

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

**Im Test:
DataCore SANmelody** 13

**Im Test:
VMware vSphere 4.0** 19

**Einkaufsführer:
NAS-Lösungen im Überblick** 38

**Workshopserie:
Neuerungen im Microsoft Forefront
Threat Management Gateway (1)** 47

Storage

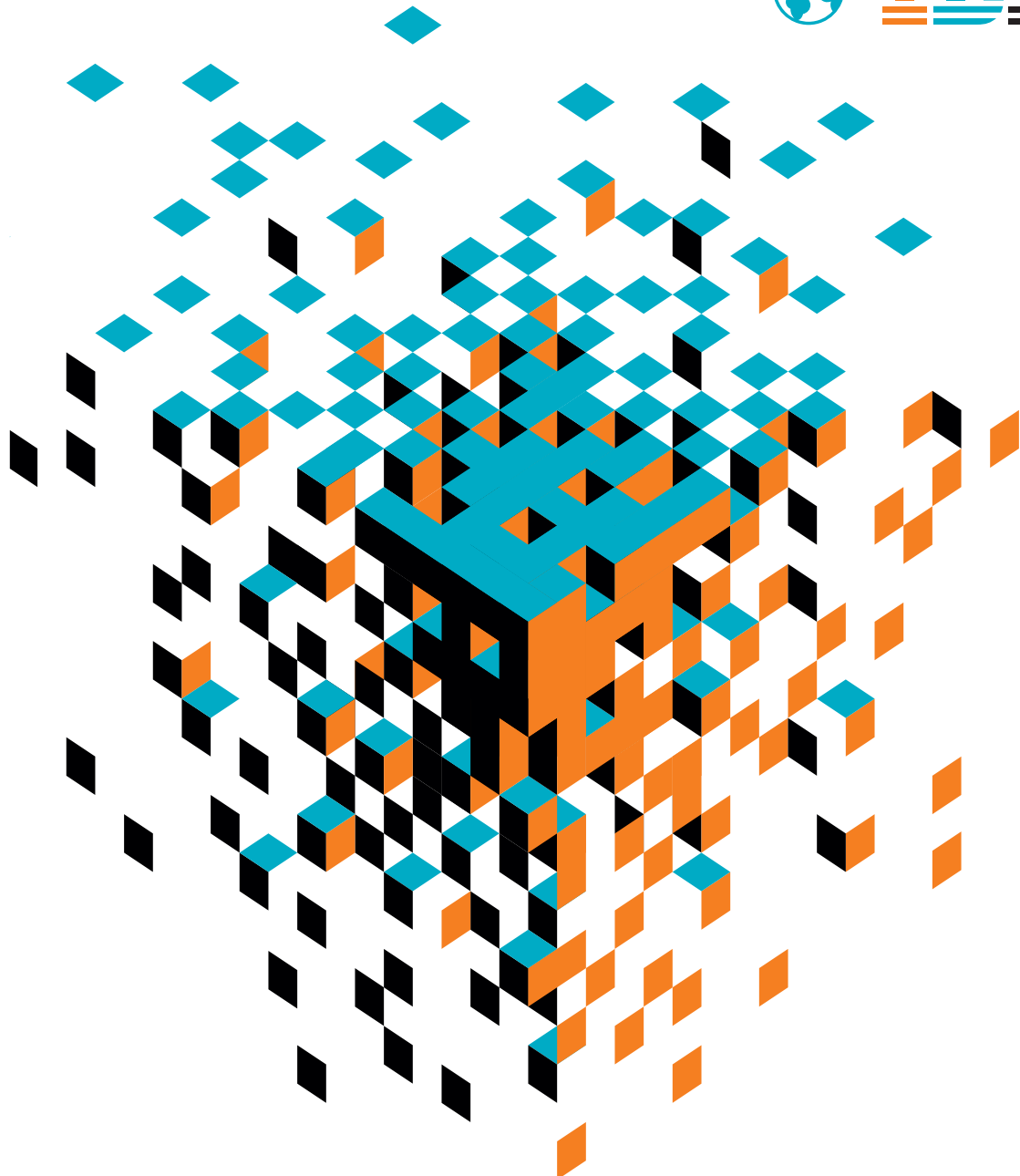


Service-Management, zu Ende gedacht.

Die Fähigkeit, Dinge smart zu gestalten – sie digital zu erfassen, zu vernetzen und zu intelligenten Systemen zu verbinden –, macht es möglich, heute so verschiedene Infrastrukturen wie Stromnetze, Bahnstrecken oder Fertigungsstraßen zu umfassen. Aber wie verzahnt man die Infrastrukturen von Business und IT so, dass Ihre Kunden die Service-Qualität bekommen, die sie erwarten – und Ihr Unternehmen die Flexibilität, die Sie brauchen? Der Ansatz von IBM zum Service-Management hilft Ihnen, Services transparenter zu gestalten, sie besser zu kontrollieren und stärker zu automatisieren. Das Ergebnis: eine dynamischere Infrastruktur, in der sich neue Services leicht ergänzen und vorhandene ebenso leicht modifizieren lassen. Alle 20 Top-Telekommunikationsanbieter und 7 der 10 größten Automobilhersteller bieten mit Hilfe von IBM flexible Services weit über ihr Rechenzentrum hinaus.

Smarte Unternehmen brauchen intelligente Software, Systeme und Services.

Also: Machen wir den Planeten ein bisschen smarter. Wie, erfahren Sie unter ibm.com/management/de



Gesetzlich geschützte Daten

Liebe Leser,

seit dem 1. September dieses Jahres sieht der Daten-GAU in etwa so aus: IT-Abteilungsleiter Horst F. von der Immerkorrekt GmbH kommt am ersten Tag nach seinem Urlaub morgens in sein Büro, seine beiden favorisierten Tageszeitungen unter dem Arm. Viel Zeit zum Lesen der beiden Blätter hat er heute nicht, denn die Geschäftsführung hat ihn schon für 9 Uhr zu einem "dringenden Termin" geladen. Also verliert Horst F. keine Zeit und blättert hastig zum Sportteil der Zeitung, doch an Seite 5 bleibt er hängen. Dort prangt eine halbseitige Anzeige seines Unternehmens. Doch die Freude über den offenbar gewaltigen Werbefeldzug seines Arbeitgebers hält nur bis zur nächsten Sekunde, als Horst F. lesen muss: "Die Immerkorrekt GmbH weist darauf hin, dass am 14. September 2009 circa 500.000 Kundendatensätze Dritten unrechtmäßig zur Kenntnis gelangt sind. Wir entschuldigen uns dafür bei unseren Kunden".



Am nächsten Tag hatte Horst F. dann wieder viel Zeit zum Zeitung lesen, vornehmlich die Stellenanzeigen.

Zu einem derartigen Szenario kann es dank des neu im Bundesdatenschutzgesetz (BDSG) eingeführten Paragraphen 42a kommen. Diese, als Reaktion auf die Skandale rund um den "Verlust" von Kundendaten eingeführte Regelung, nimmt Unternehmen in die Pflicht, sobald personenbezogene Daten in die Hände Unbefugter gelangen. 42a legt fest, dass in einem solchen Falle jeder Betroffene vom Unternehmen informiert werden muss oder – falls dies einen "unverhältnismäßigen Aufwand erfordert" – in zwei überregionalen Tageszeitungen per Anzeige publik gemacht wird. Schlechtere PR für ein Unternehmen dürfte es kaum geben. Und für eine IT-Abteilung erst Recht nicht.

Einerseits sollten gut geschulte Kollegen und eine Handvoll technischer Maßnahmen wie Verschlüsselung oder Data Leakage Prevention die Gefahr eines solchen Vorfalls minimieren. Doch wer sich über den Einsatz von Cloud-Computing – wie etwa mit VMware vSphere 4 (im Test ab Seite 19) – Gedanken macht, dürfte nun eine Sorge mehr haben. Denn besonders wenn es um den Schutz von sensiblen Daten geht, ist es unumgänglich zu wissen, wo diese gespeichert werden und wer darauf zugreifen kann.

Viel Vergnügen beim Lesen, Ihr

John Pardey
 Chefredakteur IT-Administrator

1,5 Millionen geklante Datensätze Identitätsdiebstahl Datenklau bei Monster.c Kriminelle Machenschaften Mit **itWatch** wäre das nicht passiert!

Risiken am Endpoint managen und beherrschen:

Ermitteln Sie **vollautomatisch alle Risiken am Endpoint**: Genutzte Ports, Devices, Anwendungen, Austausch kritischer Dateien, verbundene Netze etc. Definieren Sie auf dieser Basis Ihre **individuelle Sicherheitskultur** mit **Freiräumen**, Verboten und **Systems Management Zielen** - ganz ohne Aufwand.

CITRIX®/Terminalserver:

Schützen Sie Ihre **CITRIX-** und **Terminal-Server** vor allen unerwünschten Daten, dem **unerlaubten Datenabfluss (Data Loss)** und vor nicht erwünschten **mobilen Anwendungen (portable apps)**. Der Schutz basiert nicht nur auf Dateinamen, sondern geht über den **Content Filter** und die **Pattern Prüfung** tief in die Dateien hinein.

Data Leakage Prevention mit itWatch:

Verschlüsselung kann mit persönlichen Schlüsseln oder einem Firmenschlüssel erzwungen werden. Sie sind compliant und Ihre **Daten bleiben im Unternehmen**. Firmenschlüssel sind nur auf Firmenrechnern verwendbar. **Datenlecks werden geschlossen** - erlaubte Dateibewegungen protokolliert.

Liechtenstein muss nicht sein

In Krisenzeiten nimmt das Risiko des Datendiebstahls zu. Unzufriedene Mitarbeiter erhöhen ihren Marktwert durch "mitgenommene" Daten.

ApplicationWatch:

Mit **ApplicationWatch** bestimmen Sie, **wer welche Programme nutzen darf**. Als **weltweite Alleinstellung** kontrollieren Sie zusätzlich den Zugriff der Anwendungen auf alle Dateien - lesend oder schreibend - unabhängig von den Nutzerrechten, nach Namen und Inhalt.

itWatch



GmbH

Endpoint Security, die mitdenkt

+49 89 620 30 100 - www.itWatch.de - Info@itWatch.de

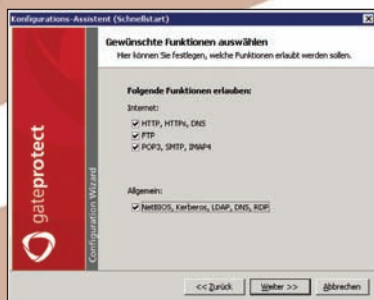
Besuchen Sie uns: **Platin-Sponsor** auf der **it-sa** in Nürnberg, **13.-15.10.**, oder in: **Leipzig, Stuttgart, Wien, Dubai, Athen, München ...**

INHALT

IT-Administrator – Ausgabe Oktober 2009

Storage

Im Test: gateProtect GPO-125



Das größte Sicherheitsrisiko heutiger Firewall-Systeme besteht darin, dass zur effektiven Abwehr von Angriffen immer komplexere Sicherheitsfunktionen integriert sein müssen. Das führt zwangsläufig dazu, dass die Konfiguration der Schutzsysteme kompliziert und unübersichtlich wird. Daraus folgt meist eine fehlerhafte Konfiguration, die aus

dem Sicherheitssystem oft ein offenes Scheunentor macht. gateProtect will mit dem eigens entwickelten eGUI – dem ergonomic graphic user interface – die Bedienbarkeit wieder in den Mittelpunkt stellen. Ob das gelungen ist, haben wir in einem Test für Sie herausgefunden.

Seite 33

Konzepte für Storage-Umgebungen

Das Bilden eigener Speichernetzwerke im Unternehmen gilt gemeinhin als eine vielversprechende strategische Entscheidung – lassen sich doch sowohl die Leistung erhöhen als auch mittelfristig die Kosten senken. Doch was genau gilt es zu bedenken und zu tun, um diesem Ziel tatsächlich gerecht zu werden? Nur mit den richtigen Strategien und Einstellungen wird das Speichersystem schneller. IT-Administrator zeigt Ihnen in diesem Beitrag, worauf es bei Storage-Umgebungen ankommt.



Seite 43



Server- und
Systemmanagement



Clientmanagement



Storage



Sicherheit



Messaging

Themenübersicht



Virtualisierung



Netzwerkmanagement



Job/Weiterbildung



Recht

AKTUELL

- 06 News**
- 10 ITANet aktuell:**
IT-Administrator-Workshop am 29. Oktober 2009 in Böblingen
Klarheit im virtuellen Dschungel
- 11 IT-Administrator vor Ort:** ice:2009, 22. August, Lingen/Ems
Pflichttermin für Admins

PRODUKTE

- 13 Im Test:** DataCore SANmelody
SAN im Eigenbau
- 19 Im Test:** VMware vSphere 4.0
Wolkiges Betriebssystem
- 26 Im Test:** Synology DS209+II NAS-System
Kompakter Netzwerkspeicher
- 33 Im Test:** gateProtect GPO-125
Sicherheit per Drag-and-Drop
- 38 Einkaufsführer:** NAS-Lösungen im Überblick
Brücken zwischen den Inseln

PRAXIS

- 43 Systeme:** Konzepte für Storage-Umgebungen
Viele Wege zum optimalen Speicherplatz
- 47 Systeme:**
Neuerungen im Microsoft Forefront Threat Management Gateway (1)
Neue Mauern für den Schutzwall
- 52 Workshopserie:**
Virtual Desktop Infrastructure mit VMware View einrichten (4)
Anwendungen virtualisiert
- 56 Workshopserie:** Drucken unter Linux (2): CUPS
Einfach drucken
- 61 Workshopserie:** Active Directory-Replikation meistern (3)
Alle Standorte im Griff
- 66 Workshopserie:**
Anwendungsvirtualisierung mit Microsoft App-V 4.5 (2)
Dicke Applikationen durch dünne Drähte
- 71 Workshop:** Tipps zur PowerShell 2
Active Directory-Verwaltung mit der PowerShell

Tipps, Tricks & Tools

WISSEN

- 76 Know-how:** Fibre Channel over Ethernet
Symbiose für optimale Speichereffizienz
- 79 Buchbesprechung**
"Video-Training VMware vSphere 4" und "Head First Networking"

Website & Fachartikel online

RUBRIKEN

- 03 Editorial**
- 05 Inhalt**
- 69 Seminarmarkt**
- 81 Das letzte Wort**
- 82 Vorschau, Impressum, Inserentenverzeichnis**

Tunnel soweit das Auge reicht

Die Produktpalette von **Lancom** wächst um zwei **VPN-Gateways**: Mit den Modellen **7100 VPN** und **9100 VPN** sind in der Grundausstattung 100 beziehungsweise 200 gleichzeitige VPN-Verbindungen möglich. Beide Geräte verfügen über vier GBit-Ethernet-Ports, einen USB-2.0- und einen ISDN-Basis-Anschluss. Ein LCD-Display auf der Vorderseite des einen Höheneinheit messenden 19 Zoll-Gehäuses gibt Auskunft über den Gerätestatus. Die integrierte Firewall mit Sicherheitsfunktionen wie Stateful-Inspection und Denial-of-Service-Protection wird durch dynamisches Bandbreitenmanagement sowie Backup-, High-Availability- und Redundanzfunktionen über ISDN und VRRP ergänzt. VPN-Unterstützung nach IPSec-Standard mit 3-DES- oder AES-Verschlüsselung, inte-

grierter Hardwarebeschleunigung und der Unterstützung digitaler Zertifikate soll für die nötige Sicherheit bei der Anbindung von Filialen und Home Offices sorgen. Die kostenlos mitgelieferten Managementsysteme LANconfig und LANmonitor bieten neben der Fernwartung kompletter Installationen und Setup-Assistenten auch eine vollständige Echtzeitüberwachung und -Protokollierung. Das Modell 9100VPN ist ab sofort zum Preis von rund 4.000 Euro erhältlich. Die optional erhältliche Aufrüstung auf 500 oder 1.000 gleichzeitige VPN-Kanäle bietet der Hersteller für 1.000 respektive 1.800 Euro an. Das kleinere Modell 7100VPN kostet 2.300 Euro, wobei auch hier für 670 Euro eine Aufrüstung auf 200 VPN-Tunnel erhältlich ist. (ln)

Lancom: www.lancom-systems.de



100 gleichzeitige VPN-Verbindungen sind mit dem VPN-Gateway "Lancom 7100 VPN" möglich

Mehr Virtualisierung für Red Hat

Red Hat bringt **Version 5.4** des Betriebssystems **Enterprise Linux** (RHEL) auf den Markt. Die neue Version bietet **erweiterte Virtualisierungsfunktionalitäten** dank der Integration der KVM-Technologie (Kernel-based Virtual Machine), der Intel Virtualization Technology for Directed I/O (Intel VT-d) sowie I/O-Virtualisierung PCI-SIG SR-IOV. Dadurch wird es möglich, virtuellen Maschinen auf einer Plattform mit Intel-Xeon-Prozessoren der 5500-Serie mehrere I/O-Geräte zuzuweisen. Darüber hinaus bietet das neue Release einen laut Hersteller verbesserten I/O-Durchsatz und zusätzliche Tools für Entwickler. Zudem wartet das Release mit Optimierungen für den Einsatz auf unterschiedlichen Hardware-Plattformen auf. Dies betrifft die bereits

erwähnten Intel Xeon-Plattformen sowie AMD Istanbul. Zu den Netzwerkverbesserungen gehört das Generic Receive Offload (GRO), das neue Prozessor-Komponenten in aktuellen Netzwerkadaptern nutzt. Auch Performance-Verbesserungen im Bereich Fibre Channel over Ethernet (FCoE) soll Version 5.4 mit sich bringen. Nicht zuletzt bietet das neue Release Optimierungen im Hinblick auf Gerätetreiber für Disk, Netzwerk, Grafik oder OFED InfiniBand. Administratoren können sich zudem über Verbesserungen im Toolset Systemtap für die Performance-Überwachung freuen. Ab sofort ist die neue Version erhältlich. In der Server-Variante ist RHEL mit einem Jahr Support für rund 350 US-Dollar erhältlich. (dr)

Red Hat: www.redhat.com/rhel/



"O&O Defrag 12" teilt den Datenbestand in unterschiedliche Zonen ein und will Defragmentierungen und Programmstarts so deutlich beschleunigen

Defragmentierung nach Maß

Software-Hersteller **O&O** bringt mit Version 12 eine Neuausgabe von **O&O Defrag** auf den Markt. Das Defragmentierungstool verfügt über neue Funktionen wie etwa die Einteilung der Festplatten in Daten-Zonen sowie zusätzliche Defragmentierungsmethoden. Das Werkzeug analysiert bei der ersten Defragmentierung den Datenbestand und ordnet diesen, abhängig von Verwendungszweck und Zugriffshäufigkeit, drei verschiedenen Bereichen zu. In die erste Zone werden Systemdateien eingeordnet, in der zweiten Zone Benutzerdaten und Einstellungen und die dritte Zone ist für wenig benutzte Dateien sowie sehr große Dateien reserviert. Diese logische Gruppierung soll nicht nur die Dauer des System- oder Programmstarts, sondern auch die Folgedefragmentierungen verkürzen. Der Anwender kann den unterschiedlichen Zonen weitere Dateien zuordnen und für diese die Art der Defragmentierung wählen. Zudem hat der Nutzer nun statt der Überwachung des gesamten Systems die Möglichkeit, einzelne Laufwerke auszuwählen, deren Fragmentierungsgrad ständig kontrolliert und optimiert werden soll. Wie bereits in der Vorgängerversion übernimmt die O&O Enterprise Management Console die zentrale Netzwerksteuerung der Defrag-Software. Die Server-Edition kostet 250 Euro, während der Preis der Workstation-Edition ab fünf Lizenzen 35 Euro beträgt. (ln)

O&O: www.oo-software.com/home/de/

Kein Anschluss für Unberechtigte

Fair Computer Systems hat seine Software zur **Endpoint-Security** komplett überarbeitet und stellt **Security.Desk .NET in Version 4.0** vor. Neben einer optimierten Benutzerführung hat der Hersteller die Software mit zahlreichen funk-



Komplett neu gecodet verfügt "FCS Security.Desk .NET 4.0" über eine ganze Reihe neuer Sicherheits-Features

tionalen Erweiterungen ausgestattet: So soll der grafisch und inhaltlich verbesserte Kontrollstand auf einen Blick darüber informieren, wie die Schnittstellen und Ports von Geräten genutzt werden und wo eventuelle Sicherheitslücken vorliegen. Darüber hinaus lassen sich ab sofort Berechtigungen für die Nutzung von Modems und UMTS-Geräten vergeben. Die schwarze Liste für Dateitypen gestaltet sich noch flexibler. Benutzer haben die Möglichkeit, auch weitere zu überwachende Dateitypen anhand eindeutiger Signaturen oder Dateierendungen zu ergänzen. Weiterhin lässt der neue Kommunikationsserver einen direkten Datenaustausch mit den Clients über Named Pipes zu, anstatt mit der bisher üblichen Netzwerkfreigabe zu arbeiten. Das Programm basiert nun außerdem vollständig auf dem Microsoft .NET Standard. Das Lizenzmodell basiert auf Staffelpreisen, die sich nach der Anzahl der überwachten Clients richten. So kosten beispielsweise 50 Lizenzen rund 500 Euro. (ln)

Fair Computer: www.fair-computer.de

Aus Alt mach Neu

IGEL Technology stellt eine neue **Migrationssoftware** vor: Der **Universal Desktop Converter** (UDC) stattet PCs, die letzte Generation der IGEL-Vorgängermodelle und ausgewählte Thin Clients von Drittanbietern wie Neoware und Dell mit der aktuellen IGEL Universal Desktop-Firmware aus. Dabei müssen zu migrierende PCs nicht mehr geöffnet werden, die Software installiert sich vielmehr selbst von einem bootfähigen USB-Token. Unterstützt werden Standard-PCs mit x86-kompatiblen Prozessoren, mindestens 512 MByte RAM und 1 GByte Flash- oder Festplattenspeicher (IDE oder SATA). Alle Thin Client-Migrationen bieten dabei laut Hersteller vollen Treibersupport. Die Liste an migrierbaren Thin Client-Typen will IGEL kontinuierlich erweitern. IGEL bietet den Linux-basierten USB-Stick dabei in drei Ab-

stufungen an, die den aktuellen Thin Client-Firmware-Paketen Entry, Standard und Advanced entsprechen. Neben der Installationsroutine beinhaltet der Universal Desktop Converter auch die IGEL Universal Management Suite 3 zur Fernadministration der migrierten Endgeräte. Der Universal Desktop Converter ist ab sofort mit den aktuellen IGEL Firmware-Paketen Entry, Standard und Advanced ab 39 Euro pro Lizenz erhältlich. (dr)

IGEL: www.igel.de



Mit einem USB-Stick plus Lizenz-SIM werden aus alten PCs IGEL Thin Clients

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

Open-Xchange erweitert den Funktionsumfang seiner Linux-basierten **Open Source-Groupware** um die Unified-Communications-Lösung **VoipNow** von **Rack-Soft**. Damit können die Anwender neben E-Mail, Adress-, Termin- und Aufgabenverwaltung von Open-Xchange auch die Telefonie-, Fax-, Präsenz- und Instant-Messaging-Dienste von Rack-Soft in einer integrierten Applikation mit einheitlicher Benutzeroberfläche nutzen. (dr)

www.open-xchange.com

Die **ReadyNAS-Produktfamilie** von **Netgear** unterstützt ab sofort den Remote Agent für Linux und UNIX Server (RALUS) der Symantec-Software Backup Exec für Windows Server. Durch die verbesserte Kommunikation zwischen Linux-basierten ReadyNAS-Systemen und Backup Exec-Servern will der Hersteller die Backup- und Recovery-Leistung in Symantec-Umgebungen deutlich steigern. Nutzer installieren dazu auf dem NAS-Speicher einen Agenten, der direkt mit der Backup-Software kommuniziert. Das von Symantec lizenzierte RALUS-Add-On wird ab Version 10.5 von Backup Exec unterstützt und steht zum Preis von 395 US-Dollar zum Download zur Verfügung. (ln)

www.netgear.de

NetIQ veröffentlicht Version 8.5 des **Directory and Resource Administrator** zur Verwaltung von Active Directory-Umgebungen. Die Software erlaubt eine granulare Steuerung von Administrator- und Benutzerrechten. Neben der Zentralisierung von Audit- und Reporting-Maßnahmen und der Automatisierung häufig wiederkehrender Aufgaben ermöglicht die Lösung auch die Durchsetzung von Sicherheits- und Managementrichtlinien. Ein hoch skalierbares Repository für Audit-Protokolle soll zudem verhindern, dass Aufzeichnungen manipuliert werden können. Darüber hinaus beansprucht das Repository laut Hersteller weitaus weniger Speicherplatz als datenbankorientierte Technologien. Der Lizenzpreis für 100 Nutzer beträgt rund 1.350 Euro. Ebenfalls in einer neuen Version erscheint der **Group Policy Administrator 6.1**. Die Management-Suite verfügt über ein sicheres Offline-Repository für die Verwaltung von Group-Policy-Objekten. Die Lösung ermöglicht neben der Offline-Modellierung und Analyse des Richtlinienresultats (RSOP – Resultant Set of Policy) auch das Management mehrerer Forests und Domains – auch solcher, die als nicht vertrauenswürdig eingestuft werden. Auf diese Weise sollen IT-Teams die Auswirkungen von Group-Policy-Objekten auf ihre Produktionsumgebung besser vorhersagen können. NetIQ Group Policy Administrator kostet für 100 Benutzer 760 Euro. (ln)

www.netiq.com/de/

NAS für virtualisierte Umgebungen

Iomega erweitert sein Portfolio an **NAS-Appliances** für kleinere Unternehmen und präsentiert das **StorCenter ix4-200d**. Verfügbar in Varianten mit 2, 4 und 8 TByte Kapazität nutzt das Desktop-Gerät die Software EMC LifeLine. Dabei handelt es sich um ein eigens entwickeltes Linux-Betriebssystem sowie eine Applikations-Suite, die für den Schutz der Daten sorgt und plattformübergreifend PC-, Macintosh- und Linux-Computer unterstützt. Der NAS-Würfel lässt sich mit RAID 5, 10 und JBOD konfigurieren. Um Ausfallzeiten zu minimieren, bestehen die vier Laufwerke im Inneren des Geräts aus SATA II-Festplatten, die vom Anwender im laufenden Betrieb ausgetauscht werden können. Die Speicherzentrale verfügt zudem über Dual-Gbit-Ethernet und drei USB 2.0-Ports für den Anschluss von Druckern und zusätzlichen USB-Laufwerken. Zu den weiteren Funktionen gehören iSCSI Block-Level-Zugriff, Device-to-Device-Replikation, Windows Active Directory-Einbindung sowie die zertifizierte Möglichkeit, den NAS-Speicher in mit VMware virtualisierten Umgebungen einzusetzen. Die Appliance ist ab sofort erhältlich und kostet in der 2 TByte-Variante rund 600 Euro, während die 8 TByte fassende Version mit rund 1.500 Euro zu Buche schlägt. (ln)

Iomega: <http://go.iomega.com/de/>



Bietet iSCSI-Unterstützung und ist für virtualisierte Umgebungen zertifiziert:
Der NAS-Speicher "Iomega StorCenter ix4-200d"

Vereinfachtes Systemmanagement

Matrix42 stellt **Version 12** der **Systemmanagement-Software Matrix42 Empirum** vor. Neben einer breiten Unterstützung für die neuen Betriebssysteme Windows 7 und Server 2008 will die neue Version eine besonders flexible Softwarepaketierung und eine verbesserte Usability für Administratoren bieten. Die Integration weitreichender und in der Praxis gebräuchlicher Virtualisierungstechniken ist zur Version v12 noch einmal verstärkt worden. Das Inventory der Suite identifiziert nun virtualisierte Computer und ordnet diese den entsprechenden Host-Systemen zu. Eine mit VMware ThinApp virtualisierte Anwendung wird dabei als solche erkannt und im Lizenz-Management korrekt abgebildet. Daneben erkennt die Software nun auch Mac OS X-Rechner bei der Inventarisierung. Administratoren steht nun eine optimierte Oberfläche zur Verfügung, in der die wichtigsten und oft verwendeten Aktionen leichter zugänglich sind. Noch mehr administrative Regelaufgaben als bisher lassen sich in Version 12 dabei direkt aus der webbasierten Konsole durchführen. Der "Package Wizard", der den Administrator bei der Erstellung von Softwarepaketen unterstützt, wurde zudem überarbeitet und soll nun ebenfalls einfacher zu verwenden sein. Bei 100 Clients beträgt der Preis für die Suite 5.625 Euro. (dr)

Matrix42: www.matrix42.de

Datenspeicher kompakt und sicher

Buffalo Technology bietet mit der **DriveStation HD-CX** ein neues Speichergerät mit integrierter Hardwareverschlüsselung an. Die DriveStation fasst je nach Ausführung zwischen 500 GByte und 2 TByte an Daten und sichert diese mittels AES-256 vor unbefugten Zugriffen. Hierfür kommt die Windows-Software "Secure Lock Manager" zum Einsatz, über die sich die Verschlüsselung steuern lässt. Neu ist auch ein Stromsparmmodus, der die DriveStation abschaltet, sobald der angeschlossene PC herunterfährt. Anschließen lässt sich der Speicher via USB. Daneben stellt der Hersteller die externe USB-Festplatte **MiniStation HD-PX** vor. Auch sie schützt die gelagerten Dateien via Verschlüsselung und fasst bis zu 640 GByte. Ab sofort sind beide Produkte erhältlich. Die DriveStation ist zu einem Preis ab 70 Euro zu haben, die MiniStation kostet mindestens 67 Euro. (dr)



Der Access Point "SMCE21011" lässt sich dank PoE-Funktionalität auch an Orten ohne Stromanschluss betreiben

Strom durchs Netzkabel

SMC Networks bietet mit dem Modell **SMCE21011** ab sofort einen neuen **Wireless Access Point** für den Unternehmenseinsatz an. Die Dual-Band-Funktion des Geräts stellt Administratoren vor die Wahl, ob sie Geräte im 2,4-GHz-Frequenzband betreiben oder zur 5-GHz-Frequenz wechseln. Der Netzwerk-Funker verfügt über drei MIMO-Antennen (Multiple Input, Multiple Output), die sich entfernen und zur Erhöhung der Reichweite durch High-Gain-Antennen ersetzen lassen. Ferner unterstützt die WLAN-Komponente bis zu acht virtuelle Access Points. Damit können Nutzer den Datenverkehr verschiedener Benutzergruppen als logische Einheiten zusammenfassen. Jedes virtuelle Gerät lässt sich dabei separat konfigurieren. Dies umfasst neben der Vergabe einer eigenen SSID zudem allgemeine Sicherheitsvorgaben. Aufgrund der Unterstützung von Power-over-Ethernet (PoE) ist der Access Point unabhängig vom Stromversorgungsnetz des Firmengebäudes und kann damit auch an schwer zugänglichen Orten eingesetzt werden. Der Verkaufspreis des SMCE21011 liegt bei rund 360 Euro. (ln)

SMC Networks: www.smc.com

schlossene PC herunterfährt. Anschließen lässt sich der Speicher via USB. Daneben stellt der Hersteller die externe USB-Festplatte **MiniStation HD-PX** vor. Auch sie schützt die gelagerten Dateien via Verschlüsselung und fasst bis zu 640 GByte. Ab sofort sind beide Produkte erhältlich. Die DriveStation ist zu einem Preis ab 70 Euro zu haben, die MiniStation kostet mindestens 67 Euro. (dr)

Buffalo Technology:

www.buffalo-technology.com/products/external-drives/



Die Leser des Fachmagazins PC Welt haben entschieden: 1&1 ist wieder die Marke des Jahres 2009 im Bereich Webhosting.

Neu

Ein schöner Grund, sich mit tollen Angeboten zu bedanken! Und darum gibt's ab jetzt unbegrenzten Traffic bei allen 1&1 WebHosting-Paketen! Außerdem bekommen Sie bei 1&1 viele Domains 1 Jahr lang für 0,- € und sparen bei Hosting-Paketen, Servern und E-Shops 50 % in den ersten 6 Monaten. Also, worauf warten Sie noch?

1&1 WebHosting

UNLIMITED

Unlimited Traffic – bei allen Hosting-Paketen!

Aktion gilt nur noch bis 31.10.2009!

HOSTING

Komplett-Lösungen für den perfekten Internet-Auftritt

z. B. 1&1 Homepage Business:

- 3 Inklusiv-Domains
- Neu: 5 GB Webpace
- **UNLIMITED** Traffic

6 Monate

**50 %
Rabatt!**

~~14,99~~
€/Monat*

6,99
€/Monat
danach ab 14,99 €/Monat*

Aktion gilt nur noch bis 31.10.2009!

SERVER

Hochleistungs-Server für gehobene Ansprüche

z. B. 1&1 Dedicated Server

Dual-Core XL:

- AMD Opteron™ 1218
- 2 x 2,6 GHz
- **UNLIMITED** Traffic

6 Monate

**50 %
Rabatt!**

~~99,99~~
€/Monat*

49,99
€/Monat
danach ab 99,99 €/Monat*

Weitere Preis-Aktionen finden Sie im Internet!

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



Jetzt informieren und bestellen unter:

01805 / 001 535

14 ct/Min. dt. Festnetz,
Mobildfunktarife ggf. abweichend

www.1und1.info

1&1

IT-Administrator-Workshop am 29. Oktober 2009 in Böblingen

ITANet Schirmherrschaft:



ITANet Workshop-Partner:

KROLL ONTRACK®

Klarheit im virtuellen Dschungel

von John Pardey

Vor einem Berg vielversprechender Virtualisierungs-Möglichkeiten stehend, fragen sich IT-Verantwortliche heute zu Recht, welche der Technologien ihre IT tatsächlich voranbringt und welche eher kritisch zu hinterfragen sind. In unserem Workshop "Virtualisierung" nehmen wir uns dieser Problematik an und analysieren zusammen mit unabhängigen Experten den aktuellen Stand der Technik bei Hypervisoren und Hardware und zeigen Szenarien auf, in denen Virtualisierung schnell Erfolge bringt.

Bevor jedoch unser Workshop in Böblingen startet, haben wir diesmal einen besonderen Programmpunkt für unsere Teilnehmer: als Gast der Kroll Ontrack GmbH steht eine Führung durch einen Reinraum an. Hierbei können die Teilnehmer erfahren, welche Maßnahmen bei einer professionellen Datenrettung notwendig sind.

Stand der Dinge

Im Anschluss an die Reinraumführung wenden wir uns dem aktuellen technologischen Stand der Virtualisierung zu. Ein IT-Verantwortlicher gewinnt unter dem Dauerbeschuss des Marketings der zahlreichen Anbieter sicher leicht den Eindruck, dass es der Königsweg sei, alle Server und jedes Gerät zu virtualisieren. Daher wendet sich Holger Gantikow, Systems Engineer bei der sience + computing ag, im Workshop zunächst der Frage zu, was Hypervisoren aktuell leisten, wo ihre Stärken und Schwächen liegen und welche Einsatzgebiete sinnvoll sind. Ergänzend dazu betrachten wir den Stand der Hardware-Unterstützung. Der zweite Vortrag des Nachmittags widmet sich der Datenrettung in virtuellen Umgebungen. Ist die Datenrettung schon in physikalischen Systemen oft nur von Experten zu bewerkstelligen, so gilt dies für "virtualisierte Daten" umso mehr.

Schnelle Erfolge und Management

Nach einer kurzen Kaffeepause zeigt Nicholas Dille, Berater bei der sepago GmbH, auf, wie sich virtualisierte Desktops in eine bestehende IT-Infrastruktur integrieren lassen. Dille legt dar, wie diese vielversprechende Technologie von IT-Abteilungen als Ergänzung einer Zentralisierungs- und Bereitstellungsstrategie für die Clients zum Einsatz kommt. Als letzter Dozent des Tages widmet sich schließlich Nico Lüdemann, Geschäftsleiter Systeme und Services acocon GmbH, der Frage, in welchen Bereichen die Virtualisierung ihre Stärken ausspielen kann. Lüdemann analysiert dabei, in welchen Bereichen Unternehmen "Quick Wins" mit der Virtualisierung realisieren können, in welchen Bereichen also die Einführung virtueller Infrastrukturen schnell Vorteile für das Unternehmen bringt.

Ein Workshop also, zu dem sich alle IT-Verantwortlichen, die den Einstieg in die Virtualisierung vor Augen haben oder den Einsatz von Virtualisierungstechnologien weiter ausbauen wollen, schnell einen Platz sichern sollten. Die Anmeldeinformationen finden Sie im Kasten auf dieser Seite. Der für alle Abonnenten kostenlose Workshop steht ab sofort zur Registrierung offen und wir würden uns freuen, Sie in Böblingen begrüßen zu dürfen.

iläNet
Die System und Netzwerk User Group

Die Agenda des Workshops

- 12.00 Uhr:** Begrüßung
- 12.15 Uhr:** Reinraum-Führung
- 13.00 Uhr:** Aktueller Stand der Technologie:
 - Hypervisoren – Stärken, Schwächen, Einsatzgebiete
 - Hardwareunterstützung für Virtualisierung
 Dozent: Holger Gantikow, sience + computing ag
- 14.00 Uhr:** Datenrettung in virtuellen Umgebungen
Dozent: Holger Engelland, Kroll Ontrack
- 14.45 Uhr:** Pause
- 15.00 Uhr:** Virtuelle Desktops als Ergänzung einer Zentralisierungs- und Bereitstellungsstrategie
Dozent: Nicholas Dille, sepago GmbH
- 16.00 Uhr:** Quick Wins der Virtualisierung: Server, Desktops, Storage, Netzwerk – wo anfangen?
Dozent: Nico Lüdemann, acocon GmbH
- 17.00 Uhr:** Diskussion mit Dozenten und Teilnehmern
- 17.30 Uhr:** Ende des Workshops

Ort: Kroll Ontrack GmbH, Hanns-Klemm-Str. 5, 71034 Böblingen

Teilnahmegebühren:
Für IT-Administrator Abonnenten kostenlos.

Anmeldung bis zum 20. Oktober unter
www.it-administrator.de/workshops

Workshop "Virtualisierte Infrastrukturen" am 29.10.



ice:2009, 22. August, Lingen/Ems

Pflichttermin für Admins

von John Pardey

Mittlerweile ist die ice zu einer echten Institution gewachsen und so es ist nicht verwunderlich, dass die 250 kostenlosen Plätze in diesem Jahr nach weniger als 30 Tagen restlos vergriffen waren. Attraktive und praxisnahe Themen, die von engagierten Dozenten vorgetragen werden, lockten IT-Verantwortliche Ende August scharenweise ins Emsland. Wir waren in Lingen vor Ort.

Nach der Eröffnung durch den Linger Oberbürgermeister Heiner Pott, der die Teilnehmer im Emsland willkommen hieß, und der Keynote von Dr. Johannes Loxen, Geschäftsführer der Ser-Net GmbH, teilte sich das Auditorium in vier Vortragsreihen auf. Zu den bekannten Reihen "IT Pro", "Business" und "Developer" gesellte sich dieses Jahr der "VT Track", der sich auf Virtualisierungsthemen konzentrierte.

Wir stellten uns zunächst zusammen mit Nils Kaczinski im IT-Pro-Track die Frage "Active Directory Recovery – wie mache ich's richtig?" und erhielten vom langjährigen Autor des IT-Administrator auch die gewohnt kompetenten Antworten. Kaczinski trug vor, wie sich das AD-Recovery von Version zu Version des Windows Servers unterscheidet: vom berühmten-berühmten authoritative / non-authoritative Restore über das Tombstone Recovery unter Windows Server 2003, den mit Windows 2008 eingeführten Active Directory Snapshots hin zum brandneuen Active Directory-Papierkorb in Windows Server 2008 R2.

Kaczinski führte anhand von Videos die notwendigen Schritte des AD-Recovery in allen vier Verfahren vor, bot Tipps, Tricks und Tools. Wer noch nicht

auf die deutlich vereinfachten Verfahren des Windows Server 2008 R2 zurückgreifen kann, dem sei ein Tool des Dozenten ans Herz gelegt: Werding 2.1 [1] ist ein VB-Script, das beim Tombstone Recovery unter Windows Server 2003 unter anderem die Gruppenmitgliedschaften in gelöschten Objekten wiederherstellt.

Sicherheit von Host und E-Mail

In einem weiteren Workshop widmete sich nun Marc Grote mit seinem Vortrag der Virtualisierung und konkret dem Thema der Sicherheit von Hyper-V. Er griff die Bedenkenlosigkeit auf, mit der viele IT-Verantwortliche die Sicherheit von virtuellen Servern und dem Host kompromittieren: die Sorglosigkeit, dass ein sicherer Host allein ausreicht oder auch mangelhaftes Patchen der VMs. Die große Anzahl erschienener Zuhörer deutete jedoch eher darauf hin, dass die Erkenntnis, dass Sicherheit in virtuellen Infrastrukturen nicht trivial ist, sich zunehmend durchsetzt. Grote stellte dem eine ganze Reihe von Best Practices entgegen, die von der Installation (Nutzung von Server Core, Patchstrategien, Härten des Hostsystems) über den Umgang mit den VMs im Hyper-V (Speicherorte für VHD und VMC, Speicherzuordnung, Storage-Zugriff der VM) bis hin zur Gast-Sicher-

heit (RAM- und CPU-Monitoring, Virens Scanner, Patching) reichten. Wer sich mit dieser Thematik im Detail befassen möchte, dem sei der Download der ice-Vortragsunterlagen [2] empfohlen.

Nach dem wie immer hervorragenden Mittagessen nahm sich Heiko Brenn, Senior Consultant bei GROUP Technologies, in seinem Vortrag der Aufgabenstellung an, zu verhindern, dass sensible Daten per E-Mail das Unternehmen verlassen. Dabei gibt es laut Brenn nicht nur die Problematik, dass viele Unternehmen gar nicht wüssten, welche Daten per E-Mail nach draußen gehen, sondern auch das äußerst heikle Thema der rechtskräftigen Willenserklärung per E-Mail. Um die Kontrolle über die ausgehende elektronische Post zu erlangen, empfahl Brenn die Absender- und Empfängerprüfung, eine Inhaltsprüfung sowie eine Dateianhangsanalyse.

All dies sei mit aktueller Technologie zu bewerkstelligen. Komplexer stellte sich das Thema der Verschlüsselung und digitalen Signatur dar. Denn neben der schwierigen Handhabung und der kostspieligen Einführung von entsprechenden Infrastrukturen müsste eben auch der jeweilige Partner – also der Empfänger der E-Mail – in Sachen Ver-

schlüsselung die gleiche "Sprache" sprechen. Und dies sei in der Praxis noch immer das zentrale Hindernis. Doch auch hier böten sich, wie Brenn dem hellhörig gewordenen Auditorium mitteilte, inzwischen Lösungsansätze.

Diskussion in kleiner Runde

Zusätzlich zu den vier Tracks bot sich den Teilnehmern vor der Veranstaltungshalle eine weitere Gelegenheit, ihr Wissen auf den neuesten Stand zu bringen. Citrix hatte dort einen weiteren Vortragsraum aus einem LKW aufgebaut. Hier fanden sich zum "Geek Speak" rund um "Virtuelle Desktops vs. Terminaldienste" – wohl geschuldet dem parallel laufenden Windows 7-Vortrag – nur eine Handvoll Interessierter ein, um dem Für und Wider der beiden Technologien zu lauschen. Eine durchaus spannende Diskussion, die klarmachte, dass virtuelle Desktops aktuell nur für 15 bis 20 Prozent der User wirklich sinnvoll sind. Alles in allem er-

freute sich der Citrix-Truck jedoch einiger Beliebtheit und rundete das ice-Programm sehr gut ab.

Wieder in den it-Emslandhallen stand nun 64-Bit-Windows mit Helge Klein, Berater bei der sepago GmbH, auf der Agenda. Er legte dar, unter welchen Umständen sich ein Umstieg in die 64-Bit-Welt lohnt und was dabei zu beachten sei. Administratoren sollten sich vor einem anvisierten Umstieg jedoch genau informieren, ob dem gestiegenen RAM-Bedarf der Server nicht auch mit Physical Address Extension (PAE) und WOW 64 (Windows-On-Windows 64-Bit) Genüge getan ist, denn diese erlauben immerhin eine Adressierung von 64 GByte RAM auf 32-Bit-Systemen. Solle jedoch der Schritt in die echte 64-Bit-Welt vollzogen werden, so empfiehlt Klein, bei der Migration Augenmerk auf das Drucken und die Skripte zu haben, denn dort lägen die Fußangeln eines solchen Projekts.

Fazit

Die ice:2009 überzeugt nach wie vor mit ihrem Konzept, eine kostenlose Veranstaltung für die IT-Pro-Community anzubieten. Die hohe inhaltliche Qualität des Tages lässt sich in diesem Beitrag nur ansatzweise darstellen, da der Autor, physikalischen Gesetzen gehorchend, 75 Prozent der Vorträge verpasste. Und dass Organisator Nicki Wruck neben der Organisation einer solchen Veranstaltung nicht müde wird, für das Wohl der Kleinsten unsere Gesellschaft [3] zu werben, ist mehr als lobenswert. Wir sind nächstes Jahr wieder dabei. 

[1] Werdung 2.1

www.kaczinski.de/2006/11/19/werdung-v2/

[2] Vorträge der ice:2009

www.ice-lingen.de/pages/de/site.php?page=download

[3] Com for Children

www.comforchildren.de

Links



27-28 Oktober 2009
Congress Frankfurt

co-located mit



Show Highlights

- 100 Tutorien
- SNIA Experten
- Internationale Analysten
- über 50 Hersteller erwartet
- Hands-on Lab
- Freier Zutritt für Anwender und Channel*

SNIA Experten referieren über

- Virtualisierung
- Solid State Storage
- Security
- Networking
- File Systeme
- Datensicherung

*mit Promo code M17S09

www.snweurope.net

SNW Europe is co-owned by SNIA & Computerworld, organised by Angel Business Communications Ltd and endorsed by SNIA Europe. Virtualization World and Datacenter Technologies are both co-owned by Angel Business Communications Ltd and SNIA Europe.

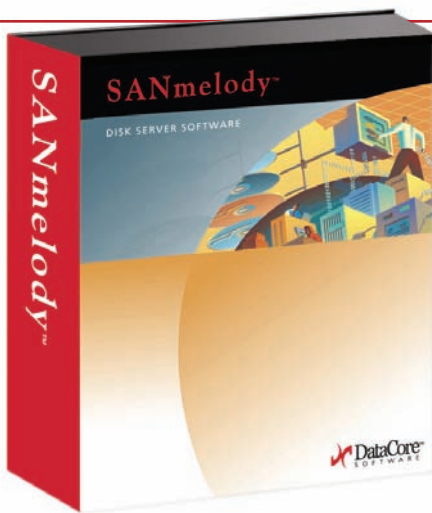




Im Test: DataCore SANmelody

SAN im Eigenbau

von Jürgen Heyer



Wer bei der Speicherbereitstellung im SAN oder via iSCSI nicht in teure Spezialhardware investieren möchte, findet in SANmelody von DataCore eine interessante Alternative. Unter Verwendung von preiswerter Standard-Hardware lassen sich mit der Software leistungsfähige Storage-Server konfigurieren. IT-Administrator hat sich diesen SAN-Baukasten einmal näher angesehen und verschiedene Szenarien durchgeprobt.

Eine der großen Stärken der Speicher- und SAN-Virtualisierungssoftware SANmelody ist unbestritten deren flexible Konfigurierbarkeit für unterschiedlichste Anforderungen und Speichervolumen. Es lassen sich Storage-Server gleichermaßen sowohl für SAN- als auch für iSCSI-Umgebungen konfigurieren. Ebenso erfüllt die Software verschiedene Verfügbarkeitsanforderungen inklusive High Availability (HA) durch Spiegelung und mehrpfadige Anbindungen der Endsysteme.

SANmelody verwaltet bis zu 32 TByte Speicher, läuft problemlos auf virtuellen Maschinen und adressiert den Speicherbedarf von kleineren und mittleren Unternehmen im iSCSI- und Fibre-Channel-Umfeld. Ferner hat DataCore noch das Enterprise-Produkt SANSymphony im Portfolio, das über Multi-Tier-Umgebungen hinweg skaliert und sich für High-End-Speichersysteme eignet.

Getestet haben wir jedoch SANmelody 3.0, das als Basis Windows 2008 Server voraussetzt. Aufgrund der besseren Speicherskalierung empfiehlt der Hersteller die 64-Bit-Version, also beispielsweise Windows 2008 Server 64 Bit mit einer Hauptspeicherunterstützung bis zu 32 GByte. Unsere Testsysteme haben wir mit Windows 2008 Server Enterprise SP2, 64 Bit, konfiguriert.

Am Anfang steht die Planung

Im Vorfeld der Installation fällt sofort auf, dass DataCore hervorragende Arbeit bei der Dokumentation geleistet hat. Immerhin gibt es diverse Konfigurationsmöglichkeiten sowie Optionen und es sind verschiedene Voraussetzungen zu beachten. Ein sogenannter "Best Practice Guide" spricht alle wichtigen Dinge an, zeigt die verschiedenen Verschaltungsmöglichkeiten auf und gibt Tipps zur optimalen Performance. Darüber hinaus lässt sich bei der Installation eine Online-Hilfe einrichten, die auf Wunsch beim Aufruf von SANmelody erscheint und Assistenten-ähnlich die ersten notwendigen Schritte beschreibt. Über entsprechende Verlinkungen in dieser Beschreibung kann der Administrator schnell an die relevante Stelle springen.

