&R alle Informationen hinsichtlich der ursprünglichen Konfiguration gespeichert hatte und diese auch vorschlug, also eine Wiederherstellung auf dem gleichen Datastore und im gleichen Ressourcenpool. Darüber hinaus gibt es die Möglichkeit, einzelne VM-Dateien oder Dateien eines Gastbetriebssystems wiederherzustellen. Bei einem Windows-Gast öffnet B&R die VMDK-Dateien in einem Explorerähnlichen Fenster. Der Administrator kann nun das Dateisystem durchsuchen und Dateien oder auch ganze Verzeich-

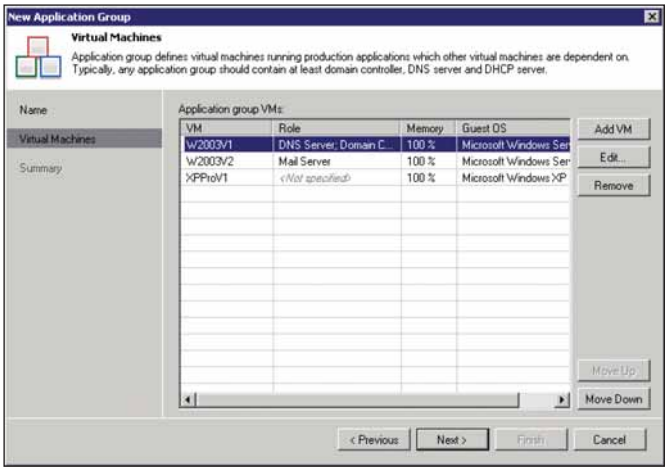


Bild 3: Über die Definitionen kompletter Applikationsgruppen kann B&R Surebackup skriptgesteuert auch die Funktion zusammenhängender VMs in einer Sandbox prüfen

nisse über die Zwischenablage auf den Backup-Server oder eine erreichbare Freigabe kopieren.

Eine Besonderheit, die sich allerdings teilweise noch im Betastadium befand, ist AIR (Application Item-Level Recovery). Zum Testzeitpunkt gab es vier AIR-Module (Universell, SQL, Exchange und Active Directory), die einzeln nachzuinstallieren waren. Ziel ist die Wiederherstellung einzelner Applikationsobjekte wie ein Exchange-Postfach, eine Tabelle aus einer SQL-Datenbank oder ein AD-Objekt. Im Test versuchten wir uns mit der Wiederherstellung einer SQL-Tabelle, was sich letzten Endes als gar nicht so einfach herausstellte. Vielmehr bestätigte sich die Maxime, dass ein Administrator komplexere Szenarien schon einmal durchgespielt haben sollte, bevor es zum Ernstfall kommt. Prinzipiell funktioniert AIR so, dass das gewünschte Backup ähnlich wie bei Surebackup in einem Virtual Lab gestartet wird. Dann öffnet ein Assistent auf dem im Virtual Lab laufenden System die Applikation – also in unserem Fall die SQL-Datenbank – und zeigt alle gefundenen Objekte an. Der Administrator kann nun die benötigten Objekte auswählen und auf das Produktionssystem übertragen lassen, wahlweise unter dem alten Namen oder auch unter einem neuen, falls eine Tabelle beispielsweise nur zum Teil wiederhergestellt werden soll. Im Test gestaltete sich dieser Weg dann doch als etwas hürdenreich, wobei das weniger B&R anzulasten war, sondern vielmehr dem Verhalten des SQL-Servers.

Der Einstieg erfolgt bei AIR über die Administrationskonsole am Veeam Backup-Server, um die Bereitstellung eines Virtual Lab zu beantragen. Als relativ umständlich empfanden wir, dass anschließend der Enterprise Manager zu öffnen war, um diesen Antrag genehmigen und weitere Eingaben tätigen zu können. Erst danach arbeitete der Virtual Lab Manager am Backup-Server weiter, um das Virtual Lab tatsächlich aufzubauen und den Wiederherstellungsassistenten zu starten. Als sich dieser Assistent bei der SQL-Datenbank auf der VM im Virtual Lab anmelden wollte, klappte dies nicht. Der Grund hierfür war, dass wir für die SQL-Anmeldung die Windows-Authentifizierung nutzen wollten, aber innerhalb des Labs kein Domänencontroller zur Verfügung stand. Glücklicherweise hatten wir den SQL-Server mit gemischter Authentifizierung installiert, konnten uns so mit dem lokalen sa-Account behelfen und die gelöschte Tabelle erfolgreich wiederherstellen. Andernfalls wäre es notwendig geworden, in der Sandbox auch noch einen dazugehörigen Domänencontroller mitlaufen zu lassen.

AIR funktioniert also durchaus, ein Administrator sollte aber vorbereitet an eine Wiederherstellung herangehen, damit er nicht erst im Ernstfall die beste Vorgehensweise ermitteln muss. So sieht es B&R wie oben beschrieben vor, dass ein Virtual Lab nicht auf ein System beschränkt ist, wenn es darum geht, eine funktionsfähige Insel zu bauen. Dieses Feature ist aber bei Bedarf auch einzusetzen und ein Administrator sollte es vorher austesten, um sofort zu wissen, wie in seinem Fall der AIR-Restore am schnellsten zum Ziel führt.

Intelligente Platzsparmaßnahmen

Für eine schnelle und möglichst platzsparende Arbeitsweise hat B&R diverse Mechanismen integriert. So führt das Programm bei wiederkehrenden Aufträgen nur anfangs ein Vollbackup durch und sichert dann inkrementell. Damit sich aber keine endlose Schlange an Ergänzungen ergibt, unterstützt B&R ein so genanntes Full Synthetic Backup an definierbaren Wochentagen. Steht ein derartiges Backup an, führt B&R erst wie üblich eine inkrementelle Sicherung durch. Anschließend erstellt es aus dem letzten Vollbackup und allen dazwischen liegenden Inkrements ein neues (voll synthetisches) Vollbackup, bezogen auf diesen Tag. An den nächsten Tagen wird wieder nur inkrementell gesichert. Der Vorteil besteht darin, dass B&R die Daten nach dem allerersten Vollbackup immer nur inkrementell von der Produktions-VM holt. Daraus erzeugt es dann intern Vollsicherungen, was die Produktion nicht belastet.

Eine weitere Variante ist das umgekehrte inkrementelle Backup (Reversed incremental backup). Hierbei erzeugt B&R kein Inkrement mit den aktuellen Änderungen, sondern tauscht in der Vollsicherung die geänderten, alten Blöcke gegen die neuen aus und erstellt aus den alten eine inkrementelle Datei. Dadurch liegt immer der letzte Sicherungsstand als Vollsicherung vor und erst ein Restore auf einen älteren als den letzten Stand erfordert das zusätzliche Einspielen von Inkrements. Wer sich nicht allein auf die inkrementelle Arbeitsweise verlassen möchte, kann selbstverständlich auch echte Vollsicherungen wöchentlich oder monatlich durchführen. Herkömmliche Sicherungsverfahren mit Vollsicherungen und darauf aufbauenden Inkrements lassen sich also auch realisieren.

Obwohl ein Sicherungsjob das Backup mehrerer VMs enthalten kann, behandelt B&R jede VM logisch getrennt. Ist bei einer VM die Sicherung erfolgreich, bei einer anderen aber nicht, so wird auch nur für diese ein erneuter Versuch gestartet. Schlägt dieser zweite Versuch ebenfalls fehl, erstellt B&R von dieser VM eine Vollsicherung, aber nicht von allen. Nachdem VMs häufig durch Klonen vervielfältigt werden, haben deren VMDK-Dateien viele identische Blöcke. Um das platzsparend zu nutzen, unterstützt B&R eine Deduplizierung, indem es identische Blöcke nur einmal speichert. Je nach genutztem Speicherort empfiehlt sich die Wahl einer von drei Optionen, die letztendlich unterschiedliche Blockgrößen verwenden. Wird die Sicherung lokal (auf SAN, DAS oder lokalen Platten) gespeichert, ist die Option "Local target" zu empfehlen. Hier arbeitet B&R mit großen Blöcken, die schneller verarbeitet werden, wobei allerdings die Deduplizierungsrate geringer ist. Bei der Sicherung über das Netz, genannt "Lan target", arbeitet B&R mit mittelgroßen Blöcken.

Für den Transfer über eine langsame WAN-Strecke, bezeichnet mit "WAN target", arbeitet B&R mit kleinen Blöcken, um über eine hohe Deduplizierungsrate die zu übertragende Datenmenge möglichst zu reduzieren.

Zusätzlich beherrscht B&R eine Kompression in drei Stufen sowie die Speicherung ohne Kompression. Hier empfiehlt sich eine Abstimmung mit der zur Verfügung stehenden CPU-Leistung des Backup-Servers. Keine Kompression sollte speziell dann gewählt werden, wenn das genutzte Plattensystem selbst ebenfalls komprimiert oder dedupliziert.

Gute Dokumentation

Sehr gut gefallen hat uns das 170-seitige Benutzerhandbuch. Die Gliederung ist sehr übersichtlich und alle Funktionen sind detailliert beschrieben, so dass der Leser schnell versteht, wie alles funktioniert. Vorteilhaft ist auch, dass Veeam nicht mit Grafiken gespart hat, die etwas oftmals leichter visualisieren als ein langer Text. Wertvoll sind auch konkrete Tipps und Beispiele, welche Kompression wann zu verwenden ist und welches Sicherungsverfahren sich wofür am besten eignet. Wer sich die Mühe macht, dieses Handbuch zu studieren, ist nachher bestens für das Arbeiten mit B&R gerüstet.

Allerdings vermissten wir eine in die Software integrierte, kontextsensitive Hilfe. Es gibt zwar eine allgemeine Hilfe, es dürfte aber vor allem am Anfang durchaus vorkommen, dass ein Administrator in einem Menü vor einer Optionsauswahl steht und nicht genau weiß, welche in der jeweils vorliegenden Konstellation die beste ist. Dann bleibt ihm nichts anderes übrig, als im großen Handbuch nachzuschlagen. Hier müssen wir allerdings positiv bemerken, dass wir im Test aufgrund des übersichtlichen Aufbaus auf unsere Fragen immer schnell eine Antwort fanden.

Fazit

Schon seit längerem hatten wir Veeam Backup & Replication 5.0 als neue Sicherungssoftware für virtuelle Umgebungen unter VMware ESX im Visier und mussten uns zweimal bezüglich einer Testversion vertrösten lassen. Das Warten hat sich aber gelohnt, denn das Resultat ist ein überaus flexibel einsetzbares und sehr leistungsfähiges Produkt, um virtuelle Maschinen zügig sowie zuverlässig zu sichern und auch wiederherstellen zu können. Ein absolutes Novum ist das Feature Surebackup, die Möglichkeit, eine Sicherung einfach dadurch zu testen, indem die enthaltenen VMs in einer isolierten Umgebung, einer Sandbox, gestartet werden, um Lauffähigkeit und Konsistenz zu prüfen. Dabei werden die Sicherungsdateien nicht verändert. Ein weiteres Novum ist das so genannte Instant VM Recovery, bei dem bei Ausfall einer Produktions-VM eine vorhandene Sicherung ohne vorherigen Restore als Ersatz-VM gestartet werden kann, um so eine längere Downtime zu vermeiden. Überzeugt haben uns dabei nicht nur diese neuen Ideen, sondern auch deren Umsetzung, die in Verbindung mit einer intuitiven Administrationskonsole ein sicheres Arbeiten ermöglichen.

Neben der Datensicherung ganzer VMs und deren Wiederherstellung erlaubt Backup & Replication auch die mehrfache oder kontinuierliche Replizierung einer VM auf einen anderen ESX-Server sowie den Restore einzelner VMDK-Dateien sowie einzelner Dateien aus Sicht des Gastbetriebssystems. Als recht komplex hat sich allenfalls AIR gezeigt, die Möglichkeit, einzelne Objekte auf Applikationsebene wiederherzustellen. Die Assistenten für Active Directory, MS SQL und Exchange sind von der Funktionsweise her nicht ganz trivial. Falls ein Administrator eine dieser Funktionen nutzen möchte, sollte er sie in seiner individuellen Umgebung genau austesten, um zu wissen, welche Voraussetzungen für einen erfolgreichen Ablauf notwendig sind.

Wer momentan mit dem Backup und Restore seiner virtuellen Umgebung nicht zufrieden ist, sollte auf jeden Fall einen Blick auf dieses interessante Produkt werfen. Neben der von uns getesteten Enterprise-Version gibt es noch eine etwas abgespeckte Standard-Version. Sie ermöglicht die Surebackup-Funktion nur manuell. Weiterhin wird AIR nicht unterstützt und eine Dateisuche ist nur in aktuellen Sicherungen möglich, aber nicht in älteren. *(dr)*

Produkt

Software zur Datensicherung und -wiederherstellung in virtuellen Umgebungen unter VMware ESX.

Hersteller

Veeam
www.veeam.com

Preis

CPU-Sockel-basierte Lizenzierung (maximal sechs Cores pro CPU), Standard Edition 527 Euro pro CPU, Enterprise Edition 791 Euro pro CPU, Staffelpreise für größere Umgebungen.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Sicherungsvarianten	8
Konsistenzprüfung der Sicherungen	9
Wiederherstellung einzelner Objekte	7
Wiederherstellungsvarianten	9
Platzsparende Datenablage	8

Dieses Produkt eignet sich

optimal für mittlere und größere virtuelle Umgebungen unter VMware ESX mit SAN-Anbindung. Hier kann das Produkt seinen Funktionsumfang am besten zur Geltung bringen.

bedingt, falls nur LAN zur Kommunikation zu Verfügung steht und kein SAN genutzt wird. Hier ist darauf zu achten, dass die LAN-Bandbreite nicht zum Nadelöhr wird.

nicht für Umgebungen, die bei der Virtualisierung nicht auf VMware ESX setzen oder gar nicht virtualisieren.

Veeam Backup & Replication 5.0

1&1 WEBHOSTING

„1&1 WebHosting bietet uns zahlreiche Inklusiv-Features, die unsere Homepage noch informativer und erfolgreicher machen. Für uns ist 1&1 der perfekte Partner."

Markus Fügenschuh
www.skischule-ostrachtal.de

PROFESSIONELLE HOMEPAGE

1&1, der größte Webhoster weltweit, garantiert beste Hosting-Qualität und wertvolle Inklusiv-Features:

1. PLATZ
PRODUKT DES JAHRES 2010/2011
PC Magazin
Ausgabe 05/2011

Inklusiv-Domains!

.com .de .eu .net

Ihre perfekte Internet-Adresse: Sie können aus .de, .at, .info, .com, .net, .org, .biz und .eu wählen.

Mehr Webspace!

Selbst für aufwändige Website-Projekte bieten Ihnen unsere Pakete ausreichend Webspace.

Webdesign-Software!

Adobe® Dreamweaver® CS4 und NetObjects Fusion® dienen als optimale Basis für hochwertiges Webdesign, sogar optimiert für die Ausgabe auf mobilen Endgeräten.

Entwickler-Tools

ZF git php

PHP6 (beta), Zend Framework, Versionsmanagement (git), Cron Jobs und Shell-Zugang bieten die perfekte Spielwiese für professionelle Webdesigner.

Grüne Rechenzentren!

Ihre Daten liegen sicher in unseren Hochleistungs-Rechenzentren, die mit Strom aus erneuerbaren Quellen betrieben werden. Das spart 30.000 Tonnen CO_2 pro Jahr.

1&1 HOMEPAGE-PAKETE 6 MONATE FÜR 0,– €/Monat danach ab 6,99 €/Monat*

AKTION NUR BIS 30.04.2011!

z. B. 1&1 HOMEPAGE PERFECT

- 2 Inklusiv-Domains
- 4 GB Webspace
- UNLIMITED Traffic
- 5 MySQL-Datenbanken
- Zend Framework
- PHP6 (beta), PHP5
- Perl, Python
- SSI
- NetObjects Fusion® 1&1 Edition
- Google Sitemaps
- 24/7 Profi-Hotline
- uvm.

~~6,99 €/Monat*~~ **0,– €/Monat*** 6 Monate 0,– €, danach nur 6,99 €/Monat.*

Weitere sensationelle Angebote, z. B. .de, .info Domains 1 Jahr für 0,29 €/Monat*, im Internet.

1&1

MEMBER OF united internet

Jetzt informieren und bestellen:

0 26 02 / 96 91
0800 / 100 668

www.1und1.info

*Ausgewählte 1&1 Homepage-Pakete z.B. 1&1 Homepage Perfect 6 Monate für 0,– €/Monat, danach 6,99 €/Monat. Einmalige Einrichtungsgebühr 9,60 €. .info und .de Domain 0,29 €/Monat im ersten Jahr (danach .de Domain 0,49 €/Monat, .info Domain 1,99 €/Monat), keine Einrichtungsgebühr. 12 Monate Mindestvertragslaufzeit. Preise inkl. MwSt.

Im Test: Arkeia Backup Appliance APA110

Zentrum der Datensicherung

von Sandro Lucifora

Der Vorteil einer Backup-Appliance liegt im zentralen Management und der zentralen Datenhaltung. Ohne Appliance benötigt sonst jedes zu sichernde Gerät eine Backup-Software und einen eigenen Backup-Datenspeicher. Nicht nur Hardware- und Softwarekosten werden mit einer Appliance minimiert, sondern auch der Administrationsaufwand beschränkt sich auf nur noch ein Gerät. Mit der Arkeia Backup Appliance APA110 testete IT-Administrator ein derartiges Gerät in einem mehrwöchigen Test.

Zur Integration des Arkeia Backup-Werkzeugs hat der Administrator die Wahl zwischen der klassischen Softwarelösung, betrieben auf einem beliebigen PC, einer virtuellen Backup-Appliance für VMware oder der physischen Appliance. Eine Testversion der Arkeia Network Backup-Software oder der virtuellen Appliance können Sie von der Webseite herunterladen. Damit lassen sich vor dem Kauf die Software des Backup-Servers, der Backup-Agents und das Disaster Recovery risikolos testen.

Wir entschieden uns für den Test der Stand-Alone-Lösung. Zur Auswahl stehen bei Arkeia vier Serien – 110, 210, 310 und 510. Die Unterschiede beziehen sich auf die Anzahl von Festplatteneinschüben, die RAID-Systeme, die externen Schnittstellen, die Technik des internen Bandlaufwerkes und die Bauform des Gehäuses. Das getestete System der 110-Serie liefert eine Ausstattung, die für kleine und mittlere Netzwerkstrukturen ideal ist.

Der Hersteller gibt an, dass sein Produkt die Daten von nahezu jedem Gerät im Netzwerk, egal welches Betriebssystem und ob Client, Mail-Server oder Datenbank, sichern kann. Dabei sollen 150 Plattformen unterstützt werden; bei der Zählung fließen verschiedene Versionen und Ausprägungen der Betriebssysteme ein.

Unkomplizierte Inbetriebnahme

Das mit zwei Höheneinheiten recht kompakte Gerät ist nicht für den Rackeinbau vorgesehen. Es verfügt über zwei Festplatteneinschübe mit 1 TByte Kapazität und ein integriertes LTO-3-Bandlaufwerk. Die verbaute Intel-Celeron CPU und 512 MByte Hauptspeicher zeigen, wie genügsam das System in Bezug auf die Hardware ist. Die Software basiert auf einem Linux-Kernel und wird über ein übersichtliches Webfrontend administriert. Nach dem Stromanschluss muss der Anwender nur noch das Netzwerkkabel einstecken, die Appliance hochfahren und kann sofort starten.

Um die Appliance im Netz anzusprechen, muss der IT-Verantwortliche ihr eine IP-Adresse zuweisen. Von Hause aus "hört" das Gerät auf die IP 10.10.10.10. Um hierauf zuzugreifen, stellten wir die Verbindung zum Computer direkt über ein Cross-Connect-Kabel her und wiesen dem Netzwerkanschluss unseres Rechners manuell seine IP aus dem Adressraum zu. Der Aufruf über den Webbrowser gelang danach sofort. Nach dem Login hinterlegten wir bei der Appliance – entgegen der Hersteller-Empfehlung – keine statische IP-Adresse aus unserem Netzwerk, sondern stellten auf DHCP um.

Bevor die Appliance nach ihrem Anschluss an den Netzwerk-Switch neu gebootet und eine Netzwerkadresse bezogen hat, haben wir im DHCP-Server des Netz-

Unterstützte Plattformen

Insgesamt unterstützt Arkeia mit dem Backup-Agent über 150 Plattformen. Dazu gehören beispielsweise FreeBSD, OpenBSD, Linux, Apple Mac OS X, IBM PowerPC, HP HP-UX, SUN Solaris ab 8, VMware ESX 3 sowie Windows-Server und -Clients.

Eine vollständige Übersicht finden Sie unter dem **Link-Code B4T41**.

werks für die MAC-Adresse der Appliance – die auf einem Aufkleber an der Rückseite des Gerätes steht – eine feste IP reserviert; so bekommt die Appliance trotz DHCP immer dieselbe IP. Die restliche Anpassung an die Netzumgebung verlief im Hintergrund, da das System über DCHP alle notwendigen Angaben wie IP-Adresse, DNS, Gateway, NTP-Server und so weiter erhält.

In der Backup-Appliance ist ein mehrstufiges Rechtekonzept integriert: So lassen sich verschiedenen Administratoren ausgewählte Funktionen zur Verfügung stellen. Auf der niedrigsten Stufe kann ein Benutzer lediglich seine oder andere Dateien wiederherstellen. Positiv fiel zudem auf, dass die Konfiguration von Systemeinstellungen selbst für den Administrator noch einmal mit einem zusätzlichen Passwort abgesichert war.

Unnötiger Aufwand bei Einrichtung der Backup-Clients

Nach dem Einloggen zeigt sich die Oberfläche der APA110 sehr übersichtlich. Klassisch befinden sich links die Menüpunkte und in der Mitte ist der jeweilige Seiteninhalt zu sehen. Zu jedem Menüpunkt findet sich auf der Inhaltsseite zudem ein Help-Button. Der Aufbau der Seiten ist sowohl im Internet-Explorer 7 und 8 als auch dem Firefox 3.x angenehm schnell.

Im Testverlauf fiel uns negativ auf, dass die Oberfläche nur in englischer Sprache verfügbar ist. Positiv anzumerken ist, dass das mitgelieferte – jedoch auch englische – Handbuch gut strukturiert und nützlich für den Einstieg und beim Einarbeiten sehr hilfreich ist. Zudem bietet die Online-Dokumentation in Form eines Wikis eine vielfältige Hilfestellung bei allen Fragen rund um die Konfiguration und Installation der Clients.

Ist die Grundkonfiguration erfolgt, soll dem ersten Backup nichts mehr im Wege stehen. Dazu hangelten wir uns schlicht am Menübaum herunter und beantworteten drei unmissverständliche Fragen "What to backup?", "Where to backup?" und "When to backup?".

Doch schon beim ersten Menüpunkt stellten sich zunächst einige Fragezeichen ein: Denn für die Angabe, was zu sichern ist, benötigt die Appliance zunächst eine Liste aller möglichen Clients – den Nodes. Ein Node kann nur ein Rechner werden, auf dem der Arkeia-Backup-Client installiert ist. Und hierin begründet sich auch die Aussage des Herstellers über die Anzahl der unterstützten Systeme. Arkeia liefert für sehr viele Systeme eigene Backup-Clients und unterscheidet nicht nur zwischen dem Betriebssystem-Hersteller und dem Computer-System, sondern auch bezüglich der verwendeten CPU Architektur und ob es ein 32- oder 64-Bit-System ist. Zudem ist auch die auf dem System betriebene Applikation relevant – so gibt es zum Beispiel zusätzliche Datenbank- und Application-Agents für Exchange und Lotus sowie MS SQL-Server, MySQL oder Postgres – um nur einige Beispiele zu nennen. Aufgrund dieser Individualisierung der Clients erreicht Arkeia auch die bestmögliche Zusammenarbeit auf dem System.

Somit sind die Agents unerlässlich, damit sich die Backup-Appliance mit dem jeweils zu sichernden System austauscht. Wegen dieser zentralen Bedeutung der Clients ist es für uns nicht nachvollziehbar, warum sich der Administrator diese erst noch mühsam auf der Download-Seite von Arkeia zusammensuchen und herunterladen muss. Es wäre wesentlich hilfreicher, über das Webfrontend der Appliance eine entsprechende Vorselektion des Betriebssystems mit dem Link auf den aktuellen Client im Internet zur Verfügung zu stellen. Anders verläuft die Einbindung von NAS-Systemen: Hier erfolgt die Kommunikation nicht via Agent, sondern direkt über das Network Data Management Protocol (NDMP).

Für uns hieß es an dieser Stelle, den richtigen Backup-Client aus der langen Liste zu lokalisieren und zu installieren. Leider haben wir im Test keine MSI-Daten für diese Aufgabe erhalten, so dass wir auch keine verteilten Installationen durchführen konnten. Dies stellt einen unnötigen Mehraufwand für den Administrator dar.

Von Vorteil ist, dass der Backup-Client keine weitere Interaktion des Users benötigt und sich nach der Installation auch automatisch in der Arkeia-Software als Node anmeldet. Neben den physikalischen

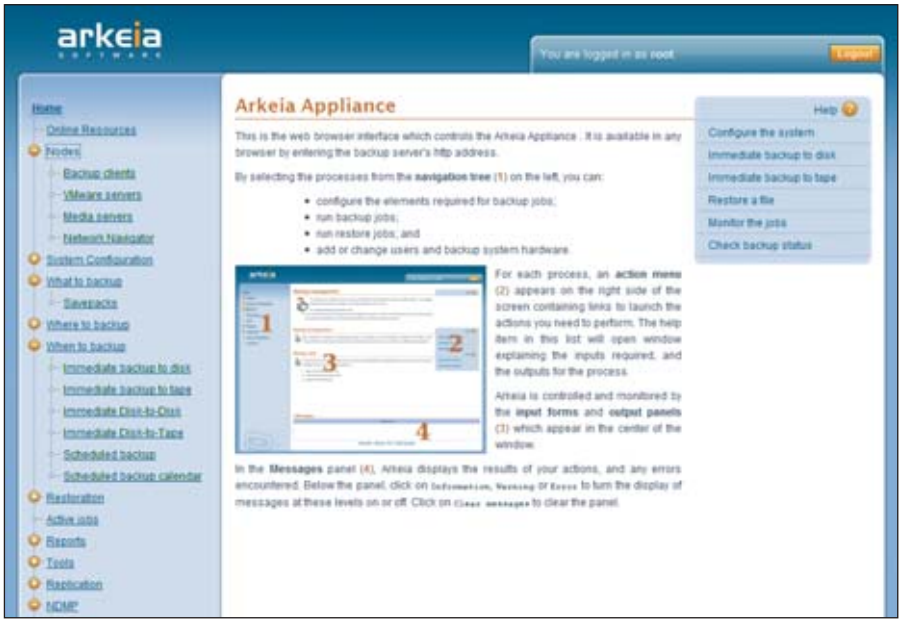


Bild 1: Das Webfrontend ist übersichtlich, jedoch nur in Englisch verfügbar

Bild 2: Die Nodes sind alle Netzwerk-Geräte, die aufgrund des installierten Backup-Clients von der Appliance gesichert werden können

Clients unterstützt das System auch VMware-Server. Wieso hier Windows Hyper-V außen vor bleibt, konnten wir nicht erschließen. Hyper-V wird jedoch über einen separaten VSS-Agent unterstützt.

Hoher Aufwand bei der Erstkonfiguration lohnt sich

Nachdem die Agenten installiert waren, prüften wir mit Hilfe des "Network Navigator", ob die Appliance vollen Zugriff auf die Rechner im Netz hat. Damit stellten wir sicher, dass sich aus der Ferne die Gerätedaten sowie die Verzeichnisstruktur abrufen ließen. Für die Kommunikation zwischen Appliance und Client nutzt die Software den Port 617. Während der Austausch bei Windows XP- und 2003-Rechnern recht schnell eingerichtet war, weigerten sich Vista- und Windows 7-Rechner zunächst. Hier mussten wir die Ports der Firewalls manuell öffnen.

Nachdem die Nodes registriert waren und den vollen Zugriff erlaubten, machten wir uns daran, die ersten Backup-Jobs zu erstellen. Was sich zunächst einfach anhört, war jedoch nicht ohne Unterstützung der Hilfe und der FAQs möglich, da sich uns die Logik der Konfiguration nicht sofort erschloss. Arkeia splittet hier in sogenannte "Savepacks" und "Drivepacks": Die Savepacks enthalten die Konfiguration der zu sichernden Daten und die Sicherungsart (vollständig, inkrementell, komprimiert). Dazu wird das Savepack angelegt und über einen oder mehrere Datenbäume die zu sichernden Daten ausgewählt. Im Drivepack konfigurierten wir anschließend den Speicherort (Festplatte, Band, Speicherpool, Backup-Server).

Was uns zunächst aufwändig erschien, zeigte sich bei mehreren Backups als zeitsparend, da sich angelegte Savepacks kopieren und diese für den jeweiligen Client modifizieren lassen. Aber auch bereits definierte Savepacks ließen sich für weitere Backup-Aufgaben nutzen. Durch das Festlegen der Gültigkeit eines Savepacks können sogar mehrere Jobs für einen Client existieren.

Durch den modularen Aufbau wird ein Savepack auch für mehrere Speicherorte verwendet, ohne dass der Administrator alle Daten neu eingeben muss. So sicherten wir ein Savepack in der Woche tagsüber inkrementell auf die schnellere Festplatte und am Wochenende nachts und als Vollbackup auf das langsamere Bandlaufwerk. Bei einem anderen Savepack untersuchten wir die Replizierung zwischen Drivepacks, indem wir die am Tag erstellten Backups in der Nacht zusätzlich auf ein Band archivierten. Im Task-Planer legten wir fest, wann welche Sicherung in Kombination zwischen Savepack und Drivepack erfolgt. In Zusammenarbeit mit dem Kalender lassen sich Sicherungen auch nur an bestimmten Tagen vorplanen. Was uns im ganzen Zusammenspiel der Konfigurationen fehlte, ist eine Echtzeit-Replikation der Daten vom Client zum Backup-Server. Alternativ könnten auch inkrementelle und differenzielle Backups für einen möglichst geringen Datenverlust genutzt werden, doch erlaubt Arkeia als kürzesten Siche-

Produkt
Gerät zur Datensicherung und Wiederherstellung sowie zum Desaster Recovery in kleinen und mittleren Infrastrukturen oder auch in verteilten Standorten.

Hersteller
Arkeia Software
www.arkeia.de

Preis
APA110-Serie: von 2.500 Euro bis 5.000 Euro, je nach Ausstattung.

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

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

Unterstützte Backup-Clients	8
Konfiguration der Backups	5
Flexibilität bei den Sicherungszielen	7
Durchführung paralleler Sicherungen	6
Wiederherstellung	7

Dieses Produkt eignet sich

optimal für die Sicherung von bis zu zehn Rechnern – auch in Zweigstellen –, da die Kapazität und Handhabung ideal hierfür sind.

teilweise als Basis für die Datensicherung mittelgroßer IT-Landschaften, da eine weitere Appliance (und/oder eine größere Kapazität) notwendig werden können.

nicht für den Einsatz in einem Rechenzentrum, da die Kapazität nicht ausreichend ist.

Arkeia Backup Appliance APA110

rungszyklus lediglich einen Tag – hier fehlt definitiv der Zyklus in Stunden oder gar Minuten.

Durch die Vernetzung mehrerer Appliances sind zudem redundante Datensicherungen möglich. Eine Überlegung hierzu ist, dass Appliances in Abteilungen oder Niederlassungen tagsüber dortige Rechner sichern. Nachts wechselt das System seine Rolle in einen Backup-Client und die Daten werden dann auf einem zentralen Backup-Server gesichert. So lassen sich auch umfangreiche Backup-Strukturen erstellen, die dank der Vielzahl an unterstützten Plattformen eine redundante Sicherung der unternehmenswichtigen Daten erlauben.

Sorgenfreie Rücksicherung

Wer Daten sichert, will diese im Notfall auch wieder zurückspielen. Dazu bietet Arkeia zwei Möglichkeiten an: Die Rücksicherung auf Dateiebene und das Disaster Recovery (die Notfallwiederherstellung). Um Daten auf Dateiebene wiederherzustellen, nutzt der IT-Verantwortliche die Weboberfläche. Hier konnten wir in der Selektion zwischen ganzen Laufwerken bis hin zu einzelnen Dateien auswählen und die Rücksicherung starten. Dies verlief zuverlässig und unspektakulär.

Über den VSS-Agent gesicherte Applikationen, wie Datenbanken und Exchange-Server, werden hier ebenfalls ausgewählt. Dabei kann ein komplettes Backup der Applikationsdaten oder zum Beispiel eine einzelne Datenbank wiederhergestellt werden. Für das Disaster Recovery benötigten wir ein Bootmedium. Hierauf wird das "Arkeia live O/S" – das als ISO-Datei vorhanden ist – kopiert. Dabei kann es sich um eine CD oder ein USB-Stick handeln, je nachdem, welche Bootoptionen der Computer zulässt. Alternativ kann auch ein Rechner mit PBX-Unterstützung über das Netzwerk das Mini-O/S booten. Nach dem Booten des Zielrechners wählten wir das zurückzuspielende Backup aus, starteten den Prozess und nach einiger Zeit stand uns das wiederhergestellte System zur Verfügung.

Fazit

Ziel einer Backup-Appliance ist es, die Daten der IT-Infrastruktur zu sichern und im Bedarfsfall wiederherzustellen. Dieses Ziel erreicht Arkeia mit der APA110 voll und ganz. Neben Servern und Arbeitsstationen mit den unterschiedlichsten Betriebssystemen sichert das Testgerät auch Datenbanken und E-Mailsysteme. Zudem sprechen die übersichtliche Web-Oberfläche und die Kombination von Band- und Festplatten-Backups für das Gerät.

Lediglich die Handhabung des Backups ist gewöhnungsbedürftig. Hier hat der Hersteller noch Luft nach oben, um sein System zu verbessern. Das Sichern und Rücksichern der Daten verläuft zuverlässig. Durch die Vernetzung mehrerer Backup-Appliances untereinander wächst das Werkzeug mit der IT-Struktur mit. *(jp)*

Im Test: Primera Disc Publisher Pro Xi

In Serie produziert

von Thomas Bär

Wer schon einmal mehr als fünf Exemplare einer identischen CD/DVD mit einem einfachen Brenner erstellen durfte, der weiß um die Dauer und die gefühlte Stupidität dieses Vorgangs. Kommt es mehrmals im Jahr zu einem solchen Szenario, beispielsweise für ein Softwareupdate, eine Datenarchivierung oder den Versand eines elektronischen Katalogs auf Scheibe, so kann sich die Anschaffung einer automatisierten Lösung schon lohnen. IT-Administrator hat sich den Primera Disc Publisher Pro Xi im Test genauer angesehen und DVDs in Serie produziert.

Der Brennroboter Primera Publisher Pro Xi hat ungefähr die Größe einer handelsüblichen Mikrowelle. Anstelle einer Türe lässt sich die halbdurchsichtige Gehäuseklappe nach oben öffnen. Durch diese Art der Öffnung muss sichergestellt sein, dass knapp 60 Zentimeter Höhe zwischen der Stellfläche und dem nächsten Objekt über dem Brennroboter frei ist. Ansonsten benötigt der Publisher Pro eine Stellfläche von zirka 48x48 Zentimetern. Das komplett aus Kunststoff gefertigte Gehäuse ist ordentlich verarbeitet und die Zugriffsklappe, die für die tiefblaue Innenraumbeleuchtung durchlässig ist, gibt dem gesamten Gerät einen edlen Touch. Im Innenraum sind ein kleiner Roboterarm und zwei Behälter zur Aufnahme von Rohlingen zu sehen.

Zweitlaufwerk oder Blu-ray-Brenner auf Wunsch

Primera liefert den Brennroboter in zwei Varianten aus: Während der Publisher Pro Xi mit einem Brenner ausgestattet ist, kommt das Modell Pro Xi2 mit zwei Laufwerken daher. Der mit einem Hochgeschwindigkeits-Brenner ausgestattete Pro Xi erstellt laut Hersteller bis zu 32 optische Medien in einer Stunde, abhängig von der Kapazität des zu brennenden Materials. Der größere Bruder Pro Xi2 schafft mit 60 Medien über die zwei Laufwerke beinahe die doppelte Menge. In der üblichen Auslieferung von Primera verfügt der Roboter über zwei Zufuhr- und Ausgabebehälter mit einer Kapazität für je 50 Disks. Kommen herkömmliche 4,7 GByte DVD-Rohlinge zum Einsatz, so kann ein Administrator mit diesem Modell maximal 235 GByte im Standardbetrieb sichern, ohne selbst Hand anlegen zu müssen.

Auf Kundenwunsch liefert der Hersteller das System auch mit einem oder zwei Blu-ray-Brennern aus, was bei Verwendung von 50-GByte-Rohlingen und 100er Zufuhrbehältern im so genannten Kiosk-Betrieb einer maximalen theoretischen Speicherkapazität von rund 9,76 TByte entspricht. Im Kiosk-Betrieb legt der Automat eine bespielte Scheibe nicht in das zweite Behältnis ab, sondern wirft diese direkt aus. Somit lassen sich beide Zufuhrbehälter für leere Medien nutzen.

Installation ohne Hürden

Die Installation des Primera Publisher Pro Xi ist alles andere als kompliziert. Auf der Rückseite des Geräts findet der Benutzer lediglich den Anschluss für USB und für die Stromversorgung. Sowohl das Stromkabel als auch das USB-Kabel sind für die üblichen Anschlussszenarien lang genug bemessen. Der Brennroboter gibt gewöhnlich nur in Aktion ein Geräusch von sich. Der Lüfter wird in erster Linie beim Druckvorgang und eher kurz aktiv. Sobald der Greifarm im Gehäusein-

Systemvoraussetzungen

Für den Betrieb des Brennprogramms PTPublisher ist ein aktuelles Windows-System nötig. Neben Windows arbeitet der Roboter auch mit Apple-Rechnern unter Mac OS X. Als Anforderungen für Windows gibt der Hersteller mindestens eine Intel Celeron-CPU, 1 GByte RAM und Windows XP an. Für Mac OS 10.5 oder höher sollte es eine Motorola G5- oder Intel-CPU und mindestens 512 MByte Arbeitsspeicher sein. Erreicht der Computer nicht diese Anforderungen, ist eine fehlerfreie Zusammenarbeit mit dem Brennroboter nicht garantiert – was nicht heißt, dass es möglicherweise nicht dennoch funktioniert. Entscheidend für gute Brennergebnisse ist, dass die USB-Verbindung direkt und ohne Hub aufgebaut wird.

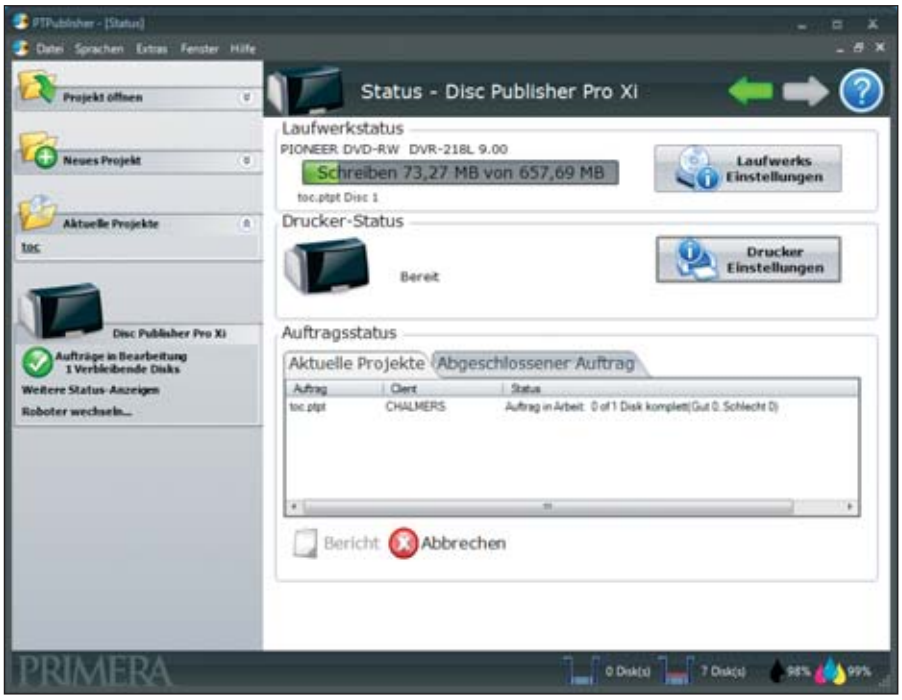


Bild 1: Primera liefert den Brennroboter mit einer einfachen und insgesamt leicht zu bedienenden Software aus

neren arbeitet oder ein Brennvorgang stattfindet, fallen deutlich wahrnehmbare Arbeitsgeräusche an, die jedoch einem Betrieb in einem Büro nicht entgegenstehen. Die einzigen Eingabeelemente auf der Kopfseite sind der Ein/Aus-Schalter und ein Knopf, der die Druckeinheit mit den Tintentanks in die Mitte des Gehäuses fährt.

