IT-ADMINISTRATOR.DE

01/2010

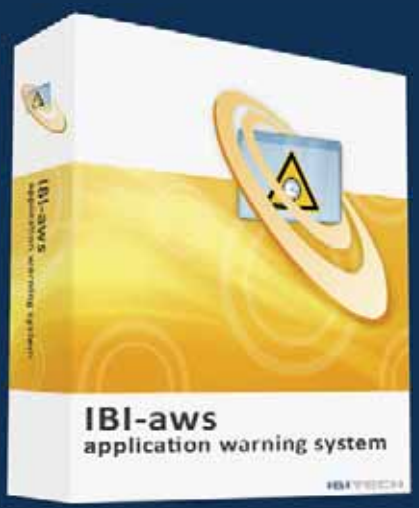
€ 12,60 ISSN 1614-2888

iadministrator

Das Magazin für professionelle System- und Netzwerkadministration

Monitoring und Inventarisierung

IBI-aws – die überlegene Informationslösung zwischen IT und Anwendern.



Informiert über Applikationsstörungen, IT-Probleme und Wartungsfenster.

- Zielgenaue Information
- Eingrenzung der Zielgruppe nach Applikation, IP-Bereich, AD-Gruppe
- Zeitliche Begrenzung der Meldung
- Verbindungslose Kommunikation
- Kein Setup benötigt
- Keine offenen Ports
- Keine Admin-Rechte notwendig
- Weniger Ressourcen, mehr Qualität
- Zufriedene Anwender und Supporter

mehr Info und Demo unter www.ibi-aws.de

EDITORIAL

Wechselgerüchte

Liebe Leser,

vieles spricht dafür, dass 2010 das Jahr von Windows 7 wird. Zweifellos ist die Wucht, mit der Microsofts Marketingmaschine das neue Betriebssystem in den Markt drückt, enorm, doch davon wird sich der IT-Verantwortliche sicherlich weniger beeinflussen lassen als der Endanwender. Beeindruckt sind beide dennoch: Dass Windows 7 in England sogar Harry Potters neuestes Abenteuer von der Spitze der Bestsellerliste verdrängen konnte, ist natürlich Wasser auf die Mühlen der Redmonder und zeigt, dass Windows 7 schnell die Wohnzimmer erobern wird. Doch auch die deutschen IT-Verantwortlichen zeigen sich einkaufsfreudig in Sachen Vista-Nachfolger, wie eine Umfrage der größten europäischen Windows User Group – der NT AG aus Böblingen – zeigte: 42 Prozent der insgesamt 375 befragten Unternehmen gaben an, innerhalb von sechs Monaten migrieren zu wollen, weitere 32 Prozent planen ebenfalls mit Windows 7, ohne jedoch einen konkreten Zeitrahmen anzugeben.

Ein Grund für die schnelle Wechselbereitschaft ist dabei – neben den durch das Auslassen von Vista entstandenen Betriebssystem-Altlasten auf den Clients – die Tatsache, dass eine Migration heute bei Weitem nicht mehr die Herausforderung darstellt wie noch vor einigen Jahren. Dies zeigt unser Vergleichstest von vier Client-Management-Suiten ab Seite 16 mehr als deutlich. Erstmals haben wir dabei im Rahmen eines Vergleichstest eben dieses Migrationsszenario als zentrale Anforderung an die Produkte definiert und entsprechend untersucht.

So startet das neue Jahr im IT-Administrator mit einem spannenden Vergleichstest rund um "Monitoring und Inventarisierung". Wir müssen allerdings zugeben: mit etwas mehr "Monitoring" wäre uns ein recht unangenehmes Ereignis aus der Dezember-Ausgabe erspart geblieben. Dort testeten wir den Scaleo Home Server 2205 und kamen zu einem guten Ergebnis. Nur kurz nach dem Erscheinen des Hefts wies uns jedoch ein Leser darauf hin, dass der Server beim Anbieter nicht mehr zu haben sei. Warum das erst sechs Monate zuvor erschienene Gerät nur noch auf der Restrampe verschleudert wird, dazu äußerte sich der Hersteller uns gegenüber bisher nicht. Wir können uns nur bei Ihnen, liebe Leser, entschuldigen und unser Produktmonitoring dieses Jahr noch weiter intensivieren.

Ein frohes neues Jahr und viel Vergnügen beim Lesen, Ihr

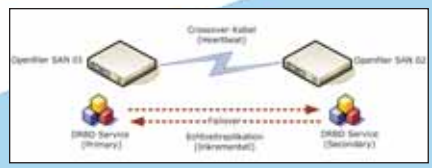
John Pardey
Chefredakteur IT-Administrator

INHALT

IT-Administrator – Ausgabe Januar 2010

Monitoring und Inventarisierung

SAN-Hochverfügbarkeit mit Openfiler und DRBD-Cluster (1)



Einen Hochverfügbarkeits-Cluster unter Linux zu realisieren, ist inzwischen kein Hexenwerk mehr. Der Einstieg in die Oberklasse der Verfügbarkeit lässt sich mit einfachen Mitteln umsetzen. Dank der Open Source-Projekte Openfiler, DRBD und Heartbeat lassen sich Hochverfügbarkeits-Storage-Infrastrukturen kostengünstig verwirklichen. In diesem Workshop führen wir Sie Schritt für Schritt zu einem hochverfügbaren SAN.

Seite 32

Exchange Server 2007 SP2

Mit SP2 für Exchange Server 2007 erweitert Microsoft die aktuelle Version von Exchange um neue Funktionen und macht die Serverlösung bereit für Exchange Server 2010. Da diese Version bald in den Startlöchern stehen wird, sorgt das Service Pack 2 für Exchange 2007 für die notwendige Kompatibilität mit dem Nachfolger. Wir zeigen Ihnen, welche Neuerungen Microsoft integriert hat und auf was Sie achten müssen, wenn Sie das Service Pack auch in komplexeren Umgebungen, zum Beispiel auf dem Essential Business Server 2008 oder mit installiertem Forefront Security für Exchange, integrieren wollen.

Seite 51

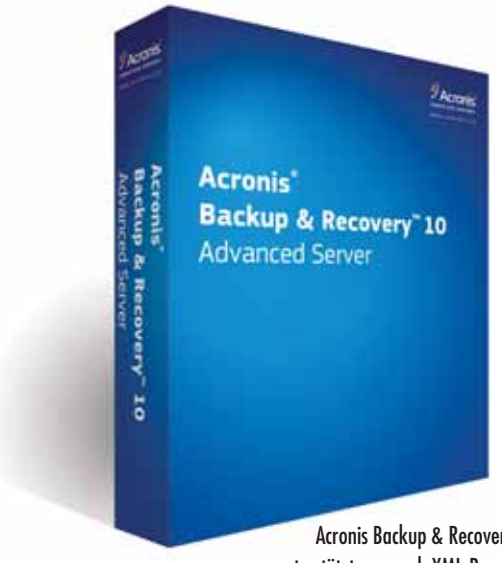
Themenübersicht

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

Virtuelle Maschinen als Backup

Acronis integriert mit dem **Update 1** die Funktion **Instant Restore** in die Software **Acronis Backup & Recovery 10**. Instant Restore soll die Wiederanlaufzeiten von IT-Systemen durch das Vorhalten einer einsatzbereiten virtuellen Maschine verringern. Fällt das Produktivsystem aus, kann die Arbeit ohne signifikante Unterbrechung in der virtuellen Maschine fortgeführt werden, solange Reparaturen oder ein Austausch von Hardware stattfinden. Das Feature unterstützt VMware ESX/ESXi, vCenter Server und Microsoft Hyper-V Umgebungen. IT-Verantwortliche haben dabei die Möglichkeit, sich beispielsweise eine Liste von virtuellen Maschinen des VMware vCenter auf dem Acronis Management-Server anzeigen zu lassen oder durch die Verwendung von Acronis in vCenter bereits vorhandene virtuelle Maschinen automatisch zu registrieren. Neben der Instant Restore-Funktion finden Nutzer in dem Update zu Acronis Backup & Recovery 10 ein zentralisiertes Reporting zur Analyse von Backup-Ergebnissen. Mit XML-basierten Reporting-Funktionen und einer Zusammenstellung vordefinierter Berichte lassen sich der gegenwärtige Systemzustand analysieren und Trends erkennen. Ab 56 Euro ist die Backup- und Recovery-Software in der Workstation-Variante erhältlich. Die Advanced Server-Edition liegt bei einem empfohlenen Herstellerpreis von 899 Euro. *(dr)*

Acronis: www.acronis.de/backup-recovery/u1/



Acronis Backup & Recovery 10 unterstützt nun auch XML-Reporting

Funker für hohen Datendurchsatz

Netgear bietet den **WLAN-Access Point WNDAP350** aus der **ProSafe 802.11n Dualband-Reihe** an. Das Gerät unterstützt simultan Geräte, die im 5 GHz-Frequenzband (802.11a und 802.11n) funken, als auch Geräte mit 2,4 GHz-Technologie (802.11b/g und 802.11n). Der über SNMP administrierbare Access Point unterstützt Power-over-Ethernet (PoE). Mit Point-to-Point- und Point-to-Multipoint-Bridging über Wireless Distribution System (WDS) eignet er sich zudem für den Einsatz über große Distanzen. Der WNDAP350 ist ausgestattet mit einem 10/100/1000 GBit Ethernet-Port mit Auto Uplink, einem Konsolen-Port für die lokale Konfiguration und Überwachung sowie internen Antennen mit 6 dBi. Für die Sicherheit drahtloser Netzwerke unterstützt der Access Point WPA, WPA2, Rogue AP Detection, 802.1x mit RADIUS-Authentifizierung, Wireless Access Control, Authentifizierung über MAC-Adressen, Unterstützung von VPN Pass-Through, Secure SSH Telnet und Secure Sockets Layer (SSL) Remote Management Login. Über das Browser-basierte ProSafe Control Center lässt sich das Gerät verwalten. Alternativ steht mit SNMP MIB I, MIB II und 802.11 MIB auch eine Netzwerkmanagement-Software zur Verfügung. Daneben werden sämtliche gängigen 802.1x Port-basierten Authentifizierungsprotokolle wie Extensible Authentication Protocol (EAP), Transport Layer Security (TLS), Protected EAP (PEAP) und Tunneled TLS (TTLS) unterstützt. Der neue ProSafe 802.11n Dualband Wireless Access Point ist ab sofort für 308 Euro verfügbar. *(dr)*

Netgear: www.netgear.de

Bietet zahlreiche Sicherheitsfeatures: Der Wireless N-Access Point WNDAP350 von Netgear

Management und Sicherheit im Bundle

Avocent stellt seine Managementplattform mit den neuen Versionen der LANDesk Management Suite 9 und der LANDesk Security Suite 9 vor. Die **Management Suite 9** ist eine Software-Asset-Management-Lösung, die eine verbesserte Auffindung und Kontrolle für Softwarelizenzen ermöglichen und Informationen zur Verfügung stellen soll. Mit der neuen Version, welche die Migration zu neuen Betriebssystemen wie Windows 7 unterstützt, können IT-Verantwortliche Hardware-unabhängige Imaging Best Practices implementieren, um in einer gemischten Hardware-Plattform effizientes Provisioning zu erreichen. Benutzerprofile und Einstellungen lassen sich ebenfalls migrieren und mit einem neuen Universal-Migration-Assistenten verwalten. Das mehrstufige Sicherheitskonzept in der Security Suite 9 soll es daneben ermöglichen, Fehler aufzufinden und für Mängelbeseitigung an lokalen wie auch entfernten Standorten mit angepassten Standort-spezifischen Sicherheitsrichtlinien zu sorgen. Die beiden Suiten bieten ein detailliertes Reporting für zentralisierte und dezentralisierte IT-Umgebungen, so dass Unternehmen ihre IT-Assets proaktiv kontrollieren können. Ab sofort ist das neue LANDesk-Management 9 für 92 US-Dollar pro Rechner erhältlich. *(dr)*

LANDesk: www.landesk.com/nine/

Switch mit Citrix-Software an Bord

Arista Networks stellt den **GBit-Ethernet-Switch Arista 7048** vor, der für die **Verteil-Ebene** (Leaf) des Netzwerks konzipiert ist. Der Hersteller hat die klassische Netzwerkhierarchie auf zwei Ebenen reduziert: So gibt es für ihn nur noch die Kern-Ebene (Spine) und Verteil-Ebene (Leaf). Der neue Arista 7048 ist ein Multi-Layer-Switch in Kabelgeschwindigkeit, der über 48 RJ-45 GBit-Ethernet-Ports und vier 1/10 GBit-Ethernet-Uplinks verfügt. Das Gerät liefert damit bis zu 40 GBit/s Übertragungskapazität für die Verbindung mit dem Kernbereich (Spine) des Netzwerks. Auf dem Switch läuft das "Arista Extensible Operating System" (EOS). Es bietet offenen Zugang zu Linux-Tools und erweiterbaren Netzwerkservices. Zudem erlaubt es die einfache Integration von Anwendungen anderer Anbieter wie zum Beispiel Citrix NetScaler VPX. Das EOS unterstützt unternehmenskritische Rechenzentrumsfunktionen wie Stateful Fault Repair (Selbstheilung) und Software-Upgrades im laufenden Betrieb. Erstmals hat der Hersteller hier die NetScaler Load-Balancing- und Application Security Software von Citrix Systems integriert. Durch die Citrix NetScaler VPX-Integration ist das Load-Balancing über mehrere Server innerhalb eines Racks hinweg massiv vereinfacht. Ab sofort ist der Switch für 8.568 Euro bei SEiCOM erhältlich. *(dr)*

Arista Networks:
www.aristanetworks.com/en/7048_Switch

Schneller NAS-Würfel fürs Homeoffice

Buffalo Technology präsentiert mit der neuen **LinkStation Duo** ein **Zweiplatten-NAS für den SOHO-Bereich**. Das Gerät mit einer maximalen Speicherkapazität von 4 TByte verfügt laut Hersteller über einen Datendurchsatz von bis zu 40 MByte/s. Die beiden Festplatten arbeiten entweder im RAID-0-Modus für schnellere Datenzugriffe oder lassen sich im RAID-1-Modus als redundanter Speicher konfigurieren. Über den USB-Anschluss kann der Nutzer eine zusätzliche externe USB-Festplatte zur Erweiterung des Speicherplatzes oder als Laufwerk für Datensicherung unter Nutzung der mitgelieferten Software "Memeo Auto Backup" einbinden. Für eine einfache Integration in bestehende Netzwerke bietet die LinkStation Duo einen Active Directory-Client. Um Energie zu sparen, schaltet sich der Netzwerkspeicher automatisch mit dem Computer ein und aus. Darüber hinaus soll die DLNA-Zertifizierung für eine geregelte Kommunikation zwischen der LinkStation Duo und unterschiedlichen Media-Clients sorgen. Das NAS Gerät ist ab sofort zu einem Preis von rund 260 Euro erhältlich. *(ln)*

Buffalo Technology:
www.buffalo-technology.com

Trotz des Fokus auf den SOHO-Bereich verfügt die "LinkStation Duo" bereits über Active Directory-Unterstützung

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

O&O bietet die Datenrettungssoftware **UnErase** in Version 6 an. Das Tool läuft damit auch unter Windows 7. Versehentlich gelöschte Dateien lassen sich zudem nun direkt von Digital-Kameras, Speicherkarten und USB-Sticks wiederherstellen, sofern diese unter Windows als Laufwerk unterstützt werden, abgesehen von exfat-Dateisystemen. Zudem lassen sich wiederhergestellte Dateien nun auf Netzwerk-Shares ablegen, damit nicht versehentlich weitere noch zu rettende Daten auf der Festplatte überschrieben werden. Für 25 Euro ist die Software erhältlich. *(dr)*

www.oo-software.de

IGEL integriert den **Quest vWorkspace-Softwareclient** in die Linux-Modelle der aktuellen Universal Desktop Thin Client-Serien. Mit dem Client lassen sich virtualisierte Desktops und Anwendungen aus unterschiedlichen Plattformen bereitstellen und über eine einheitliche Managementkonsole verwalten. vWorkspace unterstützt unter anderem Hyper-V, VMware ESX oder Parallels Virtuozzo sowie Microsoft Terminal Services (Remote Desktop Session Host). Der vWorkspace Client ist ab sofort in den Linux-Firmware-Paketen "Standard" und "Advanced" für IGEL-Kunden kostenfrei verfügbar. *(dr)*

www.igel.com

Mit Version 2.2 seines **Advanced VPN Client** stellt **LANCOM Systems** den nach eigenen Angaben ersten **IPsec VPN-Client mit Windows 7-Unterstützung** vor. Weitere Neuerungen in der Version 2.2 sind Profilexporte, zusätzliche Hash-Algorithmen, optimierte Log-Ausgaben für eine vereinfachte Fehlersuche sowie der Tipp des Tages, der nützliche Hinweise zum Einsatz der Software gibt. Daneben unterstützt der VPN-Client auch Verbindungen über UMTS und GPRS. Der Advanced VPN Client 2.2 ist ab sofort zum Preis von 99 Euro erhältlich. *(dr)*

www.lancom.de

Actino Software gibt die Verfügbarkeit von **pdfHarmony** bekannt. Mit der Anwendung können Unternehmen PDF-Dokumente auf einem Datei- oder Archivierungsserver automatisch prüfen, reparieren und für die weitere Verwendung aufbereiten. Das Programm soll so zum einen dafür sorgen, dass Dateien vollständig PDF-konform sind und keine technischen Fehler beinhalten. Zum anderen will das Tool unterschiedliche Einstellungen bei der Kompression, der Schrifteinbettung oder den Metadaten ausgleichen. pdfHarmony läuft unter Windows, Mac OS, Linux, Solaris, HP-UX, AIX und AS400 und kostet rund 3.500 Euro. *(ln)*

www.actino.de

Sicherheit per Mausklick

phion bringt Version 4.2 der softwarebasierten **Web Application Firewall airlock** auf den Markt. Zu den Neuerungen gehören neben einer verbesserten Performance auch eine Vielzahl neuer Funktionen, verpackt in eine vollständig überarbeitete Benutzeroberfläche. Eine neue Reverse Proxy-Seite verbindet nun die Übersichten der virtuellen Hosts, Mappings und Backend Hosts. Die grafische Darstellung dieser Verbindungen soll die Navigation vereinfachen und einen schnellen Überblick über den Datenfluss verschaffen. Verbindungen können dabei interaktiv editiert werden und das Hinzufügen oder Entfernen bestehender Verbindungen ist mit einem Mausklick realisierbar. Administrator-Rechte lassen sich zudem rollenbasiert steuern. Der Administrator-Login basiert dabei nun auf dem airlock-Authentisierungsdienst und erlaubt die Anbindung vorhandener Benutzerverzeichnisse wie LDAP, DB oder Radius. Ein Administrator kann sich dadurch mit seinem bestehenden Benutzernamen und Passwort anmelden. Alternativ stehen zudem auch starke Authentisierungsverfahren zur Wahl. Sämtliche Konfigurations- und Regeländerungen werden mit Version 4.2 in einer Configuration History abgespeichert. Bei Bedarf kann so ein schneller Rollback durchgeführt werden. Zudem lässt sich präzise nachvollziehen, wer welche Änderungen zu welchem Zeitpunkt durchgeführt hat. Ab sofort ist die neue Version verfügbar. Für bestehende airlock-Nutzer mit Wartungsvertrag ist das Upgrade kostenfrei. Ansonsten ist die Web Application Firewall ab 14.000 Euro zu haben. *(dr)*

phion: www.phion.com/DE/products/websecurity/Pages/default.aspx

Leistungsfähiges Speichersystem

Fujitsu vervollständigt mit der Modellreihe **ETERNUS DX 400** sein Portfolio an **RAID-Systemen für den Midrange-Bereich**. Die Speichergeräte lassen sich entweder über Fibre Channel mit maximal 8 GBit/s oder iSCSI mit 1 GBit/s in bestehende Storage-Umgebungen einbinden. Die Serie besteht aus den Modellen DX410 und DX440, die sich vor allem hinsichtlich der Anzahl an Host-Schnittstellen sowie der maximalen Skalierbarkeit der Speicherkapazität unterscheiden. Die kleinere Variante verfügt über höchstens 8 FC- oder 4 iSCSI-Anschlüsse, bietet Platz für 210 Festplatten und stellt so bis zu 209 TByte Speicherplatz bereit. Davon lassen sich je nach RAID-Level aber maximal 147 TByte effektiv nutzen. Version DX440 ist jeweils mit der doppelten Menge an Schnittstellen und Festplatteneinschüben ausgestattet. Beide Geräte arbeiten mit der Data Block Guard-Technologie, die einen zusätzlichen Schutz zum RAID bietet: So werden pro 512 Byte weitere acht Byte Paritätsinformationen gesichert. Der Hersteller will auf diese Weise Inkonsistenzen bei den auf Platte oder im Cache gespeicherten Daten unmittelbar feststellen und beheben. Außerdem sind im Lieferumfang Funktionen zum Kopieren und Spiegeln der Daten enthalten. Ein 128-Bit AES-Schlüssel soll Daten auf Disk-Laufwerken außerhalb der Systeme unlesbar machen. Der Einstiegspreis für Modell DX410 als Base-Unit mit 2 Host-Ports beträgt ohne Festplatten rund 26.000 Euro. *(ln)*

Fujitsu: www.fujitsu.de

Fujitsus RAID-System aus der Serie "ETERNUS DX 400" lässt sich auf über 420 TByte skalieren

Datenbank auf den Stick

Mit dem kostenlos erhältlichen Tool **dbHero pack'n'go** bietet **code Hero** eine Software an, mit der sich der **Schnappschuss einer MS-SQL-Server-Datenbank** schnell, komprimiert und verschlüsselt auf einen USB-Stick ziehen lässt. Der Entwickler will es für Admins auf diese Weise vereinfachen, massive MS-SQL-Datenbanken zu bewegen, ohne vorher eine lizenzpflichtige Software installieren zu müssen. Bei der Snapshot-Erstellung greift das Programm weder auf Skripte oder XML, sondern eine binäre Codierung zurück. Dies soll die Archivierung und Wiederherstellung von Datenbanken laut Hersteller deutlich schneller machen. Während sich die mobile Variante nur zum Erstellen des Schnappschusses eignet, benötigen Unternehmen zur Verwaltung, zum Wiedereinspielen oder der teilweisen Wiederherstellung von Datenbanken die Vollversion von dbHero. Mit der Software ist es außerdem möglich, einzelne Tabellen oder ganze SQL-Datenbanken direkt von einem Server zum anderen zu bewegen. Wer zur Archivierung von Datenbanken nicht auf Snapshots zurückgreifen will, kann mit dbHero auch SQL-Skripte generieren. Ferner beherrscht die Software das Bulk Copy-Format zur Erstellung von BCP-Skripten. Die Vollversion des Datenbank-Tools ist zu einem Preis von rund 150 Euro erhältlich. *(ln)*

code Hero: www.code-hero.com

Clientmanagement mit Bandbreitenkontrolle

Aagon gibt den Startschuss für Version 3.7 seiner **Clientmanagement-Software ACMP**. Neben der Unterstützung von Windows 7 und Server 2008 R2 widmet sich das neue Release vor allem der optimierten Übertragung von zu installierenden Softwarepaketen zwischen einem ACMP-Server und den Zielrechnern. Ab sofort lässt sich für jeden Client im Netzwerk festlegen, wie viel Bandbreite er für den Datenaustausch mit einem ACMP-Server beanspruchen darf. Mobilrechner mit einer langsamen Verbindung müssen sich ihre Software nicht mehr herunterladen, sondern lassen sich per Datenträger mit frischen Anwendungen versorgen. In der Pro-Version verschaffen zudem zahlreiche neue Client Commands dem Administrator zusätzliche Möglichkeiten bei der Automatisierung von Wartungsaufgaben. Durch die Skriptsprache lässt sich beispielsweise vor und nach der Installation eines Softwarepakets ein von bestimmten Bedingungen abhängiges Kommando starten. Kleinere Optimierungen finden sich ferner im Lizenzmanagement. Hier lassen sich nun zu jeder Lizenz eines Pakets mehrere Dateien verlinken, was eine bessere Übersicht über die vorhandenen Nutzungsrechte verschaffen soll. ACMP 3.7 inklusive Helpdesk ist seit Mitte Dezember verfügbar. Der Preis pro Lizenz ist gestaffelt und beträgt bei 25 bis 99 PCs 65 Euro. *(ln)*

In Version 3.7 der Clientmanagement-Suite "ACMP" lässt sich die Nutzung der Bandbreite granularer bestimmen

Aagon Consulting: www.aagon.com

Zwergenaufstand gegen Eindringlinge

Securepoint bietet das **TERRA UTM-Gateway Black Dwarf** als **Major-Release-Update in Version 10** an. Dabei hat der Hersteller das Protokoll IKEv2 in die neue UTM-Version integriert. Dadurch lassen sich VPNs ohne zusätzlichen VPN-Client mit Windows 7 nutzen. Eine automatische Regelgenerierung unterstützt die IT-Verantwortlichen beim Aufbau der sicheren IPSec-Verbindungen. In Version 10 befindet sich nun auch der POP3-Proxy, den Securepoint reimplementiert hat. Über ein eingebautes Mail-Relay unterstützt das Gerät zudem SMTP und erlaubt via Greylisting Ausnahmen von Domains, Empfängern oder Absendern. Eine User-Validation über SMTP validiert zudem die Empfänger gegenüber dem Mailserver, während der Administrator das Spam-Tag im E-Mailheader nach eigenen Anforderungen editieren kann. Die neue Browser-Oberfläche soll die Konfiguration und Administration einfacher und übersichtlicher gestalten. Eine vordefinierte Security-Policy erlaubt dabei eine einfache Konfiguration über einen Setup-Wizard bei der Installation, so dass eine sichere Grundpolicy einfach und schnell erstellt werden kann. Für 310 Euro ist das Gerät ab sofort erhältlich. *(dr)*

DeviceLock: www.devicelock.de

Das TERRA UTM-Gateway Black Dwarf schützt kleinere Netzwerk-Umgebungen

In unserem NAS-Einkaufsführer vom Oktober 2009 (Brücken zwischen den Inseln, S. 38-41) haben sich in der Übersichtstabelle leider einige Fehler eingeschlichen. Diese betreffen die Produktbezeichnungen, die Bilder und die Abmessungen der Geräte. Unter www.it-administrator.de/markt/marktuebersichten/1009-NAS-Produkte.pdf steht die korrigierte Fassung der Tabelle zum Download bereit. Wir bitten unsere Leser um Entschuldigung.