Nach dem Studium des Guides ist es erforderlich, das zu konfigurierende Szenario genau zu planen und sowohl die Hardware als auch das Betriebssystem entsprechend vorzubereiten. Da SANmelody ausschließlich über zertifizierte Fachhändler vertrieben wird, sollten diese für eine derartige Planung der erste Ansprechpartner sein. In der Regel führt der Systempartner die Inbetriebnahme vor Ort durch. Administratoren, die selbst einmal mit SANmelody arbeiten wollen, sei gesagt, dass der von DataCore angebotene Download einer 30-Tage-Testversion nicht alle Optionen enthält und nur einfache Konstellationen zulässt, durchaus aber einen ersten Einblick vermittelt. Für unseren Test stellte uns der Hersteller eine Version mit vollem Funktionsumfang zur Verfügung.

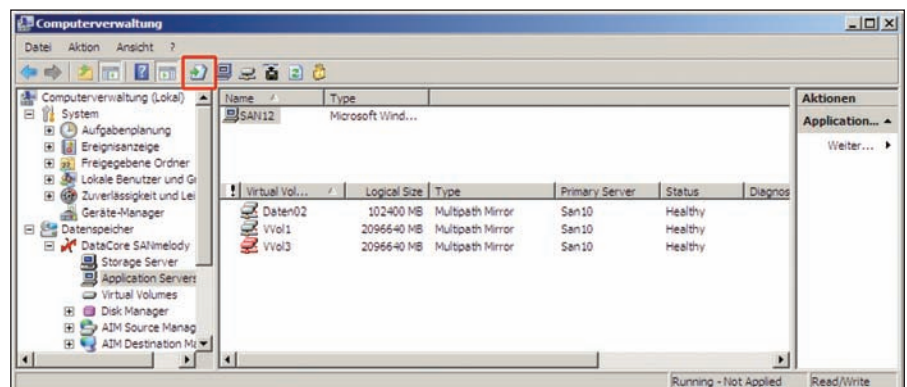


Bild 1: SANmelody erweitert die Computerverwaltung.

Erst der Apply-Button in der Kopfzeile bestätigt die rot markierte Aktion endgültig.



Wie schon eingangs erwähnt, ist für das aktuelle SANmelody 3.0 Windows 2008 Server Voraussetzung, vorzugsweise in englischer Sprache. Im Test haben wir mit der deutschen Version gearbeitet und diesbezüglich keine Probleme feststellen können. Installiert sein muss weiterhin das .NET-Framework 3.51. Ist der Einsatz von iSCSI vorgesehen, sollte das Servicepack 2 von Windows 2008 Server installiert sein, alternativ auch ein spezieller Hotfix (KB 961570), der auf Nachfrage bei Microsoft erhältlich ist und einen Fehler im iSCSI-Umfeld bereinigt. Außerdem muss der iSCSI-Initiator vor der SANmelody-Installation aktiviert werden, damit das Setup einige iSCSI-Parameter zur Vermeidung von Timeouts anpassen kann.

Wichtig ist, die zukünftigen Storage-Server mit ausreichend LAN- oder Fibre-Channel-(FC)-Adaptoren auszustatten. So benötigt beispielsweise ein Speicherserver im SAN-Umfeld mit Spiegelung und Multipath-Anbindung der Endsysteme bis zu sechs FC-Anschlüsse (zwei zum FC-Plattensystem, zwei für die Spiegelung zum Partner und zwei für die Anbindung der Server, welche die bereitgestellte Kapazität nutzen sollen), um einen Single Point of Failure (SPOF) zu vermeiden. Bei einer iSCSI-Konfiguration sollten der iSCSI-Datenverkehr und der administrative Zugriff über getrennte Adapter laufen, außerdem ist in einer Produktionsumgebung der Einsatz von 10-Gbit-Ethernet für iSCSI ratsam.

Weiterhin empfiehlt DataCore, den administrativen Zugriff auf die Speicherserver vom öffentlichen Firmen-LAN zu trennen, beispielsweise mittels VLAN-Konfiguration. Es gibt nämlich keinen Grund, warum irgendjemand, außer dem Administrator, überhaupt direkt auf solch einen Server zugreifen sollte. Die Speicherserver sollten auch nicht Mitglied einer Domäne sein, sondern in einer Arbeitsgruppe zusammengefasst werden, damit nicht Domänenrichtlinien unbeabsichtigt Einstellungen verändern. Zudem empfiehlt DataCore, die automatischen Windows Updates zu deaktivieren, da der Hersteller sein Produkt

nur auf Servicepack-Ebene freigibt, aber die Hotfixes nicht testet. Ein Virens Scanner sollte schon aktiv sein, aber keine Backup-Software, da diese unter Umständen Laufwerke bei der Sicherung kurzzeitig sperrt.

Sinnvolle Erweiterung der Computerverwaltung

Als Benutzeroberfläche bedient sich SANmelody der Computerverwaltung und erweitert die MMC mittels Snap-Ins um einen ganzen Funktionsblock. Außerdem wird die Taskleiste um ein Icon ergänzt, über das die Computerverwaltung komfortabel geöffnet werden kann. Vorteilhaft ist die Integration insofern, da der Administrator bei der Konfiguration gelegentlich den Gerätemanager sowie die Datenträgerverwaltung benötigt und dann nicht zwischen verschiedenen Oberflächen springen muss. Ein überaus wichtiges Bedieninstrument ist der Apply-Knopf, um durchgeführte Änderungen zu bestätigen und zu aktivieren. So werden neu eingerichtete Objekte wie Volumes oder Verbindungswege anfangs rot unterlegt, was dann mit Betätigung von "Apply" verschwindet. Manchmal sind nur bestimmte Optionen ausgegraut, so dass eine weitere Konfiguration nicht möglich ist, oder

ein Objekt, das nach einer vorherigen Aktion für den nächsten Konfigurationsschritt benötigt wird, ist (noch) nicht vorhanden. Dann lohnt sich ein Blick in die Fußzeile der Computerverwaltung, wo meist der Hinweis "Not Applied" zu finden ist.

Gelegentlich ist es notwendig, die Computerverwaltung zu schließen und wieder zu öffnen, damit sich die Anzeige aktualisiert. Hierauf weist SANmelody allerdings in der Regel mittels Popup hin. Innerhalb des SANmelody-Funktionsblocks sind die meisten Punkte selbsterklärend und übersichtlich aufgebaut. Es gibt Rubriken für die Anlage der Storage-Server und der Application-Server. Im Disk Manager lassen sich die SANmelody zugeordneten Festplatten verwalten. Die beiden Punkte "AIM Source" und "Destination Manager" dienen zur Verwaltung der Option für eine asynchrone Datenkommunikation, weitere Snap-Ins sind für Snapshots und die Diskpfade zuständig. Wichtig sind weiterhin getrennte Punkte zur Verwaltung der Anbindung mittels Fibre Channel und iSCSI. In der Trace Console können – vor allem zur Fehlersuche – die auflaufenden Meldungen eingesehen werden.

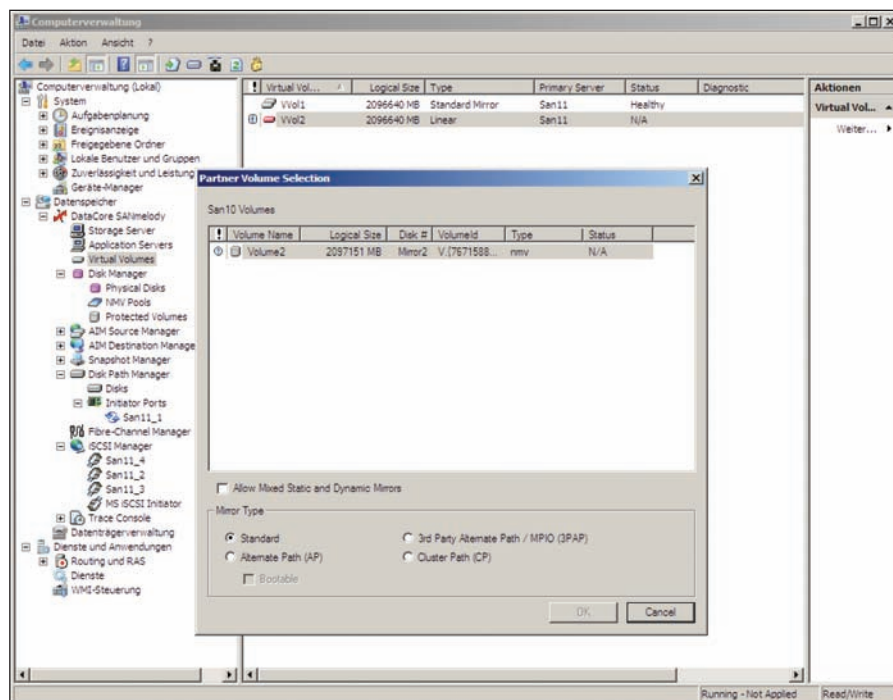


Bild 2: SANmelody unterstützt hinsichtlich der Spiegelung mehrere Verfahren, sowohl mit einem als auch mit mehreren Pfaden



Insgesamt ist bei der Bedienung von SANmelody etwas Erfahrung notwendig. Auch sollte der Administrator eine gewisse Ruhe mitbringen und auf vermeintliche Probleme nicht mit hektischen Aktionen reagieren. Gerade Spiegelprozesse benötigen Zeit und SANmelody ist sehr sparsam mit der Anzeige von Arbeitsfortschritten. Vielmehr arbeitet es im Hintergrund und im Test sprang die Anzeige öfters plötzlich von "Mirror Down" auf "Healthy" um, ohne den Betrachter dazwischen durch Prozentangaben zum Arbeitsfortschritt zu beruhigen. Sollte bei einer Resynchronisation ein Arbeitsfortschritt angezeigt werden, wunderten wir uns im Test über die großen Sprünge beispielsweise von null über 25 gleich auf 100 Prozent. In solchen Situationen half Abwarten mehr, als das System mit weiteren Aktionen noch zusätzlich zu beschäftigen.

Konfiguration von einfach bis komplex

Im ersten Schritt konfigurierten wir eine einfache Umgebung, um eine Festplatte als iSCSI-Volume bereitzustellen, was uns mitsamt der SANmelody-Installation innerhalb von 30 Minuten problemlos gelang und sich auch mit der via Webseite erhältlichen Trial-Version realisieren lässt. Mit der Installation von SANmelody aktiviert das Programm automatisch alle Netzwerkkarten und iSCSI-

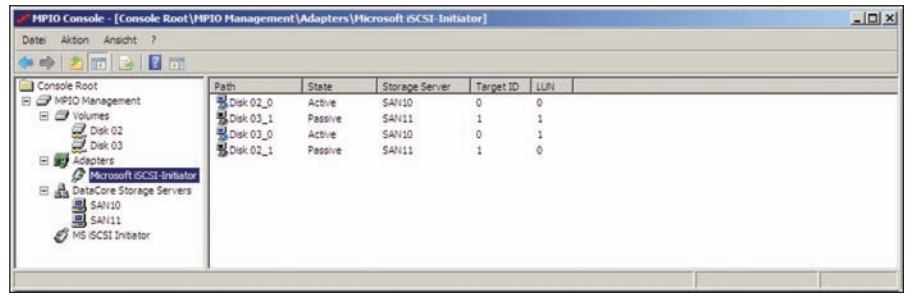


Bild 3: In der MPIO Console am Application-Server sind die mehrpfadige Anbindung und deren Status sehr übersichtlich ablesbar

HBAs als iSCSI-Target. Für die Bereitstellung der Festplatte als normales Laufwerk ist diese in der Festplattenverwaltung zu partitionieren, allerdings ohne sie zu formatieren und ohne einen Laufwerksbuchstaben anzugeben.

Damit ist das Laufwerk innerhalb von SANmelody sichtbar, um ein so genanntes Virtual Volume zu erstellen. Weiterhin ist innerhalb von SANmelody für den Application-Server, der dieses Volume nutzen soll, ein Eintrag anzulegen und eine Zuordnung vorzunehmen. Hier ist die Darstellung erfreulich übersichtlich, denn in einem Fenster sind alle Application-Server aufgelistet, die von einem Storage-Server versorgt werden. Um nun eine Verbindung zu definieren, muss der Administrator dem Application-Server-Eintrag die zugehörige WWN oder den iSCSI-Initiator zuordnen und in einem weiteren Schritt das bereitzustellende Vo-

lume auf diese Verbindung mappen. Leider gibt es außer der guten Online-Hilfe keinen Assistenten zur Unterstützung.

Deutlich komplexer wird die Konfiguration, wenn zwei Storage-Server mit synchroner oder asynchroner Datenspiegelung zusammenarbeiten sollen. Die Krönung ist letztendlich, wenn die gespiegelten Daten dann noch zur Vermeidung eines Single Point of Failure (SPOF) über mehrere Pfade mit dem Application-Server verbunden werden sollen. Gerade in diesem Fall ist es wichtig, für alle Verbindungen ein eindeutiges Namenskonzept zu nutzen, damit keine fehlerhaften Verbindungen eingerichtet werden und die Konfiguration später noch nachvollziehbar bleibt. Wir haben uns im Test mit einer Schaltskizze beholfen, in die wir alle Bezeichnungen und Adressen eingetragen haben. Der große Vorteil der Datenspiegelung mittels SANmelody besteht darin, dass auch

Gut, wenn man seinen Schutz immer dabei hat

GeNUCard: Sicherheitspaket für Laptops



IT-Security to go

GeNUA
www.genua.de



hierfür keine spezielle Hardware benötigt wird. Im einfachsten Fall lassen sich die Daten von zwei Standardservern mit großen internen oder externen Raid-Platten-Arrays spiegeln und so über verschiedenen Betriebsstätten und einige Kilometer Entfernung hinweg redundant halten.

Die Option "Asynchronous IP Mirroring" (AIM) erlaubt einen unidirektionalen, asynchronen Datenabgleich auch über Verbindungen mit geringerer Bandbreite, wobei die Daten hier von einem Quell-Server auf einen Zielsystem übertragen werden. Je nach Entfernung und Situation kann der Transfer mittels FTP oder SMB erfolgen. Eine weitere Option von SANmelody ermöglicht das Anlegen von Snapshots. Diese eignen sich nicht nur für Wiederherstellungen, sondern lassen sich zudem im Schreib-Lesemodus wieder zur Verfügung stellen, um beispielsweise zusätzliche Tests mit einem bestimmten Datenbestand durchzuführen.

Partnerschaft für Hochverfügbarkeit

Zum Aufsetzen einer Spiegelung wird zwischen zwei Servern eine Partnerschaft konfiguriert, wobei der eine als der primäre Server und der andere als der sekundäre fungiert. Für den Aufbau einer Partnerschaft muss auf den Systemen ein gleichnamiger Benutzer mit identischem Passwort angelegt und dieser Benutzer beim

Dienst "Storage Domain Server", der die Koordination zwischen den Partnern übernimmt, für die Anmeldung eingetragen werden. Nach dem Einrichten der Partnerschaft ist die SANmelody-Verwaltung immer nur auf einem Partner lese-/schreibberechtigt, auf dem anderen kann nur gelesen werden, damit nicht durch widersprüchliche Eingaben von zwei Seiten Konflikte entstehen. Eine Umschaltung ist aber möglich, indem der lese-/schreibberechtigte Partner zuerst in den Lesemodus geschaltet wird. Dann kann der andere die Schreibfunktion übernehmen. Dies ist notwendig, wenn beispielsweise auf beiden Seiten für eine Erweiterung neue Laufwerke angelegt werden müssen.

Eine normale Spiegelung hält die Daten zwischen den beiden Partnern synchron, die angeschlossenen Applikationsserver greifen aber ausschließlich über den primären Server auf die bereitgestellten Datentöpfe zu. Fällt der primäre Storage-Server aus, geht der Zugriff verloren, obwohl die Daten noch vorhanden sind.

Durch die einfache Anbindung existiert also immer noch ein SPOF. Um dies zu vermeiden, unterstützt SANmelody Multipathing und ermöglicht in dieser Kombination High Availability (HA). Wer dies nutzen will, darf auf keinen Fall die Multipathing-Funktion (MPIO) von Windows 2008 Server aktivieren. Vielmehr ist

auf jedem Applikationsserver ein von DataCore gelieferter MPIO-Treiber mit Konsole zu installieren. In der Konsole lässt sich anschließend sehr gut kontrollieren, ob alle Storage-Server, Volumes und Pfade sichtbar sind beziehungsweise erkannt wurden. Auch im Gerätemanager von Windows müssen die bereitgestellten Volumes als SCSI Disk Devices entsprechend der vorhandenen Pfade mehrfach sichtbar sein. Sollte dies nicht so sein, empfiehlt es sich, die Hardwareerkennung im Gerätemanager aufzurufen. Ist sonst kein Fehler in der Konfiguration vorhanden, sollten die fehlenden Einträge erscheinen.

Aufgrund entsprechender iSCSI- und SAN-Vorkenntnisse hatten wir uns vorgenommen, alle Szenarien ohne Unterstützung selbst zu konfigurieren, was uns mit Hilfe der guten Dokumentation erfolgreich gelang. Allerdings wird die Konfiguration zunehmend komplexer, vor allem, wenn Hochverfügbarkeit und Spiegelung gewünscht sind. Daher vertreibt DataCore, wie schon erwähnt, seine Produkte nur über zertifizierte Fachhändler, die im Regelfall die Inbetriebnahme durchführen, was sicher die beste Vorgehensweise ist. Sofern ein Administrator anschließend selbst Erweiterungen hinzufügen möchte, sollte er bei der Inbetriebnahme intensiv mitarbeiten, dann dürfte einer späteren eigenen Betreuung nichts im Wege stehen.

Mehr Platz durch Thin Provisioning

Wer einen ständig wachsenden Kapazitätsbedarf hat, weiß es zu schätzen, wenn diese Erweiterungen im laufenden Betrieb stattfinden können, ohne die Arbeit der Anwender zu beeinträchtigen. Hier ist das so genannte Thin Provisioning eine gute Hilfe. Während normalerweise die angelegten Laufwerke für den Anwender in ihrer ursprünglichen Größe sichtbar werden, legt SANmelody beim Thin Provisioning mit den Network Managed Volumes (NMV) eine Virtualisierungsebene dazwischen. Standardmäßig definiert SANmelody ein NMV mit 2 TByte Kapazität,

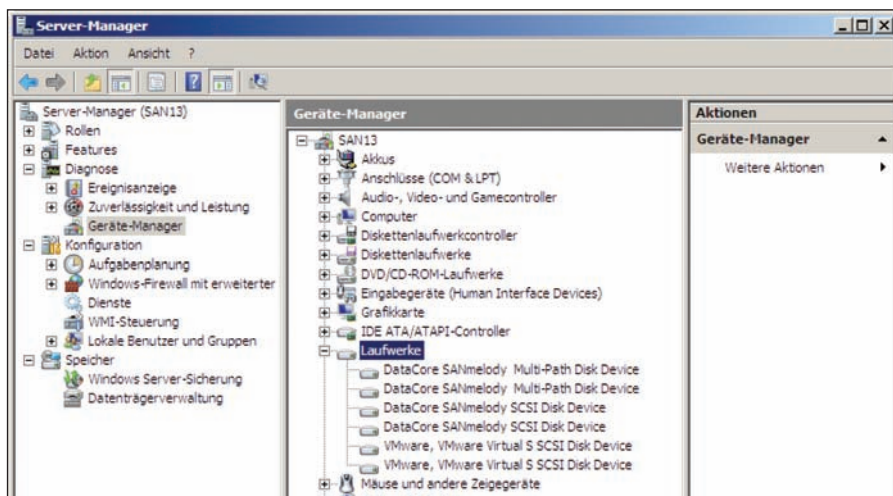


Bild 4: In dieser Situation ist pro Multi-Path Disk Device nur ein SCSI Disk Device sichtbar. Dies deutet auf einen Pfadausfall oder eine Failover-Situation hin.

LANCOM



... connecting your business

Das beste WLAN aller Zeiten!

Die höchsten Datenraten aller Zeiten, die beste Funkfeldabdeckung, maximale Kompatibilität – 802.11n setzt neue Maßstäbe im Wireless LAN. Drinnen wie draußen.

Machen auch Sie Ihr Netz zukunftsfähig – und steigen Sie um auf die 802.11n Indoor & Outdoor Access Points, Clients und „11n-ready“ WLAN-Controller von LANCOM.

Ob im kleinen Netz mit wenigen Access Points, im Controller-basierten WLAN mit Tausenden von Geräten, für den Hotspot-Betrieb oder im Freien: 802.11n WLAN von LANCOM sorgt überall für ungekannte Leistungsfähigkeit.



STORAGE/NETZWERKE
LANCOM OAP-310agn



LANCOM
Systems

www.lancom.de



egal, wie viel Platz auf den dahinterliegenden Laufwerken tatsächlich vorhanden ist. Beginnend mit einem physikalischen Laufwerk kann sogar ein NMV-Pool mit mehreren 2-TByte-Laufwerken angelegt werden. Der Applikationsserver sieht dann entsprechend viele 2-TByte-Laufwerke, obwohl das physikalische Raid-Array beispielsweise nur 500 GByte groß ist.

Wichtig ist nun natürlich die Überwachung des tatsächlichen Datenwachstums, wozu SANmelody bei einem einstellbaren Schwellwert (Standard: 80 Prozent) einen Eintrag ins Ereignis-Log schreibt, der sinnvollerweise automatisch an die Administratoren weitergeleitet werden sollte. Denn ist die physikalische Platte komplett vollgeschrieben, können die Anwender nichts mehr ergänzen, auch wenn sie noch genügend Platz sehen. Die Administratoren müssen nun entsprechend der Belegung rechtzeitig neue physikalische Platten hinzufügen. Das geschieht aber im Hintergrund, ohne dass der Anwender davon etwas merkt.

Failover-Tests sind unabdingbar

Wer eine HA-Lösung benötigt und konfiguriert hat, kommt nicht umhin, deren Funktion intensiv zu testen, um vor der produktiven Nutzung eventuelle Fehler aufzudecken. So mussten wir bei der iSCSI-Konfiguration mit Software-Target und -Initiator feststellen, dass der Failover zwar problemlos klappte, wenn wir am primären Storage-Server SANmelody stoppten oder den Server herunterfuhren. Der Application-Server konnte ohne Unterbrechung auf die bereitgestellten Volumes zugreifen. Beim harten Ausschalten aber störten längere Timeouts die Kommunikation zwischen dem Application-Server und dem sekundären Storage-Server massiv. Eine Analyse mit Unterstützung von DataCore brachte das Ergebnis, dass wir bei der Installation nicht die korrekte Reihenfolge gewählt hatten und die iSCSI-Parameter nicht passten. Nach einer Neuinstallation von SANmelody traten diese Probleme dann nicht mehr auf.

Bei der De- und Neuinstallation konnten wir uns übrigens davon überzeugen, dass SANmelody hierbei auf Wunsch die kompletten Einstellungen speichert und wiederherstellt, so dass wir nichts neu konfigurieren mussten.

Wird ein Storage-Server neu gestartet, egal aus welchem Grund, ist SANmelody anschließend gestoppt und muss manuell gestartet werden. Das ist gut so, damit der Administrator die notwendige Resynchronisation in eine lastarme Zeit legen kann und nicht ein plötzlicher Reboot mit anschließender Synchronisation womöglich den produktiven Betrieb stört.

Fazit

SANmelody stellt sich insgesamt als interessante Alternative vor allem für kleinere und mittlere Unternehmen dar, die hochverfügbaren Plattenspeicher benötigen, aber nicht in teure, spezielle Hardwarelösungen investieren wollen. SANmelody zeigte sich im Test als breitbandig einsetzbar und sehr variabel skalierbar bis zu 32 TByte verwalteter Kapazität. Reicht dies nicht aus, besteht die Möglichkeit zum Umstieg auf die umfangreichere Enterprise-Version SANsymphony.

Vorteilhaft ist bei SANmelody 3.0 die breite Hardwareunterstützung auf Basis von Windows 2008 Server. Aufgrund volumenabhängiger Lizenzen steigen die Kosten mit dem Umfang der Nutzung, was einen preisgünstigen Einstieg ermöglicht. Durch unterschiedliche Konfigurationsmöglichkeiten lässt sich genau das Szenario abbilden, welches vom Unternehmen benötigt wird. Vorteilhaft ist, dass sich sowohl synchrone Spiegel als auch asynchrone über längere Strecken hinweg aufbauen lassen. Allerdings ist SANmelody entsprechend der diversen Optionen und Konfigurationsmöglichkeiten vergleichsweise komplex, so dass ein Kunde sich bereits bei der Konzeption und beim späteren Aufbau auf die Empfehlung und die Realisierung durch einen zertifizierten DataCore-Partner verlassen sollte. (In)



Produkt

Software zur Speicher- und SAN-Virtualisierung.

Hersteller

DataCore
www.datacore.de

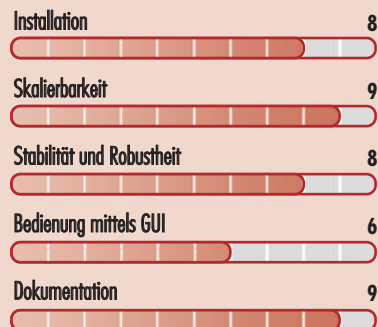
Preis

Die Preise richten sich nach den benötigten Optionen und der verwaltbaren Kapazität. Der Einstiegspreis für SANmelody liegt bei rund 720 Euro für 3 TByte Datenkapazität, iSCSI-Unterstützung und Thin Provisioning. Ein Paket zusätzlich mit synchroner und asynchroner Spiegelung sowie Snapshots kostet für 0,5 TByte etwa 1.250 Euro und für 3 TByte zirka 4.350 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für kleinere und mittlere Umgebungen, die hohe Anforderungen an die Datenverfügbarkeit stellen. Dies gilt sowohl für physikalische Systeme als auch Virtualisierungslösungen.

bedingt für kleine Umgebungen, die keine Spiegelung benötigen. Hier sind NAS-Appliances mit iSCSI-Support eventuell preislich interessanter. Bedingt geeignet erscheint uns SANmelody für sehr große Umgebungen. Hier gilt abzuwägen, ob statt großer Plattensysteme (EMC, IBM, Hitachi) mit entsprechender HA-Funktionalität auch der Einsatz von SANsymphony angedacht werden kann.

nicht für Umgebungen, wo sich die Speicheranforderungen durch direkt angeschlossene oder gar interne Raid-Platten realisieren lassen. Dies stellt zweifellos die kostengünstigste Lösung dar.

SANmelody



Im Test: VMware vSphere 4.0

Wolkiges Betriebssystem

von Dennis Zimmer

VMware vSphere ist nach mehrmonatiger öffentlicher Betaphase Ende Mai mit viel Lärm und Marketingaktivitäten offiziell erschienen und in die virtuellen Regale des VMware-Shops und der Reseller eingezogen. Zuvor hatte der Hersteller Kinosäle in der ganzen Welt angemietet, um Kunden und Partner auf den Launch des Produktes und die neuen Funktionen aufmerksam zu machen. Dabei war das Wort "Cloud" in aller Munde und vSphere wurde als erstes Cloud-Betriebssystem betitelt. Der folgende Test soll Aufschluss darüber geben, ob VMware wirklich der große Wurf gelungen ist oder ob die Konkurrenz eine gute Chance hat, zügig technologisch aufzuschließen.

Bevor wir im Rahmen unseres Tests die zwischen VMware Infrastructure (VI) 3.x und vSphere 4.0 bestehenden Unterschiede unter die Lupe nehmen konnten, mussten wir uns zunächst mit den neuen Editionen und den jeweiligen Lizenzierungsverfahren auseinandersetzen. Waren es mit VI 3.x noch drei Editionen (Foundation, Standard, Enterprise), kann der Kunde bei vSphere 4.0 zwischen insgesamt sechs Editionen wählen: Essentials, Essentials Plus, Standard, Advanced, Enterprise und Enterprise Plus. Einen Überblick über die Unterschiede der einzelnen Editionen gibt VMware unter [1]. Wie unter VI 3.x besteht ferner die Möglichkeit, den Hypervisor ESXi als alleinstehenden Server kostenfrei zu nutzen. Neben dem Funktionsumfang ist auch die Anzahl der nutzbaren Kerne pro CPU-Sockel von entscheidender Bedeutung, da nur die Versionen Advanced und Enterprise Plus bis zu zwölf Kerne pro Sockel unterstützen, während alle anderen Editionen nur sechs Kerne zulassen.

Kostenfaktor CPU-Lizensierung

Wer sich nun fragt, wo denn bei sechs Kernen das Problem liegt, sollte den Blick Richtung Jahresende richten: Für diesen Zeitpunkt hat Intel die neuen Acht-Core-CPU's angekündigt. Sobald acht Kerne pro CPU verbaut sind, muss der Nutzer

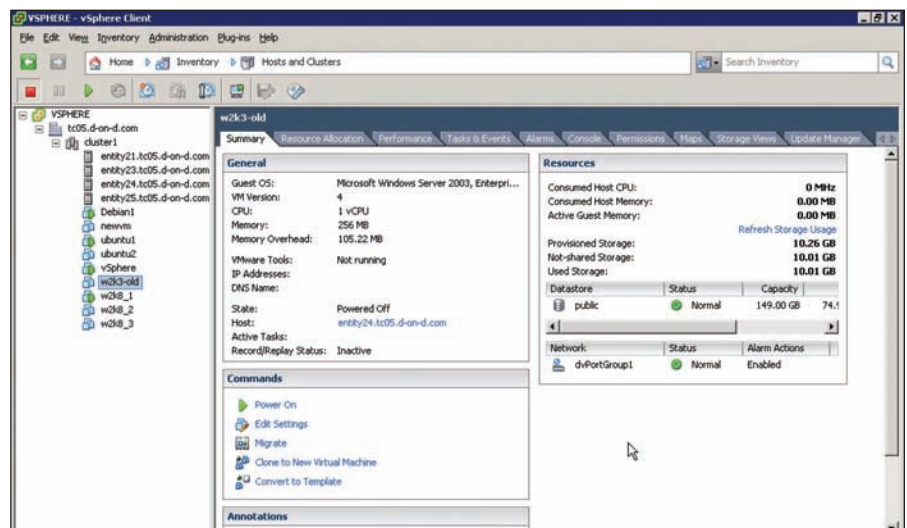


Bild 1: vSphere bietet eine äußerst funktionale Verwaltungsoberfläche

von vSphere zwangsweise etwa von einer Standard- auf eine Advanced-Lizenz wechseln, was mit Mehrkosten in Höhe von 1.450 US-Dollar pro Sockel zu Buche schlägt. Apropos Sockel: Das Lizenzmodell hat VMware vom Zweier-Bundle für CPU-Sockel auf lediglich einen Sockel umgestellt. Das heißt, es ist nun problemlos möglich, ein Serversystem mit einer CPU zu lizenzieren, allerdings müssen die Lizenzkosten bei acht Sockeln mit acht multipliziert werden.

Viele Gegner des früheren VI 3-Lizenzservers werden aufatmen, da dieser aus

vSphere verschwunden ist – zumindest in reinen vSphere-Umgebungen. Der Lizenzserver ist einem wesentlich einfacheren Verfahren mit einem Lizenzschlüssel gewichen, der auf den einzelnen ESXi-Hosts eingetragen oder mittels vCenter verwaltet wird. Nur wer weiterhin ESXi 3-Systeme mittels vSphere vCenter verwalten möchte, muss noch einen VI 3-Lizenzserver betreiben und diesen in der vCenter-Konfiguration hinterlegen. Alle VMware-Kunden, die über aktive Wartungsverträge verfügen, versorgt der Hersteller automatisch mit den entsprechenden Lizenzupgrades, was im neuen Lizenzpor-



tal [2] einsehbar ist. Stimmen die dort hinterlegten Daten nicht, sollte VMware kontaktiert werden. Wer Lizenzen nicht blind kaufen möchte, kann alle Produkte auf der Webseite von VMware herunterladen und für 60 Tage testen.

Installation bleibt einfach

Die Installation von vSphere ist nach wie vor sehr einfach und intuitiv gehalten und es haben sich nur wenige Änderungen gegenüber VI 3 ergeben. Im ESX-Umfeld liegt die größte Änderung in der Umstellung auf 64 Bit, die sowohl die Service Console als auch den VMkernel betrifft. Außerdem ist die Service Console bei ESX nicht mehr direkt in den Partitionen der Festplatte verewigt, sondern in einer eigenen vmdk-Festplattendatei auf dem Hersteller-eigenen VMFS-Dateisystem. Natürlich kann alles auch nach wie vor lokal oder im SAN liegen. Vorhandene ESX 3- und ESXi 3-Systeme können zumeist problemlos mit dem VI Host Upgrade Utility, das mit dem vSphere Client installiert wird, auf ESX 4 beziehungsweise ESXi 4 aktualisiert werden. Die VMware-Verwaltung vCenter lässt sich virtuell oder physikalisch installieren, allerdings sind zwei CPUs und 3 GByte Hauptspeicher Pflicht, damit der VMware-Support in vollem Maße greift.

Für sämtliche auf der Installations-DVD verfügbaren Komponenten müssen drei Datenbanken vorgehalten werden, eine für vCenter selbst, eine für den Update Manager und eine für den Orchestrator. Die beiden Komponenten Guided Consolidation und Converter kommen ohne Datenbank aus. All diese Komponenten lassen sich auf einem einzigen System installieren oder auf getrennten Systemen mit jeweiligem Zugriff auf den vCenter Server.

Der Client der VMware-Verwaltung nennt sich jetzt vSphere Client und kann zur Verbindung mit einem ESX- oder ESXi-Host oder einem vCenter Server genutzt werden. Ist bereits ein älterer VI-Client

vorhanden, so koexistieren beide Client-Programme friedlich nebeneinander. Diese Kombination ist sogar nötig, wenn VI 3 und vSphere gleichzeitig verwaltet werden sollen.

Intuitive Konfiguration und Verwaltung

Wie von VMware bekannt, ist die Konfiguration der ESX- und vCenter-Systeme sowie die Anlage und Nutzung der virtuellen Maschinen sehr einfach und intuitiv zu bewerkstelligen. Allerdings täuscht diese Tatsache über die wirkliche Komplexität der virtuellen Infrastruktur hinweg. Während kleine Umgebungen meist kein Problem darstellen, sind mittlere und größere Installationen sehr komplex und erfordern umfangreiches Wissen im Server-, Netzwerk-, Storage- sowie Applikationsbereich. Dass virtuelle Infrastrukturen unter vSphere sehr umfangreich ausfallen können, das beweisen die unterstützten Konfigurationsmöglichkeiten für Host, Storage, Netzwerk und die virtuellen Maschinen.

Damit erobert sich VMware definitiv die Krone der Möglichkeiten virtueller Hardware zurück. Allerdings sind viele der Maximalkonfigurationen vor allem für kleinere Kunden nicht wirklich interessant. Weiterhin ist es möglich, mehrere vCenter mittels Linked vCenter-Modus in einer Konsole zusammenzufassen, was viele Großkunden sehr freuen wird.

Die Berechtigungsstruktur von vCenter war bereits unter VI 3 sehr umfangreich und vorbildlich, hat sich aber unter vCenter nochmals verbessert. So sind neue Rollen und Berechtigungen hinzugekommen. Es ist nun möglich, auch Netzwerken oder Datastores eigene Berechtigungen zuzuweisen. Mittels Kommandozeilenwerkzeugen wie der vSphere-CLI oder der PowerShell-Integration PowerCLI sind tägliche Administrationsarbeiten und Auswertungen per Skript realisierbar. Die vSphere-CLI ist neben Windows und Linux als virtuelle Appliance im OVF-Format verfügbar und lässt

sich daher sehr schnell in die virtuelle Infrastruktur als vMA (Virtual Management Assistant) integrieren.

Wer auf der Suche nach einer weit umfangreicheren Möglichkeit ist, welche die internen Prozesse und Tätigkeiten als Workflows – beispielsweise mit Berechtigungs- und Genehmigungsverfahren – in der virtuellen Infrastruktur interaktiv oder zeitgesteuert ausführt, ist beim Orchestrator richtig. Dieser wird direkt bei der vCenter Installation mit aufgespielt und muss danach nur noch konfiguriert und auf die jeweiligen Bedürfnisse angepasst werden. Bedauerlicherweise ist dieses Produkt im Gegensatz zu den anderen Komponenten wie dem Update Manager oder Data Recovery nicht ins vCenter-Management integriert und dürfte aufgrund der hohen Komplexität eine deutliche Hürde für die meisten Administratoren darstellen. Ohne externe Berater werden sich wohl die wenigsten Kunden mit dem Orchestrator zurechtfinden.

Wenn Sie sich mit der Einführung von oder der Aktualisierung auf vSphere 4.0 auseinandersetzen, dann sollten Sie in jedem Fall die zu verwendende Hardware evaluieren und deren Zertifizierung im Kompatibilitäts-Wegweiser von VMware [3] überprüfen.

Unser Testaufbau bestand aus einem Storage-System NetApp FAS2020 mit vier GBit-Anschlüssen (NFS + iSCSI) und zwei 4-Gbit-Fibre Channel-Anschlüssen. Daher waren als Protokolle zu den HP DL385 G5 Servern NFS, iSCSI und Fibre Channel möglich. Die Netzwerke waren über Ciscos Catalyst 2950 mit 48 Ports und Brocades SilkWorm angebunden und jeweils redundant ausgelegt. Auf jeweils einem Serverpaar haben wir VMware ESX 4 und VMware ESXi 4 installiert. Zuvor war auf jeweils einem der Server ESX 3.5 bzw. ESXi 3.5 installiert. Diese Server aktualisierten wir mittels Host Upgrade Utility und Update Manager. Wir verbanden uns hierzu über das Microsoft Remote Desktop Protocol (RDP) auf einen Windows 2003-Client, von dem aus der weitere Zugriff auf die Server- und Storage-Systeme sowie die Netzwerkkomponenten erfolgte.

Systemvoraussetzungen



STORE. SHARE. PROTECT.

Plattformunabhängige Business Storage Lösungen



Brandneue Advanced Network Speicher für kleine und mittlere Firmennetzwerke

Die NETGEAR ReadyNAS® Produktreihe bietet höchstqualitative und dabei günstige Speicherlösungen: Von Desktop-Geräten der Serien **ReadyNAS NVX** und **ReadyNAS PRO** über die Rackmount-Produkte **ReadyNAS2100** bis zum **ReadyNAS3200** mit 12 Festplatten-Slots und bis zu 24 TB Kapazität

- Hochleistungsspeicher für kleine Unternehmen oder Abteilungen
- Gleichzeitiger Support für die NAS- und SAN-(iSCSI)-Funktionalität
- Dual Gigabit Ethernet ports mit load balancing und failover
- Zuverlässige, automatische Datensicherung mit der Option zum externen Speichern: ReadyNAS Vault bietet HighEnd-Online-Speicherung mit 128 Bit SSL-Verschlüsselung
- Plattformübergreifender Support für Windows®, Macintosh® und UNIX®/Linux Systeme
- Einfach in der Administration und erstaunlich energieeffizient
- 5 Jahre Hardware-Garantie

ReadyNAS NVX: Desktop, 4 Slots

- Drei USB 2.0 ports | RAID 0, 1, 5, X-RAID2

ReadyNAS Pro: Desktop, 6 Slots

- Drei USB 2.0 ports | RAID 0, 1, 5, 6, X-RAID2 | DHCP Server und Printserver

ReadyNAS2100: Rackmount, 4 Slots

- Drei USB 2.0 ports | RAID 0, 1, 5, X-RAID2 | X-CHANGE – Schnellwechselsystem für boards

ReadyNAS3200: Rackmount, 12 Slots, bis zu 24 Terabyte

- Redundante Energieversorgung | Zwei USB 2.0 Ports | iSCSI | RAID 0, 1, 5, 6, X-RAID2



ReadyNAS®
Vault™

ReadyNAS Vault (optional) sichert Daten zusätzlich auf einer webbasierten HighEnd-Storage-Farm. Voller Zugriff auf Ihre Daten von jedem Internetzugang – 128 Bit SSL gesichert.



NETGEAR®
Connect with Innovation™

www.netgear.de/ReadyNAS

Wichtige Funktionen im Überblick

Viele Funktionen haben wir bereits erwähnt, allerdings möchten wir auf die wichtigsten und die am meisten beworbenen Funktionen beim Betrieb einer virtuellen Infrastruktur genauer eingehen.

Kein Ausfall durch Fault Tolerance

Als Erstes sei hier Fault Tolerance (FT) genannt, eine Funktion, die es ermöglicht, virtuelle Maschinen doppelt und aktuell vorzuhalten. Beim Ausfall des Systems wird der Doppelgänger so schnell aktiv geschaltet, dass der Anwender nichts von der Downtime merkt. Technisch ein weiterer Schritt, der die fantastischen Funktionen durch die Virtualisierungsschicht und die damit einhergehende Hardware-unabhängigkeit aufzeigt. Trotzdem lässt sich über den Nutzen im Unternehmen streiten und ist es eine genaue Überlegung wert, welche Systeme in diesem Maße schützenswert sind, da dies mit einer Mehrbelastung und Mehrkonfiguration der ESX-Hardware einhergeht. Außerdem müssen die genutzten Prozessoren im Hostsystem sehr aktuell sein, damit FT funktioniert: Prozessoren der Intel-Serie 31xx, 33xx, 52xx, 54xx, 74xx oder AMD-Prozessoren der Serie 13xx, 23xx, 83xx sind mögliche Chipsätze. FT benötigt einen korrekt konfigurierten High Availability-Cluster, der sich darum kümmert, die virtuellen Maschinen ausgefallener Hostsysteme auf den übrigen ESX Systemen innerhalb des Clusters neu zu starten. Durch die Option VM Monitoring ist es möglich, virtuelle Maschinen automatisch neu zu starten, falls deren Heartbeat nicht mehr zu vernehmen ist, etwa durch einen Windows-Bluescreen.

Durchdachtes Ressourcen-Management

Bei zusätzlich im Cluster aktiviertem DRS (Distributed Resource Scheduler) werden die virtuellen Maschinen aufgrund der analysierten CPU- und Memory-Werte mittels VMotion optimal auf den Host-Systemen im Clusterverbund verteilt. Die DRS-Erweiterung DPM (Distributed Power Management) kann zudem die physikalischen Ressourcen

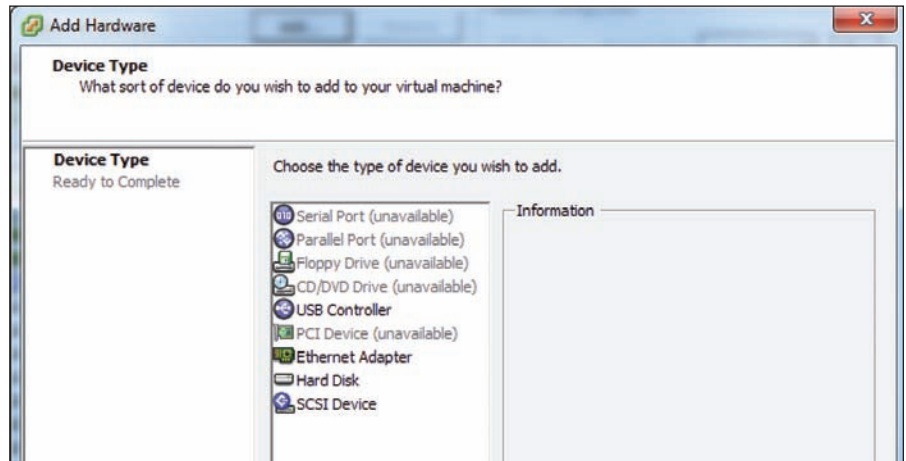


Bild 3: vSphere verfügt über wesentlich mehr Möglichkeiten, virtuelle Hardware bei einer laufenden VM hinzuzufügen

ausnutzen, um nicht benötigte Hostsysteme stromsparend in einen Standby-Modus zu versetzen. Sobald die Ressourcen der abgeschalteten Systeme wieder benötigt werden, fährt DPM diese automatisch wieder hoch.

Die Funktionen der vorherigen Generationen 2 (VMotion) und 3 (Storage VMotion) sind weiter verbessert und die CPU-Kompatibilität ist dank EVC (Enhanced VMotion Compatibility) erhöht worden. Identische CPUs sind nicht mehr zwingende Voraussetzung, wenn auch nach wie vor nicht alle Konfigurationen abgedeckt werden. Storage VMotion hat eine grafische Oberfläche erhalten, die unter VI 3.5 vielen VMware Anwendern gefehlt hat. Im Endeffekt lassen sich unter vSphere nun grafisch unterstützt aktive virtuelle Maschinen zwischen Hostsystemen und Storage-Systemen migrieren, ohne dass es zum Ausfall kommt.

Eine sehr ansprechende Funktion stellen die Host Profiles dar, welche die Speicherung aller Konfigurationsdaten eines Hostsystems in Profilen unterstützen. Diese Profile lassen sich zur Prüfung der Hostsysteme auf Gleichheit nutzen und es ist möglich, bestehende Hostsysteme mittels Host Profiles zu konfigurieren. So kann ein ESX-Host mittels Installationsmedium rudimentär installiert werden und die Konfiguration findet mittels Host Profile dann schnell und einfach statt.

Backup und Recovery für VMs mit Bordmitteln

Als Sicherheitszentrale verfügt vSphere über vShield Zones für die Hostsysteme, eine Kombination aus Verwaltungs-Appliance und Firewall Appliances, die den Datenverkehr zwischen den virtuellen Maschinen auf den Hostsystemen kontrollieren und einschränken. Außerdem hat der Hersteller eine VMsafe-Schnittstelle entwickelt, die es Virenschutzherstellern erlaubt, den gesamten Datenverkehr der virtuellen Maschinen zu überwachen, ohne dass dazu eine Gastagenteninstallation notwendig ist. Bezüglich der Datensicherheit existiert nun eine Backupschnittstelle (vStorage API for Data Protection) für Dritthersteller, die das Consolidated Backup Framework (VCB) ersetzt. VCB wird in der jetzigen Version allerdings auch weiterhin mit vSphere funktionieren.

Die größte Änderung ist VMware Data Recovery, eine Appliance, die sich direkt ins VMware Management integriert und die Sicherung und das Wiederherstellen von virtuellen Maschinen unterstützt. Eher unerwartet greift VMware damit Lösungen der Unternehmen vizoncore (vRanger) und Veeam (Backup & Replication) stark an. Trotz Versionsstand 1.0 ist diese eigene Recovery-Lösung bereits sehr gelungen und integriert sich perfekt in die virtuelle Infrastruktur. Einige Bugs, vor allem beim Restore der VMs in bestimmten



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

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

Getestet im Datacenter on Demand



Situationen, trüben den sehr guten Eindruck etwas. Allerdings wurden hier bereits Bugfixes veröffentlicht. Sehr interessant ist die bereits integrierte Deduplizierungs-Funktion, welche die Datenmenge deutlich minimiert, da redundante Dateien nicht mehrfach vorhanden sind. Die benötigte Sicherungskapazität ist damit deutlich geringer.

Thin Provisioning und Distributed Switches

Ebenso hat sich im Storage- und Netzwerkumfeld einiges getan. Zwar werkeln viele Funktionalitäten eher im Hintergrund, allerdings sind auch direkt sichtbare Änderungen erfolgt. Im Storage-Umfeld handelt es sich hier um die Softwareversion des Thin Provisioning (TP), was Nutzer von VMware Workstation und VMware Server bereits als dynamisch wachsende Festplatten kennen. Kurz gefasst sind virtuelle Festplatten mit TP immer nur so groß wie die darin abgelegten Daten. Während eine 10 GByte Festplattendatei (vmdk) beim iSCSI- und FC-Einsatz unabhängig der wirklichen Nutzung immer 10 GByte groß war, so belegt eine TP-Platte genau 5 GByte, wenn nur 5 GByte der ursprünglich vorgesehenen 10 GByte genutzt werden.

Im Netzwerkumfeld sind klar die Distributed Switches im Vordergrund, die zentral im vCenter angelegt (maximal 16) und den ESX Hosts zugeteilt werden können.

Dadurch entfallen lästige Fehlerquellen wie die Benennung der bisher bekannten (und natürlich nach wie vor verfügbaren) virtuellen Switches und Portgruppen. Diese führten bei inkonsistenten Namen und Zuordnungen zwangsweise zu Problemen bei VMotion, DRS und HA.

Allerdings bietet die vNetwork Distributed Switch-Funktion weitaus mehr als nur gleiche Konfigurationen über die Hosts, so dass nun ein- und ausgehende Pakete auf Traffic Shaping und Security getrimmt werden können und neben den VLANs auch die neue Erweiterung "Private VLANs" genutzt werden kann. Zu guter Letzt bieten die Distributed Switches Möglichkeiten für Dritthersteller, eigene virtuelle Switches zu integrieren, was Cisco mit dem Nexus 1000v bereits realisiert hat. Dadurch ist das Netzwerkteam in der Lage, neben den physikalischen Cisco Switches die virtuellen Nexus Switches zu verwalten und somit den Serveradministrator zu entlasten.

Mehr Möglichkeiten für virtuelle Maschinen

Die virtuellen Maschinen haben neben deutlicher Erhöhung der Hardwarelimits auch funktionelle Verbesserungen erfahren. So sind etwa die Performancewerte der virtuellen Maschine nun mittels VMware-Tools im Windows Gast mit Hilfe von *Perfmon* einsehbar. Zudem lassen sich Eventmeldungen wesentlich bes-

ser auslesen und umfangreiche Alarmer definieren. Deutlich erweitert präsentiert sich die Liste der unterstützten Gastbetriebssysteme, so dass nun volle Unterstützung für Windows 2008 inklusive Gastanpassung bei Kloning sowie für Debian herrscht.