Gemäß den Gepflogenheiten beim Umgang mit USB-Geräten sollte der Nutzer auch beim Primera Disc Publisher Pro Xi zunächst die Produkt-CD einlegen und die Software installieren. Hier geht es weniger darum, den Treiber bereits im Vorfeld ins System zu integrieren, als schlicht darum, dass ein Software-Assistent bei der Bestückung mit CDs/DVDs, dem Anschluss und dem Einsetzen der Tintenpatronen behilflich ist. Erst nachdem der mehrsprachige Softwareassistent einige grundlegende Einweisungsdialoge angezeigt hat, beginnt die Installation des Brennprogramms "PTPublisher".

Der Installation der eigentlichen Brenn-Software folgt das Beschriftungs-Programm "SureThing CD Labeler 5" in der Primera-Edition. Beide Programme belegten im Ordner "Programme" gemeinsam rund 80 MByte Speicherplatz. Nach Abschluss der Einrichtung fordert das System den Anwender zum Neustart auf und der Brennroboter führt einen Kalibrierungsdruck durch. Insgesamt ist der Einrichtungsvorgang einfach – einzig eine Frage bleibt dem Neuling, der das Gerät in einem schlecht ausgeleuchteten Raum aufbaut, zunächst unerschlossen: Muss die schwarze Tintenpatrone jetzt in die linke oder die rechte Halterung eingesetzt werden? Bedingt durch die blaue Innenbeleuchtung sind die farblichen Unterschiede zwischen der in grau gehaltenen Schwarz-Kartusche und der in lila hergestellten Farb-Patrone kaum zu erkennen. Mechanisch würde die Patrone auch in die falsche Halterung passen. In der kommenden Gerätegeneration will Primera anstelle der monolithischen Farbpatrone einzelne Farbpatronen liefern. Die Tintenpatronen für den Brennroboter gilt es auf Vorrat zu kaufen – diese lassen sich über den lokalen Fachhandel kaum beziehen.

Standardbrenner bringt ausreichend Leistung

Das Herzstück eines Brennroboters ist der verwendete Brenner. In der getesteten Variante war der Roboter mit einem einzelnen DVD-Brenner ausgestattet. Hierbei handelt es sich nicht um eine Spezialanfertigung. Vielmehr steckt ein Standard-SATA-Brenner, der DVR-218L von Pioneer, im Gehäuseinneren. Dieses 22x DVD-R/+R Gerät liest und schreibt CDR, DVD-R und DVD+R Medien. Aufgrund der Dual-Layer-Fähigkeit beim Umgang mit DVDs erhöht sich die maximale Speicherkapazität auf rund 8,5 GByte Rohdaten je Medium.

Der 218L brennt DVD+R und DVD-R Medien maximal mit 22facher Geschwindigkeit, was einer theoretischen Übertragungsrate von 30.470 KByte je Sekunde entspricht. Dual-Layer Medien vom Typ DVD+R DL und DVD-R DL werden vom Pioneer-Laufwerk mit zwölffachem Tempo beziehungsweise maximal 16.620 KByte pro Sekunde bespielt. Selbiges Tempo gilt für DVD-RAMs. Wiederbeschreibbare Medien sind gewöhnlich etwas langsamer in der Schreibgeschwindigkeit, hier bildet auch das Pioneer-Modell keine Ausnahme. DVD-RW Medien brennt das System mit 6- und DVD+RW mit 8-facher Geschwindigkeit. Als Brenngeschwindigkeit bei Standard-CDs weisen die technischen Angaben 40x oder 6.000 KByte pro Sekunde aus. Bei Verwendung von insgesamt gering verbreiteten CD-RW-Medien sinkt die Geschwindigkeit auf 32x oder 4.800 KByte pro Sekunde.

Dass der Brenner lediglich mit 2 MByte Cache-Speicher ausgestattet ist, machte sich in unserem Test nicht negativ bemerkbar. Frühere Versionen der Brennroboter waren mit Laufwerken mit 8 MByte Cache ausgestattet. Die Fähigkeit des aktuellen Brennermodells, auch LabelFlash-Rohlinge zu bedrucken, dürfte in der Praxis kaum Anwendung finden, da unmittelbar im selben Gerät ein Farbdrucker zur Verfügung steht. Label-

flash ist eine Weiterentwicklung von Lightscribe, einem Brennverfahren, bei dem mithilfe des Laserstrahls in eine spezielle Schicht des Mediums eine Beschriftung gebrannt wird. Beide Varianten benötigen spezielle Rohlinge und ein Beschriftungsvorgang dauert zwischen sieben und zwanzig Minuten. Zudem muss der Rohling im Laufwerk umgedreht werden, was der Roboter an sich schon nicht durchführen könnte.

Tintenstrahl-Druckwerk mit ansprechenden Ergebnissen

Die zweite Komponente des Duplizier- und Druckautomaten ist der integrierte 4.800 dpi-Tintenstrahldrucker von Lexmark. Wie bei einem normalen Drucker erledigen die Standarddialoge des Betriebssystems auch für den Primera Pro-Xi alle Druckeinstellungen. Die einzelnen Settings offenbaren dann aber die sehr speziellen Möglichkeiten: Anstelle der üblichen Papierformate erscheinen hier Einträge wie "Disc (116mm Image)", "Disc 120mm" oder "Business Card Disc". Zwar unterstützt der Drucker darüber hinaus Mini-Discs im Format 80 mm, doch lassen sich die 3-Zoll-Maxi-CDs nicht im mitgelieferten Medienhalter positionieren. Wer diese Mediengröße bearbeiten will, benötigt einen optionalen Adapter. Die Anlage ist in der Standardauslieferung komplett auf die übliche Größe von DVDs beziehungsweise CDs ausgerichtet. Einstellungen zum Druckbereich, zur Farbwahl, zur Auflösung und zur Zusammensetzung der Farben entsprechen weitgehend den üblichen Begrifflichkeiten eines Tintenstrahldruckers und erfordern keinen Blick in die Onlinehilfe.

Einstellungen zur Kalibrierung des Druckers finden sich ebenfalls in den Optionen der Druckersteuerung von Windows. In dem von uns getesteten Gerät waren keinerlei Anpassungen an den Einstellungen notwendig. Die bedruckten Medien machten einen absolut professionellen Eindruck und lediglich die Materialfarbe des Rohlings selbst zeugt von dessen Herstellung in einer Kleinserie. Der Hersteller selbst bietet für die Drucker passende Rohlinge an und bezeichnet diese als Tuff-Coat-Medien mit WaterShield-Oberfläche. Derartige Medien sind wasser-, kratz- und schmierfest und haben eine glänzende Oberfläche, die dem fertigen Datenträger einen edlen Eindruck gibt. Es ist jedoch möglich, Medien von anderen Herstellern zu verwenden. In einem normalen Elektronik-Fachgeschäft erhielten wir kompatible, tintenstrahl-bedruckbare Rohlinge von verschiedenen Anbietern. Auch diese konnten nach dem Druck optisch überzeugen, jedoch ohne die glänzende Oberfläche.

Solide Brennsoftware mit kleinen Schwächen

Zunächst haben wir getestet, ob wir den Disc Publisher Pro Xi auf einem Windows 7-Rechner in der x64-Ausprägung auch mit dem Brennprogramm Nero 9 ansprechen können. Zwar lässt sich mit dem Werkzeug wie gewohnt ein Brennauftrag definieren, doch eine Ansteuerung des Roboterarms ist mit der Software nicht möglich. Das System öffnet lediglich die Lade des DVD-Brenners und erwartet vom Benutzer das manuelle Einlegen des Rohlings.

Um also die Fähigkeiten des Brennroboters wirklich nutzen zu können, ist der Einsatz der mitgelieferten PTPublisher-Software unumgänglich. Das Programm bietet die gebräuchlichen Funktionen einer Brennersoftware und unterstützt insgesamt elf Dialogsprachen, unter anderem Deutsch. Will der Benutzer beispielsweise einen Serienauftrag eines identischen Datenträgers anlegen, führt ein Assistent durch insgesamt drei Dialogfenster. Neben reinen Datenprojekten bietet die Software auch Audio- und Videoprojekte. Der Funktionsumfang der Brennsoftware kann in Teilbereichen allerdings nicht mit der Marktkonkurrenz mithalten. Fügt der Nutzer beispielsweise einen gesamten Ordner über die grafische Oberfläche einem Brennauftrag hinzu, so ist es ihm nicht mehr möglich, selektiv einige Dateien aus diesem Ordner aus dem Auftrag zu entfernen. Werden die Brennaufträge für Kleinserien indes bereits im Filesystem vorbereitet, so ist die Arbeit mit der Brennersoftware einfach und in sich stimmig. Sofern gewünscht, verwendet der PTPublisher Label-Designs von der mitgelieferten Gestaltungssoftware SureThing auf Windows-PCs oder DiscCover für Macintosh-Rechner. Mit beiden Programmen lassen sich Fotos, Hintergrundmotive, Texte und Grafiken überall auf der Oberfläche des Rohlings platzieren. Im Gegensatz zu anderen Drucksystemen bedruckt der Disc Publisher Pro Xi die komplette Fläche randlos bis an den Innenring.

Nützliche Zusatzprogramme

Für Administratoren ist das PTBackUp eine besonders wichtige Funktionalität. Dieses Feature führt automatisch über einen Scheduler zuvor definierte Aufträge aus. Der Task-Planer kennt dabei lediglich die Einstellungen "täglich", "wöchentlich" und "monatlich" und erlaubt die Festlegung eines Startzeitpunkts. Im Zusammenspiel mit der Funktion "Spanning", der Verteilung eines Brennauftrags auf mehrere Rohlinge, ist so eine automatische Archivierung von Logfiles, ein- und ausgehenden E-Mails, Sicherungsdateien oder sonstigen Informationen möglich. Diese Verteilung funktioniert jedoch nur, wenn eine einzelne Datei nicht die Medienkapazität übersteigt. Beispielsweise funktioniert die Sicherung einer 750 MByte großen Datei auf CDRs nicht, da die Software die Datei nicht teilen kann. Die Software beschriftet die Medien automatisch mit Datum und Zeitstempel und zuvor definierten Informationen sowie dem nützlichen "DVD n von n".

Überzeugende Fehlertoleranz

Doch wie reagiert der Brennroboter, wenn sich ein Fehler einschleicht? In einem Schwung von Rohlingen legten wir testhalber Medien ein, von denen wir schon im Vorfeld wussten, dass diese aufgrund von Materialfehlern un-

tauglich sein würden. Der Roboter verwarf diese Medien dann tatsächlich. Er legte im Rahmen des Brennauftrags die Rohlinge in den Brenner, dieser untersuchte sie einige Augenblicke und öffnete die Schublade. Der Roboterarm hob den betreffenden Rohling aus der Lade und ließ ihn in einem Abwurfbereich zwischen den Rohling-Behältern fallen. Für den Anwender ist somit vollkommen klar, dass es sich bei den aussortierten Medien um nicht brauchbare Rohlinge handelt. Der Brennvorgang wurde unter Verwendung der anderen Rohlinge fortgesetzt.

Ein einziges Mal während der Testphase ging der Roboter davon aus, dass sich zwei Rohlinge in der Schublade des Brenners befinden würden, und machte den Benutzer in einem Dialogfenster auf diesen vermeintlichen Missstand aufmerksam. Wie bei einem Papierstau bei einem gewöhnlichen Drucker ist es auch hier die Sache des Anwenders, das Problem zu beheben. In dem hier beschriebenen Fall bestand die Lösung im Öffnen der Klappe und Drücken eines Knopfs. Der Roboter eignet sich aufgrund der Fehlertoleranz daher ausgezeichnet zur Erstellung von Endlosbrennaufträgen. Selbst ohne eine speziell angepasste Brennsoftware, wie sie Anbieter von Archivierungslösungen offerieren, ist die regelmäßige Überführung von Daten aus definierten Ordnern auf optische Medien möglich.

Integration in andere Lösungen möglich

Ausgestattet mit 50 oder gar 100 Rohlingen ist ein weiteres Einsatzfeld des Brennroboters die Erstellung von Medien direkt aus anderen Lösungen heraus. Beispiele für solche Anwendungen sind medizinische Bildbearbeitungs- oder PACS-Systeme im DICOM-Format, Überwachungs- und Archivierungssysteme in der Strafverfolgung oder beispielsweise On-Demand-Lösungen für Video- und Audiodaten. Um den Integrationsprozess zu vereinfachen, bietet der Hersteller Entwicklern kostenlos ein so genanntes Software Developers Kit für Windows- als auch für Mac-Plattformen an. Primera unterstützt nach eigenen Angaben als einziges Unternehmen im Duplizierungsmarkt aktiv Fremdentwickler für Windows, Mac und sogar Linux.

Fazit

Ausgestattet mit einer insgesamt hohen Produktionsgeschwindigkeit, einer guten Druckqualität, der Erweiterbarkeit der Software-Module, Kompatibilität zu Windows- und Mac-Betriebssystemen und moderaten Anschaffungs- und Stückkosten ist die Disc Publisher Pro Xi-Serie für kleinere und mittelgroße Unternehmen eine gute Wahl. Ein weiterer Pluspunkt: Während einige Marktbegleiter auf einen deutschsprachigen Support komplett verzichten, ist dieser bei Primera im Kaufpreis enthalten. *(ln)*

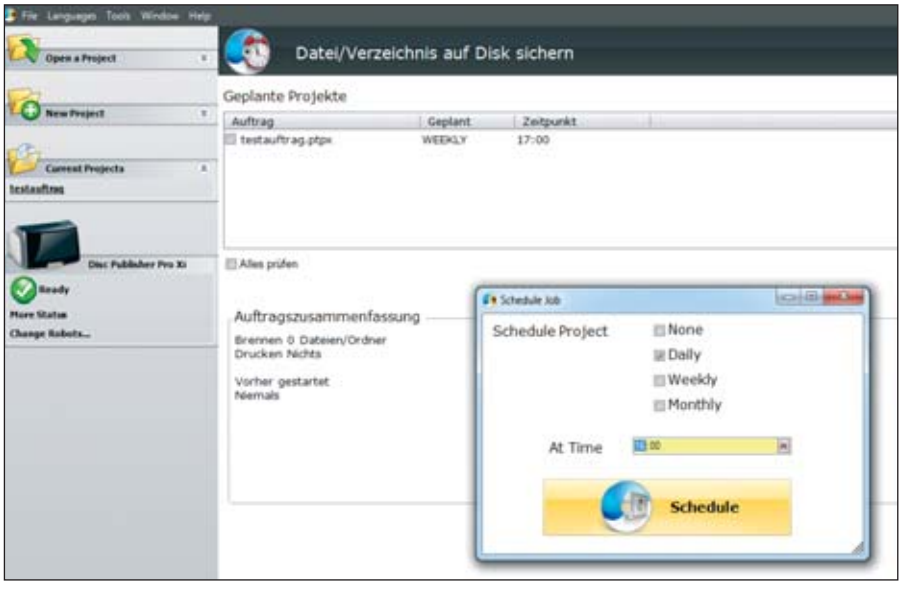


Bild 2: Automatische Aufträge über den Scheduler machen den Brennroboter zu einem rudimentären Archivierungssystem – jedoch ohne eine Datenbank, um gewünschte Inhalte schnell wiederzufinden

Produkt

Brennroboter zur automatisierten Erstellung von optischen Speichermedien.

Hersteller

Primera Technology
http://primera.eu/de

Preis

Das Modell Pro Xi kostet rund 2.000 Euro, die Variante Pro Xi2 schlägt mit knapp 2.200 Euro zu Buche. Farb-Tintenpatronen mit hoher Ergiebigkeit sind für 46 Euro erhältlich, schwarze Patronen kosten rund 43 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Brennqualität	6
Druckqualität	9
Geschwindigkeit	6
Label-Designer	7
Fehlertoleranz	6

Dieses Produkt eignet sich

optimal für Unternehmen, die regelmäßig große Mengen an optischen Medien brennen und dabei auf eine gute Beschriftungsqualität angewiesen sind.

bedingt für Unternehmen, die nur selten optische Medien in Serie produzieren.

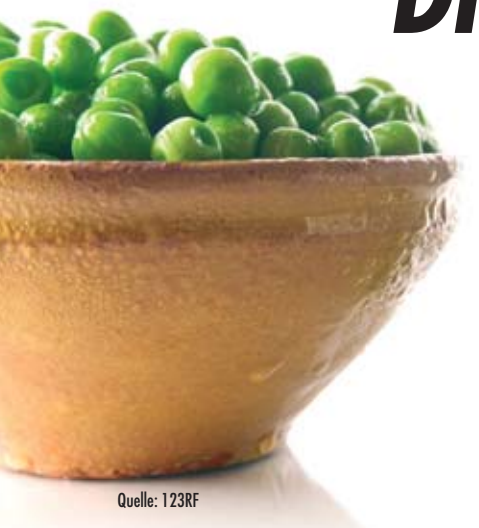
nicht für Unternehmen, in denen keine CD/DVD/BD-Medien gebrannt werden.

Primera Disc Publisher Pro Xi

Erfolgreiche Strategien für Backup & Recovery

Die guten ins Töpfchen…

von Sascha Giebelhausen



Quelle: 123RF

Mal ehrlich: Wer kann als IT-Administrator schon von sich behaupten, dass er noch nie einem Anwender mitteilen musste, dass seine Daten nicht wiederherstellbar sind? Ein ungutes Erlebnis, das umso stärker wiegt, wenn es sich um unternehmenskritische Informationen handelt. Um derlei Datenverlusten vorzubeugen, stellen wir Ihnen in diesem Artikel Strategien zum Thema Backup und Recovery vor, mit denen Sie je nach Unternehmensschwerpunkt für eine Sicherung der wirklich wichtigen Daten sorgen.

Natürlich sollten IT-Verantwortliche auch beim Thema Backup den Fokus auf die Kernprozesse eines Unternehmens richten. So ist etwa eine reine Büroumgebung häufig auf die klassischen Infrastrukturdienste angewiesen: Verzeichnisdienste, E-Mail, Terminalserver, Storage-Systeme, Datenbankserver oder auch die IP-basierte Telefonanlage. Daher ist die Funktionalität und Verfügbarkeit dieser Technologien permanent zu gewährleisten. In kritischen Infrastrukturen hingegen – häufig anzutreffen bei produzierenden Unternehmen – ist es häufig so, dass die klassischen Büroapplikationen und -dienste gar nicht existieren oder für den Betrieb nicht zwingend erforderlich sind. Aufgrund dieser gravierenden Unterschiede bei der prozessualen Ausrichtung eines Unternehmens ist der wichtigste Punkt bei der Einführung eines Backups immer die Planung. Die Umsetzung, also welche Backup-Lösung zum Einsatz kommt, kann erst nach der Konzeptionierung erfolgen, da erst dann alle Anforderungen festgelegt werden.

Wichtige Daten identifizieren

Häufig schätzen die Betreiber eines Rechenzentrums oder die Anwender mehr Daten als höchst kritisch ein, als es in Wirklichkeit sind. Hinzu kommt, dass die Funktionen einer existierenden Backuplösung oft nicht bekannt sind. Die Folge ist nicht selten, dass Unternehmen eine weitere Lösung mit neuen Lizenzen kaufen, obwohl es eigentlich bereits eine Backup-Infrastruktur gibt. Die Konzeptionierungsphase sollte deshalb immer mit der Analyse der zu sichernden Daten beginnen.

Datenspezifikation bedingt Backup-Art

Über ein Backup lassen sich verschiedene Typen von Daten sichern. Die Spezifikation der zu sichernden Daten spielt eine große Rolle, da zwischen Anwendungs- und Betriebssoftware, System-, Anwendungs- und Protokolldaten unterschieden wird. So finden sich in einer Sicherung einzelne Dateien und Ordner, Datenbanken oder virtuelle Infrastrukturen wie XEN, VMware oder Microsoft Hyper-V. Leider kann ein Backup nicht alles abdecken – beispielsweise lässt sich mit einer reinen Datensicherung kein Betriebssystem speichern. Dies ist lediglich mit einem sogenannten Abbild (Image) möglich. Mit dem Speicherabbild lassen sich ganze Partitionen sichern und wiederstellen, es werden alle Daten auf der Partition inklusive Speicherort gesichert. Dies ist notwendig, da für das Starten des Betriebssystems einige Dateien (wie etwa die Auslagerungsdatei) an einer vordefinierten Stelle auf der Festplatte abgelegt sein müssen.

RAID ersetzt kein Backup

Wer wurde nicht schon einmal von besonders schlauen Zeitgenossen auf einen scheinbar so einfachen IT-Sachverhalt hingewiesen: "Backupsoftware ist unnötig, spiegel einfach jeden Server mit einem RAID 1 und falls eine Festplatte kaputt ist, schaltet der Server um und nutzt die funktionierende Festplatte weiter." Dieser technische Prozess ist zwar insoweit korrekt, ein RAID erhöht jedoch nur die Ausfallsicherheit eines Servers – gegen eine Veränderung oder gar Löschung der Daten ist das Unternehmen damit nicht gewappnet, da ja jede Löschung automatisch auf die zweite Festplatte gespiegelt wird.

Per Definition ist ein Backup eine teilweise oder vollständige Kopie von Daten auf ein gesondertes Speichermedium. Technisch gesehen ist ein RAID zwar eine Art Backup. Dies stimmt aber nicht ganz, denn ein professionelles Backup darf nach der Sicherung nicht mehr verändert werden und sollte auf einem anderen physikalischen Gerät abgelegt sein. Hinzu kommt, dass laut den gesetzlichen Anforderungen jedes Unternehmen zu einer ordentlichen, nachvollziehbaren und revisionssicheren Buchführung verpflichtet ist. Insofern die Buchführung nicht noch mit Stift und Papier erfolgt, muss eine Firma ein Backup kaufmännischer Daten vorhalten können.

Kosten und Lebensdauer unterschiedlicher Speichermedien		
Speichermedium	**Kosten**	**Lebensdauer**
Optische Datenträger	0,70 Euro pro GByte	Zehn bis 100 Jahre
Bänder	0,40 Euro pro GByte	50 Jahre
Festplatten	1,80 Euro pro GByte	Zehn Jahre

Es gibt jedoch Ausnahmen: So kann ein einzelner Domänencontroller in einer Active Directory-Domäne ohne weiteres mit dem Imaging-Verfahren gesichert und wiederhergestellt werden. Sobald jedoch ein weiterer Domänencontroller in derselben Domäne existiert, stellt sich das Ganze etwas anders dar. Eine einfache Rücksicherung ist dann nicht mehr möglich, da in diesem Fall die Replikation fehlschlagen würde. In so einem Fall ist dann wiederum ein Daten-Backup die empfohlene Vorgehensweise für die Sicherung und Wiederherstellung.

Verfügbarkeitsanforderungen berücksichtigen

Als zweiter entscheidender Schritt folgt die Analyse der Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten und des Rekonstruktionsaufwands der Daten ohne Datensicherung. Zur Berechnung des Datenvolumens gilt es, eine Speicherplatzanalyse durchzuführen. Dabei kann die Erstellung einer Matrix (mit den Spalten "Server", "lokaler Pfad und Speicherbedarf", "Anzahl der Wiederherstellungspunkte", "gesamter Speicherbedarf") helfen. Zur Minimierung des Speicherplatzbedarfs lassen sich die Daten nach Kritikalität aufteilen. Dabei kann zwischen unternehmenskritischen Daten (kaufmännische Dokumente, Anwendungsdaten et cetera) und privaten Daten (Informationen auf Home-Laufwerken) unterschieden werden. Zudem variieren die Aufbewahrungsfristen je nach Kernkompetenz des Unternehmens. Was jedoch immer gilt: Laut dem Handels- und Steuerrecht ist jedes Unternehmen verpflichtet, kaufmännische Dokumente und Daten wie Jahresabschlüsse, Handelsbücher und Rechnungen für mindestens zehn Jahre unveränderbar aufzubewahren.

Die Wahl des Speichermediums

Grundsätzlich gibt es drei Arten von Speichermedien: Optische Datenträger, Magnetbänder und Festplatten. Davon haben sich jedoch die letzten beiden in professionellen Infrastrukturen bewährt. Der Preis spielt sowohl bei der Backup-Lösung selbst als auch bei den Speichermedien eine erhebliche Rolle. Des Weiteren gibt es gravierende Unterschiede bezüglich der Lebensdauer verschiedener Datenträger. In der Tabelle "Kosten und Lebensdauer unterschiedlicher Speichermedien" finden Sie hierzu eine Aufstellung. Die Preise sind marktübliche Preise und nicht auf die günstigsten DVDs oder Festplatten vom Discounter, sondern auf Produkte für den Einsatz in Unternehmen bezogen. Als Grundlage für die Tabelle verwendeten wir etwa eine SAS-Festplatte mit 15.000 Umdrehungen oder ein LTO4-Band der Marke IBM. Welche Daten auf welches Medium geschrieben werden, hängt immer von der Datenmenge und dem Änderungsvolumen ab.

Optimierung der Sicherungen

Beim aktuellen Datenwachstum ist es wichtig, den bestehenden Speicherplatz sinnvoll zu nutzen und nicht einfach täglich eine Volldatensicherung von allen Daten zu erstellen. Gangbar sind hier derzeit zwei weitere Arten des Backups: Für das tägliche Backup der Daten ist eine inkrementelle Datensicherung das Mittel der Wahl. Dabei werden lediglich alle geänderten Daten seit der letzten inkrementellen oder Volldatensicherung kopiert. Diese Methode kann je nach In-

Bild 1: Die möglichen Gründe für Datenschäden sind vielfältig

frastruktur sehr viel Zeit, Bandbreite im Netzwerk und Speicherplatz sparen. Es gibt jedoch auch Nachteile, denn durch eine inkrementelle Datensicherung erhöhen sich bei einer Rücksicherung Zeit und Aufwand. Dies liegt daran, dass erst die letzte Vollsicherung und danach alle inkrementellen Datensicherungen Schritt für Schritt wiederhergestellt werden müssen. Sollte es seit der letzten Vollsicherung nur wenige Änderungen gegeben haben oder eine hohe Verfügbarkeitsanforderung an die betroffenen Daten bestehen, ist eine differenzielle Datensicherung empfehlenswert. Dabei kommt es lediglich zu einem Speichern aller seit der letzten Vollsicherung geänderten Daten. Damit lässt sich bei der Rücksicherung viel Zeit sparen. Noch recht neu auf dem Markt sind Datensicherungslösungen, die eine Datei unmittelbar nach einer Änderung sichern. Diese Lösungen dienen natürlich einem kontinuierlichen Schutz von Daten und werden häufig für die Absicherung unternehmenskritischer Daten wie E-Mails, Freigaben oder Datenbanken genutzt.

Generationen-Prinzip sorgt für sichere Daten

Wer sich für eine der genannten Datensicherungsarten entschieden hat, muss noch eine Methodik für die Speicherung oder gar Archivierung der Daten finden. Hier hat sich in der Praxis ein Generationenprinzip bewährt. Dieses ist auch als Großvater-Vater-Sohn-Prinzip bekannt.

Sohn-Generation

Diese Generation definiert sich in der Regel als tägliche Datensicherung. Sie sollte an jedem Werktag erfolgen und nach sieben Tagen ablaufen. Empfehlenswert ist hier eine inkrementelle oder differentielle Datensicherung, da sichergestellt sein sollte, dass die Sicherung am nächsten Morgen vor Beginn der Normarbeitszeit abgeschlossen ist. Da innerhalb der ersten fünf Werktage die meisten Wiederherstellungsanforderungen seitens der Anwender angetragen werden, bietet sich hier als Speichermedium eine interne/externe Festplatte, ein SAN oder ein NAS an. Häufig handelt es sich dabei nur um einzelne Dateien oder Ordner.

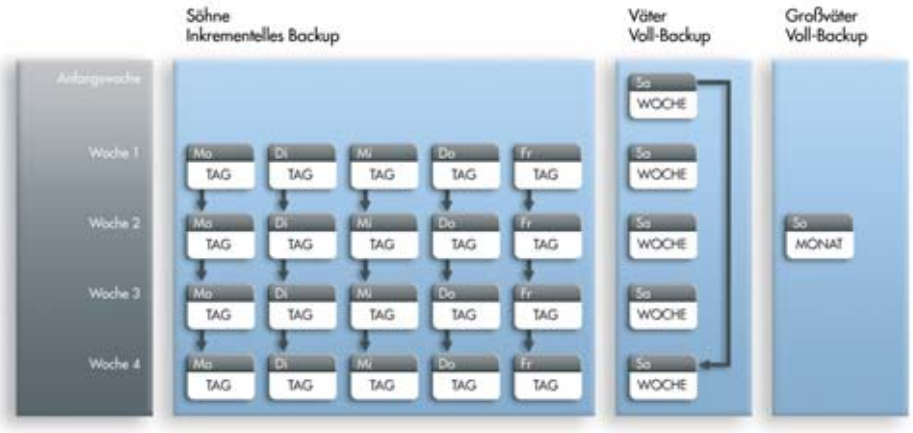


Bild 2: Das Generationen-Prinzip stellt in der Großvater-Stufe die Grundlagen zur späteren Archivierung bereit

Vater-Generation

Die Vater-Generation ist die Wochensicherung und wird normalerweise für vier Wochen vorgehalten. Diese Sicherung ist bevorzugt eine Volldatensicherung und in den meisten Fällen auf Tape abgelegt. Ja nach Infrastruktur oder Backupstrategie kann dies allerdings auch jedes andere Sicherungsmedium sein.

Großvater-Generation

Als Monatssicherung wird zu guter Letzt die Großvater-Generation bezeichnet, da diese bis zu zwölf Monate, und damit am längsten, aufbewahrt werden sollte. Dabei kommt es nicht nur darauf an, die Daten vor Überschreibung zu schützen. Es ist zudem von enormer Wichtigkeit, die Sicherungsmedien zu archivieren. Dies kann über ein Bankschließfach, einen Tresor oder einen Datenträger in einem anderen Gebäude erfolgen. Denn es muss ausgeschlossen sein, dass im Brandfall die Server und die Sicherungen verloren gehen. Dabei sollte stets klar sein, dass eine Tür, eine Wand oder ein Schrank mit einer bestimmten Brandschutzklasse nur für eine gewisse Zeit der Hitze standhalten. Auch sollte der Faktor Naturgewalten nicht außer Acht gelassen werden.

Dem Anwender auf die Finger schauen

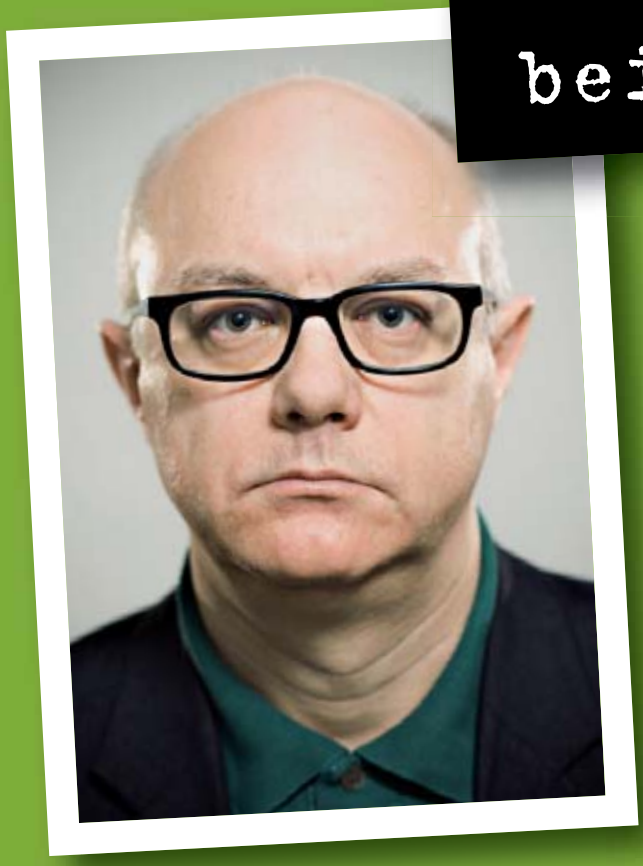
Wie bereits erwähnt, sollte ein Ziel bei der Einführung einer Backup-Lösung eine lange Verwendung sein – fünf Jahre sind hier ein durchaus anstrebenswerter Zeitraum. Daher gilt es stets, das Datenwachstum zu berücksichtigen und ausreichend Puffer in die Speicherplatzanalyse einzuarbeiten. Auch die Ablage von privaten Daten auf Firmenrechnern kann, verstärkt durch das Generationenprinzip, einen exponentiellen Anstieg des benötigten Speicherplatzes zur Folge haben.

Jedoch gibt es für alle Herausforderungen Lösungen: So können durch Quotas die Home-Laufwerke von Anwendern begrenzt oder durch eine interne Verfahrensanweisung das Speichern dienstlicher Daten auf dem selbigen Speicherort unterbunden werden. Wer den Wunsch hat, das Speichern bestimmter Dateitypen einfach zu verbieten, kann dafür ein File Screening anwenden. Dieses sortiert unerwünschte Dateien einfach aus und verhindert, dass etwa private Videos wertvollen Speicherplatz belegen. Viele dieser Funktionen sind bereits Bestandteil der aktuellen Serverbetriebssysteme von Microsoft. *(ln)*

Sascha Giebelhausen ist IT-Security Consultant bei der adMERITia GmbH. Seinen Blog finden Sie unter blog.port389.de.

Vergisst kein Detail in der internen Kalkulation.

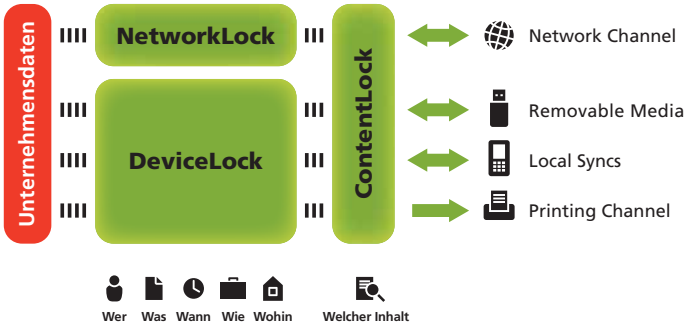
Aber die Datei beim Kunden.



Mitarbeiter sind auch nur Menschen.
Da kann es passieren, dass Daten unverschlüsselt in falsche Hände geraten. Oder gelöscht werden. Oder manipuliert. Oder mit Viren verseucht. Schützen Sie sich davor!

- Kontrolle sämtlicher PC-Schnittstellen, inkl. Webmail, FTP, Facebook & Co.
- Schutz vor Datenbeschädigung und -verlust durch Unachtsamkeit oder Vorsatz
- Individuelle Justierbarkeit
- Für kleine, große und größte Netzwerke
- Über 4 Mio. Installationen
- Referenzen in hochsensiblen Branchen
- Neu! Jetzt mit vollständiger Content- und Kontext-Prüfung

Die Datenflusskontrolle der DeviceLock Endpoint DLP-Suite



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

[www.devicelock.de]

DeviceLock®
Proactive Endpoint Security

Apple iPad im Unternehmenseinsatz

iPadministrator

von Christian Knermann

Adressierte Apple mit iPhone und iPad zunächst hauptsächlich den Consumer-Markt, erfreuen sich die Geräte nicht zuletzt seit Erscheinen des iPhone 4 auch im geschäftlichen Umfeld zunehmender Beliebtheit. Mit dem Betriebssystem-Update auf iOS 4.2.1 haben vom iPhone bekannte Funktionen wie das Multitasking ihren Weg auch auf das iPad gefunden. Für Administratoren stellen sich in Sachen iPad hauptsächlich die Fragen, welche Funktionen zur Verwaltung sich bieten und ob das Gerät auch zu administrativen Zwecken taugt. Diesen Fragen sind wir mit dem Einstiegsmodell mit 16 GByte und Wi-Fi-Unterstützung nachgegangen.

Beim ersten Einschalten weist das Gerät in unmissverständlicher Bildsprache darauf hin, dass es über USB mit einem Computer verbunden werden möchte, auf dem die Apple-Software iTunes installiert ist. Ohne die Freischaltung über iTunes ist das iPad nicht verwendbar. iTunes ist für Mac OS X ab Version 10.5 sowie Windows ab XP SP2 verfügbar. Für die 64-Bit-Varianten von Windows Vista und 7 gibt es einen separaten Installer [1].

Bei der Installation werden neben iTunes selbst weitere Komponenten installiert: "Bonjour" dient der automatischen Erkennung weiterer Apple-Dienste und -Geräte im Netz. Dazu wird ein entsprechender Systemdienst eingerichtet. Der "Apple Mobile Device Support" dient der Anbindung des iPad und verankert sich mit zwei Diensten im System, dem "Apple Mobile Device" und dem "iPod Service". Hinzu kommt der "iTunesHelper" als systemweites Autostart-Objekt, das dafür sorgt, dass iTunes automatisch startet, sobald das iPad angeschlossen wird.

Weiterhin werden die Multimedia-Umgebung Quicktime sowie Apple Application Support als Voraussetzungen für iTunes installiert. Zu guter Letzt hält Apple Software Update alle Komponenten auf aktuellem Stand. Die Update-Funktion war in der Vergangenheit in die Kritik geraten, da sie standardmäßig weitere Apple-Software wie den Browser Safari zur Installation selektierte. Inzwischen ist diese Einstellung aber geändert worden. Die zusätzlichen Komponenten werden zwar weiterhin angeboten, müssen nun aber explizit ausgewählt werden, falls die Installation gewünscht ist.

Aktivierung nur mit iTunes

Ist das iPad nach der Installation von iTunes mit dem Rechner verbunden, so wird es aktiviert. Im Verlauf dieses Prozesses verlangt iTunes nach einer Apple ID beziehungsweise einem iTunes Account. Ein solcher lässt sich auch vorab oder nach Aktivierung des iPads über das Menü "Store / Benutzer-Account erstellen…" anlegen. In beiden Fällen ist wahlweise eine Kreditkarte oder ein clickandbuy-Konto als Zahlungsmethode für im iTunes Store erworbene Medieninhalte und Apps anzugeben. Dies lässt sich umgehen, indem zunächst über den App Store eine beliebige Gratis-App geladen und erst dann der Benutzer-Account erzeugt wird. Dann ist als zusätzliche Zahlungsart die Option "Keine" verfügbar. Das genaue Vorgehen beschreibt ein Apple Support-Artikel [2]. Einmal freigeschaltet, kann das iPad wahlweise über iTunes mit Apps und Medieninhalten betankt werden oder aber selbständig per WLAN kommunizieren.

Die entsprechenden Konfigurationsoptionen finden sich unter dem Punkt "Einstellungen" im Menü "Allgemein / Netzwerk". Sofern eine Internetverbindung nicht automatisch erkannt wird, ist es dort sowohl möglich Wi-Fi-Netze als auch VPN-Verbindungen anzulegen. Falls es sich um ein verstecktes Funknetz handelt, kann der Benutzer die SSID manuell eingeben. Es werden die Verschlüsselungstypen WEP, WPA und WPA2 unterstützt – die letzteren beiden sowohl in der Personal-Variante mit Preshared-Key als auch in der Enterprise-Variante mit Radius-Authentifizierung, die alle ohne Komplikationen funktionierten.