So stimmt's

Virtuelle Maschinen im Griff

Radware stellt den **vAdapter** für die **VMware-Plattform** vor. Die Software synchronisiert die bestehende Konfiguration der **Application Delivery Controller** (ADC) mit allen wichtigen Änderungen im virtuellen Rechenzentrum automatisch und in Echtzeit. IT-Verantwortliche können einen Cluster virtueller Maschinen, der einen Service in der virtuellen Umgebung darstellt, direkt auf die entsprechende ADC-Konfiguration abbilden. Wird eine VM dem virtuellen Service-Cluster hinzugefügt oder daraus entfernt, konfiguriert vAdapter den ADC automatisch in Echtzeit um. Alle manuell und automatisch vorgenommenen Änderungen an den Einstellungen werden zudem aufgezeichnet. Für Compliance-Zwecke und Nachverfolgung der Änderungen steht so ein vollständiges Protokoll bereit. Die neue Komponente ist Teil der Application Delivery Suite und lässt sich in die AppDirector und Virtual Director Produkte sowie die Alteon Application Switches integrieren. Dabei ist die Software als Plug-In für VMware vCenter und als Web-basierte Stand-alone-Variante verfügbar. Neben AppDirector und den Alteon Application Switches arbeitet vAdapter mit Managementsystemen anderer Anbieter zusammen und unterstützt verschiedene ADC-Geräte. vAdapter steht ab sofort kostenlos als Virtual Appliance im Open Virtual Machine Format (OVF) für VMware-Umgebungen zum Download bereit. *(dr)*

Radware: www.radware.de

1&1 Dynamic Cloud Server

FLEXIBLER

Nach Bedarf konfigurieren. Einfach online –

1&1 DYNAMIC CLOUD SERVER

Hochleistungsserver mit eigener dedizierter Serverumgebung und vollem Root-Zugriff. CPU-Anzahl, Festplattenspeicher und Arbeitsspeicher können jederzeit nach Bedarf konfiguriert werden – der Preis passt sich automatisch an.

Konfigurieren Sie Ihren Server individuell. Starten Sie mit dem 1&1 Dynamic Cloud Server Basis-Paket:

- **1 AMD Opteron™ 2352 Core (bis auf 4 Cores erweiterbar)**
- **1 GB RAM (bis auf 15 GB RAM erweiterbar)**
- **100 GB Webspace (bis auf 800 GB Webspace erweiterbar)**
- **Linux (Windows optional)**
- **Unlimited Traffic**
- **Voller Root-Zugriff**
- **Parallels Plesk Panel 9**
- **24/7 Hotline und Support**

Große Einführungs-Aktion:

3 Monate gratis!*

Basis-Paket

~~39,99 €/Monat*~~

3 Monate für 0,– €/Monat, danach 39,99 €/Monat.*

0,– €/Monat*

*Große Einführungs-Aktion: Das 1&1 Dynamic Cloud Server Basis-Paket gibt es 3 Monate für 0,– €, danach 39,99 €/Monat. Einmalige Einrichtungsgebühr 39,– €. 12 Monate Mindestvertragslaufzeit. Preise inkl. MwSt.

MEMBER OF united internet

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

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

1&1 Innovation!

SERVER

jederzeit.

Als einer der ersten Server-Hoster weltweit präsentiert 1&1 seinen neuen Dynamic Cloud Server – die individuelle Server-Lösung, mit der Sie Leistung und Performance jederzeit ganz flexibel an Ihre aktuellen Bedürfnisse anpassen können.

Weitere attraktive Server-Angebote im Internet!

1&1

www.1und1.info

IT-Administrator-Workshop "VoIP im Unternehmensnetz" am 25. Februar 2010 in München

ITANet Workshop-Partner:

Netcordia™
Simply a better way to manage

Wer hören will, muss messen

von Mathias Hein und John Pardey

Quelle: mipan - Fotolia.com

Voice over IP stellt besondere Anforderungen an die Netzinfrastruktur. Daher bilden umfassende und qualitative Messungen, ob und welche Teile des vorhandenen Netzwerks hinsichtlich Gesprächsqualität, Minimierung der Verzögerungen und Zuverlässigkeit VoIP-fähig sind, die Basis für den Umbau der Dienste und der Netze. Auf der Basis einer "VoIP-Ready-Messung" muss nicht mehr pauschal in VoIP investiert werden, sondern gezielt nur da, wo das Netzwerk einen "Upgrade" notwendig hat. In unserem Workshop erfahren Sie, wie Sie Predeployment-Messungen vornehmen können, welche Parameter besonders zu beachten sind und wie sich gängige Probleme lösen lassen.

Die Telefon- und Datenkommunikation ist im heutigen geschäftlichen Umfeld als Kommunikationsmittel wichtiger denn je. Immer mehr Applikationen aus der Telefon-, Video- und Datenwelt sind bereits oder werden in naher Zukunft untrennbar als so genannte Unified Communications (UC) miteinander verknüpft. Daher ist die vollständige Integration der Systeme nicht mehr aus der Kommunikation wegzudenken.

Dabei geht jeder Vorbereitungs- und Realisierungsphase ein erheblicher Planungsaufwand voraus. Grundlage jeder VoIP-Integration ist die umfassende Überprüfung der vorhandenen Netzwerke. Die Planungsannahmen werden so in der Praxis getestet und der Netzplaner versichert sich vor der Umstellung auf das neue System, dass die neuen Anwendungen in Zukunft problemlos im Netzwerk arbeiten.

VoIP-Fähigkeit vor dem Einkauf messen

Um die VoIP-Readyness eines oder mehrerer Unternehmensnetzwerke feststellen zu können, ist es nicht notwendig, die geplanten Komponenten (Telefone, Server, Gateways) anzuschaffen und zu installieren. VoIP-Simulatoren beziehungsweise -Analysatoren übernehmen die Aufgabe, tausende von Anwendern und deren Telefonverhalten nachzubilden und Schritt für Schritt in das Netzwerk einzuspielen.

Um die Performance und Leistungsgrenze der VoIP-Komponenten zu ermitteln, ist im Vorfeld ein umfassender Produkttest in einem Testnetz notwendig. Dabei kann der IT-Verantwortliche zuverlässig erkennen, an welchen Stellen das Netz VoIP-fähig ist und wo nicht. Wichtiger noch: Er erhält Aufschluss darüber, in welcher Qualität sich die VoIP-Anwendung bereitstellen lässt. Schwachstellen werden noch vor der eigentlichen Installation und Inbetriebnahme erkannt, Nachbesserungen vorgenommen.

Bei einer Vormessung sollten die Anwendungsbedingungen über einen längeren Zeitraum hinweg erfasst werden. Ein zu kurzer Mess- und Testintervall berücksichtigt oftmals nicht die verkehrsreichsten Zeiten. Bei Voice over IP besteht die Herausforderung darin, die Sprache in hoher Qualität und ohne Performance-Einbußen für die bestehenden Anwendungen zur Verfügung zu stellen. Die Basis dafür bilden die Funktionalität und Skalierbarkeit der VoIP-Komponenten. Die Akzeptanz bestimmt die Quality of Service (QoS) der Signalisierung und der eigentlichen Sprachübermittelung.

Messung im bestehenden Netz

Die Qualität der Komponenten im Zusammenwirken mit den vorhandenen

Netzwerk- und Server-Systemen spielt eine wichtige Rolle, wenn es um die Voice-Readiness des Netzwerks geht. Kleinste Ungereimtheiten können oft eine Kettenreaktion auslösen. Die Suche nach der Ursache der Schwachstellen wird oft zur Suche nach der Nadel im Heuhaufen.

Der Workshop zeigt auf, wie Sie in VoIP-Vormessungen überprüfen,

- ob das Netzwerk VoIP-Ready ist,
- wie gut VoIP im bestehenden Netzwerk funktionieren wird,
- an welchen Stellen im Netzwerk Engpässe bestehen und/oder nachgebessert werden muss.

Es wird ein bestehendes und für andere Anwendungen genutztes Netzwerk auf VoIP-Readyness getestet. Zwischen im Netz verteilten Messendpunkten wird der VoIP-Verkehr entsprechend eines zu definierenden VoIP-Nutzungsprofils erzeugt. Dabei können tausende VoIP/UC-Anwender mit entsprechendem VoIP-Codec simuliert werden.

Diesen und vielen weiteren Themen (siehe Kasten "Agenda") wendet sich Mathias Hein in unserem Workshop am 25. Februar zu. IT-Verantwortliche, die den Einstieg in VoIP vor Augen haben oder aktuell Probleme mit der Sprachübermittlung im Unternehmensnetzwerk beobachten, sollten diesen Workshop nicht verpassen. Die Anmeldeinformationen finden Sie im Kasten auf dieser Seite. Der für alle Abonnenten kostenlose Workshop steht ab sofort zur Registrierung offen und wir würden uns freuen, Sie in München begrüßen zu dürfen.

iTANet
Die System und Netzwerk User Group

Die Agenda des Workshops

13.00 Uhr: Begrüßung

13.15 Uhr: Voice over IP - Teil 1

- Status des Marktes und Marktentwicklungen
- Problembereiche bei VoIP
  - Verzögerung
  - Packet Loss
  - Jitter
  - Gateways/NATs
  - SIP Trunks
- Ohne QoS geht die Sprache im Netz verloren

Dozent: Mathias Hein

14.30 Uhr: Kaffeepause

14.45 Uhr: Avoiding 8 out of the 10 Network Failures

Dozent: Simon Horrocks, EMEA Regional Sales Manager Netcordia

(Vortrag in englischer Sprache)

15.30 Uhr: Voice over IP - Teil 2

- Messszenarien mit Live-Demo zur Fehlersuche für den Praktiker:
  - Vormessungen
  - E-Model vs. PESQ
  - Sprachanalyse
  - Langzeitmonitoring
- Ausblick in die Zukunft

Dozent: Mathias Hein

17.30 Uhr: Ende des Workshops

Ort: ExperTeach Training Center, Wredestraße 11, 80335 München

Teilnahmegebühren:
Für IT-Administrator Abonnenten kostenlos.

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

Agenda des Workshops "VoIP" am 25. Februar

Mathias Hein verfügt über 25 Jahre Berufserfahrung und arbeitet als freier IT-Berater und Fachautor. Daneben ist er an der FH Reutlingen und der Berufsakademie Mannheim als freier Dozent tätig. An der ComConsult Akademie ist er Referent für die Themenbereiche Switching, TCP/IP und Netzmanagement. Als freier Autor im Fachbuchbereich und in den einschlägigen Fachzeitschriften trägt Mathias Hein regelmäßig zur Wissensvermittlung bei.

Mathias Hein erhielt zum Beginn seiner Karriere als einer der ersten Netzwerker in Deutschland die Aufgabe eines Produktspezialisten bei dem Distributor Wetronic (München). In seinen anschließenden Tätigkeiten als technischer Leiter bei Fuba Communication (Hilden) und Rockwell Communications (London) erwarb er sich den Ruf als pragmatischer Troubleshooter im Bereich der Netzwerke. Von 1990 bis 1994 arbeitete Hein als freier Unternehmensberater (Netzanalyse, Planung, Projektierung und Implementierung) sowie als TCP/IP-Trainer für diverse Schulungsunternehmen. Anschließend arbeitete er fünf Jahre als Marketingmanager für Bay Networks (Deutschland, Österreich und Schweiz). Seit 1999 ist er als freier Unternehmensberater, Autor und Trainer tätig.

Der Dozent

Microsoft TechEd, 9. bis 13. November 2009, Berlin

Windows 7 auf dem Kudamm

von John Pardey

Mehr als 6.800 Teilnehmer aus 104 Ländern fanden Anfang November den Weg nach Berlin, um der europäischen Ausgabe von Microsofts zentraler technischer Fortbildungsveranstaltung, der TechEd 09, beizuwohnen. Überraschende Neuerungen oder strategische Ankündigungen seitens des Veranstalters blieben aus, was die Teilnehmer jedoch nicht entmutigte, sich in den über 600 Sessions mit den zahlreichen bereits verfügbaren neuen Technologien wie etwa Windows 7, Server 2008 R2 und Exchange 2010 intensiv vertraut zu machen.

Trotz bunter Ausleuchtung blieb die TechEd-Keynote eher blass

Den Eröffnungstag der TechEd auf das gleiche Datum zu legen, an dem in Berlin 20 Jahre "Mauerfall" ganz offiziell gefeiert wurden, führte einerseits durch gesperrte Innenstadtstrassen zu gewissen Problemen bei der Anreise, andererseits bot sich der internationalen Teilnehmerschaft die Gelegenheit, diesen historischen Feiertag aus erster Hand mitzuerleben.

So führte denn auch Achim Berg, Vorsitzender der Geschäftsführung der Microsoft Deutschland GmbH, mit großem Bezug zu diesem Jubiläum in die Keynote ein. Zu dieser trat dann Stephen Elop, President Microsoft Business Division, an. Dabei postulierte Elop die "New Efficency", die sich mit dem Einsatz von Windows 7, Windows Server 2008 R2 und Exchange 2010 im Unternehmen erreichen lasse.

Besonders Exchange 2010, das Elop im Rahmen der Keynote als "weltweit verfügbar" ankündigte, ermögliche laut einer Forrester Studie [1, 2] 70 Prozent Kostensenkung durch ein vereinfachtes Hochverfügbarkeitsmodell und Unterstützung für günstigere Speichermöglichkeiten. Ein Blick in die entsprechende Studie zeigt allerdings, dass hierbei Exchange 2010 nur mit seinen Vorgängermodellen verglichen wurde, zudem basiert die Studie auf lediglich neun Interviews mit IT-Verantwortlichen.

Weitere zentrale Aspekte der Keynote waren selbstverständlich die beiden neuen Windows-Versionen sowie die neuen Funktionen des System Center 2007 R2. Alles in allem jedoch blieb die Keynote, trotz Unterstützung durch Videoeinspieler und Massagesessel, eher blass, denn etwas wirklich Neues hatte Elop nicht zu verkünden.

Sessions und mehr

Doch den Teilnehmern blieb die Wahl aus mehr als 600 Vorträgen, Hands-on-Laboren und verschiedenen anderen Vortragsformaten, um Neues zu erfahren. Dieses breite Angebot nutzten Administratoren und Entwickler – die TechEd-Woche in Berlin war, im Gegensatz zu den vergangenen Jahren, wieder eine gemeinsame Veranstaltung für Entwickler und Administratoren – reichlich, viele Sessions waren bis zum Bersten gefüllt.

Darüber hinaus bot sich die Möglichkeit, vor Ort Zertifizierungsprüfungen abzulegen, in direkten Kontakt zu Microsoft-Experten aller Fachrichtungen zu treten oder sich in der großen Ausstellung mit den Angeboten der wichtigsten Unter-

nehmen in Sachen Hard- und Software sowie Entwicklungslösungen vertraut zu machen. Und wer einmal keine Lust oder Energie für die eigene Weiterbildung aufbringen konnte, dem bot sich die Gelegenheit, im Sandsessel oder vor der XBox eine freie Minute zu verbringen. Die Organisation vor Ort bot einen perfekten Mix, um die Woche in Berlin ebenso angenehm wie lehrreich zu verbringen.

Zentrale Themen

Bei der angesprochenen Zahl von Vorträgen fällt es naturgemäß schwer, einen inhaltlichen Fokus auszumachen, denn die Auswahl an Sessions war mindestens ebenso groß wie die unterschiedlichen Interessen der Teilnehmer. An einigen ganz zentralen Themen neben der allgegenwärtigen Virtualisierung war für den Admin jedoch kein Vorbeikommen:

Der PowerShell gehört die Zukunft der Administration: So ist der Anteil über die GUI erreichbarer Verwaltungsaufgaben von 97 Prozent in Windows Server 2003 auf 85 Prozent in Windows Server 2008 R2 gesunken. Microsoft postuliert diese Steigerung der Bedeutung der Arbeit auf der Kommandozeile seit Jahren – und macht nun Ernst. Wer in seinem Unternehmen über die Einführung des neuen Servers und Windows 7 nachdenkt, kommt an der Powershell nicht mehr vorbei!

Mobilität und verteilte Standorte rücken in den Fokus der Administration: Zweifellos wandelt sich unsere Arbeitswelt. Home Office, hochmobile Mitarbeiter und verteilte Außenstellen geben auch der IT immer mehr den Takt vor. Hier reagiert Microsoft immer stärker mit explizit auf derartige Konstellationen ausgelegte Features, die den IT-Verantwortlichen in die Lage versetzen, derartige Anforderungen umzusetzen.

IPv6 kommt: Eine weitere eindeutige Botschaft aus Berlin ist, dass IPv6 nicht mehr aufzuhalten ist – und diesmal wirklich. Die IP-Adressknappheit ist dabei zwar nach wie vor ein wichtiges Thema, doch dass Microsoft nunmehr Features anbietet, die auf IPv6 aufbauen, ist ein deutlicher Fingerzeig an jeden Administrator, sich mit dem neuen Protokoll intensiv zu beschäftigen.

Sicherheit, Sicherheit, Sicherheit: Zahlreiche Sessions fokussierten die IT-Security aus den verschiedensten Blickwinkeln, sei es nun die Verschlüsselung mobiler Daten mit BitLocker, Zugriffsschutz oder das Bewusstsein der Mitarbeiter über mögliche Bedrohungen. Einen der "interessantesten" Sätze zu diesem Thema gab Marc Estberg, Verantwortlicher für die Compliance der MS Cloud Services (etwa Hotmail oder LiveID) zum Besten. Estberg, der für mehrere hunderttausend Server verantwortlich zeichnet, sagte trocken: "Patchmanagement is dead". Vielmehr würde nur eine klare Prozessorientierung in Sachen Compliance, IT-Governance und Patchmanagement, die zwischen IT und Fachabteilung eingerichtet werde, für nachhaltige Sicherheit in großen Umgebungen sorgen.

Alter Bluescreen, neuer Desktop

Neben den Neuerungen fand sich auch ein alter Bekannter auf der Agenda wieder: der Bluescreen. Daniel Pearson, bekannter Trainer und ehemaliger Kollege von Marc Russinovich, kam nicht umhin, auch im Jahr 2009 aufzuzeigen, wie die Informationen eines Windows Crash Dump zu entschlüsseln sind, um den Ursachen von Bluescreens auf die Schliche zu kommen. Inhaltlich unterschied sich dieser Vortrag kaum von vergleichbaren Präsentationen zu NT 4.0, doch das dichte Gedränge im Saal verriet, dass das Thema nach wie vor aktuell ist. Mit Hilfe diverser Sysinternal-Tools [3] lassen sich mit einiger Detektivarbeit etwa Bluescreen-verursachende Treiber finden.

Einen wichtigen und neuen Hinweis hatte Person auch noch für die Zuhörerschaft: soll Windows im Falle eines Stopp-Fehlers den vollständigen Crash Dump schreiben können, muss die Auslagerungsdatei mindestens so groß sein wie das RAM des betroffenen Systems, denn die Informationen eines solchen Crash Dumps enthalten den kompletten Speicherinhalt zum Zeitpunkt des Absturzes. Und da Windows aus Sicherheits- und Integritätsgründen das Speicherabbild in die *pagefile.sys* schreibt, muss diese logischerweise genügend Kapazität hierfür bieten.

Zu guter Letzt sei aus der Fülle der gebotenen Informationen noch Microsofts MDOP (Desktop Optimization Pack) hervorgehoben, das fast so präsent war, wie einige der weiter oben als zentral angesprochenen Themen. Die Möglichkeiten, die diese Sammlung von Tools in Sachen Virtualisierung und Desktopsupport bietet, sind wirklich für jeden Administrator einen Blick wert. Das leider nur für Software Assurance-Kunden verfügbare Softwarepaket bietet neben Werkzeugen zur Applikationsvirtualisierung (App-V) und Desktopvirtualisierung (Med-V) auch Diagnose- und Wiederherstellungstools, einen Inventarisierungsdienst und erweiterte Einsatzmöglichkeiten für Gruppenrichtlinien.

Letztendlich dürften die Teilnehmer Berlin hochzufrieden und mit einer Fülle neuem Know-how verlassen haben. Die Auswahl wie auch die technische Tiefe der Vorträge waren überzeugend, wenn auch der ein oder andere namhafte Sprecher vermisst wurde. Derart gut gerüstet steigen sicher viele IT-Verantwortliche gut gerüstet in die in vielen Unternehmen anstehende Migration zu Windows 7 ein.

Links

[1] Forrester-Studie zu Exchange 2010
http://go.microsoft.com/?linkid=9694416
[2] Forrester-Studie zu Windows Server 2008 R2
http://go.microsoft.com/?linkid=9695563
[3] Sysinternals
www.sysinternals.com

Im Vergleichstest: Migration auf Windows 7 mit vier Client-Management-Suiten

Bequeme Fahrt nach oben

von Thomas Bär

Die große Nachfrage nach Windows 7 überraschte selbst Microsoft. In zahlreichen Unternehmen steht nun die Migration von XP-Systemen auf Windows 7 an. Doch ist der nahtlose Umstieg auf das neue Betriebssystem nicht einfach. In unserem Vergleichstest nahmen wir vier Client-Management-Suiten unter die Lupe, die sowohl bei der Verteilung als auch dem künftigen Betrieb helfen sollen.

Quelle: photo25th - Fotolia.com

Mit den richtigen Client-Management-Suiten fällt der Umstieg auf Windows 7 nicht schwer

Migrationen von einer auf die nächste Betriebssystem-Generation sind für IT-Administratoren in aller Regel mit Aufwand und Schwierigkeiten verbunden. Um die Angst vor Programm-Inkompatibilitäten beim Upgrade auf Windows 7 zu nehmen, hat Microsoft den Windows-XP Modus für den Weiterbetrieb von älteren Programmen in den Vista-Nachfolger integriert. Hierbei handelt es sich um eine komplett vom eigentlichen Betriebssystem unabhängige Windows XP SP3 Installation auf Basis von Virtual PC. Dieser ist aus Sicht des Administrators jedoch wie ein eigenständiger PC in Bezug auf Patches oder Virenschutz zu betrachten. Dass Microsoft die Lizenz für das virtualisierte XP als Dreingabe zusteuert, sollte über den administrativen Mehraufwand nicht hinwegtäuschen. Um "ältere Software", so genannte Legacy Applications, in virtuellen Umgebungen bereitzustellen, gibt es andere etablierte Lösungen wie beispielsweise VMware ThinApp, die dem Windows 7 XP-Modus überlegen sind. Zudem erfordert der XP-Modus in Windows 7 CPUs der neueren Generation, was eventuelle PC-Neukäufe nach sich zieht.

Eine direkte Übernahme aller Programme, Dateien und Einstellungen von Windows XP zu Windows 7 ist ohne Weiteres nicht möglich. Das so genannte "Inplace Upgrade" bleibt Windows Vista vorbehalten – XP-Rechner, die auf Windows 7 umgestellt werden sollen, müssen neu installiert werden. Alle Programme, Einstellungen und Daten gehen bei diesem Vorgang zwangsläufig verloren. Für die Übernahme von Dateien und Einstellungen bietet Microsoft den "Windows Easy Transfer". Dieses Tool eignet sich jedoch in erster Linie für den Einsatz bei privat genutzten Einzel-PCs und übernimmt zudem nur die Konfiguration von Microsoft-Produkten. Wer nicht selbst mit Skripten die Übernahme realisieren will, dem stehen verschiedene Systems-Management- oder Client-Lifecycle-Management-Lösungen zur Auswahl.

Identische Funktionsweise

Für unseren Vergleichstest haben wir die vier gängigsten Suiten für den Mittelstand ausgewählt, die zum Testzeitpunkt die Migration auf Windows 7 unterstützten. Eines haben die unterschiedlichen Systemmanagement-Suiten dabei gemeinsam: ihre Arbeitsweise und die Anforderungen an die Umgebung. Im Netzwerk wird stets ein PXE-Server (Preboot Execution Environment) eingerichtet und alle Client-Computer müssen im BIOS in der Bootreihenfolge zunächst "LAN" ausgewählt haben. So ist gewährleistet, dass neue Computer stets in den Konsolen aufgelistet und anstehende Kommandos wie etwa die Neuinstallation eines Betriebssystems in jedem Fall beim Neustart ausgeführt werden. Liegen keine Aufträge für den Client vor, so startet dieser das Betriebssystem von der lokalen Festplatte.

Nach dem Start des Betriebssystems kommt es wieder zu einer Gemeinsamkeit: Es wird typischerweise eine Agent-Software gestartet, die den Computer zentral über die Steuerkonsole der Management-Software ad-

ministrierbar macht. Ohne eine Agent-Installation wären die Steuerungsmöglichkeiten einfach zu gering. Bevor ein Betriebssystem verteilt werden kann, muss es zunächst in die Systems-Management-Software integriert werden. Alle Programme verwenden dafür einen Wizard, der das Installationsmedium auf einen Server überträgt. In größeren Umgebungen mit verschiedenen Standorten, die über schmalbandige Leitungen verbunden sind, ist möglicherweise das Vorhalten verschiedener Softwaredepots, üblicherweise per einfacher Dateifreigabe, empfehlenswert.

Wird eine Betriebssystem-Ferninstallation von Windows 7, Windows Server 2008 oder Windows Vista durchgeführt, so geschieht dies mit der Hilfe von WinPE, dem "Windows Preinstallation Environment". WinPE, die Installationsdateien und die benötigten Treiber werden vom Verwaltungsserver geladen und in einer speziellen Service-Partition abgelegt. Einen Neustart später beginnt eine "unattended Installation" von Windows.

Vorbereitung der Migration

Sobald eine größere Anzahl von Computern in einem Zug oder in kurzer Zeit migriert werden soll, ist es ratsam, einen Plan für das Unterfangen auszuarbeiten. Im ersten Schritt gilt es, die vorhandene PC-Infrastruktur auf die zu erfüllenden Hardware-Voraussetzungen zu überprüfen. Je nach Version der Systems-Management-Lösung sind entsprechende Filter oder Reporte gleich vorbereitet oder müssen manuell erstellt werden. Neben der Erfüllung der Grundvoraussetzungen müssen die passenden Treiber bereitstehen. Für die Installation des Betriebssystems sind zunächst die Treiber für das Festplatten/RAID-System und die Netzwerkkarte zwingend erforderlich, da ohne diese beiden keine Einrichtung von Windows 7 gelingt. Weitere Treiber können später, passend zur Maschine, auch als Softwarepaket nachinstalliert werden.

Roaming-Profile

Die serverbasierten Benutzerprofile, so genannte Roaming-Profile im Active Directory, werden durch Windows Vista/7-Clients verändert. Das Profil auf dem Server wird neu angelegt und durch das Anhängen der Bezeichnung ".V2" erweitert, da sich die komplette Struktur der Profilordner verändert hat. Dies bedeutet, dass es nicht möglich ist, Daten zwischen einem Standard-Profil und einem V2-Profil zu teilen. Eine Alternative besteht in der Möglichkeit der Ordnerumleitung, da umgeleitete Ordner für Anwendungsdaten, Desktop oder Eigene Dateien von verschiedenen Betriebssystemen genutzt werden können.

Bei der Frage, welche benutzerspezifischen Einstellungen – von individuell angelegten Netzlaufwerken und Druckerverknüpfungen über das Desktop-Hintergrundbild bis hin zur E-Mailsignatur – ihren Weg von XP zu Windows 7 finden sollen, unterscheiden sich die Ansätze der Hersteller. Entweder lassen sich in einer grafischen Maske Programmeinstellungen anhaken oder über Skriptsprachen die entsprechenden Registry-Schlüssel und Dateien übertragen. Eine Übertragung aller Einstellungen auf das neue Betriebssystem ist in den seltensten Fällen praktikabel.