Nutzer von vSphere können virtuelle Maschinen nun in vAPPs integrieren, eine Sonderform des Resource Pools. Diese erlaubt es, virtuelle Maschinen zu gruppieren und mit zentralen Konfigurationen (Ressourcen, IP Adressen, Eigenschaften) auszustatten. Diese vAPPs sind per OVF (Open Virtual Machine Format) mobil und in andere virtuelle Infrastrukturen – Stichwort Cloud – importierbar. Damit ist es möglich, Applikationen, die aus mehreren virtuellen Servern bestehen, in einer vAPP zu verwalten, zu aktualisieren und zu betreiben.

Migration

Das vCenter-Upgrade, das vor den ESX Server-Upgrades durchgeführt werden sollte, lief im Test problemlos durch und die Integration der ESX 3.5-Systeme war nach der Übernahme des VI 3-Lizenzservers direkt möglich. Zur Migration der ESX-Server stehen neben dem manuellen Upgrade mittels Installations-DVD zwei weitere Werkzeuge zur Verfügung: vSphere Host Upgrade Utility und Update Manager. Während das Host Upgrade Utility als Standalone-Komponente mit dem

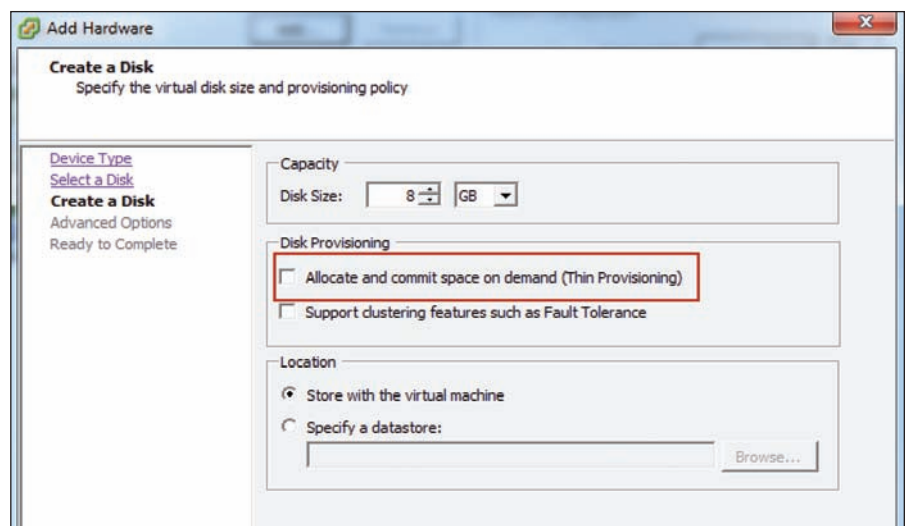


Bild 4: Um Kapazitäten einzusparen, können bei vSphere die virtuellen Festplatten mit den Daten wachsen



vSphere-Client einhergeht, ist der Update Manager als zentrale Instanz nutzbar, die auf Wunsch zeitgesteuerte Upgrades durchführt. In beiden Fällen wird die Installations-DVD geladen und auf den ESX-Host übertragen, wo danach automatisch die Aktualisierung stattfindet. Außerdem gibt es einen Rollbackmodus, der bei fehlgeschlagenem Upgrade automatisch das alte ESX-System wieder startet.

Die Migration verlief während des Tests zumeist problemlos und nur einen Migrationstest mussten wir mittels Host Upgrade Utility manuell nachziehen. Durch den Rollback Modus kam es aber zu keinem Datenverlust oder einem Gang ins Rechenzentrum. Ebenso verliefen die Aktualisierung der VMware Tools und die anschließende virtuelle Hardwaremigration von Version 4 (VI 3) auf Version 7 (vSphere) reibungslos, sowohl manuell als auch mit der neuen Funktionalität des Update Managers. Wer physikalische Systeme oder virtuelle Maschinen aus anderen Produkten migrieren will, dem hilft dabei der Dienst "Guided Consolidation", der eine Analyse der Systeme auf Integration in VMware durchführt, und der VMware Converter, der die Migration der Systeme in die vSphere Umgebung im aktiven (per Agent) oder abgeschalteten Zustand (per Boot-CD) automatisch durchführt.

Alte Drittanbieter-Tools nicht immer kompatibel

VMware Kunden, die recht zügig auf vSphere wechseln möchten, sollten sich darüber im Klaren sein, dass noch nicht alle Zusatzprodukte von Drittherstellern und

von VMware selbst kompatibel zu vSphere sind. Da wären derzeit die beliebten Produkte VMware View zur Virtualisierung von Desktops und deren Verwaltung, VMware Site Recovery Manager zur Verwaltung eines Ausfallrechenzentrums und des Tests beziehungsweise der Liveschaltung im Ausfall und das Verwaltungsprodukt Stage Manager. Lifecycle Manager und Lab Manager stehen seit August dieses Jahres mit vSphere-Support zur Verfügung.

Fazit

Uns erschien der Test wie eine kleine Zeitreise, da sich sehr vieles geändert hat oder hinzugekommen ist. Daher konnte dieser Test auch nicht alle Funktionen ausführlich behandeln. Gleichzeitig müssen wir die Änderungen aber etwas relativieren, da einige der Funktionen nur mit den großen und kostspieligen Editionen zur Verfügung stehen. So ist es letztendlich von der gekauften Edition abhängig, wie viel Erfahrung und neues Wissen notwendig ist, um vSphere optimal zu bedienen. Kleinere Unternehmen werden mit den Essentials Editionen vorliebnehmen und damit nur sehr wenige Funktionen nutzen. Unternehmen, die auf die Advanced oder Enterprise Plus Editionen setzen, können sich allerdings bereits auf massive Schulungsmaßnahmen vorbereiten. Die Änderungen zwischen VI 3.5 und vSphere sind einfach enorm.

In jedem Fall ist es VMware durch die wesentlich verbesserte Verwaltungsoberfläche, allen voran durch das vCenter, gelungen, die Administration deutlich zu erleichtern. Mittels neuer Alarme, Update Manager-Erweiterungen und Data Recovery-Integrationen kommen Überwachung, Backup und Restore sowie Migrationsthemen aus einer Hand. Diese Aspekte betreffen wohl den Großteil der VMware-Kundschaft und bringen diesem viel Nutzen. Die neuen Hype-Funktionen wie Hot-Add-Hardware, Fault Tolerance, Storage VMotion, Distributed Switches oder Host Profiles sind erst in den teureren Versionen verfügbar und bieten sich so eher für den gehobenen Mittelstand und Großunternehmen an. (In) 

Produkt

Software zur Verwaltung von virtualisierten Umgebungen.

Hersteller

VMware
www.vmware.de

Preis

Der Hersteller lizenziert vSphere über Prozessorsockel. Abhängig von der genutzten Edition steigt der Preis pro CPU Sockel an. In der Enterprise Plus-Edition etwa schlägt ein Prozessor mit 3.495 US-Dollar ohne Support zu Buche. Es existieren zwar Preise auf der Webseite von VMware, allerdings sind nur die Dollar-Preise korrekt eingetragen. Die Euro-Preise des deutschen Portals sind teils fehlerhaft umgerechnet. Daher sollten Sie einen Wiederverkäufer Ihrer Wahl ansprechen, um die besten Kaufoptionen zu erfahren.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für Unternehmen, die produktive Infrastrukturen ausfallsicher und mit möglichst viel Bedienkomfort virtualisieren möchten. Die meisten Vorteile können mittelgroße und große Unternehmen aus allen Funktionen ziehen.

bedingt für Unternehmen, die nur kleine Virtualisierungsinfrastrukturen betreiben, diese aber trotzdem kostengünstig ausfallsicher halten möchten.

nicht für Unternehmen, die keine Virtualisierung nutzen oder einführen möchten oder bereits mit der bestehenden Virtualisierungslösung sehr zufrieden sind und keinen Wechsel wünschen. Weiterhin zählen sehr kleine Unternehmen mit bis zu fünf Servern nicht zum Zielpublikum.

vSphere 4.0

[1] Editionsübersicht VMware vSphere 4.0

www.vmware.com/products/vsphere/buy/editions_comparison.html

[2] Lizenzportal von VMware

www.vmware.com/support/licensing.html

[3] Übersicht zu VMware-kompatibler Hardware

www.vmware.com/go/hcl/

Links



DURCHDACHT BIS INS LETZTE DETAIL.



Leistungsstark.
Intelligent.



DER NEUE PRIMERGY RX200 S5

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

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

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

Intel, das Intel Logo, Xeon und Xeon Inside sind Marken der Intel Corporation in den USA und anderen Ländern.

FUJITSU

**Im Test: Synology DS209+II NAS-System**

Kompakter Netzwerkspeicher

von Christian Knemann



Für kleine und mittlere Umgebungen sind NAS-Speicher meist das Storage der Wahl. Sie lassen sich unkompliziert ins Netzwerk integrieren und stellen Arbeitsgruppen oder einzelnen Mitarbeitern Daten zur Verfügung. Mit der NAS-Box "DS209+II" bietet Synology ein solches kompaktes Speichersystem an. Im IT-Administrator-Test konnte das Gerät zeigen, was in ihm steckt.

Der taiwanische NAS-Spezialist Synology [1] bietet mit der DiskStation-Familie eine breite Produktpalette, beginnend beim Ein-Festplatten-System für Privatanwender bis hin zu erweiterbaren Rack-Geräten für den Einsatz im Rechenzentrum. In der Nomenklatur der Modelle steht die erste Ziffer für die Anzahl möglicher Festplatten, gefolgt von zwei Ziffern für das Modelljahr. Mit der "DiskStation DS209+II" fand die neueste Servergeneration für zwei Festplatten in unsere Testumgebung. Das Gerät passt mit Abmessungen von 22 x 15 x 9 cm auf sowie unter jeden Schreibtisch. Es ist ausgestattet mit einer 1.06 GHz PowerPC-CPU und 512 MByte RAM. Eine USB 2.0- und eine eSATA-Schnittstelle finden sich an der Vorderseite des Gehäuses, zwei weitere USB 2.0 Ports, GBit-Ethernet sowie der Anschluss für das externe Netzteil auf der Rückseite. Intern können zwei 3,5-Zoll-SATA Festplatten untergebracht werden, wahlweise mittels mitgelieferter Adapterrahmen auch 2,5 Zoll-HDDs.

Wir verbauten 3,5 Zoll-Platten vom Typ "Samsung SpinPoint P80SD" mit jeweils 160 GByte und 7.200 Umdrehungen pro Minute. Die Montage gelang schnell und unkompliziert. Dazu mussten wir lediglich die obere Hälfte des Gehäuses nach vorne schieben und abnehmen. Die Fest-

platten wurden im Inneren konventionell mit jeweils vier Schrauben in einem Metallrahmen fixiert und verkabelt. Hot-swap-fähige Festplatteneinschübe, die extern zugänglich sind, bieten erst die größeren NAS-Systeme ab vier Platten. Anschließend wurde die Abdeckung wieder geschlossen und mit zwei Schrauben

arretiert. So gerüstet konnten wir die Box in Betrieb nehmen, die vom DHCP-Server mit einer IP-Adresse versorgt wurde.

Übersichtliches Management

Der Erstkontakt erfolgt über einen grafischen Assistenten, der auf der mitgelieferten CD für Windows und Mac OS X ent-



Bild 1: Die Ersteinrichtung über den Assistenten gelingt mit wenigen Klicks

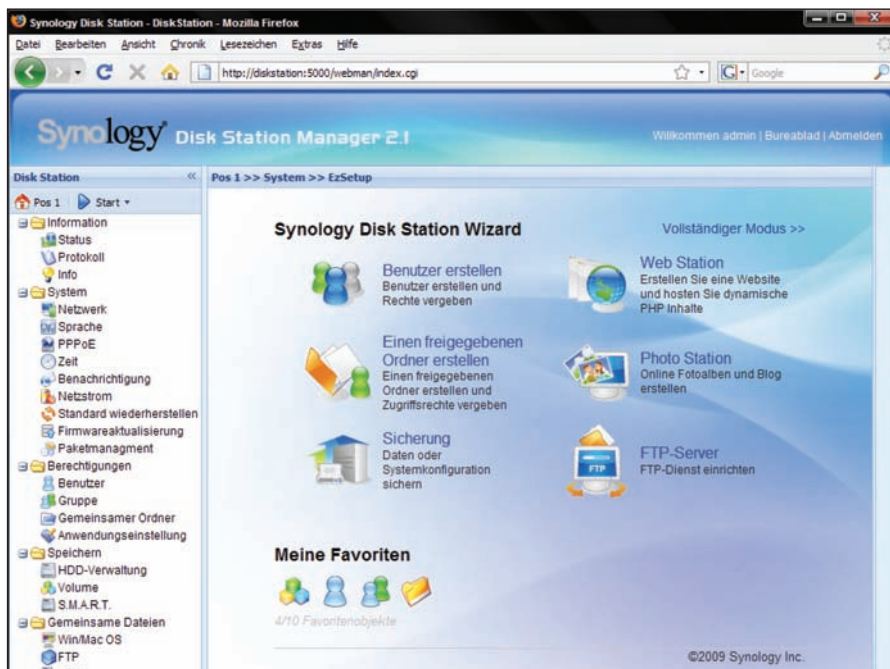


Bild 2: Die Management-Oberfläche verhält sich dank AJAX fast wie eine Windows-Applikation

halten ist. Unter Windows erlaubt das Autorun-Menü den Zugriff auf die Dokumentation. Weiterhin ist es möglich, den Assistenten direkt von der CD zu starten oder lokal zu installieren, wobei der Windows-Firewall automatisch eine Ausnahme hinzugefügt wird. Unter Mac OS X mussten wir dagegen zunächst manuell eine Ausnahme in der Firewall eintragen. Zusätzlich stehen der Backup-Client "Data Replicator 3" und der "Download Redirector" zur Auswahl. Letzterer delegiert Downloadaufträge vom Client an das NAS-System. Wir installierten die drei Tools auf einem Windows XP SP3-Client und starteten den Assistenten, der die Box automatisch fand und einrichtete. Beim "Setup per Mausklick" geht das Gerät vollautomatisch unter dem Namen "DiskStation" per DHCP in Betrieb, "Schrittweises Setup" erlaubt, die Netzwerkkonfiguration manuell vorzunehmen sowie Datum und Zeitzone zu setzen. Das ist aber auch später noch möglich. Wir entschieden uns für die einfache Installation, die nur wenige Minuten Zeit in Anspruch nahm. Anschließend konnten wir aus dem Assistenten heraus über den Button "Verwalten" den web-basierten "Disk Station Manager 2.1" starten. Es handelt sich da-

bei um eine in AJAX realisierte und für alle Synology-Modelle einheitliche Management-Oberfläche, die im Test ohne Probleme sowohl im Internet Explorer 8.0 als auch im Firefox 3.0 sowie Safari ihren Dienst verrichtete.

Sämtliche Optionen sind am linken Fensterrand in einer Ordnerstruktur gruppiert, häufig benötigte Optionen lassen sich per Drag & Drop als Favoriten auf die Startseite ins Hauptfenster ziehen. Unter "Information" teilt die DiskStation ihren aktuellen Status mit. Dies umfasst unter anderem Betriebszeit, Systemtemperatur, insgesamt belegten Speicherplatz, Netzwerkkonfiguration sowie Status und Temperatur der einzelnen Festplatten. Im Bereich "Protokoll" informieren mehrere Kategorien über vergangene Ereignisse wie Systemmeldungen, Verbindungen, FTP-Zugriffe oder Sicherungsvorgänge. Im Ordner "System" sind sämtliche systemnahen Einstellungen zusammengefasst, so die Netzwerkkonfiguration und die Spracheinstellungen für die Oberfläche und E-Mails.

Die DiskStation erweist sich als Sprachta-
lent und bietet 18 Sprachen an: neben

Deutsch und Englisch unter anderem Französisch, Italienisch, Spanisch, Polnisch und Türkisch. Mindestens für die deutsche Ansicht konnten wir feststellen, dass die Lokalisierung gut gelungen ist. Lediglich der Link "Bureablad" in der Kopfzeile direkt neben dem Abmelde-Button erschloss sich uns nicht sofort. Ein Umschalten auf die englische Ansicht ergab, dass der "Desktop" und damit die Startseite der Admin-Oberfläche gemeint ist. Ein Upgrade auf die neueste Firmware-Version DSM 2.1-0845 beseitigte dieses Problem.

Es finden sich weiterhin die Möglichkeiten, per PPPoE direkt eine Internetverbindung zu initiieren und die Zeit einzustellen, was auch die Kommunikation mit einem externen NTP-Server einschließt. Benachrichtigungen über kritische Ereignisse verschickt die Station an einen SMTP-Server und bis zu zwei E-Mailadressen auch mit vorheriger Authentifizierung und per SSL/TLS gesichert.

Energiespar-NAS

Die Einstellungen im Bereich "Netzstrom" tragen dem gestiegenen Umweltbewusstsein Rechnung. So lassen sich die internen Festplatten nach einer vorgegebenen Frist in den Ruhezustand versetzen. Zur Auswahl stehen 10, 15, 20 und 30 Minuten sowie eine bis fünf Stunden. Gleiches gilt für extern angeschlossene USB-Platten. Es ist außerdem möglich, die Station zeitgesteuert automatisch aus- und wieder einzuschalten. Die Zeitpunkte lassen sich abhängig von Tageszeit und Wochentag definieren. Allerdings lassen sich keine verschiedenen Zeiten für unterschiedliche Wochentage festlegen. Soll die Station außerhalb des Zeitplans aufwachen, hilft nur der Schalter an der Gehäusefront – Wake-on-LAN beherrscht das Gerät nicht.

Der Hersteller gibt den durchschnittlichen Stromverbrauch mit 30 Watt bei Zugriffen, 28 Watt im Leerlauf sowie 14,4 Watt im Ruhezustand der Festplatten an. Unsere im Test gemessenen Werte lagen geringfügig darüber mit einer Wirkleistung von 33 Watt bei laufenden Datei-

Wer zieht die Grenzen eines Unternehmens – die Mitarbeiter oder die IT?

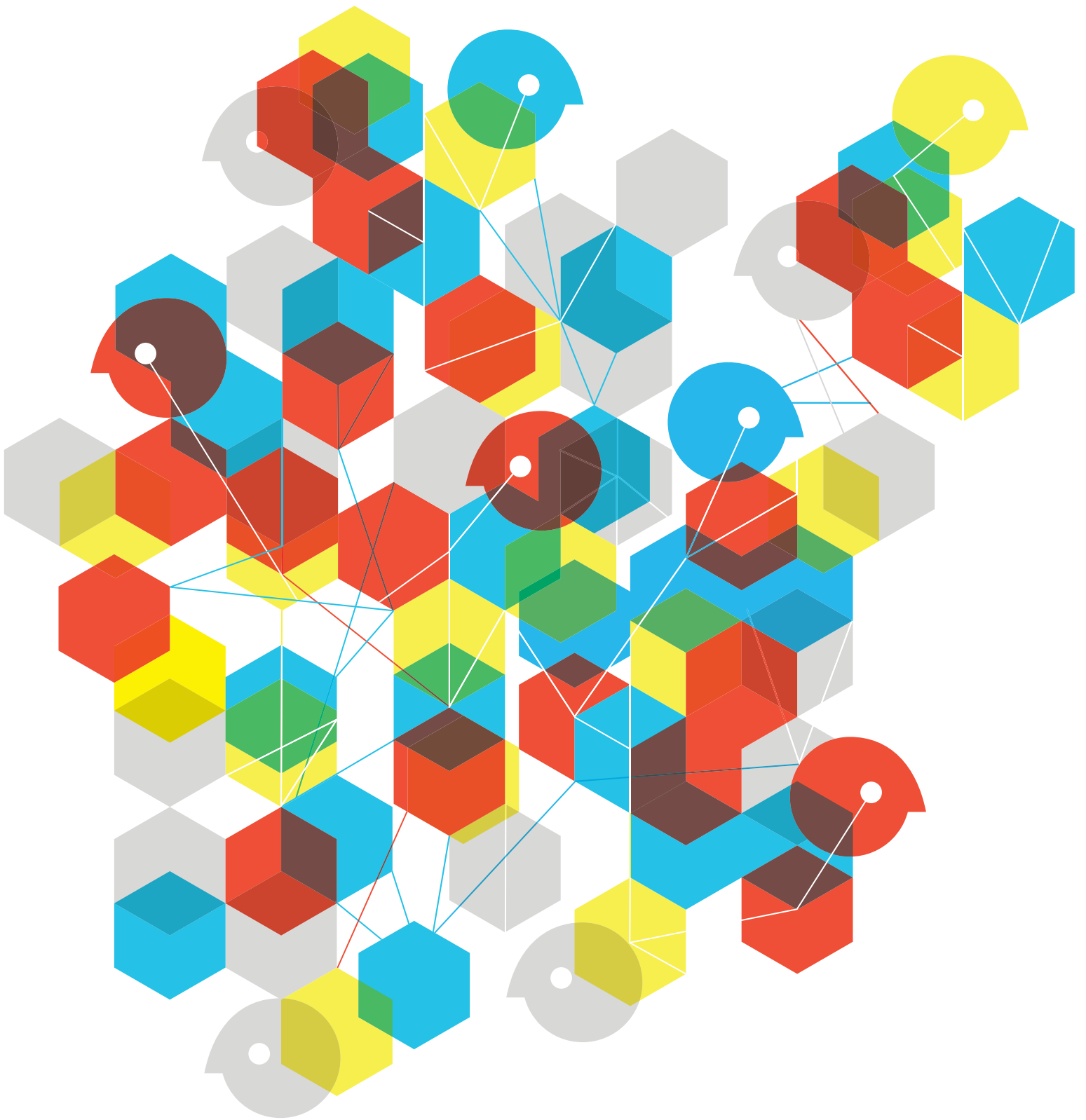
Unternehmen kontrollieren gerne, wer bei ihnen ein und aus geht – bei ihren Gebäuden ebenso wie bei ihren Netzwerken. Aber was, wenn man zunehmend mit Menschen zusammenarbeitet, die sich außerhalb solcher Sperren aufhalten: mit Partnern, Zulieferern, Kunden und Mitarbeitern im Außendienst oder Home-Office?

Genau deshalb erweitert IBM das Collaboration-Portfolio um Tools wie Social Software, Wikis, Instant Messaging – und schafft zugleich neue Formen des Zugriffs, z. B. per Cloud Computing. Mit Cloud-basierten Lösungen wie LotusLive spielt es keine Rolle mehr, auf welcher Seite einer Firewall sich einzelne Mitglieder eines Teams befinden. Alle können ungehindert zusammenarbeiten, und zwar auf dem hohen Sicherheitsstandard, den sie von IBM gewohnt sind.

Anders ausgedrückt: Sie können das Teamwork in und um Ihr Unternehmen nahtlos ausbauen, ohne dafür eigens eine kostspielige und komplexe Infrastruktur aufzubauen. Sie müssen Ihre Grenzen nicht einreißen, um über sie hinauszuwachsen.

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





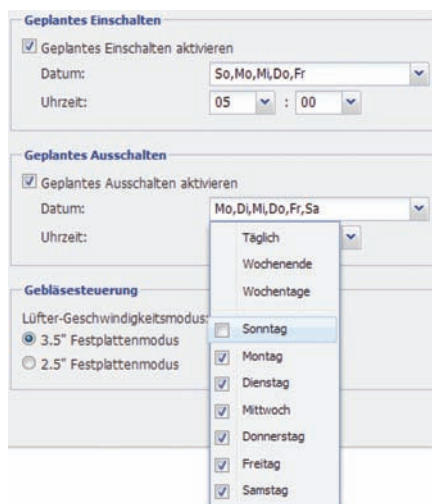


Bild 3: An wählbaren Tagen schaltet sich die Station zeitabhängig ein und wieder aus

operationen. Bei einem Leistungsfaktor von 0,47 (optimal wäre 1) betrug die Scheinleistung 70 VA. Im Leerlauf wurden 30 Watt sowie 20 Watt bei ruhenden Platten gemessen. Die etwas höheren Werte sind natürlich den im Test eingesetzten Platten mit 7.200 Umdrehungen geschuldet. Werden stattdessen im praktischen Betrieb energiesparende Disks, wie die im NAS-Bereich beliebte Western Digital WD10EADS mit 5.400 Umdrehungen, eingesetzt, lässt sich der Leistungsbedarf weiter reduzieren.

Vielfältige Freigaben

Die grundlegenden Arten der Dateifreigabe regelt der Punkt "Gemeinsame Dateien". Standardmäßig sind der Windows-Dateidienst sowie AppleTalk aktiv. Letzteres dient der Unterstützung älterer Macs über das Linux-Paket "Netatalk". Mac OS X-Clients benötigen dies nicht mehr, da sie per SMB zugreifen. Weiterhin stehen FTP, NFS und der webbasierte Zugriff "File Station" zur Verfügung, standardmäßig aber zunächst inaktiv. Wir konfigurierten den Windows-Dateidienst auf die Arbeitsgruppe unserer Test-PCs und fanden das Gerät erwartungsgemäß in der Netzwerkumgebung, natürlich noch ohne Freigaben. Zunächst waren nun die Festplatten zu partitionieren. Dazu erstellten wir unter "Speichern / Volume"

ein Laufwerk, wozu uns die Modi JBOD, RAID 0 und RAID 1 angeboten wurden. Die Modi RAID 5, wahlweise mit Spare, und RAID 6 sind den größeren Modellen vorbehalten und grau unterlegt angezeigt. Wir wählten RAID 1.

Die Verzeichnisse innerhalb eines Volumens lassen sich unter "Berechtigungen / Gemeinsamer Ordner" verwalten. Wir legten testweise mehrere Ordner an, die sich optional in der Netzwerkumgebung verbergen lassen. Dies funktioniert, anders als von Windows File Servern gewohnt, ohne dass der Freigabename mit einem "\$" endet. Die Berechtigungen werden basierend auf lokalen Gruppen oder einzelnen Benutzern vergeben. Zur Auswahl stehen "Lesen / Schreiben", "Nur Lesezugriff" oder "Kein Zugriff". Sofern der NFS-Dienst aktiv ist, können zudem NFS-Berechtigungen auf Basis von Hostnamen oder IP-Adressen der zugreifenden Client-Rechner vergeben werden. Wir legten unter "Berechtigungen / Benutzer" einige Accounts an und wählten deren Namen identisch zu den Anwendern auf unseren Windows-Rechnern in der Arbeitsgruppe. Vergaben wir auch das Passwort identisch, war es uns umgehend möglich, ohne explizite Authentifizierung auf Freigaben der DiskStation zuzugreifen. Die DiskStation fügt sich somit wie ein Windows-Dateiserver in die Arbeitsgruppe ein.

Daraufhin sollte die Station unserer Active Directory Domäne beitreten. Wir konfigurierten dazu unter "Win / Mac OS" den Namen der Domäne und die IP-

Adresse eines Windows Server 2003 R2 Domain Controllers. Nach der obligatorischen Abfrage eines administrativen Domänen-Accounts registrierte sich die DiskStation im AD als Samba 3.0.20b Computer. Unter "Berechtigungen / Benutzer" wurden uns umgehend neben den lokalen auch die Domänen-Benutzer angezeigt. Der "Benutzer-Home-Dienst" erleichtert die Bereitstellung individueller Ordner pro Benutzer, interessant beispielsweise für persönliche Dateien oder Roaming Profiles. In den Privilegieneinstellungen der freigegebenen Ordner konnten wir ebenso Domänen-Benutzer wie auch Domänen-Gruppen mit Zugriffsrechten versehen.

Dienste im Netz

Im Ordner "Netzwerkdienste" lassen sich unter "Webdienste" sämtliche webbasierten Funktionen der Station auf HTTPS umstellen. Dabei bietet sich auch die Gelegenheit, ein eigenes Zertifikat zu importieren, was zu empfehlen ist. Andernfalls kommt es auf Grund des von Synology selbst signierten Zertifikats beim Zugriff per Browser zwangsläufig zu einer Sicherheitswarnung. Mit der Option "Web Station aktivieren" lässt sich die Box als Webserver verwenden. Dabei stehen als Optionen PHP und MySQL zur Verfügung. Anschließend kann die Station unter "DDNS" veranlasst werden, sich bei einem von vier DynDNS-Anbietern zu registrieren. Zur Wahl stehen 3322.org, NoIP.com, Two-DNS.de und DYNDNS.org. Im Bereich "Terminal" lassen sich Telnet- und SSH-Zugang zum System aktivieren. Letzterer ist Voraussetzung, um per SSH File Transfer Protocol (SFTP)

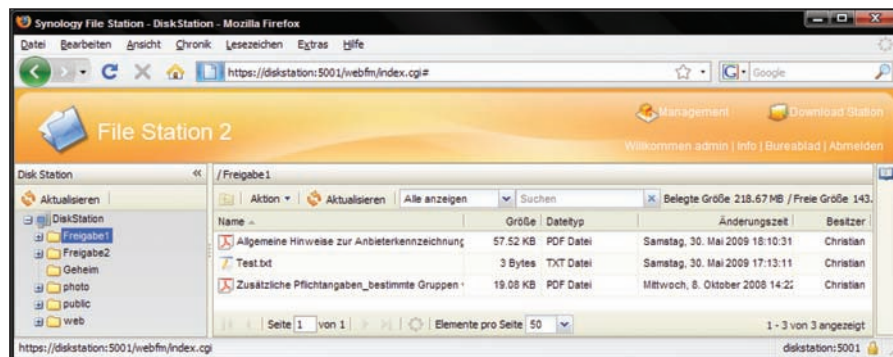


Bild 4: Die "File Station 2" erlaubt Dateioperationen per Browser

mit der DiskStation zu kommunizieren, was diese aber nicht per Default unterstützt.

Um SFTP zu aktivieren, sind einige manuelle Modifikationen am System erforderlich. Das Synology-Wiki [5] erklärt, was zu tun ist. So meldeten wir uns via PuTTY [2] per SSH als "root" am System an, das sich als "BusyBox v1.1.0" entpuppt. Das root-Passwort ist identisch zu dem des Users "admin". Gemäß der Installationsanleitung des Herstellers [3] setzten wir das Itsy Package Management System (IPKG) passend zur PowerPC (ppc_85xx) Architektur unseres Systems auf. Unter [4] ist ein umfangreiches Repository vorkompilierter IPKG-Pakete verfügbar, mit denen sich die Funktionalität der DiskStation erweitern lässt. Gemäß [5] installierten wir die Pakete *zlib* sowie *coreutils* und befolgten die weiteren Anweisungen des Howtos.

Abschließend editierten wir die Datei */etc/passwd* und setzten für ausgewählte Benutzer den Login von *"/sbin/nologin"* auf *"/bin/sh"*. Daraufhin konnten wir, beispielsweise mit dem Client WinSCP [6], per SFTP auf die Station zugreifen und Daten transferieren. Entgegen einem Hinweis im Wiki blieb der Login für unsere Benutzer in der Datei *passwd* auch nach Änderungen der Benutzerrechte über die Weboberfläche erhalten und wurde nicht überschrieben. Das Wiki weist aber richtig darauf hin, dass durch die entsprechende Modifikation ein potenzielles Sicherheitsrisiko entsteht, da sich Benutzer neben dem SFTP-Zugriff zwangsläufig auch direkt am System anmelden und auf das Dateisystem zugreifen können. Unser Ausflug auf die Kommandozeile diente entsprechend hauptsächlich dem Zweck, das Potenzial der Disk-

Station für Erweiterungen aufzuzeigen. So finden sich online viele weitere Pakete, wie der DNS Forwarder und DHCP-Server "Dnsmasq", ein Freeradius-Server sowie zahlreiche Module für PHP und Perl. Bei Modifikationen des Systems hilft neben dem Wiki das aktive Forum [7].

Wer davor zurückschreckt, selbst Hand anzulegen, findet unter "Gemeinsame Dateien / FTP" die Option "Nur SSL/TLS-Verbindung erlauben". Ist diese aktiv, kann als Alternative zu SFTP/SCP der ebenfalls verschlüsselte Dateitransfer via "FTP über TLS" mit expliziter Verschlüsselung zum Einsatz kommen. Eine weitere Alternative ist die "File Station 2", zu aktivieren unter "Gemeinsame Dateien", die den Zugriff auf das Dateisystem via Browser erlaubt.

Backup mit Synchronisierung

Mit dem "Data Replicator 3" können Nutzer Verzeichnisse von Windows-Clients auf eine Freigabe der DiskStation sichern. Dabei stehen drei Modi zur Auswahl. Der Punkt "Sofort" sichert die gewählten Verzeichnisse einmalig. "Zeitplan" führt regelmäßige Sicherungen durch, während "Sync" die Verzeichnisse dauerhaft überwacht. Dabei werden sämtliche Änderungen umgehend auf die DiskStation repliziert. Es ist einstellbar, ob beim Löschen des Originals auch das Replikat gelöscht werden soll. Weiterhin kann das Gerät eine definierte Anzahl an vorherigen Versionen erhalten. Dabei findet sich der aktuelle Stand der Synchronisation im Ordner "latest". Im Ordner "past" landen die alten Versionsstände. Dabei kommen in der Verzeichnisstruktur allerdings keine symbolischen Links zum Einsatz. Im Ordner "past" wird stattdessen eine identische Ordnerstruktur erzeugt, in die nur ältere Stände von Dateien kopiert werden, die sich im aktuellen Bestand tatsächlich geändert haben.

Wie der Name schon vermuten lässt, eignet sich der "Data Replicator 3" nur für dateibasierte Sicherungen. Vollständige Backups der Windows-Clients mitsamt Systemstatus und der Restore der Clients

Das im Howto referenzierte Paket *openssh_5.1p1-1_powerpc.ipk* ist nicht mehr im Repository verfügbar. Stattdessen muss die neuere Version *openssh_5.2p1-1_powerpc.ipk* per wget heruntergeladen werden.

Hinweis



OBERN
KOPF
UNTEN
NAS*

*Wahrscheinlich haben Sie schon eine übergroße Stirn entdeckt. Die zuverlässigere Storage-Lösung im Unternehmen: Professionelle Netzwerkspeicher (NAS), die u.a. CIFS/SMB, NFS, FTP, HTTP und RSYNC verstehen.



exonas 200 R2 Serie

80MB/s
über einen
Gbit Port
per SMB

- Netzwerkspeicher mit bis zu 12TB auf 2 HE
- 4x Gigabit mit Link Aggregation und Fail Over
- Intel Dual Core CPU, Intel Serverchipsatz, 4GB RAM
- Snapshots, Deduplizierung (Single Instance Storage)
- Windows Storage Server 2008 auf zusätzlichem RAID1
- Pro-Service mit Express-Vorabtausch



exonas 200 R2 Windows
mit 8TB

3135**

Sonderpreis bis 31.10. (statt 3244**)

exonas 300 R2 Serie

- Netzwerkspeicher mit bis zu 24TB auf 3 HE
- 2x Gigabit mit Link Aggregation und Fail Over
- Intel Xeon CPU, Intel Serverchipsatz, 4GB ECC RAM
- Hardware-RAID-Controller
- redundantes Netzteil (800W)
- iSCSI, Active Directory Integration
- scheduled und manuelle Snapshots
- mit Windows, Open-E oder Openfiler
- Pro-Service mit Express-Vorabtausch



exonas 300 R2 Openfiler
mit 24TB

5382**

Sonderpreis bis 16.10. (statt 5612**)



xtivate

Storage und Netzwerkzubehör

0800/98 48 28 3 xtivate.de/exonas
0800/XTIVATE

kostenlos aus deutschem Fest- & Mobilnetz - Mo - Sa 9:00 - 19:00 Uhr

xtivate ist ein Shop der WWWgroup GmbH (Michael Sanger, Jens Wöhrer, Jörg Weßmann) | Zieglhüttenweg 4, 98693 Ilmenau - Druckfehler und Irrtümer vorbehalten. Alle eingetragenen Warenzeichen sind Eigentum der jeweiligen Firmen und Organisationen. **Preise in Euro inkl. 19% MwSt., gültig solange Vorrat reicht. Es können Versandkosten bis max. 12,50 EUR anfallen.



- [1] **Synology**
www.synology.com/deu/
- [2] **PutTY Download**
www.chiark.greenend.org.uk/~sgtatham/putty/download.html
- [3] **Installationsanleitung im Synology-Wiki**
www.synology-wiki.de/index.php/IPKG/
- [4] **Vorkompilierte IPKG-Pakete**
<http://ipkg.nslu2-linux.org/feeds/optware/syno-e500/cross/unstable/>
- [5] **Datei-Bearbeitung per SFTP oder SCP mit WinSCP**
www.synology-wiki.de/index.php/SFTP_SCP/
- [6] **WinSCP**
<http://winscp.net/eng/docs/lang:de/>
- [7] **Forum zu Synology-Produkten**
www.synology-forum.de
- [8] **Kompatibilitätsliste von Synology**
www.synology.de/deu/products/compatibility.php

Links



sind damit nicht möglich. Auf der Kompatibilitätsliste von Synology [8] sind aber zahlreiche alternative Backup-Programme geführt, mit denen die DiskStation zusammenspielt. Neben den Bordmitteln von Windows XP und Vista sind beispielsweise Symantec BackupExec oder EMC Retrospect gelistet. Die Backups der DiskStation verwalten die User über den "Disk Station Manager". Damit die Station als Ziel für Backups anderer Stationen oder rsync-Server dienen kann, muss dies unter "Sicherung / Netzwerksicherungsdienst" explizit aktiviert werden. Unter "Sicherung / Sicherung" lassen sich die lokalen Sicherungspläne verwalten. Die Station synchronisiert ihren Datenbestand wahlweise auf einen lokal per USB oder eSATA verbundenen Speicher, eine andere Synology DiskStation oder einen beliebigen rsync-Server im Netz.

Schmucke Medienbibliothek

Im Ordner "Anwendungen" stehen weitere Zusatzfunktionen zur Auswahl, die zum Teil für den Heim- und Unternehmenseinsatz interessant sein dürften. So lassen sich über die "Download Station" Download-Aufträge an die Station dele-

gieren. Die Funktion lässt sich zum einen als separate Webanwendung, zum anderen über den Windows-Client "Download Redirector" bedienen. In der Client-Anwendung können URLs explizit eingetragen oder über die sogenannte "Drop Zone", ein Icon am rechten Bildschirmrand, per Drag & Drop übergeben werden. Den PC können die Anwender anschließend ausschalten – die Downloads führt die Station autonom zu Ende. Neben HTTP- und FTP-Downloads lassen sich auch BitTorrent, eMule und Binary Usenet Links übergeben. Die "Surveillance Station" zeichnet Videostreams von bis zu zehn IP-Kameras auf. Die "Photo Station" dient der einfachen Veröffentlichung von Fotos und Videos. Zudem empfiehlt sich die DiskStation als Medienbibliothek und kann als UPnP- und als iTunes-Server verwendet werden. Über die Webanwendung "Audio Station" ist es möglich, die im Ordner "music" gespeicherten Files per browser-integriertem Player wiederzugeben.

Zusätzliche Funktionen stehen im Download-Bereich der Synology-Webseite als vorgefertigte SPK-Pakete bereit, die sich über die Weboberfläche via "System / Paketverwaltung" auf die Box kopieren und aktivieren lassen. Im Angebot finden sich das Logitech SqueezeCenter, der Webalizer als Statistikmodul für die "Web Station" sowie die Anwendung "Mail Station", mit der sich die DiskStation als POP3/IMAP/SMTP-Server einsetzen lässt.

Fazit

Mit der DiskStation DS209+II hat Synology ein NAS-System im Angebot, das für Home Offices und kleinere Unternehmen gleichermaßen interessant ist. Die Pflichtübung der Dateifreigaben meisterte das Gerät im Test ohne Probleme. In der Kür begeisterte das System mit der intuitiv zu bedienenden Oberfläche "Disk Station Manager 2.1", die das Handbuch weitestgehend erübrigte, sowie nützlichen Zusatzfunktionen, wie dem Download-Manager. Wer auf eigene Faust den Funktionsumfang erweitern möchte, wird Gefallen am offenen Kommandozeilen-

Zugang und dem umfangreichen Angebot an IPKG-Paketen finden. Soll neben Dateien auch der Systemstatus der Client-Computer gesichert werden, ist Backup-Software von Drittanbietern gefragt. Für den September ist Version 2.2 des DiskStation Managers angekündigt, die unter anderem mit Unterstützung für iSCSI, Apple Time Machine, RapidShare-Downloads und einer integrierten Firewall aufwarten soll. (dr)



Der Autor dieses Artikels, Dipl.-Inform. (FH) Christian Knermann, ist stellv. Leiter des IT-Managements am Fraunhofer Institut für Umwelt-, Sicherheits- und Energietechnik UMSICHT in Oberhausen.

Produkt

Network Attached Storage (NAS)
für zwei Festplatten.

Hersteller

Synology Inc.
www.synology.com

Preis

375 Euro (ohne Festplatten)

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Installation und Inbetriebnahme	9
Bedienbarkeit der Weboberfläche	9
Stromverbrauch	9
Mitgelieferte Backup-Software	5
Erweiterbarkeit	9

Dieses Produkt eignet sich

optimal für kleinere und mittlere Unternehmen sowie Zweigstellen.

gut für Windows, Mac OS- und Linux-Clients.

weniger für den Einsatz im Rechenzentrum in Großunternehmen.

Synology DS209+II



Im Test: gateProtect GPO-125

Sicherheit per Drag-and-Drop

von Sandro Lucifora

Das größte Sicherheitsrisiko heutiger Firewall-Systeme besteht darin, dass zur effektiven Abwehr von Angriffen immer komplexere Sicherheitsfunktionen integriert sein müssen. Das führt zwangsläufig dazu, dass die Konfiguration der Schutzsysteme kompliziert und unübersichtlich wird. Daraus folgt meist eine fehlerhafte Konfiguration, die aus dem Sicherheitssystem oft ein offenes Scheunentor macht. gateProtect will mit dem eigens entwickelten eGUI – dem "ergonomic graphic user interface" – die Bedienbarkeit wieder in den Mittelpunkt stellen. Ob das gelungen ist, haben wir in einem Test für Sie herausgefunden.

Mit der Firewall GPO-125 haben wir eine Appliance als Einstiegslösung im Test. Sie ist für Unternehmen mit bis zu 25 Mitarbeitern ausgelegt. Zu den Features gehören Application Level Firewall, VPN SSL über Zertifikate, Anti-Spam mit Real Time Detection, Antivirus, Intrusion Detection, URL- und Content Filtering.

Internet-Verbindung einrichten

Der "rote Kasten" wird nach dem Anschluss im Netzwerk als Gateway definiert und regelt so den zukünftigen Datenverkehr ins und aus dem Internet. Die Internetverbindung baut das System wahlweise über PPPoE beziehungsweise PPTPoE und ein angeschlossenes DSL-Modem auf oder es nutzt einen separaten, eigenständigen Router. Als dritte Option bietet der Internet-Wizard auch die ISDN-Wählverbindung an, die jedoch in der GPO-Appliance fehlschlägt, da diese Funktion eine eingebaute ISDN-Karte voraussetzt. Das ist der Hinweis, dass die gateProtect-Lösung nicht nur auf einer fertigen Appliance arbeitet, sondern auch als Software-Lösung auf einem eigenen Server installiert werden kann.

Bedient beziehungsweise eingerichtet wird die Appliance ausschließlich durch den Administrations-Client oder das Command Center, das einen sinnvollen Einsatz findet, wenn mehrere gateProtect-Firewalls im Überblick und/oder zusammenhängend ad-

ministriert werden. Nach der Installation richteten wir mit dem Installations-Wizard eine PPPoE-Verbindung über ein angeschlossenes DSL-Modem ein. Im Test wählten wir zudem zeitweise auch einen Router für den Internetzugang. Dabei fiel uns auf, dass der Router unbedingt an einem separaten der vier Netzwerk-Ports der Appliance angeschlossen oder in einem anderen IP-Bereich betrieben werden muss. Zudem darf im Router keine Firewall-Funktion aktiviert sein und jeglicher Datenverkehr muss weitergeleitet werden. Ansonsten finden die in der Appliance definierten Regeln teilweise keine Anwendung, da diese gegebenenfalls schon vorab durch den Router gestört werden.

Failover: Wenn eine Leitung weg ist

Klar von Vorteil ist die Möglichkeit, mehrere Internetverbindungen konfigurieren und als Backup-Leitung festlegen zu können. In der Praxis zeigte sich diese Funktion jedoch nur unter bestimmten Voraussetzungen als optimal – was jedoch nichts mit der Appliance selbst zu tun hatte. Im Test richteten wir über eine zweite DSL-Leitung



Bild 1: Die wichtigsten Dienste werden schon bei der Einrichtung der Internet-Verbindung vordefiniert

eine Failover-Funktion ein. Im simulierten Ausfall der Hauptleitung hat die Appliance in wenigen Sekunden das Routing auf die Backup-Leitung umgestellt – eine einwandfreie Leistung der Firewall. Doch technisch betrachtet laufen beide DSL-Zugänge über dieselbe Hausleitung – auch, wenn es sich dabei um unterschiedliche DSL-Anbieter handelte. Fällt also eine Leitung aus, weil es Probleme in der Hauszuführung gibt (zum Beispiel am Telekom-Knotenpunkt), sind beide DSL-Zugänge offline. Was in diesem Fall durch die Backup-Funktion aufgefangen wird, sind zum Beispiel Ausfälle bei der Zugangsauthentifizierung eines DSL-Anbieters. Zudem zeigt ein Failover seine Wirkung, wenn die zwei-



te Backupleitung auf einem anderen Weg ins Haus kommt wie die Hauptleitung – zum Beispiel über einen anderen Verteilerpunkt oder via Fernseekabel.

Berechtigungen

Über die eGUI der gateProtect-Appliance galt es nun, die erste Konfiguration für die Internet-Nutzung vorzunehmen. Der Assistent richtete zu Anfang die wichtigsten Dienste zur Nutzung ein. Wir haben so recht schnell die Dienste HTTP/S, DNS, FTP und die Mailfunktionen POP3 und SMTP freigeschaltet. Damit konnte sofort jeder im Netzwerk das Internet mit den wichtigsten Funktionen nutzen.

Grundsätzlich ist erst einmal jeglicher Datenverkehr, sowohl ein- als auch ausgehend, gesperrt. Daher ist eine individuelle Nachjustierung der Regeln schnell notwendig. Um diese vorzunehmen, mussten wir uns entscheiden, ob sich die weiteren Berechtigungen auf die angeschlossene Hardware oder hardwareunabhängig auf den Benutzer beziehen. Wir nutzten im Test beide Möglichkeiten. Die Einstellungen erfolgten über das eGUI-Interface des Administrations-Client. Das vorhandene Analyse-tool für blockierte Zugriffe hilft bei der ersten Fehlersuche und zeigt die Ports an, über die von intern oder extern zugegriffen werden soll, die Firewall dies jedoch verhindert hat. Wir haben Ihnen dazu in unserem Link-Bereich [1] eine Übersicht der bekannten Ports von Programmen und Trojaner in einer Liste zusammengestellt.

Regeln für die Hardware

Im Test haben wir die Regeln für den angeschlossenen Exchange-Server so erweitert, dass von außen der Zugriff auf Outlook Web Access möglich ist. Durch die eGUI konnten wir das Vorhaben sehr einfach umsetzen. Mittels Drag-and-Drop haben wir ein neues Objekt auf die Arbeitsfläche gezogen und diesem den Namen des Servers, den Objekt-Typ Server, die Netzwerkkarte und die IP-Adresse des Servers zugeteilt. Im nächsten Schritt stellten wir mit dem Verbindungswerkzeug einen Anschluss zum Internet her,

Protokoll	Port	Ursprung	Benutzer	In-Interface	Ziel	Out-Interface	Datum/Uhrzeit
tcp	1433	221.142.230.143		internet	217.7.204.86	Firewall	16.04.2009 11:07:00
tcp	40132	98.136.137.23		internet	217.7.204.86	Firewall	16.04.2009 11:07:00
tcp	80	61.139.105.162		internet	217.7.204.86	Firewall	16.04.2009 11:07:00
tcp	40132	98.136.137.23		internet	217.7.204.86	Firewall	16.04.2009 11:07:00
udp	137	192.168.163.207		eth0	192.168.163.200	Firewall	16.04.2009 11:07:00
udp	445	78.139.245.180		internet	217.7.204.86	Firewall	16.04.2009 11:06:00
udp	137	192.168.163.207		eth0	192.168.163.200	Firewall	16.04.2009 11:06:00
tcp	2396	BUCHÉ		eth0	192.168.40.1	internet	16.04.2009 11:05:00
tcp	2395	BUCHÉ		eth0	192.168.198.1	internet	16.04.2009 11:05:00
tcp	80	61.139.105.162		internet	217.7.204.86	Firewall	16.04.2009 11:05:00
tcp	2396	BUCHÉ		eth0	192.168.40.1	internet	16.04.2009 11:05:00
tcp	2395	BUCHÉ		eth0	192.168.198.1	internet	16.04.2009 11:05:00
tcp	80	61.139.105.162		internet	217.7.204.86	Firewall	16.04.2009 11:05:00
udp	137	192.168.163.207		eth0	192.168.163.200	Firewall	16.04.2009 11:05:00
tcp	80	61.139.105.162		internet	217.7.204.86	Firewall	16.04.2009 11:04:00
tcp	10080	61.139.105.162		internet	217.7.204.86	Firewall	16.04.2009 11:04:00
tcp	80	61.139.105.162		internet	217.7.204.86	Firewall	16.04.2009 11:04:00
tcp	80	61.139.105.162		internet	217.7.204.86	Firewall	16.04.2009 11:04:00
udp	137	192.168.163.207		eth0	192.168.163.200	Firewall	16.04.2009 11:04:00
udp	80	61.139.105.162		internet	217.7.204.86	Firewall	16.04.2009 11:03:00
udp	137	192.168.163.207		eth0	192.168.163.200	Firewall	16.04.2009 11:03:00

Bild 2: Die Übersicht der abgewiesenen Zugriffe gibt Aufschluss über Ports, die eventuell konfiguriert werden müssen

indem wir nur das Objekt für das Internet und den neu erstellten Server anklickten – es öffnete sich der Regeleditor, in dem die Regel für HTTPS eingerichtet wird. Zusätzlich benötigten wir für den Remote-Zugriff via HTTPS den Port 4125. Da es für diesen keinen fertig eingerichteten Dienst gab, legten wir diese Regel mit wenigen Mausklicks neu an.