Es ist weiterhin möglich, ein oder mehrere VPN-Profile zu verwalten [3]. Unterstützt werden L2TP, PPTP und Cisco IP-

Sec. Pro VPN-Profil lässt sich jeweils ein separater Webproxy eintragen. Darüber hinaus sind im App Store zusätzliche Clients für mehrere SSL-VPN Varianten kostenfrei verfügbar, darunter unter anderem Cisco AnyConnect. Weitere Informationen liefern zwei Apple Support-Artikel [4,5].

Wir verbanden uns mittels Preshared-Key testweise mit einer Cisco ASA, was ohne Probleme gelang. Bei jedem Verbindungsaufbau ist das individuelle Passwort erneut einzugeben. Es ist nicht möglich, das Passwort dauerhaft im Gerät zu speichern. Ist der Netzwerkkontakt etabliert, stellt sich die Frage nach den grundlegenden Funktionen, wie sie im geschäftlichen Alltag gefragt sind.

Arbeiten mit Browser, E-Mail & Co.

Das iPad bringt Apples Browser Safari mit, der auf dem Rendering-Engine WebKit basiert und durch das Zoomen mittels Fingergesten einen angenehmen Umgang mit Webinhalten ermöglicht – natürlich nur, solange diese nicht als Flash-Objekt vorliegen. In den Einstellungen können Sie im Menü "Safari" einige Parameter setzen. Als Suchmaschinen stehen Google, Yahoo! und Bing zur Wahl. Der Punkt "Betrugswarnung" deaktiviert, falls gewünscht, den integrierten Phishing-Filter. Auch JavaScript und der Pop-Up Blocker können einzeln aktiviert oder deaktiviert werden. Cookies werden standardmäßig nur von besuchten Seiten akzeptiert. Alternativ stehen die Optionen "Nie" oder "Immer" zur Wahl. Letzteres lässt auch Cookies von Drittanbietern zu. Die Kontrolle über gespeicherte Inhalte ist eher rudimentär. Verlauf, Cookies und Cache lassen sich jeweils nur komplett löschen.

Der Zugriff auf E-Mail, Kalender, Kontakte und Notizen erfolgt auf dem iPad über vier einzelne Apps, die im grundlegenden Funktionsumfang des Geräts enthalten sind. In den Einstellungen können unter "Mail, Kontakte, Kalender" entsprechende Accounts angelegt werden. Neben Microsoft Exchange werden unter anderem Google Mail- und Yahoo-Konten unterstützt. Über den Punkt "Andere" lassen sich IMAP- und POP-Server ansprechen. Wir legten zwei Mail-Accounts an, ein Postfach auf einem Microsoft Exchange Server 2003, der per Microsoft ISA Server und Outlook Web Access SSL-gesichert im Web erreichbar ist, sowie ein IMAP-Postfach. Im ersten Fall war neben der E-Mailadresse und Anmeldeinformationen für die Windows-Domäne lediglich der FQDN des ISA-Servers erforderlich, um SSL-verschlüsselt auf den Exchange-Server zuzugreifen.

Anwender können so allerdings nur E-Mail, Kontakte und Kalenderobjekte synchronisieren. Ein Zugriff auf die Notizen des Exchange-Postfachs ist auf diesem Weg nicht möglich, dies funktioniert nur auf dem Umweg über iTunes. Push-Mail, also die umgehende Benachrichtigung über neue E-Mails, kommt standardmäßig nur für den Posteingang zum Tragen. Soll dies auch für weitere Ordner des Postfachs erfolgen, müssen Sie die entsprechenden Unterordner explizit auswählen. Hierbei und beim Arbeiten mit den Postfächern zeigte sich, dass der Mailclient von iOS 4.2.1 einen Kritikpunkt nach wie vor nicht ausräumt: So wird in der Ordnerauswahl die komplette Ordnerhierarchie immer vollständig expandiert. Wer mit vielen Unterordnern arbeitet, ist damit zu häufigem Scrollen gezwungen.

Bei der Integration des IMAP-Postfachs hinterlegen Anwender die Posteingangs- und -ausgangsserver mit den entsprechenden Anmeldeinformationen. Neben den E-Mails können via IMAP auch Notizen synchronisiert werden. Ein Abgleich per Push ist nicht möglich, stattdessen kann das Laden neuer E-Mails wahlweise manuell oder zeitgesteuert erfolgen, wobei Intervalle von 15, 30 oder 60 Minuten zur Auswahl stehen. Der Zugriff auf mehrere Mail-Accounts ist auf einfache Weise möglich. Die Mail-App fasst über die Ansicht "Alle" die Posteingänge der angebundenen Accounts zusammen. Somit erscheinen die E-Mails aller Konten chronologisch sortiert in einer gemeinsamen Ansicht.

Der Mail-Client bietet Unterstützung für gängige Attachements wie Grafikformate (GIF, JPEG, PNG, TIFF), Text-Formate (TXT, RTF), Adobe PDF, die Anwendungen der Apple iWork Suite sowie Microsoft Office-Formate. Dabei werden Word, Excel und Powerpoint der Versionen 97 bis hin zum aktuellen Office 2010 erkannt und in einem Viewer geöffnet. Von dort lassen sich die Dokumente je nach Typ in anderen Apps öffnen.

Zentrales Management nur mit starken Einschränkungen

Alle bislang beschriebenen Konfigurationsschritte haben wir direkt am Gerät vorgenommen. Über iTunes wird das iPad zwar aktiviert und mit iOS-Updates versorgt (zudem wird jeweils ein Backup des Geräts angelegt, sobald es mit iTunes verbunden wird), auf diesem Weg lassen sich aber keine Einstellungen zentralisiert propagieren. Um im Unternehmensumfeld zahlreiche iPads auszurollen, müsste ein Administrator entweder sämtliche Geräte von Hand vorkonfigurieren oder auf entsprechend versierte Endanwender hoffen. Sind die Geräte dann einmal verteilt, ist zudem kein zentrales Management und keine Kontrolle unternehmensweiter Sicherheitsrichtlinien mehr möglich.

Erschwerend kommt hinzu, dass ein iPad mit einer iTunes-Installation in einer 1-zu-1-Beziehung steht. Wird das iPad mit einer anderen iTunes-Instanz verbunden, so lassen sich mit dem iPad gekaufte Apps und Inhalte zwar übertragen, dies ist aber deutlich zeitaufwändiger als ein regulärer Synchronisationsvorgang, so dass es sich in der Praxis nicht empfiehlt, ein iPad häufig an unterschiedlichen Rechnern zu verwenden. Verfügt ein Endanwender selbst über eine iTunes-Installation, entzieht sich ein iPad somit weitestgehend der Fürsorge des Administrators.

Es ist möglich, iTunes über Registrierungsschlüssel restriktiv zu konfigurieren

[6], und wenn die entsprechenden Client-Computer einer Active Directory Domäne angehören, lassen sich diese Einstellungen auch als Gruppenrichtlinie zentral verteilen. Auf diesem Weg wird natürlich nur iTunes beeinflusst und nicht das iPad selbst. Um dieses Thema zu adressieren, stellt Apple einige Ressourcen [7] bereit, allen voran das kostenlose iPhone-Konfigurationsprogramm 3.2. Das Tool ist für Microsoft Windows [8] und Mac OS X [9] verfügbar und trotz seines Namens auch auf das iPad anwendbar.

Die Oberfläche des Tools ist an iTunes angelehnt. In einer Leiste am linken Bildschirmrand verwalten Sie innerhalb einer Bibliothek mehrere Geräte, indem Sie ihnen Konfigurationsprofile zuweisen. Der gleichnamige Ordner ist anfänglich noch leer. Über die Schaltfläche "Neu" legen Sie ein neues Profil an, das mit einem eindeutigen Namen versehen werden muss. Die Dropdown-Box unter dem Punkt "Sicherheit" stellt zur Wahl, ob es dem Endanwender erlaubt ist, das Profil wieder vom iPad zu entfernen. Die Einstellung "Nie" verbietet dies und sperrt durch das Profil vorgegebene Einstellungen gegen Änderungen. Die Möglichkeiten der Profile gehen über die Einstellungen hinaus, die am Gerät selbst möglich sind. So können Sie die Code-Sperre an die Sicherheitsanforderungen des Unternehmens anpassen und beispielsweise erzwingen, dass ein alphanumerisches Passwort nötig ist. Es kann eine Ablauffrist zwischen einem und 730 Tagen definiert werden, nach der der Code geändert werden muss. Sofern gewünscht ist, dass sich das Gerät nach Falscheingabe des Codes selbständig löscht, konfigurieren Sie zwischen einem und 16 Fehlversuchen (in den lokalen Einstellungen des iPad lässt sich die Vorgabe von zehn Fehlversuchen ohne das Konfigurationsprogramm nicht ändern).

Im Bereich der "Einschränkungen" finden sich einige Einstellungen, die sich auf das iPhone beziehen und auf das iPad nicht anwendbar sind. Dies betrifft zum Beispiel die Verwendung der beim iPad nicht vorhandenen Kamera. Andere Optionen haben im Unternehmensumfeld durchaus auch auf dem iPad ihre Daseinsberechtigung. So ist es möglich, die Verwendung von Youtube oder dem iTunes Music Store zu verbieten, sowie verschlüsselte Backups zu erzwingen. Letzteres ist dringend zu empfehlen, da sämtliche Einstellungen und Inhalte vom iPad in ein Backup wandern.

Ist ein Profil fertig konfiguriert, lässt es sich über die Geräte-Ansicht installieren. Es wird dabei allerdings nicht sofort angewendet. Die Installation muss der Anwender auf dem iPad manuell bestätigen. Alternativ zur direkten Installation via USB können Sie ein Konfigurationsprofil auch als E-Mail-Anhang oder Web-Download verteilen. Dazu bietet das Konfigurationsprogramm eine Export-Option, die ein Profil als XML-Datei mit der Endung *.mobileconfig speichert. Die Sicherheitsoption "Konfigurationsprofil signieren" schützt das Profil zwar gegen nachträgliche Änderungen, es ist aber lesbar und enthält beispielsweise WLAN-Schlüssel im Klartext.

Die dritte Option "Verschlüsseltes, signiertes Konfigurationsprofil für dieses Gerät erstellen" verschlüsselt das Profil komplett. Es wird dabei aber pro zu konfigurierendem iPad eine eigene Datei erzeugt, was den Rollout an eine größere Anzahl von Endgeräten erschwert. Hinzu kommt, dass es in allen Fällen dem Endanwender überlassen bleibt, die Installation des Profils durchzuführen. Es ist somit auf diesem Weg nicht möglich, zentrale Vorgaben automatisiert auf einer größeren Anzahl von Endgeräten durchzusetzen und nachträglich zu verändern. Sofern eines der E-Mailkonten auf einem Microsoft Exchange-Server gehostet wird, bietet sich als Alternative die Konfiguration von ActiveSync-Richtlinien [10] an. Auf diesem Wege lassen sich zwar längst nicht alle Einstellungen des iPads adressieren, aber es ist immerhin möglich, den Passwort-Schutz auf dem Gerät zu erzwingen und Vorgaben zur Komplexität des Codes zu machen. Weiterhin können Sie das Gerät über den Exchange-Server im Verlustfall aus der Ferne zurücksetzen.

Verteilung von Apps

Der zentralen Verteilung von Applikationen steht deren Verknüpfung mit individuellen iTunes-Accounts entgegen. So wird es im Unternehmensumfeld kaum praktikabel sein, ein und denselben Firmen-Account mit entsprechenden Zahlungsinformationen auf den iPads aller Endanwender zu benutzen. Eine Alternative bietet der App Store mit der Option, Apps zu verschenken. So kann ein Administrator über den Firmen-Account Apps beschaffen und an User zuweisen, die mit individuellen iTunes-Accounts – wahlweise mit einer persönlichen oder keiner

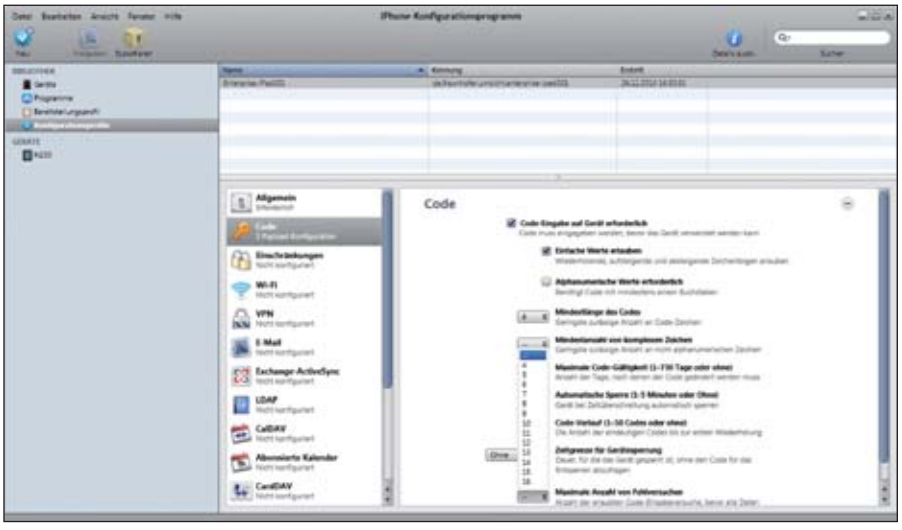


Bild 1: Das Konfigurationsprogramm bietet Einstellungen, die lokal auf dem iPad nicht verfügbar sind

Bild 2: Die Installation eines Profils muss am Gerät bestätigt werden

Zahlungsmethode – eingeloggt sind. Die Installation der App muss der Endanwender allerdings selbst durchführen.

Wollen Sie jedoch selbstentwickelte Apps verteilen, führt der Weg über eine kostenpflichtige Teilnahme an Apples Developer Programm. Diese ist erforderlich, da Apps signiert sein müssen, damit das iPad sie akzeptiert und ausführt. Apps lassen sich in ein sogenanntes Bereitstellungsprofil verpacken und wahlweise über iTunes oder das iPhone-Konfigurationsprogramm installieren. Details liefert der "Enterprise Deployment Guide" [11].

Apps für die Remote-Administration

Soll das iPad für den Administrator auf Reisen als alleiniger Begleiter das Notebook komplett ersetzen, stellt sich insbesondere die Frage nach Möglichkeiten zur Fernwartung und zum Zugriff auf Unternehmensanwendungen. Im App Store finden sich hierzu einige Clients für unterschiedliche Remote-Protokolle.

Der dänische Anbieter MochaSoft [12] bietet Clients für RDP und VNC. Wenngleich der "Remote Desktop for iPad" den Zugriff auf Microsoft Server-Betriebssysteme aus lizenzrechtlichen Gründen vom Hersteller offiziell nicht unterstützt, funktioniert dieser doch zufriedenstellend. Unterstützt werden Verbindungen zu Windows XP, Vista und 7. Der Client "Mocha VNC for iPad" unterstützt die Spielarten RealVNC, Tight VNC und UltraVNC sowie das Remote-Management von Mac OS X. Beide Clients sind als kostenlose Lite Versionen verfügbar, die Vollversionen schlagen mit jeweils 4,99 Euro zu Buche. Bereits die Lite Versionen eignen sich für den gelegentlichen Zugriff auf Remote-Systeme, beispielsweise um nach dem Stand der Dinge im Ereignisprotokoll zu sehen. Mauscursor und Klicken werden über Fingertippen realisiert. Für Eingaben kommt die virtuelle Tastatur des iPads zum Einsatz. Einige Funktionen, die für produktives Arbeiten eigentlich unerlässlich sind, so etwa die Emulation der rechten Maustaste oder Sondertasten wie die Windows-Taste oder Strg+Alt+Entf, sind allerdings den kommerziellen Varianten vorbehalten. Ähnliches gilt für die App "Telnet for iPad": Der grundsätzliche Zugriff auf Linux Shells ist mit diesem Werkzeug in der Lite Version möglich. Erweiterte Eingaben und Tastenkombinationen bietet auch hier nur die Vollversion für 4,99 Euro. Im Test gelangen uns allerdings nur nicht mehr ganz zeitgemäße und aus Sicherheitsgründen nicht wirklich vertretbare Telnet-Verbindungen, SSH-Verbindungen kamen nicht zustande.

Für SSH-Zugriffe und zudem als VNC-Client empfiehlt sich das mit 7,99 Euro etwas teurere "iSSH" von Zingersoft [13]. Die Software kann mehrere gleichzeitige Verbindungen aufbauen und unterstützt das Multitasking von iOS 4.2.1. Der Hersteller kündigt auf seiner Webseite zudem die Unterstützung der Protokolle RDP und NoMachine NX sowie einen separaten X11-Client an.

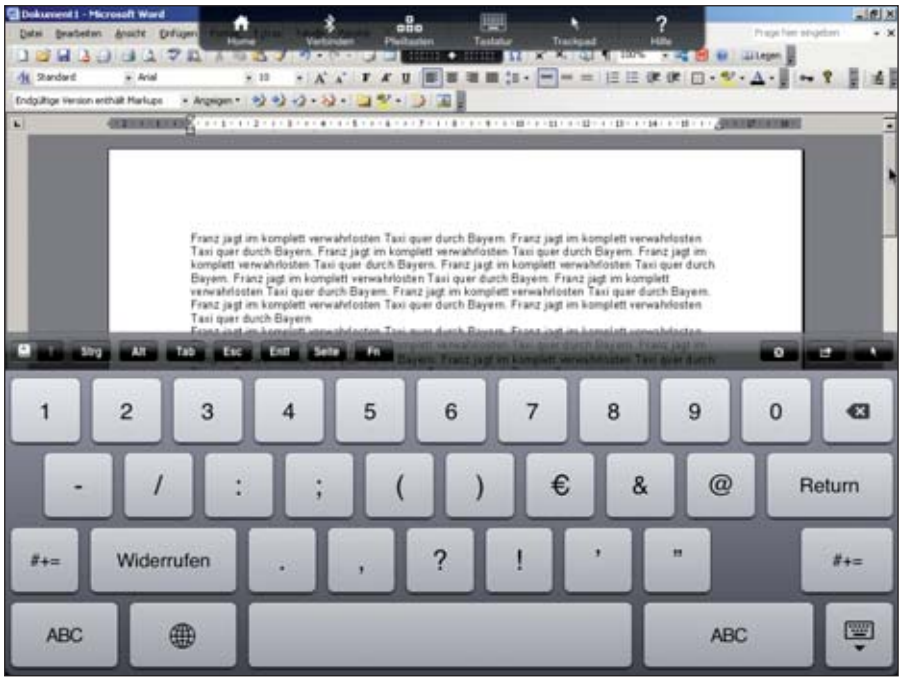


Bild 3: Der Citrix Receiver for iPad bietet nützliche Zusatzfunktionen, die die Bedienung von Windows-Applikationen erleichtern

Eine XenApp- oder XenDesktop-Infrastruktur vorausgesetzt, bringt der kostenfreie "Citrix Receiver for iPad" [14] Applikationen und Desktops mittels ICA-Protokoll auf das iPad-Display. Der Client erwartet dazu lediglich die Adresse eines Webinterface-Servers. Der Zugriff kann dabei auch von extern SSL-gesichert über das Citrix Access Gateway erfolgen. Nach erfolgreicher Authentisierung bietet der Client sämtliche verfügbaren Ressourcen in einer optisch an den App Store angelehnten Ansicht an. Einzelne Anwendungen oder Desktops lassen sich mittels Tippen der Startseite des Receiver hinzufügen und von dort starten.

In einer laufenden Session lässt sich am oberen Bildschirmrand eine Leiste ausklappen. Diese enthält einige Funktionen, welche die Arbeit auch auf dem kleinen iPad-Display und ohne externe Tastatur erleichtern. So ist es möglich, ein On-Screen-Display mit Pfeiltasten einzublenden, um den Cursor beispielsweise in Texten zu bewegen. Die Tastatur blendet das übliche virtuelle Keyboard des iPads ein, das allerdings um eine zusätzliche Leiste mit Funktionstasten wie Strg, Alt und Tab ergänzt wurde. Tippen löst einen Mausklick an der entsprechenden Stelle aus. Alternativ dazu blendet das Trackpad einen Mauszeiger in die Remotesession ein, der sich mittels Wischgesten positionieren lässt. In diesem Modus löst ein Tippen an beliebiger Stelle einen Mausklick an der Position des Cursors aus. Tippen mit zwei Fingern entspricht einem Rechtsklick. Auch mit diesen Hilfsmitteln lassen sich Remote-Anwendungen natürlich nicht beliebig schnell und flüssig bedienen. Aber immerhin ist es mit dem Receiver möglich, selbst komplexere Anwendungen zielgerichtet zu steuern.

Fazit

Auch ohne Zusatzprogramme ist das iPad durch die Unterstützung gängiger Office-Formate für den geschäftlichen Alltag gut gerüstet. OpenOffice-Dokumente bleiben allerdings außen vor und auch via S/MIME verschlüsselte E-Mails liest die Mail-App nicht, so dass nicht alle Anwendungsfälle abgedeckt sind. In den meisten Fällen reichten die Funktionen aber aus und mit den diversen Remote Clients kann selbst ein Administrator grundlegende Monitoring- und Wartungsaufgaben aus der Ferne erledigen. Ist eine größere Menge von Geräten zentral zu verwalten, lassen die aktuell gebotenen Möglichkeiten allerdings noch Wünsche offen. Apple bietet zwar eine Schnittstelle für das kabellose Management [15], überlässt die Entwicklung entsprechender Infrastrukturlösungen aber Drittanbietern.

Bestehen die Ziele vor allem darin, unterwegs grundsätzliche E-Mail- und PIM-Aufgaben zu erledigen sowie Medieninhalte zu konsumieren, kann das Gerät allerdings mit seiner Bedienbarkeit und der langen Akkulaufzeit überzeugen und gibt sich im Handgepäck deutlich schlanker als ein Netbook. *(jp)*

Link-Codes

[1] iTunes 10.2 für Windows (64 Bit)
B4P61

[2] iTunes App Store-Account ohne Kreditkarte erstellen
B4P62

[3] VPN unter iOS konfigurieren
B4P63

[4] Unterstützte Protokolle für VPN
B4P64

[5] VPN Server Configuration for iOS 4 Devices
B4P65

[6] Client-Computer unter Windows: So verwalten Sie Steuerungsfunktionen in iTunes
B4P66

[7] iPad Enterprise-Support
B4P67

[8] iPhone-Konfigurationsprogramm 3.2 für Windows
B4P68

[9] iPhone-Konfigurationsprogramm 3.2 für Mac OS X
B4P69

[10] "iPad in Business Deployment Scenarios and Device Configuration Overview"
B4P60

[11] "iPhone OS Enterprise Deployment Guide"
B4P6A

[12] MochaSoft
B4P6B

[13] Zingersoft iSSH
B4P6C

[14] Citrix Receiver für iPad
B4P6D

[15] "iPhone in Unternehmen: Kabellose Anmeldung und Konfiguration"
B4P6E

Vorteilspreis für IT-Administrator Abonnenten

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

Exchange-Training

München, 06. Juli 2011
Hamburg, 16. August 2011

Trainings-Partner:

Die Komplexität einer Exchange-Infrastruktur ist äußerst hoch und nur mit solidem Wissen ist der Administrator in der Lage, diese zuverlässig und verfügbar zu betreiben, sowie wichtige Features bereitzustellen, die die Anwender für ihre tägliche Arbeit benötigen.

Daher bietet IT-Administrator ein ganztägiges Exchange-Training in Hamburg und München an, das praxisnahes Know-How zu Hochverfügbarkeit, der Veröffentlichung von Exchange im Internet und Troubleshooting vermittelt.

Themen des Trainings:

Hochverfügbarkeit in Exchange Server 2010
- Design
- Konfiguration und Management

Veröffentlichung von Exchange (2003, 2007, 2010) ins Internet über TMG
- OWA
- Outlook Anywhere
- ActiveSync

Troubleshooting Exchange (2003, 2007, 2010)
- Einführung in Tools zur Fehlerdiagnose
- Performance Monitoring

Referent: Jürgen Haßlauer, infoWAN GmbH

Termin: 06. Juli 2011
Ort: ExperTeach Training Center München, Wredestr. 11, 80335 München

Uhrzeit: 10.00 bis ca. 17.30 Uhr

Anmeldeschluss: 28. Juni 2011

Termin: 16. August 2011
Ort: ExperTeach Training Center Hamburg, Esplanade 6, 20354 Hamburg

Uhrzeit: 10.00 bis ca. 17.30 Uhr

Anmeldeschluss: 09. August 2011

Trainings-Partner:

Teilnahmegebühren:
Für IT-Administrator Abonnenten Euro 95,- (zzgl. 19% MwSt.), für Nicht-Abonnenten Euro 165,- (zzgl. 19% MwSt.).
Die Teilnehmerzahl ist auf 25 begrenzt.

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

Distributed File System unter Windows Server 2008 R2 einrichten

Verteilte Daten-Sicherheit

Quelle: Spectral-Design - Fotolia.com

von Thomas Gronenwald

Stets drohen sie: unerwartete Hardwareausfälle, notwendige Wartungszyklen, Stromausfälle oder sogar Komplettausfälle einzelner Rechenzentren. Mit einem vergleichbar geringen Aufwand und geeigneten Maßnahmen bleibt das Restrisiko jedoch kalkulierbar. Eine sehr interessante Möglichkeit im Dateiserver-Umfeld ist neben dem typischen, aber kostspieligen Cluster das DFS (Distributed File System). In diesem Workshop zeigen wir Ihnen, wie Sie das DFS unter Server 2008 R2 optimal nutzen.

Viele Administratoren denken beim Stichwort verteiltes Dateisystem vor allem an "verschiedene Server unter einer Freigabe", damit liegen Sie im ersten Moment auch gar nicht so falsch – im Gegenteil. DFS bietet aber weitaus mehr Funktionalitäten, die einen Einsatz viel universeller gestalten können. Klassischerweise verwenden Administratoren einen Cluster, um die Verfügbarkeit von Fileservern zu erhöhen. Das DFS kann durchaus eine lohnenswerte Alternative sein, denn auch hiermit lassen sich redundante Umgebungen aufbauen – einige Fallstricke gilt es jedoch stets zu betrachten. Um das verteilte Dateisystem unter Windows Server 2008 R2 vollumfänglich und redundant einsetzen zu können, sind einige konzeptionelle Aspekte genauer zu prüfen und abzuwägen.

Ausfallsicherheit im Netzwerk

Soll eine IT-Infrastruktur ausfallsicher sein, reicht es üblicherweise nicht, viel Geld in neue und hochleistungsfähige Server zu investieren. Vielmehr gilt es, ein Hauptaugenmerk auf die Basisinfrastruktur zu legen, das physikalische Netzwerk. Angefangen beim Rückrat der Infrastruktur sind die heutzutage redundant untereinander vernetzten Core-Switches eine Mindestanforderung in jeder größeren Umgebung. Identisch verhalten sich die Etagenverteiler (Switches) – auch hier ist eine redundante Anbindung an die jeweiligen Core-Switches nicht nur erstrebenswert, sondern ein Pflichtprogramm. Eine Konstellation aus Layer 3-Switching im Core- und einem Layer 2-Switching im Etagenbereich bildet somit eine durchaus leistungsfähige Netzwerkinfrastruktur. Ebenso empfiehlt es sich, alle Serversysteme redundant an die Core-Switche anzubinden. In Zeiten der immer stärker in den Vordergrund tretenden Virtualisierung ein eher leicht zu realisierendes Ziel.

Ausfallsicheres Active Directory

Normalerweise sollte ein ausfallsicheres Active Directory bereits selbstverständlich sein. Die Realität zeigt aber, dass auch hier zu oft schwerwiegende Fehler sowohl bei der Konzeption als auch im eigentlichen Betrieb gemacht werden. In einem ausfallsicheren Active Directory ist es mehr als erstrebenswert, mindestens zwei Domain Controller (DC) zu betreiben, welche die Anmeldedienste und den globalen Katalog bereitstellen. Existieren mehrere Standorte, sind entsprechend weitere Domain Controller nach Bedarf zu platzieren. Zudem bilden in der Regel die vorhandenen DCs eine redundante DNS-Struktur zur ordnungsgemäßen Namensauflösung. Ohne ein funktionierendes und ausfallsicheres Active Directory kann nämlich auch keine redundante DFS-Struktur betrieben werden.

In Zeiten der Virtualisierung sollte daneben mindestens ein DC pro Domäne physikalischer Natur entsprechen. Plausible Gründe hierfür gibt es reichlich: Probleme mit der Zeitsynchronisation und dem Virtualisierungshost, Pause- und Safe State-Modus von virtuellen Maschinen, die zum Komplettausfall führen, nicht unterstützte Snapshots (Imagebackups und Imagerestores), die unweigerlich zum USN Rollback führen, und so weiter.

Grundlagen des DFS

Neben den genannten Aspekten müssen Sie je nach Infrastruktur noch zusätzliche Punkte betrachten. So sind beispielsweise Notfall-, Administrations- und Sicherheitskonzepte wesentliche Bestandteile einer redundanten DFS-Struktur. Bevor Sie mit der generellen Konfiguration beginnen können, widmen wir uns kurz den Grundlagen beziehungsweise den einzelnen Begrifflichkeiten zum Distributed File System. Unterschieden wird innerhalb des DFS unter Windows Server 2008 R2 zwischen:

- DFS-Stamm (DFS-Root)
- DFS-Namespace (DFS-N)
- DFS-Ordner (DFS-Folder)
- DFS-Ordnerziele (DFS-Target)
- DFS-Replikation (DFS-R)

DFS-Stamm (DFS-Root)

Der DFS-Stamm ist der Ausgangspunkt des Namespaces. Hier wird zwischen eigenständigen- und domänenbasierten Namespaces unterschieden. Der Unterschied liegt hier vor allem beim Aufruf des Namespaces. Auf einen domänenbasierten DFS-Stamm wird über den Domänennamen zugegriffen: "\\Domain.xyz\Namespacestamm". Hingegen wird auf einen eigenständigen DFS-Stamm mit dem jeweiligen Computerkonto zugegriffen: "\\Servername\Namespacestamm". Der große Vorteil eines domänenbasierten Namespace ist, dass dieser auf mehreren Namespace-Servern (in diesem Szenario unsere Domänen Controller) gehostet werden kann, um die Verfügbarkeit des Namespaces zu erhöhen. Ebenso ist eine Replikation von Zielordnern nur über einen domänenbasierten Namespace möglich.

DFS-N (Namespace)

Bestandteil einer jeden DFS-Struktur ist zudem der sogenannte DFS-Namensraum (DFS-N). Der Namespace-Server kann ein Mitgliedsserver oder ein Domänencontroller sein. Der DFS-N stellt sozusagen die Wurzel der Freigabe bereit, unterhalb der dann die Freigaben der übrigen Server verknüpft werden. Die Voraussetzungen für die Nutzung von DFS-N sind:

- Nutzung eines Serverbetriebssystems zum Bereitstellen eines Namespaces,
- Installation entsprechender Rollendienste (DFS und DFS-Namespace),
- Ausführung des DFS-Dienstes.

DFS-Folder und -Targets

Ordner werden innerhalb einer DFS-Struktur für die Gliederung des Namespaces genutzt – so erhält dieser eine Hierarchie. DFS-Ordner wiederum werden genutzt, um das DFS-Target zu verlinken. Ein Ordnerziel ist dabei ein UNC-Pfad einer Freigabe, der einem Ordner in einem Namespace zugeordnet wird. Das Ordnerziel ist der Ort (Fileserver), an dem die Daten und Inhalte somit gespeichert werden. Wenn Benutzer einen Ordner mit verknüpften Ordnerzielen im Namespace durchsuchen, erhält der Client einen Verweis, der ihn transparent an eines der Ordnerziele umleitet.

DFS-R (Replikation)

Einige Vorteile von DFS haben wir nun bereits kennengelernt. Hierzu zählt beispielsweise die Bereitstellung von Freigaben unterschiedlicher Server innerhalb eines Namensraums. Hinzu kommt ein einfacher Zugriff auf Dateien mit hoher Verfügbarkeit, Lastenausgleich und WAN-freundlicher Replikation. Hierbei besteht die Möglichkeit, Daten redundant zu speichern – also einen DFS-Ordner über beliebig viele Fileserver replizieren zu lassen. Genauer gesagt bedeutet dies, dass jeder Server über eine Freigabe verfügt, die mit einer anderen Freigabe beliebig vieler anderer Server repliziert werden kann – und das nicht nur innerhalb eines Standortes, sondern auch über das WAN. In der Praxis sind das beispielsweise Freigaben, die Dokumente und Vorlagen, sowohl in der Unternehmenszentrale als auch in den einzelnen Zweigstellen, bereitstellen. Die jeweiligen Server sind dementsprechend an den einzelnen Standorten platziert.

Denkbar sind hier ebenso Szenarien, die von redundanter Datenhaltung bis zu diversen Sicherungskonzepten reichen. Eine wesentliche Neuerung bei der DFS-Replikation ist die Option "Schreibgeschützter replizierter Ordner". Ein solcher Ordner ist ein replizierter Ordner auf einem bestimmten Server, in dem die Benutzer keine Dateien hinzufügen oder ändern können. Dies ist hilfreich bei schreibgeschützten Ordnern, die mit einem oder mehreren zentralen Servern synchron bleiben sollen – etwa Installationsordner für Software oder Ordner, die veröffentlichte Dokumente und Vorlagen enthalten. Vor Windows Server 2008 R2 konnte ein schreibgeschützter replizierter Ordner nur simuliert werden, indem die Freigabeberechtigungen und Zugriffssteuerungslisten (Access Control Lists, ACLs) manuell für den Ordner festgelegt wurden, um das unbeabsichtigte Ändern oder Hinzufügen zu vermeiden.

Neuerungen unter Server 2008 R2

Neu unter Windows Server 2008 R2 ist zum einen die Möglichkeit, die Option "Access-based Enumeration" in den DFS-Verwaltungstools zu konfigurieren. Bei der "Zugriffsbasierten Aufzählung", so wird es etwas unsauber ins Deutsche übersetzt, werden nur die Dateien und Ordner angezeigt, für die der jeweilige Benutzer Zugriffsberechtigungen besitzt. Besitzt ein Benutzer für einen Ordner keine Leseberechtigungen, wird der Ordner in der Benutzeransicht ausgeblendet. Ebenso neu sind einige Leistungsverbesserungen. DFS-Namespaces unter Windows Server 2008 R2 umfassen drei neue Leistungsindikatoren, mit denen Sie unterschiedliche Aspekte von DFS-Namespaces überwachen können:

DFS-Kompatibilität

Betriebssystem	DFS-Client	DFS-Root	DFS-Ziel
Windows Server 2008	Ja	Ja	Ja
Windows Vista	Ja	Nein	Ja
Windows Server 2003 (Web, Standard, Enterprise, Datacenter)	Ja	Ja	Ja
Windows XP	Ja	Nein	Ja
Windows 2000 Server	Ja	Ja	Ja
Windows 2000 Professional	Ja	Nein	Ja
Windows NT4 Server	Ja	Ja (kein Domain-Mode)	Ja
Windows NT4 Workstation	Ja	Nein	Ja
Windows 98 und Me	Ja (kein Domain-Mode)	Nein	Ja

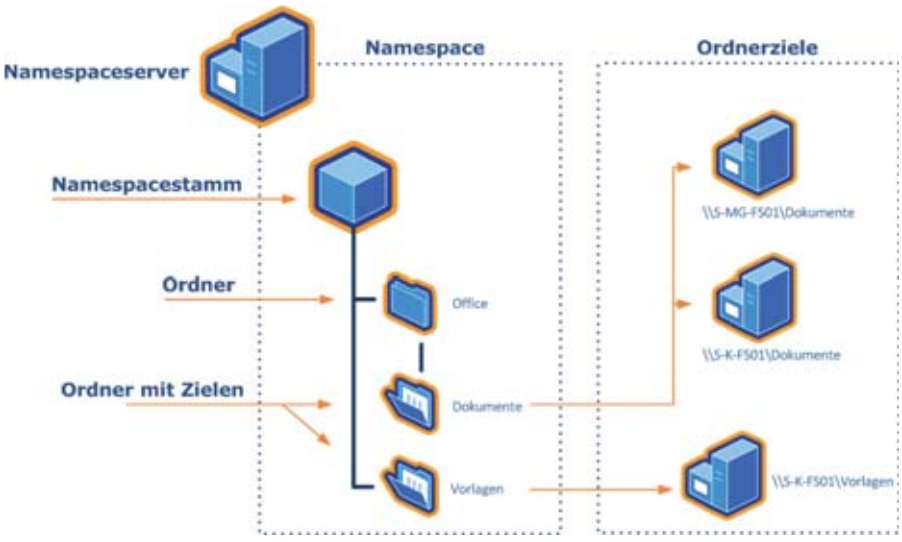


Bild 1: Der DFS-Namensraum (Namespace) ist Bestandteil jeder DFS-Struktur

- DFS-Namespace-Dienst – API-Warteschlange: Zeigt die Anzahl der zu bearbeitenden Anforderungen in der Warteschlange des DFS-Namespace-Dienstes an.
- DFS-Namespace-Dienst – API-Anforderungen: Zeigt Leistungsdaten über Anforderungen (etwa das Erstellen eines Namespaces) an den DFS-Namespace-Dienst an.
- Weiterleitungen für DFS-Namespace-Dienst: Zeigt Leistungsdaten über verschiedene Weiterleitungsanforderungen an, die vom DFS-Namespace-Dienst verarbeitet werden.

Beim Bereitstellen großer domänenbasierter Namespaces im Windows Server 2008-Modus mit 5.000 DFS-Ordnern (Verknüpfungen) oder mehr benötigt der DFS-Namespace-Dienst deutlich weniger Zeit zum Starten. Auch beim Bereitstellen sehr großer domänenbasierter Namespaces im Windows Server 2008-Modus mit mehr als 300.000 DFS-Ordnern zeigt das Release 2 Verbesserungen.

Versucht ein DFS-Client das erste Mal, auf einen domänenbasierten Namespace zuzugreifen, stellt ein Domänencontroller dem Client eine Liste von Namespace-Servern zur Verfügung. Diese Liste von Namespace-Servern wird als Stammweiterleitung bezeichnet. Unter Windows Server 2008 R2 können Sie einzeln die Weiterleitungen zu bestimmten Namespace-Servern aktivieren und deaktivieren. Dadurch können Administratoren einen Namespace-Server zeitweise offline schalten, um Wartungsarbeiten durchzuführen.

Redundante DFS-Struktur

Um eine redundante Infrastruktur betreiben zu können, haben Sie nun bereits einige essenzielle Bestandteile kennengelernt. Wie könnte nun ein Beispiel-Szenario für ein Unternehmen mit einem einzelnen Standort aussehen? Hierfür gilt es folgende Fragestellungen zu beantworten:

- Entspricht Ihre Netzwerkinfrastruktur den genannten Anforderungen?
- Können Sie auf ein funktionierendes und ausfallsicheres Active Directory zurückgreifen?

Wenn Sie beide Fragen mit "Ja" beantworten, können Sie mit der weiteren Konzeptionierung beginnen. Hierzu sind folgende Fragen zu klären:

- Welche Server stellen Ihre DFS-Namespaces bereit?
- Ist für eine ausreichende Redundanz gesorgt?
- Gibt es Abhängigkeiten oder Sicherheitsrichtlinien, die eine Kombination von Rollen untersagen?