Dass alle zu installierenden Anwendungen auch für den Einsatz unter Windows 7 freigegeben sein müssen, das versteht sich beinahe von selbst. Bevor jedoch eine Verteilung an viele PCs in Angriff genommen wird, empfiehlt es sich, eine intensive Prüfung der Schlüssel-Applikationen durch die jeweiligen Fachabteilungen durchführen zu lassen. Da diese Prüfung eine gewisse Zeit in Anspruch nehmen wird, sollte mit diesem Vorgang möglichst früh begonnen werden. Programme, die besonders eng mit der Hardware verzahnt sind, beispielsweise für Zusatzkomponenten bei Notebooks, Sicherheitsprogramme oder Applikationen, die einen Dongle benötigen, gelten als heikel, was das Betriebssystem angeht.

Andere Systeme als Windows XP

Generell kann eine Migration von Windows Vista auf Windows 7 auf dem gleichen Weg erfolgen, wie in diesem Artikel beschrieben. Im Gegensatz zu XP ist aber auch eine Inplace-Installation auf Windows 7 möglich. Eine komplette Neuinstallation mit gezielter Übernahme der persönlichen Einstellungen der Benutzer dürfte jedoch stets der "saubere Schritt" sein.

Rechner mit Windows 2000 Professional als Betriebssystem finden sich in Unternehmen typischerweise in Bereichen, in denen es keinen Internetzugriff oder gar Netzwerkzugriff gibt. Die Hardware eines Windows 2000-PCs wird die Anforderungen von Windows 7 kaum erfüllen, somit ist das Auslesen der Benutzereinstellungen und Daten und die anschließende Übertragung auf einen neuen PC mit Windows 7 der wahrscheinlichste Weg der Umstellung.

Windows NT 4.0 und Windows 95/98-Computer dürften aktuell nur noch äußerst selten im Produktivbetrieb sein. Da diese PCs die Mindestvoraussetzungen für Windows 7 ebenfalls kaum erfüllen dürften, ist mit einer direkten Migration kaum zu rechnen. Gibt es zwingende Gründe für den Betrieb der bereits seit Jahren aufgekündigten Betriebssysteme, so ist möglicherweise eine Virtualisierung der benötigten Software mit VMware ThinApp eine Möglichkeit des Weiterbetriebs. Die Virtualisierung des gesamten Systems mit Hilfe von VMware Workstation, Virtualbox oder Microsoft Virtual PC wäre ebenfalls ein gangbarer Weg, jedoch mit dem Manko der zusätzlichen Betreuung durch die IT.

Baramundi Management Suite

Die "Baramundi Management Suite" (BMS) des in Augsburg ansässigen Softwarehauses Baramundi ist ein modular aufgebautes System. Wie beinahe bei allen Management-Suiten steht auch bei der BMS eine hohe Anzahl von Modulen für einen geringeren manuellen Aufwand bei der Migration. Die aktuell vorliegende Version 8.0 SP1 der BMS ist bereits vollständig zu Windows 7 kompatibel. Zwingend erforderlich für den Wechsel des Betriebssystems ist "Baramundi OS-Install" zur automatischen Installation von Betriebssystemen und "Baramundi Deploy", die Softwarekomponente zur Verteilung der gewünschten Applikationen.

Windows AIK

Das "Windows Automated Installation Kit" (WAIK) besteht aus Programmen und Hilfedokumenten zur Unterstützung der Konfiguration und Bereitstellung von aktuellen Windows-Betriebssystemen. Indem Windows AIK verwendet wird, lassen sich Windows-Installationen automatisieren, Windows-Abbilder mit ImageX erfassen, Abbilder mit der Abbildverwaltung für die Bereitstellung (DISM) konfigurieren und bearbeiten, Windows PE-Abbilder erstellen sowie Benutzerprofile und Daten mit dem Migrationsprogramm für den Benutzerstatus ("User State Migration Tool") migrieren. Darüber hinaus liefert Windows AIK das "Volume Activation Management Tool" (VAMT), mit dem der Aktivierungsvorgang für Volumenlizenzen automatisiert und zentral verwaltet werden kann.

Sollen Benutzereinstellungen von den vorherigen Windows XP Installationen auf den neuen Windows 7 PC übernommen werden, ist zudem der Einsatz des "Baramundi Personal Backup" erforderlich. Das ebenfalls optional erhältliche "Baramundi Patch Management" bietet die Möglichkeit, die Verteilung von Sicherheitsupdates, Patches, Hotfixes und Service Packs von Microsoft zentral aus der Baramundi Console heraus durchzuführen. Eine detaillierte Preisangabe für eine Umgebung mit 500 Clients wurde uns mit dem Hinweis auf die einzelnen, getrennt zu lizenzierenden Module nicht mitgeteilt.

Die Baramundi Management Suite ist eine optisch und funktionell sehr ansprechende Software, die sich dem Benutzer zügig erschließt. Das mag nicht darüber hinwegtäuschen, dass alle Programme der Kategorie "Systems-Management" oder "Client-Lifecycle-Management" einer gewissen Einarbeitungszeit und einer Schulung bedürfen. Bei der Suche nach Windows 7-tauglicher Hardware setzt Baramundi auf den originalen "Windows 7 Upgrade Advisor" von Microsoft, der in die BMS integriert wurde. Anstatt jeden Rechner von Hand zu prüfen, wird der Advisor über einen Baramundi-Job angestoßen und auf allen erreichbaren PCs durchgeführt. In einem aussagestarken Report erhält der Administrator Hinweise über alle potentiellen Software-, Hardware- oder Treiber-Probleme. Über die Homepage des Herstellers wird diese Prüfung auch für Nicht-Kunden zum Festpreis angeboten.

Die Betriebssystem-Ferninstallation mit Baramundi OS-Install verwendet die native OS-Installation von Windows, was bei den meisten aktuellen Computersystemen mit einem sehr geringen Aufwand bei der Treiberpflege einhergeht. Sollten Anpassungen an der WinPE-Installationsumgebung erforderlich sein, so werden diese mit dem Microsoft Tool "WAIK" (siehe Kasten) vorgenommen. Alle anderen Komponenten wie Grafikkarten- oder Soundkartentreiber werden später wie Programmpakete verteilt.

Besonders in größeren Umgebungen ist die Abbildung individueller Organisationseinheiten äußerst wichtig, die nach unterschiedlichsten Merkmalen wie Netzwerkanbindung, Standorten oder Kostenstellen aufgebaut sein kann. Die Migration ist in der BMS ein gewöhnlicher "Job", der sich auf beliebige Ziele ausführen lässt. Die intelligente zentrale Jobsteuerung von Baramundi ermöglichte es in unserem Test, sowohl Gruppen von Client-PCs, dynamische Gruppen von Clients oder einzelne Clients mit jeweils einem Job zu behandeln.

Das Paketieren von Software übernimmt im Baramundi-Umfeld das bekannte "AdminStudio" auf Basis von MSI-Paketen. Die Verwendung von MSI, insbesondere bei An-

Bild 1: Der Statusverlauf der einzelnen Jobs ist in der Baramundi BMS durch ein einfaches und selbsterklärendes Farbschema erkennbar

Produkt
Client-Management-Suite mit Windows 7-Unterstützung.

Hersteller
Baramundi
www.baramundi.de

Preis
Bei Abnahme von 500 Lizenzen beträgt der Listenpreis pro Client 49,70 Euro.

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

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

Installation/Bedienung	8
Funktionsumfang	8
Reporting für Windows 7	8
Übernahme von Einstellungen	8
Migrations-Durchführung	10
Gesamtbewertung	**8,4**

Baramundi BMS 8.0

Neue Version 3 ab sofort verfügbar

Ein neuer Ansatz im IT Asset Management

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

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

NetSupport DNA ist ein vollständig modular aufgebautes System zur Lizenzverwaltung und Inventarisierung von umfangreichen Hard- und Software-Installationen. Neben frei konfigurierbaren Benachrichtigungs- und Alarmfunktionen bietet es ein umfassendes Überwachungssystem für die Nutzung des Internet und der installierten Software. Selbstverständlich lassen sich Software-Anwendungen und Daten mittels Push & Pull-Funktionen komfortabel über Internet und LAN im Netzwerk verteilen.

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

Mittels einer neuen Energie-Monitoring-Komponente können potentielle hohe Energieverbrauche von Computern innerhalb verschiedener Unternehmensbereiche erkannt werden. NetSupport DNA bietet darüber hinaus auch eine vollständige AD-Integration, marktführende Fernwartungsfunktionen und optional einen ITIL-basierenden Helpdesk.

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

NETWORKcomputing AWARDS 2009
SERVICE MANAGEMENT PRODUCT OF THE YEAR
WINNER

PC PRO

NetworkComputing AWARDS 2008
FINALIST

PCPlus

Weitere Informationen und den kostenlosen Testdownload finden Sie hier

www.netsupportdna.com

PCIS

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

wendungen, gewährleistet gemäß den Erfahrungen des Herstellers ein Maximum an Kompatibilität mit Windows 7, insbesondere auch im Hinblick auf 64-Bit-Systeme. Die automatisierte Verteilung gewünschter Pakete im Anschluss an eine Migration ist bei Baramundi problemlos möglich.

Wie alle Hersteller warnen auch die Consultants von Baramundi davor, alle benutzerspezifischen Einstellungen blind auf das migrierte Windows 7-System zu übertragen. Die simple Übertragung kann bei Client-Computern zu abweichenden Konfigurationen führen, was die Fehlersuche, beispielsweise bei Druckerproblemen, unnötig erschwert. Korrekte Einstellungen lassen sich über "Baramundi Deploy" definieren. Ist trotzdem eine Übernahme der Einstellungen gewünscht, kann dies auch pauschal mit "Baramundi Personal Backup" erfolgen.

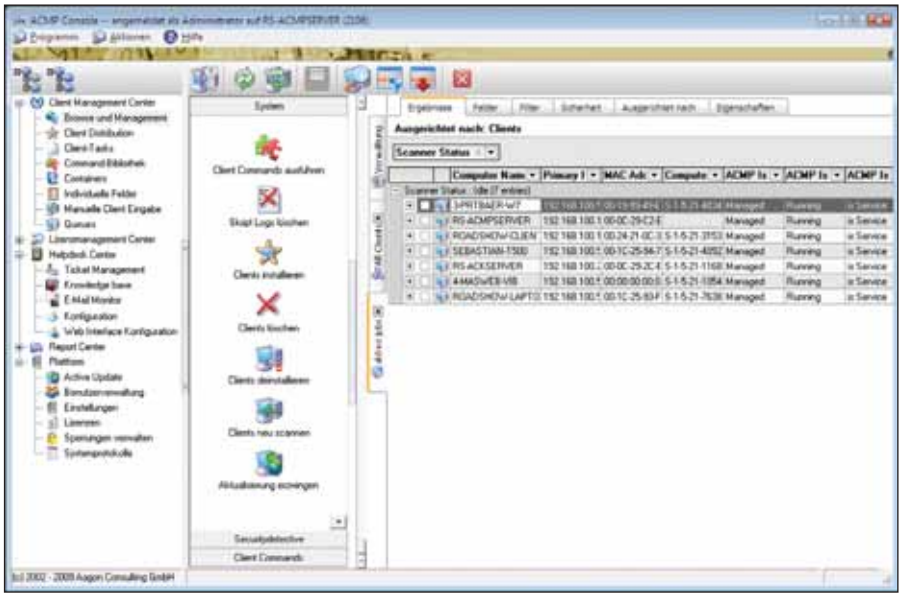


Bild 2: Nach der Migration wird die ursprünglich unter Windows XP installierte Maschine als Windows-7 System neu in die ACMP-Auflistung aufgenommen

Aagon ACMP Suite

Aagon aus dem westfälischen Soest bietet das Basissystem seiner Software seit vielen Jahren kostenlos an. Für die Migration von Betriebssystemen bedarf es erwartungsgemäß weiterer Module: die ACMP Pro-Version und das OS-Deployment Programm "ACK". Die beiden Programme ACK und ACMP sind miteinander verknüpft, so dass eine Installation eines Betriebssystems über ACMP angestoßen und von ACK durchgeführt wird. Die komplette Vorbereitung der Migration und die Definition einer Softwarequeue an sich werden jedoch in der Oberfläche von ACK durchgeführt.

Welche Computer für die Migration gerüstet sind und welche nicht, ermittelt der Administrator mit einem im ACMP Inventory vorgefertigten Report, dem so genannten "Advanced Windows 7 Report". Dank der Verwendung von Ampelfarben erklärt sich diese Untersuchung von allein und weist zudem aus, welche Komponente eine Voraussetzung erfüllt oder eben nicht.

Zur Ermittlung der Hardware-Umgebung bietet Aagon ACMP einen speziellen Client, der sich nach der Erfassung der Hard- und Softwaredaten automatisch, ohne eine Spur zu hinterlassen, wieder vom System entfernt. Für den eigentlichen Migrationsvorgang ist der volle ACMP-Client auf jedem PC erforderlich, da über diesen die Sicherung der Benutzereinstellungen erfolgt.

Neben der Prüfung und Aufrüstung von Hardware geht es an die Vorbereitung zur Softwareverteilung. Hierzu ist wieder ein Inventory-Bericht von ACMP die Grundlage um festzustellen, welche Applikationen im Unternehmen überhaupt eingesetzt werden. Ist eine Anpassung für Windows 7 erforderlich, so werden die Pakete mit Hilfe von ACMP neu paketiert oder liegen bereits vom Hersteller als MSI-Paket vor.

Die benutzerspezifischen Anpassungen, wie beispielsweise Desktop-, Drucker- oder Softwareeinstellungen, werden bei der Windows-Migration unter ACMP nicht mit einem eigens dafür vorgehaltenen Sicherungsprogramm gespeichert. Die Übertragung von Dateien und Einstellungen wird in einer Kombination des in ACMP integrierten Microsoft Migrations-Tools und den individuellen Skript-Kommandos "Client Commands" realisiert. Bei den

Produkt
Client-Management-Suite
mit Windows 7-Unterstützung.

Hersteller
Aagon
www.aagon.de

Preis
In dieser Mindestkonfiguration liegt der Listenpreis je Client bei Abnahme von 500 Lizenzen bei 50,08 Euro. In der ACMP-Suite Variante, die um das Lizenzmanagement (SWdetective) und das Sicherheitsmanagement (SecurityDetective) erweitert ist, liegt der Preis bei 53,83 Euro je Client.

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

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

Installation/Bedienung	9
Funktionsumfang	7
Reporting für Windows 7	8
Übernahme von Einstellungen	6
Migrations-Durchführung	10
Gesamtbewertung	**8**

Aagon ACK 4.3 / ACMP Pro 3.6

Client Commands handelt es sich um eine sehr einfach zu erlernende Skriptsprache, die in einem dafür entwickelten Editor durch Drag and Drop-Kommandos zusammengestellt wird. Die Einfachheit der Skriptsprache darf jedoch nicht darüber hinwegtäuschen, dass die Speicherorte der gewünschten Einstellungen dem Administrator bekannt sein müssen.

Für eine Automatisierung von Vorgängen bieten sich in ACMP die so genannten "Container" an, eine dynamische Zusammenstellung von Objekten – im Falle der Migration handelt es sich um Computer. Taucht ein PC beispielsweise mit den Eigenschaften "Betriebssystem Windows 7" und "kein Adobe Acrobat Reader installiert" in einem Container auf, so kann darauf ein Regelwerk wie "Installiere Acrobat Reader im Silent-Modus und übermittle Registry-Key zur Bestätigung der Lizenzvereinbarungen" vollautomatisch aktiviert werden. Alternativ können zuvor festgelegte Softwarepakete direkt mit dem Migrationsvorgang fest verbunden werden.

Frontrange enteo

Frontrange enteo, das einst unter dem Namen "Netinstall" vertrieben wurde, bietet sich ebenfalls für die Migration von Windows XP nach Windows 7 an. Aus dem umfangreichen Portfolio des Herstellers werden dazu das Inventarisierungsmodul "Discovery", die Betriebssystem-Installation "OSD", die Softwareverteilungs- und Paketierungssoftware "Netinstall" und das "LiveManage" zur Sicherung und Wiederherstellung von Benutzereinstellungen und Daten benötigt.

Für das Vorbereiten der Migration sowie das Berechnen der Updatekosten bietet enteo einen integrierten Assistenten. Mit Hilfe der so erstellten Vorlagen und der Berücksichtigung von Zeiten und Kosten für die jeweiligen Hardwarekomponenten wird dann ein Bericht für alle inventarisierten Client-PCs erstellt, in dem die Clients nach ihrem Erfüllungsstatus der Hardwarevoraussetzungen gruppiert werden. Anhand dieses Berichts wird ausgewertet, welche Clients die Voraussetzungen erfüllen, welche ausgetauscht werden müssen und welche nach Aufrüstung von Hardwarekomponenten die Voraussetzungen erfüllen. Daraus lassen sich Zeitaufwand und Kosten ableiten.

Bild 3: Mit einer Migrationskosten-Berechnung in Frontrange enteo gewinnt der Administrator ein wichtiges Gespür dafür, welche Kosten auf das Unternehmen zukommen

Im Fall einer festen Liste von Anwendungen und Windows-Optionen lassen sich die Anwendungseinstellungen bekannter Applikationen etwa von Adobe, Microsoft oder Mozilla mit "LiveManage" übernehmen. Das Gleiche gilt für Windows-Optionen wie die Explorer-Einstellungen oder das Desktop-Hintergrundbild. Nicht in der Auflistung genannte Programme lassen sich über eigene Datei- und Registrierungsregeln ebenfalls übernehmen.

Der Import, die Paketierung und Zuweisung der passenden Treiber zu den einzelnen Geräten ist stets eine große Herausforderung, nicht nur im Falle einer Migration. Das integrierte Treiber-Repository von enteo vereinfacht diese Aufgabe im Vergleich zu anderen Lösungen. Neue Treiber werden dem Repository einfach von der Treiber-CD oder über eine automatische Erkennung auf einem bereits eingerichteten PC hinzugefügt. Die Treiber stehen danach unternehmensweit fertig vorbereitet für jede Installation zur Verfügung und werden von enteo dynamisch

Produkt
Client-Management-Suite mit Windows 7-Unterstützung.

Hersteller
Frontrange
www.frontrange.de

Preis
Der Listenpreis aller genannten Module und einer Fernwartungssoftware liegt bei 54,81 Euro je Client bei Abnahme von 500 Lizenzen.

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

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

Installation/Bedienung	8
Funktionsumfang	8
Reporting für Windows 7	10
Übernahme von Einstellungen	9
Migrations-Durchführung	10
Gesamtbewertung	**9**

Frontrange enteo v6 SR2

oder auf Basis von Regelwerken zugewiesen. Regelwerke sind erst dann erforderlich, falls es zu Treiberkonflikten kommt – ansonsten werden die Treiber in der Baumstruktur der Software unter "Manage Users & Computers" sehr weit oben eingehängt und Windows ermittelt selbstständig die benötigten Treiber.

Über die dynamische Zuordnung bietet auch enteo, wie die anderen betrachteten Programme, die Möglichkeit, Software-Installationen und Einstellungen vollautomatisiert durchführen zu lassen. Trotz diesem nach einem "blassen Standard" klingenden Vorgang erlaubt enteo die Einrichtung möglichst individueller Umgebungen.

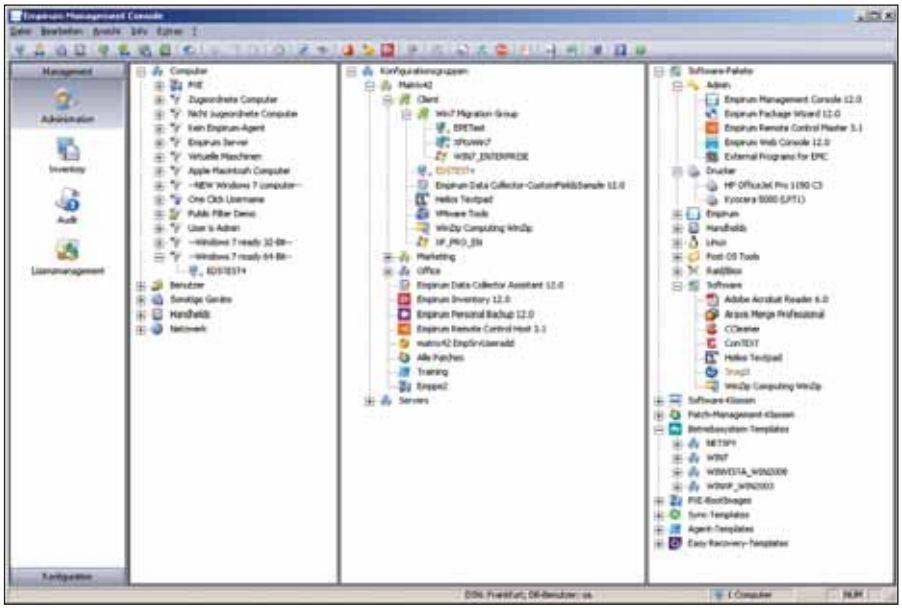


Bild 4: Nach der Migration mit Matrix42 Empirum wandern umgestellte PCs automatisch gemäß den Filterkriterien in Gruppen, über die weitere Installationen oder auch Benachrichtigungen angesteuert werden können

Matrix42 Empirum

Im April 2009 fusionierten die Karlsruher Update4u Software AG und die Neu-Isenburger Matrix42 AG und firmieren seither unter dem Namen Matrix42 AG. Dank dieser Firmenehe verfügt Matrix42 nicht nur über eine Systems-Management-Software, sondern auch über ein umgebendes Service Management. Sind beide Management-Programme gemeinsam im Einsatz, ist die Bestellung eines "Windows 7 Migrations-Auftrags" über einen webbasierten "Self Service Catalog" mit Abbildung eines Genehmigungsvorgangs und der Verrechnung der resultierenden Kosten realisierbar.

Aber auch ohne den so genannten "Service Store" von Matrix42 ist eine automatisierte Migration mit den Matrix42 Programmen Inventory, Personal Backup, Software Management und OS Installer möglich. Die Matrix42 Empirum "Windows 7 Migration Suite" mit der Fernwartung Remote Control und dem Disaster-Recovery Tool "Easy Recovery" liegt bei 65,45 EUR je Client.

Bei der Suche nach nicht Windows-7-fähiger Hardware wird der Administrator in der Empirum Management Console (EMC) durch inventargestützte Filter und drill-down-fähige Reports unterstützt. Matrix42 differenziert in diesen Filtern nach 32- und 64-Bit Systemen. Eine Anpassung der Filterkriterien ist mit Bordmitteln möglich. Empirum bietet eine besondere Hilfe bei der Feststellung, welches die wohl wichtigsten Applikationen im Unternehmen sind. Hinter "Application Usage Tracking", kurz AUT, verbirgt sich ein Tool, das die Häufigkeit und Dauer der Verwendung von Programmen auf den Client-Computern auf Wunsch protokolliert.

Benötigte Treiber lassen sich bei Empirum über verschiedene Wege ermitteln. Werden die Computer schon vorher über Empirum verwaltet, so sind die Hardware-Merkmale wie Hersteller- oder Geräte-ID bereits bekannt. Über den Update-Service vom FTP-Server von Matrix42 können diese Treiber entweder automatisch aktualisiert werden oder über die Installations-Ordner mit den INF-Dateien manuell integriert werden. Bisher nicht verwaltete Geräte werden über PXE mit einem PXE-Spy-Image versorgt und die erkannte Hardware protokolliert.

Benutzereinstellungen und Dateien, die nach der Migration auf dem neu installierten PC zur Verfügung stehen sollen, werden mit Hilfe des "Personal Backups" auf einem Server zwischengespeichert. Wie Personal Backup welche Daten sichern soll, lässt sich für unterschiedliche Backup-Jobs einzeln festlegen. Für bekannte Programme wie Microsoft Office, Firefox oder Adobe Acrobat, aber auch für weniger verbreitete Programme sind Vorlagen enthalten. Wie Applikationseinstellungen werden auch Bildschirmhintergründe, Druckerverknüpfungen oder ODBC-Einstellungen gesichert. Das Einbinden eigener Registry- oder Datei-Einträge, das Aufrufen von Skriptjobs vor oder nach Erstellung der Sicherung oder nach deren Wiederherstellung eröffnen ein sehr breites Einsatzfeld.

Im Gegensatz zu den anderen Programmen startet Matrix42 zur Vorbereitung der Migration zunächst einen Client auf Linux-Basis, das so genannte "Empirum Preboot Environment" (EPE). EPE übernimmt die Vorbereitung der Migration wie das Kopieren der Installationsdateien, die Hardware-Erkennung, die Übermittlung der benötigten Treiber und die Einrichtung der Service Partition. Anschließend startet das so kopierte WinPE die eigentliche Installation. Neu in der aktuellen Version "Patch 2" ist die Fähigkeit, vorhandene Datenpartitionen zu er-

halten, sofern die zuvor von Windows XP verwendete Systempartition mindestens 25 GByte groß war.

Nachdem der Computer unter Windows 7 neu installiert wurde, beginnen die Software-Installation und die Wiederherstellung des Personal Backups. Die dynamischen Filter in Empirum bieten sich für vollautomatisierte Installationsszenarien an, in denen gemäß Kriterien unterschiedliche Pakete eingerichtet werden. PCs mit mehr als 8 GByte Arbeitsspeicher lassen sich so mit anderen Softwarepaketen versorgen als PCs mit nur 2 GByte RAM. Die Filter bieten darüber hinaus Zusatzfunktionen, wie beispielsweise das Anstoßen eines E-Mail-Versands. So könnte sich der Administrator für jedes migrierte System über seinen Blackberry informieren lassen.

Fazit

Alle vier System-Management-Lösungen eignen sich für die Migration von XP auf Windows 7. Die Betrachtung offenbart eines ganz deutlich: Der Erfolg einer Migration liegt in erster Linie an einer guten Vorarbeit. Ohne eine halbwegs standardisierte Arbeitsumgebung wird das Umstellen ein schwierigeres Unterfangen. Wer noch keinen genauen Überblick über die Beschaffenheit der IT-Infrastruktur besitzt, wird zunächst mit der Inventarisierung der PC-Systeme und deren Software beginnen müssen. Auch diese Aufgabe meistern alle vier Test-Kandidaten über das Setzen entsprechender Filter. Bei der Frage, welche Software in welchem Umfang genutzt wird, ist Matrix42 Empirum den Konkurrenten mit dem "Application Usage Tracking" einen Schritt voraus.