Täglich sollte sich die Uhr dieses Servers über das Internet abgleichen, daher erlauben wir auch den NTP-Dienst für den Server. Da die Abfrage nur vom Server in das Internet und nicht umgekehrt erfolgen darf, legten wir hierbei auch die umgekehrte Datenfluss-Richtung fest: Bei den zuvor angelegten Regeln musste vom Internet über die jeweiligen Ports auf den Server zugegriffen werden. Der NTP-Dienst darf nur vom Server ins Internet verbinden. Diese Richtungen werden anhand von grünen Pfeilen im Regeleditor dargestellt. Nach der Aktivierung der Regeln haben wir die Firewall für diese Funktion fertig konfiguriert. Angenommen, im Netzwerk sollen sich nun acht von 25 Computern über den NTP-Dienst Zeit-synchronisieren. In diesem Fall muss dieser Dienst nicht für jeden Computer, also für acht separate Objekte, aktiviert werden. Vielmehr lässt sich hierfür per Drag-and-Drop eine Com-

puter-Gruppe einrichten. Dieser werden dann die einzelnen Rechner per IP-Adresse zugeordnet und die entsprechende Regel zentral definiert.

Regeln für die Benutzer

Ein geteilter Arbeitsplatz ist nicht mehr ganz neu: Das bedeutet, dass ein Computer zum Beispiel durch zwei oder mehr Teilzeitkräf-

Performance

- Firewalldurchsatz: 200 MBit/s
- VPN (AES 192) Durchsatz: 50 MBit/s
- E-Mails pro Tag: 5.000
- Gleichzeitige Verbindungen: 250.000

Firewall

Layer Funktion, Single Sign On (xUA), Paketfilter, IDS, NAT, DHCP-Server, DMZ, Bridging, Internet-Failover, Webblocking, Mailfilter.

Besondere Features

High-End-Firewall-Funktion, Extended User Authentication, VPN Gateway (SSL mit X.509 Zertifikaten und IPSec), Proxies (HTTP, FTP, POP3, SMTP, SIP), Application Level (Deep Packet Inspection), Hochverfügbarkeit, VLAN.

Optional

Spam-Filter auf Commtouch-Basis, Virus Filter von Kaspersky sowie Web-Filter von IBM.

Technische Daten





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

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

Virtualisierung

zum Abonnenten-Vorzugspreis* von

nur € 29,90!

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

Liefertermin:
Mitte Oktober 2009

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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



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

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

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

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

Ich zahle ☐ per Bankeinzug

Firma: _____

Geldinstitut: _____

Name, Vorname: _____

Kto.: _____ BLZ: _____

Straße: _____

oder ☐ per Rechnung

Land, PLZ, Ort: _____

Datum: _____

Tel.: _____

Unterschrift: _____

E-Mail: _____

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

So erreichen Sie unseren
Vertrieb, Abo- und
Leserservice:

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

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



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

ITA 1001 VII

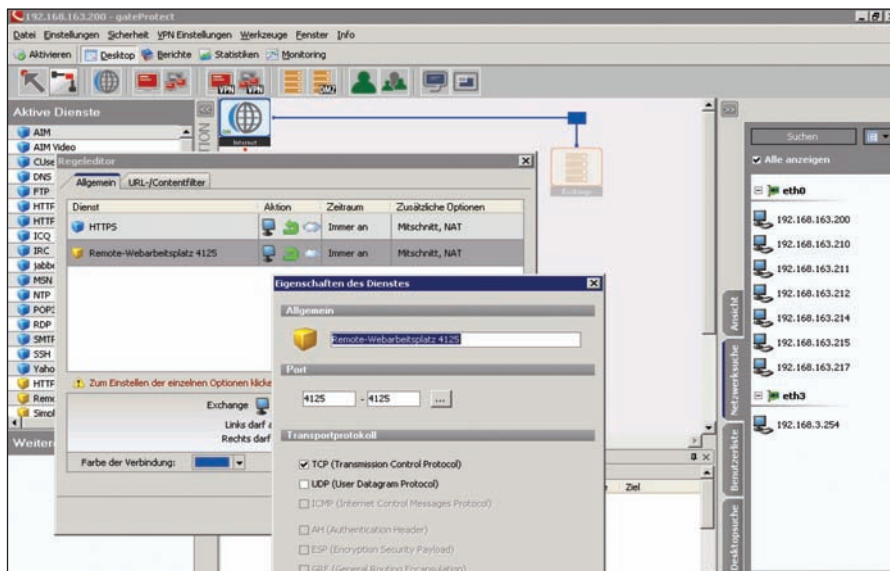


Bild 3: Vordefinierte Regeln lassen sich über den Regeleditor eintragen und auch eigene Regeln hinzufügen

te mit unterschiedlichen Aufgaben gemeinsam genutzt wird. In diesem Fall ist es nicht immer erwünscht, für einen Computer, sondern vielmehr für einen einzelnen Benutzer verschiedene Regeln festzulegen. Wie bei den IP-basierten Regeln werden in der eGUI auch Anwender und Anwendergruppen als Objekte behandelt. Der Vorteil dabei ist, dass die Regeln dadurch Hardware-unabhängig funktionieren. In unserem Testszenario arbeiteten zum Beispiel mehrere Entwickler an verschiedenen Rechnern – einige sind freie Mitarbeiter und benutzen zeitversetzt den selben Computer. Nicht alle dieser Mitarbeiter durften per FTP Daten auf den Produktiv-Server hochladen. Um das zu realisieren, griffen wir auf die Benutzerauthentifizierung für Regeln zurück. Dazu aktivierten wir zunächst die Benutzerliste aus dem AD des Netzwerks.

Im Anschluss legten wir auf der Arbeitsfläche des Administrations-Clients – nach demselben Prinzip wie zuvor Computer und Computer-Gruppen – Benutzer beziehungsweise Benutzergruppen an. Statt einer IP-Adresse ordneten wir die Benutzernamen aus dem AD als Mitglied des neuen Objektes zu. Im nächsten Schritt verbanden wir das Internet-Objekt mit der Benutzergruppe und trugen über den Regeleditor die Berechtigung zum FTP-Zugriff ein. Damit der Firewall bekannt ist, an

welchem Computer sich der Benutzer befindet, muss sich dieser per Web-Browser an der Appliance anmelden. Solange die Browsersitzung geöffnet ist, erhält der Computer mit der ermittelten IP-Adresse die Regeln des angemeldeten Benutzers; in unserem Test war der FTP-Upload an jedem Computer, aber abhängig von den Benutzern möglich. Mit dieser Funktion können auch tiefgehende Sicherheiten gesteuert werden. Wie in unserem Szenario der Teilleistung lässt sich so auch ein HBCI-Zugriff, um Online-Kontoaktivitäten vorzunehmen, ausschließlich auf Benutzerebene ermöglichen.

Gefilterter Datenstrom

Die Sicherung des Netzwerkes auf Port-Ebene bildet die Basis für den Schutz der eigenen Daten vor Angreifern. Doch verstecken sich auch in den übertragenen Daten selbst weitere Sicherheitsrisiken. So können zum Beispiel Trojaner und Viren über die freigegebenen Protokolle eingeschleust werden. Auch Schadcode von Internetseiten findet durch die offene Tür Einlass in das Netzwerk. Um auch diese Risiken auszuschließen, hat die GPO-125 drei weitere, effektive Schutzmechanismen:

- Der Webfilter ist eine Kombination aus URL- und Content-Filter. HTTP-Suchanfragen werden automatisch mit

erlaubten Kategorien von Webseiten und Inhalten abgeglichen und bei Notwendigkeit geblockt. Die Filtergruppen können dabei individuell aus 60 hinterlegten Filter-Kategorien zusammengestellt werden.

- Die Scan-Engine für Antivirus basiert auf der Technologie von Kaspersky. Das Gateway scannt dabei HTTP, FTP, POP3 und SMTP auf unerwünschten Code. Dateien werden auf der Firewall auf Viren gescannt und erst dann an den anfragenden Benutzer weitergegeben. Mit der konfigurierbaren Antivirus-Datei-Größe legten wir fest, bis zu welcher Größe eine Datei auf Viren gescannt wird. Hierzu haben wir das Limit auf bis zu 30 MByte angehoben. Trotz dessen, dass die gesamte Datei im Speicher der Appliance gescannt wird, konnten wir keine spürbaren Performance-Einbußen feststellen. Lediglich der FTP-Upload wies wenige Sekunden Verzögerung auf. Im Bedarfsfall muss der Administrator für das eigene Unternehmen hier den idealen Wert durch Ausprobieren herausfinden.
- Der Spam-Filter der UTM-Firewall scannt den E-Mailverkehr auf bekannte Spam-Signaturen und löscht oder markiert die erkannten E-Mails. Das Besondere hierbei ist, dass das eigentliche Filtern extern erfolgt und somit keine Ressourcenauslastung erfolgt. Durch die

Der Vorteil der PPTP-VPN-Verbindung ist unter anderem, dass diese mit den Windows-Bordmitteln erstellt und genutzt werden kann. Als Nachteil kann sich schnell zeigen, dass das Gateway auf den VPN-Tunnel umgestellt wird. Daher erfolgt bei aktiver PPTP-VPN-Verbindung der Internetzugriff über den VPN-Tunnel und das verbundene Netzwerk. Im Gegensatz ist sowohl an der Appliance als auch dem Arbeitsplatz die Einrichtung der IPSec-Verbindung wesentlich aufwändiger. Zudem wird ein eigener VPN-Client benötigt. Dadurch erfolgt jedoch nur das Routing an interne Adressen in das verbundene Netzwerk; Zugriffe auf das Internet laufen unverändert über die bestehende Internetverbindung. Nachteil bei diesem VPN-Typ ist, dass er den Tunnel nur mit einem Subnetz verbinden kann. So können Sie über die GPO-125 nicht auf mehrere Netzwerke hinter der Firewall zugreifen.

Tipp: PPTP-VPN vs. IPSec-VPN





eingesetzte Real Time Detection-Technik erkennt die Appliance Spam, Virus und Phishing-Attacken anhand von charakteristischen Mustern schon bei deren erstmaligen Ausbrechen. Dadurch sollen laut Hersteller mehr als 97 Prozent der Spam-Versender rechtzeitig und vor der Verbreitung erkannt und abgefangen werden. Im Test stellten wir vielfach fest, dass die Appliance Spam-Mails erkannt hat, die durch andere Spam-Filter wie Spam-Assassin und kostenpflichtige Produkte unbehellig durchgelassen wurden.

Vorteilhaft bei diesen Viren- und Spam-Scannern: Es ist unerheblich, über welches System und von welchem Provider die E-Mails ins Haus kommen – ob sie via POP3 abgefragt oder über SMTP zugestellt werden. Jeder Datenfluss über die Protokolle findet die passende Prüfung.

Virtual Private Network

Oft ist der Zugriff mit dem Notebook oder dem Heimarbeitsrechner auf die internen Daten gewünscht. Die Lösung dafür ist das VPN. Diese Funktion liefert die Appliance serienmäßig mit. Dabei konnten wir uns im Test zwischen der einfachen PPTP-Lösung, einer IPSec-Verbindung oder dem VPN-SSL-Zugriff entscheiden. Für den Einsatz von PPTP mussten wir lediglich den User aktivieren und haben über die Windows-Netzwerkeinstellung die VPN-Verbindung aufgebaut. Der Aufwand für die Einrichtung von IPSec war dagegen deutlich höher. Da wir IPSec über ein Zertifikat und nicht mit PSK einsetzen, mussten wir zunächst mit dem Zertifikatsmanager ein Host-, dann die jeweiligen Client-Zertifikate erstellen. Danach wurde die IPSec-Verbindung eingerichtet. Clientseitig haben wir den gateProtect-IPSec-Client verwendet. Dieser benötigt noch das IPSec-Zertifikat, das aus

dem Administrations-Client exportiert und auf dem Arbeitsplatz aktiviert wird. Für jeden VPN-Tunnel beziehungsweise jede Verbindung mussten wir dann das VPN-Objekt auf der Arbeitsfläche des Administrationsclients platzieren und mit dem internen Netzwerk verbinden. Das Objekt war damit der VPN-Endpunkt der Verbindung. Durch den bekannten Regeleditor legten wir auch hier wieder fest, welche Aktivitäten durch das VPN in das interne Netzwerk erlaubt waren.

Wissen, was passiert

Die Statistiken geben dem Administrator schnell Aufschluss darüber, welche Seiten am meisten frequentiert sind. Die Übersicht der Dienste lässt erkennen, welcher Dienst wie stark genutzt wurde. Aufschlussreich ist auch die Übersicht des Traffics nach Arbeitsplätzen. Die Übersicht der Abwehr zeigte in unserem Test zum Beispiel, dass innerhalb von nur vier Tagen 529.816 eingehende Zugriffe abgewiesen sowie 67 Viren über HTTP(S), vier über POP3 und 885 Spam-Nachrichten erkannt wurden – eine stolze Statistik. Das Balkendiagramm der abgewiesenen Zugriffe zeigte für einen Tag den Spitzenwert von 149.896 Hits.

Fazit

Die Appliance GPO-125 ist für Unternehmen mit bis zu 25 Mitarbeitern ausgelegt und als Stand-Alone-Gerät konzipiert. Bei etwa 300 Benutzern wird das Arbeiten über die Firewall sehr zäh. Trotz der gut gelungenen und intuitiv zu bedienenden eGUI von gateProtect ist die Konfiguration einer Firewall immer noch nichts für den einfachen Anwender. Das Handwerk selber ausführen zu können, befreit nicht von der Notwendigkeit zu wissen, was gemacht werden muss. Die Erfahrung zeigt, dass Anwender mangels Wissen eine Firewall oft komplett aufmachen. Der erfahrene Administrator jedoch kann durch die eGUI eine ganze Menge Zeit und Arbeit sparen. Die Drag-and-Drop-Funktion, die einfache Regelkonfiguration und die Benutzerauthentifizierung lassen in kurzer Zeit sonst mühevoll erstellte Si-

cherheitseinstellungen entstehen. Die erfolgreich eingesetzten Viren-, Content- und Spam-Filter als auch die VPN-Lösungen runden die Funktionalitäten ab. Die Appliance bietet allerdings wie die kleinere Variante GPO-75 keinen HTTPS-Proxy. Mit der gateProtect GPO-125 hatten wir nichtsdestotrotz ein Gerät im Test, das in seiner Bedienung und Funktionsweise als auch in der Preisgestaltung ein rundes Bild liefert – und das besitzt durchaus Seltenheitswert. (dr)

Produkt

Sicherheits-Appliance mit Firewall, Webproxy, VPN, Antivirus und Spam-Filter.

Hersteller

gateProtect
www.gateprotect.de

Preis

Appliance GPO-125:
ab 846 Euro
Sicherheits-Paket (Virus-, Web- und Spam-Filter):
1 Jahr: 295 Euro
3 Jahre: 797 Euro (entspricht 266 Euro/Jahr)

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für kleinere und mittlere Unternehmen mit bis zu 25 Anwendern.

teilweise für Netzwerke mit 50 und mehr Usern.

nicht für den Schutz mit großem Datenverkehr/Aufkommen.

gateProtect GPO-125 V8.5

[1] Portliste

www.it-administrator.de/downloads/
datenblaetter/1009-gateprotect-Portliste.pdf

Links





Quelle: Sergey Galushko – Fotolia.com

NAS-Lösungen im Überblick

Brücken zwischen den Inseln

von Thomas Hümmler

Kleine Netzwerke sind oft dezentral ausgelegt. Jeder Anwender speichert seine Daten auf der eigenen PC-Festplatte. Eine Brücke zwischen diesen Dateninseln lässt sich einfach per N(D)AS bauen. Dank des sogenannten Network (Direct) Attached Storage kann jeder von überall auf Daten zugreifen. Wir erklären Ihnen in diesem Artikel die Grundzüge der Technik und stellen Ihnen einige Geräte für die eher kleine Geldbörse vor.

Daten lagern überall: auf dem PC, dem Notebook, Backups vielleicht sogar auf CDs und DVDs. Auf dem einen Rechner ist die Buchhaltung, auf einem anderen liegen die Briefvorlagen und auf allen finden sich unterschiedliche Internetlinks mit den zugehörigen Passwörtern. Früher hatte der Einzelne für solche Fälle eine Diskette oder ein ZIP-Medium, später eine wiederbeschreibbare CD, dann den USB-Stick. Auf diesen beweglichen Speichern waren wichtige Vorlagen, Tabellen oder die E-Mailsignatur verwahrt, um sie jederzeit und überall griffbereit zu haben. Doch inzwischen ist das Datenaufkommen, weil multimedial, wesentlich größer – und wenn mehrere auf dieselben Daten zugreifen wollen, wird gerade das Vorhalten und Synchronisieren der Daten zur echten Herausforderung.

Die Unterschiede zwischen NAS und NDAS

Abhilfe schafft ein dedizierter Fileserver. Günstiger, sparsamer und schneller einsatzbereit ist allerdings NAS. NAS steht für Network Attached Storage – Speicher, der mit dem Netzwerk verbunden ist. Dieser Speicher in Form von Festplatten wird

meist über einen mitgelieferten Server zur Verfügung gestellt. Damit sind dann Funktionen wie eine eigene Benutzerverwaltung möglich oder das Streamen von Audio- und Video-Dateien. Auf NAS-Speichern kommt oft ein Linux- oder Unix-Dateisystem zur Verwendung. Ein NFS- oder Samba-Server regelt den Zugriff und Speicherplatz. Die Konfiguration geschieht häufig über Web-Oberflächen, Ein- und Ausgabegeräte wie Tastatur, Maus und Bildschirm sind am NAS nicht vorgesehen. Über einen Ethernet-Anschluss werden NAS-Geräte und die daran angeschlossenen Festplatten im Netzwerk bereitgestellt. In Verbindung mit einer dauerhaften Online-Verbindung lässt sich von überall auf die Daten zugreifen.

Dies geht bei NDAS nicht: Der Network Direct Attached Storage wird direkt ins Netzwerk eingebunden. Dort verhält er sich zwar genauso wie NAS-Speicher, allerdings ist ein Zugriff von außen über Router nicht möglich. Auf Server-Funktionen muss der Benutzer bei NDAS ebenfalls verzichten. Ein Media- oder Backup-Server lässt sich damit folglich nicht aufbauen, lediglich Dateien dort ablegen und im Netz bereitstellen.

NDAS-Festplatten sind aus Sicht des Betriebssystems wie ein lokaler Datenträger, die über ein Netzwerkprotokoll namens LPX (Lean Packet Exchange) angesprochen werden. Dafür müssen auf den Rechnern, mit denen die Nutzer auf die NDAS-Speicher zugreifen sollen, auch die entsprechenden Treiber eingerichtet werden. Diese Treiber binden die NDAS-Laufwerke dann als virtuelle SCSI-Laufwerke ein. Anschließend lassen sich die Platten in der Regel mit den auf diesen Betriebssystemen gebräuchlichen Dateisystemen formatieren. Die Anzahl der gleichzeitigen Zugriffe ist begrenzt, für kleinere Unternehmen jedoch vollkommen ausreichend. Ungefähr ein Dutzend Nutzer können parallel ohne größere Performance-Verluste darauf zugreifen.

Form und Größe

NAS-Geräte können, müssen aber nicht so groß sein wie ein PC. Einer der kleinsten Server ist das NSLU2 von Linksys, an den sich zwei USB-Festplatten anschließen lassen. Der Server mit einem Intel-ARM-Prozessor wiegt gerade mal 160 Gramm und ist leicht zu übersehen: Das Gerät ist 13 Zentimeter hoch, 9,5 Zentimeter tief und 2,5 Zentimeter breit –



kleiner also als die meisten Taschenbücher. Der Aufbau von NDAS-Geräten ist im Allgemeinen ähnlich. In einen Gehäuse stecken eine oder mehrere Festplatten. Gekoppelt mit der entsprechenden trivialen Elektronik stellen sie die Daten bereit. Außen am Gehäuse prangen LEDs und zum Ein-/Ausschalter gesellt sich ein RJ-45-Stecker für das Ethernet; alternativ gibt es Modelle mit WLAN-Adapter für das Funknetz. Die meisten NDAS-Geräte haben außerdem einen USB-Anschluss, seltener auch einen Firewire-Adapter. So lassen sich die Geräte gleichzeitig als externe Festplatten direkt am Rechner oder an einen entsprechend ausgestatteten Router anschließen. Einige NDAS-Systeme mit mehreren Festplatten können im RAID-Level 0 und 1 betrieben werden. RAID 0, das sogenannte Striping, fasst zwei oder mehr physikalisch vorhandene Platten zu einer großen virtuellen zusammen. Diese ist dann so aufgeteilt, dass die Blöcke auf die verschiedenen Festplatten verteilt

werden. Ein Zugriff auf unterschiedliche Blöcke kann dann schneller – weil parallel – erfolgen. Das RAID-Level 1 bietet dagegen nur die halbe Speicherkapazität. Grund dafür ist, dass von den zwei Festplatten eine ständig gespiegelt wird, um Datenverlust zu vermeiden.

Vorzüge und Nachteile

Die Vorteile von NDAS sind schnell aufgelistet. Die Geräte lassen sich allein ohne Server im Netzwerk betreiben – und sind dort von überall erreichbar. Sie können auch einfach am USB-Anschluss eines Rechners verwendet werden. Als weiterer Vorzug wird immer wieder die geringe Lärmbelastung genannt. Das trifft aber nur bedingt zu. Zwar arbeiten viele ohne Lüfter. Doch wegen der hohen Umdrehungszahlen der Festplatten vibrieren die kleinen Gehäuse eher als große Desktop-Rechner. Das kann genauso störend sein wie das PC-Gebläse. Nicht selten gibt es Festplatten, die im Betrieb piepen oder pfeifen. Abhilfe: Platzieren Sie den Spei-

cher im trockenen Kellerraum und verbinden ihn über die Steckdose per DLAN mit dem Netzwerk-Switch.

Der Nachteil von NDAS gegenüber dem Server-betriebenen NAS: NDAS-Geräte sind nur im eigenen Netzwerk sichtbar. Wer über das Internet an die Daten heran will, muss auf NAS ausweichen. Alternativ dazu ließe sich ein alter PC verwenden. Mit Linux kann der zum Samba-Server avancieren und alle Geräte im Netz bedienen. Worauf noch zu achten ist: Wer mit großen Dateien arbeitet, sollte als Dateisystem keinesfalls FAT32 verwenden. Das System ist begrenzt auf 2 GByte als maximale Dateigröße. Schon die ISO-Datei einer DVD ist mehr als doppelt so groß. Außerdem wird ab und zu von Problemen berichtet, wenn Nutzer von unterschiedlichen Betriebssystemen auf ein NAS zugreifen sollen. Hier hilft nur Testen. Dabei ist hilfreich, dass online gekaufte Ware ohne Angabe von Gründen innerhalb von zwei Wochen zurückgegeben werden kann. (ln)

Microsoft



Termine:

07.10.09

in München

18.11.09

in Hannover

20.11.09

in Düsseldorf

23.11.09

in Frankfurt a. M.

25.11.09

in Karlsruhe

Einfachere Verwaltung, intuitive Benutzerführung und ideales Zusammenspiel Ihrer Systeme – erfahren Sie auf der Joint Launch Roadshow, was heute und in Zukunft zählt. Lassen Sie sich die Veranstaltung in Ihrer Nähe nicht entgehen!

Melden Sie sich am besten gleich an unter www.microsoft.de/jointlaunch09/event

© 2009 Microsoft Corporation. Alle Rechte vorbehalten.

Because it's everybody's  business



	ReadyNAS Duo 2000	Data Tank Gateway	HD-35NAS+	StorCenter ix2 Network Storage
				
Hersteller	Netgear	Freecom	Buffalo	Iomega
Web	www.netgear.de	www.freecom.de	www.buffalo-technology.com	http://go.iomega.com/de
Anschlüsse	1 x RJ-45, 3 x USB 2.0, 2 x SATA-Einschub	1 x RJ-45 WAN, 4 x RJ-45 LAN, 1 x WLAN, 2 x USB 2.0	1 x RJ-45, 2 x USB 2.0	1 x RJ-45, 4 x USB 2.0
Transferrate	10/100/1000 MBit/s	10/100/1000 MBit/s	10/100/1000 MBit/s	10/100/1000 MBit/s
Kapazität	-	1 TByte	ab 1 TByte	ab 2 TByte
Gewicht	2,1 kg	2,9 kg	9,1 kg	10 kg
Abmessungen	175 x 150 x 146 mm	211 x 115 x 37 mm	136 x 60 x 209 mm	200 x 80 x 125 mm
Sonstige Ausstattung	NTI Shadow für ReadyNAS für Windows und Macintosh, ReadyNAS Discovery Dienstprogramm, Ethernet-Kabel, Handbuch, Festplattenrahmen, Installations-CD	NTI Shadow Backup Software CD (PC), Ethernet-Kabel, zwei WLAN-Antennen, Handbuch auf CD	Memo Zero-Touch AutoBackup Software	Ethernet-Kabel, Kurzanleitung, Lösungs-CD
Beschreibung	Das Netgear ReadyNAS DUO 2000 ist ein NAS-Server mit Platz für zwei Festplatten. Das Gerät unterstützt Linux, Mac OS X und Windows sowie die Dateiprotokolle CIFS/SMB, AFP, NFS, HTTP/S, FTP/S und RSYNC. Als Mediaserver streamt das Gerät Musik, Fotos und Videos auf einen Mediaplayer oder einen netzwerkfähigen Flachbildfernseher. Ein integrierter BitTorrent-Client erlaubt Downloads aus dem Internet. Übrigens: Es gibt das Gerät unter anderer Typenbezeichnung auch mit zwei eingebauten Festplatten. Günstiger ist es aber, die Platten selbst einzubauen. So schlägt das Gerät mit einer 1-TByte-Platte insgesamt mit etwa 300 Euro zu Buche, während das fertig konfigurierte Netgear-Gerät RND2110 ungefähr 700 Euro kostet.	Das Freecom DataTank Gateway hat einen 2.6er Linux-Kernel und läuft auf einer ARM9-CPU mit 400 Mhz. Das Gerät gibt es mit 1 und 2 TByte (649 Euro) Speicher, aufgeteilt jeweils auf zwei Festplatten. Die zwei Festplatten können im RAID-0- (Striping) oder RAID-1-Level (Mirroring) konfiguriert werden. Der DataTank besitzt einen SYNC-Schalter zum Synchronisieren von Dateien mit dem Computer und umgekehrt. WLAN bis 54 MBit/s wird unterstützt, der DataTank ist gleichzeitig Client und Access Point. FTP-, SSH- und Web-Server sorgen dafür, dass sich der DataTank auch über das Internet erreichen lässt, die eingebaute Firewall schützt den Zugriff. Außer Linux werden Mac OS X und Windows unterstützt.	Das Gerät von Buffalo ist eine der kostengünstigsten Rackmount-NAS-Lösungen. Es enthält vier SATA-Festplatten ab 250 GByte bis 2 TByte und unterstützt die RAID-Modi 0, 1, 5 und 10. Active Directory für Windows Server 2003 wird ebenso unterstützt wie die Protokolle TCP/IP, SMB, FTP, HTTP und NTP (zur Zeit-synchronisation). Ein LC-Display an der Front zeigt den Status des Geräts an; mit einer Web-Oberfläche wird der NAS-Server konfiguriert. Über eine serielle Schnittstelle lässt sich die TeraStation zudem mit einer USB verbinden.	Dieser NAS-Server mit einer 400-MHz-Freescale-CPU und 512 MByte RAM hat einen Linux-Kernel und vier Hotswap-fähige Festplatten, die als RAID-5-System vorkonfiguriert sind. Als Netzwerkdateiprotokolle werden CIFS/SMB, NFS und FTP unterstützt. Über den CUPS-Server und die USB-Schnittstellen können bis zu vier Drucker angeschlossen werden. Das Gerät funktioniert als Client in einer Active-Directory-Domäne, allerdings nicht selbst als Domänencontroller. Über ein browserbasiertes Tool konfiguriert der Benutzer das System. Den NAS-Server gibt es auch mit 3, 4 und 6 TByte Speicher; die Preise dafür liegen bei 790 Euro, 930 Euro und 1.080 Euro.
Preis	210 Euro	499 Euro	ab 630 Euro	ab 650 Euro



	Storage Center Turbo SC101T	Network Drive	HD-35NAS+	StorCenter ix2 Network Storage
				
Hersteller	Netgear	Freecom	Teac	Iomega
Web	www.netgear.de	www.freecom.de	www.teac-shop.de	http://go.iomega.com/de
Anschlüsse	1 x RJ-45, 2x SATA-Einschub	1 x RJ-45, 1 x USB 2.0	1 x RJ-45, 1 x USB 2.0	1 x RJ-45, 2 x USB 2.0
Transferrate	10/100/1000 MBit/s	10/100 MBit/s	10/100 Mbit/s	10/100/1000 MBit/s
Kapazität	-	500 GByte	500 GByte	1 TByte
Gewicht	k.A.	1,2 kg	2,3 kg	2,2 kg
Abmessungen	175 x 150 x 146 mm	211 x 115 x 37 mm	136 x 60 x 209 mm	200 x 80 x 125 mm
Sonstige Ausstattung	SmartSync Pro Backup-Software, Ethernet-Kabel, Installationsanleitung	NTI Shadow Backup Software, Ethernet-Kabel, USB-Kabel, Handbuch auf CD	USB-Kabel, Handbuch, Treiber-CD	Ethernet-Kabel, Kurzanleitung, Lösungs-CD
Beschreibung	Im Gegensatz zu anderen Lösungen sind beim Storage Center Turbo keine Festplatten mit dabei. Das NDAS-Gerät ist aber für bis zu zwei 3,5-Zoll-SATA- oder SATA2-Festplatten vorbereitet. Damit es läuft, muss im Netzwerk ein DHCP-Server vorhanden sein. Weitere Systemvoraussetzung ist Windows 2000 (SP4), XP Home oder Pro (mit SP1 oder SP2). Eine Datensicherung kann im RAID-1-Level auf die zweite Platte im Gerät erfolgen.	Das Network Drive von Freecom hat vor zwei Jahren einen Design-Preis bekommen. Das nützt allerdings Linux-Benutzern nichts, denn dieses Gerät unterstützt laut Datenblatt nur Windows und Mac OS X. Auch berichten einige Käufer, dass dieses Gerät sehr langsam sei. An der Festplatte kann es nicht liegen: Das NDAS-Laufwerk hat eine 500-GByte-Festplatte mit neun Millisekunden Zugriffszeit bei 7.200 Umdrehungen. Es kann über USB oder im LAN genutzt werden. Ein Konfigurations-Assistent erleichtert das Verwalten im Netzwerk. Die Software NTI Shadow Backup ermöglicht einfache Backups. Von dem Netzwerklaufwerk gibt es noch eine 1-TByte-Version für 179 Euro.	Das TEAC HD-35NAS+ wird automatisch über DHCP konfiguriert. Es hat eine Web-basierte Verwaltung und unterstützt Macintosh und Windows. Die integrierte 500-GByte-Festplatte dreht mit 7.200 Umdrehungen und hat 8 MByte Cache.	Das Iomega StorCenter bietet 1 TByte oder 2 TByte (250 Euro) Speicherplatz. An den zwei USB-2.0-Anschlüssen lassen sich weitere Festplatten und Drucker in das Netzwerk einbinden; dazu müssen auf jedem Client die entsprechenden Druckertreiber installiert sein. Linux, Macintosh und Windows werden unterstützt, als Dateisysteme kommen CIFS/SMB (Windows), NFS (Linux) und FTP in Frage; FTP kann immer nur für eine Freigabe aktiviert werden. Arbeitsgruppen werden ebenso wie Windows-Domänen unterstützt.
Preis	61 Euro	105 Euro	105 Euro	205 Euro

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



Konzepte für Storage-Umgebungen

Viele Wege zum optimalen Speicherplatz

von Thomas Bär

Das Bilden eigener Speichernetzwerke im Unternehmen gilt gemeinhin als eine vielversprechende strategische Entscheidung – lassen sich doch sowohl die Leistung erhöhen als auch mittelfristig die Kosten senken. Doch was genau gilt es zu bedenken und zu tun, um diesem Ziel tatsächlich gerecht zu werden? Nur mit den richtigen Strategien und Einstellungen wird das Speichersystem schneller. IT-Administrator zeigt Ihnen in diesem Beitrag, worauf es bei Storage-Umgebungen ankommt.

Was für verschiedene andere Technologien gilt, findet auch beim Storage seine universelle Anwendbarkeit: Je mehr Geld auf den Tisch gelegt wird, desto höher sind die Leistungen, die solche Systeme erzielen. Spielt die Kostenbetrachtung jedoch wie bei den meisten Unternehmen eine deutlichere Rolle, beginnt mit der Auswahl der Komponenten die sinnvolle Zusammensetzung des Storage-Systems.

DAS, NAS und SAN – drei ähnlich klingende Abkürzungen, die zwar im Prinzip das Gleiche leisten, jedoch auf unterschiedlichen Wegen. "Direct Attached Storage" (DAS) sind Festplattensysteme, die intern am Computer beziehungsweise Server angeschlossen sind. Die Bereitstellung von Speicherplatz für Client-Computer und die Nutzung der Festplatten für Datenbanksysteme sind die klassischen Nutzungen. Für kleinere Unternehmen eignet sich DAS hervorragend, da dieser Speicherplatz ohne Zusatzkenntnisse bereitgestellt wird und zudem keine Zusatzkosten erfordert. Eine flexible Vergrößerung des Speicherplatzes durch Einschieben weiterer Festplatten ist allerdings nur schwer möglich. Bei DAS-Systemen handelt es sich zumeist um Windows- oder Linux-Server, Be-

triebssysteme, die über eine sehr große Bandbreite an Technologien verfügen, jedoch nicht speziell auf die Aufgabe als "Filer" optimiert wurden. Administrativ erzeugen diese Systeme einen höheren Aufwand, da viele Updates und Patches einzuspielen sind. In einer nur gering ausgelasteten Umgebung sind beispielsweise Windows-Server im Zusammenspiel mit dem Distributed Filesystem (DFS) jedoch eine leicht zu administrierende und flexible Form der Bereitstellung von Freigaben.

Bei Network Attached Storage (NAS) kommen im Vergleich zu DAS dedizierte Systeme zum Einsatz. Die Maschine kümmert sich also ausschließlich um die Aufgabe der Speicherplatzbereitstellung und ist dafür optimiert worden. Dateibasierende Dienste wie SMB/CIFS (Windows-Freigaben) oder NFS (Linux-Shares) stellen die Kernfunktion dieser Geräte dar. Da die Verbindung über TCP/IP hergestellt wird, bleibt ein gewisser Protokoll-Overhead, der die Geschwindigkeit trotz GBit-Netzwerken ausbremst.

Besonders seit der Einführung von iSCSI stellen NAS-Filer eine kostengünstige Alternative zum traditionellen SAN mit Fibre Channel-Anbindung dar. Ohne die

Verwendung von iSCSI werden NAS-Filer direkt über SMB/CIFS oder NFS angesprochen – mit iSCSI kommt es zu einer direkten, blockbasierten Verbindung zwischen dem eigentlichen Nutzserver und der NAS-Appliance. Der blockbasierte Zugriff ist für Datenbanksysteme oder für den professionellen Einsatz von Virtualisierungsprodukten von Bedeutung, da beide Technologien den direkten Zugriff auf die Festplatten erfordern. Die Grenzen von SAN und NAS verschwimmen seit dem Erscheinen von iSCSI zusehends und es kommt nicht von ungefähr, dass die so entstandene Kombination als "IP-SAN" bezeichnet wird.

Fibre Channel-SAN

Während IP-SAN auf die bekannte Ethernet-Verbindung setzt, wird bei FC-SAN ein spezielles, eigenes Speichernetzwerk auf Fibre Channel-Basis verwendet. Dieses eigenständige Speichernetzwerk ist das Argument für SAN – alle Serversysteme, die in einem SAN integriert sind, können auf alle Storage-Systeme in sehr hoher Geschwindigkeit zugreifen. Das ermöglicht die Konsolidierung der einzelnen Storage-Systeme und bietet eine gemeinsame Verwaltung und Nutzung der Festplattenspeicher auch über die Betriebssystemgrenzen hinweg.

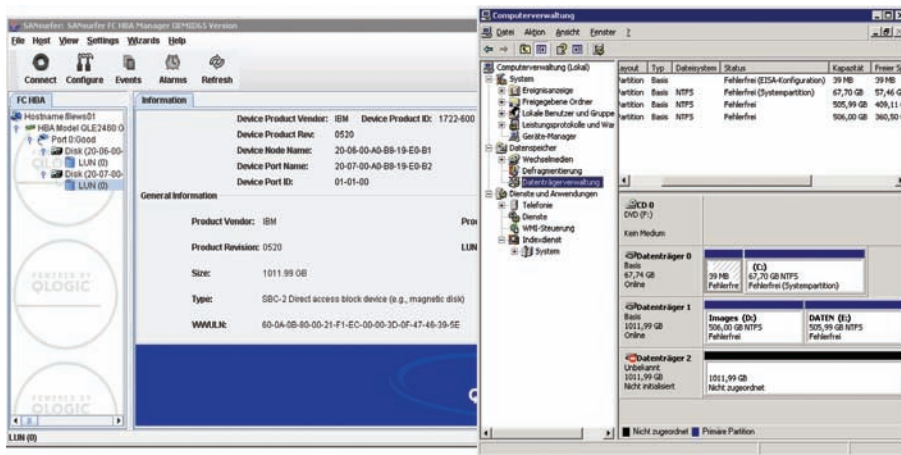


Bild 1: FC-SAN-Systeme werden über FC-HBAs verbunden. Das lokale Betriebssystem greift auf sie wie auf lokale Festplatten zu.

Ein FC-SAN besteht aus den Hostbus-adapttern (HBA) der Server, den Netzwerkkomponenten, wie Hub oder Switch, und den Storage-Komponenten. Bei diesen Elementen handelt es sich sowohl um Festplatten-/RAID-Systeme als auch Tape-Libraries. Die Festplattenspeicher werden für den Server in Einheiten verknüpft und als virtuelle Festplatte angesteuert. Das Betriebssystem und die Applikationen benötigen somit keine Änderungen, es muss nur ein passender Treiber für den Host-Bus-Adapter geladen werden. Grundsätzlich sind FC-SAN-Systeme sehr gut für die Schaffung einer ausfallsicheren Umgebung geeignet – sofern alle Komponenten mehrfach angelegt wurden.

Unterschiede zwischen FC- und IP-SAN

Die Entscheidung für Fibre Channel oder IP-SAN ist natürlich abhängig von den eingesetzten Applikationen im Unternehmen. Die Stärken von FC sind der sequentielle Zugriff und die Bearbeitung sehr großer Dateien. iSCSI eignet sich indes sehr gut für Applikationen mit Random-Zugriffen. Bei kleinen Blockgrößen kann iSCSI möglicherweise schneller sein als Fibre Channel. Eine Vielzahl von Tools etwa für Snap Shots, Replikation, Thin Provisioning oder für die Einbindung in virtuelle Strukturen ist bei iSCSI-Systemen häufig standardmäßig im Lieferumfang enthalten.

Aus der Sicht des angeschlossenen Servers spielt die Art der Anbindung nur eine untergeordnete Rolle. Beide Systeme, Fibre Channel und IP-SAN, bieten virtuelle Festplatten, die direkt vom Server verwendet werden. Der Hauptunterschied liegt in der Geschwindigkeit. Fibre Channel ist für eine serielle und kontinuierliche Hochgeschwindigkeitsübertragung von großen Datenmengen speziell konzipiert worden. Bei einer Anbindung mit 8 GBit/s im Duplex-Betrieb werden Datentransferraten von bis zu 800 MByte/s erreicht. Die übertragenen FC-Frames mit einer Länge von bis zu 2.112 Bytes haben mit nur 36 Bytes einen sehr geringen Protokoll-Overhead.

Wie beim FC-SAN kommt es beim Einsatz von iSCSI zu einer virtuellen Punkt-zu-Punkt-Verbindung mit blockbasiertem Zugriff auf die virtuellen Festplatten. Der Protokoll-Overhead, der mit Ethernet einhergeht, ist jedoch größer als bei Fibre Channel und ein geordnetes, seriellles Eintreffen der Datenpakete ist bei Ethernet nicht garantiert. Obwohl Ethernet ursprünglich für den allgemeinen Netzwerktransfer entwickelt wurde, eignet es sich dennoch für die Storage-Anbindung. Mit der Einführung von 10 GBit-Ethernet ist das Hauptargument "Langsamkeit" gegen IP-SAN hinfällig. Die erreichbaren Durchsätze können mit rund 900 MByte pro Sekunde mithalten, sofern korrekt ge-

plant und entsprechend leistungsfähige Komponenten eingesetzt werden.

Neuer Stern am Himmel: Fibre Channel over Ethernet

Die jüngste Entwicklung im Storage-Bereich stellt "Fibre Channel over Ethernet" (FCoE) dar. FCoE transportiert FC-Pakete über verlustfreie Ethernet-Netzwerke und erlaubt damit die Nutzung von Standard-Netzwerken unter Beibehaltung des FC-Protokolls. Technisch betrachtet ersetzt FCoE die Layer 0 und 1 des Fibre Channel-Stacks durch Ethernet und ermöglicht so eine Integration in bestehende FC-Netzwerke. Im Gegensatz zu iSCSI läuft FCoE nicht über TCP/IP, sondern direkt über Ethernet im Netzwerk-Protokollstack und ist folglich nicht routbar.

Für den Betrieb in FCoE-Netzwerken benötigen Sie so genannte "Converged-Network-Adapter" (CNA), die sowohl die Funktion eines Ethernet- als auch eines FC-Adapters übernehmen. CNAs entlasten die CPU der Systeme, indem sie die Verarbeitung der Ethernet-Pakete selbst vornehmen. Die Leistungen von FCoE hängen sehr stark von der Bandbreite der Ethernet-Verbindungen ab und erreichen nach Abzug des Protokoll-Overheads maximal 110 MByte/s (Gbit-Ethernet) oder 1,1 GByte/s (10 Gbit-Ethernet).

Einsatz von iSCSI TOE NICs

Die Verwendung von iSCSI ist für viele kleinere und mittlere Unternehmen die einfachste und kostengünstigste Lösung, um auf SAN umzusteigen. Jedes aktuelle Betriebssystem liefert die notwendige Software-Komponente, den "iSCSI Software Initiator", mit. Die Aufgabe dieser Software lässt sich einfach beschreiben: die SCSI-Steuerungskommandos an das Storage-System in TCP/IP-Pakete kapseln. Dieser Vorgang verbraucht nur sehr wenige CPU-Ressourcen. Wichtiger als die reine CPU-Leistung des Filers und des Servers, der über iSCSI zugreift, ist die Performance der verwendeten Netzwerkkarten. Die TCP/IP-Verbindungen an sich erzeugen grundsätzlich eine messbare und

auch spürbare Systemlast. Diese Last wird dabei üblicherweise vom Hauptprozessor des Systems getragen. Spezielle Netzwerkkarten, so genannte “iSCSI TCP/IP TOE NICs”, unterstützten die CPU, indem ein spezieller Chip diese Aufgaben übernimmt (Offloading). Als allgemeine Regel kann gelten, dass iSCSI TOE NICs (auch iSCSI HBAs genannt) ab einer mittleren CPU-Auslastung von 50 Prozent während der üblichen Zugriffszeit, 65 Prozent zur Spitzenlast und bei 75 Prozent Auslastung bei Sicherungs- und Spiegelungs-Aufgaben zum Einsatz kommen sollten.

iSCSI HBAs erscheinen gegenüber dem Betriebssystem als SCSI-Karte, die direkt mit den angeschlossenen Laufwerken kommuniziert. Ein weiterer Vorteil der iSCSI HBAs ist die Fähigkeit, direkt über iSCSI zu booten. Da iSCSI HBAs über eigene iSCSI-Initiatoren angesprochen werden, muss die Kompatibilität zum Betriebssystem genau geprüft werden. Intel, einer der größten Hersteller von Netzwerkkarten und I/O-Chips, bezieht zu den speziellen iSCSI HBAs eine deutliche Stellung, die besagt, dass die Leistung der regulären Netzwerkkarten im 1- und 10 GBit-Ethernet-Bereich vollkommen ausreichen würde. Entfällt das Booten des Betriebssystems vom SAN und ist mit keiner besonders intensiven Auslastung zu rechnen, so kann auf iSCSI HBAs verzichtet werden.

Trennung von SAN und LAN

Ein weiterer klarer Vorteil der iSCSI-Anbindung gegenüber Fibre Channel ist die Nutzung der bereits vorhandenen Netzwerk-Hardware. Anstelle von FC-Hubs kommen die deutlich günstigeren Ethernet-Switches zum Einsatz. Im Idealfall betreiben Sie das Storage-Netzwerk komplett getrennt vom LAN. Somit ist gewährleistet, dass ausschließlich für das SAN bestimmter Netzwerkverkehr in diesem Segment übertragen wird und es zwischen den Bereichen nicht zu Multi- oder Broadcast-Verkehr kommt. Ist die Verwendung eines separaten Ethernet-Switches nicht möglich, so ist zumindest die Trennung der Bereiche mit VLANs vorzunehmen.

Fast-Ethernet mit 100 MBit/s ist für ein Storage-Netzwerk aus heutiger Sicht überholt. Am Markt etabliert sind heute 1 GBit-Verbindungen und der Wechsel auf 10 GBit ist bereits im Gange. Ein durchschnittlicher Server im Geschäftsumfeld erzeugt rund 50 bis 200 IOPs (Input/Output Operations je Sekunde) mit einem Datenvolumen von 5 MBit/s. Erfahrungsgemäß lassen sich an einem 1-GBit-Ethernet-Port 80 MByte/s mit 10.000 IOP/s übertragen, ohne dass eine Limitierung von Seiten des Netzwerkanschlusses selbst zum Tragen kommt. Rechnerisch betrachtet können somit bis zu 16 Server über einen einzigen GBit-Port durch einen iSCSI-Filer bedient werden. Die Backplane-Leistung moderner Switches liegt um ein Vielfaches über diesem Wert und dürfte kaum zum "Flaschenhals" werden.

Optimierung mit Jumbo Frames

Kaum ein Begriff ist mit so viel Mythen belegt wie die “Jumbo Frames” des Ethernet. Durchforsten Sie das Internet nach Informationen dazu, so reicht die Bandbreite vom “Lebenselixier der Geschwindigkeit” bis hin zu “einer der dümsten Erfindungen überhaupt”. Die Standardgröße der kleinsten Übertragungseinheit im Ethernet, das Frame, ist zwischen 64 Byte und maximal 1.522 Byte lang. Vergleichen Sie diese Größe mit der typi-

schen Cluster-Größe eines Dateisystems – 4.096 Byte in der Standardeinstellung von Microsofts NTFS –, so wird deutlich, dass für die Übertragung eines einzelnen Speicherblocks des Dateisystems mehrere Ethernet-Frames erforderlich sind.

Viele Frames bedeuten jedoch gleichzeitig ein Ansteigen des Protokoll-Overheads und eine intensivere Nutzung von Interrupts. Jedes Paket muss von der CPU in seine Daten- und Steueranteile zerlegt werden, die Prüfsummen berechnet und anschließend alle Pakete zusammengeheftet werden. Viele kleine Pakete machen folglich einen größeren Aufwand. Die Festlegung auf maximal 1.522 Byte je Frame war jedoch keine absurde Entscheidung. Ein Blick in die Historie von Ethernet verdeutlicht die Notwendigkeit, dass viele kleine Pakete in einem damaligen Netzwerk mit vielen Hubs und Kollisionen die bessere Wahl darstellten. Für ein dediziertes Speichernetzwerk ist die Größenbegrenzung auf 1.522 Byte nicht unbedingt erforderlich.

Alle beteiligten Komponenten wie Switches, Initiators und Targets müssen Sie auf einen exakt gleichen Wert einstellen. Praktischerweise sollte die Jumbo-Frame-Größe die Clustergröße des Dateisystems übersteigen. Typischerweise werden Fra-

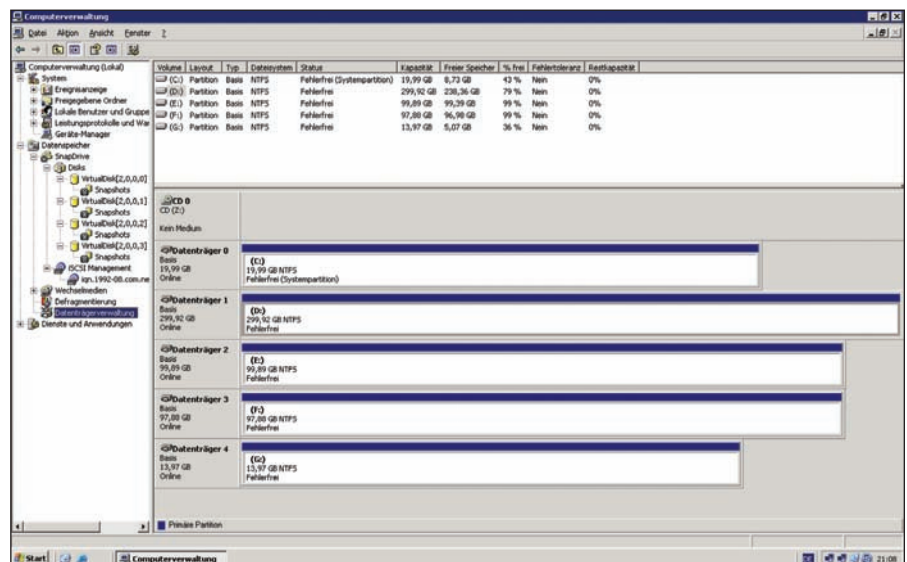


Bild 2: IP-SAN-Systeme verhalten sich gegenüber dem Server-Betriebssystem ebenfalls wie lokale Platten. Zusatzprogramme wie Snapshots werden häufig bei iSCSI NAS-Systemen kostengünstig mitgeliefert.