In der Praxis ist es durchaus möglich, den domänenbasierten Namespace auf bereits vorhandene Domain Controller oder Fileserver (Windows Server 2008 R2 SP1) zu platzieren. In der Regel entsteht hierdurch keine negative Beeinträchtigung hinsichtlich der Performance – der Zugriff auf die Ressourcen geschieht bekanntermaßen nicht über den Namespace-Server, sondern direkt auf der Ressource. Nichtsdestotrotz gibt es einige starke Argumente, die einen dedizierten Namespace-Server voraussetzen. Beispielsweise sind in größeren Umgebungen verschiedene Teams für die Administration von Active Directory und DFS verantwortlich. Dementsprechend schwierig wird es mit der Delegation und den Zuständigkeiten von Berechtigungen. Ein weiterer, sehr wichtiger Grund ist das Thema Sicherheit. Im Optimalfall sind Ihre Domain Controller mit einer eigenen Security Policy (Hardening) versehen, so dass unnötige Dienste, Ports und Programme deaktiviert sind und nur der nötige Replikationsverkehr und die damit verbundenen Dienste erreichbar und aktiv sind. Hier ist es nicht ratsam, verschiedene Infrastrukturdienste zu kombinieren. Entscheiden Sie sich in diesen Fällen immer für einen dedizierten Namespace-Server. In unserem Testszenario haben wir uns lediglich wegen der einfacheren und verständlicheren Vorgehensweise für die Kombination von DFS-Namespace und DC entschieden.

Die Konfiguration von DFS ist nicht allzu schwierig. Die grundlegenden Arbeiten können Sie mit dem Assistenten vornehmen. Als Erstes müssen Sie auf Ihren Namespace-Servern (in unserem Beispiel Domain Controller, S-MG-DC01 und S-MG-DC02) die DFS-Namespace-Rolle hinzufügen. Sie benötigen für den Namespace-Server daher nur die Rollen "Verteiltes Dateisystem" und "DFS-Namespaces".

Die DFS-Funktionalität wird später von den beiden Fileservern (S-MG-FS01 und S-MG-FS02) übernommen. In diesem Fall wurde der Name "Ablage" für den

Kostenlos für IT-Administrator Abonnenten

ITANet

ITANet Workshop-Partner: VEEAM

IT-Administrator Trainings-Partner: Global Knowledge

Workshop in Frankfurt/M. und Leipzig

Update Virtualisierung 2011
am 8. Juni und 7. Juli 2011

Die Agenda:

13.00 Uhr: Begrüßung

13.15 Uhr: Server-Virtualisierung aktuell

- Herausforderung Management:
  Blinde Flecken des Monitorings und neue Werkzeuge für die Verwaltung virtualisierter Server
- Abschied vom virtuellen Switch:
  Neue Wege der Anbindung virtueller Maschinen an das Netzwerk
- Gemeinsame Verwaltung physikalischer und virtueller Server:
  Stolperfallen, Methoden, Tools

Dozent: Nico Lüdemann

14.45 Uhr: Pause

15.00 Uhr: Partnervortrag:
Veeam Backup – mehr als nur Backup

Dozent: Dirk Hannemann (Frankfurt)
Matthias Frühauf (Leipzig)

15.45 Uhr: Pause

16.00 Uhr: Desktop-Virtualisierung aktuell

- Virtuelle Applikationen versus gehosteter Desktop
- Lokale Virtualisierung für mobile Anwender
- Vor- und Nachteile, Kosten
- Wie passt das alles ins Client-Management?

Dozent: Nico Lüdemann

17.30 Uhr: Ende der Veranstaltung

Termin: 8. Juni 2011
Ort: Global Knowledge Germany Training GmbH,
Hungener Straße 6, 60389 Frankfurt
Uhrzeit: 13.00 bis ca. 17.30 Uhr

Teilnahmegebühren:
Für IT-Administrator Abonnenten kostenlos*.

Anmeldeschluss: 1. Juni 2011

Termin: 7. Juli 2011
Ort: Commundo Tagungshotel Leipzig,
Zschochersche Straße 69, 04229 Leipzig
Uhrzeit: 13.00 bis ca. 17.30 Uhr

Teilnahmegebühren:
Für IT-Administrator Abonnenten kostenlos*.

Anmeldeschluss: 1. Juli 2011

*Haben Sie ein Abonnement des IT-Administrator und möchten einen Kollegen mitbringen, erheben wir für den zweiten Teilnehmer eine Schutzgebühr von 75,- (zzgl. 19% MwSt.). Verfügt Ihr Unternehmen über kein Abonnement, wird eine Schutzgebühr von Euro 145,- (zzgl. 19% MwSt.) fällig.

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

DFS-Root ausgewählt. Sinnvollerweise haben wir uns in diesem Fall für einen domänenbasierten Namespace entschieden, so dass der DFS-Stamm "Ablage" über "\\domain.xyz\Ablage" aufgerufen wird. Aus Redundanzgründen haben wir uns für einen zweiten Namespace-Server entschieden, dieser kann nun über die DFS-Konsole im Kontextmenü des Namespaces hinzugefügt werden. Damit der zweite Domain Controller DFS-Namespace-Server sein kann, muss die Rolle "DFS-Namespaces" auf dem Zielsystem installiert sein.

DFS-Rolle und Dateiserver konfigurieren

Um die Funktionalitäten des DFS nun auch auf unseren bereitgestellten Fileservern (S-MG-FS01 und S-MG-FS02) nutzen zu können, ist die Installation der Rollen "Dateiserver" und "Verteiltes Dateisystem mit DFS-Replikation" notwendig.

Ebenso bietet es sich an in diesem Atemzug auch direkt die Management-Konsole "Ressourcen-Manager für Dateiserver" für den Fileserver hinzuzufügen. Auch können Sie an dieser Stelle jeweils eine erste Freigabe auf unsere Dateiserver erstellen:

- fg-mg-fs01-dokumente
- fg-mg-fs02-dokumente

Ordner anlegen

Nach der initialen Bereitstellung der DFS-Namespaces können Sie die ersten Ordner anlegen. Wie bereits erläutert, ist ein DFS-Ordner nichts anderes als eine spätere Dateifreigabe Ihres Fileservers. Um den Ordner "Dokumente" anzulegen, wählen Sie im Kontextmenü die Option "Ordner hinzufügen…" aus. Im gleichen Konfigurationsschritt können Sie nun für Ihren DFS-Ordner unser Ordnerziel (DFS-Target) konfigurieren. In unserem Fall soll das Ziel die im vorherigen Konfigurationsschritt angelegten Freigaben sein:

- Server: S-MG-FS01, Freigabe: fg-mg-fs01-dokumente
- Server: S-MG-FS02, Freigabe: fg-mg-fs02-dokumente

Konfiguration der Replikation

Eine durchaus sinnvolle Option ist die redundante Datenhaltung mittels DFS-R. Innerhalb der DFS-Verwaltungskonsole können Sie Replikationsknoten und Replikationsgruppen entsprechend anlegen und verwalten. In diesem Fall erstellen Sie mittels Kontextmenü des DFS-Ordners eine neue Replikationsgruppe. In unserem Szenario wollen wir damit die Replikation zwischen unseren beiden Dateiservern (S-MG-FS01 und S-MG-FS02) erreichen.

Zu allererst muss nun eine Replikationsgruppe erstellt und ein entsprechender Name vergeben werden. Hier können Sie die richtigen, durch den Assistenten vorgegebenen Einstellungen übernehmen. Die verfügbaren Server für unsere Replikationsgruppe werden nun ermittelt. Angezeigt werden die Server, die in der Konfiguration des DFS-Ordners eingetragen wurden. Im nächsten Schritt muss ein Dateiserver als primäres Mitglied definiert werden. In der Regel basiert eine Dateiserverumgebung nämlich auf bereits vorhandenen Daten. Wird nun ein zweiter Server hinzugefügt, der noch keine Datenbestände aufweist, sollen innerhalb der Replikation natürlich die vorhandenen Daten auf den neuen Server repliziert werden – unter keinen Umständen anderherum. Daher wählen Sie in diesem Konfigurationspunkt den Server aus, der bereits Daten in seiner Freigabe bereitstellt. Diese Einstellung hat im späteren Verlauf jedoch keine Auswirkungen auf die durchgeführte, bidirektionale Replikation.

Im nächsten Konfigurationsschritt muss die präferierte Topologie, die für die Replikation genutzt werden soll, ausgewählt werden. Hierzu stehen drei mögliche Optionen zur Verfügung:

- Hub and Spoke
- Full Mesh
- Keine Topologie

Für unser Beispiel kommt nur eine Option in Frage: Wir wählen die Option "Full Mesh". Dies bedeutet, dass alle an der Replikation beteiligten Server mit jedem Partner replizieren. Des Weiteren können wir nun weitere Aspekte der Replikation konfigurieren: Dazu zählen:

- Bandbreite: Mit diesem Parameter legen Sie fest, mit welcher verfügbaren Bandbreite repliziert werden soll.
- Zeitfenster: Hier können Sie einen Replikationszeitplan erstellen. Beispielsweise soll eine Replikation nur zwischen 22:00 bis 0:00 Uhr durchführt werden, um die Bandbreite für Benutzer während der Arbeitszeiten nicht zu blockieren.

Bild 2: Die DFS-Namespaces müssen als neue Rolle hinzugefügt werden

Sobald alle Einstellungen getätigt sind, erscheint das neue Replikationsobjekt innerhalb der Replikationsknoten. Hier lässt sich schnell nachvollziehen, welche Server und Replikationen vorhanden und aktuell sind. Ebenso können Sie von diesem Punkt aus mehrere Diagnose- und Wartungsfunktionen anwählen. Im Anschluss sollte die bidirektionale Replikation noch mit ein paar Test-Daten geprüft werden.

Zugriff auf ein DFS-Target

Wie bereits im Verlauf des Artikels kurz erläutert, erfolgt der Zugriff auf eine DFS-Ressource direkt und nicht über Umwege – etwa das DFS-N. Wir haben uns in diesem Szenario für einen domänenbasierten DFS-Stamm entschieden. Die innerhalb des Active Directory angelegten Attribute lassen sich zur Überprüfung der Konfiguration mittels der Microsoft Management Console "Active Directory Benutzer und -Computer" einsehen. Hierzu aktivieren Sie unter dem Reiter "Ansicht" die "erweiterten Features". Nun wechseln Sie in den Container "System" und navigieren dort bis zum Punkt "DFS-Configuration". Mit der rechten Maustaste klicken Sie auf das Objekt und wählen "Eigenschaften" und dort den Punkt "remoteServerName" aus. Hier werden nun alle konfigurierten Namespace-Server kommasepariert aufgeführt. Ebenso lässt sich die Konfiguration mittels der mitgelieferten DFS-Diagnosetools (DFSDiag) überprüfen. Der Test der Namespace-Konfiguration erfolgt mit

```
DFSDiag /TestDFSConfig
  /DFSRoot:\\domain.xyz\Ablage
```

Den Test der Domain Controller führen Sie mit dem Befehl

```
DFSDiag /TestDCs /Domain:domain.xyz
```

durch. Prüfung der Integrität von Metadaten erfolgt über

```
DFSDiag /TestDFSIntegrity
  /DFSRoot:\\domain.xyz\Ablage
  /Recurse /Full
```

Fazit

Unser Workshop hat gezeigt, dass eine funktionierende und redundante DFS-Struktur von einigen wichtigen und grundlegenden Punkten wie beispielsweise der Netzwerkumgebung und der Active Directory-Infrastruktur abhängt. Einige dieser Punkte müssen jeweils immer für die eigene Infrastruktur betrachtet und bewertet werden. Fundierte Konzepte bilden die Basis für eine langfristige, funktionierende DFS-Struktur. Die Installation und Konfiguration hingegen sollte Administratoren nicht vor allzu große Schwierigkeiten stellen. *(dr)*

Thomas Gronenwald ist IT-Security Consultant bei der adMERITia GmbH sowie Autor und Betreiber von blog.port389.de.

Fehlersuche im Ethernet mit TAPs, SPAN- und Mirror-Ports (2)

Der Kammerjäger im LAN

von Mathias Hein

Shared Media-LANs – getragen von Hubs – sind anfällig für Datenkollisionen. Diese können den Datenverkehr im gesamten Netz beeinträchtigen, sind allerdings auch recht einfach mit einem Analysator aufzuspüren. Im geswitchten Netz hingegen sind in der Regel nur einzelne Netzsegmente von Fehlern betroffen – doch die Fehlersuche ist kompliziert. Und sie stellt den Administrator vor noch höhere Hürden, findet sie in VLANs statt. Der zweite Teil unserer Workshopserie bietet Anleitungen zu Messungen in derartigen Netzen mit Mirror- und SPAN-Ports sowie TAPs.

Ein klassisches Shared Media-LAN basiert auf einem gemeinsamen Kabelmedium. Dieses stellt den gemeinsamen Kommunikationskanal im Netzwerk dar, über den die daran angeschlossenen Clients mit den Servern kommunizieren. Ein VoIP-Analysator agiert in einem solchen Netzkonstrukt nur als stiller Beobachter, da von diesem Gerät alle auf dem Netz übermittelten Pakete empfangen werden. Aus der Paketanalyse lassen sich alle Sender, Empfänger, Protokolltypen und viele weitere Details ausfiltern. Damit lassen sich die Verkehrslasten, Protokolldetails sowie die klassischen Fehler des LANs darstellen und schnell die Problemzonen aufdecken beziehungsweise die auftretenden Fehler diagnostizieren. Wichtig im Shared LAN: Es kann immer nur ein Paket auf dem Medium zu einer Zeit transportiert werden.

Messen und Analysieren in Shared Media-Netzen

Ein Hub stellt ein Netzwerk auf engstem Raum dar und unterscheidet sich von der Funktion her nicht von einem klassischen Shared Media-LAN. Jedes Endgerät erhält über einen eigenen physikalischen Port den Zugang zum Netzwerk. Dieses Netzwerk simuliert der Hub. Bei Kurzschlüssen oder bei Kabelunterbrechungen isoliert der betreffende Repeater-Port den angeschlossenen Rechner vom Rest des Netzes und verhindert, dass das gesamte Netz von dem Kabelfehler in Mitleidenschaft gezogen wird.

Datenpakete und auch Fehler breiten sich in einem Shared Medium annähernd mit Lichtgeschwindigkeit aus. Von Vorteil für die Analyse ist, dass die Platzierung des Analysators im Grunde gleichgültig ist. Nachteilig für das gesamte Netzwerk ist jedoch, dass auftretende Fehler auch das gesamte Netzwerk betreffen und im schlechtesten Fall auch den gesamten Datenverkehr aller Stationen in Mitleidenschaft ziehen können. Wird der Analysator zur Überwachung an einen beliebigen Port des Hubs angeschlossen, lassen sich alle Datenströme aufzeichnen und analysieren. Der Hub arbeitet somit als Repeater (Verstärker), der physikalische Segmente terminiert, jedoch keinerlei Einfluss auf den Inhalt der Datenpakete nimmt.

Hat eine Station im Shared Media-LAN festgestellt, dass das Übertragungsmedium frei ist, übermittelt sie die Daten über das LAN-Segment an den Empfänger. Ist im gleichen Moment eine andere Station derselben Meinung und sendet diese zeitgleich ein Paket auf das Netz, so prallen die beiden Pakete zusammen und es entsteht eine Kollision. Findet eine solche Kollision statt, sorgen die sendenden Netzadapter für die Wiederholung der Nachrichten. Erst ab der kritischen Lastgrenze von 50 bis 70 Prozent der maximalen Übertragungsbandbreite (10 oder 100 MBit/s) kommt es beim Ethernet zu echten Durchsatzproblemen beziehungsweise zum Verlust der Daten. Mit Hilfe eines Netzanalysators lassen sich die im Netz auftretenden Lasten und Fehler leicht ermitteln.

Messen und Analysieren in Netzen auf Basis von Switches

Der Einsatz von Switch-Systemen gehört heute zu den Standards in Netzwerken. Damit haben die Hub-Technik und somit auch das Shared Media-LAN mehr oder weniger ausgedient. Mit der Installation von Switches wird die Aggregat-Bandbreite (Gesamtbandbreite aller Ports) sofort um das X-fache erhöht. Die Separierung des Verkehrs führt dazu, dass ein Messgerät beziehungsweise der Analysator nicht mehr bedenkenlos an jeden Port angeschlossen werden kann. Die Separierung des Datenverkehrs durch den Switch hat zur Folge, dass sich an einem Switch-Port nur noch folgender Verkehr messen lässt:

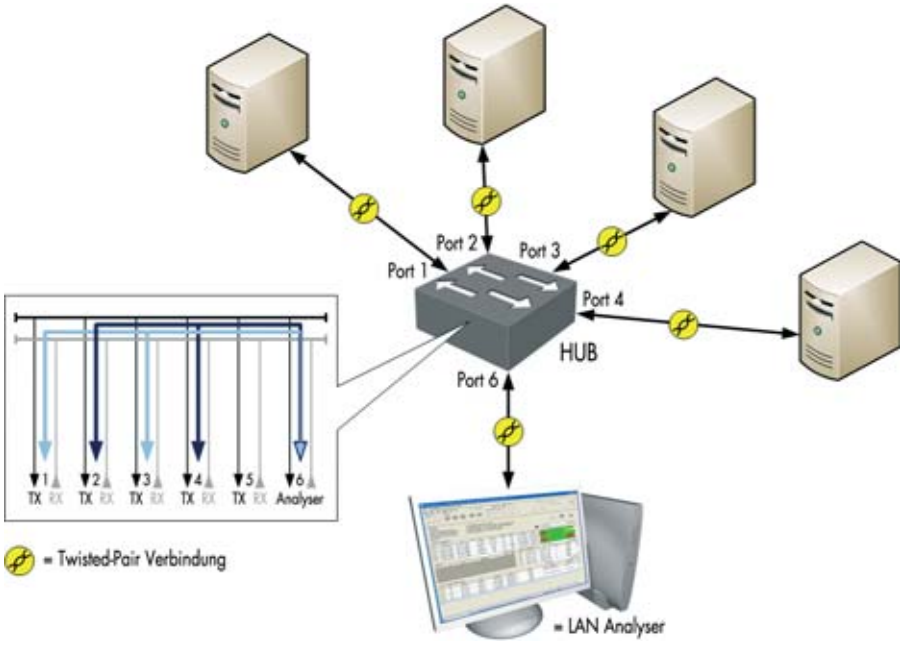


Bild 1: Funktionsweise und Messung im Shared LAN

- Unicast-Pakete, die für das am Port angeschlossene Endgerät bestimmt sind
- Unicast-Pakete mit unbekannter (nicht in der Switch-Tabelle eingetragener beziehungsweise von dieser gelernten) MAC-Adresse
- Broadcast-Pakete

Somit werden in geswitchten Netzen die für die Datenanalyse notwendigen Daten nicht an jeden Port übertragen. Wird zusätzlich noch die VLAN-Technologie im Netzwerk genutzt, ist selbst der Broadcast-Verkehr nur auf die Ports des betreffenden VLANs beschränkt. Von einer Transparenz des Netzverkehrs kann also nicht mehr die Rede sein. Daher müssen in geswitchten Umgebungen Alternativen gefunden werden, die eine Ermittlung der Datenströme ermöglichen. Die jeweiligen Lösungsmodelle haben jedoch neben vielen Vorteilen auch einige gewichtige Nachteile.

Messungen mit Zusatz-Hubs in geswitchten Umgebungen

Auf den ersten Blick bietet sich zur Lösung des Mess- und Analyseproblems in geswitchten Umgebungen der Abgriff der Daten direkt auf der physikalischen Ebene an. Bei diesem Verfahren wird ein Hub zwischen das zu messende Gerät (Server, Client PC, Etagen-Switch) und den betreffenden Switch-Port geschaltet. Damit wird mit einem simplen Trick ein Shared Media-Umfeld wiederhergestellt. Dieses Verfahren weist nur den Unterschied auf, dass das Messgerät nur bestimmte Datenströme messen kann und nur den Verkehr von und zum Server misst. Bei dieser Methode sind jedoch einige Fakten zu berücksichtigen:

- Die Polarität des Netzwerkkabels vom Hub zum Switch muss richtig konfektioniert sein (ausgekreuztes Kabel oder MDI-X Port).
- Die Anwendung beziehungsweise der Netzanschluss muss zulassen, dass die Netzwerkverbindung kurz geöffnet wird, um den Hub dazwischen zu schalten. Dieses Einschalten in die Verbindung kann oft nur zu definierten Wartungszeiten erfolgen und kann den Ablauf des Troubleshootings entscheidend behindern.

Mit dem Einbringen eines Hubs in den Kommunikationspfad wird nicht nur die physikalische Bedingung der Verbindung verändert, sondern auch das gesamte Kommunikationsverhalten. Wird ein Server oder ein Client-PC im Vollduplex-Modus an den Switch angeschlossen und anschließend ein Hub in die Verbindung eingeführt, kann per Definition der Datenverkehr nicht mehr im Vollduplex-Modus übertragen werden, da der Hub diesen nicht unterstützt. Dies kann dazu führen, dass ein fest auf den Vollduplex-Modus eingestellter Switch-Port nicht mit einem Hub-Port im Halbduplex-Modus zusammengeschaltet werden kann. Arbeitet der Switch im

Alignment- und CRC-Fehler im Detail

Symptom	Problem	Anmerkung
Alignment- oder CRC-Fehler steigen extrem stark an.	Netzkabel/Netzsegment ist zu lang.	Wird ein Netzanalysator zur Fehlerermittlung genutzt, sollte die Anzahl der von einer Station in den internen Statistiken verzeichneten Late Collisions mit den aufgezeichneten Alignment- und/oder CRC-Fehlern korrelieren.
Alignment- oder CRC-Fehler steigen proportional zur Einstreuung von elektromagnetischen Störungen.	Netzkabel/Netzsegment ist gestört.	Tritt typischerweise in einem 10BaseT-Segment auf. In diesem Fall sind die Alignment- und/oder CRC-Fehlerstatistiken verschiedener Stationen nicht korrelierbar. Hier müssten die Runt-Pakete signifikant höher als im Normalbetrieb sein.
Alignment- oder CRC-Fehler übersteigen das Normalmaß.	Das Netzwerk entspricht nicht mehr den Carrier Sense Multiple Access with Collision Detect (CSMA/CD)-Spezifikationen.	Tritt durch die Installation nicht standardkompatibler Ethernet-Komponenten (vorzugsweise Repeater und Hubs) auf.

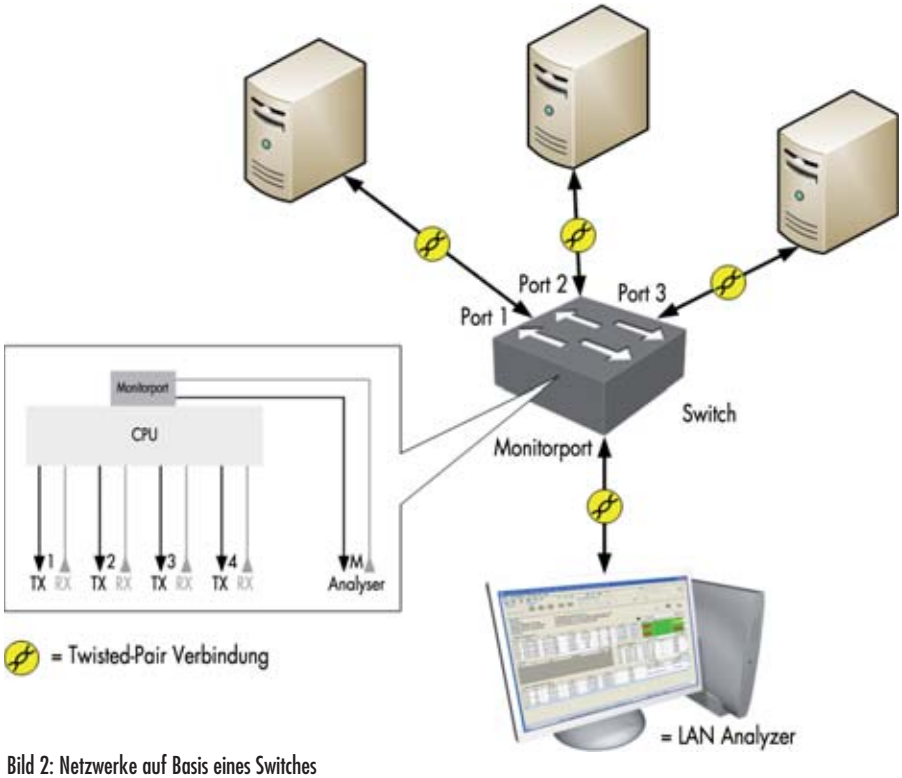


Bild 2: Netzwerke auf Basis eines Switches

Autonegotiation-Modus und kann sich dadurch automatisch an die Bedingungen des Kommunikationspartners anpassen, verändern sich jedoch einige wichtige Rahmenbedingungen der Verbindung. Hubs können versehentlich falsche Analyseinformationen liefern. Somit weist die Hub-Methode einige gewichtige Nachteile auf:

- Es kann immer nur ein Netzsegment pro Zeiteinheit gemessen werden. Wollen Sie mehrere Server gleichzeitig überwachen, sind weitere Messgeräte beziehungsweise Analysatoren erforderlich.
- Für Messungen auf Vollduplex-Verbindungen ist die Hub-Variante ungeeignet.
- Um die Messung durchführen zu können, muss die Verbindung kurzzeitig unterbrochen werden. Dies bedeutet unter Umständen für die Nutzer der Serversysteme einen kurzzeitigen Verbindungsabbruch.
- Fehler, die an den anderen Ports des Switches auftreten (CRC-Fehler, Runts et cetera), bleiben dem Analysator zumeist verborgen, da der Switch durch seine Filterintelligenz verhindert, dass defekte Pakete an andere Ports weitergeleitet werden. Dies gilt ebenso für Überlasten, Protokollfehler und so weiter.

Messen und Analysieren auf Basis von Mirror- oder SPAN-Ports

Moderne Switch-Systeme stellen für das Messen und die Analyse im Netzwerk in der Regel die Spiegelung von Switch-Ports mit Hilfe der Mirror-Port-Funktion bereit. Dadurch wird der jeweils zu untersuchende Link auf einen anderen Port des Switches, an dem der Analysator angeschlossen ist, gespiegelt. Einige Hersteller sind dabei sogar in der Lage, den Verkehr mehrerer Switch-Ports auf einem Mirror/SPAN-Port auszugeben. Der Mirror-Port wird auch als SPAN- (Switch Port Analyser) Port oder Maintenance-Port bezeichnet.

Die Weiterleitung der zu analysierenden Daten auf den Mirror/SPAN-Port sollten Sie nur nutzen, wenn dieser die Datenmengen der gespiegelten Ports auch verkraftet. Ist dies nicht der Fall, gehen Pakete verloren. Auf der sicheren Seite sind Sie, wenn der Spiegel-Port dieselbe Bandbreite aufweist wie der Quell-Port. Für längere Burst-Situationen eignet sich diese Methode allerdings nicht, da der Analysator über den Spiegel-Port nur die Hälfte der maximal möglichen Vollduplex-Bandbreite aufzeichnen kann. Darüber hinaus beeinträchtigt das Mirroring die Switch-Performance, da der Switch für die Spiegelung alle Pakete duplizieren muss. Auch der gespiegelte Port kann in seiner Performance einbrechen und die Fehlersuche produziert erst wirklich Probleme.

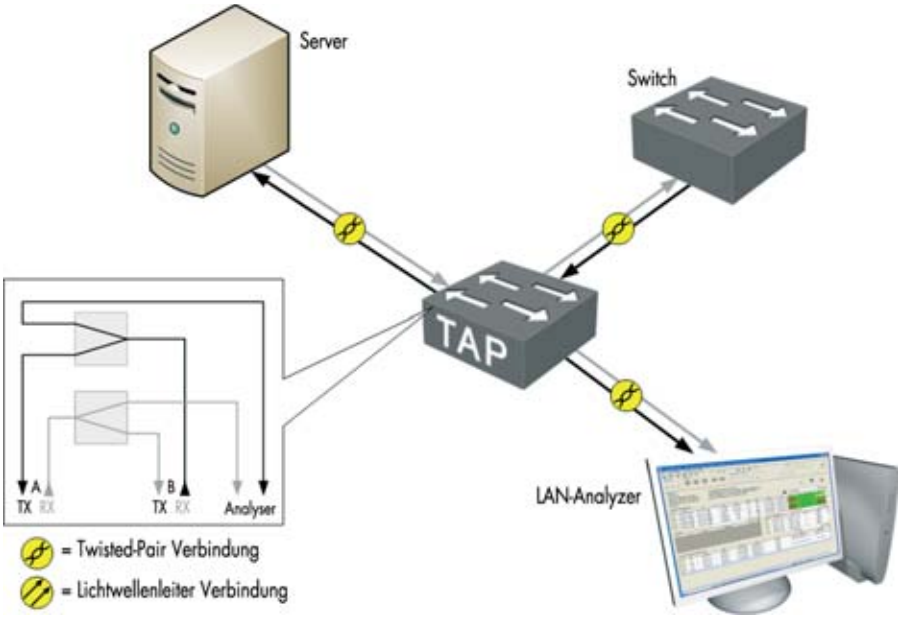


Bild 3: Analyse über den Mirror/SPAN-Port

Zum anderen verzerrt das Port Mirroring die Analyse, weil ein Switch defekte Pakete automatisch verwirft. Oft werden auch nur die Pakete eines VLANs gespiegelt. Ferner müssen Sie darauf achten, dass der Mirror-Port genügend Bandbreite hat. Spiegeln Sie also keinen 100BaseT-Port auf einen 10BaseT-Port. In einem solchen Fall spiegelt der Switch nur eine Teilmenge der Pakete und macht die Datenaufzeichnung vollkommen wertlos. Bei der Spiegelung mehrerer Ports auf einen Mirror-Port kommt es zusätzlich zu Verzögerungen, da Pakete, die gleichzeitig an den Ports ankommen, unter Umständen in einer anderen Reihenfolge am Mirror-Port ausgegeben werden.

Messen und Analysieren auf Basis von TAPs

Die in Switches integrierten Mirror- und SPAN-Ports verhindern die Durchleitung fehlerhafter Datenpakete und können Messergebnisse verfälschen. Für die genaue Erfassung der Messdaten kommen heute so genannte TAPs (Test Access Points) zum Einsatz. TAPs werden in der Literatur auch manchmal als Link-Splitter bezeichnet. Diese Geräte werden direkt in die zu überwachende Netzverbindung eingeschleift. TAPs arbeiten absolut passiv und erzeugen keine Fehler und funktionieren auch bei einem Stromausfall. Ein TAP dupliziert (hochohmige Anschaltung) alle Pakete und erzeugt aus einem Vollduplex-Link zwei Halbduplex-Datenströme mit dem Rx- und dem Tx-Verkehr. Dadurch muss der Netzanalysator mit zwei Netzwerkkarten ausgerüstet sein. Die Analysesoftware fügt die beiden Datenströme anschließend wieder zu einem Datenstrom zusammen.

TAPs unterstützen unterschiedliche Zusatzfunktionen, die die Datenaufzeichnung vereinfachen. Hier sind folgende Geräteklassen erhältlich:

- Konverter TAP: Eine LWL-Verbindung kann nicht mit einem Kupfer-Analysator gemessen werden. Die unterschiedlichen Netztechnologien erfordern eine Umwandlung der Signale. Die Lösung bietet ein Konverter TAP, der die jeweiligen Signale in ein 10/100/1000 Ethernet-Signal umsetzt. Darüber hinaus spart ein solcher Konverter die Beschaffung einer zusätzlichen LWL-Messkarte für den Analysator ein.
- Aggregator TAP: Ein normaler TAP verfügt über zwei Ausgänge (Rx und Tx). Ein normaler PC stellt jedoch nur eine LAN-Schnittstelle bereit. Ein so genannter Aggregator TAP erlaubt das Mitschneiden von Vollduplex-Links mit einer einzigen Netzwerkkarte und das Zusammenführen der beiden Datenströme im Mess/Analyse-Gerät entfällt.
- Filtered TAP: Die Netzanalyse auf hoch ausgelasteten Leitungen führt immer wieder zu Schwierigkeiten. Bei hoher Auslastung ist das Risiko groß, dass der PC nicht alle Pakete aufzeichnen wird. Ein Filtered TAP sorgt durch zusätzliche Filterfunktionen (HW-Filter im TAP), dass die gewünschten Signale am Ausgang zur Verfügung stehen. *(jp)*

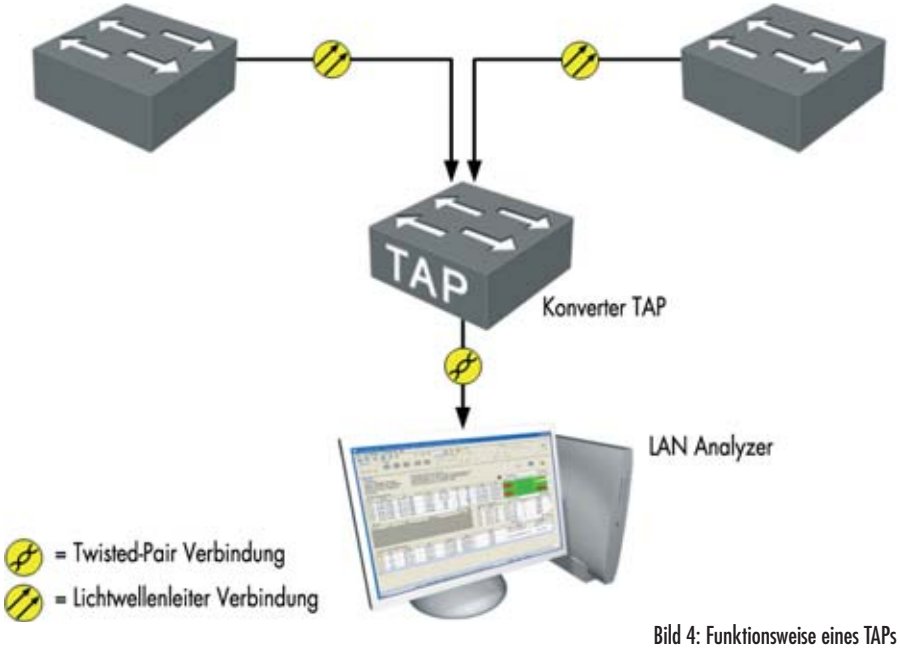


Bild 4: Funktionsweise eines TAPs

Datensicherung unter Hyper-V

Virtuelle Maschinen auf Wanderschaft

von Thomas Joos

Wer über Hyper-V und Windows Server 2008 (R2) virtuelle Server zur Verfügung stellt, muss sein Datensicherungskonzept an die virtuelle Umgebung anpassen. Die Sicherung des Hosts und der darauf laufenden virtuellen Server verlangt andere Herangehensweisen als die Sicherung herkömmlicher physikalischer Server. Wir zeigen Ihnen in diesem Workshop, wie Sie mit Hausmitteln Backups von Hyper-V anfertigen und was beim Einsatz von Microsofts Data Protection Manager wichtig ist. Außerdem erklären wir, wie Sie mit der PowerShell virtuelle Maschinen automatisiert exportieren können.

Natürlich lassen sich auch virtuelle Server mit herkömmlichen Sicherungsstrategien sichern. Dazu installieren Sie einfach auf den virtuellen Servern den oder die Agenten der entsprechenden Sicherungslösung. Das Datensicherungsprogramm behandelt diese Server dann genauso wie normale physische Server. Allerdings belastet diese Art der Sicherung den Host und bei einer Datensicherung kann es schnell zu einer Überlastung der Hardware kommen. Außerdem sichert diese Art der Datensicherung nicht die Konfiguration der virtuellen Maschine und verwendet auch nicht die optimierten Methoden, die Hyper-V zur Verfügung stellt. Die Agenten greifen ferner nicht auf den Hypervisor zurück und können daher weder Schattenkopien noch Schnappschüsse zur Sicherung nutzen.

Extrawurst für Hyper-V

Backup-Lösungen, die Hyper-V unterstützen, bauen auf dem Hyper-V-Host auf und sichern den Server auf Ebene des Hypervisors. Die Software nutzt also Schnittstellen von Hyper-V zur Sicherung. Auf diese Weise kann das Werkzeug Snapshots der virtuellen Server zur Sicherung verwenden und sich des Schattenkopiedienstes bedienen. Dies ist wesentlich effizienter, schneller und stabiler als herkömmliche Sicherungen. Die Anwendung erstellt automatisch Snapshots im laufenden Betrieb und die virtuellen Server stehen weiterhin den Nutzern zur Verfügung. Solche Online-Sicherungen belasten die Hardware des Hosts nicht und ermöglichen zudem Backups während der Arbeitszeit.

Müssen Sie mehrere virtuelle Server auf einem Host sichern, kann eine kompatible Lösung redundante Dateien erkennen und muss diese nicht doppelt sichern. Laufen auf einem Hyper-V-Host zum Beispiel zehn Server mit Windows Server 2008 R2, erkennt die Software identische Systemdateien und kopiert diese nur einmal. Diese Herangehensweise ist natürlich nicht möglich, wenn Sie mit einem Agenten innerhalb der virtuellen Maschine arbeiten, denn in diesem Fall weiß die Sicherungssoftware nichts von anderen Servern. Die zu sichernde Datenmenge vergrößert sich damit enorm und verlängert den kompletten Backup-Vorgang.

Sicherung mit Bordmitteln

Beim Backup von Hyper-V spielt der Schattenkopiedienst eine wichtige Rolle, da die Sicherung auf Schnappschüsse des physikalischen Hosts und der virtuellen Server aufbaut. Mit aktiviertem Schattenkopiedienst lassen sich Hyper-V-Server inklusive der laufenden virtuellen Server sichern. In einem Knowledge Base-Artikel [1] lesen Sie, wie Sie ein Hyper-V-Backup richtig konfigurieren und die Registry des Hosts anpassen. Weitere Beiträge, die sich ausführlich mit dem

Thema beschäftigen, finden Sie unter [2] im TechNet-Blog sowie unter [3] auf den Seiten des Microsoft Enterprise Support-Teams. Mit diesen Anleitungen können Sie einen Hyper-V-Host direkt mit der Windows Server-Sicherung sichern.

Ein Video [4] des Virtualisierungs-Teams von Microsoft zeigt Ihnen ebenfalls interessante Tipps zur Sicherung von Hyper-V. Setzen Sie zum Beispiel keine Hyper-V-kompatible Datensicherung ein, haben Sie die Möglichkeit, den Host mit der Windows Server-Sicherung in eine Datei zu schreiben und diese dann mit Ihrer Datensicherungs-Software zu bearbeiten. Auf diese Weise nutzen Sie die Vorteile von Hyper-V, ohne sich zusätzliche Anwendungen kaufen zu müssen. Nützlich ist in diesem Zusammenhang auch das kostenlose "MAP Toolkit for Hyper-V" [5]. Damit können Sie die Last von Hyper-V-Hosts messen. Das Werkzeug zeichnet die Leistung von Servern über einen festgelegten Zeitraum auf, zum Beispiel während der Datensicherung.

Snapshots von virtuellen Servern erstellen

Ganz ohne Zusatzanwendungen ermöglicht Hyper-V zumindest das Erstellen von Snapshots von virtuellen Maschinen. Die Snapshots bieten zum Beispiel die Möglichkeit, einen Server vor einer Konfigurationsänderung zu sichern. Sie können für jeden virtuellen Computer in Hyper-V maximal 50 Snapshots erstellen. Den entsprechenden Befehl finden Sie im Kontextmenü des virtuellen Rechners. Während der Erstellung des Snapshots bleibt der Server online und steht den Nutzern weiterhin zur Verfügung. Die erstellten Snapshots zeigt der Hyper-V-Manager im mittleren Bereich der Konsole an. Hyper-V speichert die Snapshots in dem Verzeichnis, das Sie in den Einstellungen des virtuellen Computers im Bereich "Speicherort für Snapshotdateien" angeben. Standardmäßig handelt es sich um das Verzeichnis "C:\ ProgramData \ Microsoft \ Windows \ Hyper-V \ Snapshots". Rufen Sie den Befehl "Zurücksetzen" im Kontextmenü des virtuellen Computers auf, wendet Hyper-V den letzten erstellten Snapshot an und setzt den Computer auf diesen Stand zurück. Snapshots ersetzen allerdings keine Datensicherung, sondern bieten nur eine Rückversicherung vor einer Konfigurationsänderung auf dem Server.