Die Berechnung der Migrationskosten indes wurde bei enteo von Frontrange dank eines entsprechenden Assistenten bestens gelöst – auch wenn eine solche Kalkulation sicherlich eher einen rechnerischen Schätzwert ergibt, denn einen auf den Cent genauen Preis. Alle Programme übernehmen individuelle Benutzerdaten auf Wunsch auf den neuen PC. Welche Einstellungen tatsächlich mitgenommen werden sollen, gilt es im Zuge eines Projekts genau zu ermitteln. Sobald es um spezielle Einstellungen geht, die in INI-Dateien oder der Registry gesichert werden, ist in jedem Fall Handarbeit gefragt.

Im Sinne eines guten Gelingens empfehlen sich darüber hinaus das rechtzeitige Informieren der Benutzer und das Anbieten von Schulungsmaßnahmen kurz vor der Umstellung. Kommt neben dem Systems-Management auch eine Service-Management-Lösung zum Einsatz, können Benutzer oder Abteilungsleiter sogar den Migrationszeitpunkt selbst festlegen und haben die resultierenden Kosten der Umstellung im Überblick. *(dr)*

Produkt
Client-Management-Suite mit Windows 7-Unterstützung.

Hersteller
Matrix42
www.matrix42.de

Preis
Der Preis je Client-Computer in dieser Zusammenstellung liegt bei Abnahme von 500 Lizenzen bei einem Listenpreis von 49,27 Euro.

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

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

Installation/Bedienung	8
Funktionsumfang	9
Reporting für Windows 7	9
Übernahme von Einstellungen	10
Migrations-Durchführung	10
Gesamtbewertung	**9,2**

Matrix42 Empirum V12

Im Test: Shavlik NetChk Protect 7.1

Mehr als nur Flickschusterei

von Jürgen Heyer

Ein aktueller Patchstand auf allen PCs und Servern im Unternehmen ist ein unverzichtbarer Schutz gegen die ständigen Wurmattacken und Hackerangriffe. Mit NetChk Protect gehört Shavlik seit Jahren zu den führenden Anbietern für Patchwerkzeuge und verspricht mit der neuen Version 7 noch mehr Flexibilität im Einsatz. So deckt das Programm auch die Funktionen Antivirus sowie Antispy ab und versucht sich zudem beim Asset Management. IT-Administrator hat das Gesamtpaket einmal genau unter die Lupe genommen.

Die Kernkompetenz von Shavlik liegt schon seit Jahren beim Patchmanagement im Windows-Umfeld. Das kommt nicht von ungefähr, denn Shavlik war maßgeblich an der Entwicklung der in Windows integrierten Updateprozesse beteiligt, so dass umfassendes Knowhow vorhanden ist. Mit seinem Produkt NetChk Protect 7.1 (NCP) verfolgt Shavlik mittlerweile mehrere Strategien. So will der Hersteller deutlich mehr Komfort, Umfang und Flexibilität beim Patchen bieten als Microsoft mit seinem kostenlosen WSUS. Außerdem hat Shavlik damit begonnen, weitere aus Client-Sicht wichtige Funktionen zu integrieren, mit dem Ziel, dem Administrator die Arbeit zu erleichtern.

Bild 1: Die Quickstart-Seite erleichtert Assistenten-gesteuert den Einstieg in NetChk Protect

Mit NCP soll der Administrator nur ein Werkzeug und eine zentrale Management-Konsole bedienen müssen, um zu patchen, Viren und Spyware fernzuhalten sowie die Ausstattung der Clients zu inventarisieren. Ein zusätzlicher Vorteil ist, dass statt mehrerer Agenten auf den Endsystemen nur einer notwendig ist, wobei das Patchen sowie das Asset Management alternativ auch ohne Agenten auskommen.

Reibungslose Installation

Die Einrichtung von NCP bereitet keinerlei Probleme. Auch wenn die Oberfläche nach wie vor nicht in Deutsch, sondern nur in Englisch verfügbar ist, klappt die Einrichtung auf einem deutschen Windows 2008 Server (64 Bit) auf Anhieb. Erfreulich ist, dass die Setup-Routine alle Systemvoraussetzungen prüft und fehlende Komponenten mitinstalliert sowie konfiguriert. Dazu gehört auch ein MS-SQL Server 2008 Express, sofern nicht ein bereits vorhandener Datenbankserver angegeben wird. Zudem legt NCP mit der Installation einige Standard-Profile an, um später bei der ersten Benutzung ohne große Vorarbeiten die wichtigsten Analysen durchführen zu können.

Beim ersten Start der Konsole fragt NCP noch einige Einstellungen ab, wie die Daten eventuell verwendeter Proxyserver, einen Standardbenutzer mit Pass-

Systemvoraussetzungen

Leistungsfähige Hardware mit Windows 2003 oder 2008 Server, SQL Server 2005 oder 2008, 2 bis 4 GByte RAM für die Konsole, agentlose Clients unter Windows NT/2000/XP/Vista/2003/2008/7, Offline Images unter ESX Server ab 3.0, VirtualCenter ab 2.0, VMware Server, Workstation und Player, Clients mit Agenten unter Windows 2000 SP4/XP SP2/Vista/2003/2008/7

wort für den Clientzugriff, die IP-Adresse für das Monitoring (falls der Server mehrere Netzwerkkarten hat) sowie Angaben für eine SMTP-Mailzustellung. Abgesehen davon sind einige zusätzliche Konfigurationseinstellungen zu tätigen, allen voran die Auswahl der Sprachversionen, die gepatcht werden sollen.

Weiterhin ist der Lizenzschlüssel einzuspielen, ohne den einige Optionen gesperrt sind. NCP kann auch ohne Lizenz genutzt werden, scannt dann aber nur einen sehr beschränkten Umfang an Microsoft-Produkten. Neben der hier vorgestellten Vollversion gibt es noch eine so genannte Audit-Version, die zwar umfassend scannt, aber keine Verteilung erlaubt und auch keine agentenbasierten Zusatzfunktionen enthält. Sie ist rund ein Drittel günstiger.

In größeren Umgebungen oder auch bei einer Segmentierung eines Unternehmens auf verschiedene Standorte, die womöglich nur über eine langsame WAN-Verbindung kommunizieren können, bietet es sich an, nicht nur mit einem Verteilserver zu arbeiten, sondern wie von NCP unterstützt mehrere Distributions-Server aufzubauen und die Clientdownloads darauf zu verteilen.

Multifunktionale Konsole

Die gesamte Bedienung erfolgt von einer zentralen Managementkonsole aus, was sehr von Vorteil ist. Auch wenn die nach wie vor recht bunte Oberfläche der Konsole einen an sich aufgeräumten Eindruck macht, so ist die Handhabung doch etwas gewöhnungsbedürftig. Immer wieder ist der Anwender versucht, auf irgendwelche Grafiken und Übersichten zu klicken, um mehr zu erfahren, doch dahinter verbergen sich keine zusätzlichen Informationen. Aufgrund der zunehmenden Funktionalität ist die Bedienung im Laufe der Jahre immer komplexer geworden, so dass für eine effiziente Nutzung eine gewisse Einarbeitung erforderlich ist.

Auf der Startseite der Konsole befindet sich rechts ein Fenster, welches den aktuellen Datenstand von NCP anzeigt und auch über die letzten Aktualisierungen berichtet. Das ist wichtig, um zu erkennen, ob die Kommunikation mit den Servern von Shavlik klappt. Die Steuerung erfolgt in erster Linie über eine Fensterleiste mit mehreren Registern auf der linken Seite der Konsole, um zwischen den verschiedenen Ansichten umzuschalten. Bereits bei den ersten Arbeitsschritten halten wir es unbedingt für erforderlich, sich Gedanken über notwendige Gruppierungen zu machen, um festzulegen, welche Clients in welchem Umfang durchsucht und aktualisiert werden sollen. Die Anlage von Maschinengruppen ist in der Regel auch die erste Arbeit bei der Einführung.

Für die Umsetzung der Gruppierung beinhaltet NCP eine fast schon erschlagende Vielzahl an Filter- und Sortierkriterien. So kann ein Administrator das gesamte Netzwerk oder auch nur eine Domäne durchsuchen sowie die Namen aus einer Datei importieren. Weiterhin kann er das Active Directory durchforsten oder einen IP-Bereich vorgeben. Eine Auswahl nach diesen Kriterien kann wiederum nach Servern, Arbeitsstationen, Domänencontrollern, SQL-, IIS-, Einwahl- und Print-Servern gefiltert werden. Zusätzlich lassen sich Gruppen verschachteln. Damit dürfte es kaum Konstellationen geben, die sich mit NCP nicht gruppieren lassen. Zudem ist es ein Leichtes, beispielsweise sowohl anhand der Unternehmensstruktur als auch nach Funktionen zu gliedern und zugleich aus allen Bereichen einige Piloten festzulegen, auf denen die Patches zuerst eingespielt werden.

Sind die Gruppen festgelegt, besteht die nächste Aufgabe in der Anlage von "Patch Scan Templates", also Profilen zur Patchanalyse. Zwei Profile sind hier bereits vorgegeben: Der "Security Patch Scan" sucht nur nach sicherheitskritischen Patches, "WUScan" ermittelt darüber hinaus auch die nicht sicherheitskritischen Patches. Für einen grundlegenden Scan sind diese Profile durchaus geeignet, für eine sinnvolle und effiziente Nutzung ist es allerdings sehr ratsam, sich zusätzlich eigene Tem-

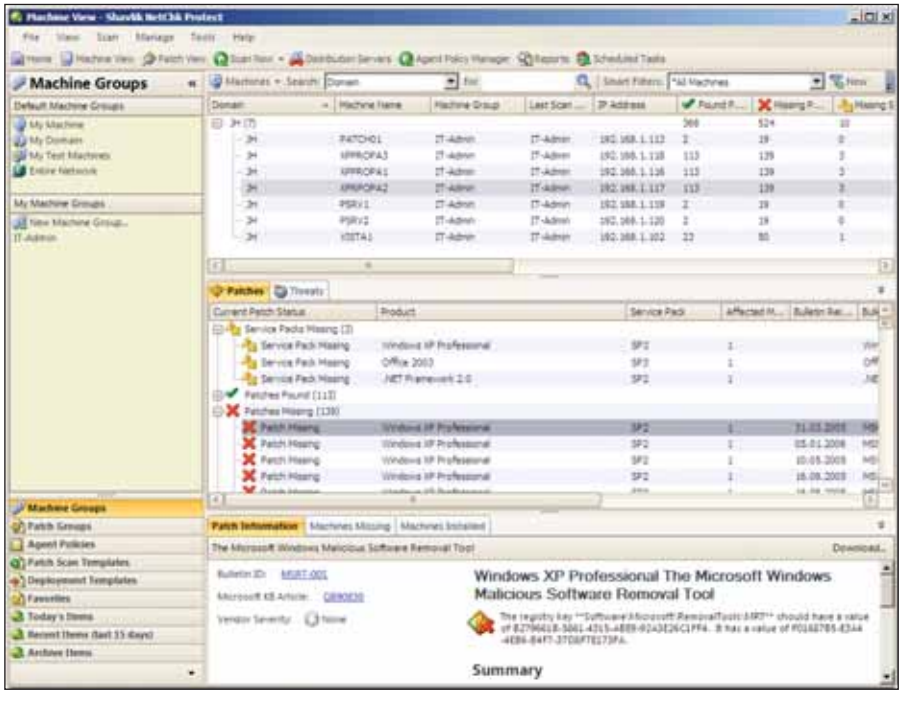


Bild 2: Sehr übersichtlich ist die Anzeige des Patchstandes für einen bestimmten Client, da sowohl die fehlenden als auch die installierten Updates aufgeführt sind

plates mit individuell passenden Parametern zu definieren.

Angesichts der Vielzahl an unterstützten Programmen, die bei der Definition eines Profils angezeigt werden, wird schnell ersichtlich, dass NCP weit mehr als Microsofts WSUS patchen kann. So lassen sich unter anderem auch die Produkte von Adobe, Citrix, Blackberry, Firefox, Google, Realplayer und Skype aktualisieren. Die komplette Übersicht der wirklich umfangreichen Liste ist bei Shavlik einsehbar. Bei der Definition eines Scanprofils lassen sich nun nur einzelne oder auch alle Produkte aufnehmen und dann wieder nach Typ (unter anderem Sicherheitspatches und Tools) sowie Bedrohungsgrad (kritisch, hoch, mittel oder niedrig) filtern.

Die Verteilung erfolgt ebenfalls über Profile, wobei der Administrator den Ablauf sehr granular steuern kann. Dies umfasst beispielsweise die Downloadgeschwindigkeit, aber auch, ob vorher ein SQL-Server oder der IIS heruntergefahren werden soll. Optional können Clients auch vor einer Verteilung gebootet werden. Weiterhin unterstützt NCP die Definition von Abhängigkeiten und möglichen Verzögerungen, wenn ein Anwender angemeldet ist, damit dieser seine Arbeit beenden kann.

Überzeugt hat uns der sehr individuell einstellbare Scheduler. Aufträge können einmalig, aber auch regelmäßig gestartet werden, weiterhin kann der Administrator vorgeben, ob Scanlauf und Patchinstallation zeitlich getrennt oder nacheinander erfolgen sollen und ob ein anschließender Reboot sofort, zu einem bestimmten Datum und/oder Zeit erfolgen soll und ob ein eventuell angemeldeter Benutzer vorher informiert wird, damit dieser den Neustart verschieben oder gar abbrechen kann. Von Vorteil ist, dass sich alle bereits definierten Profile einfach kopieren lassen, um ähnliche Profile zu bilden und dabei etablierte Einstellungen komfortabel zu übernehmen.

Übrigens ist es bei NCP kein Problem, bei Bedarf auch mit mehreren Konsolen zu arbeiten, die beispielsweise bei einem größeren Unternehmen auf unterschiedliche Örtlichkeiten verteilt sind und für die Betreuung der Clients in den jeweiligen Bereichen verwendet werden. Das beschleunigt die Prozesse, da sich unabhängig von verschiedenen Distributionsservern auch die Scanperformance verbessert, wenn sich so vermeiden lässt, dass über eine langsame Anbindung gearbeitet werden muss. Zusätzliche Konsolen sind allerdings kostenpflichtig zu lizenzieren, während die Anzahl der Distributionsserver keine Rolle spielt.

Einstieg ins Asset Management

Eine ganz neue Funktion in der aktuellen Version 7.1 ist das Asset Management, bei dem NCP die installierte Software sowie die vorhandene Hardware inventarisiert. Ähnlich wie bei den Patchprofilen ist auch für die Inventarisierung ein Profil mit den gewünschten Informationen (BIOS-Version, Netzwerk-, Prozessor- oder Plattendaten und installierte Software) zu definieren. Ein Scanlauf sowie einige Auswertungen zeigen allerdings, dass diese Funktion hinsichtlich der weiteren Verarbeitung noch ausbaufähig ist, denn die gewonnenen Informationen werden kaum aufbereitet. So kann der Administrator zwar die jeweilige Ausstattung eines Systems betrachten und gesammelte Reports erstellen, weiterführende Funktionen wie eine Lizenzverwaltung sind aber nicht integriert. Auch lassen sich zu einzelnen Assets keine zusätzlichen Informationen hinterlegen.

Nachteilig ist auch, dass alle Anzeigen stets aus Clientsicht erfolgen, also, welche Komponenten auf einem Client installiert sind. Es fehlt aber die Möglichkeit, aus Komponentensicht abzufragen, also, welches Ausstattungsmerkmal, wie eine bestimmte Software oder eine bestimmte CPU, Speicherausstattung und so weiter, auf welchen Clients zu finden ist. Hier besteht noch ein deutliches Optimierungspotential. Beim Patchmanagement sind solche Auswertungen übrigens selbstverständlich möglich: Der Administrator kann nachsehen, welche Updates auf einem Client fehlen, aber ebenso, welcher Patch auf wie vielen beziehungsweise welchen Clients fehlt.

Virtuelle Maschinen offline patchen

Eingangs wurden bereits die umfangreichen Gruppierungsmöglichkeiten für die

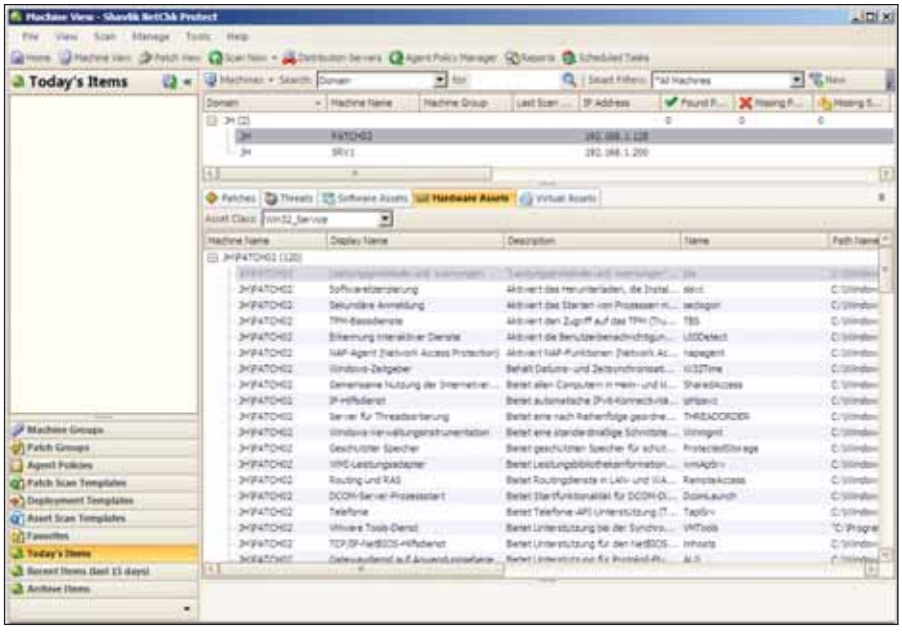


Bild 3: Das Asset Management ist noch auf reine Abfragen beschränkt, die anschließend in Listenform dargestellt werden

zu patchenden Systeme beschrieben, zu denen noch ein besonderes Feature hinzukommt. So verfügt NCP über eine wirklich beeindruckende, umfassende VMware-Unterstützung, denn in eine Gruppe können auch ganze VMware-ESX-Server sowie einzelne virtuelle Maschinen von einem ESX-Server oder auch von einer VMware Workstation-Installation mit aufgenommen werden. Für den Zugriff über einen ESX-Server muss der Administrator entsprechende Anmeldedaten hinterlegen und bei Workstation-Images den genauen Pfad oder auch einen zu durchsuchenden Ordner vorgeben. NCP durchsucht nun den ESX-Server oder auch den angegebenen Pfad nach existierenden VMs und patcht diese. Ein Administrator muss also gar nicht jede VM genau vorgeben, was auch den Vorteil hat, dass bei häufigen Änderungen immer alle gerade existenten virtuellen Maschinen erfasst werden.

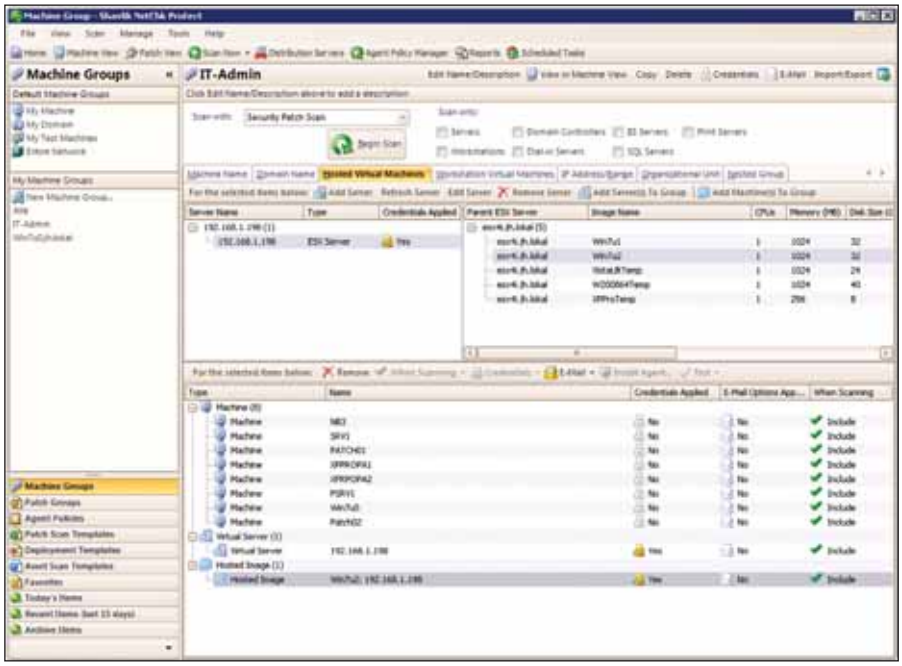


Bild 4: NCP kann alle virtuellen Maschinen eines VMware ESX-Servers einlesen und auch offline, also in ausgeschaltetem Zustand, scannen

Eine Besonderheit ist zudem, dass NCP auch ausgeschaltete virtuelle Images patchen kann. Dazu mountet das Tool die virtuellen Maschinen nacheinander, scannt diese und verteilt auf Wunsch auch die Patches. Letzteres bedeutet, dass es die Installationsdateien in das Image kopiert. Die eigentliche Installa-

tion erfolgt dann, wenn die VM das nächste Mal gestartet wird.

Im Test aktualisierten wir ein Image umfassend, insgesamt 96 Updates mit über 800 MByte Gesamtumfang kopierte NCP offline in das Image, um diese nach Starten der VM automatisch zu installieren. In diesem Zuge fiel uns allerdings ein kleinerer Fehler auf. So funktioniert ein Refresh der Anzeige der VMs auf einem in ein Scan-Profil aufgenommenen ESX-Server nicht. Werden auf dem ESX-Server virtuelle Maschinen gelöscht oder ergänzt, muss dieser aus dem Profil entfernt und wieder aufgenommen werden. Der Hersteller will diese Funktion nochmals eingehend prüfen.

Frühzeitige Betriebssystemunterstützung

Zum Testzeitpunkt im Oktober 2009 stand Windows 7 noch nicht in den deutschen Regalen. In NCP ist die Unterstützung aber bereits komplett integriert. Das Gleiche gilt für Windows Server 2008 R2. Auch wenn Unternehmen diese ganz neuen Versionen nicht sofort produktiv einsetzen, ist die frühzeitige Unterstützung dennoch sehr sinnvoll, damit die Patchfunktion bei der Einführung eines neuen Betriebssystems gleich mit evaluiert werden kann. Shavlik ist verständlicherweise auch aus eigenem Interesse an einer sehr zeitnahen Unterstützung interessiert, da sonst einige Kunden gezwungen sein könnten, erst einmal auf Microsofts WSUS zurückzugreifen.

Im Laufe des Tests versuchten wir, verschiedene Clients unter Windows XP Professional, Windows Vista 64 Bit, Windows 7 64 Bit und Windows Server 2008 64 Bit zu patchen, wobei keinerlei Probleme auftraten. Ein Vergleich der Scanergebnisse mit WSUS bei der Suche nach kritischen Patches ergab auch eine gute Übereinstimmung. Eine Suche nach allen Patches erweist sich letztendlich als nicht exakt vergleichbar, da

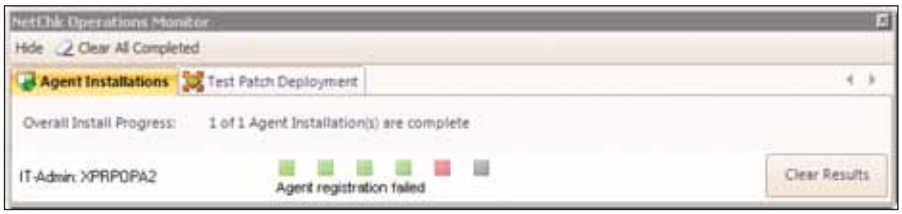


Bild 5: Falls eine Agenteninstallation fehlschlägt, gibt NCP nicht immer einen Grund aus, der eine Fehlersuche erleichtern würde

NCP deutlich mehr installierte Produkte aktualisiert als WSUS. Hier wird der Mehrwert von NCP deutlich sichtbar.

Sofern bei einem Patch eine Deinstallationsmöglichkeit vorgesehen ist, wird diese von NCP unterstützt und kann komfortabel direkt aufgerufen werden. Ob diese Möglichkeit überhaupt besteht, zeigt das Programm übersichtlich an, so dass ein Administrator dies bereits vor einer Installation sieht. Weiterhin zeigt NCP dem Administrator an, ob ein Patch bereits auf die Konsole heruntergeladen wurde oder nicht. Diesbezüglich gibt es zudem die Möglichkeit, entweder in Stundenabständen auf neu erschienene Patches zu prüfen und diese sofort herunterzuladen oder erst dann, wenn ein Scanlauf stattfindet und ein Patch tatsächlich benötigt wird.

Ein weiterer Vorteil ist, dass ein Administrator mit NCP jederzeit in der Lage ist, alle Maschinen im Netz gezielt zu scannen und zu aktualisieren. Von der Konsole aus kann er alle Systeme erreichen und muss nicht warten, bis sich die Systeme wie bei WSUS von sich aus melden (beziehungsweise dieses über Remote-Aufrufe forciert wird).

Zusätzlich zur breiten Produktunterstützung ist in NCP ein so genannter Custom Patch Editor enthalten, mit dem sich individuelle Patches konfigurieren lassen. Das erfordert allerdings umfassende Kenntnisse in der XML-Programmierung, um die notwendigen Prüfungen umzusetzen. Auf diesem Wege lassen sich aber auch beliebige Produkte mit aufnehmen, wenn deren Hersteller von sich aus passende XML-Dateien liefern.

Neben seiner Aufgabe als Patchtool kann NCP in gewissen Grenzen auch zur Softwareverteilung für die unterstützten Produkte genutzt werden, also unter anderem für Adobe Reader, Mozilla Firefox, Flash, Quicktime und Shockwave Player sowie alle .NET-Framework-Versionen. Vorsicht ist dahingehend geboten, weil die notwendige Einstellung unscheinbar und ein wenig versteckt ist, aber immense Auswirkungen hat, wenn ein Scanlauf mit einer anschließenden automatischen Patchverteilung gekoppelt ist. Dann werden womöglich auf Hunderten von Clients alle genannten Produkte (und noch einige mehr) nicht nur gepatcht, sondern gegebenenfalls auch erstmals installiert.

Mehr Features per Agent

Patchen und Asset Management arbeiten agentenlos und können somit auf den Clients angewendet werden, ohne dass dort vorher etwas installiert werden muss. Darüber hinaus kommt mit NCP ein Agent mit, der die zusätzlichen Features von NCP in Form von Viren- und Spywareabwehr aktiviert, der auf Wunsch aber auch das Patchen steuert. Um den Agenten zu installieren, sind einige Voraussetzungen zu beachten, wie eine zusätzliche Freischaltung in der Firewall der Clients (TCP-Ports 139 und 445), und dass der Remoteregistrierungsdienst sowie der Serverdienst laufen müssen.