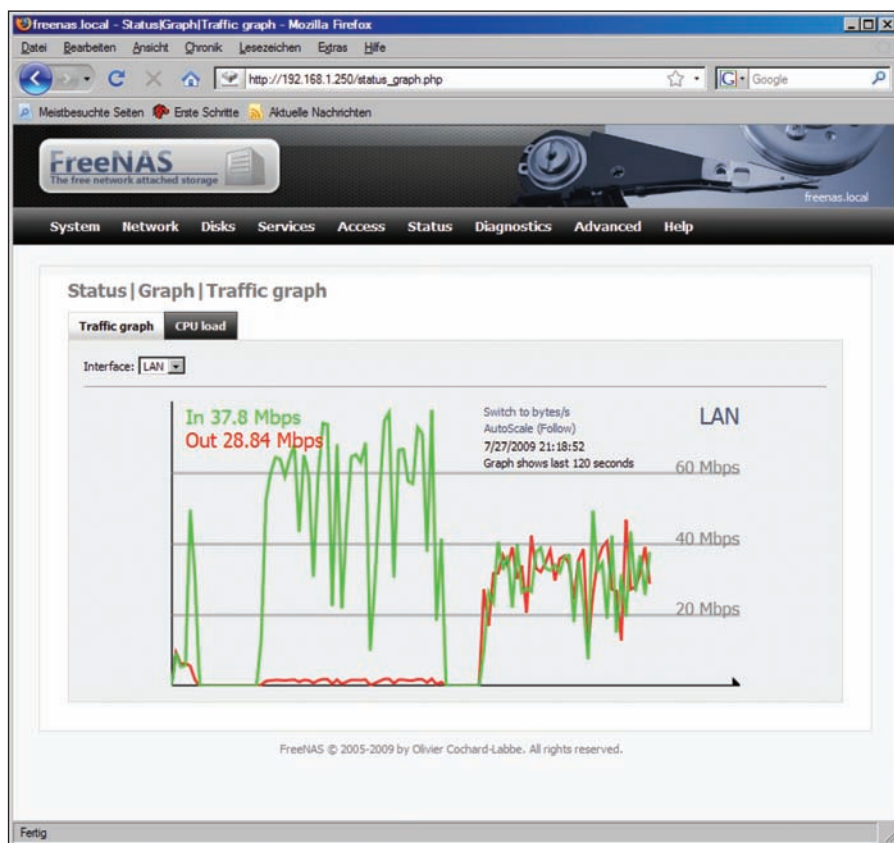


Bild 3: Dank der iSCSI-Unterstützung von FreeNAS wird selbst ein Altrechner zu einem SAN. Angeschlossen über 100 MBit-Ethernet ist mit Höchstleistung kaum zu rechnen.

megrößen von 9, 12, 14 oder 16 KByte verwendet. Die iSCSI-Performance lässt sich so um rund fünf Prozent steigern, während die CPU-Last um zwei bis drei Prozent absinkt. Diese Werte unterliegen stark den Gegebenheiten der Anlage.

Da sich die Implementierung von Jumbo Frames von Hersteller zu Hersteller unterscheidet und kein wirklicher Standard existiert, bleibt lediglich der Versuch, ob in der individuellen Umgebung die Aktivierung von Jumbo Frames eine Verbesserung der Performance mit sich bringt. Nach der Umstellung sollten Sie intensive Tests mit größeren Datenmengen durchführen, um die Stabilität der Anpassung zu prüfen. Stellen Sie beispielsweise die maximale Frame-Größe auf den Filern höher ein als auf einem Switch, so macht die Konfiguration zunächst einen funktionstüchtigen Eindruck. Unter Last werden sich jedoch Disk I/O-Fehler bemerkbar machen. Switches, Router und

Netzwerkkarten, die keine großen Frames kennen, verwerfen die Jumbo-Frames. In diesem Fall werden die "Giants"-Fehlerzähler erhöht.

Langfristigere Planungen

Typischerweise tendieren die meisten IT-Verantwortlichen dazu, mehr Storage-Speicherplatz einzukaufen, als derzeit gefordert. Die Sorge vor dem Vorwurf, dass der Speicherplatz nicht ausreichen würde, dürfte die Erklärung für dieses Verhalten sein. Doch neben den Kosten der eigentlichen Anschaffung beansprucht überflüssiger Speicherplatz Energie, administrativen Aufwand und Stellfläche. Nicht wenige Systeme dürften, bis der Speicherplatz tatsächlich verwendet wird, veraltet sein. Neben dem Einbau schneller Festplatten und der Umstrukturierung im Storage-Netzwerk gibt es noch einen weiteren Ansatz, der jedoch nur mittelbar auf die Performance Einfluss hat. Softwareanbieter wie beispielsweise Datacore mit

"SANmelody" vereinfachen die Verwaltung und die Bereitstellung von Speicherplatz für den Administrator. Die Software legt sich wie eine Abstraktionsschicht zwischen das Storage-System und den Servern. So bildet sich eine einheitliche Ansteuerung von Speichersystemen verschiedener Hersteller. Für Administratoren hat dies den Vorteil, dass sie sich um den tatsächlichen Speicherort immer weniger Gedanken machen müssen und Daten in Pools verwaltet werden.

Fazit

Mit DAS, NAS und SAN stehen Unternehmen die vielfältigsten Storage-Möglichkeiten zur Verfügung. Besonders IP-SAN könnte den Einstieg in SAN-Umgebungen vereinfachen. Unabhängig von der verwendeten Technologie ist es empfehlenswert, zunächst eine Strategie beim Ausbau der Storage-Systeme zu entwickeln. Einer der wichtigsten Tipps hierfür ist das so genannte Tiered Storage. Vereinfacht ausgedrückt werden dabei häufig benötigte Daten auf schnellen, leistungsfähigeren und in der Regel teureren Festplatten und andere auf günstigeren Platten gespeichert. Auf den Punkt gebracht, kommt Tier-1 bei Primärspeichersystemen, Tier-2 für Nearline-Systeme (mit preisgünstigen SATA-Platten) und Tier-3 bei Bandbibliotheken zum Einsatz. Wenn noch mehr Performance gefordert ist, steht Tier-0 in Form von SSD-Speichern bereit. (dr)

1. Halten Sie die Treiber für Host-Bus-Adapter und NICs aktuell.
2. Betreiben Sie so wenige Geräte wie möglich im Storage-Netzwerk.
3. Bieten Sie dem Anwender unterschiedliche Speicherebenen an.
4. Sichern Sie die wichtigen Daten auf Hochgeschwindigkeitslaufwerken.
5. Viele kleinere Festplatten im RAID-Verbund sind schneller als wenige große.
6. Standard-Tools, wie Defragmentierung, sind auch bei SAN erforderlich.

Sechs Tipps für ein leistungsfähiges SAN





Neuerungen im Microsoft Forefront Threat Management Gateway (1)

Neue Mauern für den Schutzwall

von Marc Grote

Microsoft schickt mit Forefront TMG seinen Nachfolger von ISA Server 2006 als sogenannte Unified Threat Management (UTM) Lösung auf den Markt. Mit der Fertigstellung von TMG ist im vierten Quartal 2009 zu rechnen. Bis zum Veröffentlichungstermin können sich jedoch noch einige Funktionen ändern. Microsoft spricht davon, dass die derzeit verfügbare Beta 3 Version von TMG bereits alle Neuerungen beinhaltet, welche auch in dem finalen Produkt verfügbar sein werden. IT-Administrator zeigt in diesem Beitrag, was der neue Wächter mitbringt.

Microsoft Forefront TMG [1] ist eines von vielen bereits existierenden und zukünftigen Produkten unter dem Namen Forefront. Die Produkte bieten einen umfassenden Schutz gegen aktuelle und zukünftige Sicherheitsbedrohungen und sollen gegen bekannte Risiken wie Viren, Spam und potenzielle Hacker-Angriffe schützen. Durch die Schutzmechanismen von Forefront sollen Client, Server und Netzwerk gegen Schadsoftware und gegen Gefahren aus dem Internet mittels VPN und der Firewall-Lösung Forefront TMG abgesichert werden. Die Forefront Security-Managementkonsole stellt eine zentrale Verwaltungsmöglichkeit für die einzelnen Forefront-Produkte [2] zur Verfügung.

Bereits verfügbar ist Forefront TMG in der Medium Business Edition (MBE) [3,4] als Bestandteil des Essential Business Server (EBS). Bei der MBE handelt es sich nicht um einen vollwertigen TMG-Server, die Edition wurde vielmehr speziell für den EBS entwickelt und unter-

stützt bis zu 300 gleichzeitige Benutzer. Der primäre Unterschied zwischen Forefront TMG MBE und Forefront TMG ist, dass MBE als Aufsatz beziehungsweise Erweiterung von ISA Server 2006 entwickelt wurde, wohingegen Forefront TMG die nächste Version von ISA Server 2006 sein wird. Folgende Funktionen stehen nur in Microsoft Forefront TMG, aber nicht in Forefront TMG MBE zur Verfügung:

- TMG Array Unterstützung
- Array im Arbeitsgruppen-Modus
- HTTPS-Inspection
- E-Mailschutz
- Network Inspection System
- ISP-Redundanz
- Zentrale Verwaltung von Standalone- und Array TMG-Servern
- Integration mit Forefront Stirling

Neuerungen in Microsoft Forefront TMG

Die Neuerungen [5] in Forefront TMG konzentrieren sich auf die Kontrolle des

Quelle: dounipix.de



Mit Forefront TMG erneuert Microsoft seinen Sicherheitsvorposten für Unternehmensnetze

Netzwerkzugriffs (Firewall), den Schutz vor Webmanipulationen (Web Client Schutz), E-Mailschutz (Antivirus und Antispam), Eindringlingsschutz (NIS, IDS, IPS), sicheren Remote-Zugriff (VPN, sichere Webserververöffentlichung) und eine vereinfachte Verwaltung (Assistenten). Auf diese Neuerungen gehen wir später im Artikel ein. Weitere Details zu den Anti-Malware- und E-Mail-Schutzfunktionen sowie der Funktionsweise des Network Inspection System (NIS) finden Sie zudem im zweiten Teil unserer Serie.

Voraussetzungen für TMG

Forefront TMG lässt sich in virtualisierten Umgebungen einsetzen, die Microsoft im Windows Server Virtualization Validation Program angibt. Grundsätzlich läuft Forefront TMG ausschließlich unter Windows Server 2008 und R2 64 Bit und stellt folgende Mindestanforderungen an die Hardware:

- Computer mit einem 64 Bit-Prozessor, 1,86 GHz Dual Core-Prozessor

- 2 GByte oder mehr RAM
- 2,5 GByte freier Festplattenspeicher
- Zusätzlicher Festplattenspeicher für das TMG Caching, Malware Inspektion und die Speicherung der Logdateien
- Festplatten oder Partitionen müssen mit dem NTFS-Dateisystem formatiert sein
- Mindestens eine kompatible Netzwerkkarte und mindestens eine weitere Netzwerkkarte für jedes angeschlossene Netzwerk

Installation

Die Installation von Forefront TMG gestaltet sich, wie bereits bei seinen Vorgängern, relativ einfach und mit wenig Zeitaufwand. In der Beta 3 steht nun auch ein Installations-Assistent zur Verfügung, der die notwendigen Voraussetzungen zur Installation von TMG automatisch einrichtet.

Bevor Forefront TMG installiert werden kann, sind folgende Voraussetzungen zu schaffen beziehungsweise werden diese durch den TMG-Installationsassistenten aufgespielt:

- Korrekte DNS-Namensauflösung zur Auflösung interner und externer Ressourcen
- In der Beta 3-Version kann TMG jetzt auch in einer Arbeitsgruppe installiert werden. Eine Domänenmitgliedschaft ist nicht zwingend Voraussetzung
- In dieser Beta-Version kann TMG nicht auf einem Domänencontroller installiert werden (Die Installation von TMG auf einem Domänencontroller ist allgemein keine sinnvolle Idee)
- Microsoft .NET Framework 3.5 oder höher muss installiert sein
- Installation der PowerShell 1.0 (für einen Nur-Lese-Zugriff auf die TMG Konfiguration)
- Installation der Message Queuing-Dienste und der Verzeichnisdienst-Integration

Während des Installationsprozesses wählen Sie die zu installierenden Komponenten aus. Zur Verfügung stehen die Forefront Threat Management Gateway-

Dienste, die Forefront Threat Management Gateway Management-Konsole und der Enterprise Management Server. Für die Installation einer Standalone-Version von TMG müssen Sie die Forefront Threat Management Gateway-Dienste installieren. Der Enterprise Management Server (EMS) dient zur zentralen Verwaltung mehrerer Forefront TMG-Server, der Configuration Storage Server (CSS), verwendet in ISA Server 2004/2006 Enterprise, wird weiterhin als zentraler Datenspeicher der TMG-Konfiguration verwendet. Als nächsten Schritt geben Sie lediglich die IP-Adressbereiche des internen Netzwerks an und können anschließend die Installation durchführen.

Migration von ISA Server 2006

Wenn Sie von ISA Server 2006 Service Pack 1 auf Forefront TMG migrieren, stehen Ihnen die mit SP1 hinzugekommenen Funktionen nicht zur Verfügung. Bis zur Fertigstellung von Forefront TMG ist hier nach unserer Meinung jedoch noch mit einer Änderung zu rechnen. Da ISA Server 2006 nur auf einem 32 Bit Windows Server 2003 betrieben werden kann, Forefront TMG aber nur auf Windows Server 2008 64 Bit läuft, ist keine direkte Aktualisierung möglich. Sie müssen die ISA Server-Konfiguration über die ISA Server 2006-Verwaltungskontrolle in eine XML-Datei exportieren und dann auf einer anderen Hardware Windows Server 2008 und Forefront TMG installieren und anschließend die

exportierte XML-Datei wieder importieren. Derzeit wird die Migration von ISA Server 2000, ISA Server 2004 Standard Edition, ISA Server 2004 Enterprise Edition und ISA Server 2006 Enterprise Edition nicht unterstützt.

Änderungen an der Firewall

An den grundlegenden Firewall-Funktionen hat Forefront TMG wenig Änderungen erfahren – die Einrichtung und Verwaltung von Firewall-Richtlinien hat sich nicht verändert, selbst am Design der Firewall-Verwaltung hat Microsoft kaum Änderungen durchgeführt. Das „Look and Feel“ von ISA Server 2006 zieht sich durch die gesamte TMG-Managementkonsole.

Forefront TMG stellt einige neue Anwendungs- und Webfilter zur Verfügung. Zu den neuen Filtern gehört TFTP (Trivial File Transfer Protocol), GFWA (Generic Web Protocol Analyzer), SIP (Session Initiation Protocol), SSTP (Secure Socket Tunneling Protocol) und der Malware Inspection Filter. Besondere Erwähnung sollte die neue VoIP-Unterstützung finden. Aufgrund von zahlreichen Kundenwünschen hat sich Microsoft nämlich entschieden, Voice over IP grundlegend zu unterstützen. Dies hat jedoch auch einige Einschränkungen – zu den wichtigsten gehören:

- Keine Unterstützung für das iConnect-Here Soft Phone, Polycom Sound Point



Bild 2: Das IPS von Forefront umfasst nun auch die Verhaltensanalyse



501 Phone, Microsoft Response Point und Packet8.

- Keine Secure/Multipurpose Internet Mail Extensions (S/MIME) Verschlüsselung für Nachrichten, welche mit dem Session Initiation Protocol (SIP) übermittelt werden.
- Eine Implementierung, bei der die interne PBX und die internen IP-Telefone in verschiedenen Netzwerken liegen und die interne PBX kein Media Relay ist.

TMG Clients

Forefront TMG stellt wie ISA Server 2006 eine Reihe von Clients zur Verfügung, mit denen Rechner eine Verbindung über TMG zum Internet erhalten:

- Secure NAT Client
- TMG Client (Firewall Client)
- Webproxy Client

TMG beinhaltet wenige Änderungen an den Clients, lediglich der Firewall-Client nutzt eine neue Funktion zur automatischen Erkennung von TMG-Servern. Ein Fire-

wall-Client unter ISA Server 2006 findet einen ISA Server per DHCP oder DNS im Netzwerk. Der Firewall-Client in Forefront TMG stellt eine zusätzliche Variante, den sogenannten "AD Marker", zur Verfügung. Der AD Marker wird zur automatischen Erkennung des Standorts des Firewall-Clients verwendet und dient als Fallback für die automatische Konfiguration per DNS und DHCP. AD Marker kann nur für den aktuellen Firewall-Client verwendet werden und das Fallback findet nur statt, wenn der Firewall-Client feststellen kann, dass kein AD Marker eingerichtet ist.

Web Client- und Malware-Schutz

Einen Schwerpunkt der Neuerungen haben die Microsoft-Entwickler auf den erweiterten Web Client-Schutz gelegt. Zusätzlich zu den schon in ISA Server 2006 enthaltenen Funktionen wie HTTP-Filterung und HTTPS-Inspizierung in Reverse Proxy-Szenarien stellt TMG jetzt auch Anti Malware-Funktionen zum Überprüfen von Webinhalten auf schädlichen Programmcode, einen URL-Fil-

ter sowie auf Wunsch eine ausgehende HTTPS-Inspizierung zur Verfügung.

Forefront TMG schützt den HTTP-Datenverkehr vor Malware, indem der Datenverkehr auf Malware-Signaturen untersucht und nach Vorgaben des Administrators blockiert wird. TMG verwendet dabei die gleiche Malware Protection Engine, die auch von Microsoft Forefront Client Security (FCS), Live One Care und Windows Defender verwendet wird. Einige dieser Malware-Schutzfunktionen lassen sich global konfigurieren, einige Einstellungen können Sie pro Firewall-Regel festlegen und die Malware Inspektion pro Regel aktivieren und deaktivieren. Auch stellen Sie ein, ab welcher Größe Dateien geblockt werden sollen, ob versucht werden soll, infizierte Dateien zu bereinigen, und ob verschlüsselte Dateien blockiert werden sollen. Eine detaillierte Übersicht über die Anti Malware-Funktionen in Forefront TMG finden Sie im zweiten Teil unserer Serie.

Prioritäten setzen in unsicheren Zeiten – Kosten minimieren, Nutzen maximieren

Frankfurt Marriott Hotel - 30. November 2009

Die DatacenterDynamics Konferenz und Expo ist das größte Branchentreffen der Rechenzentrums-Szene. Sie ist Anlaufpunkt für alle RZ-Entscheider, die für Planung, Bau und den Betrieb von IT-Anlagen, vom Netzwerkverteilteraum bis hin zum gesamten Rechenzentrum Verantwortung tragen.

Zu den namhaften Referenten zählen u.A.



Michael Panno

SYSback
Leiter DC Infrastruktur



Daniel Van Der Perre

APC by Schneider Electric
Green Grid



Martin Mast

Diözese Rottenburg-Stuttgart
IT Leiter



Patrick Pulvermüller

Host Europe GmbH
Geschäftsführer



Bernhard Margos

Bechtle GmbH
Geschäftsführer



Dr. Rainer Weidmann

T-Systems Enterprise Services
Leiter, Engineering Infrastructure

**Frühbucherrabatt
nutzen und
100,- Euro sparen**

Telefon
+4420 7377 1907 oder
gebührenfrei aus dem
deutschem Festnetz
unter **0800 180 4050**



FRANKFURT - 30. NOVEMBER 2009

Mediapartner:



Das Magazin für professionelle System- und Netzwerkadministration

www.datacenterdynamics.com/Frankfurt

HTTPS-Inspizierung und Web Access Policies

Forefront TMG ist in der Lage, ausgehenden HTTPS-Datenverkehr zu inspizieren, um Sicherheitsrichtlinien der Unternehmen durchzusetzen. TMG arbeitet dabei als Zertifizierungs-Stelle (CA, Certificate Authority) oder verwendet ein Zertifikat einer internen Zertifizierungsstelle, um als Client im Namen des anfragenden internen Client-PCs zu agieren. Als Administrator können Sie festlegen, ob die Benutzer darüber informiert werden sollen, dass der ausgehende HTTPS-Datenverkehr geprüft wird. Dazu ist die Installation des TMG Firewall Client auf den PCs erforderlich. Die genaue Funktionsweise der HTTPS-Inspizierung-Funktionen erläutern wir im zweiten Teil unserer Serie. Für das Erstellen der Firewall-Regeln für den ausgehenden HTTP/HTTPS-Datenverkehr steht Ihnen ein Assistent zur Verfügung, mit dessen Hilfe Sie sehr einfach Clients den Zugriff auf das Internet gewähren. Der Assistent ermöglicht auch die Konfiguration der Anti-Malware- und HTTPS-Inspizierung-Funktion. Die Managementkonsole trennt jetzt die Firewall-Regeln für den Webzugriff von den restlichen Firewall-Regeln, um für einen besseren Überblick zu sorgen.

Das in der Konsole integrierte Update Center versorgt die verschiedenen TMG-Funktionalitäten übrigens laufend mit Aktualisierungen. In der Beta 3 von TMG betrifft dies die Funktionen Anti-Malware, Anti-Virus und NIS. Sie können dabei die Update-Intervalls der einzelnen Komponenten sowie die automatische Installation der aktuellen Signaturen einstellen.

E-Mailsicherheit

Sie können Forefront TMG als SMTP-Gateway des internen Netzwerks einsetzen und so zum Beispiel in der DMZ platzieren und für die Übermittlung ein- und ausgehender E-Mails verwenden, ohne dass TMG Mitglied der Domäne sein muss. Forefront übernimmt hierbei alle Funktionen des SMTP-Routings und überprüft E-

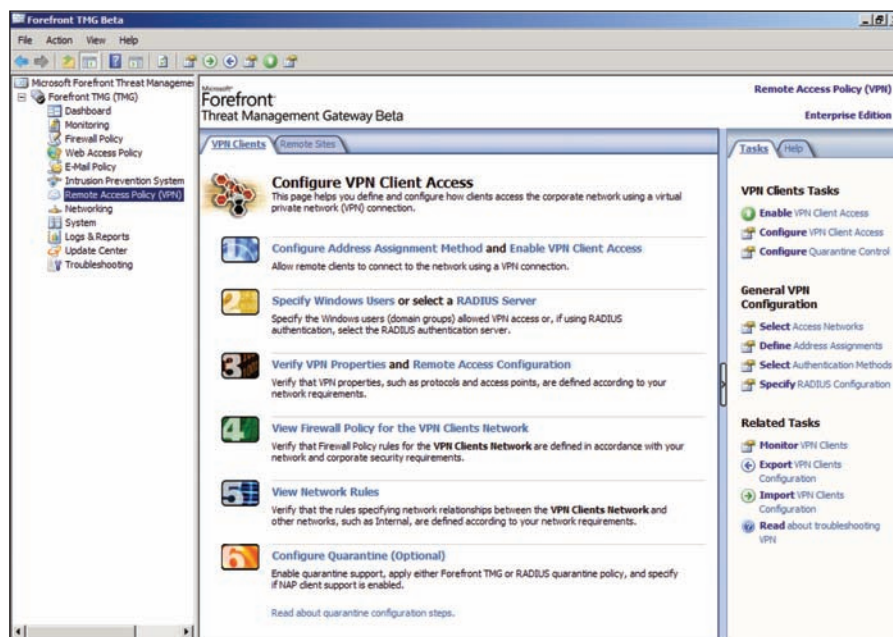


Bild 3: Eine optionale VPN-Quarantäne nimmt zunächst unsichere Rechner auf (unten)

Mails auf Spam und Viren. Für die Anti-spam-Funktionen in TMG kommen die aus Exchange Server 2007 bekannten Edge Server-Funktionen zum Einsatz. Forefront TMG ersetzt somit einen vollwertigen Exchange Edge-Server in der DMZ. Funktionen wie Edgesync werden in der finalen Version von Forefront zur Verfügung stehen. Gegenüber der CTP3-Version von TMG muss die Exchange Server Edge-Rolle jetzt nicht mehr vor TMG installiert werden – der Setup-Assistent von TMG installiert die Rolle im Rahmen des regulären Setups mit. Für die Antivirus-Funktionalität nutzt TMG Funktionen der Forefront Security-Familie. Eine detaillierte Übersicht über die Funktionsweise der E-Mail-Schutzfunktionen geben wir Ihnen im zweiten Teil unserer Serie.

Erweitertes NAT und Eindringlingsschutz

Zu den weiteren Neuerungen von TMG gehört auch die Möglichkeit, eine 1:1-NAT-Funktionalität für den ausgehenden E-Mailverkehr zur Verfügung zu stellen. Sie sind somit in der Lage, die ausgehende IP-Adresse zu spezifizieren, die unter anderen für DNS Reverse Lookups sehr wichtig ist. Das in Forefront TMG integrierte Network Inspection System (NIS)

[6] ist daneben Bestandteil der Intrusion Prevention System-Funktionen (IPS) von TMG. Mit Hilfe von NIS soll TMG in die Lage versetzt werden, unerwünschten Datenverkehr für bekannte Exploits bereits am Gateway zum Internet zu blockieren. Mit NIS soll es einen effektiven Schutz gegen so genannte Zero Day-Exploits geben, bei denen eine bekannt gewordene Sicherheitslücke im System bereits von TMG blockiert wird, damit für die betroffenen Systeme Gegenmaßnahmen in Form von Windows Updates oder ähnlichem durchgeführt werden können. NIS verwendet Signaturen von bekannten Verwundbarkeiten (Vulnerabilities), welche vom Microsoft Response Center zur Verfügung gestellt werden. Das System setzt auf das GAPA-Protokoll (Generic Application Level Protocol Analyzer), das die Generic Application Protocol Specification Language (GAPAL) und eine Analyse-Engine verwendet. Mit dessen Hilfe können Entwickler mit geringem Zeitaufwand Protokoll-Analyser entwickeln, um dynamisch auf neue Bedrohungen durch das Internet zu reagieren.

Wenig Neues beim VPN

Forefront TMG stellt wenige Änderungen im VPN-Bereich zur Verfügung. Forefront



TMG unterstützt weiterhin clientseitiges VPN und Standort-zu-Standort-VPN mit L2TP über IPSEC und PPTP sowie das SSTP (Secure Socket Tunneling Protocol). SSTP wurde mit Windows Vista SP1 und Windows Server 2008 eingeführt und kann VPN-Datenverkehr über SSL 3.0 tunneln. DirectAccess, eine neue Funktion von Windows 7 und Windows Server 2008 R2 mit dessen Unterstützung unter anderen eine permanente VPN-Verbindung von Clients zum Firmennetzwerk möglich ist, steht jetzt in der Beta 3 von Forefront TMG zur Verfügung.

Zu den Neuerungen gehört die Unterstützung von VPN-Quarantäne mit Network Access Protection (NAP) von Windows Server 2008. Auf TMG-Seite ist mit Stand der Erstellung dieses Artikels jedoch weiterhin mit dem schon aus ISA Server 2006 bekannten Remote Access Quarantäne Tool zu arbeiten, um einen RQS-

Listener zu erstellen. Clientseitig ist weiterhin ein mit dem Connection Manager erstelltes VPN-Profil zu verwenden. Eine weitere Neuerung ist die Unterstützung neuer Kryptografie-Algorithmen durch CNG (Cryptography Next Generation), mit dessen Hilfe Administratoren stärkere Verschlüsselungsmethoden (zum Beispiel AES) für VPN-Verbindungen verwenden können. CNG wurde mit Windows Server 2008 eingeführt.

Stirling und weitere Neuerungen

TMG integriert sich in das, derzeit ebenfalls als Beta erhältliche, Forefront Stirling, jetzt umbenannt in Forefront Protection Manager 2010 [7]. Bei Forefront Stirling handelt es sich um ein hochintegriertes Sicherheitssystem, das eine zentrale Managementkonsole zur Verfügung stellt. Über diese sollen sich in Zukunft alle Produkte der Forefront-Familie zentral verwalten lassen und Unternehmen so ein koordinierter Schutz für Client, Server und Edge zur Verfügung stehen. Stirling stellt eine rollenbasierte Konsole mit zentralen Richtlinien und Asset-Funktionen zur Verfügung und soll auf aufkommende Bedrohungen der internen Netzwerkinfrastruktur dynamisch reagieren. Ein Gesamtüberblick über den Sicherheitsstatus aller beteiligten Systeme sowie Reporting-Möglichkeiten runden die Funktionen von Forefront Stirling ab.

Mit Hilfe der Forefront TMG Verwaltungskonsole können Sie jetzt die Konfiguration der Netzwerkadapter vornehmen sowie manuell Netzwerkroutern erstellen. In ISA Server 2006 musste hier noch der Befehl *Route Add* auf der Kommandozeile verwendet werden. Zu den weiteren Neuerungen gehören Funktionen wie die ISP-Redundanz, bei der Forefront TMG bis zu zwei Internetverbindungen zu einer logischen Leitung bündeln oder Lastverteilung durchführen kann.

Forefront TMG verwendet als Protokollspeicher Microsoft SQL Server 2005 Express und für die verbesserten Protokollie-

rungsmöglichkeiten die Microsoft SQL Server 2005 Reporting Services. Mit Microsoft Forefront TMG Beta 3 wurden zudem wieder zwei TMG Versionen – TMG Server Standard und TMG Server Enterprise – eingeführt. Zu welchem Preis die einzelnen Versionen erhältlich sein werden, ist zum Zeitpunkt der Erstellung dieses Artikels noch nicht öffentlich verfügbar.

Es wird weiterhin eine Enterprise Version von TMG (Enterprise Edition Gateway) geben. Das TMG-Team spricht in einem Beitrag des TMG-Forums [8] von einem als "Enterprise Management Server" (EMS) bezeichnetem Produkt, welches die zentrale Verwaltung mindestens eines Enterprise Arrays oder eines alleinstehenden TMG Server übernehmen kann. Der Configuration Storage Server (CSS), erstmals mit ISA Server 2004 Enterprise eingeführt, findet in Forefront TMG weiterhin Verwendung und wird jetzt sogar auf einem alleinstehenden TMG Server als zentraler Datenspeicher verwendet.

Fazit

Microsoft Forefront TMG stellt eine Reihe von sinnvollen Neuerungen gegenüber ISA Server 2006 zur Verfügung. Einige der Neuerungen sind zwar im Markt der UTM-Lösungen nicht wirklich neu, aber Microsoft hat es verstanden, den vielen Kundenwünschen und Anforderungen gerecht zu werden und ist nun in der Lage, der aktuellen Bedrohungslage durch das Internet entgegenzuwirken. Ein Update von ISA Server 2004/2006 auf Microsoft Forefront TMG ist ein relativ einfacher Prozess, so dass sich Firewall-Administratoren leicht dafür entscheiden dürften, auf die neue Firewall von Microsoft zu aktualisieren. Microsoft schreibt sogar davon, dass ein Update von der Standard Version auf die Enterprise Version möglich sein wird.

Damit endet der erste Teil unserer Serie zu Forefront TMG. Im zweiten Teil finden Sie die Details zu den genannten Features wie HTTPS-Inspection und E-Mailsicherheit. (dr)



[1] Download der Forefront-Beta 3

www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=e05aebcd0eb-4e0f-a5db-8f236995bccd

[2] Die Forefront-Familie

www.microsoft.com/forefront/en/us/default.aspx

[3] Forefront MBE

www.microsoft.com/forefront/edgesecurity/isaserver/en/us/tmg-mbe-overview.aspx

[4] FAQs zu Forefront MBE

www.microsoft.com/forefront/edgesecurity/isaserver/en/us/tmg-mbe-faq.aspx

[5] Features der Forefront-Beta

www.microsoft.com/forefront/edgesecurity/isaserver/en/us/tmg-features.aspx

[6] NIS einschalten und einrichten

<http://technet.microsoft.com/en-us/library/dd441065.aspx>

[7] Forefront Protection Manager 2010

www.microsoft.com/forefront/stirling/en/us/default.aspx

[8] Forefront TMG-Forum

<http://social.technet.microsoft.com/Forums/en-US/FTMGNext/thread/af22bb57-6465-4535-bd46-70ff7b64b378>

Links





Virtual Desktop Infrastructure mit VMware View einrichten (4)

Anwendungen virtualisiert

von Andreas Badur und Dr. Jürgen Fechter

Dank Applikationsvirtualisierung führen Sie Programme abstrahiert vom darunter liegenden Betriebssystem aus. Im dritten Teil unserer Workshopserie sind wir auf die Voraussetzungen für die Nutzung von ThinApp zur Anwendungsvirtualisierung eingegangen. Im vierten und abschließenden Teil unserer Serie lesen Sie, wie Sie Anwendungen capturen und welche Neuerungen Version 3.1 von VMware View beinhaltet.

Schalten Sie vor dem Capture-Prozess alles ab, was diesen beeinflussen kann, indem während der Aufzeichnung ungewollt Veränderungen auf der Maschine vorgenommen werden. Dazu gehören Virens Scanner, Windows Updates oder Installations- und Remoteverwaltungstools wie SMS oder NetInstall.

Der Aufzeichnungsprozess verläuft immer in folgender Reihenfolge:

- Voraussetzungen der Software prüfen.
- Erstellen eines Snapshots der frischen Maschine (Prescan).
- Installation und Konfiguration aller Applikation, die in dasselbe Paket sollen.
- Snapshot der Maschine, nachdem die Programme installiert wurden (Postscan).
- TA ermittelt nun die Differenz zwischen erstem und zweitem Snapshot.
- Konfiguration von TA-Parametern, wie Speicherort der Sandbox, Kompression oder Zugriff von Domänenbenutzern und
- Erstellen des TA-Programmpaketes.

Klären Sie die Rahmenbedingungen der Software ab. Dazu gehört die Frage, ob ein Interpreter wie Java, PowerShell, ActivePython oder VisualC benötigt wird und wenn ja, welche Version. Falls Sie verschiedene Versionen gleichzeitig benötigen, sollten Sie zudem klären, ob es dadurch ungewünschte Wechselwirkungen mit anderer Software geben

kann. Gerade Java-basierte Anwendungen sind bekannt dafür, dass sie nicht mit jeder Version der JRE laufen. Hier empfiehlt es sich gegebenenfalls, die passende JRE mit in das Paket zu packen. Falls Sie nicht von einem Netzlaufwerk installieren können, kopieren Sie nun alle für die Installation benötigten Dateien auf Ihre saubere Maschine. Alles, was sich vor dem ersten Snapshot bereits auf der Maschine befand, wird nicht in das Paket aufgenommen.

Starten Sie nun "ThinApp Setup Capture" und klicken Sie einmal auf "Next". Unter "Advanced Settings" können Sie die Pfade des Dateisystems und der Registry bestimmen, die für die Snapshots gescannt werden sollen. Wir belassen es beim Standard, welcher für 90 Prozent der Fälle die optimale Wahl ist. Schließen Sie dieses Fenster wieder und klicken auf "Next". Dadurch wird der initiale Snapshot durchgeführt und gespeichert. Je nach Größe des installierten Betriebssystems und Leistungsfähigkeit der Maschine kann das ein paar Minuten dauern.

Als Nächstes werden Sie aufgefordert, die gewünschte Anwendung zu installieren. Minimieren Sie dazu das TA-Fenster und führen die benötigte Setup-Prozedur durch. Möchten Sie mehrere Programme in diesem Paket haben, installieren Sie nun alle nacheinander. Denken Sie auch da-

ran, die Programme einmal zu starten und wie gewünscht zu konfigurieren. Wir führten dies am Beispiel von Google Earth 5.0 (GE5) durch. GE5 lässt sich nur über einen Google-Update installieren, den wir vor dem ersten Snapshot bereits auf die Maschine legten. Nach dem Start lädt er die benötigten Komponenten herunter und richtet das Programm ein. Wir starteten GE5, deaktivierten die automatische Anzeige der Tipps und schlossen es wieder. Danach maximierten wir "ThinApp Setup Capture" und klickten auf "Next". Dadurch wurde der zweite Snapshot angefertigt und die Differenz aus beiden ermittelt. Letzteres machte TA automatisch.

Sobald dies fertig war, erschien eine Menüseite, auf der wir die "user-accessible entry points" festlegten. Dies sind die Einstiegspunkte, über die die Benutzer später das Programm starten können. Die mit * markierten Punkte "cmd.exe", "regedit.exe" und "iexplore.exe" werden immer angezeigt und dienen dem Debuggen und Testen der Software. Sie können später auch manuell ausgeschaltet werden. Für GE5 deaktivierten wir alle bis auf "Google Earth.exe", "Start Google Earth in DirectX mode.exe" und "Start Google Earth in OpenGL mode.exe". Darunter können Sie den "Primary Container" auswählen, der die Hauptmenge der Dateien und Registry enthalten soll. TA macht Ihnen hier einen

Vorschlag, Sie können aber auch selbst Einträge vornehmen. Wenn der Primary Container kleiner als 200 MByte wird, ist eine EXE-Datei optimal. Da XP und Windows 2000 Probleme mit dem Anzeigen von Icons haben, sobald die Dateigröße 200 MByte überschreitet, wird TA vorschlagen, zusätzlich eine DAT-Datei anzulegen, die den Hauptteil der Daten enthält und einen kleineren Primary Container mit .exe. Zusätzlich können Sie einen anderen Inventarnamen vergeben. Dieser wird bei Benutzung des "thinreg.exe"-Utilities (siehe Kasten "thinreg.exe"-Utility) und bei MSI-Paketen in der Systemsteuerung unter Programme angezeigt und wird intern von TA benutzt. Für GE5 gaben wir "Google Earth" ein.

Nun klickten wir auf "Next". Hier bestand die Möglichkeit, AD-Benutzer oder -Gruppen auszuwählen, die die Anwendung benutzen dürfen. Normalerweise wird hier nichts eingetragen, da es zum einen einfacher ist, dies über den Softwareverteilungsmechanismus des Unternehmens festzulegen und zum anderen bei Änderungen nicht das Softwarepaket neu erstellt werden muss. Der Speicherort der Sandbox ist der Platz, an dem später die virtualisierte Anwendung ihre Daten ablegt, die zur Laufzeit anfallen, also etwa die heruntergeladenen Geodaten von GE5. Das Benutzerprofil ist üblicherweise der richtige Ort dafür – es sei denn, Sie möchten eine portable Anwendung erstellen, die Sie auf Ihrem USB-Stick mitnehmen können. In dem Fall wählen Sie "USB Stick / portable media". Und wenn Sie die Sandbox ganz woanders haben möchten, haben Sie selbstverständlich auch die Möglichkeit einen beliebigen Pfad einzugeben. Hier sind auch UNC-Pfade möglich. Für GE5 wählten wir "User's Profile".

Nach einem Klick auf "Next" stellen wir den Isolationsmodus ein. TA unterstützt drei Modi: "Merged isolation", "WriteCopy isolation" und "Full isolation". Letzterer kann nur manuell und nicht über den Assistenten gesetzt werden. Nähere Informationen hierzu finden Sie unter "Isolationsmodi". Für GE5 wählten wir "merged isolation".

Auf der nächsten Seite legen wir den Speicherort für das Projekt fest. Sie können hier ebenfalls UNC-Pfade einsetzen. Wenn Sie die virtualisierte Anwendung mit MSI verteilen möchten, setzen Sie den entsprechenden Haken und vergeben einen Namen. Ansonsten wird eine EXE-Datei erzeugt, die sich direkt starten lässt. Der Nachteil ist, dass Dateitypzuordnungen, wie .docx zu Office 2007, manuell mit Hilfe des "thinreg.exe"-Utilities erzeugt werden müssen. Dies macht die MSI-Datei automatisch, aber Sie müssen sie dazu erst installieren. Zum Schluss können Sie eine interne Komprimierung aktivieren. VMware gibt den Komprimierungsgrad mit rund 50 Prozent an, weißt aber auch auf schlechtere Performance der Anwendungen hin. Sie sollten die Komprimierung nur benutzen, wenn Sie Platz sparen müssen, etwa auf USB-Sticks. Für GE5 ließen wir alles auf den Standardwerten stehen.

Durch einen Klick auf "Next" wurden nun die Dateien, Registry-Keys und Einstellungen in das Projektverzeichnis kopiert, welches Sie anschließend auch öffnen können. In diesem Verzeichnis liegt die Datei *Package.ini*, in der alle Einstellungen für das Erstellen des Programmpaketes festgehalten sind. Sie können diese mit einem Texteditor verändern und mit Hilfe des "Build Now"-Knopfes jedes Mal ein neues Paket erstellen lassen. Dies wiederholen Sie solange, bis Sie das gewünschte Ergebnis erzielt haben. Für GE5 brauchten wir nichts zu ändern und klickten nur auf "Build Now". Während der Erstellung wurde im Projektverzeichnis ein neuer Ordner "bin" erstellt, der am Ende das Ergebnis enthält. Wenn Sie später Ihr Softwarepaket verändern, indem Sie beispielsweise die Datei *Package.ini* oder die einzelnen Dateien namens *##Attributes.ini* in den Verzeichnissen bearbeiten, können Sie mit der *Start.bat* im Projektverzeichnis ein neues Paket erstellen.

Isolationsmodi

Mit dem Isolationsmodus stellen Sie die Abschottung der Anwendung gegenüber dem Betriebssystem ein. Es gibt die drei Modi "Merged", "WriteCopy" und "Full".

Windows 7 für Administratoren

Das umfassende Handbuch



900 S., Oktober 2009, 49,90 €
» www.galileocomputing.de/2242

SQL Server 2008

Das Programmierhandbuch



1.148 S., 3. Auflage 2009, 59,90 €
» www.galileocomputing.de/2110

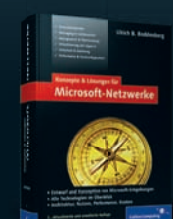
VMware vSphere 4

Video-Training



DVD, Win, Mac, Linux, 83 Lektionen,
10 Stunden Training, 59,90 €
» www.galileocomputing.de/2057

Konzepte und Lösungen für Microsoft-Netzwerke



1.307 S., 2. Auflage 2009, 69,90 €
www.galileocomputing.de/1304

www.GalileoComputing.de

Nur die ersten beiden können Sie über den Captureassistenten auswählen, letzterer muss manuell gesetzt werden. Der Assistent setzt den Parameter "DirectoryIsolationMode" in der Datei *Package.ini*, die sich im Projektspeicherort befindet, entsprechend auf "Merged" beziehungsweise "WriteCopy". Dies definiert den Standardisolutionsmode. Abweichungen können Sie innerhalb des Projektes pro Verzeichnis festlegen, in dem Sie dort die Datei

##Attributes.ini bearbeiten und einen abweichenden Wert eintragen.

Die "Merged"-Isolation erlaubt der Anwendung, Daten auf dem Dateisystem außerhalb des Paketes zu verändern. Der Vorteil ist, dass durch den Anwender gespeicherte Dokumente nicht in der Sandbox liegen, sondern vielmehr dort, wo sie erwartet werden. Der Nachteil ist, dass dadurch auch Veränderungen am Betriebssystem vorgenommen werden können. Der Capture-Assistent nimmt bei "Merged" folgende Einstellungen vor:

- In der Datei *Package.ini* wird der Wert "DirectoryIsolationMode" auf "Merged" gesetzt.
- "%Personal%", "%Desktop%" und "%SystemSystem%\spool" werden ebenfalls auf "Merged" gesetzt. Wenn Daten in den "Meine Dokumente"-Ordner abgelegt werden, speichert TA sie auf dem physikalischen Dateisystem, da TA alles auf dem Dateisystem speichert, ungeachtet der Einstellung.
- Ausgenommen davon sind die Orte "%AppData%", "%Common AppData%", "%Local AppData%", "%Program Files Common%", "%ProgramFilesDir%", "%SystemRoot%" und "%SystemSystem%". Diese bekommen "WriteCopy" verpasst, sprich die Zugriffe werden in die Sandbox umgelenkt.
- Alle Verzeichnisse, die während des Captureprozesses durch die Anwendungsinstallation erstellt werden, bekommen den Isolationsmodus "Full".

Die "WriteCopy"-Isolation erlaubt TA, Schreiboperationen zu unterbrechen und in die Sandbox umzuleiten. Dies wird für alte und/oder nicht vertrauenswürdige An-

wendungen empfohlen. Dieser Modus empfiehlt sich zudem für Desktops mit höheren Sicherheitsansprüchen, bei denen verhindert werden soll, dass Anwender Änderungen am Dateisystem oder Registry vornehmen. Dadurch wird es aber für die Benutzer schwer, ihre gespeicherten Daten zu finden, da diese in der Sandbox liegen. Der Capture-Assistent nimmt bei "WriteCopy" folgende Einstellungen vor:

- In der Datei *Package.ini* wird der Wert "DirectoryIsolationMode" auf "WriteCopy" gesetzt.
- "%AppData%", "%Common AppData%", "%Local AppData%", "%Program Files Common%", "%ProgramFilesDir%", "%SystemRoot%" und "%SystemSystem%" werden ebenfalls auf "WriteCopy" gesetzt.
- "%Personal%", "%Desktop%" und "%SystemSystem%\spool" werden auf "Merged" gesetzt.
- alle Verzeichnisse, die während des Captureprozesses durch die Anwendungsinstallation erstellt werden, bekommen den Isolationsmodus "Full".

Die "Full"-Isolation lässt sich nur manuell in den INI-Dateien des Projektes setzen. Alle Änderungen am Dateisystem oder der Registry werden in die Sandbox umgeleitet und es wird sichergestellt, dass keine

Captureprozess



Bild 1: Der Capture-Prozess läuft stets nach dem gleichen Muster ab

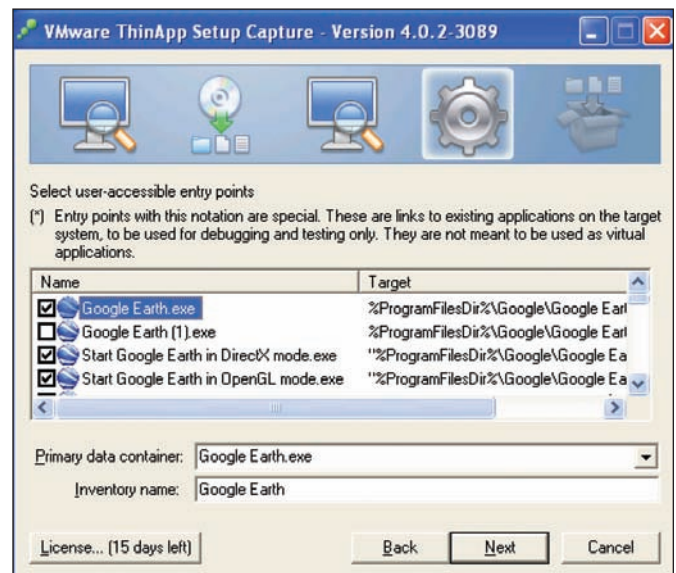


Bild 2: Über die Benutzer-Einstiegspunkte lassen sich die verfügbaren Applikationen starten. Geben Sie die hierfür benötigten Dateien an.



Wechselwirkungen zwischen der virtualisierten Anwendung und dem Betriebssystem entstehen. Dadurch werden auch Konflikte zwischen virtuell und klassisch installierten Programmen vermieden.

Sie benötigen das "thinreg.exe"-Utility, welches normalerweise unter *C:\Program Files\VMware\VMware ThinApp* liegt, um für EXE-basierte Softwarepakete Dateiverknüpfungen zu managen. MSI-basierte Softwarepakete benötigen das Tool nicht, sie lösen diese Aufgaben selbst.

Das "thinreg.exe"-Utility legt Startmenüeinträge und Desktopicons an, setzt Dateiverknüpfungen und generiert Deinstallationsinformationen für die Systemsteuerung. Klicken Sie beispielsweise eine DOCX-Datei mit der rechten Maustaste an, sehen Sie dieselben Optionen wie bei einer nativen Installation von Microsoft Office 2007. Zudem legt es Erweiterungen von Anwendungen wie Quicktime in der Systemsteuerung an.