Arbeiten mit dem Data Protection Manager 2010

Mit dem Data Protection Manager (DPM) 2010 bietet Microsoft eine eigene Lösung zur Datensicherung von Hyper-V-Hosts an. DPM 2010 kann auch andere Anwendungen sichern, bietet aber im Bereich Hyper-V vor allem in Verbindung mit Windows Server 2008 R2 eine optimale Unterstützung. Das Werkzeug fertigt im laufenden Betrieb Snapshots an, sichert die Daten dieser Online-Snapshots auf ein Festplattensystem und legt diese Daten dann wiederum auf Band ab. Die zu sichernden Server stehen dabei weiterhin online den Nutzern zur Verfügung. Ebenso ist die direkte Sicherung auf Bandlaufwerke möglich, ohne den Umweg über Festplatten oder auch parallel dazu.

Komfortables Backup über Gruppenregeln

Damit die Software eine Sicherung durchführen kann, installieren Sie auf dem Hyper-V-Host einen Agenten, der mit dem DPM-Server eine Verbindung aufbaut. Die Clients lassen sich dann über die Verwaltungskonsole von DPM im Netzwerk verteilen. Neben den herkömmlichen Daten kann das Tool den Systemstatus der Server sichern, also eine Komplettsicherung durchführen. Gemeinsame Systemdaten mehrerer Server fasst DPM automatisch zusammen und sichert nur beim ersten Server das komplette Betriebssystem. Dies hat vor allem bei der Sicherung von Hyper-V-Hosts den Vorteil, dass sich Server wiederherstellen lassen, aber doppelte Datenmengen vermieden werden. DPM 2010 ist außerdem dazu in der Lage, die neuen Cluster Shared Volumes (CSV) zu sichern, die Hyper-V R2 für die Live Migration von virtuellen Computern zwischen Clusterknoten benötigt. Bei der Live Migration von Windows Server 2008 R2 verlieren Anwender nicht die Verbindung zu den virtuellen Computern. Die virtuellen Rechner laufen dabei als Cluster-Ressourcen. Ebenfalls möglich ist die Wiederherstellung einzelner Daten innerhalb von virtuellen Festplatten (VHD).

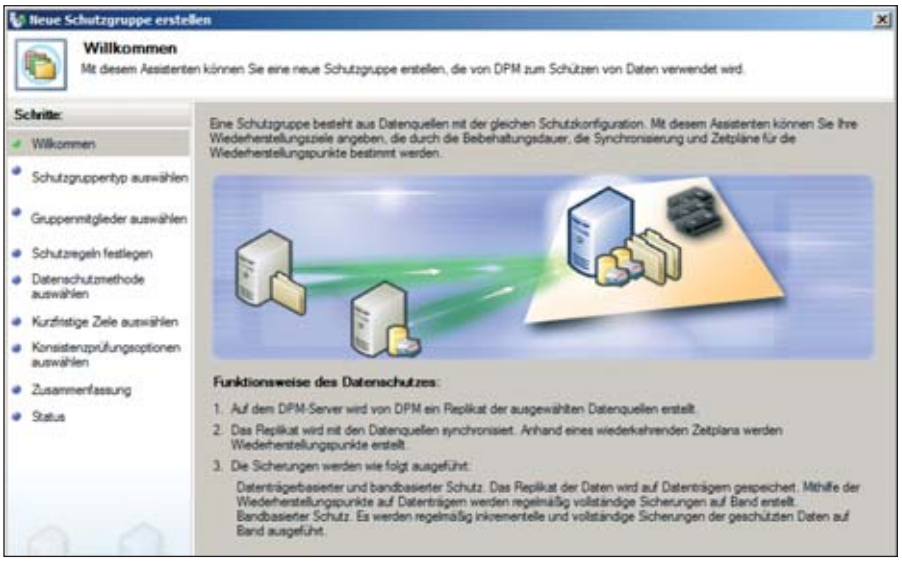
Virtuelle Computer lassen sich nicht nur auf der ursprünglichen Host-Maschine wiederherstellen, sondern auf jedem anderen Hyper-V-Host in der Infrastruktur. DPM arbeitet bei der Sicherung mit speziellen Regeln, mit denen sich Server zu einzelnen Gruppen zusammenfassen lassen. Diese Gruppen tragen die Bezeichnung Schutzgruppen und haben einen gemeinsamen Regelsatz, zum Beispiel alle Hyper-V-Hosts im Unternehmen. In diesen Regeln legen Sie beispielsweise fest, wie oft Sie den Server sichern wollen oder wie lange die Daten rückwirkend auf dem Server verfügbar sein sollen. Nicht erwünschte Dateien lassen sich außerdem von der Sicherung ausschließen.

DPM 2010 integriert sich in die anderen Produkte der System Center-Reihe und ist auch Bestandteil der Server Management Suite. So kann zum Beispiel System Center Operations Manager einen Disaster-Recovery-Vorgang starten, wenn ein Management Pack einen Ausfall bemerkt. Um DPM 2010 zu lizenzieren, benötigen Unternehmen eine Serverlizenz für System Center Data Protection Manager 2010. Für jeden gesicherten Server ist eine Enterprise-Lizenz notwendig. Die Lösung macht allerdings nur in reinen Microsoft-Netzwerken Sinn, da Produkte anderer Hersteller nicht effizient unterstützt werden.

Wiederherstellung von Hyper-V-Servern

Haben Sie virtuelle Server nicht mit einer Hyper-V-kompatiblen Lösung gesichert, müssen Sie bei einer Wiederherstellung des Hosts alle virtuellen Server manuell wiederherstellen und die Datensicherung der einzelnen Server zurückspielen. Beim

Backup über eine kompatible Anwendung vereinfachen und beschleunigen Sie diesen Vorgang, da die Anwendungen sowohl Host als auch virtuelle Server wiederherstellen können. Mit DPM 2010 lassen sich einzelne Dateien, Verzeichnisse oder der komplette Systemstatus des Servers wiederherstellen. Müssen Sie über DPM einen kompletten Server wiederherstellen, bietet die Lösung ein spezielles Tool an, über das Sie eine bootfähige CD/DVD erstellen. Auch das Booten über Netzwerk ist mit DPM möglich. Ferner bietet die Plattform eine skriptbasierte Verwaltung auf Basis der PowerShell an. Auf diese Weise können Sie virtuelle Server zur Sicherung exportieren und mit Skripten die Verwaltung von DPM automatisieren.



Die Sicherung erfolgt durch eine Definition von Schutzgruppen

Sicherung durch PowerShell-Export

Das Backup von Hyper-V-Hosts hat vor allem den Zweck, die einzelnen, auf dem Host laufenden virtuellen Server zu sichern. In der Verwaltungskonsole von Hyper-V haben Sie die Möglichkeit, die virtuellen Server zu exportieren. Exportierte Server können Sie jederzeit wieder importieren. Dies funktioniert auf dem gleichen Hyper-V-Host, aber auch auf einem anderen Rechner. Der Befehl zum Exportieren steht über das Kontextmenü von virtuellen Maschinen zur Verfügung. Diese Möglichkeit steht aber nur bereit, wenn der virtuelle Server nicht gestartet ist. Das heißt, Sie können mit dem Export keine Online-Sicherung durchführen, sondern den Server nur sichern, wenn er ausgeschaltet beziehungsweise angehalten ist. Aus diesem Grund bietet es sich an, diesen Export nachts durchzuführen, wenn keine Nutzer mit dem Server arbeiten.

Der Export-Vorgang umfasst die VHD-Dateien, Snapshots und die Einstellungen des virtuellen Servers. Die Größe der Exportdateien entspricht der Größe der Quell-Dateien. Sie müssen also beim Exportieren von mehreren Servern entsprechend Speicherplatz bereitstellen. Sie haben ferner die Möglichkeit, die virtuellen Server über das Exportieren per PowerShell-Skript zu sichern. Auch hier gilt aber wieder, dass Sie den Server herunterfahren oder anhalten müssen. Auf der Webseite [6] finden Sie ein PowerShell-Skript und eine ausführliche Anleitung, wie sich solche Export-Vorgänge vollständig über Skripte automatisieren lassen. Zwar ist eine solche Sicherung nicht als Ersatz für echte Sicherungen geeignet, als Zusatzebene kann ein Export aber ein Mehr an Sicherheit bieten.

Mit dem Skript fahren Sie virtuelle Server automatisch herunter, exportieren den Server in eine Datei und starten den Server neu. Es ist zudem möglich, dass Sie die Sicherungsdateien auf eine Netzfreigabe kopieren, nachdem Sie den virtuellen Server wieder gestartet haben. Sie benötigen für das Skript zusätzlich die PSHyperv Library [7] von James O'Neill. Die Library enthält zusätzliche Cmdlets, die die Verwaltung von Hyper-V in der PowerShell deutlich erleichtern. Das Skript zur Datensicherung von Hyper-V-Servern baut auf diesen Cmdlets auf. Ein weiteres benötigtes Werkzeug ist "Streams" [8] von Sysinternals. Der erste Schritt besteht nun darin, dass Sie mit *streams.exe* Datenströme von der PSHyperv Library-Installationsdatei entfernen müssen. Dazu entpacken Sie das Streams-Archiv und kopieren die Datei *streams.exe* und die Datei *HyperV_Install.zip* in ein Verzeichnis auf der Festplatte des Hyper-V-Hosts. Öffnen Sie dann eine Befehlszeile und geben Sie den Befehl

```
streams -d HyperV_Install.zip
```

ein. Extrahieren Sie dann die ZIP-Datei und installieren Sie die Library durch Rechtsklick auf *install.cmd* und die Auswahl von "Als Administrator ausführen". Installieren Sie das Skript nicht auf einem Windows Server 2008 R2-Core-Server, sondern auf einer vollständigen Installation von Windows Server 2008 R2, erhalten Sie zwei Fehlermeldungen, die Sie aber ignorieren können. Nach der Installation startet die PowerShell. Tippen Sie das Kommando

```
get-command -module HyperV
```

ein, um die Installation zu überprüfen. Das Fenster zeigt Ihnen anschließend die verfügbaren PowerShell-Cmdlets an, auf denen das PowerShell-Sicherungsskript aufbaut. Diese Befehle können Sie unabhängig vom entsprechenden Skript nutzen.

Im nächsten Schritt laden Sie jetzt noch die aktuelle Version des Sicherungs-Skriptes *HyperV-Backup.ps1* von der bereits erwähnten Seite [6] herunter. Entpacken Sie das Download-Archiv in ein Ver-

zeichnis auf dem Hyper-V-Host. Wenden Sie aber auch hier vorher den Befehl

```
streams -d hyperV-Backup-V0.91.zip
```

an. Nach der Installation können Sie alle Server auf einem Host schnell und einfach herunterfahren, sichern und anschließend wieder hochfahren. Das Skript hinterlegen Sie als Aufgabe auf dem Hyper-V-Host oder starten es manuell. Das Backup läuft vollkommen unabhängig von der Windows Server-Sicherung und erstellt vollständige Export-Dateien, die sich auch auf anderen Hyper-V-Hosts schnell und einfach wieder integrieren lassen. Allerdings kann das Skript wie erwähnt keine Online-Sicherungen durchführen, sondern Server nur im ausgeschalteten oder gespeicherten Zustand sichern. Um sich eine Hilfe anzuzeigen, geben Sie den Befehl *HyperV-Backup.ps1 -?* ein. Sie sehen in der PowerShell dann die verschiedenen Optionen und Beispiele zur Verwendung.

Wollen Sie zum Beispiel auf dem Hyper-V-Host die virtuelle Maschine "sql" exportieren, verwenden Sie den Befehl

```
{Pfad}\HyperV-Backup.ps1 -VM sql
  -ExportPath {Pfad}.
```

Direkt nach der Eingabe beginnt der Export-Vorgang. Ist die Maschine gestartet, fährt das Skript den virtuellen Server herunter, exportiert die virtuelle Maschine und startet die VM wieder. Wollen Sie die Sicherung zusätzlich noch im Netzwerk speichern, verwenden Sie den Befehl

```
{Pfad}\HyperV-Backup.ps1 -VM {Name
  des Servers} -ExportPath {Lokaler
  Export-Pfad} -RemotePath \\{UNC
  der Freigabe} -verbose.
```

Starten Sie das Skript automatisiert, können Sie die Option "-verbose" weglassen. Bei diesem Befehl geht das Skript genauso vor wie bei einer lokalen Sicherung und kopiert nach dem Start der exportierten VM die Sicherungsdatei in die Freigabe auf dem Netzwerk. Während des langwierigen Kopiervorgangs über das Netzwerk läuft der virtuelle Server also bereits wieder.

Automatisierung der Sicherung über den Aufgabenplaner

Neben der manuellen Export-Möglichkeit können Sie diese Sicherung automatisieren. Dazu erstellen Sie auf dem Server einfach eine neue Aufgabe im Aufgabenplaner von Windows Server 2008 R2. Diesen starten Sie am schnellsten, wenn Sie "Aufgabe" im Suchfeld des Startmenüs eingeben. Als Aktion für die Aufgabe verwenden Sie "Programm starten". Bei "Programm/Skript" müssen Sie direkt den Pfad zur PowerShell eingeben. Diesen finden Sie standardmäßig unter *C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe*. Anschließend geben Sie im Feld "Argumente hinzufügen" den Befehl in der Syntax ein, mit der Sie den Server auch manuell sichern würden.

Nach der Erstellung der Aufgabe öffnen Sie noch deren Einstellungen, da Sie noch Änderungen vornehmen müssen. Aktivieren Sie auf der Registerkarte "Allgemein" die Option "Unabhängig von der Benutzeranmeldung ausführen". Zusätzlich setzen Sie den Haken bei "Mit höchsten Privilegien ausführen". Auf der Registerkarte "Einstellungen" können Sie noch bei "Aufgabe beenden, falls sie länger ausgeführt wird als…" einen Zeitraum auswählen, nach dem der Server den Task beenden soll. Das ist wichtig, damit nach einer erfolglosen Sicherung die Anwender morgens wieder mit dem Server arbeiten können. *(ln)*

Link-Codes

[1] Sicherungen von virtuellen Maschinen unter Hyper-V
B4P41

[2] Backing up Hyper-V with Windows Server Backup
B4P42

[3] How to enable Windows Server Backup support for the Hyper-V VSS Writer
B4P43

[4] Video: Backup Hyper-V with Windows Server Backup
B4P44

[5] MAP-Toolkit for Hyper-V
B4P45

[6] Skript zur Hyper-V Sicherung mittels Powershell
B4P47

[7] PowerShell management Library for Hyper-V
B4P48

[8] Streams 1.56 von Sysinternals
B4P49

Quelle: Ryan Jorgensen – 123RF

Bare Metal Recovery von Windows Server 2008 (R2)

Out of the Dark

von Ulf B. Simon-Weidner

Fällt ein Server komplett aus, war es bisher sehr aufwendig, ihn wiederherzustellen. Seit Windows Server 2008 bietet das Betriebssystem die Wiederherstellungsmethode "Bare Metal-Recovery" mit Bordmitteln an. Damit lassen sich Sicherungen auch auf einem unbespielten System rasch wieder in Betrieb nehmen. In diesem Workshop gehen wir darauf ein, was Sie in diesem Fall schon bei der Sicherung beachten sollten, wie Sie das Backup auf verschiedenen Wegen wiedereinspielen und wie Sie sich dabei das Virtualisierungs-Format VHD zu Nutze machen.

Die direkte Wiederherstellung einer Datensicherung auf einem Server ohne Betriebssystem war vor Windows Server 2008 nur mit Drittlösungen möglich. Mit Bordmitteln hingegen blieb nur die Neuinstallation des Betriebssystems, um danach mit Hilfe der Datensicherung den Server wieder in den Ausgangszustand zurückzuversetzen – alles in allem eine sehr aufwändige Arbeit. Seit Windows Server 2008 können Sie den Server direkt wiederherstellen, ohne vorher ein Betriebssystem installieren zu müssen.

Vor dem Restore kommt die Sicherung

An erster Stelle steht immer eine erfolgreiche Datensicherung. Mit Windows Server 2008 hat Microsoft das im Serverbetriebssystem eingebaute Sicherungstool "NTBackup" gegen die "Windows Server-Sicherung" ausgetauscht. Während das Sicherungstool bei den Vorversionen standardmäßig installiert war, müssen Sie es jetzt als Feature nachinstallieren. Dies können Sie entweder in der grafischen Benutzeroberfläche des Servermanager erledigen oder Sie bedienen sich der Kommandozeile oder der PowerShell.

Installation der Windows Server-Sicherung

Die Windows Server-Sicherung lässt bei der Installation über die GUI die Auswahl der Unterkategorie "Befehlszeilentools" für das Sicherungsfeature zu. Diese Formulierung ist etwas missverständlich – nur die PowerShell-Erweiterungen der Datensicherung erfordern diese Option. Das Tool *wbadmin.exe*, das die Möglichkeiten in der klassischen Kommandozeile zur Verfügung stellt, ist in jedem Fall Bestandteil des Hauptpaketes der Datensicherung. Wenn Sie die Datensicherung lieber mittels Kommandozeile installieren möchten, verwenden Sie folgendes Kommando:

```
ServerManagerCmd.exe -install Backup
```

Mit dem Schlüsselwort "Backup" installieren Sie das Sicherungsfeature ohne Befehlszeilentools, mit dem Schlüsselwort "Backup-Tools" richten Sie alle Komponenten ein:

```
ServerManagerCmd.exe -install
  Backup-Tools
```

Auch über die PowerShell können Sie Betriebssystemkomponenten wie die Datensicherung nachinstallieren. Hierfür müssen Sie zunächst das Modul "ServerManager" laden, damit Sie im Anschluss über das Cmdlet "add-WindowsFeature" die Funktion hinzufügen können:

```
import-module ServerManager
add-WindowsFeature Backup
```

Nicht nur die Installation, sondern auch die Architektur der Datensicherung hat sich mit Windows Server 2008 geändert. Während davor eine Datensicherung in ein spezielles Dateiformat geschrieben wurde, erstellen die neuen Sicherungsmethoden ein blockbasiertes Abbild der betroffenen Partitionen (oder Volumes) als VHD-Datei. Hierbei entsprechen die VHD-Dateien dem Dateiformat für virtuelle Festplatten von Virtual PC oder Hyper-V. Zudem hat sich die Verwendbarkeit der virtuellen Festplatten erweitert, wie wir später noch sehen werden. Unterstützend kommt bei der Datensicherung der Volumenschattenkopiedienst zum Einsatz, der zu Beginn der Datensicherung einen Snapshot erzeugt, der dann gesichert wird. So ist sichergestellt, dass alle gesicherten Daten dem selben Zeitpunkt entsprechen. Durch die blockbasierte Sicherung als VHD-Datei, die ein vollständiges Abbild der Partitionen enthält,

müssen Sie die Datensicherung entweder auf ein Netzlaufwerk schreiben oder auf ein lokales Laufwerk, das nicht Bestandteil der Sicherung ist.

Optionen bei der Systemsicherung

Über die grafische Benutzeroberfläche starten Sie die Windows Server-Sicherung entweder im Servermanager unter "Dienste" oder über das Startmenü unter "Verwaltung". Dabei haben Sie die Möglichkeiten einer "Vollständigen Sicherung" – diese enthält die Daten aller lokalen Partitionen. Beachten Sie, dass Sie das Backup nur dann auf einer lokalen Partition ablegen können, wenn von dieser Partition selbst keine Bestandteile in der Sicherung enthalten sind. Für eine "Benutzerdefinierte Sicherung" sind folgende Optionen möglich:

- Bare-Metal-Recovery: Sichert alle Informationen, die notwendig sind, um das System komplett von einer Sicherung wiederherzustellen (inklusive Systemstatus, Boot- und Betriebssystempartition).
- Systemstatus: Sichert die Daten, die notwendig sind, um den Systemstatus wiederherzustellen. Bei dieser Option muss ein Betriebssystem existieren, bevor es zu einer Wiederherstellung des Systemstatus kommt.
- Einzelne Partitionen / Volumes: Hier können Sie einzelne Partitionen / Volumes wählen, die in der Sicherung enthalten sein sollen.

Wie stark die Größenunterschiede der verschiedenen Sicherungsvarianten ausfallen, ist von System zu System unterschiedlich. Zum Beispiel umfassen Sicherungen bei Domänencontrollern häufig nur zehn bis 15 Prozent mehr Daten bei einer Bare-Metal-Restore-Sicherung als bei einem Backup des Systemstatus. In diesem Fall sind Sie mit einer Bare-Metal-Sicherung deutlich flexibler. Im weiteren Verlauf gehen wir deshalb immer von dieser Art der Sicherung aus. Um ein System vollständig wiederherzustellen, ist es wichtig, all die Volumes mit zu sichern, die Daten von auf dem System installierten Applikationen enthalten.

Natürlich lässt sich die Windows Server-Sicherung auch direkt über die Befehlszeile starten. Hierzu dient das Kommando *wbadmin.exe*. Ein "Critical Volume Backup", das in der Benutzeroberfläche als "Bare-Metal-Recovery" erscheint, erstellen Sie mit dem folgenden Kommando

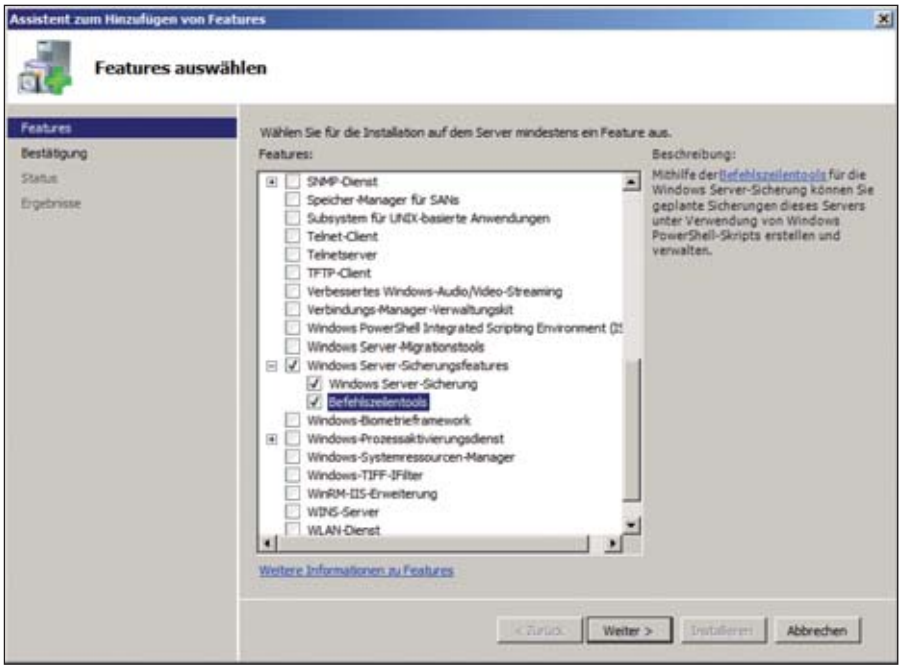


Bild 1: Installation der Datensicherungsoption im Servermanager. Die Option "Befehlszeilentools" wird nur für die PowerShell benötigt.

```
wbadmin.exe START BACKUP -backupTar-
  get:e: -allCritical -include:c:,d:
  -noVerify -vssFull -quiet
```

Die Option "-backupTarget" definiert, wohin Sie die Sicherung schreiben wollen. Der Schalter "-allCritical" legt fest, dass wir ein Bare-Metal-Recovery erstellen wollen. "-Include" ist nicht notwendig, wenn Sie nur das Betriebssystem oder einen Domänencontroller sichern. Bei Applikationsservern können Sie hierüber zusätzliche Laufwerke angeben, die die Sicherung umfassen soll. Hierbei ist wieder daran zu denken, dass ein lokales Laufwerk nur dann als Backup-Ziel dienen kann, wenn es selbst keine zu sichernden Daten enthält. Die weiteren Parameter "-noVerify"," -vssFull" und "-quiet" bedeuten, dass keine Überprüfung der Sicherung erfolgt, eine Schattenkopie verwendet wird (was empfohlen ist) und keine Nachfragen erfolgen.

Über die PowerShell erzeugen Sie eine Bare-Metal-Recovery-Sicherung mit den folgenden Kommandos:

```
Add-PSSnapIn Windows.ServerBackup
$BackupPolicy = New-WBPolicy
Add-WBBareMetalRecovery -policy
  $BackupPolicy
$BackupTarget = New-BackupTarget
  -VolumePath E:
Add-WBBackupTarget -Policy $Backup-
  Policy -Target $BackupTarget
Start-WBBackup -policy $BackupPolicy
```

Die Sicherung lässt sich am besten über gespeicherte Aufgaben einrichten. Wenn das Backup-Target im Netzwerk liegt, müssen Sie den UNC-Pfad (\\server \share...) angeben anstatt eines Laufwerk-Mappings, da Letzteres nur dann verfügbar ist, wenn Sie am System angemeldet sind. Nachdem Sie die Datensicherung eingerichtet haben, sollten Sie regelmäßig überprüfen, ob sie ordnungsgemäß durchgeführt wurde, und die diesbezüglichen Ereignisse in das Monitoring aufnehmen.

Auswahl des richtigen Backup-Sets

Durch die Speicherung der Datensicherung in eine VHD-Datei hat es Microsoft einfacher gemacht, in die Sicherung hineinzusehen. So können Sie entweder direkt einzelne Dateien zurückholen oder entscheiden, welche Systemsicherung den gewünschten Stand hat und wiederhergestellt werden soll. Hierfür müssen Sie die VHD-Datei wie in Bild 2 in das Dateisystem einbinden. Die VHD-Dateien (eine pro Partition / Volume) finden Sie auf dem Backupziel im Verzeichnis "WindowsImageBackup \ {Computername} \ {Backup-Zeit-Datum}".

Leider enthalten die VHD-Abbilder als Dateinamen lediglich GUIDs, die entsprechende Partition können Sie lediglich aufgrund der Größe oder durch Ausprobieren erahnen. Für den direkten Zugriff von einem anderen System müssen Sie gegebenenfalls noch Berechtigungen anpassen. Danach lassen sich die VHD-Dateien mounten und mit Laufwerksbuchstaben versehen. Um in eine Sicherung einzusehen, empfiehlt es sich, die Option "Schreibgeschützt" zu setzen. Nachdem die Festplatte eingebunden ist, müssen Sie noch einen Laufwerksbuchstaben setzen. Alternativ erledigen Sie diese Schritte mit dem Kommando *diskpart.exe*:

```
diskpart.exe
select vdisk file=d:\...\guid.vhd
attach vdisk readonly
```

Hiermit ist die virtuelle Festplatte verbunden, mit den Kommandos *select volume / partition* und *assign letter* müssen Sie dann je nach Struktur der Platte noch einen Laufwerksbuchstaben für das Volume auswählen. Im Anschluss erhalten Sie über den Windows Explorer oder andere Tools Einsicht in den Inhalt der Datensicherung.

Wiederherstellung in wenigen Schritten

Genauso wie bei der Sicherung können Sie auch beim Restore unterschiedliche Wegen gehen. Hierbei ist zu beachten, dass Sie immer nur die Vorgehensweise wählen können, für die in der Datensicherung genügend Informationen vorhanden sind. So ist es nicht möglich, mit einer Systemstatussicherung ein Bare-Metal-Recovery durchzuführen, während dies umgekehrt durchaus möglich wäre. Während sich beim Backup nur der Systemstatus, Bare-Metal-Recovery oder komplette Volumes sichern lassen, können Sie bei der Rücksicherung einzelne Dateien oder Ordner wiederherstellen – in diesem Fall ist das Rückkopieren von einer gemounteten VHD-Datei allerdings fast einfacher.

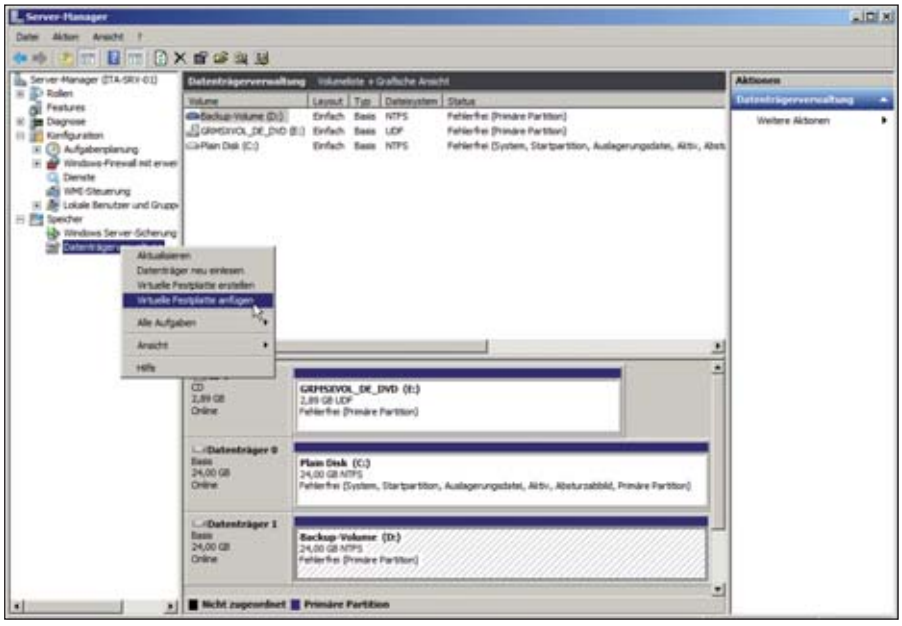


Bild 2: Die in der Sicherung erstellten VHD-Dateien lassen sich mit separaten Laufwerksbuchstaben direkt im System mounten

Die Rücksicherung für Dateien und Ordner, Systemstatus oder registrierte Applikationen starten Sie über die Verwaltungskonsole "Windows Server-Sicherung". Möchten Sie die Rücksicherung über *wbadmin.exe* durchführen, müssen Sie zunächst die Versionsnummer der wiederherzustellenden Sicherung herausfinden. Führen Sie hierzu den folgenden Befehl aus:

```
wbadmin.exe get versions
  -backupTarget:e:
```

In der Ausgabe des Kommandos notieren Sie die Versions-ID. Danach starten Sie mit diesem Kommando beispielsweise eine Systemstatus-Rücksicherung:

```
wbadmin.exe start systemstatereco-
  very -version {version-id}
  -backupTarget:e:
  -machine:ITA-SRV-01
```

Hierbei sind die Parameter "-BackupTarget" und "-Machine" optional und nur dann nötig, wenn es sich nicht um die Sicherung des lokalen Systems handelt oder diese auf einem anderen Laufwerk erstellt wurde.

Ein Bare-Metal-Recovery lässt sich allerdings nicht über die normale Verwaltungskonsole durchführen. Das wäre in den meisten Fällen wenig zielführend, denn die komplette Rücksicherung eines Servers ist ja zumeist nur dann notwendig, wenn der Server kaputt ist, die Festplatten Defekte vorweisen und/oder sich das System nicht mehr starten lässt. Diese Art der Rücksicherung können Sie daher nur über die Produkt-DVD, einen entsprechend vorbereiteten USB-Stick oder über einen Netzwerkboot anstoßen.

Rücksicherung mittels DVD

Völlig neu bei Windows Server 2008 (R2) ist die Möglichkeit, eine komplette Rücksicherung ohne installiertes Betriebssystem durchzuführen. Die einfachste Methode hierzu ist, von einer Produkt-DVD zu booten. Nach der Auswahl

Bestellen Sie jetzt

das IT-Administrator

Sonderheft II/2011!

180 Seiten Praxis-Know-how rund um das Thema

SharePoint 2010 für Administratoren

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

** IT-Administrator Abonnenten erhalten das Sonderheft II/2011 für € 24,90. Nichtabonnenten zahlen € 29,90. IT-Administrator All-Inclusive Abonnenten "zahlen" für Sonderhefte nur € 19,90 - diese sind im Abonnement dann automatisch enthalten. Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.*

Liefertermin:
Ende Oktober 2011

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

---

administrator
Das Magazin für professionelle System- und Netzwerkadministration

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

☐ **Ja**, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft II/2011 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft II/2011 zum Preis von **€ 29,90** inkl. Versand und 7% MwSt.

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____ BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

ITA 0411

So erreichen Sie unseren Vertrieb, Abo- und Leserservice:

Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville
Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de

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

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

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

der Eingabesprache wählen Sie dazu im Fenster "Windows installieren" die "Computerreparaturoptionen". Danach entscheiden Sie sich für Systemabbild-Wiederherstellung, wählen ein Systemabbild aus und starten die Rücksicherung. Sollte die Festplatte nicht erkannt werden, laden Sie zunächst den Treiber für den SCSI- oder SATA-Controller und starten dann die Rücksicherung.

Installation vom USB-Stick

Um einen USB-Riegel vorzubereiten, um von diesem ein Bare-Metal-Recovery oder sogar eine Installation durchzuführen, sind diverse Vorbereitungen nötig. Hierzu ist zunächst ein Rechner mit Vista, 7 oder Server 2008 (R2) notwendig. An diesem Rechner schließen Sie den leeren USB-Stick an und starten dann *diskpart.exe*. Danach führen Sie nacheinander die folgenden Kommandos aus:

```
List Disk
Select Disk {Nummer des USB-Sticks}
Clean
Create Partition Primary
Active
Format FS=FAT32 Quick
Assign Letter S:
```

Danach kopieren Sie alle Inhalte der Windows Boot-DVD auf den USB-Stick. Achten Sie darauf, die komplette Verzeichnisstruktur mitsamt versteckten Dateien und Systemdateien mit zu kopieren. Nun lässt sich der USB-Key, wie weiter oben beschrieben, dazu einsetzen, um Windows zu installieren oder eine Bare-Metal-Rücksicherung durchzuführen.

Alternative Netzwerkboot

Den Netzwerkboot in aller Vollständigkeit zu behandeln, würde am Thema dieses Workshops vorbeiführen und dessen Rahmen sprengen – daher an dieser Stelle nur eine kurze Beschreibung: Die Windows Deployment Services (WDS) sind eine Komponente, die sich ebenfalls im Lieferumfang des Betriebssystems befinden. Nachdem diese standardmäßig konfiguriert wurden, können Sie *Boot.WIM* für die Installationsumgebung und *Install.WIM* für die eigentliche Installation über das Netzwerk mittels Netzwerkboot verteilen. Auch so ist ein Bare-Metal-Recovery möglich, je nach System müssen Sie dazu eine bestimmte Tastenkombination drücken, damit das BIOS aus dem Netzwerk bootet.

Es gibt allerdings Umstände, bei denen die vollständige Wiederherstellung nicht so problemlos möglich ist, vor allem wenn das Restore auf einem System mit unterschiedlicher Hardware erfolgen soll. In früheren Windows-Versionen war es sehr schwierig, ein vollständiges Recovery auf einer unterschiedlichen Hardware durchzuführen. Dankenswerterweise befinden sich mittlerweile sehr viele Treiber mit im Lieferumfang des Betriebssystems. Trotzdem kann es sein, dass Sie weitere Schritte durchführen müssen, um das System wieder funktionsfähig zu machen.

Sollte das Zielsystem spezielle SCSI/SATA-Treiber benötigen, können Sie diese mittlerweile vor dem Recovery mittels USB-Stick oder sonstige Methoden einbinden. Des Weiteren bietet die Computerreparatur Möglichkeiten, den Boot-Sektor oder Boot-Dateien zu reparieren. Am besten eignet sich hierfür die Option "Startup Repair", die das Bootmenü nach einem fehlgeschlagenen Start automatisch anbietet. Eine weitere Variante, die wir zumindest erwähnen wollen, ist, ein gesichertes System (gegebenenfalls mit etwas Konfigurationsaufwand) als virtuelle Maschine zu starten, da die VHD-Dateien ja das passende Format dazu haben. Auch hier müssten Sie eventuell weitere Treiber einspielen, um die Lauffähigkeit auf dem virtuellen Host zu gewährleisten.

In diesem Zusammenhang sei erwähnt, dass Windows 7 und Server 2008 R2 das Booten von VHDs direkt auf der Hardware unterstützen. Hierzu müssen Sie dann beispielsweise eine Kopie des aktuellen Bootеintrages anfertigen und in der Kopie benennen, dass eine virtuelle Festplatte anstelle einer physikalischen zu booten ist. Dies bewerkstelligen Sie folgendermaßen:

```
Bcdedit /copy {current} /d "VHD
  Boot"
```

Notieren Sie in der Ausgabe des Kommandos die neue GUID und fahren Sie mit diesen Befehlen fort:

```
Bcdedit /set {GUID} device
  vhd=[D:]\backup.vhd
Bcdedit /set {GUID} osdevice
  vhd=[D:]\backup.vhd
Bcdedit /set {GUID} detecthal on
```

Mit Hilfe dieser Kommandos lässt sich eine VHD dann direkt booten. Auch hier kann es nötig sein, verschiedenste Reparaturmaßnahmen durchzuführen. Außerdem gilt zu beachten, dass die virtuellen Festplatten nicht auf einem komprimierten Laufwerk oder Verzeichnis liegen dürfen, dass Standby oder Ruhezustand nicht funktionieren und dass die Pagefile nicht in der virtuellen Festplatte liegen darf. Nichtsdestotrotz ist es eine sehr interessante, häufig jedoch experimentelle Variante. Für diejenigen, die noch etwas mehr experimentieren wollen: Erstellen Sie eine leere VHD-Datei, binden Sie diese in das Dateisystem ein und lassen Sie die Installation dann genau in diese Datei laufen. Hierzu müssen Sie bei der benutzerdefinierten Installation lediglich die richtige Partition verwenden und die Meldung, dass die Installation in dieser Partition unter Umständen nicht funktioniert, einfach ignorieren.

Fazit

Die Sicherungsmöglichkeiten von Windows Server 2008 und R2 ermöglichen erstmals die direkte Wiederherstellung einer Sicherung auf der reinen Hardware, ohne vorher ein Betriebssystem installieren zu müssen. Zahlreiche Varianten erlauben das Einsehen der Daten in den Sicherungsdateien, das Booten von VHDs und sogar die direkte Installation in solche virtuellen Festplatten. Durch die Image-basierte Sicherung ist das Backup deutlich schneller geworden und bedient sich der Schattenkopiedienste, um Datenintegrität herzustellen. *(ln)*

Inventarisierung von Arbeitsplatzrechnern mit ACMP Inventory

Die Gratis-Inventur

Quelle: Maksym Yemelyanov - Fotolia.com

von Thomas Bär

Wer als Administrator qualifizierte Entscheidungen über seine Clientinfrastruktur treffen möchte, muss zunächst wissen, welche Hard- und Software eigentlich vor Ort bei den Benutzern steht. Und so banal das klingt: Ab rund 20 Arbeitsplatzrechnern wird die Beantwortung dieser Frage ohne passendes Werkzeug schon schwierig. Dabei müssen Sie nicht einmal Geld investieren, um herauszufinden, welche Arbeitsplätze beispielsweise fit für die Migration auf Windows 7 sind. Denn mit der kostenlosen Inventarisierungssoftware "ACMP Inventory" von Aagon Consulting lässt sich bequem vom Schreibtisch aus der unternehmensweite Rechnerbestand aufnehmen. Dieser Workshop zeigt Ihnen wie.

Vor der Installation müssen Sie zunächst das "ACMP 3.8 FULL"-Archiv von der Website des Herstellers [1] herunterladen. Der Download ist rund 900 MByte groß, doch in Zeiten schneller DSL-Verbindungen innerhalb weniger Minuten erledigt. Extrahieren Sie dann die ZIP-Datei in ein temporäres Verzeichnis und starten Sie auf dem zukünftigen ACMP-Server das Setup mit einem Doppelklick auf *cdstart.exe*. Weitere Informationen zur Software – vom Handbuch bis hin zu verschiedenen Whitepapers – sind als PDF-Dokumente sowohl auf Deutsch als auch auf Englisch ebenfalls in dem Paket enthalten.