Zum Betrieb der Agenten sind im Vorfeld Agenten-Policies, also wieder entsprechende Profile zu bauen, wobei darin für das Scannen und die Patchverteilung einfach bereits vorhandene Tem-

plates eingetragen werden. Der Agent durchsucht das System per Scheduler in frei wählbaren Abständen auf Bedrohungen durch Viren, Spy- und Malware. Der Administrator hat zudem die Möglichkeit, über entsprechende Ausnahmelisten bestimmte ausführbare Programme zu erlauben, zu sperren oder aber dem Anwender den Aufruf nochmals bestätigen zu lassen. Neben der Virensuche in Intervallen kann der Administrator eine Prüfung bei Dateizugriff aktivieren und vorgeben, wie das System auf bestimmte Aktionen reagieren soll (Änderung der Explorer-Sicherheitseinstellungen oder der System Policies, Aufruf von Programmen und so weiter). Bei der Abwehr von Viren und schädlichem Code arbeitet Shavlik mit Sunbelt zusammen und hat die schnelle sowie schlanke Vipre-Engine integriert.

Im Test hinterließ der Agent allerdings einen etwas durchwachsenen Eindruck. Der Ansatz, verschiedene Funktionen auf diese Weise in einem Werkzeug zu vereinen, ist auf jeden Fall sehr interessant. Wir vermissen allerdings rund um Antivirus und Antispy entsprechende Informationen für den Administrator. Es ist von der zentralen Konsole aus nicht auf einen Blick erkennbar, welche Signaturversionen im Einsatz sind und ob alle Clients auch mit den aktuellsten Signaturen arbeiten. Der Administrator kann zwar einen Report erstellen, bekommt dann aber jede Maschine extra aufgeführt. Insgesamt vermissen wir hier bessere Möglichkeiten zur Auswertung, die gezielt auf einen Handlungsbedarf hinweisen. Besser ist die Information auf Clientseite, hier liefert der Agent genaue Informationen zu den Versionen und zum letzten Suchlauf.

Für ein erstes Reporting zeigt NCP bereits auf der Startseite eine Handvoll von Balkengrafiken zur Darstellung des allgemeinen Patchstandes an. Allerdings machen diese TOP-10-Anzeigen auf uns eher einen plakativen Eindruck, als dass sie wirklich weiterhelfen. Auch kann man nicht einfach auf solch eine Darstellung klicken, um dann weitere Detailinformationen zu erhalten. Auf jeden Fall hilfreicher ist die eigentliche Reportfunktion, die eine geschickte Auswahl und Filterung mit wenigen Mausklicks erlaubt. Mehr als 20 Reports sind dabei fest integriert, die Darstellung ist für eine Druckausgabe vorbereitet. Vorteilhaft ist, dass sich auf Wunsch ein automatisches Mailing per SMTP einrichten lässt.

Fazit

NetChk Protect überzeugt nach wie vor mit einem absolut leistungsfähigen Patchmanagement im Windows-Umfeld für das Betriebssystem selbst, für weitere Microsoft-Produkte sowie diverse weit verbreitete Programme. Die vielfältigen Funktionen erfordern allerdings eine gewisse Einarbeitung, und eine Einführung in einem Unternehmen setzt eine gezielte Planung voraus. Dabei ist NetChk Protect durch die Möglichkeit, sowohl mit mehreren Distributionsservern als auch mehreren Konsolen zu arbeiten, auch für sehr große Umgebungen geeignet.

Die Module Antivirus, Antispy sowie das ganz neue Asset Management zeigen durchaus den richtigen Weg auf, um die Anzahl der Werkzeuge, die für ein effizientes Clientmanagement erforderlich sind, sinnvoll zu reduzieren. Sie erscheinen uns aber insgesamt noch optimierungsbedürftig. Bei den Funktionen Antivirus und Antispy vermissen wir eine zentrale Statusübersicht, beim Asset Management die Möglichkeiten zur weiteren Nutzung und Verarbeitung der ermittelten Daten. Eine ganz andere Problematik bei derartig integrierten Lösungen ist natürlich die Tatsache, dass ein Unternehmen beispielsweise gerne mit NCP patchen möchte, aber einen anderen Virenscanner bevorzugt und vielleicht schon ein Werkzeug zur Softwareverteilung und Inventarisierung besitzt. Mit einem integrierten Werkzeug wird es sicher nicht einfacher, alle Kunden zufrieden zu stellen, wobei diese stets den gesamten Leistungsumfang von NCP bezahlen müssen. *(jp)*

Produkt

Programm für das Patchmanagement im Windows-Umfeld.

Hersteller

Shavlik
www.shavlik.com, www.prosoft.de (Distributor)

Preis

Shavlik unterscheidet zwischen Lizenzen für Workstations und Server, 100 WS-Lizenzen kosten 4.920 Euro, 10 Server-Lizenzen 984 Euro mit einer Konsole, eine weitere Konsole kostet 1.836 Euro, für andere Mengen gibt es Staffelpreise.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Installation/Bedienung	8
Patchfunktionalität	9
Antivirus/Antispy-Funktion	6
Asset Management	4
Dokumentation	7

Dieses Produkt eignet sich

optimal für mittlere und größere Umgebungen im Windows-Umfeld, die auch den vollen Leistungsumfang nutzen wollen. Hier kann das Programm seine Stärken voll zur Geltung bringen.

bedingt in kleineren Umgebungen, wenn nur wenige Systeme zu aktualisieren sind und sich der Betriebsaufwand für ein derart mächtiges Werkzeug nicht lohnt. Aus finanzieller Sicht erscheint uns das Werkzeug auch dann nur bedingt geeignet, wenn es nur zum Patchen genutzt werden soll.

nicht, wenn Windows-basierende Systeme eine untergeordnete Rolle spielen, da die gesamte Verwendung auf diese Betriebssystemfamilie aufsetzt.

Shavlik NetChk Protect 7.1

Im Kurztest: rootwerk Server Monitor

Bei Alarm SMS

von Sandro Lucifora

Mit dem Slogan "Server watching has never been so easy." wirbt das deutsche IT-Unternehmen rootwerk.de für sein Online-Monitoring. Das Angebot soll kleinen und mittleren Unternehmen die Möglichkeit geben, die Erreichbarkeit ihrer Serverdienste auch ohne eigene Infrastruktur zu überwachen. IT-Administrator hat sich den Web-basierten Dienst einmal genauer angesehen.

Da sich der Monitoring-Dienst im Internet befindet, kann dieser nur solche Server überwachen, die von extern erreichbar sind. Daher eignet sich ein solches Monitoring für interne Hardware nur bedingt. Eine Konfiguration der lokalen Firewall dahingehend, dass diese nur Anfragen des Monitoring-Dienstes zulässt, ist wenig praktikabel, da sich die IP-Adresse des Anbieter-Servers ändern kann.

Überwachung einrichten

Für unseren Test stand uns ein Business-Account zur Verfügung, der auf fünf zu überwachende IPs und je 15 Dienste begrenzt ist. In diesem Konto wird zwölfmal pro Stunde auf die Verfügbarkeit des jeweiligen Dienstes geprüft. Um einen neuen Server anzulegen, gaben wir wahlweise die IP oder einen öffentlich auflösbaren Hostnamen an. Der Assistent richtet die ersten Checks automatisch ein. Weitere lassen sich manuell hinzufügen. Dazu stehen bei der Art des Checks die Möglichkeiten Ping, TCP-Port, Web-Server, SMTP, Datenträger sowie Systemauslastung via SNMP zur Auswahl. Vermisst haben wir die Prüfung für einen POP3-Dienst. TCP-Port- und Web-Server-Check erlauben noch einige zusätzliche Angaben wir die Portnummer, den Antwortcode und die Reaktionszeiten für die Zustände "Warnung" und "kritisch". Der SMTP-Check erfolgt nur über eine definierte Grußfloskel zwischen den Servern. Wenn diese akzeptiert wird, ist für das rootwerk-Monitoring alles ok. Wir hätten uns eine intensivere Prüfung des SMTP-Protokolls gewünscht, die den kompletten Sende-Prozess testet.

Produkt

Web-basierter Dienst zur Online-Überwachung von Servern.

Hersteller

rootwerk
http://monitoring.rootwerk.de

Preis

Für eine IP-Adresse und maximal zwei Dienste ist der Service kostenlos. Mit Variante "Basic" lassen sich auf einer IP-Adresse für 4,19 Euro pro Monat maximal 15 Dienste überwachen. Version "Business" nimmt auf bis zu fünf IP-Adressen jeweils 15 Dienste unter die Lupe und kostet 8,39 Euro pro Monat.

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

Handhabung	8
Usability	7
Zuverlässigkeit	5
Konfigurationsaufwand	9
Kosten / Nutzen	5

rootwerk Server Monitor

Meldung an nur einen Empfänger

Wann das Überwachungstool die Verfügbarkeit eines Dienstes als kritisch melden soll, konnten wir beim Check individuell einstellen. Der Empfänger der Meldung lässt sich jedoch nur global in den Kontoeinstellungen festlegen. Neben lediglich einer E-Mail- und Jabber-Adresse ist auch Platz für eine Mobilnummer. An diese sendet der Service im Fall eines Falles eine SMS. Der Anbieter geht durch die derzeitige Globalisierung der Benachrichtigungen davon aus, dass bei einem Ausfall nur eine Person für alle Meldungen zuständig ist. Hier muss in jedem Fall nachgebessert werden, so dass sich verschiedene Empfängergruppen je Server definieren lassen.

Im Testzeitraum haben wir insgesamt vier Server mit unterschiedlichen Diensten überwacht. Im Grunde zeigte sich das System stabil, doch eine hundertprozentige Zuverlässigkeit haben wir bei einem von vier Servern nicht gehabt. Dort prüften wir den Webdienst, je ein Mal über Port 80 und 443. Beide Checks standen bis zum Testende auf "critical", obwohl der Server normal über http und https erreichbar war. Leider hat weder der Anbieter bei der Ursachensuche helfen können, noch gibt der Bericht Auskunft darüber, warum der Check auf kritisch gestellt ist. Kurios dabei war, dass der separate Verfügbarkeitsbericht keine Probleme und eine Uptime von 100 Prozent auflistete.

Fazit

Die Grundidee und die Umsetzung des Dienstes ist gut. Die Oberfläche lässt sich einfach bedienen und ist übersichtlich. Die konfigurierbaren Checks reichen für eine Grundversorgung aus, wünschenswert ist jedoch eine zeitnahe qualitative und quantitative Erweiterung. Die Tatsache, dass ein Serverstatus immer auf kritisch stand, obwohl alles in Ordnung war, lässt an der absoluten Verlässlichkeit des Angebotes momentan zweifeln. Betrachten wir ähnliche Angebote auf dem Markt, ist hier für 9 Euro im Monat durchaus noch Luft nach oben. *(ln)*

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

SAN-Hochverfügbarkeit mit Openfiler und DRBD-Cluster (1)

Immer für Dich da

von Thomas Gronenwald

Einen Hochverfügbarkeits-Cluster unter Linux zu realisieren, ist inzwischen kein Hexenwerk mehr. Der Einstieg in die Oberklasse der Verfügbarkeit lässt sich mit einfachen Mitteln umsetzen. Dank der Open Source-Projekte Openfiler, DRBD und Heartbeat lassen sich Hochverfügbarkeits-Storage-Infrastrukturen kostengünstig verwirklichen. In diesem Workshop führen wir Sie Schritt für Schritt zu einem hochverfügbaren SAN.

Im Zeitalter der Virtualisierung mit VMware ESX, XenServer oder Hyper-V ist ein "Single Point of Failure" gerade im Storage-Bereich nicht mehr tolerierbar – und ein redundant ausgelegtes SAN (Storage Area Network) somit eine Pflichtaufgabe. Jedoch ist dies in der Regel nur mit einem erheblichen finanziellen und personellen Mehraufwand möglich und für kleinere und mittelständische Unternehmen daher zumeist nicht finanzierbar.

In virtualisierten Infrastrukturen wird ein SAN in der Regel als gemeinsames Speichermedium genutzt. Nur zu oft wird hier in der Praxis aber aus verschiedenen Gründen auf die redundante Auslegung des SANs verzichtet. Meistens wird davon ausgegangen, dass das Storage bereits eine gewisse Ausfallsicherheit (RAID-Verbund) mitbringt. Wenn aber nun das Storage wegen eines technischen Defektes nicht mehr verfügbar ist, nutzt auch eine redundant ausgelegte Server-Umgebung nichts mehr, wenn auf den gemeinsamen Storage nicht mehr zugegriffen werden kann – Server, Anwendungen und Geschäftsprozesse stehen still.

Genau hier setzen die Open Source-Lösungen Openfiler [1], DRBD (Distributed Replicated Block Device) [2] und Heartbeat [3] an. Mit geringem Aufwand, einfachen Standardkomponenten und wenigen Konfigurationsschritten lässt sich so eine maßgeschneiderte HA-Storage-Infrastruktur aufbauen. Openfiler liefert dabei einen Funktionsumfang, der sonst nur von kommerziellen (und kostenintensiven) Geräten angeboten wird. Die dynamische Anpassung von iSCSI-Volumes, das LUN-Mapping für iSCSI-Snapshots als auch das Channel-Bonding zur Steigerung der Performance gehören zum standardmäßigen Funktionsumfang. So ist es auch möglich, Erweiterungen der einzelnen Datenspeicher bis zu einer Größe von 16 TByte vorzunehmen.

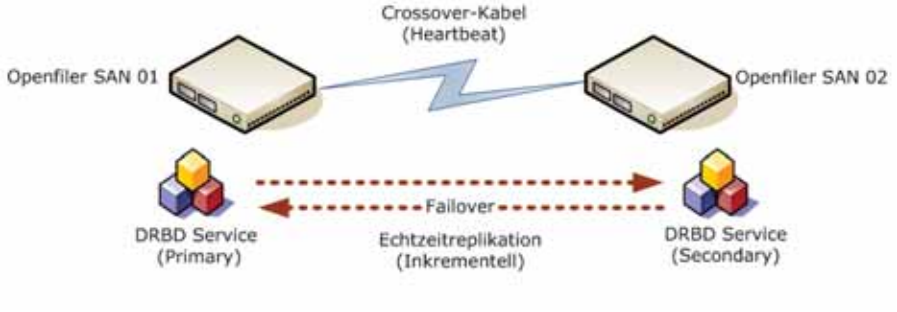


Bild 1: Schema der Funktionsweise von DRBD und Heartbeat

Die Komponenten im Detail

Openfiler basiert auf der für Storage-Anwendungen optimierten Linux Metadistribution "rPath" und steht unter der GNU General Public License Version 2 kostenfrei zur Verfügung. Das eigentliche Betriebssystem wird durch die Beschränkung auf die wesentlichen Dienste stark verschlankt. Dies ermöglicht eine Installation innerhalb von weniger als 15 Minuten und bietet zudem eine reduzierte Angriffsfläche durch den Ausschluss nicht benötigter Pakete und Dienste.

Als Grundlage nutzt die mit einem webbasierten Management ausgestattete Storage-Lösung bekannte und freie Pakete wie Samba (Dateifreigabe, CIFS), Apache (Webserver), NFS (Network Filesystem) und das iSCSI-Enterprise-Target. Zudem unterstützt Openfiler die gängigen Protokolle wie NFS, SMB/CIFS, HTTP/WebDAV und FTP. Darüber hinaus versteht sich Openfiler auch ausgezeichnet mit LDAP und dem Active Directory (im native- als auch im mixed-Mode). Openfiler kombiniert dabei diese Technologien zu einer kompakten Open Source-Storage-Komplettlösung. Mit diesem Funktionsumfang entspricht Openfiler allen Anforderungen von SAN-, NAS-, Primär- und Sekundär-Storage-Lösungen.

Die zur eigentlichen Cluster-Bildung benötigten Komponenten sind bereits in der Installationsroutine von Openfiler enthalten. Für die Bildung des Clusters werden die Pakete von DRBD und Heartbeat genutzt. Bei DRBD handelt es sich um einen Block-Device-Treiber für Linux, der

für den Aufbau von Hochverfügbarkeits-Clustern entwickelt wurde. DRBD ist dabei in der Lage, Datenblöcke über das TCP/IP-Protokoll zu transferieren – oft wird dies verglichen mit einem RAID 1 auf Netzwerkbasis.

Im Idealfall kommt für die Verbindung der einzelnen DRBD-Cluster eine dedizierte Verbindung (Heartbeat) zum Einsatz. Hier spielt es theoretisch keine Rolle, wie weit diese Systeme voneinander entfernt sind. So könnte ein System im Rechenzentrum (RZ) in Köln, das andere im RZ in Mönchengladbach stehen. Lediglich die Bandbreite sollte angemessen an die zu erwartenden Datenmengen dimensioniert werden. DRBD minimiert das Replikationsaufkommen dabei so intelligent, dass nur geänderte Blöcke repliziert werden. Dementsprechend wird unnötiger Traffic eingespart. Für die Überwachung der einzelnen Cluster-Knoten nutzen wir das Paket "Heartbeat". Dieses arbeitet im Hintergrund des DRBD-Clusters, dient zur Überwachung der Knoten und übernimmt das An-, Ab- und Umschalten der Dienste auf den jeweiligen Knoten. Zudem stellt dieser Service die gemeinsame IP-Adresse (virtuelle IP) für die Cluster-Knoten im Netzwerk zur Verfügung.

Für unseren nachfolgend dargestellten Aufbau werden unter Berücksichtigung der minimalen Systemvoraussetzungen (siehe Kasten) folgende Hardware-Komponenten genutzt:

- Zwei Systeme mit den Mindestanforderungen von Openfiler (siehe Kasten)
- Zwei Netzwerkkarten pro System
- Optimalerweise mit identisch großen Festplatten
- Openfiler 2.3 Installationsmedien (ISO), Größe: 315 MByte

Installation und erste Konfigurationsschritte

Die Installation von Openfiler ist äußerst einfach, selbsterklärend und sollte schnell erledigt sein. Openfiler unterstützt im Übrigen auch die Installation als Gast auf einem Hypervisor. Es erlaubt dabei die Installation auf Xen- und ESX-Servern. Dies sowohl auf der x86- als auch auf der x64-Architektur. Zudem stehen im Openfiler-Downloadbereich fertige virtuelle Appliances zum Download bereit. In diesem Aufbau gehen wir jedoch von einer normalen Installation auf einem Baremetal-System aus.

Bei der eigentlichen Installation können Sie zwischen einer textbasierten oder grafischen Installation wählen. Wir nutzen die grafische Variante – wobei sich die beiden Varianten nur rudimentär unterscheiden. Während der Installation müssen Sie Tastaturlayout, Hostname, Passwort, Partitionierungseinstellungen und die Konfiguration der beiden Netzwerkkarten vornehmen:

- Tastaturlayout: Für die Nutzung einer deutschen Tastatur wählen wir "German".

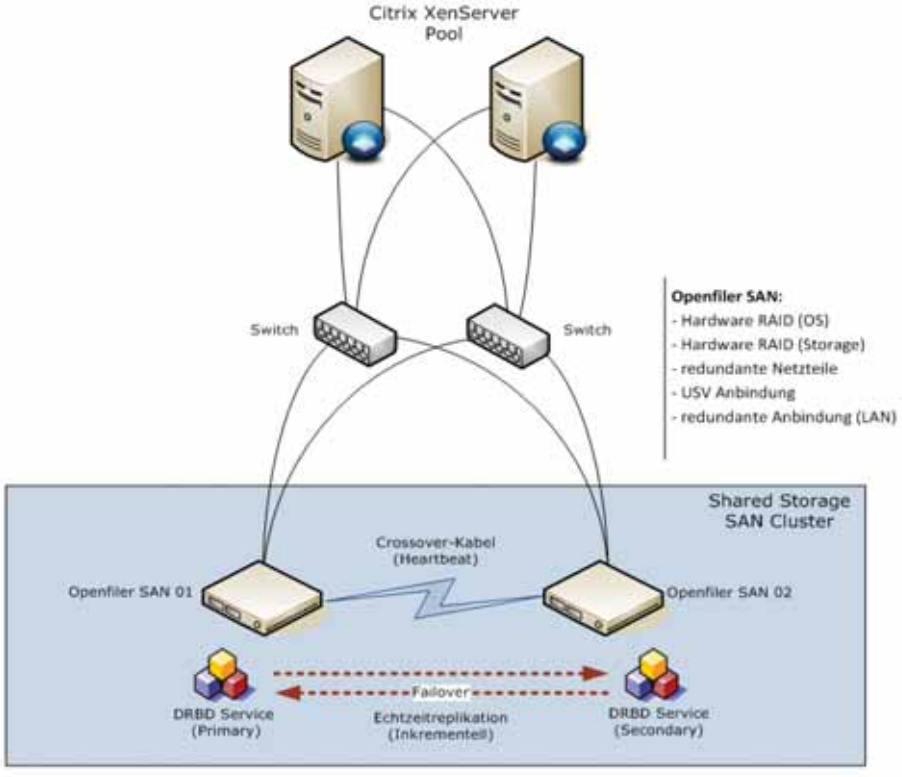


Bild 2: Unser Zielszenario als Best Practice Implementierung

Für die Installation der beiden Openfiler werden mindestens folgende Hardwareausstattungen und Systemvoraussetzungen benötigt:

- 32 Bit 1 GHz-Prozessor
- 512 MByte Arbeitsspeicher
- 512 MByte freier Speicherplatz für die Auslagerungsdatei
- 1 GByte freier Speicherplatz für das Betriebssystem
- 100-MBit-Netzwerkkarte
- Festplattenspeicher für die Datenpartition

Im Dauerbetrieb und im Unternehmensumfeld sollten Sie jedoch mindestens folgende Hardwareausstattungen und Systemvoraussetzungen nutzen, um die maximale Verfügbarkeit für Ihren Cluster zu erhalten:

- 64 Bit 1,6 GHz-Prozessor oder höher
- 1 GByte Arbeitsspeicher oder mehr
- 1 GByte freien Speicherplatz für die Auslagerungsdatei
- 2 GByte freien Speicherplatz für das Betriebssystem (OS)
- Zwei 1-GBit-Netzwerkkarten für die redundante Anbindung an ihr LAN (gegebenenfalls weitere für Channel-Bonding)
- Eine 1-GBit-Netzwerkkarte für den Heartbeat
- Festplattenspeicher für die Datenpartition
- Einen kompatiblen Hardware RAID-Controller für das Betriebssystem
- Einen kompatiblen Hardware RAID-Controller für die Daten

Des Weiteren sollten auch die Komponenten wie Netzteile und Switches redundant vorhanden sein sowie eine unterbrechungsfreie Stromversorgung (USV), um Spannungsschwankungen und Stromausfälle kompensieren zu können.

Systemvoraussetzungen

```
global {
 usage-count ask;
}

common {
 syncer { rate 100M; }
}

resource cluster_metadata {
 protocol C;
 handlers {
  pri-on-incon-degr "echo 0 > /proc/sysrq-trigger ;
   halt -f";
  pri-lost-after-sb "echo 0 > /proc/sysrq-trigger ;
   halt -f";
  local-io-error "echo 0 > /proc/sysrq-trigger ; halt -f";
 }

 startup {
  degr-wfc-timeout 120;
 }

 disk {
  on-io-error detach;
 }

 net {
  after-sb-0pri disconnect;
  after-sb-1pri disconnect;
  after-sb-2pri disconnect;
  rr-conflict disconnect;
 }

 syncer {
  al-extents 257;
 }

 on filer01.prod.zz {
  device /dev/drbd0;
  disk /dev/sda3;
  address 10.10.1.1:7788;
  meta-disk internal;
 }

 on filer02.prod.zz {
  device /dev/drbd0;
  disk /dev/sda3;
  address 10.10.1.2:7788;
  meta-disk internal;
 }
}

resource vg0drbd {
 protocol C;
 startup {
  wfc-timeout 0;
  degr-wfc-timeout 120;
 }

 disk {
  on-io-error detach;
 }

 net {
     }

 syncer {
  after "cluster_metadata";
 }

 on filer01.prod.zz {
  device /dev/drbd1;
  disk /dev/sda5;
  address 10.10.1.1:7789;
  meta-disk internal;
 }

 on filer02.prod.zz {
  device /dev/drbd1;
  disk /dev/sda5;
  address 10.10.1.2:7789;
  meta-disk internal;
 }
}
```

Listing 1: Die Datei drbd.conf nach dem Editieren

- Partitionierung: Für unsere Umgebung wählen wir eine manuelle Partitionierung mittels "Disk Druid" mit den folgenden Einstellungen: 3 GByte für die Root-Partition ("/") und 2 GByte für die Auslagerungsdatei ("swap"). Diese Partitionen erhalten keinen Eintrag in der "/etc/fstab", da später die Funktion des Heartbeats das Einbinden der Block-Devices in das Filesystem für uns übernehmen wird. Darüber hinaus 512 MByte für die Meta-Partition ("/meta") für DRBD0 sowie 2,5 GByte LVM-Datenpartition (nicht gemountet) für DRBD1. Diese Werte können Sie natürlich später in den Konfigurationsdateien Ihren eigenen Bedürfnissen anpassen.
- Hostname: Als Hostnamen verwenden wir: Filer01.prod.zz und Filer02.prod.zz.

Konfiguration der Netzwerkkarten

Jeder unserer Openfiler besitzt zwei Netzwerkkarten. Eine für die LAN-Schnittstelle und zur Administration der einzelnen Knoten (eth0) und eine für die Replikation (Heartbeat) zwischen den beiden SANs (eth1). Die Netzwerkkarte eth1 beider Systeme wird mit einem Crossover-Kabel verbunden. Folgende IP-Adressen verwenden wir für unsere Systeme:

- Filer01.prod.zz: eth0: 192.168.1.1 /24 und eth1 (Heartbeat): 10.10.1.1 /24
- Filer02.prod.zz: eth0: 192.168.1.2 /24 und eth1 (Heartbeat): 10.10.1.2 /24

Damit ist die Basiskonfiguration der Systeme abgeschlossen. Nach der erfolgreichen Installation startet Openfiler und wir können uns das erste Mal mit dem in der Installation festgelegten Benutzer "root" und dem genutzten Passwort anmelden.