Die Syntax für das Tool lautet *thinreg.exe {optional Parameter} Paketnamen*. Sie können bei "Paketnamen" mehrere Pakete angeben und auch Wildcards benutzen, um etwa alle Pakete auf einem Fileshare zu registrieren. Folgende optionale Parameter können verwendet werden:

/a,/allusers: Registriert ein Paket für alle Benutzer

/q,/quiet: Unterdrückt Ausgaben

/u,/unregister,/uninstall: Löscht die Registrierung eines Paketes; es wird dadurch auch in der Systemsteuerung unter Programme entfernt. Wenn das Paket mit */a* registriert wurde, muss hier auch wieder */a* benutzt werden

/r,/reregister: Zwingt das Utility dazu, ein bereits registriertes Paket erneut einzutragen

/k,/keep,/keepunauthorized: Verhindert, dass die Registrierungen entfernt werden, wenn der Anwender kein Recht mehr hat, das Paket zu benutzen. Ohne diese Option würde das "thinreg.exe"-Utility diese Informationen entfernen, sobald ein nicht autorisierter Benutzer die Software benutzt. In "PermittedGroups" in der "Package.ini" wird festgelegt, wer die Software benutzen darf

/noarp: Damit werden unter "Systemsteuerung / Programme" keine Einträge angelegt

/norelaunch: Wenn unter Vista erkannt wird, dass zur Ausführung von "thinreg.exe" erweiterte Rechte benötigt werden, startet sich das Tool selbstständig erneut und erzeugt ein UAC-Popup. Erweiterte Rechte benötigt zum Beispiel der */allusers* Parameter. Mit */norelaunch* wird dieser Neustart unterdrückt

"thinreg.exe"-Utility



Unabhängig vom gewählten Modus werden den Schreiboperationen auf Netzlaufwerke oder Wechselmedien in Abhängigkeit der Parameter "SandboxNetworkDrives" und "SandboxRemovableDrives" in der *Package.ini* gesteuert. Beide haben standardmäßig den Wert 0 gesetzt, wodurch die Zugriffe direkt erlaubt werden. Tragen Sie eine 1 ein, wird in die Sandbox umgeleitet. Ebenso unabhängig vom Modus werden alle Änderungen, die zur Laufzeit der Anwendung erfolgen, in die Sandbox umgelenkt.

Aktuelle Neuerungen

Zu Redaktionsschluss dieses Workshops ist VMware View in der Version 3.1 erschienen, die einige Optimierungen und Erweiterungen mitbringt. Grund genug, einen kleinen Blick zu riskieren. Eine der wichtigsten Verbesserungen ist die verkürzte Login-Zeit und die geringere Belastung der Server, so dass auf der gleichen Hardware mehr virtuelle Desktops betrieben werden können. Des Weiteren erzeugt das Logging, welches nun per Default aktiviert ist, mehr aussagekräftige Meldungen, ohne dass dadurch die Performance leidet. Weniger Bandbreite benötigt auch der verbesserte USB-Support. Hier wird nun ein separater TCP/IP-Datenstrom verwendet. Zusätzlich werden noch mehr USB-Geräte unterstützt.

Die Bearbeitung von Desktop Pools ist nun ebenfalls einfacher geworden, da die

Maske umgestaltet wurde und Sie nun beliebig zwischen den einzelnen Schritten hin- und herspringen können. Auf der Seite der Neuerungen finden wir unter anderem die geänderte Struktur der globalen Konfiguration. Für eine bessere Übersicht gibt es nun links eine Spalte, in der Sie eine Vorauswahl treffen können. Klicken Sie etwa auf Servers und danach rechts unten auf Ihren konfigurierten VCS, werden Sie gleich eine weitere Neuerungen sehen: die Möglichkeit, Backups der VCS-Konfiguration zu machen. Wenn Sie den VCS markiert haben und auf "Edit" klicken, können Sie nun auch automatisierte, regelmäßige Backups definieren.

Fazit

Im dritten sowie im vierten und abschließenden Teil des Workshops zu VMware View zeigten wir Ihnen, wie einfach und genial die Technik der Linked Clone Desktops ist. Danach warfen wir zusammen einen Blick auf die Offline Desktops und erläuterten, wie Sie mit dem enthaltenen ThinApp virtuelle Anwendungspakete aufzeichnen und bearbeiten können. Insgesamt bietet VMware hier ein sehr gutes und rundes Paket, um modernes Server-based Computing zu machen, und dort, wo es nicht geht oder keinen Sinn macht, die Verwaltung von Software mit Hilfe von Thin-App zu verbessern. (dr)

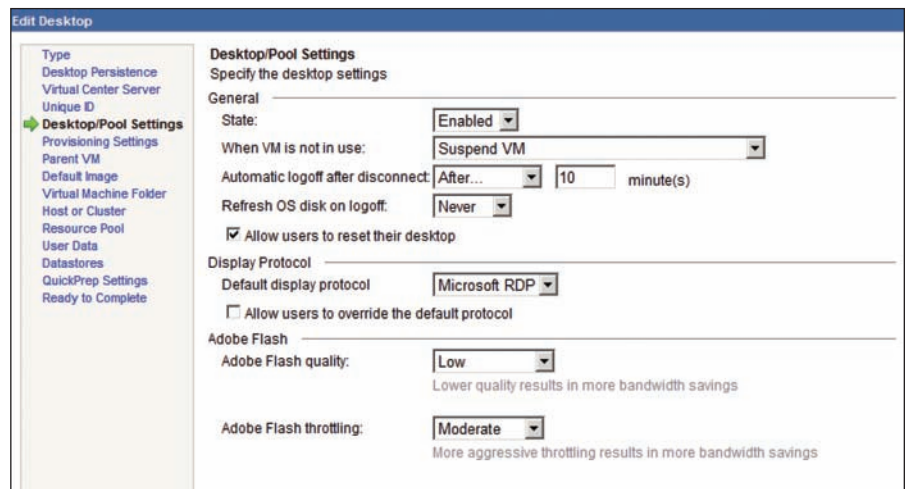


Bild 3: Neue Features der Desktoppools: Sie können nun für jeden Desktoppool die Qualität und Bandbreitennutzung festlegen



CUPS verfügt über alle Mittel, um das Drucken auch in heterogenen Netzwerken so simpel wie möglich zu gestalten

Noch vor wenigen Jahren waren in einschlägigen Linux-Foren sowie der Fachpresse Beiträge zu Drucker-Problemen an der Tagesordnung. Dies hat seit 2009 stark abgenommen. Das Einrichten und Steuern eines lokalen Druckers unter Linux ist dank moderner GUIs in KDE und GNOME sowie dem zugrunde liegenden CUPS-Drucksystem (Common Unix Printing System) schon lange kein Problem mehr. Allerdings stand in früheren Jahren vorrangig die Treiber-Problematik im Mittelpunkt der Diskussionen. Dank hervorragender Treiber-Projekte wie linuxprinting.org sowie dem der steigenden Verbreitung von Linux geschuldeten Engagement der Hersteller hat sich das Thema weitgehend erledigt. CUPS hat aber neben der Bereitstellung von Treibern und dem Verankern einer zuverlässigen Druck-Lösung im Betriebssystem noch deutlich mehr zu bieten.

Universelles Drucksystem in heterogenen Umgebungen

CUPS ist in erster Linie ein vollwertiges, Internet-fähiges Client/Server-Drucksystem und nicht vorrangig für die Bereitstellung von Treibern verantwortlich, wenngleich eine Standard-CUPS-Installation eine Reihe von Filter-Dateien mit-

bringt. Ursprünglich wurde CUPS von Michael Sweet und der Firma Easy Software Products als Nachfolger des betagten Unix-Drucksystems LPD entwickelt und ließ sich seinerzeit sowohl in einer GPL-Version als auch in Form des Produktes "ESP Print Pro" unter einer proprietären Lizenz einsetzen. Seit 2007 ist Michael

Sweet bei Apple angestellt. Apple übernahm die Rechte an CUPS und stellte die kommerzielle Variante ein. Die freie Version kommt seitdem nicht nur in Mac OS X, sondern bei zahlreichen anderen Betriebssystemen, allen voran Linux, zum Einsatz. CUPS besitzt eine Client/Server-Architektur, bei der der CUPS-Client

Drucken unter Linux (2): CUPS Einfach drucken

von Thomas Drilling

Bei Linux, Unix und Mac OS kommt zur Abwicklung von Druckaufträgen seit Jahren das Spooling-System CUPS zum Einsatz. CUPS ist netzwerkfähig, arbeitet zuverlässig und hat sich schnell zum allgemeinen Standard entwickelt. Über das Geräte- und Treiber-Management hinaus bietet CUPS eine Reihe weiterer interessanter Möglichkeiten, die wir Ihnen in diesem Workshop vorstellen. Administratoren heterogener Netze tun gut dran, sich über den Windows-Tellerrand hinaus mit CUPS zu beschäftigen.

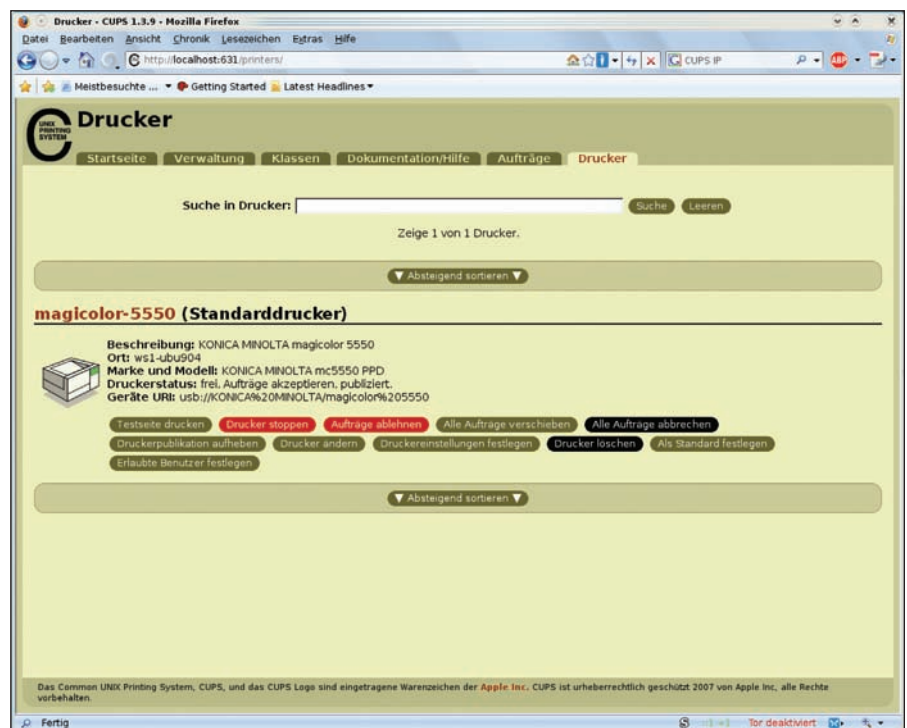


Bild 1: Das Einrichten lokaler Drucker ist mit dem CUPS-Webinterface schnell erledigt



die Druckaufträge verschickt, während sich ein CUPS-Server um den Druckvorgang auf dem Rechner kümmert, an dem das Ausgabegerät angeschlossen ist. Bei lokalen Installationen und Einzelplatzrechnern laufen Client und Server auf der gleichen Maschine.

Modularer Aufbau ermöglicht individuelle Backend-Filter

Der Druckauftrag des Clients landet zunächst in der Druckerwarteschlange, dem Scheduler, der dann die zu druckenden Daten in das portable PostScript-Format konvertiert. Danach gelangen diese Daten an ein so genanntes Backend, das sie wahlweise auf dem angeschlossenen Drucker ausdruckt – wofür es die PostScript-Daten je nach Drucker gegebenenfalls umwandelt – oder über das Netzwerk an einen anderen CUPS-Server schickt. CUPS begünstigt vor allem die Plattform-übergreifende Integration bei heterogenen Netzen, denn der CUPS-Server kann eine Vielzahl unter-

schiedlicher Formate an Druckdaten verarbeiten. Zusammen mit Samba verstehen sich auch Windows-Clients mit einem CUPS-Server. Zudem ist CUPS standardisiert: So enthält CUPS etwa einen eigenen HTTP-Server, der nicht nur die Konfiguration von jedem beliebigen Client im Netz aus im Browser ermöglicht, sondern auch die komplette Verwaltung von Druckaufträgen. Da CUPS modular aufgebaut ist, lässt es sich zudem einfach erweitern.

Der modulare Aufbau von CUPS sorgt dafür, dass sich der Backend-Filter zur Weiterverarbeitung der Daten mit Hilfe von Skripten anpassen lässt. CUPS liefert von Haus aus bereits einige Backends mit, etwa "smb" zur Ansteuerung von Windows-Druckern, "ipp" für den Zugriff auf Warteschlangen anderer CUPS-Hosts im Netzwerk über das Internet Printing Protocol, "pipe" für das Weiterleiten des Druckauftrages an ein anderes Programm, "file" für die Ausgabe in eine Datei oder

"pap" für die Ausgabe auf AppleTalk-basierten Druckern via Netatalk.

Kommunikation über IPP

CUPS steuert die Kommunikation zwischen Server und Client über das eigens entwickelte IPP-Protokoll (Internet Printing Protocol). In der Default-Konfiguration sendet CUPS in regelmäßigen Abständen eine Liste der lokalen Warteschlangen in alle erreichbaren Netze. Damit können alle Hosts, deren CUPS-Server so konfiguriert sind, dass sie diese Broadcasts hören, ohne weitere Konfiguration auf sämtliche von CUPS verwalteten Drucker zugreifen. Somit bringt IPP von sich aus eine Menge Komfort in die Drucker-Konfiguration. Schließen Sie etwa ein Notebook an das Netzwerk an, das so konfiguriert ist, dass der dortige CUPS-Server Broadcasts versendet, findet das Notebook sämtliche Drucker ohne weitere Konfiguration. Dazu muss es nicht einmal die Netzwerkadresse des CUPS-Servers kennen.



12. Gipfel für die Informationstechnologie

Gerade in Krisenzeiten spielt der Punkt Erfahrungsaustausch eine große Rolle. Probleme können diskutiert und von anderen Standpunkten aus betrachtet werden. Gemeinsam können Trends im IT-Bereich erschlossen und brisante Themen erörtert werden.

22. - 24. November 2009
Fairmont Le Montreux Palace
Montreux, Schweiz

Teilnehmer@marcusevanscy.com
www.ciogipfel.com

Neuen Herausforderungen kann man sich nur mit kreativen Ansätzen, innovativen Strategien und neuen Lösungswegen stellen.

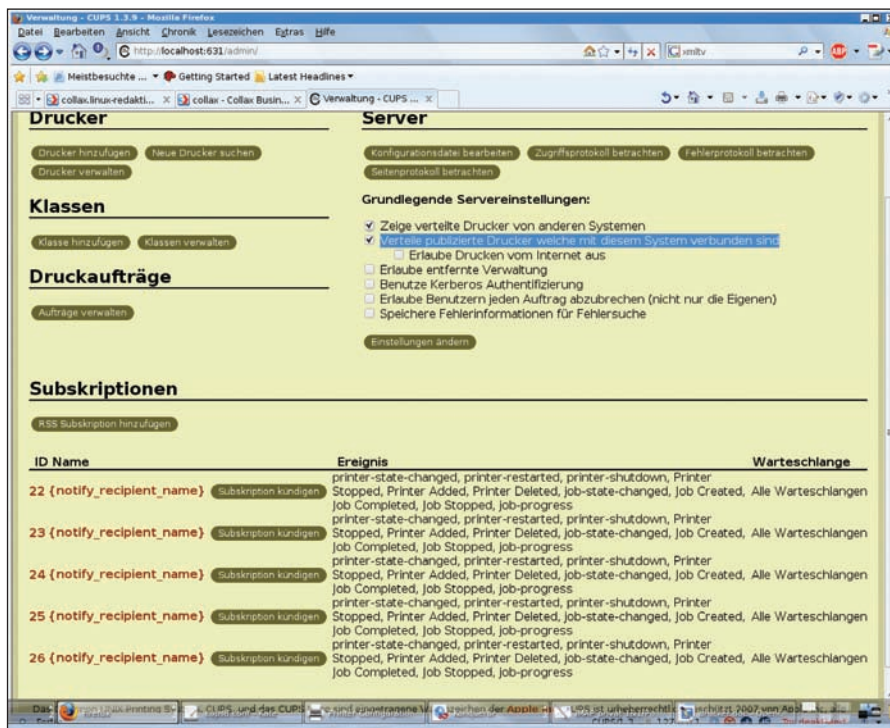


Bild 2: Im CUPS-Webinterface erledigen Sie die Netzwerkfreigabe mit wenigen Mausklicks

Allerdings bringt diese Art der CUPS-Konfiguration ein gewisses Sicherheitsrisiko mit, weil damit möglicherweise potenzielle Angreifer die Adressen und Namen Ihrer CUPS-Server, Druckerwarteschlangen und Drucker erfahren. CUPS lässt sich allerdings auch in Sicherheitsfragen weitgehend frei konfigurieren und beherrscht mehrere Authentifizierungsverfahren. Alternativ zum beschriebenen Broadcasting zum Bekanntmachen von Druckern unterstützt CUPS ein vom Client zu initiiertes "Polling". Ist serverseitiges Broadcasting aus Sicherheitsgründen abgeschaltet, kann der Client immer noch von sich aus beim Server nach Druckerwarteschlangen fragen. Allerdings muss der Client dann die Netzadresse des Servers kennen oder in Erfahrung bringen.

CUPS-Konfiguration

Bei der Konfiguration von CUPS ist zwischen Server- und Client-Konfiguration zu unterscheiden. Die Konfiguration lokaler Drucker – wenn also Client und Server auf ein und derselben Maschine laufen – ist trivial und soll an die-

ser Stelle nicht weiter erläutert werden. KDE und GNOME liefern funktionale GUIs zur Drucker-Einrichtung mit. Außerdem können Sie zur lokalen Druckereinrichtung selbstverständlich das CUPS-Webinterface unter `http://localhost:631/` im Browser benutzen. Auch das Verwalten bereits eingerichteter Drucker und Druckaufträge können Sie im Webinterface erledigen.

CUPS im Netzwerk

Im Folgenden geht es um das Freigeben und Verwalten von Druckern im Netzwerk. Ein lokal mit CUPS funktionierender Drucker ist dazu Voraussetzung. Zur Konfiguration des CUPS-Servers dienen eine Reihe von Konfigurationsdateien, die bei Ubuntu und den meisten anderen Distributionen unter `/etc/cups` zu finden sind. Die wichtigste Konfigurationsdatei zum Einrichten des CUPS-Servers ist `cupsd.conf`. Mit der Option "Browsing On" lässt sich das Browsing einschalten, was allerdings zur CUPS-Grundkonfiguration gehört, ebenso wie der Wert von "BrowseProtocol", der "cups", "slp" oder "all" lauten muss.

Schließlich legt die Option "BrowseAddress" fest, unter welcher Netzwerkadresse der Server die lokal vorhandenen Drucker nach außen publiziert. Der gesamte Abschnitt zur Druckerfreigabe sieht per Default so aus:

```
Browsing On
BrowseOrder allow,deny
BrowseAddress @LOCAL
DefaultAuthType Basic
<Location />
# Allow shared printing...
Order allow,deny
Allow @LOCAL
```

Mit

```
BrowseAddress @LOCAL
```

legen Sie etwa fest, dass der CUPS-Server seine Drucker an alle lokal vorhandenen Netzwerkschnittstellen publiziert, nicht aber an PPP-Interfaces. Für die Internet-Freigabe ist eine separate Option verantwortlich. Mit

```
BrowseAddress @IF(eth0)
```

legen Sie das gewünschte Netzwerkinterface gezielt fest, falls Sie über mehrere Ethernet-Anschlüsse verfügen. Selbstverständlich lässt sich die Freigabe auch auf gezielte Host- und Netzwerkadressen einschränken. Mit dem Kommando

```
BrowseAddress 192.168.0.10
```

veröffentlichen Sie die Warteschlangen nur auf dem Host mit der angegebenen IP-Adresse. Dabei lassen sich wie gewohnt ganze Bereiche respektive Netzwerke eintragen, wie etwa `192.168.0.*`, was das gesamte Subnetz von `192.168.0.0` bis `192.168.0.255` einschließt. Übrigens korrespondiert der Eintrag "BrowseAddress" mit der Option "Verteile publizierte Drucker welche mit diesem System verbunden sind" bei der Konfiguration im CUPS Web-Interface auf der Seite "Verwaltung".

CUPS-Konfiguration per GUI

Wem die Server-Konfiguration aus der Kommandozeile nicht behagt, findet je nach Distribution und installierter Desktop-Umgebung passende grafische Werkzeuge, die neben dem Auffinden und Einrichten von lokalen und Netzwerkdruckern auch die Konfiguration des CUPS-Servers ermöglichen. Bei SUSE finden Sie das YaST-Modul unter "Hardware / Drucker". Die zugehörigen Freigabe-Optionen, etwa zur Konfiguration der Browser-Einstellungen, finden Sie im Bereich "Drucker freigeben", was voraussetzt, dass Sie den Drucker lokal eingerichtet haben und dieser funktioniert. Hier müssen Sie dann die Option "Entfernten Zugriff zulassen" aktivieren und konfigurieren dann das Browsing, indem Sie die Optionen "Für Computer im lokalen Netzwerk" und "Drucker standardmäßig im lokalen Netzwerk bekanntgeben" aktivieren. Darüber hinaus haben Sie im Feld darunter mit Hilfe der Schaltfläche "Hinzufügen" die Möglichkeit, gezielt Netzwerkschnittstellen oder IP-Bereiche auszuwählen, die auf den Drucker zugreifen können.

Für Ubuntu-Nutzer und bei zahlreichen anderen Distributionen steht das GNOME-Werkzeug "Printing" (system-config-printer 1.1.3) zur Verfügung. Hier finden Sie die entsprechenden Einstellungen für den CUPS-Server unter "Server / Einstellungen". Markieren Sie hier die Option "Publish Shared Printers connected to this system". Mit einem Klick auf "Advanced" lässt sich unter anderem das Browsing konfigurieren.

Auch KDE4-Anwendern steht bei allen Distributionen ein KDE-Kontrollfeld zur Druckerkonfiguration zur Verfügung. Dieses ist zwar noch nicht so leistungsfähig, wie das in KDE3.x enthaltene Tool, erfüllt aber seinen Zweck. Sie finden es unter

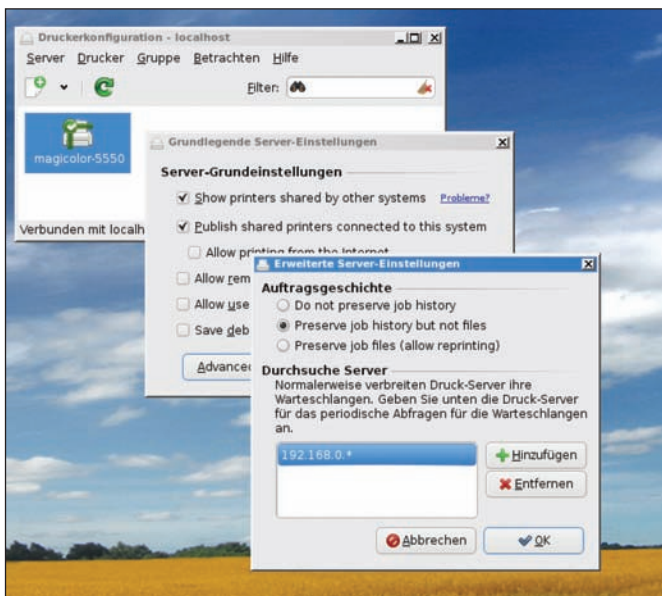


Bild 3: Das GNOME Desktop-Environment bringt ein eigenes, von Red Hat entwickeltes grafisches Werkzeug zur Druckerkonfiguration mit

Workshop in Böblingen

Virtualisierte Infrastrukturen am 29. Oktober 2009

Die Agenda:

12.00 Uhr – Begrüßung durch John Pardey, IT-Administrator Chefredakteur, und Stefan Schnettler, European Marketing Director, Kroll Ontrack

12.15 Uhr – Reinraum-Führung

13 Uhr – Beginn Workshop:

- > Aktueller Stand der Technologie:
 - Hypervisoren – Stärken, Schwächen, Einsatzgebiete
 - Hardwareunterstützung für Virtualisierung
- > Virtuelle Desktops als Ergänzung einer Zentralisierungs- und Bereitstellungsstrategie
- > Quick Wins der Virtualisierung:
Server, Desktops, Storage, Netzwerk – wo anfangen?
- > Diskussion mit Dozenten und Teilnehmern

Referenten: Nico Lüdemann, acocon GmbH;
Nicholas Dille, sepago GmbH; Holger Gantikow, science + computing AG

Workshop-Partner:

- > Datenrettung in virtuellen Umgebungen

ITANet Workshop-Partner:

KROLL ONTRACK®

Referent: Holger Engelland,
Manager Data Recovery Engineering, Kroll Ontrack

Im Anschluss besteht die Möglichkeit, am „Windows 7 HP Community Launch“ im Trainingscenter von Hewlett Packard in der Schickardstraße 32 in Böblingen teilzunehmen.

Mehr Infos und Anmeldung unter www.7launch.de

Termin: 29. Oktober 2009

Ort: Kroll Ontrack GmbH, Hanns-Klemm-Str. 5, 71034 Böblingen

Uhrzeit: 12.00 bis ca. 17.00 Uhr

Teilnahmegebühren:

Für ITANet-Mitglieder und Teilnehmer des „Windows 7 HP Community Launch“ kostenlos.

ITANet Schirmherrschaft:



Anmeldeschluss: 19.10.2009

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

“System / Printer Configuration”. Hier finden Sie die Server-Einstellungen unter “Server Settings”. Aktivieren Sie hier die Option “Share published printers connected to this system”. Die komplementäre Option am Client, die dafür sorgt, dass dieser freigegebene Browse-Listen auch abhört, heißt beim KDE- und beim GNOME-Werkzeug “Show Printers shared by other systems”.

Sicherheit durch Verschlüsselung

CUPS ist nicht nur ein standardisiertes und äußerst flexibles Drucksystem, es ist auch sicherer als seine Vorgänger. CUPS unterscheidet zur Zugriffsregelung drei Sicherheits-Modelle, den “anonymen Zugriff” gänzlich ohne Authentifizierung, die per Default verwendete Authentifizierung über “reguläre Linux-Benutzer” nebst deren Passwörtern sowie das CUPSs eigene Authentifizierungs-System mit MD5-Verschlüsselung (digest). In einer sicheren lokalen Umgebung, etwa hinter der firmeneigenen Firewall, lässt sich je nach Firmenstruktur auf eine Authentifizierung mitunter verzichten, sofern eine solche nicht für ein abteilungsspezifisches Accounting benötigt wird, das CUPS ebenfalls unterstützt. Die per Default verwendete Authentifizierung mittels Linux-Accounts überträgt Benutzernamen und Passwörter allerdings unverschlüsselt, was möglicherweise der globalen Sicherheitsphilosophie im Unternehmen widerspricht.

Verzichten Sie allerdings auf die Option, Browse-Listen ins Internet zu exportieren, bleibt die Gefährdung des gesamten Netzwerkes über das Drucksystem kalkulierbar. Als wirklich sicher lässt sich dagegen nur die CUPS-eigene digest-Authentifizierung einstufen, die Passwörter bei der Übertragung verschlüsselt. So bleibt das Sicherheitsrisiko selbst dann begrenzt, wenn ein Angreifer in den Besitz eines der Hash-Werte gelangt, der keinen Login auf dem System an sich ermöglicht. Übrigens ist CUPS bei openSUSE per Default mit digest-Authentifizierung

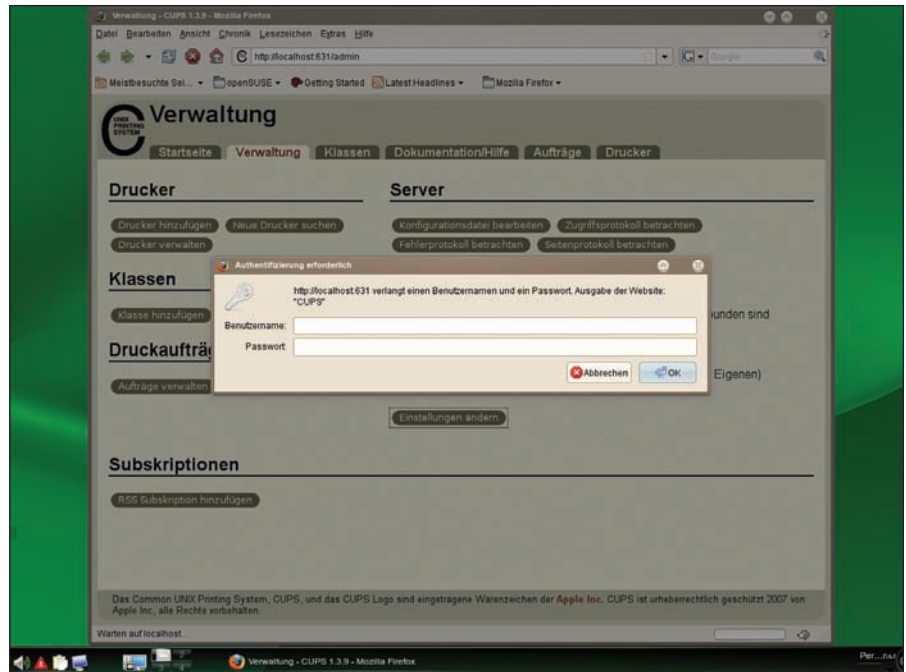


Bild 4: Mit “digest” verfügt CUPS über ein eigenes MD5-Authentifizierungs-System

konfiguriert, was Konsequenzen für die Nutzung des Webinterfaces für administrative Aufgaben hat. Ändern Sie etwa die Server-Einstellungen im Webinterface, verlangt dieses nach einer Authentifizierung. Hierbei handelt es sich allerdings nicht um einen Linux System-Benutzer, sondern um einen CUPS-Account, den Sie mit

```
lppasswd -a -g sys root
```

anlegen können. Dieser ist nicht identisch mit dem entsprechenden Linux-Account. Es ist daher ratsam, für den CUPS-Root ein anderes Passwort zu verwenden als für den System Root-Account. Möchten Sie das Authentifizierungsverfahren global ändern, müssen Sie die zentrale Konfigurationsdatei *cupsd.conf* bemühen. CUPS ist sogar in der Lage, den Zugriff auf den Cups-Server sowie den Zugriff auf Warteschlangen getrennt zu regeln und jeweils unterschiedliche Authentifizierungsverfahren zu benutzen. Das Schlüsselwort ist in allen Fällen der Parameter “AuthType”, der sich mit “digest” oder “basic” belegen lässt. Fehlt die Option ganz, ist anonymer Zugriff erlaubt. Den Zugriff auf den CUPS-Ser-

ver regeln Sie in der Sektion `</Location>`. Fügen Sie zwischen `<Location />` und `</Location>` die Zeile *AuthType digest* ein, ist der Zugriff auf den CUPS-Server ausschließlich mit den Login-Daten möglich, die Sie zuvor mit “lppasswd” eingerichtet haben. Die Sektion `<Location /admin>` dagegen steuert nur die Erlaubnis, Drucker einzurichten oder zu entfernen. Im Block `<Location /jobs>` dagegen regeln Sie, wer Druckaufträge verwalten und auch löschen darf. Ubuntu verwendet in der CUPS-Konfigurationsdatei den globalen Parameter

```
DefaultAuthType Basic
```

und in den einzelnen Location-Sektionen den Eintrag

```
AuthType Default
```

In dieser Hinsicht ist CUPS unter Ubuntu zwar prinzipiell unsicherer konfiguriert, dafür kommen Linux-Umsteiger mit der Druckerkonfiguration ohne weitere Hürden zurecht. Da Ubuntu zudem per Default keinerlei Dienste nach außen freigibt, hält sich die Gefährdung in Grenzen. (In)



Active Directory-Replikation meistern (3)

Alle Standorte im Griff

von Florian Frommherz und Nils Kaczinski

Nachdem wir im ersten Teil der Workshop-Serie die Voraussetzungen für eine Replikation des Active Directory und den Replikationsvorgang selbst vorgestellt haben, erweiterten wir im zweiten Teil örtliche Grenzen und haben die Replikation zwischen entfernten Standorten behandelt. Im dritten und letzten Teil des Workshops geben wir nun Hinweise, die im Umgang mit Active Directory und seiner Replikation nützlich sein können. So zeigen wir Ihnen unter anderem, wie Sie Replikationsverzögerung messen und am besten mit ihr umgehen.

Neben einigen Tipps für den sinnvollen Umgang mit Latenzzeiten wollen wir Sie außerdem auf häufige Missverständnisse aufmerksam machen und zeigen mögliche Stolpersteine auf, damit Sie diese mühelos übersteigen können. Denn nicht immer sind sich Administratoren darüber bewusst, dass sie ihr Verzeichnis durch gewisse Tätigkeiten – etwa das Einspielen von Snapshots – in Gefahr bringen.

Abfangen von Replikationsverzögerungen

Das Kernthema dieser Workshop-Serie ist die Replikation des Active Directory zwischen Domänencontrollern (DC). Die Replikation hilft dabei, an allen DCs den gleichen Datenbankstand herbeizuführen und sorgt dafür, dass sämtliche Änderungen überall zur Ausführung kommen. Dies mag in überschaubaren Umgebungen nachvollziehbar sein, kann in verteilten Strukturen jedoch zu Überraschungen führen, wenn neue Daten oder Änderungen nicht umgehend am anderen Ende der Gesamtstruktur ankommen. Dieses Problem wird als "Propagation Delay" oder Replikationslatenz bezeichnet: die Zeit, welche die Replikation dazu benötigt, um eine Änderung von A nach B zu kommunizieren.

Meist schlagen diese Replikationsverzögerungen dann zu, wenn eine andere Person bestimmte Änderungen an einem Objekt sehnlichst erwartet. Befindet sich diese Person an einem anderen Standort, kann es schon einmal länger dauern, bis die neuen Daten am entfernten Standort auftauchen. Wer sich der Verzögerung bewusst ist, der kann Abhilfe schaffen: Alle Active Directory MMC-Snap-Ins erlauben es, den verbundenen Domänencontroller zu ändern. Werden Anpassungen an Objekten an einem entfernten Standort erwartet, kann sich der Administrator einfach mit einem Domänencontroller des Standortes verbinden und die Änderung direkt dort durchführen – so umgeht er die Verzögerung der Replikation. Wählen Sie dazu im geöffneten Snap-in per Rechtsklick auf den Domänenknoten den Domänencontroller aus.

Sinnvoll ist dieses Vorgehen auch bei Passwortänderungen für Benutzer entfernter Standorte. Durch das Benachrichtigen des PDC-Emulators mit Hilfe der "Immediate Replication" wird die Passwortänderung an eine zentrale Stelle geschickt, um eine schnellere Verteilung neuer Kennwörter zu erreichen. Standort-DCs, die keine direkte Verbindung zum PDC herstellen können und ein Passwort vom PDC verifizieren lassen müssen, profitieren davon allerdings



Quelle: Scott Maxwell – Fotolia.com

Bei der AD-Replikation über mehrere Standorte hinweg ist Balance gefragt

nicht. In diesem Fall weist der Standort-Domänencontroller die Authentifizierung ab und nimmt ein neu vergebenes Passwort, obwohl es der Benutzer korrekt eingegeben hat, nicht an. Das direkte Ändern des Passworts auf einem DC am Standort des Benutzers umgeht dieses Problem.

Replikation von Schema-Änderungen

Das Schema, die Datenbank-Definition des Active Directory, ist für alle Domänen des Forest einheitlich. Daher baut der Verzeichnisdienst hierfür eine eigene Replikationstopologie auf, die sich in größeren Netzwerken von der Replikation der Domänendaten unterscheiden kann. Änderungen am Schema wollen gut geplant sein, denn neben der Replikationslast besteht vor allem ein Risiko, die Funktionalität des AD zu beschädigen.

Ein Beispiel: Ein Unternehmen könnte entscheiden, dass es für seine Mitarbeiter die Schuhgröße im Active Directory spei-



chern muss. Da AD hierfür kein Datenfeld vorsieht, erweitern die Administratoren das Schema und fügen der Objektklasse "User" ein neues Attribut namens "Schuhgroesse" hinzu. Die Personalabteilung pflegt die nötigen Daten ein. Einige Zeit später entfällt der Bedarf für diese Daten. Da sich Erweiterungen des Schemas nicht löschen, sondern nur deaktivieren lassen, schalten sie das Attribut "Schuhgroesse" kurzerhand ab. Mit einem Schlag sind alle Benutzerobjekte ungültig, denn die noch vorhandenen Schuhgrößen-Werte sind in einem Attribut gespeichert, das gar nicht mehr zur Klasse "User" gehört.

Dieses Szenario ließe sich durch etwas Sorgfalt leicht vermeiden, doch es illustriert, wie heikel Manipulationen am Rückgrat des AD sein können. Vor eigenen Arbeiten am Schema gilt es also, genau und vorausschauend zu planen. Doch es gibt ja auch kommerzielle Produkte, die das AD-Schema erweitern, allen voran Exchange. Solche professionellen Schema-Updates sind in der Regel gut durchdacht, sodass keine Schäden durch die Anwendung zu erwarten sind. Trotzdem ist etwas Vorsicht angebracht, denn das Update könnte durch einen Serverausfall mitendrin abrechen, und das zieht erhöhten

Support-Aufwand nach sich. Ein strukturiertes Vorgehen grenzt dieses Risiko sinnvoll ein.

Zum Ersten sollten Sie jede Schema-Erweiterung in einer abgeschotteten Testumgebung prüfen, schon um den Ablauf des Erweiterungsprogramms kennenzulernen, der bei jedem Produkt anders sein kann. Für die produktive Umsetzung im zweiten Schritt empfiehlt sich ein wenig Vorbereitung. Schema-Updates laufen auf dem Domänencontroller ab, der die Rolle "Schema-Master" innehat. Welcher das ist, verrät Ihnen das Kommando `netdom query fsmo` in der Eingabeaufforderung. Sollte das Update komplett fehlschlagen, kann es notwendig sein, den Schema-Master dauerhaft aus dem Netz zu nehmen, daher sollten Sie die Rolle gegebenenfalls auf einen DC übertragen, der keine anderen wichtigen Dienste ausführt.

Melden Sie sich direkt am Schema-Master mit einem Konto an, das der Gruppe "Schema-Admins" angehört. Zwar können Sie eine Schema-Erweiterung theoretisch remote ausführen, doch könnten in diesem Fall Netzwerk-Aussetzer zum Problem werden. Kopieren Sie alle Daten, die der Vorgang benötigt, vom Instal-

lationsmedium der Applikation auf die Festplatte, so können auch DVD-Lesefehler keinen Abbruch erzeugen. Zur Sicherheit sollten Sie nun den Schema-Master vorübergehend von der AD-Replikation ausschließen. Sollte es wider Erwarten danach zu einem kritischen Fehler beim Schema-Update kommen, so bleiben alle anderen Domänencontroller davon unberührt. Mit folgendem Kommando in der Eingabeaufforderung richten Sie dies ein:

```
repadmin /options
+DISABLE_OUTBOUND_REPL
```

Dadurch schaltet Active Directory alle ausgehenden Replikationen ab. Nun führen Sie die Schema-Erweiterung aus. Nach erfolgreichem Abschluss können Sie den Schema-Master wieder in die Replikation einbinden:

```
repadmin /options
-DISABLE_OUTBOUND_REPL
```

Sollte der Ablauf tatsächlich völlig danebengegangen sein, so führen Sie den letzten Befehl nicht aus. Stattdessen trennen Sie den nun unbrauchbaren Schema-Master vom Netzwerk und lassen ihn offline. Übertragen Sie die Schema-Master-Rolle auf einen anderen Domänencontroller und entfernen Sie den abgeschalteten ehemaligen Schema-Master aus dem Active Directory. Hinweise hierzu liefert Artikel 216498 in Microsofts Knowledge Base [1]. Aus der Praxis ist uns allerdings kein Fall bekannt, in dem dies tatsächlich nötig gewesen wäre. Nach einer Schema-Änderung ist in modernen Windows-Netzwerken nicht mit einer wesentlich stärkeren Replikation zu rechnen. Unter Windows 2000 führte jede Manipulation des Schemas noch zu einer Komplettreplikation aller Objekte – das ist seit Windows Server 2003 aber nicht mehr der Fall.

Einfaches Bestimmen der Latenzzeiten

Einzelne Änderungen an Objekten lassen sich ohne Weiteres zwischen Domänen-

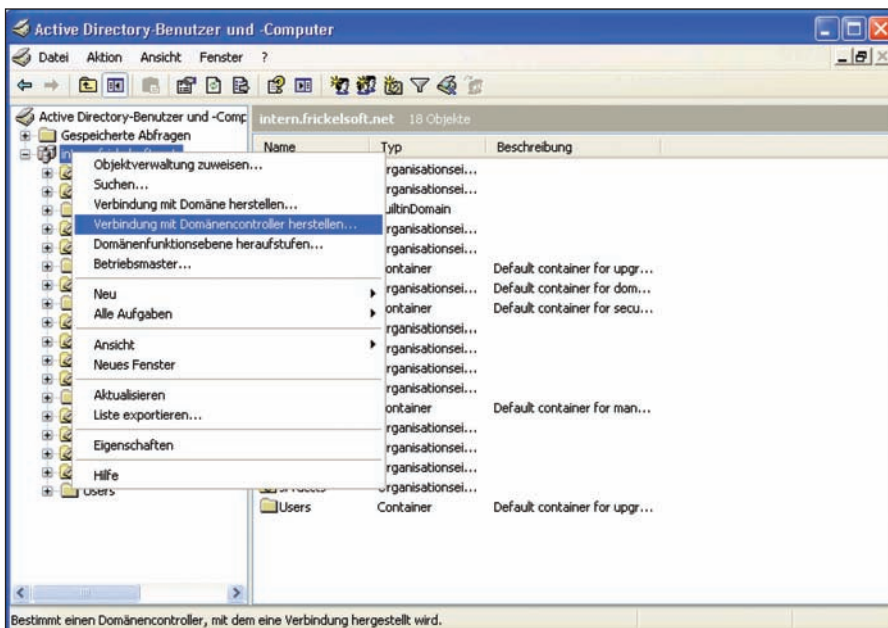


Bild 1: Die Verwaltungskonsolle "Active Directory Benutzer und Computer" erlaubt das Verbinden mit anderen Domänencontrollern

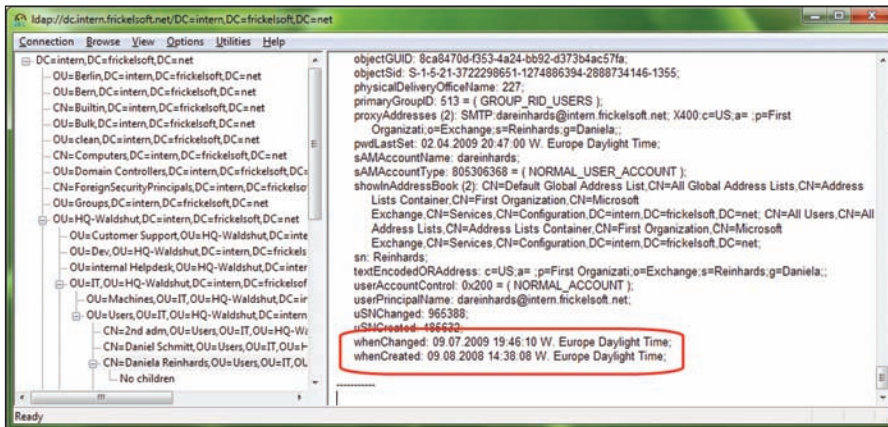


Bild 2: Das Active Directory protokolliert, wann es ein Objekt geändert hat

controllern replizieren. Bei den allermeisten Änderungen dürfte es keine Rolle spielen, wann genau alle Domänencontroller das Update in ihre Datenbank eingepflegt haben. Auf Minuten kommt es nur in seltenen Fällen an. Anders sieht das mit Schemaänderungen aus. Oder einer Massenänderung an Benutzer- und Computerattributen im Active Directory, um eine neu eingeführte Software in allen Standorten benutzen zu können. Dann ist es notwendig zu wissen, wann eine Änderung an welchem Standort vollzogen wurde. Ebenso sollte Ihnen bekannt sein, ob ein Zeitfenster, in dem das Netzwerk unbelastet ist, ausreicht, um die Änderungen zu replizieren. Hier ist eine genaue Information darüber sehr sinnvoll, wie lange das Propagieren von Änderungen an alle Domänencontroller in allen Standorten dauert.

Wie lange die Replikation benötigt, lässt sich mit etwas Mühe aus den Einstellungen im Menü „Active Directory Standorte und Dienste“ herausfinden, indem Sie die Replikationsintervalle betrachten und die maximalen Wartezeiten summieren. Praktischer geht es allerdings mit einem Test: Objekten, die eine Änderung erfahren haben, setzt Active Directory einen Zeitstempel auf. Dieser Zeitstempel wird im Attribut „whenChanged“ auf jedem Domänencontroller gespeichert – und nicht repliziert. Der Domänencontroller setzt den Zeitstempel, so-

bald er von der Änderung erfahren hat und diese in seiner lokalen Datenbank vollzogen hat. Die Zeitstempel unterscheiden sich also von DC zu DC, abhängig davon, wann sie die Änderung durchgeführt haben.

Die Verzögerung der Replikation können Sie mit Hilfe des Attributs „whenChanged“ messen, indem Sie ein Objekt auf einem Domänencontroller erstellen und dann einige Zeit warten, bis die Replikation das Objekt auf allen weiteren DCs erstellt hat. Dann prüfen Sie das Attribut des neuen Objekts auf den DCs – die Differenz des Zeitstempels zwischen „whenChanged“ auf dem Quell-DC, auf dem das Objekt erstellt wurde, und einem DC in einer entfernten Site ist die Zeitdauer, die die Replikation benötigt hat, um die Änderung zu verteilen.

Ausprobieren lässt sich diese Messung entweder von Hand, indem Sie ein Objekt in einem beliebigen NC, selbstverständlich auch den gesamtstrukturweiten, anlegen und anschließend prüfen. Pfiffiger geht es allerdings mit einem Skript namens „ADRepCheckLatency“ [2], das diese Arbeit automatisiert erledigt: Das Skript besteht aus zwei Teilskripten: Das erste Skript *ADRepCheckLatency-Inject.vbs* führt eine Änderung an einem bestimmten Objekt auf einem ausgewählten DC aus. Das zweite Skript *ADRepCheckLatency-Detect.vbs* sucht nach dieser Änderung auf einem anderen DC, den

der Admin als Parameter beim Skriptaufruf angibt. Anschließend zeigt das Skript die Zeitstempelunterschiede für die ausgewählten Domänencontroller an.

Angemerkt sei an dieser Stelle, dass eine einzelne Messung keine eindeutigen Ergebnisse liefert, da das Replikationsintervall zwischen Standorten gerade günstig sein könnte oder der Zeitplan der Replikation nicht mitspielt. Nur wiederholt durchgeführte Messungen, untereinander verglichen und im Durchschnitt betrachtet, vermitteln eine Idee, wie lange eine vollständige Replikation einer Änderung dauern wird.

Warum ein Image kein Backup ist

Replizierte Umgebungen stellen besondere Anforderungen an die Datensicherung: Da es mehr als nur eine Instanz der Daten gibt, muss das System besondere Vorkehrungen für bestimmte Situationen treffen. Betrachten Sie etwa die vielen Vektoren, die das Active Directory zur Kontrolle der Replikation zwischen den Servern verwendet (siehe Teil 1 unserer Workshop-Serie), so erkennen Sie schnell, dass ein Eingriff an der falschen Stelle zum Scheitern des Datenabgleichs führen kann. Die Datensicherung kann ein solcher Eingriff sein, denn sie dient ja gerade dazu, einen historischen Zustand der Datenbank festzuhalten, um diesen ganz oder teilweise wiederherzustellen. Active Directory bietet dafür eine Reihe von Mechanismen, die dafür sorgen, dass das Gesamtsystem dabei nicht aus dem Tritt gerät. Eine beliebte Sicherungsmethode verträgt sich allerdings nicht mit der AD-Replikation: Images und Snapshots. Denn diese beruhen darauf, dass ein ganzes Serversystem sozusagen eingefroren und auf einen exakten Zustand zurückgesetzt wird. Dies ist für Domänencontroller definitiv ungeeignet, wie ein kleines Beispiel zeigt:

Stellen Sie sich eine Domäne vor mit zwei DCs, in der es die Objekte „User1“, „User2“ und „User3“ gibt. Der Server



DC1 hat die letzte Änderung mit der Update Sequence Number (USN) 1147 ausgeführt. Aufgrund der Replikation weiß DC2 dies und speichert für DC1 den High-Watermark-Vektor 1147. In diesem Moment – sagen wir um 14:31 Uhr – erzeugt der Administrator ein Image von DC1. Die Domäne arbeitet weiter und DC1 führt einige weitere Änderungen aus. Um 17:41 Uhr repliziert er das Objekt “User4” mit der USN 1203 an seinen Partner. Dieser speichert die Daten und den neuen High-Watermark-Vektor 1203 für DC1.

Fünf Minuten später hat DC1 einen Fehler und der Administrator spielt das Image von 14:31 Uhr wieder ein. DC1 startet normal – offenbar ist das Problem behoben. Doch der Schein trügt, denn nun fangen die Schwierigkeiten erst an. Denn um 14:31 Uhr kannte DC1 das Objekt “User4” noch gar nicht. Er kann es aber nicht von seinem Replikationspartner erhalten, denn dieser ist ja auf dem aktuellen Stand und weiß, dass DC1 das Objekt bereits kennen muss. Nun ändert sich auf DC1 ein Objekt, wofür er die USN 1148 vergibt. Beim Replikationsversuch erkennt DC2 einen Fehler: Die USN 1148 ist für DC1 gar nicht aktuell, er erwartet Nummer 1204 für die nächste Änderung. Als Folge schaltet DC1 seine Replikation ab und meldet im Eventlog die Fehler 2095 und 2103.