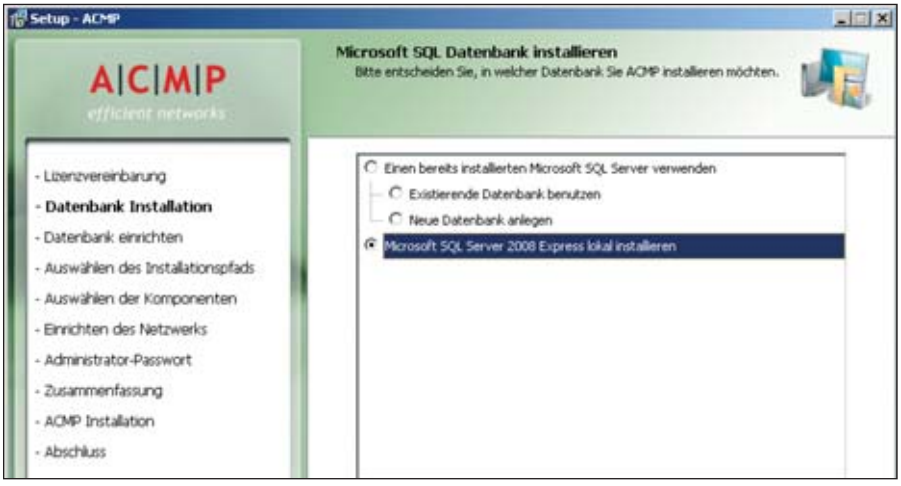


Bild 1: Auf Wunsch installiert das ACMP-Setup die benötigte Datenbank gleich mit

Die Installation von ACMP Inventory beginnt mit dem Klick auf "ACMP Set-up" im Begrüßungsmenü. Wählen Sie im folgenden Dialog zunächst die gewünschte Sprache für den Installationsvorgang aus und akzeptieren Sie die Lizenzbedingungen. Darauf folgt die Auswahl der gewünschten Datenbankumgebung. Für diesen Workshop wählen Sie hier den untersten Eintrag "Microsoft SQL Server 2008 Express lokal installieren" aus. Den passenden Datenbank-Client installiert der Setup-Assistent auf Wunsch automatisch dazu. Klicken Sie hierzu noch "Microsoft Native Client automatisch installieren" an. Je nach Geschwindigkeit Ihres Servers dauert die Datenbank-Installation jetzt ein paar Minuten. Möglicherweise ist zudem ein Neustart des Rechners erforderlich, sofern Microsoft-Komponenten nachinstalliert werden mussten.

Läuft die Datenbank für ACMP auf dem Server, wählen Sie als Nächstes den gewünschten Speicherpfad für die ACMP-Installation. Dann folgt die Auswahl der zu installierenden Funktionen, bei ACMP "Solutions" genannt. In der Standardeinstellung "Vollständige Installation" richtet der Installer das ACMP Base System einschließlich ACMP Inventory, ACMP Pro, Client Commands, Helpdesk Solution, Reports, Securitydetective und dem SWdetective ein. Durch einen Klick auf "Weiter" stimmen Sie dieser Komplettinstallation zu. Um nur den kostenlosen Inventarisierer zu installieren, wählen Sie die anderen Komponenten vorher ab. Allerdings stellt Ihnen Aagon neben dem unbegrenzt nutzbaren ACMP Inventory 15 Test-Lizenzen für jede Erweiterung zur Verfügung. Daher kann es nicht schaden, diese Komponenten gleich mit zu installieren.

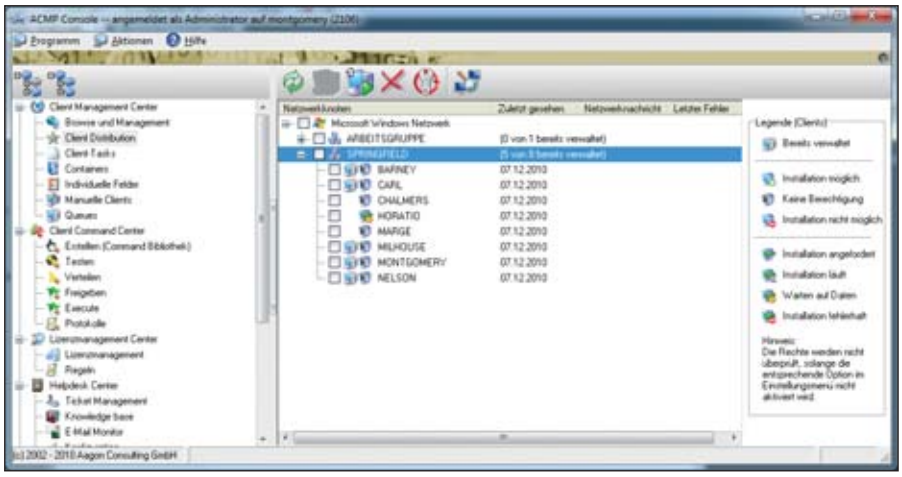


Bild 2: Die Verteilung der Clientsoftware geschieht per Login-Skript oder per Push-Kommando

Im Anschluss daran folgt die Festlegung der TCP-Ports für die Kommunikation zwischen dem ACMP-Server und den ACMP-Agenten auf den Arbeitsplatzrechnern. In der Standardeinstellung verwendet der ACMP-Server den TCP-Port 2106 und die Client-Maschinen Port 2107. Sofern es in Ihrer Umgebung Applikationen gibt, die diese Ports bereits nutzen, können Sie die von ACMP verwendeten Ports hier entsprechend anpassen. Sie sollten dabei nur sicherstellen, dass keine Firewalls die beiden Kommunikations-Ports blockieren. Denn seit dem Service Pack 2 von Windows XP ist die Firewall des Betriebssystems standardmäßig aktiviert. Eine Anleitung zur Konfiguration der Windows-Firewall in einer Active Directory-Umgebung mithilfe einer Gruppenrichtlinie finden Sie als PDF-Dokument auf der Website von Aagon unter [2]. Mit der Eingabe des ACMP-Administratorkennworts haben Sie die Installation erfolgreich abgeschlossen.

Möchten Sie ACMP zukünftig nicht direkt am ACMP-Server, sondern von Ihrem Arbeitsplatzrechner aus administrieren, können Sie dort eine weitere Kopie der ACMP-Konsole installieren. Öffnen Sie hierzu von Ihrem Arbeitsplatz aus eine Laufwerks- oder UNC-Verbindung auf die Freigabe "ACMP" des ACMP-Servers und starten Sie aus dem Ordner "Console" die *Setup.exe* mit einem Doppelklick zur Installation.

ACMP-Client verteilen

ACMP Inventory bietet grundsätzlich zwei verschiedene Wege an, um Informationen von Client-Computern auszulesen und an die zentrale Datenbank zu übermitteln: per einmaliger Ferninstallation des ACMP-Agenten auf allen Arbeitsplatzrechnern oder durch Verwendung des so genannten "OneScanClient". Der OneScanClient sammelt dabei alle Daten eines Client-Computers, sendet diese an den ACMP-Server und beendet sich dann wieder. Der OneScanClient läuft also ohne eine feste Installation auf dem jeweiligen PC ab. Übergeben Sie zudem die Option "/silent" an die Datei *OSCLnch.exe* auf der ACMP-Freigabe, so läuft der Scan beispielsweise automatisch per Login-Skript nach dem Bootvorgang des Clients ab, ohne dass der Benutzer davon etwas mitbekommt. Das kleine Programm startet jedoch auch problemlos per Doppelklick. Das können Sie einfach ausprobieren, indem Sie aus der "ACMP"-Freigabe im Ordner "OneScanClient" das Programm *OSCLnch.exe* auf Ihrer Workstation starten.

Typischerweise wird die Client-Software von ACMP jedoch fest auf allen Arbeitsplatzrechnern und gegebenenfalls auch Servern installiert. Denn so stehen Ihnen jederzeit auf Knopfdruck die Daten aller eingeschalteten Rechner topaktuell zur Verfügung. Die Verteilung des ACMP-Agenten über den Punkt "Client Distribution" ist insgesamt sehr einfach und erledigt sich weitgehend von allein. Melden Sie sich dazu in der ACMP-Konsole an und klicken Sie dort in der linken Baumstruktur des Menüs unter "Client Management Center" auf den Eintrag "Client Distribution". In der Fenstermitte der Konsole öffnet sich jetzt die aktuelle Netzwerksicht auf das Microsoft-Windows-Netzwerk und zeigt alle derzeit aktiven Computer der Domäne sowie Rechner von Arbeitsgruppen an.

Wählen Sie jetzt einfach einen kompletten Domänen- oder Arbeitsgruppennamen aus, um auf allen dort organisierten

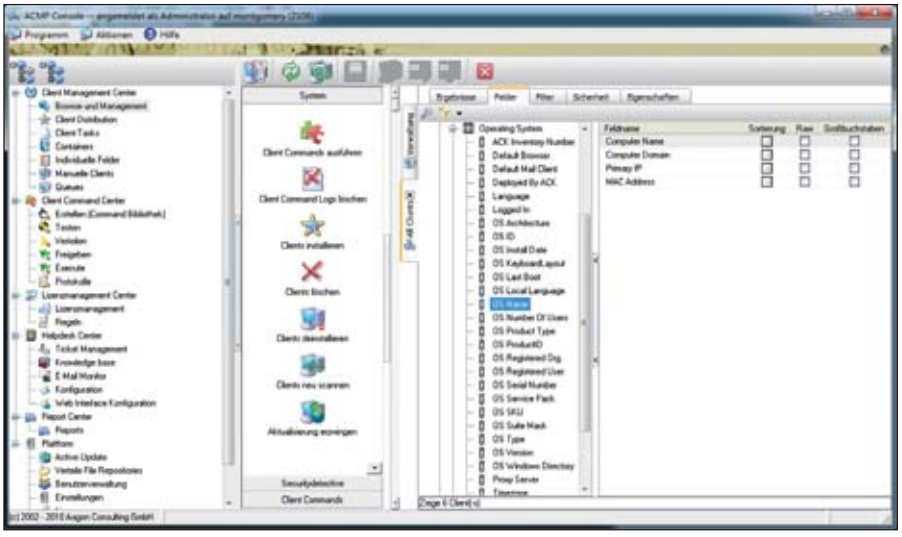


Bild 3: Viele Auswertungen bringt ACMP von Haus aus mit. Ergänzungen und Anpassungen sind mit wenigen Mausklicks erledigt.

PCs den ACMP-Client zu installieren. Möchten Sie zunächst nur mit einer Auswahl von Computern beginnen, öffnen Sie stattdessen den passenden Netzwerkknoten und wählen Sie dort die gewünschten PCs mit Hilfe der Optionsfelder aus. Oberhalb der Auflistung der Netzwerkknoten finden Sie eine Schaltfläche mit einem grünen Pfeil zur Verteilung der Client-Software auf die Zielrechner. Nach einem Klick auf das Icon erscheint ein Dialogfeld zur Eingabe der Anmeldeinformationen für die Client-Installation. Da Sie noch kein Standardinstallationskonto in den Optionen definiert haben, geben Sie hier die Anmeldeinformationen eines administrativ berechtigten Benutzers ein. Das Eingabeformat entspricht den aktuellen Windows-Gepflogenheiten in der Form "Domänenname\Benutzername".

Nach dem Absenden der Login-Daten verändert sich nach ein paar Sekunden das Symbol vor den in der Liste ausgewählten Client-PCs. Mit Hilfe der Legende auf der rechten Fensterseite können Sie ablesen, in welchem Status sich die jeweilige Installation befindet. Die Installation des Agenten auf den Client-Computern läuft vollkommen automatisch ab. Der Anwender am Arbeitsplatz sieht lediglich ein neues Symbol in der Taskleiste von Windows, wird bei seiner Arbeit jedoch nicht gestört. Einige Minuten später hat der Installer dann alle Clients eingerichtet und auch gleich inventarisiert. Kommt es bei der Ferninstallation auf einem Client zu Schwierigkeiten, so liegt dies in den allermeisten Fällen an einem von zwei Dingen: einer aktiven Firewall ohne Portfreigabe oder fehlenden Administrationsrechten auf dem Zielrechner.

Abfragen beliebig anpassen

ACMP Inventory liest eine sehr große Anzahl von Werten aus seinen Client-Rechnern aus und speichert diese in seiner zentralen Datenbank ab. Um die Ergebnisse des ersten Inventarisierungslaufs zu sehen, klicken Sie in der linken Baumstruktur der ACMP-Konsole auf "Browse und Management", öffnen dort den Knoten "Base Queries" und klicken doppelt auf "All Clients". Nun sehen Sie alle Rechner, die ACMP gefunden und inventarisiert hat. Per Doppelklick auf einen Rechnernamen erhalten Sie die kompletten Daten dieses PCs. Um wieder in die Liste aller Clients zurückzukehren, können Sie entweder die Detailansicht des gewählten Clients über das X-Symbol des hochkant geschriebenen PC-Namens schließen oder einfach den Reiter "All Clients" auswählen.

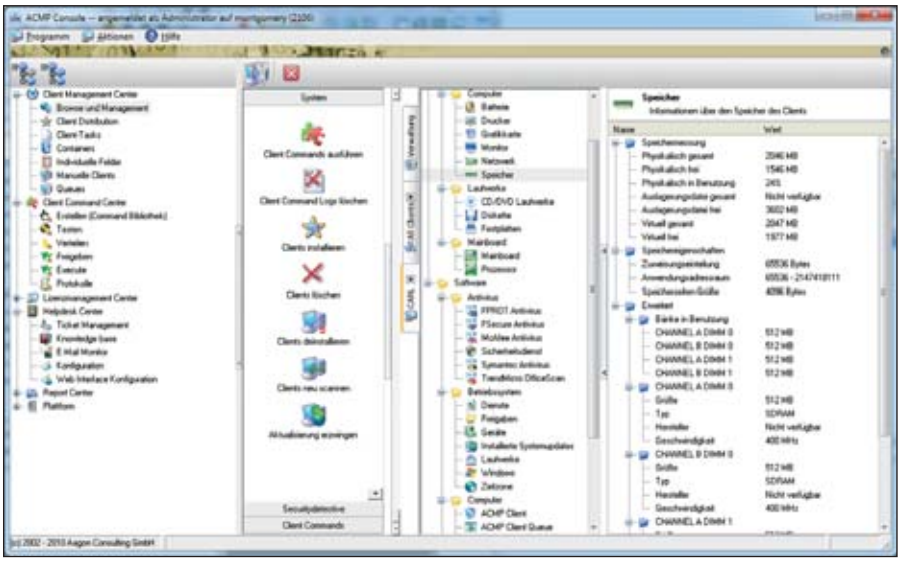


Bild 4: Per Doppelklick offenbart ACMP alle zur Verfügung stehenden Daten

Im nächsten Schritt dieses Workshops geht es daran, diese Übersicht nach eigenen Wünschen anzupassen und durch weitere Felder zu ergänzen. Wählen Sie hierfür zunächst in der Registerleiste den Eintrag "Felder". Um beispielsweise das Betriebssystem, die Seriennummer und das installierte RAM der Clients anzuzeigen, öffnen Sie den Zweig "Operating System", erneut den Zweig "Operating System" und ziehen den Eintrag "OS Name" per Drag and Drop auf die rechte Fensterseite. Genauso gehen Sie mit dem Zweig "Hardware / Machine" und dem Eintrag "System Serial" sowie unter "Operating System / Memory Usage" mit dem Eintrag "Physical Memory Total" vor. Alternativ können Sie auch über die Suchfunktion, als kleine Lupe symbolisiert, die Einträge suchen lassen. Klicken Sie nun in der Registerleiste auf "Ergebnisse" und aktualisieren Sie die Ansicht mit der Taste "F5" oder durch einen Klick auf das Aktualisierungssymbol in der Menüleiste. Die erweiterte Auswertung mit Betriebssystem, Seriennummer und Speicherausbau wird Ihnen nun angezeigt.

Systemanforderungen

ACMP Inventory aus der ACMP-Suite von Aagon Consulting gibt sich im Vergleich zu einigen Marktbegleitern genügsam in Bezug auf seine Hardwareanforderungen: Ein Windows Server 2003 mit einer Dual-Core-CPU, 2 GByte Arbeitsspeicher und eine 40 GByte-Festplatte reichen für einen ACMP-Server bereits aus. Für die Inventarisierung und Administration von bis zu 1.000 Client-Computern genügt ACMP zudem Microsoft SQL Server Express als Datenbank. Bei mehr Anwendern sollte ein vollwertiger SQL-Server zum Einsatz kommen.

Datenbank- und ACMP-Server lassen sich problemlos auf derselben Maschine installieren. Sofern der Windows Server über den Windows Update Service auf dem neuesten Stand ist, sind auch alle benötigten Komponenten für die Installation von ACMP Inventory bereits vorhanden. Fehlt Software wie beispielsweise das Service Pack 3 für das Microsoft Dotnet-Framework 2.0 oder höher, erkennt dies die Setup-Software von ACMP und wartet mit der Installation solange, bis Sie die fehlenden Komponenten nachinstalliert haben.

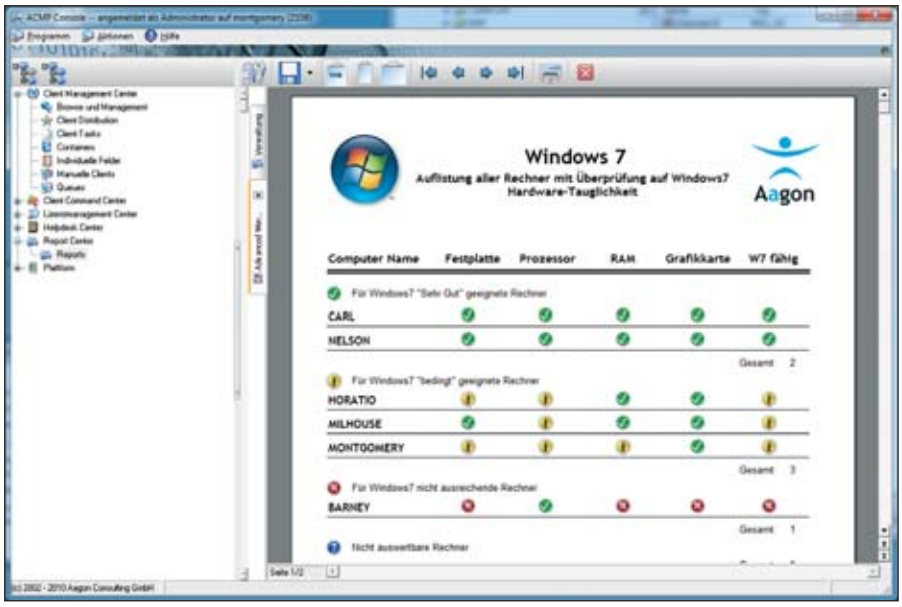


Bild 5: In wenigen Sekunden fertig: der Migrations-Report von XP zu Windows 7

Recht elegant hat der Hersteller das Gruppieren von Rechnern gelöst. Möchten Sie die Übersicht beispielsweise nach Betriebssystemen gruppiert sehen, ziehen Sie einfach den Spaltenkopf "OS Name" der Tabelle in den grauen Bereich zwischen Menüleiste und Tabelle. Über die Anzeige der "Entries" wissen Sie nun innerhalb weniger Sekunden, wie viele Windows XP-Rechner es in Ihrem Netzwerk gibt. Um die Gruppierung wieder aufzuheben, ziehen Sie den Eintrag einfach aus dem grauen Feld heraus. Sollte Ihnen die erweiterte Abfrage gefallen, können Sie diese über das Diskettensymbol in der Menüleiste speichern. In dem folgenden Dialogfeld geben Sie der Abfrage einen Namen oder speichern eine bereits vorhandene Abfrage mit Ihren Änderungen ab. Da Sie in der Baumstruktur im rechten Fenster beliebig viele Ordner und Unterordner anlegen dürfen, können Sie sich so verschiedenste Übersichten abspeichern.

Abfragen filtern und exportieren

In der Praxis kommt es sehr oft vor, dass Sie von einer Übersicht eigentlich nur einen kleinen Teil der Daten sehen möchten, ohne jedoch gleich eine neue Abfrage erstellen zu müssen. Hierfür sind die "Filter" das geeignete Arbeitsmittel. Die Filterfunktionen von ACMP beziehen sich stets auf die aktuelle Ansicht und bieten Ihnen Wildcards (Joker-Zeichen) sowie die bekannten booleschen Operatoren.

Möchten Sie in Ihrer Abfrage beispielsweise nur die Computer sehen, die eine IP-Adresse aus dem Bereich 192.168.1.100 bis 192.168.1.199 haben, so können Sie folgendermaßen einen passenden Filter einrichten: Klicken Sie zunächst in der Menüleiste auf das Icon mit der Tabelle und dem Filtersymbol. Bestätigen Sie dann den Eintrag "Primary IP" durch einen Doppelklick. Wählen Sie jetzt im Dialogfeld "Benutzerdefinierter Filter" "ähnlich" und im Freitextfeld "192.168.1.1__" und klicken Sie auf die Schaltfläche "flt". Der Unterstrich symbolisiert dabei einen Platzhalter. Im unteren Fensterbereich sehen Sie noch einmal die Filterkriterien, die bei dieser Ansicht zum Einsatz kommen. Durch das Setzen eines weiteren Filters können Sie diese Ansicht auf Wunsch noch weiter eingrenzen. Die Sortierung der Ansicht nehmen Sie über einen Doppelklick auf den Spaltenbezeichner vor. Den Export der aktuellen Ansicht in eine CSV-Datei starten Sie über die Schaltfläche mit dem roten Pfeil vor der Tabelle. Hier müssen Sie lediglich einen Dateinamen angeben und das Feldtrennzeichen auswählen.

Windows 7-Report

Mit ACMP Inventory und den bisher vorgestellten Funktionen ist es nicht schwer, sich beispielsweise alle PCs anzeigen zu lassen, die für den Betrieb unter Windows 7 geeignet sind. Noch leichter geht es mit einem von Aagon vordefinierten Bericht, den Sie auch als HTML-Datei speichern können. Um den Report einzusehen, klicken Sie in der Baumstruktur auf "Report Center", dann auf "Reports" und selektieren dort die Rubrik "Hardware". Wählen Sie dann den Knoten "DE", um eine deutschsprachige Auswertung zu erhalten, und im Anschluss den "Advanced Windows 7 Check" aus. Über die Parameter Festplatte, Prozessor, RAM und Grafikkarte baut ACMP Inventory jetzt einen Report auf, der über Ampelfarben schnell erkennbar aufzeigt, welche Maschine "sehr gut geeignet", "bedingt geeignet" und "nicht ausreichend" für Windows 7 ist.

Fazit

Eine zuverlässige und umfangreiche Inventarisierung aller PC-Arbeitsplätze ist die Basis für ein effizientes Clientmanagement. Hierzu zählen unter anderem eine automatische Verteilung von Betriebssystemen und Anwendungen, Lizenzmanagement, ein Helpdesk sowie die Automatisierung der zahlreichen kleinen administrativen Tätigkeiten, die jeden Tag in einem Unternehmensnetz anfallen. Mit ACMP Inventory haben Sie hierfür eine gute Grundlage gelegt, die Sie bei Bedarf über die Produkte von Aagon erweitern können. Das Reinschnuppern in die Zusatzfeatures ermöglichen die kostenlosen 15 Test-Lizenzen, die bereits installiert und aktiviert sind. *(dr)*

Link-Codes

[1] ACMP-Download-Seite
B3P11

[2] Windows Firewall in AD-Umgebung anpassen
B3P12

Exchange Server 2010

Verwaltete Exchange 2007-Ordner importieren

von Robert Lindermeier

Wer unter Exchange 2007 die Funktion "verwaltete Ordner" genutzt hat, wird sich wundern, dass es in der Verwaltungskonsole von Exchange 2010 keine Möglichkeit mehr unter der Organisationskonfiguration gibt, um die verwalteten Ordner und die angezeigten E-Mail-Tipps beim Klick auf den Ordner zu ändern. Das Feature bot sich zudem an, um etwa automatisch den Ordner "Gelöschte Objekte" der Postfächer durch Exchange entleeren zu lassen oder um ältere E-Mails automatisch aus dem Postfach zu entfernen.

Der Grund für dessen Verschwinden liegt darin, dass Exchange 2010 die Funktion "Messaging-Datensatzverwaltung" durch die "Aufbewahrungsrichtlinien" ersetzt. Um nun die bestehenden Richtlinien für verwaltete Ordner in Aufbewahrungsrichtlinien zu überführen, hat Microsoft eine Portierungsmöglichkeit vorgesehen. Dazu starten Sie in der Exchange Verwaltungskonsole über "Organisationskonfiguration / Postfach" den Assistenten "Port von verwaltete Ordner zu Tag". Da oftmals die ursprüngliche Konfiguration schon ein paar Tage zurückliegt und Sie möglicherweise nicht mehr genau wissen, welche Postfach-Ordner von der Richtlinie für verwaltete Ordner betroffen waren, sollten Sie sich zuerst die bestehenden Richtlinien über folgendes Shell-Cmdlet anzeigen lassen:

```
get-managedFolderMailboxPolicy | fl
```

Nun erhalten Sie neben dem Namen der Policy auch die Angabe darüber, welche Postfachordner im Detail von dieser Policy gesteuert werden. Diese Angabe finden Sie im Abschnitt "ManagedFolderLinks":

```
ManagedFolderLinks : {Junk E-Mail,
  Deleted Items, Sent Items, Inbox}
Name : Postfachrichtlinie Your-Admin
When created : 07.07.2007
….
```

Mit diesen Informationen können Sie die Portierung starten. Im Dialog vergeben Sie unter "Tagname" einen passenden Namen. Hier ist es durchaus sinnvoll, einen erklärenden Namen zu verwenden. In unserem Beispiel portieren wir die Einstellungen für den verwalteten Ordner "Gelöschte Objekte", der automatisch alle Elemente entfernt, die länger als drei Tage dort abgelegt sind.

Nach der Angabe des Tagnamens wählen Sie den betroffenen Ordner "Gelöschte Objekte" aus und vergeben einen Tipp-Kommentar, der dem Benutzer angezeigt wird, sobald er auf den Ordner klickt. Dieser Tipp wird nicht nur in Outlook, sondern auch in Outlook Web App angezeigt. Diesen Vorgang wiederholen Sie nun für alle in Exchange 2007 erstellten verwalteten Ordner. Im nächsten Schritt müssen Sie nun die importierten Tags über eine neue Aufbewahrungsrichtlinie aktivieren und die Postfächer zuordnen. Mit

```
remove-managedFolderMailboxPolicy
  -identity "Postfachrichtlinie
  Your-Admin"
```

entfernen Sie abschließend die "alte" Richtlinie für verwaltete Ordner. *(dr)*

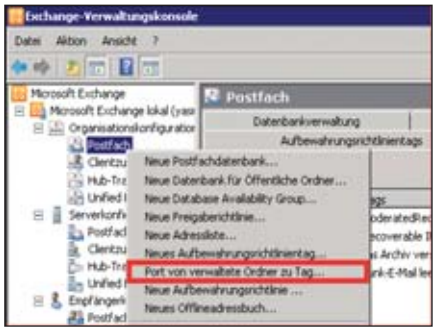


Bild 2: Über die Organisationskonfiguration finden Sie die Portierungsmöglichkeit in die Aufbewahrungsrichtlinien

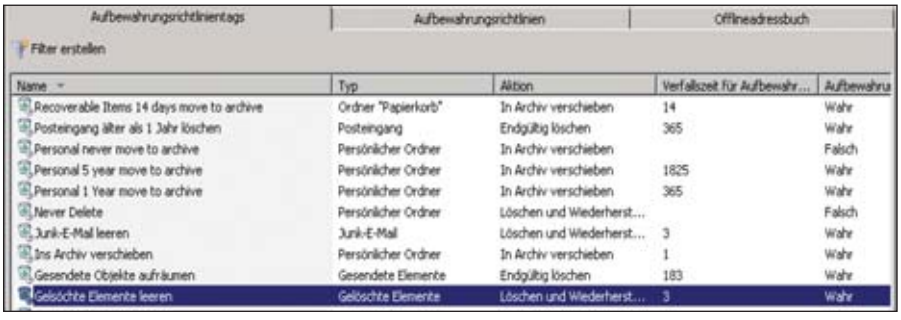


Bild 1: Über die Aufbewahrungsrichtlinien lassen sich die unter Exchange 2007 definierten Regeln weiter verwenden

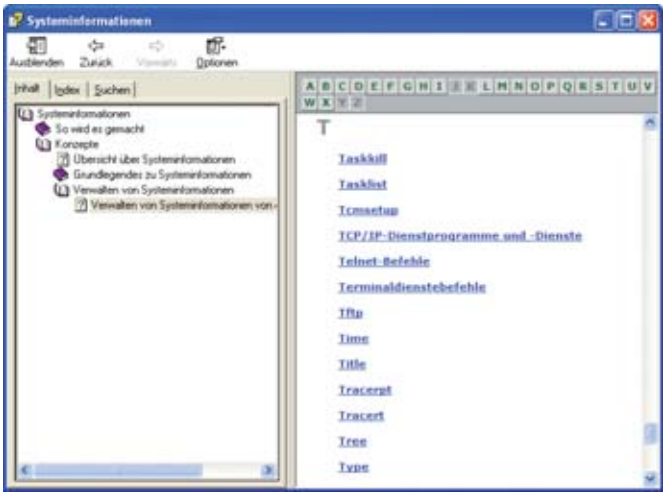
Tipps & Tricks ohne Gewähr

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.

Microsoft Windows

Die **PowerShell** ist ja derzeit sehr beliebt – zu Recht, wie ich finde. Allerdings wird dabei meiner Meinung nach oft übersehen, dass auch schon die reguläre **Kommandozeile eine Vielzahl nützlicher Funktionen** bietet, die dem Administrator die **tägliche Arbeit erleichtern**. Haben Sie vielleicht noch ein paar Geheimtipps auf Lager, die den Umgang mit der Kommandozeile betreffen?

Je nach Aufgabenfeld wartet die Kommandozeile mit einer ganzen Reihe an nützlichen Befehlen auf. Wenn Sie beispielsweise schnell aus dem Prompt zum Windows Explorer wechseln wollen, tippen Sie einfach *start.* ein. Vergessen Sie dabei nicht den Punkt, sonst funktioniert das Kommando nicht. Das Kommando *shutdown* ist sicherlich schon vielen Admins bekannt. Achten Sie bei der Verwendung des Befehls darauf, dass Sie ihn stets mit einem Parameter einsetzen müssen. Der Schalter "-s" bewirkt einen einfachen Shutdown, während der Schalter "-r" einen Neustart bewirkt. Durch den zusätzlichen Einsatz des Parameters "-f" erzwingt das System ein Ende aller Prozesse. Besonders praktisch ist der Parameter "-m", der zusammen mit einem UNC-Pfad des Remote-Herunterfahren eines entfernten Rechners bewirkt. Das Kommando *tasklist* führt alle derzeit laufenden Prozesse aus, die sich mit *taskkill /{PID des Prozesses}* beenden lassen. Auch hier gibt es diverse Schalter – der Remote-Schalter zum Zugriff auf ein fremdes System ist hier "-s". Mit "-u" und "-p" können Sie dem Kommando die entsprechenden User-Credentials mitgeben. Ein weiterer nützlicher Befehl ist *assoc*, mit dem Sie sich alle bestehenden Dateiendungs-Verknüpfungen anzeigen lassen. *driverquery* hingegen bringt alle auf einem Rechner installierten Treiber auf den Bildschirm – mit dem Parameter "-s" kann dies ein entfernter PC sein. Dies ist nur ein kleiner Auszug aus der Kommandoliste der klassischen Eingabeaufforderung. Windows XP besitzt eine Befehlszeilenreferenz, die Sie der Einfachheit halber als Verknüpfung auf dem Desktop hinterlegen können. Erstellen Sie dazu eine neue Verknüpfung mit beliebigem Namen und geben Sie als Ziel *%windir%\Help\nsinfo32.chm* an. Starten Sie die Verknüpfung mit einem Doppelklick, gehen Sie auf den Reiter "Index" und wählen Sie unter dem Menüpunkt "Systeminformationsprogramm" die Option "Verwalten über die Befehlszeile aus". *(ln)*



Windows XP verfügt über eine Referenz, die alle Befehle für die Kommandozeile auflistet

Seit kurzem ist ja das **Service Pack 1 für Windows 7 und Server 2008 R2** verfügbar. Müssen wir etwas Besonderes beachten, damit die **Installation erfolgreich** verläuft? Gerade in Bezug auf unsere virtualisierte Landschaft, die wir unter Hyper-V betreiben? Hier gibt es ja, wie ich gelesen habe, mit dem neuen Service Pack diverse neue Funktionen.

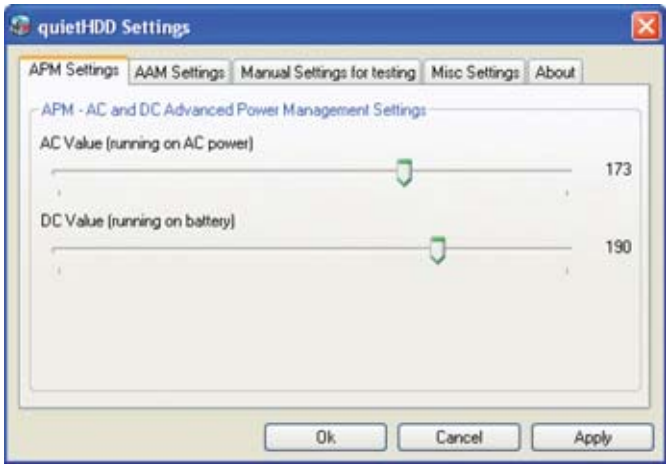
Wie bereits in der Vergangenheit wird das Service Pack (SP) für beide Betriebssysteme (Client sowie Server), sämtliche Architekturen (x86, x64, IA64) und mehrere Sprachen einsetzbar sein. Vor

der Installation sollten Sie auf jeden Fall ein vollständiges Backup anlegen, um bei einem Fehler rasch alle wichtigen Daten wiederherstellen zu können. Um Schwierigkeiten bereits im Vorhinein einen Riegel vorzuschieben, sollten Sie frühzeitig prüfen, ob die verwendete Hardware, die Treiber und alle Applikationen mit dem SP kompatibel sind. Was zudem oftmals übersehen wird: Ein Anti-Virus-Programm kann eine SP-Installation erheblich beeinflussen. Sie sollten den Scanner daher für den Zeitraum der Installation deaktivieren. Sind nun noch (temporär) 10 GByte freier Festplattenspeicher vorhanden, kann es losgehen. Nach der Installation belegt das SP1 zwischen 2,5 und 3,3 GByte Speicherplatz. Viele Neuerungen des SP1 betreffen Hyper-V. Nur mit dem jüngsten Update können Sie etwa von neuen Funktionen wie "RemoteFX", "Dynamic Memory" und "ARP Spoofing Prevention" Gebrauch machen. Bevor Sie diese Features aktivieren, sollten Sie allerdings bei einem Hyper-V Failover Cluster alle Nodes aktualisieren. Damit virtuelle Maschinen die neuen Optionen nutzen können, müssen Sie zudem die Integration Services auf den neuesten Stand bringen. Dies erübrigt sich, wenn auf der virtuellen Maschine selbst ebenfalls das Service Pack 1 zum Einsatz kommt. Die Remote Server Administration Tools (RSAT) für Windows 7 sollen bis April 2011 verfügbar sein. Bis zu diesem Zeitpunkt steht laut Microsoft dann auch das Service Pack 1 für System Center Virtual Machine Manager (VMM) bereit. Beide Updates benötigen Sie, um die neuen Funktionen von Hyper-V verwalten zu können. *(Michel Lüscher/ln)*

ServerTalk *Weitere Informationen zum Service Pack 1 und Hyper-V finden Sie auf www.server-talk.eu*

Auf einigen neuen, identischen **Arbeitsplätzen mit Windows 7** tritt häufiger das Problem auf, dass der **Computer beim Kopieren auf ein externes USB-Medium nicht mehr reagiert** oder der Kopiervorgang abbricht. Ich habe keine Idee, woran dies liegen könnte – sonst funktionieren die Rechner einwandfrei. Haben Sie hier einen Tipp?
Unter Umständen liegt auf Ihren Rechnern eine verhängnisvolle Kombination von Hard- und Software vor. Problematisch wird es immer dann, wenn auf einem PC Windows 7 oder Server 2008 R2 läuft und das System mit mehr als 4 GByte RAM ausgestattet ist. Wenn dann noch ein spezieller USB-Chipsatz – das NVIDIA USB Enhanced Host Controller Interface – dazukommt, kann es zu den von Ihnen beschriebenen Problemen kommen. Lösen lassen sich diese nur, wenn sie ein im Knowledge Base-Artikel 976972 beschriebenes Update auf die entsprechenden Systeme aufspielen. *(ln)*
Link-Code: B4PE3

Für den schnellen Fernzugriff von unterwegs habe ich mir ein kleines **Netbook gekauft**. Mit diesem bin ich recht zufrieden, allerdings beschäftigen mich zwei Fragen: Zum einen denke ich darüber nach, das vorinstallierte Windows 7 Starter durch eine **höhere Windows-Version** zu ersetzen. Würden Sie dies empfehlen? Zum anderen bin ich durch ein recht lautes Festplattengeräusch verunsichert, das sich wie ein Kratzen anhört. Eine genaue Untersuchung der Festplatte mit HDDScan hat jedoch keine Fehler ergeben, auch die S.M.A.R.T-Werte sind alle in Ordnung. Was kann das sein?
Zunächst zum ersten Teil Ihrer Frage: Ob sich ein Upgrade von Windows 7 Starter lohnt, hängt stark von der Hardware Ihres Netbooks und den Einsatzzwecken ab. Viele für den Unternehmenseinsatz erforderliche Funktionen wie Bitlocker oder der Domänenbeitritt sind nur in der Professional beziehungsweise Ultimate-Version verfügbar – allerdings ist hier die Frage, ob diese Editionen auf Ihrem Netbook laufen. Eine allgemeingültige Empfehlung können wir an dieser Stelle nicht abgeben. Wie immer Sie sich entscheiden – vergleichen Sie bei einem Anytime Upgrade die Preise. Microsoft selbst verlangt in der Regel immer am meisten – Drittanbieter liegen hier oft bis zu einem Drittel günstiger. Was das gruselige Geräusch der Festplatte betrifft, liegt höchstwahrscheinlich eine Unverträglichkeit Ihres Festplatten-Modells mit den Funktionen zum Energiemanagement vor. Knapp gesagt liegt das Kratzen an einem zu diesem Zeitpunkt eigentlich ungewollten Wechsel der Festplatte vom Schlaf- zum Zugriffsmodus. Beheben lässt sich diese Problematik möglicherweise durch ein spezielles Tool, das die APM-Einstellungen des Systems verändert. Seien Sie jedoch gewarnt, ein He-



Das Tool "quiethdd" macht sich an den Energieeinstellungen zu schaffen – Veränderungen sollten hier mit Bedacht gesetzt werden

rumspielen an diesen Einstellungen kann die Lebensdauer des Magnetspeichers stärker negativ beeinflussen als das Kratz-Geräusch. Zudem sind in Foren diverse Berichte nachzulesen, dass das unangenehme Kratzen mit zunehmender Lebensdauer des Netbooks immer seltener wird. *(ln)*

Link Code: B4PE4

Unsere Anwender haben uns von folgendem Problem berichtet: Wer unter Exchange Server 2007 versucht, ein **Raumpostfach (Ressource) länger als 24 Stunden buchen** zu wollen, trifft in den Einstellungen auf den Hinweis "Diese Ressource akzeptiert keine Besprechungen, die länger als 1440 Minuten dauern". Mit dieser Aussage ist dann auch **keine Buchung des Raumes** möglich. Gibt es irgendeine Möglichkeit, eine Ressource länger als einen Tag zu reservieren?