Konfiguration der Systemkommunikation

Damit die Systeme miteinander kommunizieren können, müssen Sie nun die Datei */etc/hosts* anpassen. Dies funktioniert schnell und einfach mit dem Text-Editor "vim" [4,5]. Für Filer01.prod.zz:

```
root@filer01 ~# vim /etc/hosts
# Filer01.prod.zz
  127.0.0.1 filer01.prod.zz
  localhost.localdomain localhost
  10.10.1.2 filer02.prod.zz
  10.10.1.2 filer02
```

Und für Filer02.prod.zz:

```
root@filer02 ~# vim /etc/hosts
# Filer02.prod.zz
```

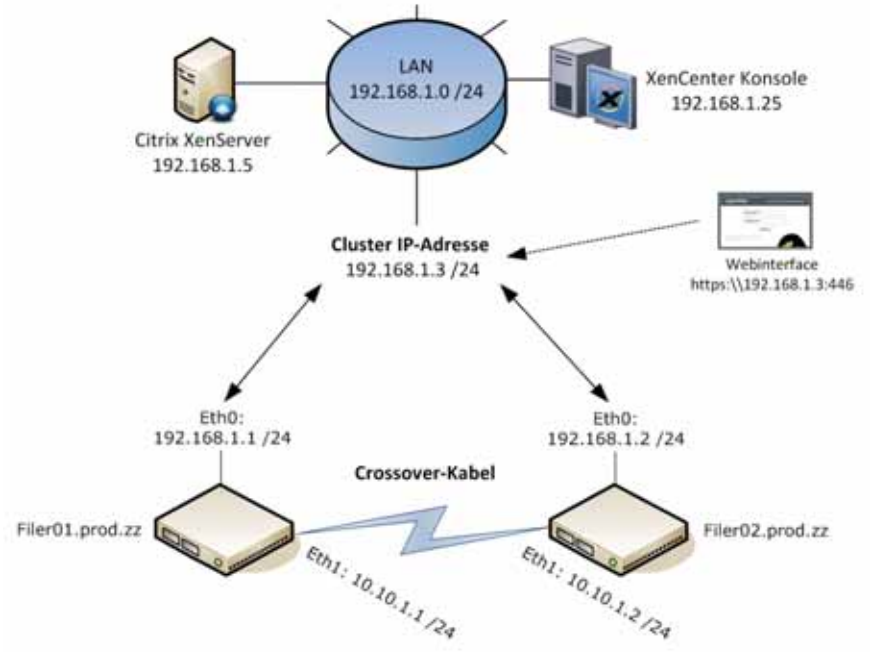


Bild 3: Die Workshop-Umgebung im Detail

Fast Lane, die Spezialisten für:

Training & Consulting rund um sichere IT-Infrastrukturen

Content Security • Endpoint Security • Firewalls • Security Management • VoIP Security • Virtual Private Networks • Wireless Security

Erfahren Sie mehr unter **www.flane.de** oder rufen Sie uns an: **+49 (0)40 25334610.**

Die nächsten Kurstermine:

Anti-Hacking Workshop (HACK)
22.02.10 Frankfurt, 15.03.10 Berlin, 22.03.10 München
Sicherheitsrelevante Problematiken bei Webapplikationen (EHACK)
22.02.10 Frankfurt, 29.03.10 Frankfurt 10.05.10 München
Voice Anti-Hacking Workshop (VHACK)
15.02.10 Frankfurt, 01.03.10 Frankfurt, 07.04.10 München
WLAN Anti-Hacking Workshop (WHACK)
08.03.10 Frankfurt, 29.03.10 Hamburg, 10.05.10 München
Malware Inside (MWI)
25.02.10 Frankfurt, 08.04.10 Frankfurt, 06.05.10 München
Check Point CCSA & CCSE Power Workshop (CPPW)
01.02.10 Hamburg, 22.02.10 Hamburg, 29.03.10 München
Securing Your Web with Cisco IronPort S-Series (SYW)
04.02.10 Hamburg, 25.02.10 Frankfurt, 29.03.10 Frankfurt
Securing Your Email with Cisco IronPort C-Series (SYEPW)
01.02.10 Hamburg, 22.02.10 Frankfurt, 29.03.10 Berlin

Implementing Cisco IOS Network Security (IINS)
01.02.10 Frankfurt, 15.02.10 Berlin, 08.03.10 Hamburg
Securing Networks with Cisco Routers & Switches (SNRS)
01.02.10 Frankfurt, 08.02.10 Düsseldorf, 15.02.10 Hamburg
Securing Networks with ASA Fundamentals (SNAF)
01.02.10 Berlin, 08.02.10 Frankfurt, 15.02.10 Frankfurt
Securing Networks with ASA Advanced (SNAA)
01.02.10 Hamburg, 08.02.10 Berlin, 15.02.10 Frankfurt
Implementing Cisco Intrusion Prevention System (IPS)
09.02.10 Hamburg, 15.02.10 Hamburg, 23.02.10 Frankfurt
Implementing Cisco Network Admission Control (NAC)
22.02.10 Frankfurt, 29.03.10 Hamburg, 26.05.10 Berlin
Implementing Cisco NAC Appliance (CANAC)
24.02.10 Hamburg, 03.03.10 Hamburg, 30.03.10 Düsseldorf
Implementing Cisco Security Monitoring, Analysis & Response System (MARS)
16.02.10 Hamburg, 16.03.10 Düsseldorf, 23.03.10 Düsseldorf

cisco PARTNER Learning Solutions

CISCO TRAINING & CONSULTING SERVICES.
LIEBER GLEICH MIT FAST LANE.

fast lane

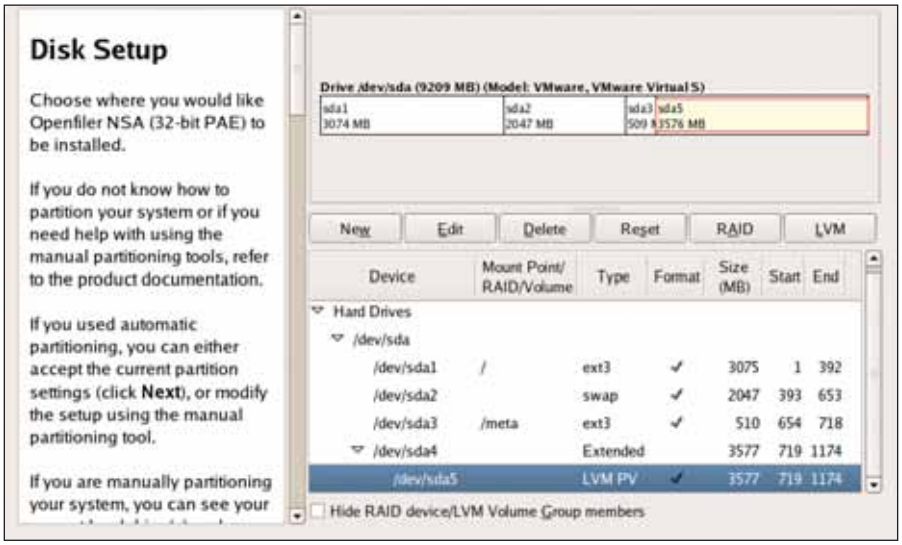


Bild 4: Die Partitionierung lässt sich bei Openfiler später speziellen Gegebenheiten anpassen

```
127.0.0.1 filer02.prod.zz local-
host.localdomain localhost
10.10.1.1 filer01.prod.zz
10.10.1.1 filer01
```

Zum Test der getätigten Einstellungen reicht ein Ping auf die jeweiligen IP-Adressen:

```
root@filer01 ~# ping 10.10.1.2
root@filer02 ~# ping 10.10.1.1
```

Erhalten wir dort jeweils eine Antwort auf unsere ICMP-Anfrage, funktioniert die Namensauflösung.

SSH Shared Keys einrichten

Damit unsere Systeme ohne die Eingabe des jeweiligen Passwortes miteinander kommunizieren können, generieren wir für jedes System einen SSH Shared Key: für Filer01.prod.zz mit *root@filer01 ~# ssh-keygen -t dsa* und entsprechend für Filer02.prod.zz mit *root@filer02 ~# ssh-keygen -t dsa*. Diese Befehle generieren den Public Key "id_dsa.pub" im Pfad "~/.ssh/". Diesen müssen Sie nun nur noch mittels SCP (Secure Copy) auf den jeweils anderen Server kopieren. Zunächst mit folgendem Befehl für Filer01.prod.zz:

```
root@filer01 ~# scp .ssh/id_dsa.pub
  root@filer02.prod.zz:~/.ssh/
  authorized_keys2
```

Und wie gewohnt analog für Filer02:

```
root@filer02 ~# scp .ssh/id_dsa.pub
  root@filer01.prod.zz:~/.ssh/
  authorized_keys2
```

Konfiguration des Clusterdienstes

Nun widmen wir uns der Konfiguration des eigentlichen Clusterdienstes. Die Konfiguration hierzu wird innerhalb der *drbd.conf* vorgenommen. Diese Datei muss nach der Konfiguration auf beiden Servern identisch sein. Im ersten Schritt erstellen Sie eine Sicherungskopie der *drbd.conf* für Filer01:

```
root@filer01 ~# mv /etc/drbd.conf
  /etc/drbd.conf.bak
```

Die *drbd.conf* editieren wir anschließend mittels "vim".

```
root@filer01 ~# vim /etc/drbd.conf
```

Unsere Beispieldatei *drbd.conf* sollte nun in etwa so aussehen wie in Listing 1.

Nachdem Sie die Datei gespeichert haben, kopieren Sie diese mittels SCP nun auch noch auf den zweiten Server:

```
root@filer01 ~# scp /etc/drbd.conf
  root@filer02.prod.zz:/etc/
  drbd.conf
```

Lesen Sie im zweiten Teil unserer Workshopserie, wie Sie den Heartbeat konfigurieren, eine erste Volume Group anlegen sowie iSCSI-Target und LUN für XenServer vorbereiten. *(jp)*

Links

[1] Openfiler
http://openfiler.com/community/download/

[2] Projektseite DRBD
www.drbd.org

[3] Projektseite Heartbeat
www.linux-ha.org

[4] Vim
www.vim.org

[5] Text-Editor Vim-Befehlsreferenz
www.linux-fuer-alle.de

Lizenzierung von Microsoft-Produkten (1)

Das richtige Lizenzpaket

von Thomas Joos

Die Lizenzierung von Microsoft-Produkten ist keine einfache Sache und stellt Unternehmen nicht selten vor zahlreiche Rätsel. In diesem Beitrag bringen wir Licht ins Dunkel und erklären, welche Lizenzierungswege Sie beschreiten können und was Sie dabei unbedingt beachten sollten. Wir klären zudem die verschiedenen Fachbegriffe und weisen Sie auf kritische Punkte hin, die Sie beim Vertragsabschluss besser berücksichtigen. Im ersten Teil unserer Serie beschäftigen wir uns grundlegend mit verschiedenen Lizenztypen und gehen dabei besonders auf Volumenlizenzen ein.

Lizenzieren Sie ein bestimmtes Serverprodukt, zum Beispiel Windows Server 2008 (R2) oder Exchange Server 2007/2010, benötigen Sie zunächst eine Serverlizenz, die Sie zur Installation berechtigt. Diese Lizenz können Sie über eines der Microsoft-Lizenzprogramme erwerben oder einzeln über Fachhändler beziehen. Außer der entsprechenden Serverlizenz müssen Sie bei Produkten, die mit Clientzugriffslizenzen (Client Access Licenses, CALs) lizenziert werden – zum Beispiel Windows Server oder Exchange Server – für jeden Benutzer oder Computer eine zusätzliche Lizenz erwerben. Eine CAL ist nur eine Lizenz, keine Software. Sie gestattet es Benutzern oder PCs, auf einen Server zuzugreifen und dessen Dienste zu nutzen.

Neben einzelnen CALs für den Zugriff auf die verschiedenen Server bietet Microsoft auch CAL-Pakete an, die den Zugriff auf mehrere verschiedene Produkte mit nur einer Lizenz erlauben. Diese CALs tragen die Bezeichnung "Microsoft Core Client Access License". Wenn Sie also den Einsatz mehrerer Microsoft-Produkte planen, sollten Sie beim Händler unbedingt nachfragen, ob eine solche Core-Lizenz verfügbar ist. Mit diesen Mehrfach-Lizenzen lassen sich einige Kosten sparen. In den folgenden Abschnitten zeigen wir Ihnen, welche Möglichkeiten es gibt, Produkte bei Microsoft zu erwerben und wie diese zu lizenzieren sind. Kaufen Sie Produkte wie Office, die keinen Server benötigen, lizenzieren Sie nur die Anzahl der Computer, auf denen Sie die Büroanwendung installieren. Zu den Besonderheiten dazu kommen wir noch.

Volumenlizenzen nach Maß

Diese Art der Lizenzierung richtet sich an Kunden, die zahlreiche Produkte von Microsoft für eine große Anzahl Anwender lizenzieren müssen. Microsoft bietet vier verschiedene Arten an, wie Sie Produkte bei entsprechend berechtigten Partnern erwerben können: License, License & Software Assurance Package, Software Assurance, Software Assurance Services. Hierbei handelt es sich im Grunde genommen um Produktlizenzen, die Sie mit Unterstützung von Microsoft noch ergänzen können für Schulungen, Support und Beratung. Die einfachste Version der Volumenlizenz ist "License". Erwerben Sie ein Produkt unter dieser Lizenz, dürfen Sie dieses Produkt im Unternehmen in der Anzahl einsetzen, wie Sie Lizenzen gekauft haben. Bei dieser Art der Lizenzierung benötigen Sie keine Vorversion des Produkts, da es sich immer um eine Vollversion handelt.

Die nächste Stufe dieser Lizenzierung ist das "License & Software Assurance Package". Da Sie bei diesem Paket regelmäßig Zahlung vornehmen, erhalten Sie das Recht, immer die aktuellste Version des Produkts einzusetzen, das im Vertrag genannt ist. Unternehmen, die beispielsweise ein solches Paket für Windows XP abgeschlossen haben, dürfen sowohl Windows Vista als auch Windows 7 einsetzen. In viele Verträge integriert Microsoft darüber hinaus noch die Möglichkeit, vergünstigt an Schulungen teilnehmen oder umsonst den Produkt-Support anrufen zu dürfen. Die Anzahl dieser Anrufe ist oft Verhandlungssache. Microsoft bietet verschiedene Stufen der Software Assurance an, die Sie unterschiedlich bezahlen müssen. Meistens handelt es sich dabei um Zusatzleistungen zu den erworbenen Produkten. Auf Basis dieser Grundlage entscheiden Sie, welches Programm der Volumenlizenz Sie verwenden, um Lizenzen zu kaufen. Die einzel-

Microsoft® Product List

	Product Notes (Ctrl + Click)	Date Available	SKU	Select / Select Plus*					
				L	L&SA			SA	
					3Yr	2Yr	1Yr	3Yr	2Yr	1Yr
Dynamics CRM 4.0 Limited CAL		01/08	SRV		3	2	2	2	1	1
Dynamics CRM 4.0 Limited External Connector		01/08	SRV		63	50	38	38	25	13
Dynamics CRM 4.0 Professional Server		01/08	SRV		125	100	75	75	50	25
Dynamics CRM 4.0 Workgroup Server		01/08	SRV		63	50	38	38	25	13
Duet™ for Office and SAP Server 1.5		10/09	SRV	1	3	2	2	2	1	1
Duet™ for Office and SAP Server 1.5 User CAL		10/09	SRV	1	3	2	2	2	1	1
Enterprise CAL Suite (Device & User)	38	10/06	SRV		13	10	8	8	5	3
Exchange Hosted Archive (User SL)	39	04/06		5 points						
Exchange Hosted Archive Extra Storage (Add-on SL)	39	04/06		1 point						
Exchange Hosted Continuity (User SL)	39	04/06		1 point						
Exchange Hosted Encryption (User SL)	39	04/06		1 point						
Exchange Online Deskless Worker (User SL)	40	04/09								
Exchange Online Standard (User SL)	41	10/08								
Exchange Online Extra Storage (Add-on SL)		10/08								
Exchange Server 2007 Enterprise CAL with Services Promo 2007	42	12/06	SRV		3	2	2			
Exchange Server 2007 Enterprise CAL with Services (Device & User)	42	12/06	SRV	1	3	2	2	2	1	1
Exchange Server 2007 Enterprise CAL without Services (Device & User)		12/06	SRV							
Exchange Server 2007 Enterprise Edition	43	12/06	SRV	50	125	100	75	75	8	25
Exchange Server 2007 Standard Edition	43	12/06	SRV	10	25	20	15	15	10	5
Exchange Server 2007 Standard for Small Business		10/09	SRV							
Exchange Server 2007 External Connector		12/06	SRV	200	500	400	300	300	200	100
Exchange Server 2007 Standard CAL (Device & User)	44	12/06	SRV	1	3	2	2	2	1	1

Bild 1: In der offiziellen Produktliste informiert Microsoft über die Möglichkeiten für Volumenlizenzen

nen Volumenlizenzprogramme behandeln wir im nächsten Abschnitt. Diese umfassen die Volumenlizenzen und Zusatzprodukte, also nur License oder Software Assurance in verschiedenen Stufen.

Lizenzverwaltung im Internet

Ab einer Anzahl von fünf Lizenzen können Sie für verschiedene Produkte "Open License" einsetzen. Die Anzahl der Lizenzen bedeutet nicht die Anzahl an PCs oder Mitarbeitern, sondern wie viele Microsoft-Produkte Sie einsetzen. Bei zwei Computern, auf denen Sie Windows und Office installieren, haben Sie so bereits vier Lizenzen im Einsatz. Die Vertragslaufzeit beträgt dabei normalerweise zwei Jahre und Sie müssen die Lizenz sofort in einer Summe bezahlen. Unter diesem Programm können Sie Lizenzen der bereits erwähnten Programme License sowie License & Software Assurance Package erwerben. Der Vorteil bei dieser Lösung ist, dass Sie neue Produkte nachkaufen können, wenn Sie Open License für bereits eingesetzte Produkte verwenden. Die Preise sind dabei meistens deutlich niedriger als bei anderen Lizenzformen. Ein Angebot einzuholen lohnt also auch für kleine Unternehmen.

Microsoft bietet abhängig von den gekauften Lizenzen Nachlass auf Basis eines Punktesystems. Aus diesem Grund sollten Sie vor dem Erwerb von Lizenzen eine genaue Aufstellung machen, welche Produkte Sie unter der Lizenz kaufen wollen. Wie das Punkte-System funktioniert, erfahren Sie auf der Webseite [1]. Sie verwalten die eingesetzten Lizenzen und deren Anzahl über eine eigene Internetseite, die Microsoft betreibt. Dieses Portal mit der Bezeichnung "eOpen" finden Sie unter [2]. Unter Open License erworbene Produkte können Sie entweder downloaden oder Sie bestellen auf der eOpen-Webseite die Datenträger direkt bei Microsoft.

Select License bindet für drei Jahre

Ab 500 Lizenzen können Unternehmen auf "Select License" umsteigen. Bei diesem Produkt erhalten Unternehmen noch bessere Vertragskonditionen und verbesserte Preise, müssen sich allerdings statt für zwei Jahre wie bei Open License für drei Jahre binden. Microsoft ermöglicht bei diesem Produkt eine Ratenzahlung, die in ihrer Beschaffenheit abhängig von den erworbenen Produkten ist. Auch hier legt Microsoft wieder ein Punktesystem zu Grunde, das Sie sich für Ihr Unternehmen am besten von einem Partner ausrechnen lassen, der das Recht hat, Open License oder Select License zu verkaufen. Sehr große, internationale Unternehmen mit mehreren Niederlassungen und zahlreichen Mitarbeitern können auf das nächstgrößere Modell Select Plus setzen. Die Vertragslaufzeit ist dann unbegrenzt.

Ratenkauf, Mietsoftware oder Finanzierung

Vor allem mittelständische Unternehmen haben oft hohe Lizenzkosten, die sich mit Open Value aber als Ratenzahlung abfedern lassen. Microsoft bietet Open Value für Unternehmen bis 500 PCs an. Sie zahlen die erworbenen Lizenzen über drei Jahre verteilt in drei Raten. Neben dem Kauf bietet Microsoft auch Mietmodelle unter Open Value an. Dieses Programm trägt die Bezeichnung "Open Value Subscription". Microsoft bietet verschiedene Preisstufen für Open Value an. Ab 250 PCs erhalten Unternehmen verbesserte Konditionen. Open Value enthält automatisch immer Software Assurance. Das bedeutet, dass Sie immer die neueste Version des Produkts einsetzen dürfen, das Sie lizenziert haben.

Bild 2: Auf einer speziellen Webseite finden sich Informationen über Finanzierungsmöglichkeiten beim Lizenzkauf

Die größere Version von Open Value mit der Bezeichnung Enterprise Agreement ist vor allem für große Unternehmen ab 250 PCs gedacht und bietet bei drei Jahren Laufzeit verbesserte Konditionen. Auch hier hat Microsoft verschiedene Rabattmodelle im Angebot, die abhängig von den PCs im Unternehmen sind. Unternehmen sollten hier stets verhandeln, da Microsoft und dessen Partner oft flexibler sind als bekannt. Mit den beiden Programmen Open Value Subscription (bis 500 PCs) oder Enterprise Agreement Subscription (ab 250 PCs) erhalten Unternehmen die Möglichkeit, Software zu mieten.

Der Ablauf ist der gleiche wie beim Kauf. Der große Unterschied besteht zum Ende der Laufzeit. Hier können Unternehmen die Software entweder billig erwerben oder den Mietvertrag verlängern. Alternativ können Sie den Vertrag komplett einstellen, müssen die Software dann aber deinstallieren. Hier ist die Zahlung ebenfalls auf jährliche Raten, die sich über drei Jahre erstrecken, verteilt. Open Value und Enterprise Agreement beruhen nicht auf der Anzahl der Lizenzen oder Software, die Sie einsetzen, sondern die Vertragsgrundlage ist die Anzahl der PCs im Unternehmen. Steigt diese Anzahl an, müssen Sie den Vertrag zur nächsten Jahresrate anpassen. Im aktuellen Jahr sind keine weiteren Kosten für neue PCs zu berücksichtigen.

Microsoft ermöglicht den Erwerb von Lizenzen zudem über eine Finanzierung. Im Gegensatz zum Ratenkauf oder der Miete nehmen Sie bei dieser Art des Produktkaufs einen Kredit bei Microsoft. Microsoft bietet solche Kredite für die verschiedenen Lizenzprogramme an, auch für Hardware-Produkte, die Sie bei Drittherstellern erwerben und auf denen Anwendungen von Microsoft installiert sind. In welcher Höhe Sie einen Kredit aufnehmen und wie die Zahlungsmodalitäten sind, klären Sie direkt mit Microsoft. Unternehmen haben dabei die Möglichkeit, die Rückzahlung der Raten flexibel zu gestalten. Bei Bedarf sind Zahlungsaufschübe und Pausen möglich. Mehr Informationen zu diesem Thema erfahren Sie auf einer eigenen Webseite [3].

Downgrade-Rechte und Zweit-Kopie

Neben den herkömmlichen Produktlizenzen in Zusammenhang mit Benutzerlizenzen bietet Microsoft für viele Produkte auch Sonderrechte an, die gerade für Volumenlizenz-Kunden interessant sind. Downgrade-Rechte bietet Microsoft für die meisten Produkte an. Mit diesem Recht haben Sie die Möglichkeit, ein aktuelles Produkt zu erwerben, zum Beispiel Windows Server 2008 R2, aber eine ältere Version einzusetzen, zum Beispiel Windows Server 2003. Der Vorteil dabei ist, dass Sie bei der zukünftigen Migration zu dem neuen Produkt keine neuen Lizenzen kaufen müssen, sondern bereits die aktuelle Version des Produkts lizenziert haben. Setzen Sie allerdings keine Volumenlizenz ein, sondern eine Original Equipment Manufacturer-Lizenz (OEM), müssen Sie überprüfen, ob ein Downgrade im Vertrag explizit erlaubt ist.

Re-Imaging-Rechte sind für Betriebssystemlizenzen auf Arbeitsstationen wichtig. Diese ermöglichen das Erstellen des Images eines Rechners und dessen Verteilung im Unternehmen. Planen Sie das Deployment eines Produktes per Image, sollten Sie vorher sicherstellen, dass der Lizenzvertrag dies auch erlaubt. Cross-Language-Lizenzen setzen vor allem internationale Unternehmen ein. Diese Lizenz ermöglicht die Installation eines Produkts in einer anderen Sprache. So können Sie beispielsweise ein französisches Office-Paket erwerben und eine deutsche Version von Office installieren.

Weiterhin interessant ist das Recht der Zweit-Kopie: Setzen Unternehmen beispielsweise Office 2007 auf den Arbeitsstationen ein, besteht die Erlaubnis, die Bürosoftware zusätzlich auf mobilen Computern zu installieren, wenn auf dem PC des entsprechenden Anwenders Office 2007 lizenziert ist. So müssen Unternehmen nicht doppelt lizenzieren, wenn Mitarbeiter mit zwei Computern arbeiten. Alle Produkte der Volumenlizenzverträge erlauben das. Setzen Sie OEM-Versionen ein oder andere Lizenztypen, müssen Sie zuvor in den Lizenzbestimmungen überprüfen, ob das Recht integriert ist. Allerdings darf laut dem Microsoft Lizenzvertrag nur der so genannte "primäre" Benutzer die Zweitkopie be-

Downgradepfade für Small Business Server 2008			
SBS 2008	**SBS 2003 R2**	**SBS 2003**	**SBS2000**
SBS 2008 Standard	SBS 2003 R2 Standard	SBS 2003 Standard	SBS 2000
SBS 2008 Premium	SBS 2003 R2 Premium	SBS 2003 Premium	Nicht verfügbar
SBS 2008 Suite	SBS 2003 CAL	SBS 2003 CAL	SBS 2000 CAL
SBS 2008 CAL für Premium Benutzer oder Geräte	SBS 2003 CAL	SBS 2003 CAL	SBS 2000 CAL

nutzen. Das ist der Benutzer, der an dem PC die meiste Zeit verbringt. Das Recht der Zweitkopie gilt allerdings nicht für Betriebssysteme, sondern nur für Office und andere Client-Produkte.

Desaster Recovery-Konzepte haben den Zweck, einen ausgefallenen Server auf einem Ersatzgerät wiederherzustellen. Solange der Ersatzserver, Cold-Backup-Server genannt, im laufenden Betrieb nicht eingeschaltet wird, können Sie in der Regel Softwaretitel, die Sie lizenziert haben, auch auf diesem Server installieren. Bei einem Ausfall des produktiven Servers kann der Cold-Backup-Server zur Wiederherstellung genutzt werden. Sie sollten allerdings bei Ihrem Händler dieses Lizenzrecht überprüfen lassen, da es nicht in allen Verträgen enthalten ist.

Sonderfall Business Server 2008

Bei der Lizenzierung des Small Business Server 2008 hat sich im Vergleich zu seinem Vorgänger Small Business Server 2003 am Grundprinzip wenig verändert. Um einen Small Business Server zu lizenzieren, müssen Sie zunächst die Grundlizenz der Standard oder der Premium Edition erwerben. Diese Lizenz berechtigt zur Installation des Small Business Server 2008. Bei den Zugriffslizenzen (CAL) unterscheidet Microsoft zwischen zwei Paketen: Die Pakete Small Business Server 2008 und Essential Business Server 2008 sind nahezu identisch:

- SBS (EBS) 2008 CAL Suite: Diese Lizenzen benötigen Computer oder Geräte, um auf das SBS-Netzwerk und die Funktionen des Servers zuzugreifen.
- SBS (EBS) 2008 CAL Suite für Premium Benutzer oder Geräte: Mit diesen Lizenzen ist lediglich der Zugriff auf die Premium-Funktionen des Servers gestattet, im Grunde genommen also hauptsächlich auf den SQL Server 2008.