Diese Situation ist als “USN Rollback” bekannt. Das Active Directory erkennt solche Fehler, kann sie aber nicht beheben. Abhilfe für den Admin: Er muss Active Directory von DC1 entfernen und ihn neu zum DC hochstufen. Allerdings können bereits Folgeprobleme aufgetreten sein, etwa doppelte Security-IDs, die nur schwer zu beheben sind. Diese Probleme entstehen immer wieder, wenn Admins ein Image eines Domänencontrollers wiederherstellen. Der einzige Tipp kann hier nur lauten: Setzen Sie niemals einen DC per Image (oder per Snapshot auf VM- oder SAN-Ebene) auf einen historischen Zustand zu-

rück. Nutzen Sie zur Datensicherung das unterstützte Verfahren, also das System-State-Backup. Nur so können Sie auf die korrekte Replikation vertrauen.

Problemzonen Sysvol und Netlogon

Keine Beschreibung der AD-Replikation ist vollständig, wenn sie nicht eine wichtige Komponente des Windows Server Systems bis 2008 beschreibt: FRS. Das Kürzel steht für den “File Replication Service” in Windows, der neben Freigaben des Distributed File Systems (DFS) auch die für Domänen wichtigen Verzeichnisse Sysvol und Netlogon repliziert. Mit diesen beiden veröffentlichten Verzeichnissen macht Active Directory System- und Gruppenrichtlinien verfügbar und bietet eine zentrale Ablagestelle für das Standard-Benutzerprofil für neu angelegte Benutzer. Durch die Replikation durch FRS kann Windows die Daten auf alle Domänencontroller verteilen.

FRS zeigt in seiner Funktionsweise viele Parallelen zu Active Directory. Es ist ein Multi Master-System, das allen Domänencontrollern erlaubt, schreibend auf alle Daten in den replizierten Verzeichnissen zuzugreifen. Der Dienst erkennt mit Hilfe eines Änderungsjournals und der Nutzung von Aktualisierungsnummern – wie Active Directory mit USNs –, welche Partner Änderungen erhalten müssen. Bei der Replikation der Daten müssen sich Administratoren nicht sorgen: FRS ist sich des Standorts bewusst und erkennt, wenn sich ein Replikationspartner in einer anderen Site befindet. Gemäß der in der Konsole “Active Directory Standorte und Dienste” hinterlegten Standortdaten hält es sich an ein konfigurierbares Replikationsintervall zwischen entfernten Standorten: eine Replikation pro Stunde.

Führen Sie sich die Ähnlichkeiten zwischen FRS und Active Directory vor Augen und vergleichen die Komponenten, die für eine erfolgreiche Verteilung von Änderungen Betriebsbereitschaft melden

müssen, unter anderem DNS und Kerberos, erkennen Sie schnell: Soll die Replikation von FRS erfolgreich funktionieren, müssen Sie das Verzeichnis und die Dienste pflegen. Obwohl FRS durchgeführte Änderungen in ein Änderungsjournal schreibt und sich Aktualisierungsnummern (USN) für jede geänderte Datei notiert, kann es in Einzelfällen zu Problemen kommen: Ist ein Replikationsmitglied offline und alle weiteren FRS-Mitglieder erstellen so viele Aktualisierungen, dass vorangegangene Einträge des Änderungsjournals aus Platzmangel überschrieben werden, kann der Offline-Knoten den Anschluss verlieren. Wird die zuletzt vom außer Betrieb genommenen DC erhaltene Änderungs-USN durch eine Flut von Änderungen im Journal überschrieben, gehen zuvor notierte Aktualisierungen verloren. Dieses Verhalten heißt auch “Journal Wrap”.

Um den verlorenen Bruder zurück in die Gemeinschaft zu holen, müssen Sie die FRS-Synchronisation zwischen den Domänencontrollern wiederherstellen. Sie wählen hierzu einen geeigneten Domänencontroller aus, der alle aktuellen Anpassungen repliziert hat und konfigurieren ihn als Replikationsquelle. Den problematischen Domänencontroller konfigurieren Sie als Replikationsziel. Er soll sich alle Änderungen vom Quell-DC holen. Die Neusynchronisation beginnt mit dem Stoppen des FRS-Dienstes auf Quell- und Ziel-DC. Anschließend muss der Registry-Schlüssel “BurFlags” in

[1] Entfernen von Daten aus dem Active Directory nach fehlgeschlagener Domänencontroller-Herabstufung
<http://support.microsoft.com/kb/216498/de/>

[2] Skript zur Messung von Replikations-Latenzen
<http://www.faq-o-matic.net/?s=ADRepCheckLatency>

[3] Beheben von Journalumbruch-Fehlern auf Sysvol- und DFS-Replikatsätzen
<http://support.microsoft.com/kb/292438/de/>

Links



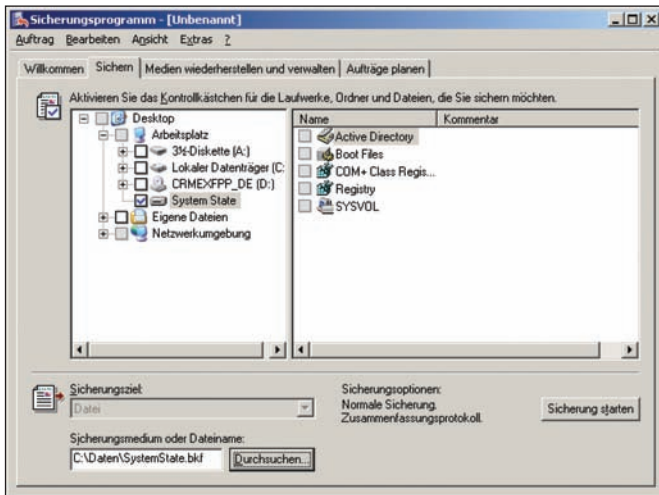


Bild 3: Die Datensicherung des AD sollte nur über geeignete Werkzeuge geschehen, etwa dem eingebauten Backup

“HKLM \ SYSTEM \ CurrentControlSet \ services \ NtFrs \ Parameters \ Cumulative Replica Sets \ {GUI}” angepasst werden. Für den Quell-DC wählen Sie “D4” (hexadezimal), um ihn als “authoritative” zu markieren.

Den zweiten DC, der den Datenbestand des Quell-DCs übernehmen soll, versehen Sie mit dem Wert “D2” (hexadezimal). Gibt es mehrere aus dem Tritt gekommene DCs, konfigurieren Sie alle weiteren DCs ebenfalls mit “D2”, um auch diese zu zwingen, den Datenbestand vom Quell-DC zu laden. Abschließend starten Sie den FRS-Dienst neu. Nach dem Neustart setzen Sie den Schlüssel “BurFlags” auf seinen Vorgabewert “0” zurück. Ist die Neusynchronisation auf dem Ziel-DC abgeschlossen, listet die Ereignisanzeige das Event 13516. Das Verfahren ist in einem weiteren Knowledgebase Artikel [3] ausführlich beschrieben.

Fazit

Active Directory ist ein leistungsfähiger Verzeichnisdienst für Windows-Netzwerke, der ausgefeilte Methoden enthält, um Veränderungen der Umgebung nachzuvollziehen oder Probleme selbst zu beheben. In den meisten kleineren Umgebungen verrichtet Active Directory klaglos seinen Dienst. Nimmt der Admin aber Änderungen an der Konfiguration vor oder treten Fehler auf, für die Active Directory keine Mechanismen enthält, ist es wichtig, die Interna zu verstehen. Unser Workshop hat Ihnen einige der wichtigsten Hintergründe vorgestellt. (In)

Florian Frommherz ist Microsoft-MVP für Gruppenrichtlinien und Systemingenieur bei der Controltech Engineering AG in Liestal in der Schweiz.

Nils Kaczinski ist Microsoft-MVP für Directory Services und Consulting-Leiter der WITstor in Hannover.

Intensivseminar IT-SECURITY in München

27. bis 29. November 2009

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

Diese Hacker-Techniken werden behandelt:

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

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

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

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

Termin: 27. bis 29.11.2009

Ort: GeNUA, Domagkstraße 7, 85551 Kirchheim bei München

Uhrzeit: jeweils 9.00 bis ca. 17.00 Uhr

IT-Administrator Trainings-Partner

GeNUA

Teilnahmegebühren:

Für ITANet-Mitglieder bzw.

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

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

Anmeldeschluss: 16.10.2009

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



Anwendungsvirtualisierung mit Microsoft App-V 4.5 (2)

Dicke Applikationen durch dünne Drähte

von Nico Lüdemann

Im ersten Teil dieser Workshopserie beschäftigten wir uns mit den Grundlagen, der Installation der Serverkomponenten sowie der Basiskonfiguration von App-V 4.5. Zum aktuellen Zeitpunkt verfügen wir bereits über einen voll funktionalen Microsoft Application Virtualization Management-Server, der an den notwendigen Stellen angepasst wurde und auf dem die entsprechenden Strukturen für die Bereitstellung von Anwendungspaketen erstellt sind. Im zweiten Teil des Workshop erstellen wir nun die für unsere Umgebung gewünschten Anwendungspakete, stellen sie im App-V Server bereit und ermöglichen den Benutzern den Zugriff darauf. Und natürlich wollen wir im Nachhinein auch nachvollziehen können, wie gut oder schlecht unsere Umgebung arbeitet und werfen einen Blick auf das Monitoring von App-V. Somit dreht sich in diesem Workshop alles um die Anwendungen und die Benutzer.

Zur Erstellung der Pakete für die Verteilung mittels App-V kommt eine bisher noch unbekannte Komponente ins Spiel – der “Microsoft Application Virtualization Sequencer”, also das Paketierungswerkzeug von App-V. Im Kern handelt es sich hierbei um eine kleine Windows-Anwendung, die in der Lage ist, den Installationsvorgang einer Anwendung zu überwachen und hierbei alle Datei- und Registryzugriffe zu isolieren. Hierzu werden vom Sequencer alle Handles überwacht, die während des Paketierungsvorgangs aufgerufen werden.

Installation des Sequencers

Und genau aus dieser Tatsache und der Vorgehensweise der Snapshot-Erstellung einer Anwendung ergeben sich die Rahmenfaktoren für den Einsatz des Sequencers:

- Er sollte auf einem dedizierten System ausgeführt werden, das exklusiv für diesen Zweck genutzt wird.
- Auch sollten Sie auf diesem System jegliche unnötige Zusatzsoftware wie etwa Virens Scanner vermeiden – das klingt zwar im ersten Moment etwas gewagt, aber in Ihren frisch erstellten

Anwendungspaketen sollten neben den Programmdateien keine Protokolle und Pattern Ihres Virens scanners eingebettet sein, nur weil dieser sich während des Sequenzierens gerade aktualisiert hat. Daher setzen Sie ein eigenständiges System ein, das Sie im optimalen Fall virtuell betreiben und somit für jeden Erstellungsvorgang mittels Snapshot wieder in einen “sauberen” Zustand versetzen können.

- Bezüglich des eingesetzten Betriebssystems sollten Sie den Rat befolgen, auf dem Sequencer jeweils das Betriebssystem (mit dem Service Pack-Standard) zu nutzen, auf dem später auch die Anwendungspakete genutzt werden sollen – hierdurch können Sie sich viele Phänomene und somit Aufwände einsparen.

Ansonsten gibt es an dieser Stelle nur eine weitere kleine Anforderung zu berücksichtigen: App-V nutzt für die Darstellung des virtuellen Dateisystems einen eigenen (ebenfalls virtuellen) Laufwerksbuchstaben: im Standard das Laufwerk “Q”. Dieses wird auf den End-

geräten später über die Installation des App-V-Clients automatisch erstellt, auf dem Sequencer jedoch muss es physikalisch existieren, damit Sie nach Möglichkeit die Anwendungsinstallation in dieses Laufwerk vornehmen können. Somit spricht auch diese Anforderung für den Einsatz eines virtuellen Sequencers, da Sie diesem somit problemlos eine zusätzliche virtuelle Festplatte für das Q-Laufwerk zuordnen können. Sind diese Punkte erfüllt, können Sie direkt mit der Installation des Sequencers fortfahren.

Nach dem Aufruf der Installationsroutine und dem Bestätigen der Lizenzvereinbarung können Sie den gewünschten Installationsordner des App-V Sequencers wählen und schon beginnt der Kopiervorgang der benötigten Programmdateien. Salopp gesagt können Sie an dieser Stelle eigentlich gar nichts falsch machen. Das ändert sich jedoch schlagartig nach der Beendigung der Installation, welche direkt die Option zum Starten des Sequencers bereithält. Zwar kommt das Programm zunächst reichlich unspektakulär daher, jedoch entscheidet spätestens ab



dem Zeitpunkt, an dem Sie “Datei / Neues Paket...” wählen, quasi jede Option über den Erfolg des Paketierungsvorgangs.

Erstellen von Anwendungspaketen

Nach dem Starten des Sequenzierungs-Assistenten müssen Sie dem zu erstellenden Anwendungspaket zunächst einen Namen geben. Eine Beschreibung ist optional, Sie sollten sie aber trotzdem vergeben, um später besser nachvollziehen zu können, wie und wo Sie das entsprechende Paket erstellt haben. Die an dieser Stelle ebenfalls wählbaren “erweiterten Überwachungsoptionen” beziehen sich auf die Einstellung des Streamingpaketes und die Verwaltung etwa von Systemdateien. Diese Einstellungen sollten Sie insbesondere am Anfang im Standard belassen.

Direkt im nächsten Dialogschritt beginnt auch schon der Installationsvorgang der gewünschten Anwendung, den Sie über “Überwachung starten” initiieren. Der Assistent fragt Sie nun nach dem primär zu überwachenden Ordner beziehungsweise dem Ablageort des virtuellen Dateisystems. Dieser Ordner sollte auf Laufwerk Q liegen und eine Benennung entsprechend der 8+3-Konventionen haben.

Was dann folgt, ist im Kern eine standardmäßige Installation der gewünschten Anwendung – etwa des Microsoft Office 2003 – mit einigen kleineren Anpassungen beispielsweise bezüglich der Dateipfade in die Richtung des im obigen Schritt ausgewählten Laufwerk-Q-Pfades (also `Q:\Office.2k3\Microsoft Office`). Bezüglich der auszuwählenden Option ist es an dieser Stelle sinnvoll, wenn Sie alle Optionen auswählen – das Streaming des Anwendungspaketes überträgt später ohnehin nur die Paketeile auf das Endgerät, welche auch benötigt werden. Somit spielt die reine Größe des Paketes nur eine untergeordnete Rolle. Auch Erweiterungen wie Service Packs oder – insbesondere für MS Office – AddOns, wie etwa das Kompatibilitätspaket für Office 2007, können Sie

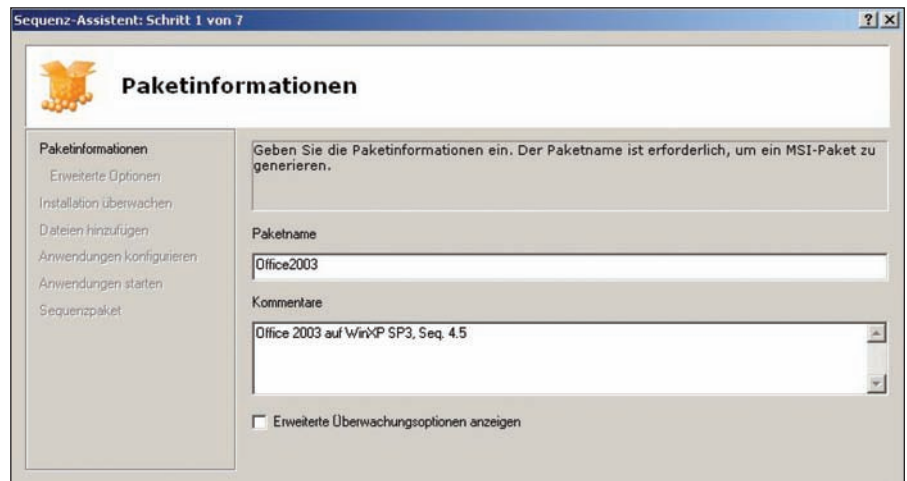


Bild 1: Eine gute Dokumentation des erstellten Paketes ist bei der weiteren Verarbeitung hilfreich

in diesem Schritt ebenfalls mitinstallieren und konfigurieren.

Nachdem Sie alle gewünschten Aktionen durchgeführt haben, können Sie die Überwachung mittels “Überwachung beenden” abschließen. Das System führt anschließend einige administrative Aufgaben durch und bietet Ihnen dann die Möglichkeit, manuell weitere Dateien in das Paket mit aufzunehmen. Dies kann beispielsweise dann Sinn machen, wenn Sie eigene Erweiterungen wie etwa Vorlagen oder Ähnliches in das Paket integrieren wollen.

Im darauffolgenden Schritt bietet Ihnen der Assistent eine Liste aller Anwendungen beziehungsweise aller Anwendungsverknüpfungen, die er während des Überwachungsvorganges erkannt hat. Diese können Sie nun bearbeiten, entfernen oder auch um eigene Verknüpfungen erweitern, die Sie für das Anwendungspaket noch benötigen. Wichtig ist an dieser Stelle zu wissen, dass jede der hier dargestellten Verknüpfungen sich später als OSD-Datei manifestiert und somit als Anwendung an die Benutzer bereitgestellt werden kann. Zwar können Sie auch später noch Anwendungen nachpflegen, dies ist dann aber aufwändiger, als es direkt an dieser Stelle mit durchzuführen.

Sobald Sie mit der Definition beziehungsweise Auswahl der Anwendungen fertig sind, folgt ein Schritt, der ganz we-

sentliche Auswirkungen auf die spätere Leistung des Streamings der Anwendungen hat – das Starten der Anwendungen, wie Bild 3 zeigt. Bei diesem Vorgang starten die Anwendungen zum ersten Mal innerhalb der virtuellen Umgebung und dabei wird analysiert, welche Module und Dateien der Anwendung für den jeweiligen Vorgang benötigt werden. Diese speichert App-V dann im Anwendungspaket – dem Streamingfile – an einer exponierten Stelle, dem so genannten “Feature Block 1”. Der Feature Block 1 wird beim ersten Programmstart eines Benutzers als Erstes und vollständig auf das Endgerät gestreamt und dann dort gecacht.

Somit liegt hier ein großes Potenzial, den Vorgang sehr zu beschleunigen, indem Sie den Feature Block 1 möglichst klein und schlank halten. Andererseits kann es für das Caching und einen eventuellen Offline-Betrieb durchaus sinnvoll sein, ein paar Module mehr an dieser Stelle abzulegen. Grundsätzlich lautet die Empfehlung, dass Sie an dieser Stelle die am häufigsten genutzten Anwendungen mit den dann wiederum am häufigsten genutzten Funktionen kurz durchklicken – wie in unserem Beispiel in Bild 2: Hier starteten wir Microsoft Excel und Word, da es sich hierbei um die wesentlichen Anwendungen handelt.

Haben Sie auch diesen Schritt erfolgreich abgeschlossen, wird das Paket “sequenziert”, also endgültig erstellt und in die jeweiligen Feature-Blöcke gegliedert. Ab

diesem Zeitpunkt ist der Assistenten-durchlauf abgeschlossen und das Paket steht Ihnen für einige manuelle Nacharbeiten zur Verfügung. Sie können nun beispielsweise einsehen, wie die Konfiguration des Paketes aussieht und wie groß beispielsweise der Feature Block 1 geworden ist – im konkreten Beispiel sind es nur etwa 46 MByte im Vergleich zu einer Gesamtpaketgröße von 1,25 GByte.

Grundsätzlich müssen Sie an dieser Stelle keine Anpassungen vornehmen. Es macht jedoch Sinn, auf der zweiten Reiterkarte "Bereitstellung" einmal zu prüfen, ob die Standardwerte für Ihre Umgebung angebracht sind. Hier finden sich die Verbindungskonfigurationen für den späteren Betrieb auf einem App-V Management Server sowie etwa auch Einstellungen für die Betriebssysteme, auf denen das Paket lauffähig sein soll.

Erinnern wir uns an dieser Stelle an den ersten Teil dieses Workshops zurück, in dem wir die Installation der Serverkomponenten vorgenommen haben, so müssen wir bedenken, dass das Verbindungsprotokoll RTSPS im Standard nicht installiert wurde und somit für Verbindungen nicht zur Verfügung steht. Auch möchten wir unterhalb des Content-Ordners vielleicht nicht alle Pakete direkt im Verzeichnis liegen haben, sondern gegebenenfalls in Unterverzeichnissen

organisieren. Aus diesen Gründen sollten Sie die in Bild 3 dargestellten Einstellungen vornehmen.

Anschließend können Sie das Paket über "Datei / Speichern unter" speichern. Im optimalen Fall natürlich direkt in den Content-Ordner und hierbei in das oben gewählte Unterverzeichnis, also in unserem Fall "Office2003".

Erweiterte Optionen – Scripting und Offline-Einsatz

Haben Sie auf diese Weise erst einmal ein Paket erstellt, empfiehlt sich ein kleiner Blick in das entsprechende Verzeichnis, um zu erkennen, woraus denn ein solches Anwendungspaket besteht. Im Kern finden sich im Anwendungsverzeichnis eine Vielzahl von OSD-Dateien (Anwendungsdefinitionen), eine oder mehrere relativ große SFT-Dateien (Archivdateien) sowie eine SPRJ-Datei, in der das Gesamtpaket beschrieben ist.

Besonders interessant ist nun an dieser Stelle eine der OSD-Dateien, da Sie hierin die Definitionen der einzelnen Anwendungen sehen können. Wie Sie relativ schnell erkennen, handelt es sich bei den OSD-Dateien um Beschreibungen im XML-Format, in denen alle Parameter und Eigenschaften der zu veröffentlichen Anwendung beschrieben sind. So finden Sie etwa bei dem Parameter

"CODEBASE HREF..." den Pfad und die Verbindungseinstellungen zur Archivdatei (*.SFT). Eine Suche nach "FILENAME" zeigt Ihnen beispielsweise den Pfad zur Programmdatei an.

Grundsätzlich können Sie die Einstellungen der Anwendung in dieser Datei auch manuell nachbearbeiten, sollten anschließend aber darauf achten, sie im UTF-8-Format zu speichern. Eine Anpassung der OSD-Datei kann beispielsweise dann notwendig sein, wenn Sie für die erfolgreiche Bereitstellung der Anwendung etwa noch vor, während oder nach dem Aufbau der virtuellen Laufzeitumgebung Skriptbefehle ausführen müssen. So können Sie über den Parameter "SCRIPT" die Ausführung von Skripten zu verschiedenen Zeitpunkten (PRE STREAM, POST STREAM, PRE LAUNCH, POST LAUNCH, POST SHUTDOWN) initiieren.

Hierbei können Sie ebenfalls auswählen, ob Sie die Befehle mittels "SCRIPTBODY" direkt in die OSD-Datei schreiben oder mittels "HREF" ein externes Skript aufrufen. Spätestens über die Optionen sind Sie in einem sehr hohen Maß in der Lage, Anwendungen virtualisiert an Ihre Benutzer bereitzustellen.

Darüber hinaus haben Sie auch die Möglichkeit, Anwendungspakete ohne einen App-V-Server einzusetzen. Hierzu wählen Sie im Sequencer die Option "MSI-Paket generieren". In diesem Fall generiert der Sequencer ebenfalls alle gewohnten Dateien und zusätzlich ein MSI-Paket, über das die Anwendung anschließend per MSI-Verteilung (etwa per GPO oder System Center Configuration Manager) zur Verfügung gestellt wird. In jedem Fall muss aber auf dem gewünschten Endgerät der App-V-Client installiert sein.

Installation und Konfiguration der Clientkomponenten

Um den App-V-Client wiederum möglichst aufwandsarm in Ihrer Umgebung zu verteilen, bietet sich ebenfalls die MSI-

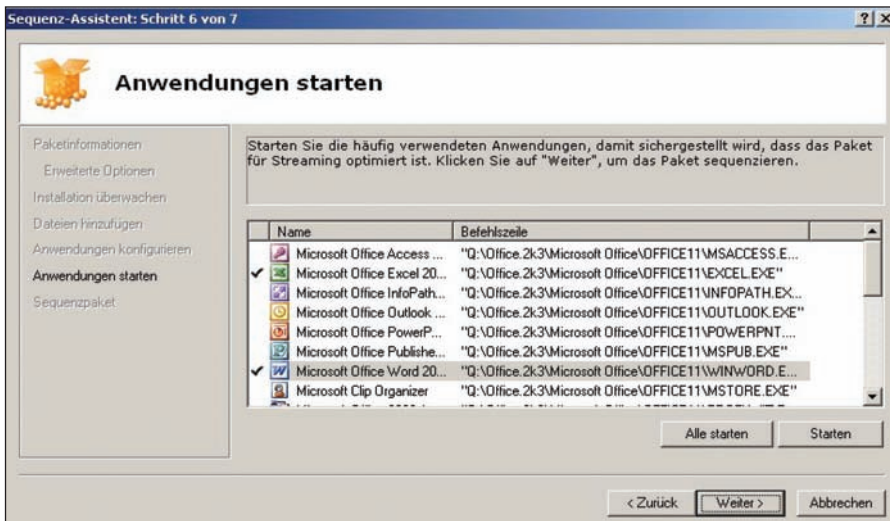


Bild 2: Das erste Starten der Anwendungen ist entscheidend für die Größe des "Feature Block 1" und somit der Performance

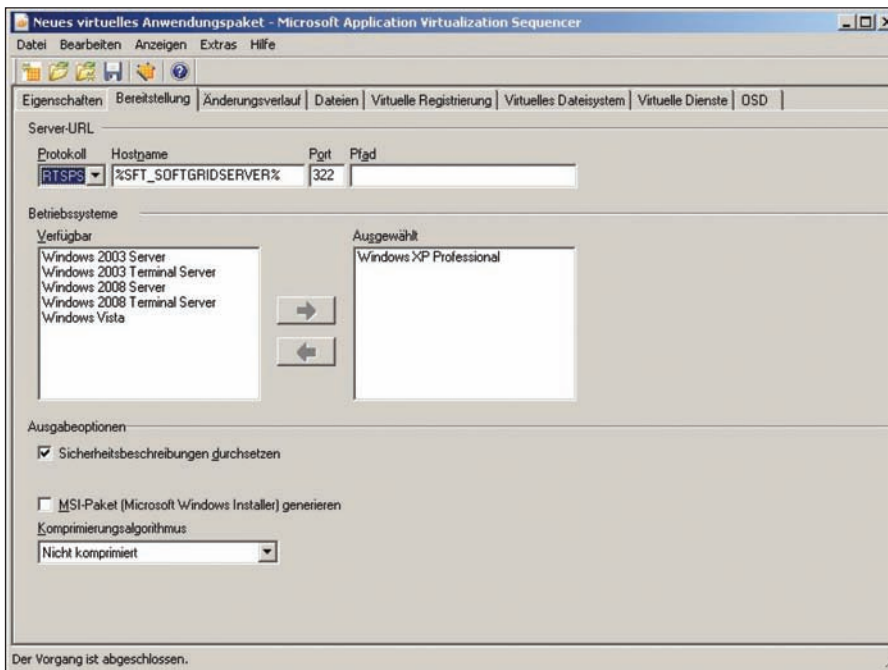


Bild 3: Unter dem Reiter "Bereitstellung" legen Administratoren fest, unter welchen Betriebssystemen das neue Paket laufen soll

Verteilung an. Zwar liegt der App-V-Client auch als ausführbares Setupprogramm vor, für eine automatisierte Verteilung empfiehlt sich jedoch die Verwendung der ebenfalls vorliegenden MSI-Datei. Diese verteilen Sie wie gewohnt per Gruppenrichtlinie oder andere Verteilungswerkzeuge auf die Endgeräte und konfigurieren sie anschließend ebenfalls per GPO. Hierzu stehen sowohl von Microsoft als auch von Drittanbietern entsprechende Administrative Vorlagen (ADM/ADMX) im Internet zur Verfügung. Sofern Sie die Konfiguration manuell durchführen, lässt sich der Client nach der Installation über das Startmenü unter "Verwaltung / Application Virtualization Client" konfigurieren. Im Regelfall wird an dieser Stelle nur eine Eingabe notwendig sein – die Konfiguration der Serververbindung. Diese finden Sie unter "Publishing Servers" und können die Daten dort hinterlegen.

Nun fehlt nur noch ein Schritt, bevor der Client in der Lage ist, bereitgestellte Anwendungen zu starten – Sie müssen die Systemvariable "SFT_SOFTGRIDSERVER" setzen und mit dem Namen des Servers füllen. Dieser Schritt lässt sich recht leicht erklären: Wenn Sie einen erneuten

Blick in eine der OSD-Dateien werfen, werden Sie dort in den Verbindungseinstellungen sehen, dass genau diese Variable für die Adressierung des Servers genutzt wird. Natürlich könnten Sie in allen OSD-Dateien beziehungsweise schon während des Sequenzierens einen festen Servernamen an dieser Stelle verwenden, jedoch würde Sie dies im Nachgang extrem unflexibel bei einer eventuellen Änderung des Servernamens machen. Die Verwendung einer Variablen auf den Clients ist hierbei deutlich einfacher zu handhaben.

Mit diesem Schritt ist der Arbeit am Client zunächst abgeschlossen und Sie können nun die erstellten Anwendungspakete auf dem Server veröffentlichen.

Bereitstellen von Anwendungen

Für die Bereitstellung von Anwendungen an die nun in Betrieb genommenen Clients wenden wir uns wieder der App-V Management Console auf dem Server zu. Wählen Sie hierbei über einen Rechtsklick auf "Anwendungen" die Option "Anwendungen importieren" aus. Hiermit starten Sie einen Dialog, in dem Sie die Projektdatei des Anwendungspaketes auswählen können.

Da die Projektdatei wiederum alle Informationen über alle in dem Paket enthaltenen Informationen beinhaltet, stellen Sie auf diesem Weg direkt alle Anwendungen hlag bereit. Auf diesem Wege konfigurieren Sie beispielsweise auch für alle Anwendungen den Ablageort im Startmenü. Nach dem Abschluss der Dialogschritte ist die Veröffentlichung abgeschlossen und Sie können die Anwendungen in der Konsole einsehen.

Starten von Anwendungen

Haben Sie auf diese Weise alle gewünschten Anwendungen über die App-V Management Console veröffentlicht, sind die Benutzer nun in der Lage, darauf zuzugreifen. Hierzu sollten Sie im Client ein-

SEMINARMARKT

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

www.it-administrator.de/seminarmarkt

Mit Wissen zum Erfolg



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

CITRIX

DataCore

IGEL

Microsoft

SONICWALL

SWH

Buchen Sie noch heute!

02327.9912-425

www.adn.de/training



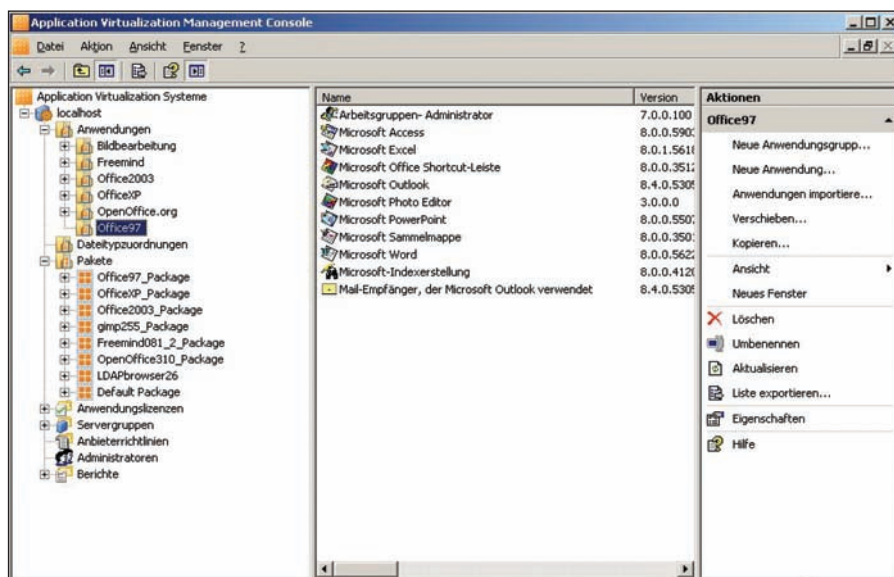


Bild 4: Die Veröffentlichung ist abgeschlossen und die Anwendungen erscheinen in der Management Console

mal kurz den Server “refreshen” beziehungsweise sich als Benutzer einmal kurz ab- und wieder anmelden. Anschließend finden Sie die bereitgestellten Anwendungen je nach Veröffentlichungsort im Startmenü, auf dem Desktop oder an beiden Stellen vor. Über einen Doppelklick auf eine der Anwendungsverknüpfungen wird die Anwendung gestartet, was Sie in einem kleinen Statusbalken über den Tasktray nachvollziehen können. Ab diesem Zeitpunkt lässt sich die Anwendung von den Benutzern ganz regulär verwenden.

Troubleshooting und Reporting

Für den Fall, dass die Anwendungen nicht wie gewünscht starten oder Sie im Nachhinein nachvollziehen wollen, wie die Anwendungen von den Benutzern verwendet wurden, stehen in App-V diverse Protokollierungsstufen und ein integriertes Berichtswesen, welches schnell einen Ein- und Überblick verschafft, bereit.

Bei der Protokollierung unterscheiden wir grundsätzlich zwischen der Serverseitigen Protokollierung und der Protokollierung auf dem Endgerät. Auf dem Server ist die erste Stufe der Protokollierung die Windows Ereignisanzeige. In dieser finden sich eine Vielzahl von Informationen, Warnungen oder Fehlermeldungen, wenn etwas mit dem System nicht stimmt.

Insofern lohnt ein Blick in die Ereignisanzeige in jedem Fall. Insbesondere für Probleme mit dem Streaming oder der Funktionalität der Management-Komponenten existiert aber auch eine Protokolldatei im Dateisystem, welche noch tiefere Einblicke ermöglicht. Diese Datei mit dem Namen *SFT-SERVER.LOG* finden Sie im Installationsverzeichnis des Management Servers im Unterordner “LOGS”. In dieser Datei finden Sie Einträge zu jeder Serveraktion – gleich ob erfolgreich oder fehlgeschlagen –, so dass dies die universelle Informationsquelle darstellt. Allerdings beinhaltet sie auf der anderen Seite wiederum so viele Informationen, dass der vorherige Blick in die Windows Ereignisanzeige auf jeden Fall trotzdem sinnvoll ist.

In Bezug auf die Berichtsoptionen der App-V-Umgebung finden Sie diese in der Management Console unter dem Punkte “Berichte”. Hier können Sie über einen Rechtsklick einen neuen Bericht erstellen und dabei über einen Assistenten auswählen, welche Art von Bericht Sie gerne einsehen würden. So verschafft Ihnen beispielsweise der Bericht “Systemverwendung” einen guten

Überblick darüber, wie Ihre App-V-Server genutzt werden. Auch der Bericht “Anwendungsverwendung” kann interessant sein – er ermöglicht, eine Aussage über die Nutzung einer einzelnen Anwendung zu treffen.

Fazit

Durch die Anwendungsvirtualisierung mit App-V verlieren auch komplexe Szenarien schnell an Bedrohung, denn was sind schon 40 Anwendungen und Anwendungsversionen, wenn Sie sie ohne Abhängigkeiten und negative Wechselwirkungen untereinander auf die Endgeräte verteilen können – ganz ohne Installation der Anwendungen. Jeder Benutzer ist direkt und auf nur einem Endgerät in der Lage, beispielsweise Access 97 und 2003 parallel zu nutzen – zumindest dann, wenn Sie ihm die entsprechenden Anwendungsberechtigungen hierfür erteilt haben. Dies reduziert den Aufwand in der Administration, am Benutzer und nicht zuletzt in vielen Fällen auch die Anzahl der benötigten Endgeräte. (jp)



Dieser Beitrag ist eine Vorabveröffentlichung aus dem im Oktober 2009 erscheinenden IT-Administrator-Sonderheft “Virtualisierung – Aufbau und Betrieb virtueller Infrastrukturen”.

Sie erhalten auf 180 Seiten zahlreiche praxisnahe Anleitungen zur konkreten Umsetzung von Virtualisierungsprojekten. Zugleich gewährt das Sonderheft dem Leser aber auch einen Einblick in die Stärken und Schwächen der verschiedenen Lösungen und hilft so bei der Produktauswahl.

Als Abonnent können Sie das Sonderheft jetzt zum Vorzugspreis von € 29,90 bestellen (Nicht-Abonnenten erhalten das Sonderheft zum Preis von € 34,90. Die Preise verstehen sich jeweils inklusive Versand und 7% MwSt.).

Jetzt Vorbestellen:
Sonderheft Virtualisierung





Tipps zur PowerShell 2

Active Directory-Verwaltung mit der PowerShell

von Rolf Masuch

In den Ausgaben 07 und 08/2008 des IT-Administrator haben wir Ihnen die PowerShell als Werkzeug für die Windows-Administration vorgestellt. Dabei stand das Erlernen der Sprache im Vordergrund. Jetzt muss die PowerShell [1] in unserer neuen Tipp-Reihe beweisen, dass sie auch alltagstauglich ist. Dazu haben wir uns für diesen Monat die Verwaltung des Active Directory als Aufgabe gestellt.

Die neuen AD-Cmdlets im Modul

Die neue PowerShell 2, die mit Windows 7 und Windows Server 2008 R2 verfügbar sein wird, stellt einen Satz von 76 Cmdlets zur Verwaltung des Active Directory bereit. Microsoft hat diese Cmdlets dabei als Modul implementiert. Diese neue Variante der Bereitstellung ist erst mit der Version 2 möglich. Zusätzlich wird mit diesem Modul ein Provider für das Active Directory eingebunden. Damit lässt sich die Domäne als Laufwerk verbinden. Der Standardlaufwerksbezeichner ist "AD". Auf diesem Weg wechseln Sie mit dem einfachen Befehl `cd AD:` in das Active Directory, ganz so, als würden Sie zwischen Laufwerken im Dateisystem wechseln. Der Prompt ändert sich auf "PS AD:>" und zeigt so das neue Laufwerk an.

Installation der Rollen

Um in den Genuss der neuen Cmdlets zu kommen, müssen Sie unter Windows Server 2008 R2 die Rolle "Active Directory Directory Services" (AD DS) installieren. Alternativ können Sie die Rolle "Active Directory Lightweight

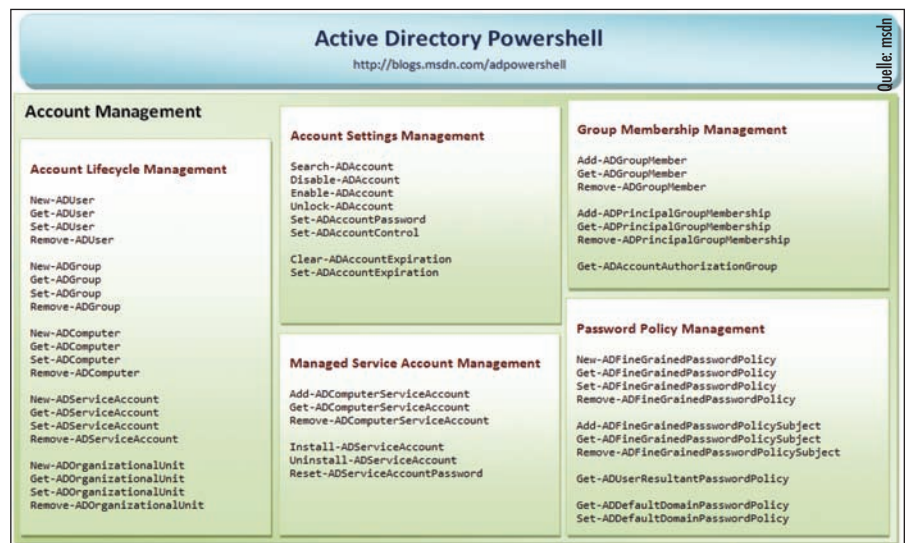


Bild 1: Dies sind nur einige der Active Directory-Cmdlets der PowerShell

Directory Services" (AD LDS) auswählen. Anschließend aktivieren Sie in den Features die "Remote Server Administration Tools" (RSAT) mit allen Teilloptionen. Natürlich kann auch bereits zur Installation die PowerShell zum Einsatz kommen. Dazu laden Sie zuerst das Modul zur Serververwaltung mit dem Befehl

```
import-module servermanager
```

Danach installieren Sie die neuen Cmdlets mit

```
Add-WindowsFeature -Name "RSAT-AD-Powershell" -IncludeAllSubFeature
```

Das Cmdlet "Add-WindowsFeature" stammt aus dem Modul ServerManager. Zusätzlich wird ein installiertes .NET Framework 3.5 SP1 benötigt.

Nutzung des Active Directory-Moduls

Um jetzt endgültig die neuen Cmdlets nutzen zu können, laden Sie das Modul mit dem Befehl

```
import-module ActiveDirectory
```

Während des Ladevorgangs sehen Sie einen Windows-Dialog mit einem Fortschrittsbalken. Bleibt dieser bei 50 Prozent stehen, stimmt die Namensauflösung nicht. In diesem Fall müssen Sie zunächst die korrekte Auflösung sicherstellen.

Nachdem das Modul erfolgreich geladen wurde, wird das Laufwerk "AD" als Standardlaufwerk verbunden. Andernfalls wird Ihnen dieser Text angezeigt: "WARNING: Fehler beim Initialisieren des Standardlaufwerks: 'Es wurde kein Standardserver gefunden, auf dem die Active

Worüber Administratoren morgen reden

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

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

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

Jetzt einfach und kostenlos
bestellen unter:



www.it-administrator.de/newsletter

Directory-Webdienste ausgeführt werden.“ Hierfür kann es mehrere Gründe geben. Entweder ist der neue Dienst “Active Directory Web Services” (ADWS) auf dem Zielsystem nicht gestartet oder ist dort nicht installiert.

Alternativ kann auch der Port (TCP 9389) zum Service geblockt sein. Die Cmdlets und der Provider wurden aber trotzdem erfolgreich geladen. Wenn die Verbindungsprobleme gelöst sind, können Sie das Laufwerk manuell verbinden:

```
New-PSDrive -PSProvider ActiveDirectory -Name AD -Root "" -Server "server.domain.tld"
```

Gegebenenfalls müssen Sie den Befehl noch um den Schalter “-Credential (get-credential)” ergänzen, um das Laufwerk mit einem administrativen Konto zu verbinden.

Arbeiten auf dem Active Directory

Um sich anzeigen zu lassen, welche neuen Cmdlets Ihnen jetzt zur Verfügung stehen, geben Sie das Kommando

```
(Get-Module ActiveDirectory).  
ExportedCommands | format-table  
-AutoSize
```

ein. Nachdem Ihnen nun die neuen Cmdlets zur Verfügung stehen, können Sie, wie Sie es eventuell bereits mit den Quest Active Directory-Cmdlets getan haben, Objekte über die PowerShell im Active Directory anlegen, verwalten oder löschen. So legt etwa dieser Befehl ein neues Benutzerkonto an:

```
New-ADUser -Name "Benutzer"  
-SamAccountName "Benutzer"  
-GivenName "Ben" -Surname "utzer"  
-DisplayName "Ben Utzer" -Path  
'ou=Management,DC=domain,DC=tld'  
-OtherAttributes @{msDS-PhoneticDisplayName="utzerBen"}
```

Oder Sie legen mit folgendem Befehl eine neue Gruppe an:

```
New-ADGroup -Name "DemoGruppe"  
-SamAccountName demoGruppe  
-GroupCategory Security  
-GroupScope Global  
-DisplayName "DemoGruppe" -Path  
'ou=Management,DC=domain,DC=tld'  
-Description "Beispielgruppe"
```

Besonders einfach wird das Hinzufügen von Benutzern zu Gruppen mittels des Cmdlets Add-ADGroupMember. Der Befehl lautet

```
Add-ADGroupMember DemoGruppe  
Benutzer
```

Während die bisher genannten Cmdlets für die Kontenverwaltung genutzt werden, gibt es noch weitere Cmdlets, die für die Topologie-Verwaltung oder das Management aller weiteren Active Directory Objekte eingesetzt werden können.

Fazit

In der Version 1 der PowerShell war die Schnittstelle zum Active Directory nur rudimentär implementiert. Das neue Modul ActiveDirectory, das Ihnen mit Version 2 zur Verfügung steht, hat diese Lücke effektiv geschlossen.

Damit steht auch Unternehmen, die keine Freeware einsetzen können, die volle Stärke der PowerShell in der Zusammenarbeit mit dem Active Directory direkt aus Redmond zur Verfügung. (dr) 

Rolf Masuch ist Product Manager bei ABSC GmbH sowie MCSE 2003 und Messaging Spezialist, MCT seit 1996, MCTS Windows 7 und Gründer der deutschsprachigen PowerShell-Anwendergruppe D/A/CH.

[1] PowerShell Anwendergruppe
Deutschland/Schweiz/Österreich
www.powershell-ag.de/ps/

Links



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



Tipps & Tricks ohne Gewähr



Über den Taskmanager **Prozesse zu beenden**, geht in der Regel ja recht flott. Manche Prozesse lassen sich jedoch nicht so einfach stoppen, außerdem fände ich es sehr praktisch, **mehrere Vorgänge auf einmal** zu beenden. Geht dies nur mit entsprechenden Tools oder helfen mir dabei auch Bordmittel?

Über die grafische Benutzeroberfläche von Windows steht Ihnen abgesehen von Zusatztools nur der Taskmanager zur Verfügung, der in seinen Funktionen recht eingeschränkt ist. Deutlich mehr Macht verleiht Ihnen der Befehl *taskkill*, den Sie über die Eingabeaufforderung ausführen. Zunächst einmal sollten Sie sich mit dem Kommando *tasklist* die laufenden Prozesse anzeigen lassen. Nun können Sie anhand der Prozess-ID mehrere laufende Tasks löschen. Der Befehl hierfür lautet

```
taskkill /pid {ID des Prozesses}
/pid {ID des Prozesses}
```

Besonders renitenten Prozessen wie dem Windows Explorer versetzen Sie mit dem Zusatzschalter "/f" ein Ende. Dann erzwingt das System einen Abbruch des Tasks. Der Befehl hierfür lautet *taskkill /f explorer.exe*. Besonders interessant bei der Verwendung des Kommandos ist die

Möglichkeit, von der eigenen Konsole aus über das Attribut "/s" auch auf anderen Rechnern im Netzwerk Prozesse zu beenden und dabei über den Schalter "/f" auf zahlreiche Filter zurückzugreifen. Das Kommando

```
taskkill /s 192.168.45.33 /fi
"imagetitle eq Internet"
```

etwa beendet alle Prozesse auf dem Rechner mit der angegebenen IP, die mit den Namen "Internet" beginnen. "*" lässt sich bei der Verwendung von Filtern stets als Wildcard verwenden. Über *taskkill /?* rufen Sie eine genaue Beschreibung des Befehls auf. (In)

Sind mehrere Nutzer auf einem Windows-Rechner angemeldet, muss ich den Wechsel von einem auf den anderen User immer über das Startmenü und die Abmelden-Option auslösen. Gibt es hier nicht eine Möglichkeit, den aktuellen Anwender schneller abzumelden, um zur Anmeldemaske für einen neuen Nutzer zu kommen?

Wenn Sie das Abmelden eines Nutzers beschleunigen wollen, können Sie dies auch über ein Symbol auf dem Desktop tun, der auf den Befehl *tsdiscon.exe* zugreift. Legen Sie dazu mit der rechten Maustaste eine neue Verknüpfung mit dem Pfad "c:\windows\system32\tsdiscon.exe" an und geben Sie der Verknüpfung einen beliebigen Namen. In Zukunft können Sie mit einem Dop-

pelklick auf das neu erstellte Symbol den aktuellen User abmelden und rufen direkt das Anmeldefenster für einen neuen Nutzer auf. Beachten Sie, dass die beendete User-Session aufrechterhalten wird, so dass der Anwender nach einem erneuten Wechsel wieder vollen Zugriff auf alle von ihm gestarteten Programme hat. (In)

Wie so viele Admins schätze ich die Tools aus der Sysinternals-Schmiede sehr. Nicht immer habe ich jedoch meinen USB-Stick mit den wichtigsten Werkzeugen dabei, und das Zusammenstellen und Herunterladen der einzelnen Programme beansprucht dann doch eine gewisse Zeit. Kann ich die Tools nicht auch irgendwie direkt über das Internet starten?

Wie Sie richtig vermuten, besteht eine Möglichkeit, die Werkzeuge von Sysinternals direkt über eine Internetverbindung zu starten. Die Adresse des Servers lautet "live.sysinternals.com". Noch schneller als über den Browser – sofern Ihnen der Name des von Ihnen gewünschten Tools bekannt ist – rufen Sie die einzelnen Werkzeuge aus dem Command Prompt auf. Der Befehl

```
\\live.sysinternals.com\tools
\autoruns.exe
```

etwa startet direkt auf Ihrem Desktop ohne Rückfrage das Tool "Autoruns", das alle automatisch gestarteten Anwendungen und Prozesse auflistet. (In)



Linux

Auch wenn sich Linux mit deutlich **geringeren Systemanforderungen** begnügt als andere Betriebssysteme, bin ich gerade auf meinem Netbook stets darum bemüht, den **Ressourcenanspruch des OS weiter nach unten zu schrauben**. Doch besonders was die Auslastung des Arbeitsspeichers betrifft, besteht noch Optimierungsbedarf. Haben Sie ein paar Tipps für mich, wie ich die Ansprüche meines Rechners ans RAM noch weiter nach unten schrauben kann?