Die Lösung steckt hier tief in den Systemeinstellungen und lässt sich unter Exchange 2007 am besten mit der PowerShell verwirklichen. Dazu setzen Sie in der PowerShell das Kommando *get-mailbox* wie folgt ein:

```
get-mailbox | Where-Object { $_.Is-
  Resource -eq 'true'} | Set-Mail-
  boxCalendarSettings -MaximumDura-
  tionInMinutes 20160
```

Dieser Befehl setzt die maximale Dauer zum Beispiel auf 14 Tage (= 20.160 Minuten). Der Wert lässt sich natürlich frei anpassen. Beachten Sie, dass dieses Kommando unter Exchange 2010 nicht mehr funktioniert, da das CMDlet "Set-MailboxCalendarSettings" nicht mehr existiert. Änderungen lassen sich hier nur über die Eigenschaften des Raumpostfachs erreichen. *(Sepago/ln)*

Mehr Tipps zu den Themen Exchange und Terminaldienste lesen Sie auf http://blogs.sepago.de

Auf einigen Stationen unseres Netzwerks kommt noch **Outlook 2003** zum Einsatz. Auf einigen dieser Rechner **fehlt im Menü "Extras" der Abwesenheits-Assistent**. Kann ich den Assistenten irgendwie nachinstallieren oder was muss ich tun, damit er wie auf den anderen PCs auch im entsprechenden Menü auftaucht?

Um den Abwesenheits-Assistenten nachträglich zu installieren, gehen Sie wie folgt vor: Klicken Sie im Menü "Extras" auf "Optionen" und wählen Sie "Andere" aus. Klicken Sie dann auf "Erweiterte Optionen" und anschließend auf "Manager hinzufügen". Wenn in der nun erscheinenden Liste die "Exchange-Erweiterungsbefehle" auftauchen, wählen Sie diese aus. Wenn nicht, klicken Sie auf "Installieren" und in der folgenden Add-In-Aufstellung auf Emsuix.ecf. Beenden Sie nun mit mehreren Klicks auf "OK" die Einstellungen, schließen Sie Outlook und starten Sie Windows neu. Wenn der Abwesenheits-Assistent dann immer noch nicht im Menü erscheint, müssen Sie die Registry verändern. Starten Sie dazu mit *regedit* die Registrierungsdatenbank und navigieren Sie zum Schlüssel "HKEY_LOCAL_MACHINE / SOFTWARE / MICROSOFT / EXCHANGE/ CLIENT / EXTENSIONS". Legen Sie dort einen neuen Eintrag (REG_SZ) mit dem Namen "Exchange Extensions" an und weisem Sie diesem Eintrag folgenden Wert zu: "4.0 emsuix32.dll; 7; 011111111111110 ; 1111011100". Nun müsste sich spätestens nach einem Neustart der Abwesenheits-Assistent wie oben beschrieben nachinstallieren lassen. *(ln)*

Thunderbird

Von einem Firmenkonto frage ich meine **E-Mails mit Thunderbird** ab, und zwar über einen **IMAP-Account**. Dabei aktualisiert der E-Mailclient bei jeder Abfrage den Posteingangsordner. Nun fände ich es aber äußerst praktisch, wenn jeder der von mir angelegten Ordner auf den neuesten Stand gebracht wird. Kann ich diese Funktion Thunderbird irgendwie beibringen?

Eine Aktualisierung aller IMAP-Ordner ist möglich – sofern der zu kontaktierende Mailserver dies unterstützt. Die entsprechenden Settings auf Client-Seite verstecken sich bei Thunderbird in den erweiterten Einstellungen, die Sie über den Menü-Pfad "Extras / Einstellungen/ Erweitert / Konfiguration bearbeiten" erreichen. Hier gilt es nun, zwei Werte zu verändern: Den Wert "mail.check_all_imap_folders_for_new" müssen Sie auf "true" setzen, während der Eintrag "mail.imap.use_status_for_biff" auf "false" zu stellen ist. Beachten Sie, dass mit diesen Einstellungen je nach Anzahl der Ordner die Aktualisierung über IMAP recht viel Zeit in Anspruch nehmen kann. *(ln)*

Thunderbird verhindert bei empfangenen E-Mails ja automatisch das **Laden von externen Grafiken**. Dies finde ich aus Sicherheitsaspekten im Prinzip auch sehr praktisch, allerdings würde ich mir eine Art **Whitelist von Domänen** wünschen, bei der der E-Mailclient verlinkte Grafiken automatisch anzeigt. Wie kann ich dies erreichen?

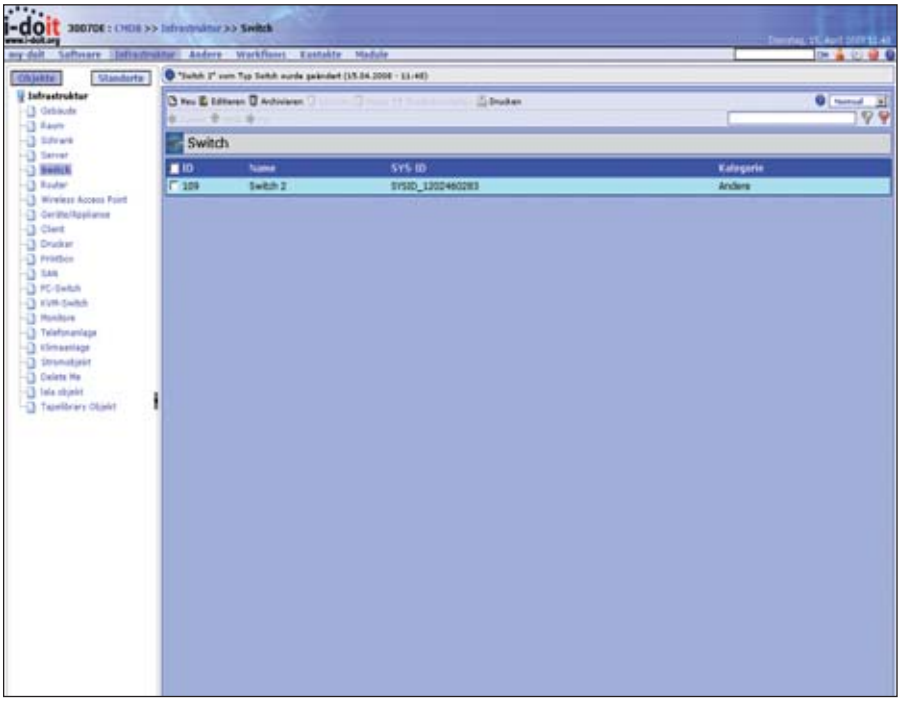
Auch hier finden sich die entsprechenden Einstellungen wieder in der erweiterten Konfiguration, der entsprechende Eintrag lautet "mail.trusteddomains", als Wert können Sie hier einfach die gewünschten Domains, durch Komma ohne Leerzeichen getrennt, eintragen. Wildcards und Subdomains sind an dieser Stelle nicht erlaubt. Beachten Sie zu-

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

dem, dass Sie hier nicht die Domain der Absender-Mail eintragen müssen, sondern die Domäne, von der die anzuzeigenden Grafiken kommen. Sind Sie hier nicht sicher, empfiehlt es sich, einen Blick in den Quelltext einer Mail zu werfen, deren Absender auf die Grafik-Whitelist soll. *(ln)*



Ebenso aufgeräumt wie eine gute IT-Dokumentation präsentiert sich die Oberfläche von i-doit

Tools

Die **Dokumentation der IT-Infrastruktur** ist für IT-Verantwortliche nach wie vor gleichermaßen wichtig wie zeitraubend. Doch richtig ausgeführt hilft sie, in vielen Situationen – etwa beim Troubleshooting – Zeit zu sparen. Insbesondere natürlich, wenn die Dokumentation nicht von Hand, sondern automatisiert mit einem Tool erstellt wurde. Wenn diese Software dann auch noch frei verfügbar ist und gleichzeitig weitere mächtige Features bietet, lohnt sich ein genauerer Blick.

Beim freien Werkzeug **i-doit** steht die **Erfassung und technische Dokumentation aller eingesetzten IT-Komponenten** im Vordergrund. Der Detailgrad liegt dabei im Ermessen des Anwenders und reicht von einer reinen Erfassung der relevanten Hersteller- und Modellinformationen bis zur exakten Repräsentation der zugrunde liegenden Infrastruktur. Das gilt in gleichem Maße für die Verbindungsdaten von Strom-, Speicher- und Datennetzen oder die Verwaltung und Zuweisung von Software und Lizenzen. Neben der technischen Dokumentation erlaubt i-doit die **Erfassung und Zuordnung von Vertrags- und Betriebsdaten** zu den dokumentierten Objekten. Sei es der Wartungsvertrag mit Kontakt und Ablaufdatum, die Notfallplanung für Komponenten und Systeme, digitale Handbücher oder Konfigurationsdaten. Alle Dokumente in i-doit unterliegen dabei einer Versionsverwaltung, so dass Änderungen und Anpassungen nachvollziehbar bleiben. Eine Benachrichtigungsfunktion und einstellbare Schwellenwerte erlauben automatische Erinnerungen per E-Mail. Neben den direkten Abhängigkeiten, die sich aus den Verbindungsdaten oder der Zuweisung von Software an Systeme ergeben, können auch manuelle Abhängigkeiten dokumentiert werden, die sich indirekt aus den IT-Geschäftsprozessen ergeben. Das Logbuch der Software protokolliert alle Änderungen, die an einem Objekt vorgenommen wurden. Verbunden mit einer Kommentierungsfunktion lassen sich diese Logbucheinträge zudem mit weiteren Informationen versehen, um etwa den Grund einer Änderung festzuhalten. Darüber hinaus dient das Logbuch für verschiedene Module als Archiv, um darin den Status oder Ereignisse aus dem Echtbetrieb abzulegen. *(jp)*

Link-Code: B4PE1

Kommerzielle Lösungen für das **Client-Management** bieten heutzutage alles, was der Administrator sich zur Verwaltung seiner Anwender-PCs wünschen kann: **Automatische Software- und Betriebssystemverteilung, Inventarisierung und Lizenzmanagement**. Doch diese Features haben auch ihren Preis und sind für kleinere Umgebungen daher meist nicht rentabel.

Als Open Source-Alternative bietet sich hier **opsi** – ein freies Client-Management-System zur Verwaltung von Windows-Clients auf Basis von Linux-Servern – an. Opsi bietet eine automatische Softwareverteilung für PCs, automatische Betriebssysteminstallation, Hardware- und Software-Inventarisierung sowie Lizenzmanagement. Der opsi-client-agent sorgt auf dem PC dafür, dass nach jedem Boot und vor dem Login überprüft wird, ob Software zu installieren ist. Ist dies der Fall, so wird die Software mit dem script-gesteuerten Setup-Programm opsi-Winst auf dem Client installiert. Die Betriebssysteme Windows XP, 2003, Vista, Windows 7 und 2008/R2 (32 und 64 Bit) lassen sich mit dem Werkzeug automatisch installieren. Mit dem opsi-Modul hwaudit werden Hardwareinformationen per WMI ausgelesen und an den opsi-server zurückgemeldet. Die Daten der Hardwareinventarisierung stellt opsi in einer nach Geräteklassen sortierten Übersicht dar. Hier bietet opsi die Möglichkeit der Auswahl von Clients nach Hardware-Kriterien wie zum Beispiel der Größe des Arbeitsspeichers. Das opsi-Lizenzmanagement-Modul verwaltet die Lizenzen für die diversen nicht-freien Softwareprodukte, die auf mit opsi verwalteten Clients eingesetzt werden. *(jp)*

Link-Code: B4PE2

Quelle: Atringo

Datenrettung durch externe Dienstleister

Professionelle Hilfe beim Speicher-Crash

von Nicolas Ehrschwendner

IT-Verantwortliche in Unternehmen lösen technische Probleme am laufenden Band. Sie sind überall zur Stelle, wo es brennt. Doch es gibt auch Situationen, in denen sie machtlos sind. Wenn beispielsweise Defekte in den Speichersystemen eines Unternehmens auftreten, wird es ernst. Können die Mitarbeiter nicht mehr auf die Daten zugreifen oder es gehen Daten komplett verloren, stoßen auch viele Administratoren an ihre Grenzen. IT-Administrator zeigt in diesem Artikel einerseits Tücken von Speichersystemen auf. Andererseits erfahren Sie, worauf Sie achten sollten, wenn Sie sich Hilfe durch professionelle Datenretter holen.

Die meisten Unternehmen versuchen, einem Verlust von Daten bestmöglich durch moderne Speicher-Management-Systeme vorzubeugen. Damit im Ernstfall die dort gespeicherten Unternehmensdaten wiederhergestellt werden können, beinhalten solche Systeme automatische Backup-Funktionen. Zum Beispiel bietet sich hier die Speichertechnik CDP (Continuous Data Protection) an. Diese erfasst Änderungen kontinuierlich, anstatt punktuelle Backups anzulegen, die dann viel Zeit und Speicherplatz beanspruchen. Ganz gleich, welche Speichertechnik zum Einsatz kommt, Administratoren können mithilfe der regelmäßig angelegten Sicherungskopien zwar bei vorübergehenden Speicherproblemen und kleineren Fehlern Datenverlust verhindern. Bei gravierenden Schäden am Speichermedium selbst müssen jedoch in der Regel Experten herangezogen werden, um die Unternehmensdaten zu retten.

NAS und seine Tücken

Viele Firmen setzen zur Sicherung ihrer Daten auf Network Attached Storage (NAS). Dies sind Speichermedien, die ähnlich wie ein Computer aufgebaut sind. Sie sind beliebt, weil sie flexibel an vielen Arbeitsplätzen einsetzbar sind, ganz unabhängig vom Betriebssystem. Jedoch treten immer wieder Probleme beim Zugriff auf NAS-Daten auf. Ursachen dafür können Festplattenausfälle sein, Bedienungsfehler, aber auch Bugs in der NAS-Software. Häufig verursachen aber auch Updates der Firmware Probleme, also Aktualisierungen der Hardware-nahen Basis-Software, ohne die das NAS nicht funktioniert. Bei solchen Updates wird oft der logische Aufbau der Dateiablage unabsichtlich verändert, so dass das NAS keinen Zugriff mehr auf die gespeicherten Daten hat. Deshalb empfiehlt es sich, vor einem Update der NAS-Firmware Sicherungskopien anzulegen. Dies ist zwar nicht immer ganz einfach, schützt aber möglicherweise vor Datenverlust. Denn um Daten in einem NAS retten zu können, auf die der Administrator keinen Zugriff mehr hat, müssten alternativ externe Dienstleister beauftragt werden, die sich auf Notfälle spezialisiert haben.

Datenverlust in RAID-Systemen

Innerhalb eines NAS fällt oft die Wahl auf ein RAID-System. RAID steht für "Redundant Array of Independent Disks", also einen Speicherverbund aus mehreren einzelnen Festplatten. Mit einem RAID lässt sich eine besonders hohe Speicherkapazität bei relativ überschaubaren Kosten erreichen. Bei den meisten RAID-Systemen werden die Daten mit redundanten Informationen im Datenträgerverbund abgespeichert.

Eine Ausnahme stellt hier lediglich das RAID 0-System dar, das aus einem Verbund von unabhängigen Festplatten besteht, die zu einem Speichermedium zusammengeschlossen werden. RAID 0 ermöglicht zwar einen schnellen Zugriff auf alle Platten gleichzeitig, birgt aber auch das Risiko des Datenverlustes, wenn nur eine einzelne der Festplatten ausfällt. Andere RAID-Systeme sorgen durch das Speichern redundanter Daten dagegen dafür, dass trotz Ausfalls einer oder mehrerer einzelner Festplatten im Datenspeicher alle Daten verfügbar bleiben.

Aufgrund der relativ geringen Kosten ist beispielsweise das RAID 5-System weit verbreitet. Dafür benötigt der Nutzer mindestens drei Festplatten. Bei RAID 5 werden entsprechend dem Algorithmus des RAID-Controllers die Parity-Daten auf den angeschlossenen Festplatten verteilt. Über diese Parity-Daten lassen sich verlorene Daten wiederherstellen, auch wenn auf eine der Festplatten im Verbund gar nicht mehr zugegriffen werden kann.

Bei dem weniger verbreiteten RAID 4 dagegen werden die Parity-Daten nicht verteilt, sondern nur auf einer Festplatte gespeichert. Ein Nachteil von RAID 5 ist allerdings die relativ geringe Schreibgeschwindigkeit. Das Verfahren eignet sich daher am besten für große Datenmengen, die sich auf viele kleine Dateien verteilen.

RAID 6 bietet im Vergleich zu RAID 5 noch etwas mehr Sicherheit, da es sogar bei einem Ausfall von zwei Festplatten noch funktioniert. RAID 6 wird im Handel unter anderem auch unter dem Namen "Advanced Data Guarding" angeboten und umfasst mindestens vier Festplatten. Doch auch bei RAID 6-Systemen droht endgültig Datenverlust, wenn mehr als zwei Festplatten im Speicherverbund beschädigt sind.

Rebuild birgt besonderes Risiko

Festplatten können zum Beispiel durch einen Head-Crash irreparabel beschädigt werden. Dabei berührt der Lese- und Schreibkopf direkt die Festplattenoberfläche, was etwa durch Erschütterungen oder falschen Einbau der Festplatte geschehen kann. Ebenso kann Überspannung, zum Beispiel durch einen Blitzschlag, Defekte verursachen. In solchen Fällen kann der Administrator versuchen, die Daten auf der beschädigten Festplatte innerhalb des RAID-Systems wiederherzustellen.

Doch gerade im Prozess der Datenwiederherstellung aus den Parity-Daten, dem sogenannten Rebuild, kann es zu Komplikationen kommen. Denn für das Rebuild muss der RAID-Controller auf alle Festplatten zugreifen und die dort noch vorhandenen Daten auslesen. Fällt während dieses Vorgangs eine weitere Festplatte aus oder findet der Controller neue beschädigte Sektoren, ist auf das gesamte RAID-System kein Zugriff mehr möglich. Der Wiederherstellungsvorgang bricht ab.

Ein häufiges Problem bei RAID-Systemen in Windows-Servern ist der Einsatz des Windows-Prüfprogramms Checkdisk (CHKDSK) beziehungsweise Scandisk. Während das Hilfstool an anderer Stelle zuverlässig Dateisystemfehler reparieren kann, führt es beim Einsatz in RAID-Systemen zu Defekten, indem es die innere Logik des RAID-Systems zerstört. Innerhalb einer RAID-Anordnung sollte man das Programm deshalb in der Windows-Registry deaktivieren, um einen automatischen Start von Checkdisk auszuschließen.

SSD-Speicher schützen nicht vor Datenverlust

Als Speichermedium der Zukunft gelten derzeit Solid State Drives, kurz SSD. Wie der Name verrät, liegt deren großer Vorteil in ihrer Robustheit. Denn SSDs sind, anders als Festplatten, nicht aus vielen kleinen mechanischen Einzelteilen aufgebaut. Sie enthalten beispielsweise keine Lese- und Schreibköpfe und keine Magnetscheiben. Das oben beschriebene Head-Crash-Szenario ist hiermit ausgeschlossen. Stattdessen bestehen sie aus Flashspeicher-Bausteinen. So arbeiten sie im Vergleich zu Festplatten lautlos und verbrauchen weniger Strom. Auch die Geschwindigkeit beim Start von Windows oder dem Zugriff auf Datenbanken ist höher. Doch trotz des völlig anderen Aufbaus von SSD ist die Sicherheit nur trügerisch. Gerade die scheinbare Robustheit der Datenträger kann zu unsachgemäßer Handhabung und zu physikalischen Schäden führen.

SSDs sind im Allgemeinen schockresistenter als gewöhnliche Festplatten. Durch einen Sturz können aber trotzdem beispielsweise Haarrisse auf der Platine oder auch Beschädigungen der Kontakte entstehen. Äußere Einflüsse wie Wasser können Defekte hervorrufen, etwa einen Kurzschluss. Ebenso können Fehler in der Firmware bei SSDs zu Datenverlust führen, aber auch zu logischen Problemen, zum Beispiel wenn der Datenträger während eines laufenden Datentransfers von der Schnittstelle abgezogen wurde. Insgesamt haben SSDs also im alltäglichen Gebrauch viele Vorteile, schützen aber keinesfalls vor dem Verlust von Daten. Auch hier empfiehlt es sich, regelmäßige Backups anzulegen, wie bei jedem Speichermedium.

Im Ernstfall Experten konsultieren

Je nachdem, welche Daten durch IT-Fehler verloren gehen, drohen dem betroffenen Unternehmen hohe wirtschaftliche Schäden, Imageverlust, rechtliche Konsequenzen oder im schlimmsten Fall der Konkurs. Beispielsweise gibt es für bestimmte Unternehmensdaten Aufbewahrungspflichten, weshalb auch der Zugriff auf archivierte Daten immer gewährleistet sein muss. Deshalb ist es entscheidend für ein Unternehmen, dass bei Problemen mit den Speichermedien die richtigen Entscheidungen getroffen werden. Zwar gibt es eine Reihe von Software-Tools, die Hilfe im Notfall versprechen. Jedoch stoßen diese bei Hardware-Schäden schnell an ihre Grenzen.

Wer sich an die Hardware selbst heranwagt und Festplatten öffnet, muss sich bewusst sein, dass die Technik äußerst empfindlich ist. Schon ein scheinbar einfacher Eingriff in die Hardware birgt ein hohes Risiko und kann zum Totalausfall führen. Dies erhöht zusätzlich den Aufwand für professionelle Datenretter. Eine risikoarme Reparatur sollte deshalb in einem Reinraumlabor stattfinden.

IT-Administratoren sollten im Ernstfall auf Experten für Datenrettung vertrauen, sonst laufen sie Gefahr, durch gescheiterte Rettungsversuche Zeit zu verlieren und den Schaden nur zu vergrößern. Die Wahrscheinlichkeit, die Daten dann im Nachhinein noch retten zu können, wird immer geringer. Fachleute können den Schaden auf schnelle und diskrete Weise in Grenzen halten.

Doch woran erkennen Sie seriöse, zuverlässige Anbieter? Schließlich verlassen Sie sich nicht nur darauf, dass sie die Rettung in technischen Notfällen darstellen. Sie vertrauen ihnen auch Unternehmensdaten an, die normalerweise niemand von außen einsehen kann und darf. Hinzu kommt das Phänomen, das manche Privatleute vielleicht auch von Schlüsseldiensten kennen: So manche "Retter" nutzen die schwierige Lage ihrer Kunden durch überhöhte Preise aus, welche die Kunden nur aufgrund ihrer ausweglos erscheinenden Lage zu zahlen bereit sind.

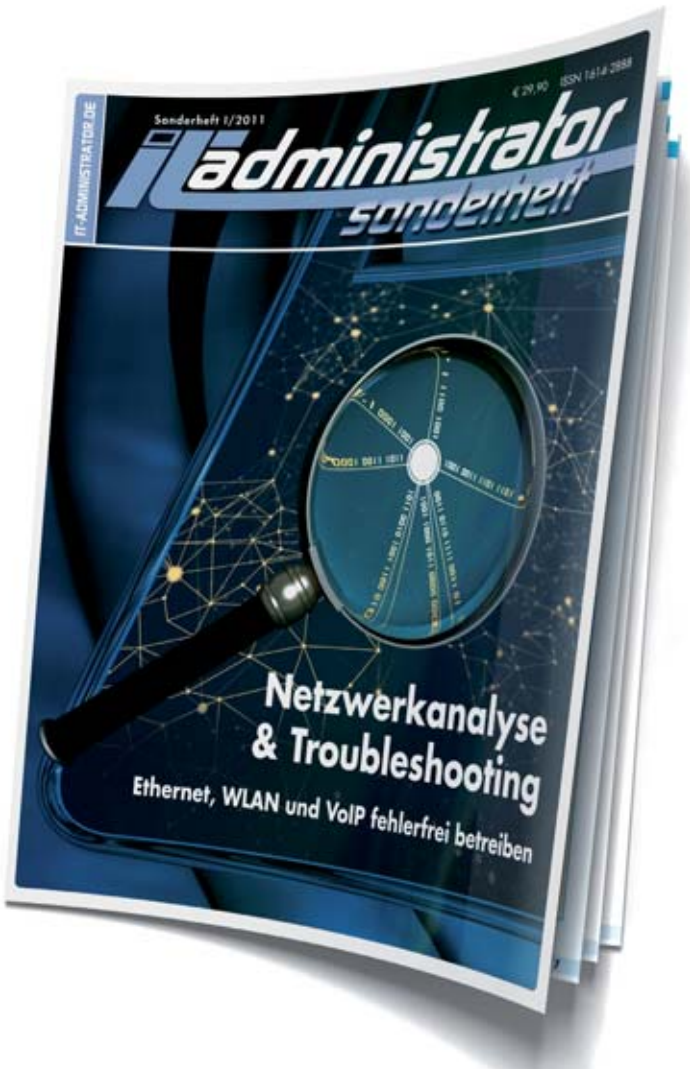
Seriöse Datenretter

Wichtig sind in der Kommunikation zwischen Kunde und Dienstleister vor allem Vertrauen und Transparenz. Der Anbieter muss seinem Kunden deutlich machen, welche technischen Möglichkeiten er in seiner Situation hat und ihn kompetent beraten, damit die richtigen Entscheidungen getroffen werden können. Dazu gehört als erster Schritt unbedingt eine Analyse des Status Quo, die anschließend mit dem Geschäftsführer oder IT-Verantwortlichen besprochen wird. Auf dieser Grundlage kann der Kunde entscheiden, ob überhaupt eine professionelle Datenrettung durchgeführt werden soll. So behält das Unternehmen einen Überblick über die anfallenden Kosten für den Notfall-Einsatz. Im Voraus einen Pauschalpreis zu versprechen, ist dagegen unseriös. Auch wenn die Kosten sich im Rahmen einer gewissen Preisspanne bewegen sollten, sind sie in der Regel nicht exakt vorhersehbar. Zudem sollten laut Attingo-Datenrettungsexperte und Mitgeschäftsführer Peter Franck Datenretter unter anderem eine spezielle Ausstattung und ein großes Kontingent an Ersatzteilen mitbringen.

Im Vorfeld recherchieren

Auch wenn es im Notfall schnell gehen muss, sollten Sie im Vorfeld versuchen, sich ein Bild von dem Dienstleister zu verschaffen. Empfehlungen finden Sie zum Beispiel über spezielle Internetforen, wo sich Erfahrungen mit anderen Administratoren austauschen lassen. Datenschutz ist für externe, seriöse Dienstleister dabei oberstes Gebot. Weder dürfen Unternehmensdaten in die Hände Dritter weitergegeben werden noch Informationen über den Datenrettungsprozess an sich. IT-Verantwortliche sollten deshalb dem Anbieter gezielt Fragen stellen, bevor sie einen Auftrag erteilen, etwa: Wo genau und von wem werden die Daten eingesehen, bearbeitet oder gespeichert? Bei einem sensiblen und heiklen Thema wie Datenrettung kommt es nämlich darauf an, trotz einer prekären Lage besonnen zu handeln und zuvor alle Optionen abzuwägen. *(dr)*

Nicolas Ehrschwendner ist Geschäftsführer bei der Attingo Datenrettung GmbH.



Bestellen Sie jetzt

das IT-Administrator

Sonderheft I/2011!

180 Seiten Praxis-Know-how rund um das Thema

Netzwerkanalyse & Troubleshooting

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

** IT-Administrator Abonnenten erhalten das Sonderheft I/2011 für € 24,90. Nichtabonnenten zahlen € 29,90. Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.*

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

administrator
Das Magazin für professionelle System- und Netzwerkadministration

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

☐ **Ja**, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft I/2011 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft I/2011 zum Preis von **€ 29,90** inkl. Versand und 7% MwSt.

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____ BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

ITA 0411

So erreichen Sie unseren Vertrieb, Abo- und Leserservice:

Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville
Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de

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

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

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

Juristische Vorgaben zur E-Mailarchivierung (1)

Elektronische Post rechtssicher verwahrt

von Patrick Prestel und Max-Lion Keller

Rund um das Thema E-Mailarchivierung haben Unternehmen zahlreiche Gesetze einzuhalten. Insbesondere entstehen erhebliche Rechtsprobleme, wenn Unternehmen ihren Mitarbeitern die private Nutzung der geschäftlichen E-Mailadresse gestatten. Dieser zweiteilige Beitrag zeigt die rechtlichen Vorgaben zur E-Mailarchivierung sowie die Konflikte mit dem Datenschutz und dem Fernmeldegeheimnis des Telekommunikationsgesetzes auf.

Die E-Mail wird vielfach in ihrer rechtlichen Bedeutung unterschätzt und oft als relativ unverbindlich eingestuft. Dies geschieht jedoch zu Unrecht, da die in einer E-Mail enthaltene Erklärung oder Information absolut rechtsrelevant ist. Vor diesem Hintergrund ist es auch kaum nachvollziehbar, dass bislang nur wenige Unternehmen das Kommunikationsmedium E-Mail wirklich beherrschen – gerade in rechtlicher Hinsicht. Oftmals sind es die Firmenmitarbeiter, die für den Inhalt und die Verwertung der ausgetauschten Nachrichten zuständig sind, während die Unternehmen sich damit begnügen, eine stabile und kosteneffiziente Telekommunikationsinfrastruktur bereitzustellen. Fragen der unternehmensgesteuerten Archivierung des eigenen E-Mailverkehrs kommen dabei oftmals zu kurz. Nur, in Deutschland ist die Palette möglicher Sanktionen bei einer nur mangelhaften E-Mailarchivierung durchaus beeindruckend.

So kann etwa eine mangelhafte E-Mailarchivierung als Verletzung handelsrechtlicher Buchführung gewertet werden und wegen der Maßgeblichkeit zugleich einer Verletzung der steuerrechtlichen Buchführungspflicht gleichkommen. Da wiederum Mängel der Buchführung die steuerrechtliche Beweiskraft der Bücher beeinträchtigt, wäre die Finanzverwaltung in diesem Fall berechtigt, den steuerlichen Gewinn nach § 162 II Abgabenordnung (AO) zu schätzen. Zudem könnte die Finanzverwaltung die Buchführungspflicht durch ein Zwangsgeld erwirken (§ 328 I AO). Eine Verletzung der Compliance-Pflicht ist ebenfalls möglich. Compliance bedeutet die Legalitätspflicht eines Unternehmens und umfasst die Sicherstellung der Rechtmäßigkeit des Handelns aller am Unternehmen beteiligten Personen. Anerkannt ist, dass die Pflicht für alle Unternehmen besteht.

Abgesehen von steuerrechtlichen Sanktionen kann die Verletzung der E-Mailarchivierungspflicht auch strafbar sein, etwa wenn durch eine unzureichende oder gar manipulative Archivierung von E-Mails das Unternehmen vorsätzlich die Übersicht über dessen Vermögensstand erschwert mit dem Ziel, Vermögensbestandteile, die im Falle der Eröffnung eines möglichen Insolvenzverfahrens zur Insolvenzmasse gehören, beiseite zu schaffen oder gar zu verheimlichen, vgl. § 283 ff. Strafgesetzbuch (StGB). Darüber hinaus regelt § 283b StGB, dass eine Verletzung der Buchführungspflicht mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft werden kann. Des Weiteren kann eine vorsätzliche oder leichtfertige Verletzung der Buchführungspflicht eine Ordnungswidrigkeit sein. Hier käme etwa eine Steuergefährdung gemäß § 379 AO in Betracht (soweit nicht eine leichtfertige Steuerverkürzung gemäß § 378 AO vorliegt).

Persönliche Haftung

Neben den genannten Gesetzesverstößen sind auch sind zivilrechtliche Sanktionen denkbar. So macht Verletzung der Buchführungspflicht den Vorstand oder Geschäftsführer der jeweiligen Gesellschaft schadensersatzpflichtig nach § 93 II Aktiengesetz (AktG) / § 43 II GmbH-Gesetz (GmbHG). Im Aktiengesetz ist festgelegt, dass eine persönliche Haftung des Vorstands dann in Betracht kommt, wenn er Entwicklungen, die zukünftig ein Risiko für das Unternehmen darstellen könnten (dazu gehört eben auch die unterlassene Speicherung geschäfts- oder steuerrechtlich relevanter E-Mails), nicht durch ein Risikomanagement überwacht und durch geeignete Maßnahmen vorbeugt (§ 91 Abs. 2 und § 93 Abs. 2 AktG).

Nahezu dieselben Anforderungen gelten für den Geschäftsführer einer GmbH, der

"die Sorgfalt eines ordentlichen Geschäftsmannes" aufzubringen hat (§ 43 Abs. 1 GmbHG). Diese zugegebenermaßen eher allgemein gehaltene Formulierung beinhaltet in der rechtlichen Praxis ganz ähnliche Folgerungen für das Risikomanagement wie für Vorstände nach dem Aktiengesetz. Kommt die Geschäftsführung oder der Vorstand – als Verantwortliche – der oben beschriebenen Pflicht zur Archivierung von E-Mails (als allgemeine Risikovorsorgepflicht) nicht nach und entsteht dadurch dem Unternehmen ein finanzieller Schaden, kann dies zu einer persönlichen Haftung der Mitglieder des Vorstands und der Geschäftsführung, unter Umständen auch der Aufsichtsratsmitglieder, (§116 AktG) führen.

Darüber hinaus wird immer wieder gerne übersehen, dass natürlich auch E-Mails bei gerichtlichen Streitigkeiten durchaus Bedeutung zukommen kann – und zwar im Rahmen der freien richterlichen Beweiswürdigung. Schon aus diesen Gründen tut jedes Unternehmen gut daran, elektronisch gespeicherte Mitteilungen revisionssicher und in einer Art und Weise zu speichern und zu indexieren, die den permanenten und schnellen Zugriff erlaubt ("Allzeit-Verfügbarkeit") und die Integrität der Daten gewährleistet.

Wegen der Umsetzung der Banken- und Kapitaladäquanzrichtlinie, besser bekannt unter dem Namen "Basel II", sind Banken und Finanzinstitute in Deutschland seit 2007 zudem gesetzlich verpflichtet, die Vorgaben des Basel II-Abkommens umzusetzen und insbesondere eine individuelle Bonitätseinschätzung des jeweiligen kreditsuchenden Unternehmens durchzuführen. Mittels dieser Bonitätseinschätzung kann sodann ermittelt werden, wie hoch die Wahrscheinlichkeit ist, dass der Kredit an die Bank auch wieder zurückgezahlt wird ("Ausfallrisiko"). Sollte dabei das Risiko eines Ausfalls als hoch eingestuft werden, wird sich die Bank dies bezahlen lassen, indem sie die Bonität des kreditsuchenden Unternehmens herabsetzt und nur ungünstige Kreditkonditionen weitergibt. Im schlechtesten Falle kommt es gar zu einer Weigerung einer Kreditgewährung. Es ist selbstverständlich, dass in diesem Zusammenhang ein besonderes Augenmerk auf dem operationalen Risiko "Risikomanagement" (und damit der E-Mail Archivierungspflicht) liegen muss.

Rechtliche Vorgaben zur E-Mailarchivierung

Ein Gesetz, das sämtliche gesetzlichen Regelungen in Bezug zur Archivierung von E-Mails zusammenfassen würde, gibt es nicht. Vielmehr muss sich der Verantwortliche die entsprechenden Regelungen mühsam aus verschiedenen gesetzlichen Bestimmungen zusammensuchen. Dies wird wohl auch ein Grund dafür sein, dass sich viele Unternehmer noch immer nicht darüber im Klaren sind, dass der Gesetzgeber sie in bestimmten Fällen konkret zur Errichtung einer effizienten und vor allem sicheren Archivierung von E-Mails verpflichtet hat. Nur wer einen Überblick über die relevanten Gesetze und Verordnungen hat und ein geeignetes Sicherheitskonzept verfolgt, kann sich hier vor rechtlichen Konsequenzen schützen. Folgende rechtliche Vorgaben wären im Zusammenhang mit der E-Mail-Archivierungspflicht beispielsweise zu nennen:

- das Handelsgesetzbuch (HGB)
- das Bundesdatenschutzgesetz (BDSG)
- das Telekommunikationsgesetz (TKG)
- die Abgabenordnung (AO)
- die GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen)

Folgende elektronische Post (also etwa E-Mails) ist zu archivieren:

1. E-Mails, die als Handelsbriefe einzustufen sind, müssen archiviert werden: In § 238 Abs. 2 HGB schreibt der Gesetzgeber für einen Kaufmann die Verpflichtung vor, eine Kopie der abgesendeten "Handelsbriefe" zurückzubehalten beziehungsweise sicher aufzubewahren (sei es in Papierform, als Grafik- oder auch Textdatei). Da unter einem Handelsbrief jedes Schreiben zu verstehen ist, das der Vorbereitung, dem Abschluss, der Durch-

führung oder auch der Rückgängigmachung eines Geschäfts dient, ist damit auch die gesamte in E-Mails gehaltene Geschäftskorrespondenz eines Unternehmens betroffen. Handelsbriefe sind jedoch nur Schreiben mit Außenwirkung; müssen also von einem Dritten gesendet oder empfangen worden sein. Zu den Handelsbriefen gehören etwa Aufträge (auch Änderungen und Ergänzungen), Auftragsbestätigungen, Versandanzeigen, Frachtbriefe, Lieferpapiere, Reklamationsschreiben, Rechnungen, Zahlungsbelege sowie schriftlich gefasste Verträge. Die E-Mail-Archivierungspflicht gilt dabei für jeden Kaufmann (vgl. §§ 1,2,3 HGB), insbesondere OHGs, GmbHs, AGs und KGs. Dagegen gilt die E-Mail-Archivierungspflicht nicht für Nichtkaufleute, wie etwa Kleingewerbetreibende und Freiberufler.

2. Sonstige E-Mails mit steuerrechtlichem Bezug sind aufzubewahren: Neben den Handels- oder auch Geschäftsbriefen sind auch all diejenigen abgesandten E-Mails aufzubewahren, die in steuerrechtlicher Hinsicht von Bedeutung sind (§ 147 Abgabenordnung, AO). Das können insbesondere E-Mails sein, die folgende Inhalte enthalten: Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und Organisationsunterlagen, die empfangenen, aber auch gesendeten Handels- oder Geschäftsbriefe, Buchungsbelege oder sonstige Inhalte, die für die Besteuerung von Bedeutung sind.

3. Art der Speicherung: Sämtliche E-Mails, die steuerlich relevante Sachverhalte enthalten, sind in elektronischer sowie rechtssicherer Form aufzubewahren beziehungsweise zu archivieren. Nach den vom Bundesfinanzministerium veröffentlichten Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) reicht es keineswegs mehr aus, die relevanten E-Mails einfach nur auszudrucken und abzuheften oder die relevanten E-Mails in maschinell nicht auswertbaren Formaten (etwa als PDF-Datei) zu archivieren.

4. Dauer der Archivierungspflicht: Gemäß § 147 Abgabenordnung sind die als Handels- oder Geschäftsbriefe einzustufenden E-Mails sechs Jahre aufzubewahren. Sollten die E-Mails dagegen Buchungsbelege, Rechnungen, Bilanzen, Jahresabschlüsse oder auch Lageberichte enthalten, betragen die Aufbewahrungsfristen grundsätzlich zehn Jahre.

Fernmeldegeheimnis bei privater Nutzung

Viele Unternehmen möchten zur Steigerung des Betriebsklimas und der Motivation ihrer Mitarbeiter die private Nutzung der Telekommunikation ihren Mitarbeitern erlauben. Eine zentrale Archivierungslösung aller unternehmenseigenen E-Mails stößt dann auf Vorbehalte, wenn das jeweilige Unternehmen den Mitarbeitern auch die Nutzung des E-Mailpostfachs zu privaten Zwecken gestattet. Stellen Sie nämlich den betriebseigenen Internetzugang für betriebsfremde (also private) Zwecke zur Verfügung, wird das Unternehmen in diesem Fall geschäftsmäßiger Anbieter von Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes (TKG) und hat das Fernmeldegeheimnis gemäß § 88 TKG zu beachten:

1. Diensteanbieter im Sinne der § 88 Abs. 1 S.1 i.V.m. § 3 Nr.6 TKG ist jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt: Zwar erscheint es auf den ersten Blick befremdend, dass der Arbeitgeber ein Diensteanbieter in diesem Sinne sein soll. Denn er tritt nicht auf dem Telekommunikationsmarkt auf und der Arbeitnehmer scheint kein außenstehender Dritter zu sein. Trotz dieser auch unter Juristen vertretenen Ansicht geht die herrschende Meinung davon aus, dass das TKG hier einschlägig ist, da unter anderem eines der Hauptziele des Gesetzes die Wahrung des Fernmeldegeheimnisses ist. Auch kommt es nicht darauf an, ob mit dem Angebot Gewinn erzielt werden soll oder nicht.