Alle Anwender oder Computer, die im Netzwerk mit dem SBS 2008 oder dem EBS 2008 arbeiten, benötigen eine Client Access License (SBS-CAL oder EBS-CAL). Da sich die Lizenzierung von Small Business Server 2008 und Essential Business Server 2008 von der Lizenzierung der jeweiligen Einzelprodukte unterscheidet, geraten Sie in Schwierigkeiten, sobald die Anzahl der vorhandenen Benutzer die mögliche Maximalzahl an Lizenzen übersteigt. SBS lässt die Anmeldung nur für so viele Mitarbeiter zu, für die Lizenzen vorhanden sind. Jeder weitere Benutzer kann sich nicht mehr anmelden. Microsoft bietet für Small Business Server 2008 Lizenzpakete mit fünf, zehn oder 20 CALs an. Für den Essential Business Server 2008 stehen Lizenzpakete mit einem, fünf, 20 oder 50 CALs (Volumenlizenz) zur Verfügung.

Eine Neuerung in der Lizenzierung seit Small Business Server 2003 sind die erweiterten CAL-Rechte. Wenn Unternehmen zusätzlich zum Small Business Server 2008 einen Windows Server 2003/2008 oder einen Exchange Server 2007 im Netzwerk integrieren, müssen für diese Server keine zusätzlichen CALs erworben werden. Die Lizenzierung der Small Business Server 2008-CALs berechtigt auch für den Zugriff auf andere Server in einem Small Business Server 2008-Netzwerk, solange die Gesamtanzahl der Lizenzen nicht überschritten wird. Sie müssen lediglich die Serverlizenzen kaufen, aber keine zusätzlichen CALs. Das gilt ebenso für die Exchange-CALs oder SQL Server-CALs. Wenn Sie zwei Small Business Server 2008-Server installieren wollen, benötigen Sie natürlich auch zwei Small Business Server 2008-Lizenzen. Unternehmen, die Lizenzen von Small Business Server 2008 erwerben, erhalten zudem das Recht, ältere Editionen des Small Business Servers zu installieren. Die Tabelle "Downgradepfade für Small Business Server 2008" zeigt, welche älteren Versionen von SBS Unternehmen installieren können, wenn sie eine SBS 2008-Lizenz erworben haben. Die rechten Spalten zeigen dabei an, welche Versionen der jeweiligen SBS-Installation installiert werden dürfen. So darf beispielsweise ein Unternehmen, das SBS 2008 Premium erworben hat, SBS 2003 R2 Premium und SBS 2003 Premium installieren.

In Small Business Server 2008 Premium Edition ist SQL Server 2008 enthalten. Unter bestimmten Umständen erlaubt Microsoft die Installation von SQL Server 2005 Standard Edition, wenn Unternehmens-Applikationen nicht kompatibel zu SQL Server 2008 sind.

In Teil zwei unserer Serie zum Thema Microsoft-Lizenzen erläutern wir die Unterschiede zwischen Geräte- und Benutzer-Lizenzen und gehen in Beispielszenarien auf die jeweils günstigsten Lizenzierungsmodelle ein. Außerdem informieren wir darüber, was Sie bei der Lizenzierung von Terminal-Servern beachten müssen. *(ln)*

Links

[1] **Microsoft-Lizenzgrundlagen**
www.microsoft.com/germany/lizenzen/ueberblick/pur/

[2] **eOpen Lizenzverwaltung**
https://eopen.microsoft.com

[3] **Finanzierungsmodelle**
http://www.microsoft.com/germany/financing/

Bestellen Sie jetzt

das IT-Administrator

Sonderheft I/2010!

180 Seiten Praxis-Know-how

rund um das Thema

Windows Server 2008 R2 und Windows 7 + Tools-CD

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

**IT-Administrator Abonnenten erhalten das Sonderheft I/2010 für € 24,90. Nichtabonnenten zahlen € 29,90.*

Liefertermin:
Ende März 2010

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

---

administrator Das Magazin für professionelle System- und Netzwerkadministration

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

☐ **Ja**, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft I/2010 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft I/2010 zum Preis von **€ 29,90** inkl. Versand und 7% MwSt.

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____ BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

ITA 0110

So erreichen Sie unseren Vertrieb, Abo- und Leserservice:

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

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

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

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

Gemeinsame Benutzerverwaltung in Windows- und Linux-Netzwerken (3)

Linux und Windows im Samba-Takt

von Thorsten Scherf

Quelle: decu - Fotolia.com

Mit den richtigen Mitteln ist Samba für Windows- und Linux-Clients kein Problem

Im dritten und letzten Teil unser Workshopserie zeigen wir Ihnen, wie Sie die bestehende Samba-Konfiguration um einen zusätzlichen Backup-Domain-Controller erweitern. Daneben konfigurieren wir den Zugriff auf die Benutzerdatenbank für Linux-Clients, so dass auch diese bei der Anmeldung von einer zentral vorhandenen Benutzerdatenbank profitieren.

Ein zusätzlicher Backup-Domänen-Controller, auch als BDC bekannt, bringt nicht nur den Vorteil der Ausfallsicherheit mit sich, auch eine Lastverteilung lässt sich mit einem oder mehreren BDCs realisieren. Dies ist besonders dann hilfreich, wenn sich das eigene Netzwerk über mehrere geographisch voneinander getrennten Standorte erstreckt. Schließlich macht es wenig Sinn, für jede Benutzeranmeldung erst eine WAN-Verbindung zum Standort des primären Anmeldeservers aufzubauen.

Mit Hilfe mehrerer BDCs lässt sich so jeder Standort mit einem eigenen Server ausstatten. Zwar verfügen die BDCs nicht über eine Schreib-Kopie der Benutzerdatenbank, jedoch handelt es sich bei den allermeisten Zugriffen auf die Anmeldeserver lediglich um lesende Zugriffe, so dass dieses Manko nicht weiter ins Gewicht fällt. Änderungen an der Benutzerdatenbank sind jedoch immer auf dem PDC durchzuführen.

BDC-Konfiguration

Da wir in unserem Setup als Backend für den Samba-PDC einen OpenLDAP-Server einsetzen, gestaltet sich die Replikation der Benutzerdatenbank sehr einfach: Wir müssen lediglich eine Replikation zwischen zwei OpenLDAP-Servern einrichten. Dazu jedoch später mehr. Auch die Konfiguration des Backup-Domain-Controller ist nicht weiter schwierig, da diese, bis auf einige Ausnahmen, identisch mit der PDC-Konfiguration ist. Nach der Installation der notwendigen Software-Pakete (*samba, samba-common, openldap, openldap-servers, openldap-clients)* ist die Samba-Konfiguration, wie in Listing1 dargestellt, entsprechend anzupassen.

Anders als auf dem PDC ist hier keine Winbind-Konfiguration notwendig, da bei einer Domänen-Controller-Konfiguration dieser Dienst nur beim Anlegen neuer Benutzer in den Samba-SAM (Security-Account-Manager) notwendig ist. Da Benutzer aber zwingend auf dem PDC erzeugt werden müssen, benötigen wir den Dienst hier also nicht. Ein weiterer Unterschied besteht in der Domain-Master-Browser-Konfiguration. Da es innerhalb einer Domäne nur einen einzelnen Master-Browser geben darf und diese Funktion bereits der PDC übernimmt, müssen Sie die Funktion auf dem BDC also unbedingt ausschalten. Beim Blick auf die WINS-Konfiguration verweist der Netbios-Namenstyp "1b" für den Master-Browser auch auf den PDC. Alle weiteren Einstellungen können Sie wie in Listing 1 vom PDC übernehmen. Im nächsten Schritt benötigt der BDC die In-

```
[global]
workgroup = TUXGEEK
security = user
domain logons = yes
domain master = no

# LDAP Backend Konfiguration
passdb backend = ldapsam:ldap://tiffy.tuxgeek.de
ldap admin dn = cn=Manager,dc=tuxgeek,dc=de
ldap suffix = dc=tuxgeek,dc=de
ldap user suffix = ou=users
ldap group suffix = ou=groups
ldap machine suffix = ou=computers
ldap idmap suffix = ou=idmap
ldapsam:trusted = yes
ldapsam:editposix = yes

# Home, Profile und Netlogon Definitionen
logon drive = H:
logon path = \\%N\profiles\%U\%a
logon script = login.bat

# Standard-Freigaben
[homes]
writable = yes

[profiles]
path = /var/lib/samba/profiles
writeable = yes

[netlogon]
path = /var/lib/samba/netlogon
```

Listing 1: Samba-Konfiguration für BDC

formation, wie die Domänen-SID lautet. Hierbei handelt es sich um eine eindeutige Kennzeichnung für die Domäne. Auf dem PDC lässt sich diese einfach mit dem folgenden Kommando auslesen:

```
# net getlocalsid TUXGEEK
SID for domain TUXGEEK is: S-1-5-21-
  2004529239-1518482450-804885372
```

Entsprechend ist diese dann auf dem BDC zu setzen:

```
# net setlocalsid S-1-5-21-
  2004529239-1518482450-804885372
```

LDAP-Backend einrichten

Damit ist die Samba-Konfiguration abgeschlossen. Als Nächstes folgt das OpenLDAP-Backend. Aufgabe der Replikation ist es ja, jede Änderung an der Samba Master-Backend-Datenbank, die in unserem Beispiel auf einem LDAP-Server gespeichert ist, auf jeden weiteren LDAP-Server eines BDCs zu verteilen. OpenLDAP bietet hierfür grundsätzlich zwei verschiedene Methoden an: Schon seit den Anfängen von OpenLDAP existiert ein eigener Replikations-Dienst namens "slurpd". Seit der Version 2.2 existiert daneben das "syncrepl"-Protokoll. Hierbei handelt es sich um eine Replikations-Engine innerhalb des eigentlichen LDAP-Prozesses (slapd).

Wir empfehlen den Einsatz des syncrepl-Protokolls aus mehreren Gründen. Zum einen benötigen Sie damit keinen zusätzlichen Server-Dienst, zum anderen ist hierbei keine Anpassung des Master-LDAP-Servers notwendig. Sämtliche Konfigurationseinstellungen finden auf den Slave-Servern, die auf den BDCs zum Einsatz kommen, statt. Somit entsteht beim Hinzufügen von weiteren BDCs keine Unterbrechung des Master-Servers. Listing 2 zeigt die zusätzliche Sektion, die Sie zur Konfiguration der syncrepl-Engine in der OpenLDAP-Konfigurationsdatei */etc/openldap/slapd.conf* eintragen müssen. Alle anderen Einstellungen sind identisch mit denen aus der Master-slapd-Konfiguration aus dem zweiten Teil unserer Serie.

Starten Sie den LDAP-Server auf dem BDC, so bezieht dieser zunächst sämtliche Daten von seinem "Provider" und speichert diese in der lokalen Datenbank ab. Danach sucht der Server alle fünf Minuten auf seinem Master nach Änderungen an der Datenbank und überträgt diese in die lokale Datenbank. Umgekehrt kann der Master Änderungen auch direkt auf den Slave-Server "pushen", sobald diese stattfinden. Hierfür setzen Sie die Anweisung *type* im Block "synrepl" auf den Wert "refreshAndPersist". So besteht eine dauernde Verbindung zwischen allen an der Replikation teilnehmenden Servern. Nach dieser Konfiguration ist der BDC nun komplett einsatzbereit und in der Lage, Benutzer über die synchronisierte LDAP-Datenbank zu authentifizieren.

Möchte nun jedoch ein Benutzer etwa sein Passwort ändern, erzeugt dies eine Fehlermeldung. Der BDC besitzt schließlich keinen schreibenden Zugriff auf die LDAP-Daten. Fügen Sie daher der LDAP-Konfigurationsdatei einen sogenannten "Referral" hinzu, und zeigt dieser auf den Master-LDAP-Server, folgt der Samba-Server diesem und somit klappt dann beispielsweise auch die Passwort-Änderung eines Benutzers, der sich auf dem BDC angemeldet hat. Erweitern Sie hierfür die Datei *slapd.conf* um den folgenden Eintrag:

```
referral ldap://tiffy.tuxgeek.de/
```

Ein weiteres Problem besteht zu diesem Zeitpunkt mit der Integrität der Daten. Diese fließen momentan noch komplett im Klartext über das Netzwerk. Um diese Sicherheitslücke zu schließen, ist auf den LDAP-Servern die Konfiguration von SSL/TLS notwendig. Dabei kommen X.509-Zertifikate zum Einsatz, die zuvor von einer Zertifizierungsstelle (Certificate Authority, CA) signiert und für echt befunden wurden.

Zu Testzwecken oder für den rein internen Gebrauch lassen sich auch selbstsignierte Zertifikate erzeugen oder Sie erstellen mittels OpenSSL eine eigene Zertifizierungsstelle, die dann Zertifikate ausstellt. Bevor wir also die bestehende LDAP-Konfiguration um die notwendigen SSL/TLS-Anweisungen ergänzen, ein kleiner Ausflug in die Welt der X.509-Zertifikate.

X.509-Zertifikate und eigene CA

Bei X.509-Zertifikaten [1] handelt es sich um einen ITU-T-Standard für eine Public-Key-Infrastruktur (PKI). Innerhalb dieser PKI stellt eine CA digitale Zertifikate aus. Diese bestehen üblicherweise aus zwei Teilen, einem öffentlichen und einem privaten Schlüssel. Der öffentliche Schlüssel ist nach einer Verifizierung des Antragsstellers durch eine Signatur der CA als authentisch zu bestätigen. Nach der Beglaubigung wird dieser Schlüssel dann als Zertifikat bezeichnet. Mit dessen Hilfe lässt sich nun der Replikationsverkehr sowie der Zugang zum LDAP-Server selbst mittels SSL/TLS schützen. Das ist auch für die Authentifizierung von Linux-Clients interessant, da ansonsten auch hier die kompletten Anmeldedaten im Klartext über das Netzwerk wandern würden.

Um ein solches X.509-Zertifikat für die LDAP-Server zu generieren, gibt es mehrere Möglichkeiten. Nachfolgend beschreiben wir den Aufbau einer eigenen CA mit Hilfe von OpenSSL [2]. Diese CA ist dann in der Lage, die Zertifikatsanfragen der LDAP-Server zu beantworten. Im ersten Schritt benötigen wir die Datei */etc/pki/tls/openssl.cnf*. Diese gilt es, entsprechend den eigenen Gegebenheiten anzupassen (siehe Listing 3).

Mit dem folgenden openssl-Befehl lässt sich dann das CA-Zertifikat mit dem da-

```
[...]
syncrepl rid=001
  provider=ldap://tiffy.example.com/
  type=refreshOnly
  interval=00:00:05:00
  searchbase="dc=tuxgeek,dc=de"
  scope=sub
  bindmethod=simple
  binddn="uid=binduser,ou=People,dc=tuxgeek,dc=de"
  credentials=redhat
```

Listing 2: Konfiguration der syncrepl-Engine

zugehörigem privaten Schlüssel erzeugen. Dieses ist für einen Zeitraum von zehn Jahren zum Signieren von Zertifikatsanfragen gültig:

```
# openssl req -config /etc/pki/tls/
  openssl.cnf -new -x509 -keyout
  /etc/pki/CA/private/myca.key -out
  /etc/pki/CA/certs/ca.crt -days
  3650
```

Für die OpenLDAP-Server selbst lässt sich nun ebenfalls wieder auf OpenSSL zurückgreifen, um eine Zertifikatsanfrage mit dem dazugehörigen privaten Schlüssel zu erzeugen. Wichtig hierbei ist, dass der Common Name des Zertifikates dem Rechnernamen des LDAP-Servers entspricht. Stimmen diese nicht überein, würde eine spätere Verifizierung des Zertifikats fehlschlagen:

```
# openssl genrsa -out /etc/pki/tls/
  private/ldap.key 1024
# openssl req -new -key
  /etc/pki/tls/private/ldap.key -out
  /tmp/ldap.csr
```

Die Datei */tmp/ldap.csr* können Sie nun an die CA senden, um diese durch eine Signatur beglaubigen zu lassen. Die CA sendet dann die unterschriebene Zertifikatsdatei *ldap.crt* zurück an den Antragsteller:

```
# openssl ca -config /etc/pki/tls/
  openssl.cnf -policy policy_any-
  thing -out /etc/pki/CA/newcerts/
  ldap.crt -infiles /tmp/ldap.csr
```

Zusammen mit dem CA-Zertifikat, das zum Verifizieren von Zertifikaten benötigt wird, kopieren Sie die Datei *ldap.crt* in das Verzeichnis "/etc/pki/tls/certs/". Damit der LDAP-Server weiß, wo die Dateien liegen, fügen Sie dessen Konfigurationsdatei */etc/openldap/slapd.conf* die folgenden Zeilen hinzu:

```
TLSCACertificateFile
  /etc/pki/tls/certs/ca.crt
TLSCertificateFile
  /etc/pki/tls/certs/ldap.crt
TLSCertificateKeyFile
  /etc/pki/tls/private/ldap.key
```

Damit auch die OpenLDAP-Client-Anwendungen in der Lage sind, mittels SSL/TLS auf die LDAP-Server zuzugreifen, kopieren Sie das CA-Zertifikat zusätzlich in das Verzeichnis "/etc/openldap/cacerts" und rufen das Tool "cacertdir_rehash" auf. Nach einem Neustart des Servers gelingt mittels *ldapsearch-ZZ* auch eine mit TLS-geschützte Abfrage des Servers. Um nun auch bei der Replikation der LDAP-Datenbank auf eine mit TLS geschützte Verbindung zurückgreifen zu können, ergänzen Sie die in Listing 2 dargestellte Replikations-Vereinbarung um die folgenden Anweisungen:

```
syncrepl rid=001
[...]
starttls=yes
tls_cacert=/etc/pki/tls/certs/ca.crt
tls_cert=/etc/pki/tls/certs/ldap.crt
tls_key=/etc/pki/tls/private/ldap.key
```

Alle Änderungen an der LDAP-Datenbank auf dem Master-Server fließen nun über eine verschlüsselte Verbindung auf den Save-Server und stehen dort zur Abfrage dem BDC zur Verfügung.

Linux-Clients einbinden

Auf Linux/Unix-Systemen funktioniert die Benutzeranmeldung üblicherweise über die Dateien */etc/passwd* und */etc/shadow*. Meldet sich ein Benutzer mit seinem Namen und Passwort an einem System an, beispielsweise über *login*, so erzeugt das Programm eine kryptografische Prüfsumme des eingegebenen Benutzerpasswortes und vergleicht das Ergebnis mit der gespeicherten Prüfsumme für diesen Benutzer aus der Datei */etc/shadow*. Stimmen beide überein, so ist der Benutzer korrekt authentifiziert, anderenfalls schlägt die Anmeldung fehl. Dieses Verfahren stößt natürlich schnell an seine Grenzen. In großen Netzwerkumgebungen werden Benutzerdaten deshalb üblicherweise auf einem LDAP-Server vorgehalten.

Für den Zugriff auf den LDAP-Server sind zwei verschiedene Subsysteme zu konfigurieren: Zum einen handelt es sich hierbei um den Name-Service-Switch (NSS) sowie um die Pluggable Authentication Modules (PAM) [3]. NSS kommt zur Abfrage von Account-Informationen zum Einsatz, PAM kümmert sich um die eigentliche Authentifizierung. Zur Konfiguration der beiden Systeme greifen Sie im einfachsten Fall auf die Anwendung "system-config-authentication" zurück (siehe Bild 1).

Authentifizierung der User

Das Tool system-config-authentication passt die Konfigurationsdateien der beiden Subsysteme anhand der angegebenen Informationen entsprechend an. Im Einzelnen handelt es sich dabei um die folgenden Konfigurationsdateien:

- */etc/nsswitch.conf (NSS)*
- */etc/ldap.conf (NSS/PAM)*
- */etc/pam.d/system-auth (PAM)*

In der Datei */etc/nsswitch.conf* erhält der Name-Service-Switch die Information, aus welchen Quellen dieser Benutzer- und Gruppen-Informationen beziehen soll. Hier taucht neben den lokalen Dateien (*/etc/passwd* und */etc/group*) dann auch der Eintrag *ldap* auf. Welcher LDAP-Server abzufragen ist, steht in der Datei

```
[ CA_default ]
dir = /etc/pki/CA
   # Speicherort der CA-Konfiguration
certs = $dir/certs
   # Zertifikatsordner
crl_dir = $dir/crl
   # Zertifikatsrückrufliste (CRL)
database = $dir/index.txt
   # Index Datei für ausgestellte Zertifikate
new_certs_dir = $dir/newcerts
   # Neue Zertfikate
certificate = $dir/certs/myca.crt
   # CA-Zertifikat
private_key = $dir/private/myca.key
   # CA privater Schlüssel
serial = $dir/serial
   # Seriennummer des letzten Zertifiktes
crlnumber = $dir/crlnumber
   # CRL Nummer
crl = $dir/crl.pem
   # Die aktuelle CRL
```

Listing 3: Open-SSL-Konfiguration

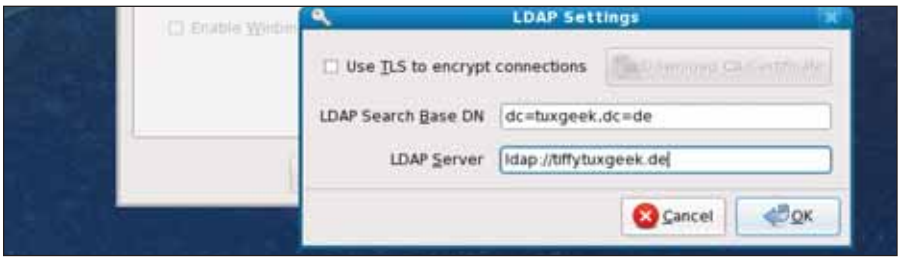


Bild 1: Über das Tool system-config-authentication lassen sich die beiden Subsysteme NSS und PAM für eine LDAP-basierte Benutzerauthentifizierung konfigurieren

/etc/ldap.conf. Bei PAM ist die Konfiguration etwas umfangreicher. Für jede Anwendung, die mit PAM zusammenarbeitet, existiert unterhalb von "/etc/pam.d/" eine eigene Konfigurationsdatei.

Über diese Konfigurationsdateien lassen sich sogenannte PAM-Bibliotheken, auch PAM-Module genannt, aus dem Verzeichnis "/lib/security/" aufrufen. Jede dieser Bibliotheken besitzt eine bestimmte Aufgabe. Beispielsweise ist *pam_unix.so* für eine klassische Authentifizierung von Benutzern über die Datei */etc/passwd* zuständig, *pam_ldap.so* dagegen authentifziert Benutzer über einen LDAP-Server.

Die PAM-Konfigurationsdateien im Verzeichnis "/etc/pam.d/" haben immer einen ähnlichen Aufbau, bestehend aus vier unterschiedlichen Sektionen:

- auth: Ist für die Authentifizierung von Benutzern verantwortlich.
- account: Hierüber lassen sich Benutzer autorisieren.
- password: Erzwingt eine bestimmte Passwort-Komplexität.
- session: Überwacht die Sitzung eines Benutzers.

In jeder dieser Sektionen lassen sich nun die nötigen PAM-Bibliotheken aufrufen. Unter */usr/share/doc/pam-version/txts/* finden Sie zu den meisten PAM-Bibliotheken eine ausführliche Hilfe. Beim Aufruf der Bibliotheken ist jeweils ein Kontroll-Flag mit anzugeben. Diese Flags bestimmen das Verhalten im Fehlerfall. PAM kennt die folgenden Kontroll-Flags:

- required: Die Bibliothek muss erfolgreich durchlaufen, ansonsten wird ein Fehler zurückgegeben, wobei jedoch nicht unmittelbar abgebrochen wird.
- requisite: Hier muss die Bibliothek ebenfalls erfolgreich durchlaufen, im Fehlerfall wird diesmal unmittelbar abgebrochen.
- sufficient: Das aufrufende Programm bekommt unmittelbar eine Erfolgsmeldung zurückgeliefert, ein Fehler wird ignoriert.
- optional: Erfolg oder Fehler haben keine Auswirkungen.

- include: Bibliotheken aus anderen Dateien lassen sich hiermit einlesen.

Bild 2 zeigt die PAM-Konfigurationsdatei */etc/pam.d/system-auth*. Diese Datei wird beim Aufruf von *system-config-authentication* erzeugt und aus anderen Konfigurationen über die include-Anweisungen eingelesen.

Interessant ist hierbei die auth-Sektion. Darin existieren insgesamt drei PAM-Module zur Authentifizierung eines Benutzers: *pam_fprintd.so* greift auf einen Fingerprint-Reader zurück, *pam_unix.so* überprüft die lokale Datei */etc/passwd* auf den sich gerade anmeldenden Benutzer und schließlich sucht *pam_ldap.so* auf den in der Datei */etc/ldap.conf* konfigurierten LDAP-Server nach dem Benutzerkonto. Wird der Benutzer über eine der drei möglichen Quellen authentifiziert, so klappt die Anmeldung am System, ansonsten verweigert *pam_deny.so* durch das Kontroll-Flag "required" den Zugang.