Neben allgemeinen Tipps wie der Wahl eines bescheidenen KDE und der Verwendung von Ressourcen-schonenden Anwendungen sollten Sie Ihr Augenmerk auf etwaige nicht benötigte, aber eventuell trotzdem automatisch gestartete Dienste richten. *cupsd*, den "Common Unix Printing System Daemon" etwa benötigen Sie nur, wenn am PC auch Drucker angeschlossen sind. Noch spezieller ist der Dienst *hplip*, was für "Hewlett Packard Linux Imaging and Printing" steht. Dieser Druckerdienst ist nur von Nutzen, wenn Sie mit dem Rechner Drucker oder Scanner von HP betreiben wollen. Stellen Sie keine Verbindungen über Bluetooth her, können Sie auf den entsprechenden Dienst *kblduetoothd* leicht verzichten. Wer die Lautstärke der Audiowiedergabe über externe Lautsprecher regelt, hat zudem keinen Bedarf am Audio-Dienst *KMix*. Allein durch das Abschalten der hier genannten Dienste lassen sich bereits über 10 MByte im Arbeitsspeicher einsparen. Wenn Sie die automatisch gestarteten Services einmal genauer durchforsten und Ihrem tatsächlichen Bedarf anpassen, ergeben sich wahrscheinlich noch weitere Möglichkeiten zur Reduzierung der Speicherlast. (In)

Mit viel Mühe habe ich eine **Gentoo-Installation** erfolgreich zum Abschluss gebracht. Das einzige Peripheriegerät, das ich nicht in Betrieb nehmen kann, ist ein **über USB angeschlossener Kartenleser**.

Da andere USB-Geräte einwandfrei funktionieren, bin ich ziemlich ratlos. Haben Sie eine Idee, wie ich meinen Gentoo-Rechner dazu bewegen kann, den Kartenleser zu erkennen?

Zunächst sollten Sie überprüfen, ob im Kernel unter "Device Drivers" die Optionen "SCSI Device Support" sowie "SCSI-Disk Support" als Modul ausgewählt sind. Da manche Multiformat-Kartenleser als ein SCSI-Gerät mit verschiedenen LUNs angesprochen werden, ist es zudem ratsam, die Option "Probe all LUNs on each SCSI-Device" abzuhaken. Mit diesen Einstellungen sollte Ihr Rechner den Kartenleser eigentlich erkennen. (In)



Mozilla / Firefox

Das **Durchsuchen von Webseiten mit "STRG+F"** ist ja wirklich sehr praktisch. Was mich dabei jedoch ziemlich nervt, ist das lästige Gefiepse des Rechners bei jedem Tastendruck, wenn Firefox das entsprechende Suchwort nicht auf der Internetseite findet. Kann ich den **penetranten Warnton** auch irgendwie abschalten?

Den Hinweiston auf ein nicht vorhandenes Suchwort deaktivieren Sie über die erweiterten Einstellungen des Browsers. Geben Sie dazu in der Adressleiste *about:config* ein und suchen Sie den Eintrag "accessibility.typeaheadfind.enable-sound" und setzen Sie diesen Wert mit einem Doppelklick von "true" auf "false". Wenn Sie lieber einen eigenen Sound statt des Standard-Tutens verwenden wollen, ist der Eintrag "accessibility.typeaheadfind.soundURL" der Ort, an dem Sie Änderungen vornehmen müssen: Tragen Sie hier statt des Wertes "beep" den kompletten Pfad zu einer WAV-Datei Ihrer Wahl ein. Ab sofort werden Sie bei einer erfolglosen Suche immer Ihren Wunsch-Sound hören. (In)

Was ich bei Firefox sehr schätze, ist die Möglichkeit, bei einem Absturz des Browsers die zu diesem Zeitpunkt geöffneten **Webseiten wiederherzustellen**. Gera-

de aber, wenn ich schnell zwischen verschiedenen Links hin- und herspringe, stellt Firefox beim Neustart veraltete Tabs wieder her. Kann ich dem Browser irgendwie beibringen, meine **Surfbewegungen noch häufiger abzuspeichern**?

Auch für dieses Problem findet sich eine Lösung in den erweiterten Einstellungen des Browsers. Standardmäßig merkt sich Firefox alle 10 Sekunden, auf welcher Seite Sie sich genau befinden und greift auf diesen Speicherpunkt zurück, wenn er Tabs nach einem Absturz des Programms wiederherstellen soll. Gerade bei schnellen Klick-Befehlen in einem Menü kann das dann aber schon mal der veraltete Stand sein. Navigieren Sie also in den erweiterten Einstellungen zum Eintrag "browser.sessionstore.interval" und verändern Sie dessen Wert von den voreingestellten 10.000 Millisekunden auf eine kürzere Zeitspanne. Dann fertigt der Browser öfter Speicherpunkte an und Sie haben gute Chancen, bei jedem Wiederherstellungs-Vorgang auch wirklich wieder auf der letzten von Ihnen angesurften Seite zu landen. (In)



Tools

Wir nutzen im Unternehmen **ADM- beziehungsweise**

ADMX-Dateien zur Bestimmung der Gruppenrichtlinien. Veränderungen in diesen Vorlagen müssen wir jedoch ganz genau dokumentieren. Haben wir hier irgendeine Chance, wie wir die entsprechenden **Einstellungen aus dem Template ohne große Umwege auslesen können**?

Eine Möglichkeit zum Auslesen der im Template bestimmten Einstellungen wä-

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

www.administrator.de



re, sie in den Gruppenrichtlinien-Editor zu importieren. Dies ist jedoch nur in einer Testumgebung ratsam, da Sie ansonsten ja die Umgebung nachhaltig verändern würden. Eine andere Möglichkeit besteht darin, die einzelnen Zeilen im Texteditor herauszukopieren. Dieses Vorgehen kann je nach Größe der Templates zuweilen jedoch sehr mühsam sein. So hat etwa *system.adm*, das mit Windows ausgeliefert wird, 13.500 Zeilen, die Sie per "copy and paste" in eine Dokumentation überführen müssten. Ein weiteres Problem: Die Policy-Definitionen enthalten nur Verweise auf Beschreibungstexte, welche im Abschnitt "[strings]" zusammengefasst sind. Diese Verweise müssen irgendwie aufgelöst werden, was von Hand äußerst mühsam ist. Hilfreich wäre es jetzt, wenn sich auf Knopfdruck die Einstellungen der Templates in eine lesbare Form überführen ließen. Dafür gibt es das Freeware Tool "adm2html".

Adm2html ist ein Kommandozeilentool, das ein ADM- oder ADMX-Template in ein HTML-Dokument wandelt. Das Design des Outputs können Sie über ein CSS-Stylesheet beeinflussen. Es gibt vier verschiedene Ausgabeformate, mit denen Sie die darzustellenden Daten je nach Wunsch strukturieren können. (ln)



Weitere Infos und eine Downloadmöglichkeit finden Sie unter: <http://blogs.sepago.de/tools/2009/02/10/adm2html/>

Dokumentation ist und bleibt eines der unbeliebtesten Themen von Netzwerk- und Systemadministratoren, besonders für so komplexe und dynamische Strukturen wie das **Active Directory**. Denn selbst wenn der Administrator hierzu eine **Dokumentation** pflegt, sind Änderungen oft so kurzfristig, dass der komplette und tagesaktuelle Überblick fehlt.

Hier hilft ein Tool unseres Autors Nils Kaczinski weiter, der mit **José** ein HTML- und skriptbasiertes Tool zur Dokumentation der Objekte des Active

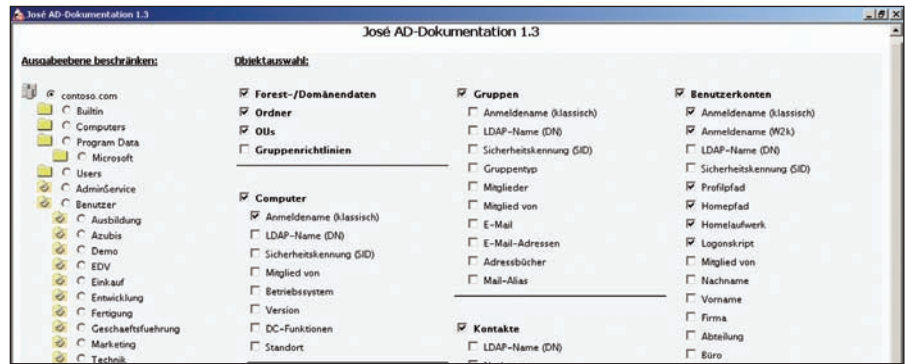


Bild 1: José bietet eine Auswahl der zu dokumentierenden Objekte des AD an

Directory bereitstellt. Das Werkzeug (Coautor ist Nils Weinhold) liest das Active Directory aus und generiert eine HTML-Datei, die Informationen über OUs, Benutzer, Gruppen, Computer, Policies et cetera enthält. Darüber hinaus zeigt José die Security-IDs (SIDs) von AD-Objekten an. Außerdem liefert es technische Informationen zur Domäne und zum Forest. Kaczinski weist allerdings darauf hin, dass José für überschaubare Umgebungen konzipiert ist, da die Abfragen, die das Tool verwendet, in großen Umgebungen zu langen Wartezeiten sowie zu größerer Netzwerklast führen können. Zudem sollte der erzeugte Report nicht wesentlich mehr als 2.000 Objekte (Benutzer, Gruppen et cetera) umfassen, weil die Anzeige im Browser sonst problematisch werden kann. Administratoren, die sehr große Umgebungen verwalten, sollten die Reports daher immer auf eine bestimmte Ebene oder eine bestimmte Objektklasse eingrenzen. (jp)

Quelle: <http://www.kaczinski.de/2007/03/18/jose-die-neue-version-13-ist-da/>

Eine andere Form der Dokumentationsproblematik stellt sich bei der Frage, welche IP-Adressen Geräte wie PCs, Notebooks, Server oder Drucker im Netzwerk belegen. Gerade in kleineren Umgebungen stellt sich oft die Frage, welche **IP-Adresse** beispielsweise für den neuen Drucker noch frei ist oder ob noch genügend IP-Adressen vorhanden sind, wenn im Sommer zehn Studenten als Aushilfen anheuern.

Das kleine und schnelle Programm **Angrý IP-Scanner** scannt jeden beliebigen IP-Adressbereich nach Rechnern ab. Das Tool findet aktive Geräte im Netzwerk und zeigt diese übersichtlich mit den entsprechenden Parametern. Neben der IP-Adresse listet das Werkzeug in seinem Bericht den Rechnernamen, Arbeitsgruppennamen sowie Domäne, die MAC-Adresse und die TTL. Neben dem Scannen von IP-Adressbereichen erlaubt der Angry IP-Scanner, die Rechner nach offenen Ports zu scannen. Dazu gibt der Administrator eine Port-Range an, die gescannt werden soll. Für eine schnelle und strukturierte Analyse der gesammelten Daten stehen verschiedene Auswahl- und Anzeige-Optionen zur Verfügung. Die Ergebnisse des Tools lassen sich als CSV-, TXT-, XML- oder als IP-Port-LST-Datei abspeichern. (jp)

Quelle: <http://ipscan.sourceforge.net/w/Home>

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



Fibre Channel over Ethernet **Symbiose für optimale Speichereffizienz**

von Robert Hasenstab

Fibre Channel over Ethernet (FCoE) gerät im Storage-Bereich immer mehr in den Blickpunkt, ermöglicht es doch die schnelle Fibre Channel-Übertragungstechnik über herkömmliche Ethernet-Netzwerke. Der folgende Artikel skizziert die Vorteile der Technologie, beleuchtet den aktuellen Entwicklungsstand und stellt Vergleiche zu anderen Standards wie iSCSI an.

Ausgangspunkt für die Entwicklung von FCoE war der Bedarf an einer Technologie, die die Vorteile der Übertragungsstandards Ethernet und Fibre Channel verbindet. So fungiert Ethernet als Übertragungstechnik für die Protokolle Common Internet File System (CIFS), Network File System (NFS) sowie Internet Small Computer Systems Interface (iSCSI). Bei Ethernet handelt es sich um eine bewährte Technologie, die in den Unternehmen sehr stark verbreitet ist und seit ihrer Einführung kontinuierlich weiterentwickelt wird. Bei einer Bandbreite von 10 MBit/s bis maximal 10 GBit/s unterstützt die Technik zahlreiche physische Media-Typen und bietet eine Vielzahl von Tools für Management, Diagnose und Troubleshooting. Nicht zuletzt gibt es eine breite Basis an Experten, Herstellern und Integratoren.

Fibre Channel (FC) hingegen wird in Storage Area Networks (SANs) eingesetzt, die Server und Speicherressourcen verbinden. FC ermöglicht heute Datenraten von rund 10 GBit/s und damit eine sehr schnelle sowie effiziente Übertragung blockbasierter Daten mit geringer Fehlerquote. FC-SANs sind heute die vorherrschende Speicherinfrastruktur in größeren Unternehmen. Dabei ist das Fibre Channel Protocol (FCP) in der Lage, Datenblöcke nahezu verzö-

gerungsfrei zu übermitteln. FC-Netze benötigen jedoch spezielle Switches (Fabrics) und Host Bus Adapter (HBA). Diese Netzwerkkomponenten und ihre Abstimmung erfordern entsprechendes Know-how und sind in der Regel erheblich teurer als Ethernet-Switches.

Ließen sich auch SAN-Speichernetze auf dem Ethernet-Standard einrichten, wäre nur noch eine Art von Netz erforderlich, was sich natürlich auf die Kosten auswirken würde. Überdies ließen sich die genannten Vorteile von Ethernet somit für FC-Netzwerke nutzen. Die Antwort darauf ist FCoE, eine noch vergleichsweise junge Technologie. Dabei werden Fibre Channel-Frames in Ethernet-Frames eingekapselt, was den verlustfreien Transport von FC-Daten über Hochgeschwindigkeits-Ethernet-Infrastrukturen ermöglicht.

Knackpunkt verlustfreies Ethernet

Herkömmliche Ethernet-Technik hat jedoch einen Nachteil: Standardmäßig ist keine verlustfreie Übertragung möglich, Frames gehen leicht verloren und die Latenzzeit ist recht groß. Protokolle wie TCP/IP müssen durch Wiederholung oder Neuansforderung für eine sichere Übermittlung der Pakete sorgen. Durch die Eliminierung von Frame-Verlusten, ein ausgefeiltes Traffic-Management, die

Priorisierung von FC-Daten gegenüber Nicht-FC-Daten sowie die gleiche Frame-Latenz wie in reinen FC-Netzen ist eine verlustfreie Datenübertragung auch im Ethernet möglich. Um dies zu erreichen, ist es notwendig, den Ethernet-Standard zu erweitern. Der neue Standard Data Center Bridging (DCB), auch bekannt als Converged Enhanced Ethernet (CEE), ist bereits in IEEE (und IETF) definiert. Die Umsetzung ermöglicht eine vollständige Unified Fabric. Damit wird ein konvergentes Netzwerk möglich, in dem alle Applikationen über eine einzige physikalische Infrastruktur laufen. Dabei unterstützen DCB-fähige Produkte mittels Priority-based Flow Control (PFC) verlustfreie Ethernet-Fabrics. Die Technologie erlaubt es, den Datenverkehr auf Basis definierter Prioritäten zu regeln. So kann in Zeiten starker Netzlast Traffic mit untergeordneter Priorität ausgesetzt werden, während geschäftskritische und verzögerungsempfindliche Anwendungen wie Datenspeicherung bevorzugt durchs Netz laufen.

Aus zwei mach eins

Mit Einführung der Fibre Channel-Technologie haben sich in den Rechenzentren vieler Unternehmen separate Netzwerke eingebürgert: ein Netz für den Datentransport, das in der Regel auf Ethernet und dem TCP/IP-Protokoll basiert, sowie



ein Netz für die Datenspeicherung, das auf Fibre Channel oder iSCSI beruht. Durch die Implementierung von Fibre Channel-Frames auf Ethernet (FCoE) in Verbindung mit dem DCB/CEE-Standard lassen sich die beiden Netze in einem einzigen Netzwerkkern (fabric) zusammenführen. Dieser ist vergleichsweise einfach zu managen und bietet dennoch eine hohe Performance. Mit Ethernet als physikalischem Transportmedium erreicht FCoE eine Bandbreite von derzeit 10 GBit/s. Bereits in näherer Zukunft sollen 40 GBit/s und später sogar 100 GBit/s möglich sein.

Das einheitliche FCoE-Netz hat zahlreiche Vorteile: Es werden deutlich weniger Kabel benötigt. Statt vier Verbindungen wie bei redundanter Anbindung (zwei für Ethernet und zwei für Fibre Channel) verlassen den Server nur noch zwei FCoE-Kabel. Auch kommt FCoE mit weniger und günstigeren Netzwerkkomponenten aus: Anstatt teurer HBAs und FC-Switches lassen sich preisgünstigere Ethernet/DCB-Switches verwenden. Dies spart nicht nur Kosten bei der Investition in die Netzwerk-Hardware. Da ledig-

lich ein gemeinsames Netz betrieben wird, nehmen die Komplexität der Infrastruktur und damit der Aufwand für die Administration ab, was sich positiv auf die TCO auswirkt. Zudem sinken der Platzbedarf und der Energieverbrauch. Letzteres ist natürlich ganz im Sinne einer umweltfreundlichen und ressourcenschonenden IT, die im Rahmen der CO₂- und Klimadebatte stark an gesellschaftlicher Bedeutung gewinnt.

Vorhandene Infrastruktur weiter nutzen

Ein weiterer Vorteil von FCoE besteht darin, dass sich durch eine nahtlose Anbindung an bestehende Ethernet- und Storage-Netzwerke die bewährten Technologien weiter nutzen lassen. So ist beispielsweise das SAN-Management für FCoE und Fibre Channel vollständig kompatibel. Zudem kommt das Protokoll mit nur einem Leistungstyp aus. Aufgrund der geringeren Leistungsaufnahme ist eine bessere Kühlung im Rack möglich. Da sowohl Ethernet-Komponenten als auch Fibre Channel-Geräte weiterhin im Netzwerk nutzbar bleiben, ist der Investitionsschutz hoch.

Nicht zuletzt verhindert die 10GBit-Ethernettechnik ungewollte Beschränkungen der Geschwindigkeit und sichert auf diese Weise eine gleichbleibend hohe Performance.

FCoE ist besonders für Unternehmen geeignet, die bereits über entsprechende Infrastrukturen verfügen, also über ein Ethernet, ein SAN oder beides. Gerade für größere Unternehmen, die aufgrund heterogener, mitunter virtualisierter Server-Landschaften eine vernetzte, zentrale Speicherarchitektur benötigen, ist FCoE eine gute Lösung. Wie bei Fibre Channel-Frames üblich, erfolgt auch in FCoE-Netzen die Übertragung und Speicherung von Daten blockbasiert, also in kleinen Datenblöcken von 4 bis 128 KByte.

Dies ist für den Administrator – verglichen mit der Speicherung von File-Daten – mit einem höheren Betreuungsaufwand verbunden, da kein direkter Zugriff auf Datei-Inhalte besteht. Die Speicherung erfolgt nicht zusammenhängend, so dass zunächst keine Daten über Anfang und Ende der Dateien zugänglich sind und Inhalte und Strukturen sich nicht unmittelbar erschließen. Dank der schnellen und effizienten Übertragung von bis zu 10 Gbit/s lassen sich jedoch auch große Datenvolumina nahezu verzögerungsfrei mit geringer Fehlerquote übermitteln.

Die Umstellung auf FCoE ist aufgrund unterschiedlicher technischer Spezifikationen der beiden Netztypologien mit ein paar Fallstricken verbunden: So muss der Größenunterschied zwischen Ethernet- und Fibre Channel-Frames überwunden werden. Während die maximale Größe eines typischen Ethernet-Frames 1.518 Byte beträgt, liegt diese bei einem Fibre Channel-Frame bei etwa 2.112 Byte. Werden Fibre Channel-Frames in Ethernet eingekapselt, erfordert dies eine Segmentierung von Frames im abgehenden und eine Reassemblierung im eingehenden Datenstrom. Dies würde zusätzlichen Overhead verursa-

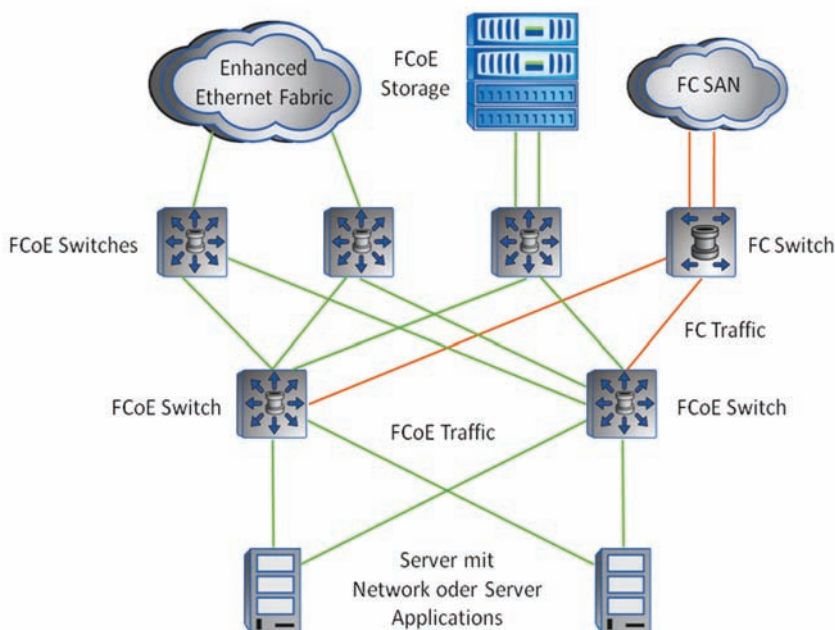
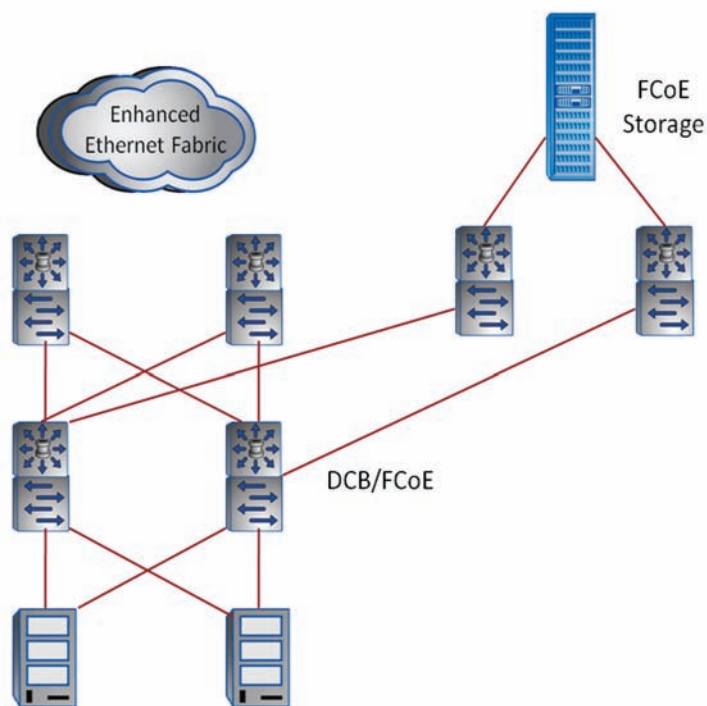


Bild 1: Ein FCoE-Netz kommt mit einer einfachen Verkabelung aus



Quelle: NetApp

Bild 2: Hersteller wie NetApp sehen eine Unified Fabric auf FCoE-Basis als Netzwerkarchitektur der Zukunft an

chen und damit das ursprüngliche Ziel einer optimierten End-to-End-Performance untergraben.

Um die Frame-Größen von Fibre Channel und Ethernet anzugleichen, wird also ein größerer Ethernet-Frame benötigt. Mit den so genannten Jumbo-Frames gibt es, wenn auch ohne offiziellen IEEE-Standard, doch zumindest einen De-facto-Standard, der Ethernet-Frames mit einer Größe von bis zu 9 KByte ermöglicht. Unterstützen alle Ethernet-Switches und Endgeräte das gemeinsame Jumbo-Frame-Format, lassen sich problemlos vier Fibre Channel-Frames in einen einzigen Ethernet-Frame einpacken – und das Problem des Größenunterschieds ist gelöst.

Es liegt nahe, dass die signifikanten Vorteile viele Storage-Verantwortliche in Unternehmen von einem FCoE-Einsatz überzeugen werden, hält sich doch der Investitionsaufwand durch die Nutzung vorhandener Netzwerkinfrastrukturen in Grenzen. So rechnen Experten noch im

Laufe des Jahres 2009 mit einer deutlichen Zunahme der Technologie in den Rechenzentren. Daher bieten einige Storage-Hersteller bereits heute ein innovatives Portfolio an FCoE-kompatibler Technik an.

FCoE als Evolution von Unified Storage

NetApp etwa sieht in FCoE die logische Weiterführung seines ganzheitlichen Unified Storage-Ansatzes, nämlich neben Fibre Channel-, iSCSI- und NAS-Protokollen nun auch FCoE in seine Enterprise-Storage-Systeme zu integrieren. Kunden, die heute eine Fibre Channel SAN-Lösung nutzen, haben damit die Möglichkeit, einfach auf die neue Technologie zu migrieren.

Dabei war das Unternehmen aktiv an der Entwicklung und Vermarktung des FCoE-Standards beteiligt und ist so in der Lage, aktuelle Technologien in diesem Umfeld anbieten zu können. Dazu zählt neben innovativen Fibre Channel-SAN-Lösungen eine durchgehende Multiprotokollunterstützung für FCoE, FC,

iSCSI, CIFS und NFS innerhalb desselben Systems. Fraglich ist, wie sich FCoE zu anderen Standards wie etwa iSCSI verhält. Auch mit IP-SANs auf iSCSI-Basis ist eine Zusammenführung von Speicher- und Datennetz denkbar. Während sich für FCoE die Fibre Channel-Tools weiter nutzen lassen, ist dies bei iSCSI nicht möglich. Denn Gateways für die Verbindung beider Standards sind nach wie vor teuer. Die Flusssteuerung erfolgt ausschließlich über höhere TCP-Protokolle und wirkt sich bei schlechten Verbindungen auf Bandbreite und Performance aus. Daher halten iSCSI-Anwender meist das Kommunikations- und Speichernetz getrennt.

Auch wenn iSCSI nicht die ideale Architektur für konvergente Netze ist, wird sie keinesfalls von FCoE verdrängt. Experten sind sich einig, dass iSCSI weiterhin seinen Platz in der Riege innovativer Storage-Technologien hat. Für viele gilt das iSCSI-Protokoll als Schlüsseltechnologie, welche die schnelle Entwicklung des SAN-Marktes weiter vorantreiben wird. Der große Trumpf von iSCSI ist die Allgegenwärtigkeit der IP-Netzwerke. So lässt sich der Standard problemlos für den Datentransport über Local Area Networks (LANs), Wide Area Networks (WANs) sowie über das Internet verwenden und ermöglicht dabei eine vom Standort unabhängige Speicherung und Wiederherstellung der Daten.

Fazit

Aufgrund der vielen Vorteile wie Nutzbarkeit der vorhandenen Netzwerkinfrastruktur und dem damit verbundenen geringen Investitionsaufwand wird sich FCoE wohl mehr und mehr durchsetzen. Gerade für Unternehmen, die ihre Netze für Datentransport und Datenspeicherung mit vertretbaren Kosten konsolidieren und dabei von hoher Performance profitieren möchten, ist FCoE eine lohnende Alternative. (In)

Robert Hasenstab ist Product Marketing Manager bei NetApp Deutschland

Video-Training VMware vSphere 4



Hören statt lesen – Audiobücher liegen voll im Trend. Und was beim “Da Vinci Code” funktioniert, sollte doch auch bei vSphere klappen, dachte sich Dennis Zimmer, ausgewiesener Virtualisierungsexperte und vielfacher Buchautor. Sein Video-Training zu vSphere 4, der neuesten Virtualisierungsplattform von VMware, kommt auf DVD zum Leser beziehungsweise Hörer. Die Lektionen, insgesamt etwa zehn Stunden Video, sind in einer einfach zu bedienenden Software verpackt, die sich den Stand der letzten Lektion merkt und dort auf Wunsch weitermacht. Über das Inhaltsverzeichnis lassen sich Kapitel und einzelne Lektionen übersichtlich anfahren, innerhalb einer Ses-

sion zeigen kleine Dreiecke in der Abspielleiste, an welchen Zeitmarken welche Themen behandelt werden. Durchweg gute Noten also für die Umgebung.

Beim Material zu vSphere 4 fällt die Bewertung etwas zwiespältiger aus. Generell ist das Training für den informierten Einsteiger gedacht. Es führt durch die grundlegenden Konzepte, Installation und Konfiguration sowie einige Anwendungsszenarien wie die Live-Migration. Doch technische Inhalte sind nur zum Teil dafür geeignet, in Bild und Ton vermittelt zu werden. Richtig gut passt es bei allem, was einen typischen Workshop-Charakter hat. So sind alle Sektionen, in denen installiert, konfiguriert und an der laufenden Maschine demonstriert wird, im Video gut aufgehoben. Tempo und Erklärung passen zusammen, gut ist zu erkennen, wo und wie etwas gemacht wird. Screenshots in einem Buch können da nicht das Wasser reichen. So weit, so gut. Fakten und Konzepte hingegen machen in den Video-Sessions keine gute Figur

und das liegt nicht nur an der etwas wenig abwechslungsreichen Präsentation. Informationen prägen sich ohne den visuellen Aspekt weniger gut ein, die Auflistung nur zu hören genügt oft nicht. Hier hätten wir uns entweder umfangreicheres Begleitmaterial oder eine visuell aufwendigere Bildschirmpräsentation gewünscht. Der Fairness halber muss allerdings gesagt werden, dass der Praxisanteil insgesamt deutlich überwiegt.

Fazit: Zuhören oder lesen ist letztendlich Geschmackssache. Die Praxisanleitungen sind im Video sehr hilfreich umgesetzt. Um Lernstoff aufzunehmen, ist das Video-Training aber weniger gut geeignet. Inhaltlich deckt das Training ein solides Arbeitswissen zu vSphere 4 ab.

Elmar Török

Autor:	Dennis Zimmer
Verlag:	Galileo Computing
Preis:	59,90 Euro
ISBN:	978-3-8362-1372-1
Bewertung:	★★★★★

Head First Networking



Head-First Networking klingt nicht nur nach Anfängerbuch, es ist auch eins. Es richtet sich weniger an den Vollprofi als zum Beispiel an den Praktikanten oder den frisch eingestellten Kollegen, der noch

wenig Ahnung von Cisco-Routern hat. Für solche Fälle ist das Buch aus O'Reillys Head First-Reihe perfekt – es erklärt die Grundlagen der Netzwerktechnik anhand extrem praktischer Beispiele mit einem extrem leicht zu verstehenden Konzept. Einzig Englischkenntnisse sind beim Durcharbeiten von “Head First Networking” gefragt. Getreu dem Head First-Konzept nutzt das Buch weniger Fließtext und dafür zahlreiche Tabellen und Bilder. Es ist deswegen

kein Bilderbuch und das technische Niveau steigt in jedem Kapitel nach den ersten Seiten massiv an. Vermutlich würde auch jeder alt gediente Admin darin noch Dinge finden, die er noch nicht wusste.

Sehr sympathisch: Die Autoren machen sich nebenbei über ein paar Klischees von Netzbüchern lustig. So wird die unvermeidbare OSI-Layer Tabelle schon im Vorspann angekündigt. Allerdings geht es sofort in die Vollen, das erste Kapitel kümmert sich um Kabel und was mit ihnen schieflaufen kann. Der didaktische Aufbau sieht jedes Mal ein Problem vor, das vom Leser gelöst werden muss. Zeichnungen und Fotos dokumentieren die Situation, nach und nach werden die möglichen Problemstellen und deren Abhilfen beschrieben. Bei den Kabeln gibt es Tipps zur richtigen Verkabelung von Räumen und Gebäuden sowie klare Anleitungen. Nach diesem Muster geht es quer durch die Netzwerkwelt: Es gibt ein eigenes Kapitel zur Fehlersuche

auf physikalischer Ebene und ein Kapitel zur Protokollanalyse mit Wireshark. Dann folgen die Themen Router, Routing-Protokolle und das Domain Name System. Wireless Networking ist ebenso vertreten wie Netzwerksicherheit. Eine kleine Anleitung zur Installation von BIND unter Windows und Linux schließt das Buch ab. Übrigens: Die OSI-Layer Tabelle taucht im ganzen Buch nicht auf.

Fazit: Ein tolles Buch, um seine Netzwerkkennntnisse aufzufrischen und zu vertiefen. Die Lektüre macht aus einem Anfänger keinen Admin, vermittelt aber viele praktische Aspekte eines Netzwerks. Ein perfektes Einsteiger- und Lernbuch.

Elmar Török

Autoren:	Al Anderson, Ryan Benedetti
Verlag:	O'Reilly
Preis:	43,95 Euro
ISBN:	978-0-596-52155-4
Bewertung:	★★★★★

<http://blog.buerstinghaus.net>

Vom Admin für Admins

Blogs sind ein schöner Zeitvertreib, um die Meinung Anderer zu verschiedenen Themen zu lesen. Oft beschränken sich die Inhalte dabei allerdings auch nur auf ebendiese Meinungen und bieten ansonsten wenig Substantielles. Anders ist dies in "Bjoern's Blog" des IT-Administrators Björn Bürstinghaus. Er ist nach eigenen Angaben seit acht Jahren im IT-Umfeld tätig, zunächst als Consultant und später als waschechter Admin, unter anderem beim Mobilfunk-Discounter simyo. Seine Schwerpunkte liegen dabei auf Windows-Systemen sowie Exchange und SharePoint. Im Unterschied zu manch anderen Blogs im Netz verbreitet Bürstinghaus dabei nicht (nur) seine eigenen Ansichten, sondern gibt konkrete Anleitungen, postet interessante und neutral geschriebene IT-News sowie eigene Erfahrungsberichte.

Die Anleitungen, oder besser gesagt Workshops, können sich durchaus sehen lassen. Schritt für Schritt führt Bürstinghaus die Besucher durch die Installation von Programmen oder dem Einrichten von Diensten. Zahlreiche Screenshots bereichern die Artikel dabei und zeigen den Lesern auf, ob sie sich auf dem rich-

tigen Weg befinden. Einer der neuesten Beiträge befasst sich beispielsweise mit der Datensicherung unter Windows 7. Darin zeigt der Autor, welche Knöpfe die User im Sicherungsassistenten drücken müssen, um ihre Dateien auf dem brandneuen Betriebssystem in Sicherheit zu bringen. Die Anzahl der so verfassten Anleitungen ist zwar noch etwas ausbaufähig – 16 waren es zu Redaktionsschluss. Doch scheint Bürstinghaus bereits an drei weiteren zu arbeiten.

Daneben informiert der IT-Profi über die neuesten Produkte und Trends in der IT-Welt. Auch hierbei dreht sich alles um die Microsoft-Welt sowie Tools zur Absicherung oder Wartung von Windows-Rechnern. So erfahren die Besucher etwa von neu verfügbaren Windows-Versionen wie der 7 Enterprise oder dem Virtual Machine Manager 2008 R2. Erfahrene Leser merken dabei sofort, dass es sich hierbei um selbst überarbeitete Nachrichten handelt und nicht um simpel abgekupferte Pressemitteilungen mit allerlei Schönfärbereien. Schließlich dürfen die Besucher auch den ein oder anderen Erfahrungs- und Testbericht lesen. Ab diesem Herbst plant Bürstinghaus derweil, ergänzend zum Blog auch ein Forum rund um Windows zu starten. Darin können sich die Teilnehmer dann über das Betriebssystem im privaten sowie professionellen Umfeld sowie Virtualisierungsfragen austauschen. (dr)



Blogt zu aktuellen Windows-Themen: Der Administrator Björn Bürstinghaus



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

Anwenderbericht:

Wienerwald - Full Backup für halbe Hendl

Die österreichische Gastronomiekette Wienerwald ist bekannt für ihre Geflügelspezialitäten. Angesichts steigender Datenmengen entschieden sich die Verantwortlichen für eine neue, skalierbare Technologie statt einer möglichen Erweiterung des vorhandenen Systems. Wir zeigen Ihnen in unserem Anwenderbericht, wie Wienerwald durch die Umstellung von einer erhöhten Kapazität bei gleichzeitig besserer Performance profitieren konnte.

www.it-administrator.de/themen/storage/fachartikel/63592.html

Video-Workshop:

Systeme sicher administrieren (2)

Um Windows auf einer größeren Anzahl von Computern unterzubringen, lassen sich verschiedene Wege beschreiten. Wer nicht den Weg eines All-Inclusive-Image oder eines Unattended Setup gehen will, kann sich beim verschlüsselten Deployment-Konzept der Open Management Architecture (OMA) bedienen. Hierbei gibt es vier verschiedene Verfahren zur OS-Verteilung, die wir Ihnen anhand einer Installation von Server 2003 in unserem Video-Workshop demonstrieren.

www.it-administrator.de/themen/server_client/fachartikel/63593.html

Fitnessprogramm für den Systemadministrator

Für Systemadministratoren ist es essentiell, sich über neue IT-Produkte und Services zu informieren und bei aktuellen Technologien auf dem Laufenden zu sein. Wir beleuchten in unserem Online-Artikel ein von IBM entwickeltes Trainingskonzept, das aktuellen Technologien und Herausforderungen verständlich erklärt. Administratoren bleiben auf diese Weise fit und steigern ihren Stellenwert im Unternehmen.

www.it-administrator.de/themen/server_client/fachartikel/63594.html

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

»Jedes Problem erweitert den persönlichen Wissensstand«

Elmar Schott (27) ist bei der A.B.S. Global Factoring AG in Wiesbaden als Systemadministrator tätig. Der Dienstleister sichert seine Kunden gegen Forderungsausfälle ab und übernimmt das gesamte Debitorenmanagement mit Buchhaltung, regelmäßiger Bonitätsprüfung, Mahnwesen und Inkasso. Eine funktionierende IT ist für das Unternehmen essentiell.

Welche Ausbildung haben Sie gemacht?

Nach der Schule habe ich eine Ausbildung zum Informatikkaufmann gemacht und erfolgreich abgeschlossen.

Warum sind Sie IT-Administrator geworden?

Mich hat das Umfeld der Administration schon während meiner Ausbildung fasziniert. Bereits in dieser Zeit hatte ich häufig mit der Implementierung von Systemen zu tun und fand diesen Aufgabenbereich spannend und abwechslungsreich. Als System-Administrator betreue ich eine reine Microsoft-Umgebung. Dazu gehören zehn Windows 2003 Server sowie 28 Windows XP Professional Clients.

Welches Netzwerk- und Systemmanagement setzen Sie ein?

Wir verwenden die Windows-eigenen Werkzeuge. Das ist für unsere aktuelle Installation völlig ausreichend.

Wie sieht Ihr Storage-Konzept aus?

In unserer Speicherumgebung setzen wir DocuWare 5.1b SP2 in einem Fail-Over-Cluster-System mit einem gespiegelten Storage ein. Sollte ein Server oder eine Storage-Komponente ausfallen, übernehmen die redundanten Systeme die Arbeit.

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

Wir müssen gewährleisten, dass bei uns im Haus der Ausfall eines Arbeitsplatzes oder Servers so kurz wie möglich gehalten wird. Bei Problemen muss also sofort reagiert werden. Dies betrifft nicht nur die Hardware und die fertig gekaufte Software, sondern auch unsere Factoring-Anwendung, die von uns selbst programmiert wird, damit sie unseren Anforderungen entspricht.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Zurzeit ist dies vorrangig die Migration unseres Dokumentenmanagementsystems DocuWare 4.6a auf die Version 5.1b SP2. Dies bedeutet nicht nur die Umstellung der Archive, sondern auch die Anpassung unserer Software bezüglich DocuWare



Geburtsdag: 24.04.1982
Familienstand: verheiratet
Hobbys: Familie und Freunde

Elmar Schott, IT-Administrator

Toolkit 5. Zum Migrationsvorgang gehört auch die entsprechende Anpassung unserer Web-Anwendung mit DocuWare 5 Web Client.

Was macht Ihnen an Ihrem Job am meisten Spaß?

Mir gefällt das große Umfeld der Administration und die Tatsache, dass jeder Tag immer anders ist als der vorhergehende. Mit jedem Problem wächst für mich auch mein persönlicher Wissensstand.

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

Die Kontrolle von Microsoft-Updates gehört nicht unbedingt zu meinen Lieblingsaufgaben. Bei der Flut von Updates muss leider aufgrund unseres Systems immer vorher geprüft werden, was diese bewirken.

Was tun Sie für Ihre Fortbildung?

Ich lese in der Regel die Newsletter der eingesetzten Fremdsoftware sowie die Handbücher. Hinzu kommen die aktuellen Informationen der Hardware-Her-

steller, deren Produkte wir bei uns im Haus installiert haben.

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

Der Kauf eines Linux-Fileservers von Level One war unglücklich, da dieser nach der Installation von SP2 auf unserem Domain Controller nicht mehr ansprechbar war. Der Hersteller bietet leider keine Lösung an – damit haben wir einen klassischen Fehlkauf getätigt.

Was war Ihr größter Erfolg als IT-Administrator?

Auf die problemlose Umsetzung der Update- und Software-Verteilung bin ich stolz.

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

Ein Anwender hat vor einiger Zeit seine eigenen Dateien in einen anderen Ordner verschoben und danach behauptet, dass wir Administratoren ihm diese gelöscht hätten. Erst nachdem wir die Ursache herausgefunden hatten, war ihm klar, wodurch das Problem verursacht worden war beziehungsweise durch wen.

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

Die größte Herausforderung ist es, den Überblick über das mittlerweile komplex gewordene System zu behalten. Da unser Haus Bankstatus hat, müssen wir auch immer einen detaillierten Überblick über die Sicherheit behalten, gleichzeitig aber auch versuchen, den administrativen Aufwand dafür möglichst gering zu halten, ohne Abstriche an der Hochsicherheit zu machen. 

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 11/09 erscheint am 2. November 2009

Schwerpunktthema:

IT-Desaster-Management – Backup & Recovery

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

Unsere Ausgabe im **Dezember** steht unter dem Schwerpunkt **Mobiles Arbeiten, Home Office und Wireless**. In unserer Test-Rubrik haben wir uns die Unified Messaging-Suite David.fx einmal genauer angesehen. In einem weiteren Artikel erklären wir außerdem, welche Sicherheits-Aspekte Sie beim Thema VoIP beachten sollten.

Als Schwerpunkt im **Januar** folgt dann das Thema **Monitoring und Inventarisierung**.

Im Vergleichstest: Tools für das Online-Backup

Workshop: Microsoft Exchange Disaster Recovery

Workshop: Gemeinsame Benutzerverwaltung unter Windows und Linux

Systeme: Neuerungen in Windows Server 2008 R2

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

Redaktion

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

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

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

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

Autoren dieser Ausgabe

Petra Adamik, Andreas Badur, Thomas Bär,
Thomas Drilling, Dr. Jürgen Fechter, Marc Grote,
Robert Hasenstab, Jürgen Heyer, Thomas Hümmler,
Nils Koczanski, Christian Knermann, Sandra Lucifora,
Nico Lüdemann, Ralf Masuch, Elmar Török,
Dennis Zimmer

Anzeigen

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

Es gilt die Anzeigenpreisliste
Nr. 6 vom 01.01.2009

LAC/2008



Produktion / Anzeigendisposition

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

Druck

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

Vertrieb

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

Abo- und Leserservice:

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

Erscheinungsweise

monatlich

Bezugspreise

Einzelheftpreis: € 12,60
Jahresabonnement Inland: € 135,-
Studentenabonnement Inland: € 67,50
Jahresabonnement Ausland: € 150,-
Studentenabonnement Ausland: € 75,-

Jahresabonnement Inland mit Jahres-CD: € 144,84
Studentenabonnement Inland mit Jahres-CD: € 77,34
Jahresabonnement Ausland mit Jahres-CD: € 159,84
Studentenabonnement Ausland mit Jahres-CD: € 84,84
E-Paper-Einzelheftpreis: € 9,45
E-Paper-Jahresabonnement: € 99,-
E-Paper-Studentenabonnement: € 49,50
Jahresabonnement-Kombi mit E-Paper: € 168,-

(Studentenabonnements nur gegen Vorlage einer gültigen Immatrikulationsbescheinigung)

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

Internet

www.it-administrator.de

Verlag / Herausgeber

Heinemann Verlag GmbH
Leopoldstraße 85
80802 München

Tel.: 089/4445408-0
Fax: 089/4445408-99

(zugleich Anschrift aller Verantwortlichen)

Web: www.heinemann-verlag.de
E-Mail: info@heinemann-verlag.de

Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

Geschäftsführung / Anteilsverhältnisse

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

ISSN

1614-2888

Urheberrecht

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

Haftung

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

Manuskripteinsendungen

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

So erreichen Sie den Leserservice

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

Bankverbindung für Abonnenten

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

So erreichen Sie die Redaktion

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

So erreichen Sie die Anzeigenabteilung

Anzeigenverkauf IT-Administrator
Anne Kathrin Heinemann
Heinemann Verlag GmbH
Leopoldstr. 85
80802 München
Tel.: 089/4445408-20
Fax: 089/4445408-99
E-Mail: kathrin@it-administrator.de

1 und 1
ADN
centerTools
CIO
DatacenterDynamics

S. 09
S. 69
S. 84
S. 57
S. 49

Fujitsu
Galileo
GeNUA
IBM
iWatch

S. 25
S. 53
S. 15
S. 02, S. 28, S. 29
S. 04

LANCOM
Microsoft
Netgear
SNW Europe
xtivate

S. 17
S. 39
S. 21
S. 12
S. 31

INSERENTENVERZEICHNIS

Die Ausgabe enthält eine Teilbeilage von ppedv, eine Titelflappe von centerTools und zwischen Seite 42 und 43 einen Einhefter der Firma REALTECH (Schirmherr 2009 der IT-Administrator User Group ITANet)

Das IT-Administrator Komplettprogramm!!!

Sichern Sie sich jetzt das **IT-Administrator
Jahresabo All-Inclusive** mit allen Monats-
ausgaben, 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/](http://www.it-administrator.de/abonnements/aboupgrade/)

Oder Sie sind Neukunde? Hier können Sie bestellen:

[www.it-administrator.de/
abonnements/jahresabo/](http://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

» ECHTE Sicherheit für IHR komplettes Netzwerk und alle Daten

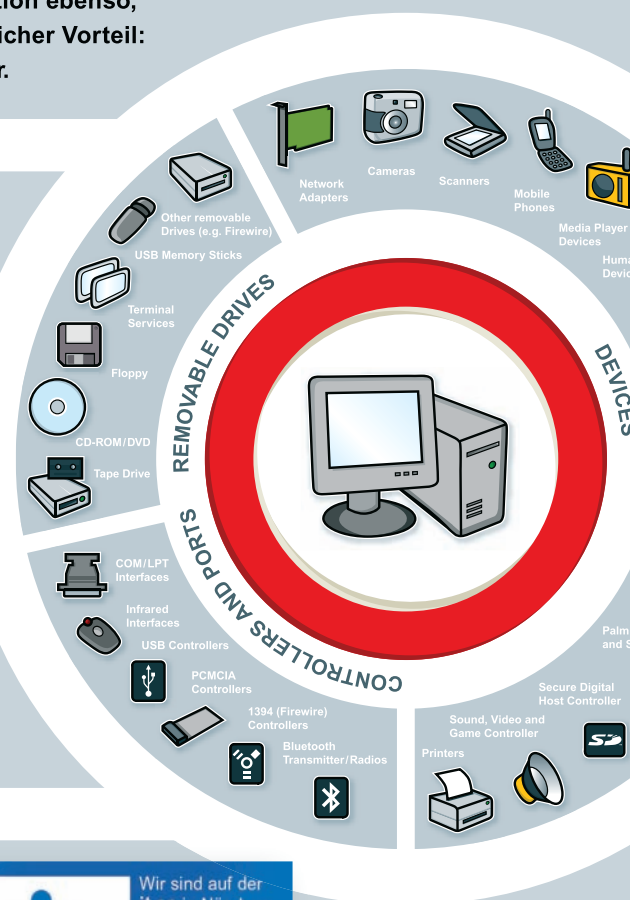
DriveLock bietet Verschlüsselung für alle Fälle: Full Disk Encryption ebenso, wie die Verschlüsselung für alle Windows Mobile Geräte. Zusätzlicher Vorteil: Im Falle eines Falles hilft Fast Recovery schnell und sicher weiter.

Im Application Launch Filter (ALF) wird festgelegt welche Programme und Applikationen auf welchem PC gestartet werden dürfen. Und welche nicht. Die Online-Datenbank kennt mehrere Millionen Anwendungen und wird beständig aktualisiert.

ALF schützt zusätzlich vor dem Öffnen ungewollter Programme und Applikationen und verhindert ggf. die Ausbreitung von Viren und anderen Schadprogrammen. So wird DriveLock zu einem Bestandteil Ihrer Anti-Viren-Strategie.

Mit der DriveLock Terminal-Server-Edition können auch Thin-Client-Netzwerke auf einfachste Art und Weise nachhaltig überwacht und professionell gesichert werden.

Wer auch unter Windows 7 alle Lücken geschlossen haben will, der hat mit DriveLock das richtige Werkzeug für heute und für die Zukunft.



DriveLock ist das optimale Werkzeug gegen absichtlichen oder zufälligen Datenklau in Unternehmen. Neben dem Sperren von Ports und Schnittstellen wie beispielsweise USB, Firewire oder Bluetooth, können mit DriveLock auch Daten auf externen Datenträgern wie USB-Sticks oder CD-ROMs verschlüsselt werden. Damit sind diese Daten auch im Falle eines Verlierens der Datenträger nicht lesbar.
Referenzen / Informationen / Testversion » WWW.DRIVELOCK.DE