2. Dritter ist der, der nicht als Diensteanbieter zählt: Insofern ist bei dem Angestellten zu unterscheiden. Hinsichtlich der privaten E-Mails ist er Dritter, hinsichtlich der geschäftlichen E-Mails jedoch nicht. Denn bei geschäftlicher Nutzung ist der Arbeitnehmer Handlungsgehilfe des Arbeitgebers und damit nicht Dritter.

3. Eine Speicherung des Inhalts der privaten E-Mails ist in jedem Falle unzulässig. Denn nur, wenn es für die geschäftsmäßige Erbringung der Telekommunikationsdienstleistung nach § 88 Abs. 3 S. 1 und 2 TKG erforderlich ist, kann eine Ausnahme zugelassen werden. Dies kann aber nicht mit dem Inhalt der E-Mail zusammenhängen. Selbst die Absicht zur Missbrauchskontrolle (etwa Verrat von Geschäftsgeheimnissen oder Begehung einer Straftat) rechtfertigt keine umfassende Archivierung.

4. Pflichtenkollision für den Arbeitgeber: Damit verstößt der Arbeitgeber bei einer Archivierung gegen das Fernmeldegeheimnis. Dies kann zu einer Strafbarkeit wegen Verletzung des Fernmeldegeheimnisses oder wegen Ausspähens von Daten (§§ 206, 202a Strafgesetzbuch) führen. Darüber hinaus können zivilrechtliche Schadensersatzansprüche entstehen. In dieser Konstellation ergibt sich eine Pflichtenkollision des Arbeitgebers. Er verletzt entweder die Straftatbestände nach §§ 206, 202a StGB (Datenschutz, Fernmeldegeheimnis) oder nach 238b StGB (Buchführungspflicht).

Im zweiten Teil stellen wir den Konflikt mit dem Datenschutzrecht dar. Anschließend gehen wir darauf ein, wie Sie die Konflikte mit dem Fernmeldegeheimnis und dem Datenschutz lösen. *(dr)*

Rechtsassessor Patrick Prestel und RA Max-Lion Keller LL.M. befassen sich mit IT-Recht in der Kanzlei Keller-Stoltenhoff, Keller, Münch (www.it-recht-kanzlei.de).

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


Quelle: RRF - Fotolia.com

Informationspflichten bei Datenlecks

Richtiges Verhalten bei Datenpannen

von Giovanni Brugugnone

Ob Datenleck, Datenpanne oder Datendiebstahl: Während die IT-Abteilung ins Rotieren kommt, um schnellstmöglich die undichte Stelle zu schließen, steht das Unternehmen bereits vor der unangenehmen Frage, ob es den Zwischenfall melden muss. Schließlich hat der Gesetzgeber gerade aufgrund der Vielzahl solcher Datenschutzskandale das "Gesetz zur Änderung datenschutzrechtlicher Vorschriften" erlassen. Das Bundesdatenschutzgesetz ist dabei eindeutig, was Informationspflichten angeht – und droht Unternehmen, die diesen nicht nachkommen, saftige Strafen an.

Im Rahmen des geänderten Bundesdatenschutzgesetzes (BDSG) sind nicht-öffentliche Stellen ebenso wie öffentliche Wettbewerbsunternehmen gemäß § 42a BDSG in bestimmten Fällen dazu verpflichtet, Betroffene und die jeweils zuständige Aufsichtsbehörde zu informieren, wenn etwa durch Datenpannen oder Datenlecks Dritte unrechtmäßig Kenntnis von personenbezogenen Daten erlangt haben. Da es also nicht nur um die Meldung an die zuständige Aufsichtsbehörde, sondern möglicherweise auch um die Informationspflicht gegenüber tausenden von Kunden geht, ist ein gehöriger Imageschaden zu befürchten. Andererseits: Wird der gesetzlichen Verpflichtung nicht oder nicht rechtzeitig nachgekommen, so kann dies gemäß § 43 Abs. 2 Nr. 7, Abs. 3 BDSG ein Bußgeld von bis zu 300.000 Euro zur Folge haben. Es steht also einiges auf dem Spiel. Besonders wichtig ist daher die Frage, in welchen Fällen § 42a BDSG überhaupt zum Tragen kommt. Und, sollte dies der Fall sein, wann und in welcher Form Aufsichtsbehörden und Betroffene dann zu informieren sind.

Datenschutz sensibler, personenbezogener Daten durch § 42a BDSG

Die Informationspflicht aus § 42a BDSG wird nur durch solche Arten personenbezogener Daten ausgelöst, die vom Gesetzgeber als besonders sensibel angesehen werden (sogenannte Risikodaten). Diese sind in § 42a BDSG abschließend aufgezählt:

- Die in § 3 Abs. 9 BDSG angegebenen besondere Arten personenbezogener Daten, also unter anderem Angaben über die ethnische Herkunft, politische Meinungen, religiöse Überzeugungen und Gesundheit.
- Personenbezogene Daten, die einem Berufsgeheimnis gemäß § 203 StGB unterliegen, wie beispielsweise bei Ärzten oder Rechtsanwälten.
- Personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder einen diesbezüglichen Verdacht beziehen.
- Personenbezogene Daten zu Bank- und Kreditkartenkonten, wie beispielsweise Kreditkarten- und Kontonummer oder auch Kontoauszüge.

Weiterhin ist erforderlich, dass oben genannte Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind.

1. Unrechtmäßige Kenntnisnahme Dritter: Bei der Feststellung, dass Daten Dritten unrechtmäßig zur Kenntnis gelangt sind, bedarf es keiner absoluten Gewissheit. Vielmehr genügt die Wahrscheinlichkeit, dass es zu einer Kenntnisnahme Dritter gekommen ist, etwa durch einen Hackerangriff. Dies betrifft beispielsweise auch Fälle des Datenverlustes durch Abhandenkommen von Laptops oder sonstiger mobiler Datenträger. Bei bloßem Verdacht oder dem Gewahrsam Dritter an Datenträgern, ohne die Möglichkeit, hierauf zuzugreifen (beispielsweise aufgrund einer sicheren Verschlüsselung), ist eine Kenntnisnahme in diesem Sinne nicht anzunehmen. Jedoch ist die alleinige Kenntnisnahme durch Dritte allein nicht ausreichend, um eine Informationspflicht nach § 42a BDSG auszulösen.
2. Schwerwiegende Beeinträchtigung: Vielmehr ist zusätzlich erforderlich, dass die

Daten in einer Weise verwendet werden, die sich für die Betroffenen schädlich auswirkt. Hierbei genügt, dass schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Ob im Einzelfall eine schwerwiegende Beeinträchtigung anzunehmen ist, bestimmt sich unter anderem nach der Art der betroffenen Daten und den potenziellen Auswirkungen (mögliche Verwendungsszenarien) der unrechtmäßigen Kenntnisnahme Dritter (etwa finanzielle Schäden bei Kreditkartendaten). Hierbei handelt es sich um eine Prognoseentscheidung, in die gemäß § 4a Abs. 1 S. 1 BDSG der betriebliche Datenschutzbeauftragte einzubeziehen ist.

Betroffene und Aufsichtsbehörde informieren

Liegen die oben genannten Voraussetzungen vor, sind die Betroffenen und die zuständige Aufsichtsbehörde nach § 42a Satz 1 BDSG unverzüglich hierüber in Kenntnis zu setzen. Nach der Legaldefinition des § 121 BGB ist darunter ein Handeln ohne schuldhaftes Zögern zu verstehen. Betrachten wir die Vorschrift des § 42a BDSG etwas genauer, wird deutlich, dass die Benachrichtigung der Aufsichtsbehörde (§ 42a Satz 4 BDSG) gegenüber der Benachrichtigung der Betroffenen (§ 42a Satz 2, 3, 5 BDSG) sowohl inhaltlich umfangreicher als auch zeitlich früher erfolgen muss:

1. Benachrichtigung der Betroffenen: Hinsichtlich der Information der Betroffenen ist der Grundsatz der unverzüglichen Benachrichtigung dahingehend eingeschränkt, dass diese erst erfolgen muss, wenn angemessene Maßnahmen zur Sicherung der Daten ergriffen wurden und die Strafverfolgung nicht mehr gefährdet wird. Dies stellt klar, dass zunächst etwaige vorhandene Sicherheitslücken geschlossen werden können, um so einer erneuten Ausnutzung dieser vorzubeugen. Darüber hinaus sollen auch etwaige Ermittlungsarbeiten

Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Stellt eine nichtöffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),
2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder
4. personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. […]

§42a BDSG

der Strafverfolgungsbehörden nicht beeinträchtigt werden. Sofern ein kriminelles Handeln im Raum steht, ist die Benachrichtigung der Betroffenen mit den jeweiligen Strafverfolgungsbehörden abzustimmen.

2. Benachrichtigung der Aufsichtsbehörde: Die zuständige Aufsichtsbehörde (der Landesdatenschutzbeauftragte) ist hingegen nach Ermittlung und Prüfung der Voraussetzungen des § 42a BDSG ohne Einschränkung unverzüglich zu benachrichtigen.

Inhalt und Form der Information des Betroffenen

Den Betroffenen ist transparent offenzulegen, was genau sich ereignete und welche Gegenmaßnahmen zur Minderung möglicher weiterer nachteiliger Folgen empfohlen werden. Die zuständige Aufsichtsbehörde ist gemäß § 42a Satz 4 BDSG zusätzlich darüber zu informieren, welche möglichen nachteiligen Folgen durch die unrechtmäßige Kenntniserlangung drohen und welche Maßnahmen bereits hiergegen ergriffen wurden (etwa Sperren von Kredit- oder EC-Karten). Der Aufsichtsbehörde ist auch mitzuteilen, ob die Betroffenen informiert und welche konkreten Maßnahmen ihnen empfohlen wurden.

Grundsätzlich ist jeder Betroffene einzeln zu benachrichtigen, eine besondere Form sieht das Gesetz hier jedoch nicht vor. Es empfiehlt sich aus Gründen der Nachweisbarkeit die Information mittels verschlüsselter E-Mail oder auf postalischem Wege etwa durch ein Einschreiben mit Rückschein. Soweit die Einzelbenachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der Fälle, kann gemäß § 42a Satz 5 BDSG die Individualbenachrichtigung durch die Benachrichtigung der Öffentlichkeit ersetzt werden. Dies kann durch Anzeigen erfolgen, die mindestens eine halbe Seite umfassen und in mindestens zwei bundesweit erscheinenden Tageszeitungen veröffentlicht werden, oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. Auch die Aufsichtsbehörden sollten aus Gründen der Nachweisbarkeit zusätzlich zur im Einzelfall erforderlichen kurzfristigen telefonischen Information schriftlich informiert werden.

Keine Informationspflicht für Auftragsdatenverarbeiter

Gehen Daten des Auftraggebers als verantwortliche Stelle beim Auftragnehmer – also dem Auftragsdatenverarbeiter gemäß § 11 BDSG – verloren, stellt sich die Frage, ob auch diesen die Informationspflichten des § 42a BDSG treffen. Eine solche Pflicht gibt es allerdings nicht, denn § 11 Abs. 4 BDSG regelt abschließend die Pflichten des BDSG, die auf Auftragsdatenverarbeiter anwendbar sind. Insoweit hat jeder Auftraggeber durch entsprechende Ausgestaltung der Verträge zur Auftragsdatenverarbeitung dafür Sorge zu tragen, dass der Auftragsdatenverarbeiter bei Datenverlust den Auftraggeber unverzüglich informiert (§ 11 Abs. 2 Nr. 8 BDSG), damit dieser seinen eigenen Pflichten aus § 42a BDSG nachkommen kann.

Prävention durch Datenschutz-Compliance

Um mit der Informationspflicht einhergehende Imageschäden und Folgekosten zu vermeiden, sind die durch § 42a BDSG erfassten Daten sowie Geschäftsgeheimnisse im Allgemeinen (Stichwort Wirtschaftsspionage) durch geeignete Maßnahmen zu schützen. Denkbar sind hier im Rahmen einer umfassenden Datenschutz-Compliance Maßnahmen wie die Verschlüsselung von Daten und Datenträgern sowie die Beschränkung von Zugriffsrechten nach dem "Need-to-know-Prinzip".

Die umfassende Verschlüsselung von mobilen Datenträgern wie Laptops und USB-Sticks ist zudem sinnvoll und notwendig, um ausreichenden Schutz bei deren Verlust zu gewährleisten, indem der Zugriff Dritter und somit auch die Informationspflicht aus § 42a BDSG vermieden werden kann. Trotz aller gebotenen Vorsicht sollte aber auch der Aspekt der Datenverfügbarkeit nicht außer Acht gelassen werden. Daher sind auch bei mobilen Datenträgern regelmäßige Backups notwendig, um einmal erlangtes Know-how auf Dauer im Unternehmen zu halten.

Fazit

Für Unternehmen ist aufgrund der bei Datenpannen drohenden Kosten und Imageschäden ein gewisses Datenschutzniveau unabdingbar. Nicht zuletzt deshalb, da bei unvorhergesehenem Eintreten kurzfristige Gegenmaßnahmen die Kosten vorbeugender Maßnahmen regelmäßig bei weitem übersteigen (im Vergleich zu vorbeugenden Datenschutz-Maßnahmen verursachen nachträgliche Maßnahmen im Durchschnitt das Zweieinhalbfache an Kosten). In Abstimmung mit der IT-Abteilung, dem Datenschutzbeauftragten und dem Bereich Compliance sind insoweit etwaige Notfallszenarien zu beschreiben und geeignete Gegenmaßnahmen sowie Meldewege im Voraus festzulegen.

Für Datenpannen beziehungsweise § 42a BDSG relevante Vorfälle sollte eine zentrale Anlaufstelle installiert werden, die in der Lage ist, genau zu prüfen, ob überhaupt Informationspflichten ausgelöst wurden und wie gegebenenfalls Kontakt mit den Betroffenen, der Aufsichtsbehörde und erforderlichenfalls den Strafverfolgungsbehörden aufgenommen werden kann beziehungsweise muss. Hierbei kann ein externer Datenschutzexperte mit fundiertem juristischem und technischem Know-how wertvolle Hilfe leisten. Der Bereich Datenschutz-Compliance muss in der heutigen Zeit also zwingender Bestandteil der Unternehmens-Compliance sein und dessen Einhaltung sollte in jedem Unternehmen höchste Priorität genießen. *(dr)*

Giovanni Brugugnone ist Rechtsanwalt und Consultant Datenschutz und IT-Compliance bei der intersoft consulting services AG.

Webserver einrichten und administrieren

Die Inbetriebnahme und Wartung eines stabilen, performanten und sicheren Webservers ist alles andere als leicht. Und deshalb möchte der Autor hierzu seine langjährige Erfahrung aus dem Business-Umfeld weitergeben. Dabei schreitet Klaus M. Rodewig den Weg von der Wurzel zur Krone und lässt keinen Zweig aus. Beginnend mit der Begründung der Linux-Wahl (der Autor verwendet Ubuntu 10.4 LTS/Gentoo) und der Installation des Basissystems werden auch Fragen des Feintunings und der Dienste berücksichtigt (immerhin rund 130 Seiten von 490). Im zweiten Abschnitt wird das Hauptaugenmerk auf die Installation von Apache gelegt, wobei die Vorgehensweise sehr gut nachvollziehbar dargestellt ist. Sowohl mod_rewrite wie auch SSL und PHP finden Platz für ausreichende Erläuterung, bevor die Konfiguration der Serverdienste, Datenbanken (mySQL, PostgreSQL), Tomcat und Jabber aufgezeigt wird.

Alles Relevante für den laufenden Betrieb findet der Leser in den Folgekapiteln, begonnen mit Monitoring und der folgenden Optimierung. Der Autor zeigt die gängigen Verfahren wie SNMP, MRTG, Cacti, Nagios und die klassischen Statistiken auf. Auch wenn 35 Seiten für Nagios sinnvoll verwendet wurden, kann die Literatur natürlich keinen allumfassenden Einblick in das Tool geben – für die zum Thema passenden Zwecke sind die Beschreibungen allerdings sehr hilfreich. Beim Thema Hochverfügbarkeit reißt der Autor sowohl Xen als auch Linux-Cluster an, wenngleich er die derzeitigen Probleme der Virtualisierung mit Xen nicht verschweigt. Landscape für die webbasierende Administration von Serverlandschaften und das funktionierende Patch-Management bilden den Abschluss der Ausführungen.

Fazit: Egal, ob der Leser technisch begeisterter Anwender oder IT-Administrator im Webserver-Bereich ist: Die Inhalte dieses Buches halten die Versprechungen auf dem Klappentext ein – von der Installation über die Implementierung wichtiger Serverdienste bis hin zur Absicherung und Hochverfügbarkeit. Am Aufbau, der sauberen Darstellung und dem hohen Praxisbezug gibt es nichts auszusetzen. Minimales Manko: Ubuntu/Gentoo als Referenz-Distribution. Debian oder ein BSD-Derivat wären hier eher wünschenswert, wenngleich die distributionsspezifischen Unterschiede minimal sind. *Frank Große*

Autor:	Klaus M. Rodewig
Verlag:	Galileo
Preis:	39,90 Euro
ISBN:	978-3-8362-1708-8
Bewertung:	★★★★½

Web-Sicherheit

Wer bei vorliegendem Werk vermutet, dass sich alles nur um Apache & Co. dreht, der wird eines Besseren belehrt. Ausgehend von den Grundlagen der Informationssicherheit hat der Autor Sebastian Kübeck das Buch in drei Teile untergliedert. Im ersten Teil finden sich sowohl ein kurzer historischer Abriss wie auch die Erläuterung der Grundprinzipien der Sicherheit wieder. Ebenso eine Einführung in die Mechanismen der Authentifizierung und Autorisierung.

Einen Blick tiefer unter die Motorhaube wirft der zweite Abschnitt, der sich auf die häufigsten Schwachstellen, denen Webapplikationen unterworfen sind, fokussiert. Hier sind Kenntnisse von Progammier- oder Skriptsprachen hilfreich, denn der Leser wird mit Codeschnipseln sowohl von SQL als auch JavaScript und Java konfrontiert. Im Detail stellt Kübeck SQL-Injection- und Cross-Site-Scripting-Schwachstellen sowie Cross Site Request Forgery vor. Nicht zu vergessen die Klassiker Authentifizierungslücken, Autorisierungsfehler und Overflows, DoS-Schwachstellen sowie unsichere Konfigurationseinstellungen. Eine Produktschau darf der Leser hierbei nicht erwarten, vielmehr den Blick auf das Wesentliche und das Prinzip hinter den Schlagwörtern. Das systematische Vorgehen beim Testen und Beseitigen der Schwachstellen ist Bestandteil des letzten Teils des Buches. Programmierkenntnisse sind für das Verständnis nun unabdingbar.

Fazit: Das mit dem Untertitel "Wie Sie Ihre Webanwendungen sicher vor Angriffen schützen" betitelte Buch hat eine eher unglückliche Titelvergabe erfahren, wie sowohl der Blick ins Inhaltsverzeichnis als auch die Einleitung offenbart: "Dieses Buch versucht … dem Leser eine möglichst breitgefächerte Einführung in das Thema Informationssicherheit zu vermitteln, bevor das spezielle Thema der Absicherung von Webapplikationen behandelt wird." Eine treffende Beschreibung, die den Inhalt zwischen populärwissenschaftlichen Flair und technischer Betrachtung einbettet. Für den Einstieg in die Materie ist das Buch geeignet, wenngleich für den praktischen Teil Vorkenntnisse aus der Programmierung hilfreich sind. Administratoren, die mit der Materie ihr tägliches Brot verdienen, benötigen speziellere Literatur.

Frank Große

Autor:	Sebastian Kübeck
Verlag:	mitp
Preis:	29,95 Euro
ISBN:	978-3-8266-9024-2
Bewertung:	★★★½☆

www.apfeltalk.de

An Apple a Day…

Geräte mit einem Apfel als Logo genießen einen bislang nicht dagewesenen Hype. Egal ob iPhone, iPad oder MacBook – was Apple auf den Markt bringt, findet reißenden Absatz. Selbst endlos wirkende Schlangen vor den Apple Stores bei Produkteinführungen schrecken hartgesottene Fans nicht ab. Den Style-Faktor haben die Geräte aus Cupertino in jedem Fall auf ihrer Seite und auch an Bedienkonzepten zeigt sich Apple immer wieder innovativ. So verwundert es nicht, dass sich die Produkte auch immer mehr in Unternehmen wiederfinden. Ein iPhone hier, ein iPad dort – der Administrator ist dann gefragt, die Geräte einigermaßen sicher ins Netzwerk einzubinden. Um als Admin und auch als Apple-Fan auf dem Laufenden zu bleiben, bietet sich ein Blick auf die Seite www.apfeltalk.de an.

Die Macher der Seite, immerhin elf Apple-Begeisterte, versorgen die Besucher mit zahlreichen, tagesaktuellen News rund um Apple-Geräte und -Software. Dabei stehen auch durchaus "halboffizielle" Informationen online, zuletzt etwa über versteckte Firmware-Updates für MacBooks, die mehr RAM ermöglichen sollen. In den zugehörigen Kommentaren zeigt sich, dass es sich bei den Lesern durchaus um professionelle User handelt, die sich gerne auf technischem Niveau austauschen. Flame-Wars und nutzlose Kommentare sucht man auf Apfeltalk im Gegensatz zu manch anderen IT-Seiten quasi vergebens. So hat die Webseite nicht nur optisch viel zu bieten, sondern auch inhaltlich.

Reger Betrieb herrscht auch im zugehörigen Forum. Stolze 2,7 Millionen Beiträge haben es bislang ins Board geschafft, untergliedert in sieben Themenfelder und 47 Unterbereiche. Lange auf eine Antwort müssen Fragensteller so sicher nicht warten – sie müssen sich irgendwann vielmehr durch eine Vielzahl an Antworten wühlen. Hier scheint die deutschsprachige Apple-Fangemeinde zuhause zu sein. Zwei Moderatorinnen und drei Moderatoren sorgen für Ordnung, dürften jedoch angesichts der qualitativ hochwertigen Posts kaum den digitalen Zeigefinger erheben müssen. Für dauerhafte und fundierte Beiträge stellt Apfeltalk seinen Usern außerdem ein – zugegebenermaßen noch überschaubares – Wiki zur Verfügung. Immerhin 76 Begriffserklärungen finden sich dort bereits. Alles in allem für jeden Apple-Fan definitiv ein Muss. *(dr)*

Heimstatt für die Apple-Community: apfeltalk.de

Unser Internetauftritt versorgt Sie jede Woche mit einem neuen interessanten Fachartikel. Diesen Monat erfahren Sie auf unserer Webseite mehr zu folgenden Themen:

Datensicherung im Umbruch

Immer mehr Daten auf immer weniger Plattenlaufwerken verursachen oft massive Backup- und Restore-Probleme. In unserem Fachbeitrag im Web erläutern wir die Bandbreite verschiedener Backup-Ansätze, deren Vor- und Nachteile und bevorzugten Einsatzgebiete. Das Spektrum umfasst dabei unter anderem B2Tape, B2D mit Deduplizierung und Block Level Incremental Forever-Verfahren bis hin zu Snapshot-basiertem Backup.
www.it-administrator.de/themen/storage/fachartikel/92981.html

Mehr-Stufen-Konzepte für Backup & Recovery

Weiterentwicklungen bei der Datensicherung wie Virtualisierung verändern die Anforderungen für IT-Verantwortliche, die eine Strategie entwickeln und sie mit dem richtigen Technologie-Mix umsetzen müssen: Ist LTO-5 im Sinne der Energieeffizienz zeitgemäß? Wann lohnt sich eine Tape Library? Unser Online-Artikel beleuchtet, welche Kriterien Sie bei der Wahl von Tape, Tape Automation oder Disk-to-Disk überdenken müssen.
www.it-administrator.de/themen/storage/fachartikel/92982.html

Anwenderbericht: Open Source im Call Center

Als der Wartungsvertrag der alten Call Center-Lösung auslief, haben sich die IT-Verantwortlichen bei Toshiba Europe kurzerhand für eine Open Source-Alternative entschieden. In unserem Anwenderbericht im Web beleuchten wir, welche Hürden bei der Umstellung zu meistern waren und wie das Unternehmen neben Kosteneinsparungen auch die Servicequalität verbessern konnte.
www.it-administrator.de/themen/netzwerkmanagement/fachartikel/92983.html

Kostensenkung durch sparsame DRAM-Module

Der Einsatz von Virtualisierung bedeutet, dass pro Host wesentlich mehr DRAMs erforderlich sind. Um trotzdem den Energieverbrauch zu senken, sollten IT-Verantwortliche gerade bei Neuanschaffungen über den Einsatz moderner DRAMs mit kleineren Halbleiter-Geometrien nachdenken. In unserem Online-Beitrag berichten wir von einem Test, der das Einsparpotential von 30nm-Class DRAM-Modulen belegt.
www.it-administrator.de/themen/server_client/fachartikel/92984.html

Besser informiert: Fachartikel auf der Website des IT-Administrator

»Fordernde Projekte bereichern den Arbeitsalltag«

Jochen Springer (31) ist als Netzwerkadministrator für die IT-Infrastruktur von BRZ verantwortlich. Das Unternehmen ist mit über 450 Mitarbeitern und 19 Standorten in ganz Deutschland als IT- und Organisationsspezialist für die Baubranche tätig. Die Nürnberger unterstützen Bauunternehmen dabei, ihre Arbeitsprozesse mit speziellen IT-Lösungen effizienter abzuwickeln und ihr Unternehmen sicher zu steuern.

Warum sind Sie IT-Administrator geworden?

Mit der IT habe ich mich sehr früh intensiver befasst und hatte irgendwann das Gefühl, dazu "berufen" zu sein, in diesem Bereich zu arbeiten. Der berufliche Umstieg in die IT war quasi programmiert.

Wie finden Sie den nötigen Ausgleich zu Ihrer Arbeit?

Dabei helfen mir Familie und Hobbys.

Inwieweit hat Ihr Beruf Ihre Hobbys geprägt?

Früher schon mehr als heute, denn da gehörte ich zu den Gamern und Hardware-Bastlern. Durch die Familie haben sich die Prioritäten inzwischen verschoben.

Wie stellen Sie sich die private IT in zehn Jahren vor?

Der Trend geht sicher hin zu einer weitgehenden Vernetzung aller im privaten Umfeld genutzten Gerätschaften. Hinzu kommt eine ultra-mobile Steuerung.

Welche Aspekte Ihres Berufs machen Ihnen am meisten Spaß – und welche weniger?

Mir gefallen der Abwechslungsreichtum des Berufs und der Umgang mit kognitiv fordernden Projekten. Als bereichernd empfinde ich auch den fachlich-intellektuellen Austausch mit Kollegen. Weniger Freude machen technisch bedingte Rückschläge sowie langwierige Entscheidungsprozesse.

Haben Sie aufgrund von Fehlern beim Sicherungs- oder Wiederherstellungsvorgang schon einmal Daten verloren?

Glücklicherweise sind wir davon bisher verschont geblieben und haben in dieser Hinsicht keine Probleme.

Welche Backup-Wege setzen Sie im Unternehmen ein?

Wir nutzen Disk2Disk, Tape und VTL.

Auf welche Software greifen Sie beim Backup zurück?

Wir setzen Symantec Backup Exec, Windows Server Sicherung sowie Snapshot von VMware und Acronis True Image ein.

Nutzen Sie beim Backup auch Deduplizierung?

Wir verwenden in unserem Rechenzentrum für die Daten-Deduplizierung Data Domain von EMC.

Wie sehen in Ihrem Unternehmen die Routinen aus, wenn es um das Proben der Wiederherstellung von Daten geht?

Wir machen regelmäßige Testwiederherstellungen zufällig gewählter Systeme, um die gesamte Bandbreite unserer Infrastruktur zu überprüfen.

Hatten Sie in jüngster Zeit aufgrund gewachsener Datenmengen Probleme mit Ihrem Backup-Fenster?

Nein, bei uns läuft in dieser Beziehung bisher alles rund.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Demnächst steht die Domänenintegration einer gewachsenen externen Gesamtstruktur auf der Prioritätenliste ganz oben.

Mit welcher aktuellen IT-Technologie würden Sie gern einmal arbeiten?

Mich würde es sowohl beruflich als auch privat reizen, mit Augmented Reality, also der computergestützten Erweiterung der Realitätswahrnehmung, zu arbeiten. Insbesondere in Verbindung mit der computergestützten Bewegungssteuerung, die als Kinect bezeichnet wird, könnten sich daraus interessante Aspekte ergeben.

Welches IT-Problem oder Produkt ließ Sie in letzter Zeit verzweifeln und warum?

IT-Probleme bringen mich nicht zum Verzweifeln. Wenn keine Lösung in Sicht ist, muss man sich eben neu entscheiden und den Lösungsansatz überdenken.

Geburtstag: 22. August 1979
Familienstand: verheiratet, zwei Kinder
Hobbys: Pen&Paper Rollenspiele, Mittelaltermärkte, Technik, Motorrad

Jochen Springer, IT-Administrator

Ausbildung

- Speditionskaufmann
- Quereinstieg in die IT
- heute Netzwerkadministrator

Betreute Infrastruktur

- Rechenzentrum mit einer Vielzahl physikalischer und virtueller Server,
- heterogene Betriebssystemstrukturen mit LINUX und Microsoft Windows, wobei Windows die Szene eindeutig dominiert,
- klassische Office-Anwendungen sowie Speziallösungen für die Baubranche
- Nagios als Netzwerk- und Systemmanagement

Wenn Sie sich ein Tool wünschen könnten, was würde dieses leisten?

Das würde die lästigen, aber notwendigen Schreib- und Dokumentationsarbeiten automatisch erledigen.

Warum würden Sie einem jungen Menschen raten, Administrator zu werden?

Je stärker die Vernetzung, desto größer wird unsere Verantwortung als IT-Administrator. Wer davor nicht zurückschreckt und zudem technikaffin ist, sollte diesen abwechslungsreichen Beruf ergreifen.

Welches ist der dümmste Anwenderfehler, der Ihnen untergekommen ist?

Wirklich dumme Fehler machen nur Administratoren. Die Fehler der Anwender resultieren in der Regel aus der Unbedarftheit im Umgang mit der Technik.

Das Interview führte Petra Adamik.

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

Was haben Sie zu sagen?

Die Ausgabe 5/11 erscheint am 3. Mai 2011

Schwerpunktthema:

Server-based Computing

Im Test: Xen Desktop 5

Im Test: 2x Application Server

Workshop: Remote Desktop Gateway unter Windows 2008 nutzen

Workshop: Provisionieren von Windows 7 mit Sysprep

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

Die Ausgabe im **Juni** hat sich zum Schwerpunkt das Thema **Virtualisierungs-Management und Automatisierung** gesetzt. In unseren Tests werfen wir unter anderem einen Blick auf das Veeam Essentials Bundle. In den Workshops lesen Sie, wie Sie Hyper-V über die PowerShell verwalten und Ihre VMware-Umgebung richtig überwachen.

Als Schwerpunkt im **Juli** folgt dann das Thema **Hochverfügbarkeit**.

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

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

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

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

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

Autoren dieser Ausgabe
Petra Adamik, Thomas Bär, Giovanni Brugugnone, Nicolas Ehrschwendner, Sascha Giebelhausen, Thomas Gronenwald, Frank Große, Mathias Hein, Jürgen Heyer, Thomas Joos, Max-Lion Keller, Christian Knermann, Robert Lindermeier, Sandro Luciforo, Patrick Prestel, Ulf B. Simon-Weidner

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

Es gilt die Anzeigenpreisliste Nr. 8 vom 01.01.2011

LAC/2008

Produktion / Anzeigendisposition
Lightrays: Andreas Skrzypnik, Gero Wortmann
dispo@it-administrator.de
Tel.: 089/4445408-88
Fax: 089/4445408-99

Druck
Konrad Triltsch
Print und digitale Medien GmbH
Johannes-Gutenberg-Straße 1-3
97199 Ochsenfurt-Hohestadt

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

Abo- und Leserservice
Vertriebsunion Meynen GmbH & Co. KG
Stephan Orgel
Große Hub 10
65344 Eltville
leserservice@it-administrator.de
Tel.: 06123/9238-251
Fax: 06123/9238-252

Erscheinungsweise
monatlich

Bezugspreise
Einzelheftpreis: € 12,60
Jahresabonnement Inland: € 135,-
Studentenabonnement Inland: € 67,50
Jahresabonnement Ausland: € 150,-
Studentenabonnement Ausland: € 75,-
Jahresabonnement Inland mit Jahres-CD: € 144,84
Studentenabonnement Inland mit Jahres-CD: € 77,34
Jahresabonnement Ausland mit Jahres-CD: € 159,84
Studentenabonnement Ausland mit Jahres-CD: € 84,84
All-Inclusive Jahresabo (mit Sonderheften + Jahres-CD) Inland: € 184,64
All-Inclusive Studentenabo Inland: € 117,14
All-Inclusive Jahresabo Ausland: € 199,64
All-Inclusive Studentenabo Ausland: € 124,64
E-Paper-Einzelheftpreis: € 9,45
E-Paper-Jahresabonnement: € 99,-
E-Paper-Studentenabonnement: € 49,50
Jahresabonnement-Kombi mit E-Paper: € 168,-
(Studentenabonnements nur gegen Vorlage einer gültigen Immatrikulationsbescheinigung)

Alle Preise verstehen sich inklusive der gesetzlichen Mehrwertsteuer sowie inklusive Versandkosten.

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
80802 München
Tel.: 089/4445408-0
Fax: 089/4445408-99
(zugleich Anschrift aller Verantwortlichen)
Web: www.heinemann-verlag.de
E-Mail: info@heinemann-verlag.de
Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

Geschäftsführung / Anteilsverhältnisse
Geschäftsführende Gesellschafter zu gleichen Teilen sind Anne Kathrin und Matthias Heinemann.

ISSN
1614-2888

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

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

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

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

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

INSERENTENVERZEICHNIS

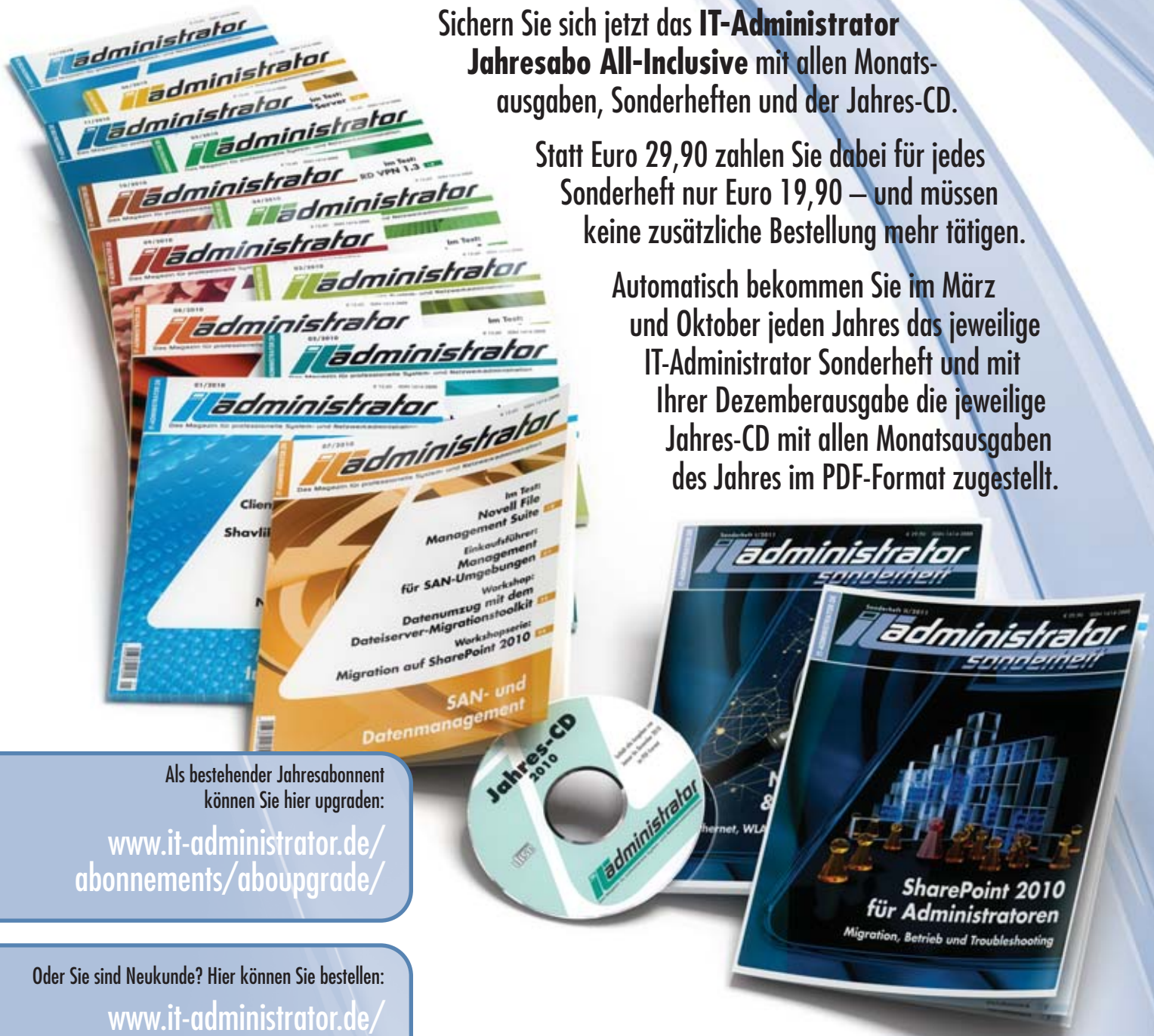
Die Ausgabe enthält eine Gesamtbeilage der Firma galileo computing.

Das IT-Administrator Komplettprogramm!!!

Sichern Sie sich jetzt das **IT-Administrator Jahresabo All-Inclusive** mit allen Monatsausgaben, Sonderheften und der Jahres-CD.

Statt Euro 29,90 zahlen Sie dabei für jedes Sonderheft nur Euro 19,90 – und müssen keine zusätzliche Bestellung mehr tätigen.

Automatisch bekommen Sie im März und Oktober jeden Jahres das jeweilige IT-Administrator Sonderheft und mit Ihrer Dezemberausgabe die jeweilige Jahres-CD mit allen Monatsausgaben des Jahres im PDF-Format zugestellt.



Als bestehender Jahresabonnent können Sie hier upgraden:

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

Oder Sie sind Neukunde? Hier können Sie bestellen:

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

www.it-administrator.de

Heinemann Verlag
Im Dialog mit Spezialisten.

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München
Tel: 0049-89-4445408-0
Fax: 0049-89-4445408-99
info@heinemann-verlag.de

Vertrieb, Abo- und Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville
Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de

Intelligente Technologien für einen smarten Planeten

Was bedeuten 1,3 Millionen Transaktionen pro Sekunde für dieses Auto?

Sie bedeuten, dass man den möglichen Käufer für dieses Auto ziemlich genau beschreiben kann. Acxiom, einer der weltweit führenden Anbieter von Marketing-Dienstleistungen und -Technologie, arbeitet mit IBM zusammen, um für Unternehmen aus über 7.000 Datenbanken detaillierte Informationen über die Wünsche ihrer Kunden zu gewinnen. Damit unterstützt Acxiom neun der zehn größten Autohersteller sowie Unternehmen aus allen wichtigen Industriezweigen. Die Grundlage dafür liefert IBM System x® mit Intel® Xeon® Prozessoren. Damit kann Acxiom 9.360 unterschiedliche Systeme auf nur 264 eX5 Systeme konsolidieren – und zwar ohne Leistungseinbußen. Ein smartes Unternehmen braucht intelligente Software, Systeme und Services.

Machen wir den Planeten ein bisschen smarter. **ibm.com**/car/de

IBM®

Hier werden Daten sichtbar gemacht, die die Vorlieben verschiedener Personengruppen für bestimmte Automobiltypen zeigen.

intel® Xeon® inside™

Leistungsstark. Intelligent.