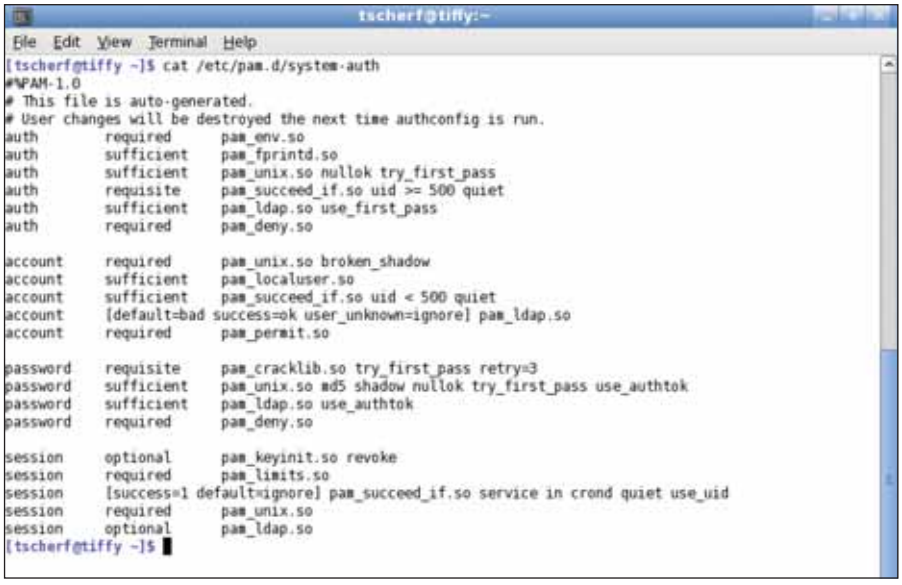


Bild 2: Über verschiedene PAM-Module lässt sich die Authentifizierung eines Benutzers flexibel gestalten

Posix-Attribute für Linux-Clients

Damit nun Linux-Clients zur Benutzeranmeldung auf die Daten des LDAP-Servers zurückgreifen können, benötigen die LDAP-Objekte natürlich die notwendigen Posix-Attribute wie beipielsweise "uidNumber", "gidNumber" und "homeDirectory". Eine Übersicht aller zwingend notwendigen Attribute liefert die Definition der Objektklasse "posixAccount". Diese finden Sie in der Schema-Datei *nis.ldif* wieder:

```
olcObjectClasses: ( 1.3.6.1.1.1.2.0
NAME 'posixAccount' DESC 'Abstracti-
on of an account with POSIX attribu-
tes' SUP top AUXILIARY MUST ( cn $
uid $ uidNumber $ gidNumber $ home-
Directory ) MAY ( userPassword $ lo-
ginShell $ gecos $
  description ) )
```

Ein Beispiel für ein solches Objekt, das sowohl die Objektklasse "posixAccount" für Linux spezifische Attribute wie auch die Objektklasse "sambaSamAccount" für Samba relevante Attribute enthält, zeigt Listing 4. Um bestehende LDAP-Objekte mit den notwendigen Posix-Attributen zu erweitern, bietet sich entweder ein grafischer Editor wie GQ an oder Sie nehmen die Änderungen auf der Kommandozeile mittels *ldapmodify* vor. Beim Hinzufügen von neuen Benutzern mittels einer LDIF-Datei lässt sich diese direkt mit den notwendigen Attributen ausstatten. Bei einer Abfrage des LDAP-Servers mittels *getent passwd* sehen Sie nun die zur Verfügung stehenden Benutzerkonten aus der Datei */etc/passwd* wie auch die Konten des LDAP-Servers. Mit dem weiter oben dargestellten Samba-Benutzer klappt also auch ein Login auf einer Linux-Maschine mittels "su" oder über die Konsole:

```
# su - thorsten
-bash-4.0# id
uid=0(thorsten) gid=10024(domadmins)
  groups=10024(domadmins)
  context=unconfined_u:unconfined_r:
  unconfined_t:s0-s0:c0.c1023
-bash-4.0# pwd
/home/TUXGEEK/thorsten
```

Melden sich die Benutzer mit ihren Accounts auf unterschiedlichen Systemen an, bietet es sich an, die Heimatverzeichnisse zentral zu verwalten und dann über den Automounter-Dienst "autofs" auf der jeweiligen Workstation einzubinden, sobald sich ein Benutzer anmeldet. Die Konfiguration für den Automounter lässt sich ebenfalls sehr leicht im LDAP selbst ablegen, sodass lokal keine Dateien zu pflegen sind. Dass die Konfiguration aus dem LDAP kommt, legen Sie wieder über einen entsprechenden Eintrag in der Datei */etc/nsswitch.conf* fest.

Samba-Konfiguration über die Windows-Registry

Damit ist die Konfiguration des Samba- und LDAP-Servers zur Verwaltung von Linux- und Windows-Benutzer-Konten

```
# ldapsearch -xLLL uid=thorsten
dn: uid=thorsten,ou=users,dc=tuxgeek,dc=de
objectClass: sambaSamAccount
objectClass: account
objectClass: posixAccount
cn: thorsten
uid: thorsten
homeDirectory: /home/TUXGEEK/thorsten
loginShell: /bin/bash
uidNumber: 0
gidNumber: 10024
userPassword:: cmVkaGF0
sambaNTPassword: B9D2D4955B330B503CC792EB6A55BB1F
sambaPasswordHistory:
   0000000000000000000000000000000000000000000000000
   0000000000000000000000000000000000000000000000000
 sambaAcctFlags: [U          ]
sambaPwdLastSet: 1254855929
sambaSID: S-1-5-21-2004529239-1518482450-
   804885372-500
```

Listing 4: Ein beispielhaftes LDAP Benutzer-Objekt mit Posix- und Samba-Attributen.

abgeschlossen. Zum Schluss noch zwei Tipps, die gerade für Windows-Administratoren interessant sind: Oftmals beklagen sich diese über die lästige Konfiguration des Samba-Servers auf der Kommandozeile mittels der Datei */etc/samba/smb.conf*. Zwar existieren einige grafische Frontends, jedoch ist es mittlerweile sogar mit Windows-Boardmitteln möglich, die komplette Samba Konfiguration durchzuführen. Die Rede ist hierbei vom heiligen Gral der Windows-Tools – dem Windows-Registry-Editor *regedit.exe*.

Samba ist seit der Version 3.2 in der Lage, die komplette Konfiguration in einer Samba-Registry-Datei anzulegen. Hierauf kann dann das regedit-Tool zugreifen, um die Konfiguration des Samba-Servers vorzunehmen. Was auf den ersten Blick vielleicht etwas seltsam anmutet, macht bei näherem Hinsehen durchaus Sinn. Die Registry ist ähnlich aufgebaut wie auch die Datei *smb.conf*. Sie besteht aus Bäumen, Schlüsseln und Wertezuweisungen. Dabei entsprechen die Schlüssel den Direktiven aus der *smb.conf* und die Werte den jeweiligen Werten der Direktiven. Der Teilbaum für die Samba-Konfiguration befindet sich dabei unterhalb von "HKLM \ Software \ Samba \ smbconf". Damit Sie auf diesen von einer Windows-Maschine aus zugreifen können, müssen Sie im ersten Schritt eine SMB-Verbindung zum Samba-Server aufbauen. Das geschieht beispielsweise durch den Aufruf von *net use* aus der MS-DOS-Eingabeaufforderung:

```
net use \\samba-server /user:root
```

Der Benutzer, unter dem Sie die SMB-Sitzung aufbauen, muss dabei über das Recht "SeDiskOperatiorPrivilege" verfügen. Zuweisen lässt sich diese Berechtigung, wie bereits im Teil 2 dieser Workshopserie beschrieben, mit dem Befehl *net rpc right*. Das Tool "smbstatus" auf dem Samba-Server sollte nun eine aktive SMB-Sitzung der Windows-Maschine auflisten. Hat dies geklappt, so starten Sie auf dem Windows-System das Tool *regedit.exe* und verbinden sich über "Datei / Computer wählen" mit dem Samba-Server. Anschließend lässt sich über den Baum "HKLM\Software\Samba\ smbconf" die Konfiguration des Samba-Servers vornehmen.

Unterhalb von "smbconf" existiert ein Teilbaum namens "global". Für jede Direktive aus der *smb.conf* lässt sich hier ein Schlüssel mit dem passenden Wert ablegen. Die Schlüssel-Namen sind dabei identisch mit den Namen der *smb.conf*-Anweisungen. Für Freigaben erzeugen Sie jeweils einen neuen Teilbaum unterhalb von "smbconf" und füllen diesen mit den gewünschten Anweisungen für die Freigabe, also beispielsweise "path" und "valid users".

Damit Samba nun auch auf die Informationen aus der Registry zurückgreift, müssen Sie dies dem Server mitteilen. Über den Eintrag "config backend = registry" in der global-Sektion der Datei */etc/samba/smb.conf* greift Samba von nun an lediglich auf die Information der Registry zu. Einträge aus der Datei *smb.conf* ignoriert Samba. Möchten Sie eine Mischkonfiguration betreiben, also Samba anweisen sowohl mit Direktiven aus der Konfigurationsdatei wie auch aus der Registry zu arbeiten, ersetzen Sie die Direktive "config backend" einfach durch "include = registry". Samba wertet dann beide Konfigurationsquellen aus. Die Registry selbst liegt dabei auf dem Server übrigens als tdb-Datei im Verzeichnis "/var/lib/samba" vor.

Zugriff für vertraute Nutzer gewähren

Ein weiteres nützliches Feature ist die Konfiguration von Vertrauensstellungen. Sollen Benutzer anderer Domänen auf Ressourcen der Samba-Domäne zugreifen, lässt sich hierfür eine entsprechende Vertrauensstellung einrichten. Dabei ist die Samba-Domäne die vertrauende, die andere Domäne die vertraute Domäne. Damit Benutzer aus einer Domäne Zugriff auf Ressourcen der Samba-Umgebung erhalten, erzeugen Sie auf dem Domänencontroller der vertrauten Domäne, dem PDC also, ein Domänen-Konto für die vertrauende Samba-Domäne.

Dazu wählen Sie im User-Manager einfach den Punkt "Policies" und dann "Trust Relationships" aus. Hier legen Sie dann ein Maschinen-Konto und ein Passwort für die Samba-Domäne an. Auf dem Samba-PDC lässt sich dann mit Hilfe des Passwortes für das Samba-Maschinenkonto der Trust vervollständigen. Dies geschieht durch den Befehl

```
# net rpc trustdom
  establish WIN-DOMAIN
```

Damit beim Zugriff aus der entfernten Domäne auf den Samba-Server die SIDs der Benutzer in entsprechende Linux-UIDs und GIDs umgewandelt werden, sollte auf dem Samba-Server der Winbind-Dienst laufen. Diesen haben wir im ersten Teil dieser Workshopserie ausführlich besprochen.

Fazit

Damit ist unser dreiteiliger Workshop zum Thema Benutzerverwaltung in Linux- und Windows-Netzwerken abgeschlossen. Auch wenn die Konfiguration auf den ersten Blick recht kompliziert erscheint, lohnt sich ein Umstieg sicherlich nicht nur aus Kostengründen. Mit Samba und Winbind erhalten Sie auch eine extrem flexible und sichere Systemumgebung. Auch Themenbereiche, die in diesem Tutorial nicht angesprochen wurden, wie beispielsweise verteilte Dateisysteme (DFS) oder Clustering (CTDB), sind mit aktuellen Samba-Versionen leicht zu bewerkstelligen. *(dr)*

Links

[1] X.509 Zertifikate
http://de.wikipedia.org/wiki/X.509/

[2] OpenSSL Projekt
www.openssl.org

[3] Zentrale Benutzerauthentifizierung mit LDAP, PAM und NSS
http://lug-s.org/dokumentation/kurse/benutzerverzeichnisse/index.html

VMware-Live-CD mit MOA 2.4.1

Portabler Werkzeugkasten

von Ulli Hankeln

Administratoren, die viel unterwegs sind, finden meist Arbeitsplätze vor, an denen die gewohnten Tools nicht installiert sind. Aus diesem Grund führen sie oft eine mehr oder weniger vollständige Toolsammlung auf Live-CDs mit sich. Leider ist das für VMware-Administratoren nicht so einfach, denn die meist benutzten VMware-Admintools fehlen auf den bekannten Live-CDs. Genau diese Lücke versucht das MOA-Projekt zu schließen, indem es die gängigsten VMware-Tools in einer portablen Umgebung – sprich Live-CD – bereitstellt. Dieser Workshop zeigt, wie Sie eine solche Live-CD mit der freien Software MOA aufbauen.

Vielen Administratoren ist sicherlich das UBCD4Win-Projekt bekannt. Dabei handelt es sich um eine Windows-basierte Live-CD mit dem Schwerpunkt System-Recovery. Das MOA-Projekt [1] basiert – ähnlich wie die UBCD4Win auch – auf Bart Lagerwijs Pebuilder, setzt aber den Schwerpunkt virtuelle Maschinen, sprich VMware. Seinen Ursprung nahm das Projekt Ende 2004, als das erste BartPE-Plug-In für VMware Workstation 4.5.2 veröffentlicht wurde. Da schnell klar wurde, dass VMware Workstation Systemanforderungen stellt, die ein "out-of-the-box" BartPE nicht erfüllt, wurde das Workstation-Plug-In um weitere System-Plug-Ins erweitert. Mittlerweile unterscheidet sich die aktuelle Version im "Look-and-Feel" kaum noch von einem normalen Windows XP oder 2003.

Das Setup

Seit Version 2.0 bietet MOA ein sehr einfach gehaltenes Setup-Tool: als Erstes benötigen Sie den Pfad zu der Windows 2003 SP 2-Installations-CD (wahlweise die Windows 2003 180 Tage-Trial-Version). Als Nächstes fragt das Setup nach, ob ein großes, ein kleines oder gar kein Treiberpaket eingebunden werden soll. Danach muss sich der User entscheiden, ob er Support für Mehr-Prozessorsysteme wünscht. Eine Live-CD mit SMP-Support bringt höhere Leistung auf heutigen DualCore- und vergleichbaren Systemen, bootet aber unter Umständen nicht auf alten Rechnern. Als Default wird daher ein Uniprocessor-Kernel verwendet.

Die nächste Frage lautet "do you want to use MOA for forensic investigations?" Beantworten Sie diese Frage mit "Ja", wird MOA so vorkonfiguriert, dass es beim Booten keine der lokal vorhandenen Partitionen mountet – sprich: mit einem Laufwerksbuchstaben versieht. Diese Option ist nur mit Windows 2003 als Quelle möglich und so erklärt es sich auch, dass MOA zwingend Windows 2003-Quellen voraussetzt und nicht mit XP funktioniert. Damit sind dann auch schon alle Fragen beantwortet und das Setup-Tool erledigt den Rest automatisch.

Nachdem das Setup-Tool die aktuelle MOA-Version und den Pebuilder 3.1.10a heruntergeladen hat, wird der Pebuilder gestartet. Dieser erledigt dann den eigentlichen Bau der CD. Zu guter Letzt hat der User noch die Option, den VMware Converter 3.0.3 einzubinden. Nach erfolgreichem Durchlauf des Setup-Tools finden Sie zwei ISO-Dateien im Unterordner "iso-out":

- Das "moa-standard.iso" bootet Rechner mit wenig RAM. Diese CD ist relativ langsam – vergleichbar etwa mit einem normalen BartPE oder einer UBCD4Win, da die ganze Zeit von CD gelesen werden muss.
- Das "moa-bandit.iso" hingegen benötigt deutlich mehr RAM (mindestens 768 MByte), ist aber deutlich schneller. Bei dieser Variante wird ein Festplatten-Image (*.img) komplett in den RAM geladen, was die Arbeitsgeschwindigkeit drastisch erhöht. Dieses Festplattenimage kann auch zum Booten von USB-Festplatten, USB-Sticks oder lokalen Festplatten verwendet werden.

Load on demand

Anders als ähnliche Windows-basierte Live-CDs bindet MOA keine zusätzlichen Programme beim Bau des Kern-Systems ein. Stattdessen beinhaltet MOA "out-of-the-box" praktisch nichts weiter als ein nacktes Windows 2003 mit Support für VMware Workstation. Derzeit erkennt MOA beim Booten alle Workstation-Versionen von 5.5.8 bis 7.0.0. Wird während des Bootvorgangs ein Ordner mit einer beliebigen dieser Versionen gefunden, so erkennt MOA die Version selbstständig und bindet sie automatisch ein. Falls keine Version gefunden wird, fragt das Tool den User nach dem entsprechenden Pfad.

Zusätzliche Programme bindet MOA nach dem "LODR-Verfahren" (Load On Demand) ein. Das heißt, zusätzliche Programme werden erst dann eingebunden, wenn sie auch wirklich gebraucht werden. Dieses neue Verfahren gleicht einen prinzipiellen Nachteil herkömmlicher Live-CDs aus:

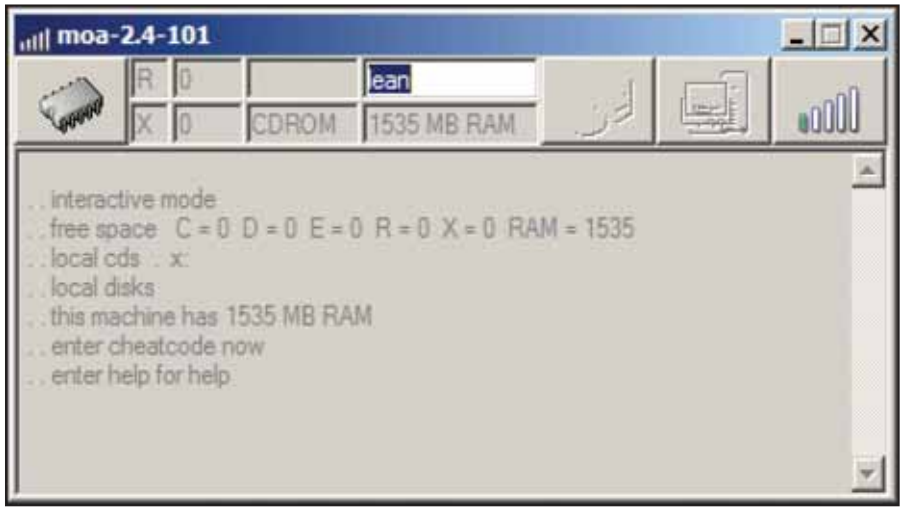


Bild 1: Durch die Eingabe von Cheatcodes erlaubt MOA die Anpassung der Live-CD während des Bootvorgangs

Diese werden schon beim Erstellen mit allen Zusatz-Programmen bestückt. Will der Administrator nachträglich Programme hinzufügen, ist das praktisch unmöglich, ohne die Live-CD von Grund auf neu zu erstellen. Dieses Problem wurde auch von den Autoren einiger Linux-Live-CDs erkannt. So gibt es zum Beispiel bei "Damn Small Linux" [2] ein Verfahren, welches erlaubt, im laufenden Betrieb Programme aus dem Internet nachzuladen. Dieses Verfahren ist zwar schon ein großer Fortschritt, aber es ist immer noch relativ umständlich, zusätzliche Programme einzubinden.

Konfiguration mit Cheatcodes

Ein normales Windows besteht, vereinfacht gesagt, aus einem System-Bereich und einem User-Bereich. Der System-Bereich findet sich typischerweise unter "C:\Windows", der User-Bereich entspricht etwa "C:\Programme" plus "C:\Dokumente und Einstellungen". MOA trennt diese beiden Bereiche konsequent: Den System-Bereich finden Sie unter dem Laufwerksbuchstaben "X:" (eine nicht veränderbare Vorgabe von Windows PE), den User-Bereich unter "R:" (R:\home, R:\programs et ectera). MOA bietet nun eine ähnliche Funktion, wie Sie sie wahrscheinlich von typischen Linux-Live-CDs kennen: "cheatcodes" – also spezielle Kommandos, mit denen Sie während des Bootvorgangs das Verhalten der Live-CD der jeweiligen Situation anpassen.

Am Anfang des Bootvorgangs wird zuerst der Systemkern geladen und anschließend erscheint ein Cheatcode-Prompt und Sie erhalten die Möglichkeit, den User-Bereich umzuleiten. Mögliche Ziele dieser Umleitung sind unter anderem eine Ramdisk, ein verschlüsselter Truecrypt-Container, eine USB-Festplatte oder ein USB-Stick. Nach Auswahl des passenden Cheatcodes wird der Boot-Vorgang fortgesetzt. Verwenden Sie die Umleitung auf eine Ramdisk, verhält sich MOA wie jede andere Live-CD und alle Veränderungen, die Sie an dem System vornehmen, gehen bei einem Neustart verloren. Wählen Sie hingegen eine Umleitung auf ein nicht-flüchtiges Medium wie zum Beispiel eine USB-Disk, bleiben Veränderungen am User-Bereich ("R:") auch über einen Neustart hinaus erhalten. Dieses Verhalten erleichtert das Arbeiten mit der CD ungemein und deswegen ist die Verwendung der MOA-CD zusammen mit USB-Festplatte oder -Stick zu empfehlen.

Hinzufügen von Programmen

Die einfachste Einbindung erlauben sicherlich portable Programme, denn diese installieren oder entpacken Sie einmal und können sie dann bei jeder späteren Verwendung einfach direkt benutzen. Komplexere kleine Programme wie zum Beispiel Starwind iSCSI-Server lassen sich

bei Bedarf durch eine "silent-installation"-Batch einbinden. Legen Sie sich einen Startmenü-Eintrag zu so einer Batch-Datei an, ist das Starten von Starwind eine Sache von Sekunden. MOA bringt von Haus aus Unterstützung für MSI-Pakete mit – dadurch lassen sich auch große Programme wie VirtualBox oder Ghost14 mit dem LODR-Verfahren innerhalb von Sekunden einbinden

Verwendung als VMware Coldclone-CD Ersatz

VMware bietet Enterprise-Kunden den Download einer WinPE 1 basierten Live-CD an. Mit dieser CD lassen sich physikalische Maschinen in eine Virtuelle Maschine (VM) konvertieren. Die Original-CD verwendet eine spezielle Version des Converters, die nicht frei erhältlich ist. MOA erreicht die gleiche Funktionalität mit der frei erhältlichen "Starter-Edition" des Converters. Die Verwendung von MOA als Coldclone-CD bietet einige Vorteile gegenüber dem Original, denn oft scheitert das Original in ganz banalen Fällen: soll zum Beispiel eine Windows 2000 Maschine importiert werden, macht schon ein Eintrag in der *boot.ini* wie

```
signature(e4fc79d6)disk(0)rdisk(0)
  partition(1)\WINNT="Microsoft
  Windows 2000 Server" /fastdetect
```

einen Import unmöglich. Ändern Sie diesen Eintrag auf

```
multi(0)disk(0)rdisk(1)
  partition(1)\WINNT="Microsoft
  Windows 2000 Server" /fastdetect
```

so funktioniert der Import hingegen problemlos. Mit MOA ist so ein Fall leicht zu handhaben, denn hier wird der Converter nicht als einziges, exklusives Programm gestartet. Zudem haben Sie die Gelegenheit, vor dem Start des Converters die *boot.ini* mit einem Texteditor zu überprüfen und gegebenenfalls anzupassen. Es ist praktisch unmöglich, eine Live-CD bei der Erstellung mit allen Treibern auszustatten, die im späteren Gebrauch irgendwann einmal benötigt werden. So ist es ganz normal, dass die Coldclone-CD gelegentlich scheitert, da der Massenspeicher-Treiber für die jeweilige physikalische Maschine nicht eingebunden ist. MOA hat schon "out-of-the-box" besseren Treiber-Support, darüber hinaus kann der Anwender bei MOA Treiber im laufenden Betrieb einbinden, was beim Original nicht möglich ist.

Auslesen von beliebigen Dateisystemen

Einige Datei-Systeme wie zum Beispiel VMFS lassen sich im Notfall oder bei forensischen Untersuchungen nicht sauber mit Live-CDs direkt auslesen. In einem solchen Fall können Sie sich mit einem MOA-System leicht behelfen. Um zum Beispiel lokale Platten mit VMFS auszulesen, booten Sie den Server in das MOA-System. Nun laden Sie eine ESXi-VM, die Sie sich auf der USB-Platte bereitgelegt haben. Dieser ESXi-VM fügen Sie mit dem "Virtual Hardware Editor" die lokalen Platten als "physicaldisk" hinzu.

Bild 2: Über die gewählte Option ermöglicht MOA das Auslesen vieler Dateisysteme

Anschließend booten Sie den virtuellen ESXi, fügen diesem die physikalischen Platten als neues Datastore hinzu und schon haben Sie die Möglichkeit, die Daten des VMFS per VEEAM FastSCP oder WinSCP auszulesen. Weiterhin sind Sie in der Lage, vorher von den physikalischen Platten einen Snapshot anzulegen – das bedeutet, Sie können lesend und schreibend auf die Daten zugreifen, ohne etwas an den physikalischen Platten zu verändern. Ein kurzes Video zu diesem Verfahren findet sich unter [3]. Und unter [4] finden Sie darüber hinaus ein Video mit einem Tutorial zu MOA.

Ausblick und Fazit

Die anstehende Version 3 von MOA setzt statt der CD-ROM als Standard-Bootmedium auf USB. Der ESX-Administrator wird sicherlich die neuen Bootoptionen ESX 3.5i und ESX 4i begrüßen. Der Workstation-User kann nun auch mit Workstation 7 unter 64 Bit-Linux die heutigen Möglichkeiten moderner Rechner voll ausschöpfen.

Jeder erfahrene ESX-Administrator sollte MOA zumindest einmal gesehen und getestet haben. In den richtigen Händen zur richtigen Zeit kann MOA wahre Wunder in punkto Zeitersparnis und Flexibilität bewirken. *(jp)*

Links

[1] Homepage und Download MOA 2.4.1
http://sanbarrow.com/moa241.html

[2] Damn Small Linux
www.damnsmalllinux.org

[3] Video: VMFS und andere Dateisysteme mit MOA auslesen
http://sanbarrow.com/latest-video-esxi-exe.html

[4] Videotutorial für MOA
http://sanbarrow.com/moa241/videos/moa241-setup.html

Exchange Server 2007 SP2

Gut gerüstet für 2010

von Thomas Joos

Quelle: Ioannis Kounadeas - Fotolia.com

Mit SP2 für Exchange Server 2007 erweitert Microsoft die aktuelle Version von Exchange um neue Funktionen und macht die Serverlösung bereit für Exchange Server 2010. Da diese Version bald in den Startlöchern stehen wird, sorgt das Service Pack 2 für Exchange 2007 für die notwendige Kompatibilität mit dem Nachfolger. Wir zeigen Ihnen, welche Neuerungen Microsoft integriert hat und auf was Sie achten müssen, wenn Sie das Service Pack auch in komplexeren Umgebungen, zum Beispiel auf dem Essential Business Server 2008 oder mit installiertem Forefront Security für Exchange, integrieren wollen.

Das zweite Service Pack enthält neben den im Anschluss beschriebenen neuen Funktionen auch alle Änderungen des Service Pack 1 sowie die des Rollup Package 8 und somit alle vorhergehenden Pakete. Ein interessanter Aspekt des SP2 für Exchange 2007 ist die Möglichkeit, im gleichen Netzwerk mit dem bald erhältlichen Exchange Server 2010 zusammenarbeiten zu können. Dies ist erst möglich, wenn alle Clientzugriff-Server im Netzwerk – zumindest aber am gleichen Active Directory-Standort – auf Exchange 2007 SP2 aktualisiert sind.

Neuerungen bei der Datensicherung

Eine Neuerung des SP2 für Exchange 2007 ist die Unterstützung der Windows Server 2008-Datensicherung mit Bordmitteln. Dazu ist im SP ein VSS-Plug-In enthalten. Nach der Installation lassen sich so Exchange-Datenbanken mit der Windows-Datensicherung sichern. Die Erweiterung ist in der Datei *WSBExchange.exe* enthalten. Der Installationsassistent integriert diese Erweiterung aber nur auf Postfachservern unter Exchange 2007. Damit lässt sich der Schattenkopiedienst zur Sicherung nutzen, es ist allerdings nicht möglich, mit Bordmitteln ESE-Streaming-Sicherungen durchzuführen.

Die Sicherung enthält immer den kompletten Datenträger als Vollsicherung, auf dem die Datenbanken installiert sind. Wiederherstellen aber lassen sich einzelne Datenbanken aus dieser Sicherung, entweder am originalen Speicherort oder an anderer Stelle. Die meisten Aufgaben dazu führt der Assistent automatisch durch. Eine Wiederherstellung enthält immer sämtliche gesicherten Speichergruppen. Es ist nicht möglich, einzelne Speichergruppen oder Datenbanken wiederherzustellen. Datensicherungen über das Netzwerk sind nicht vorgesehen. Natürlich lassen sich die Daten auf Netzwerkfreigaben sichern oder mit dem Remotedesktop durchführen.

Vereinfachte Administration

Auch die Überwachungsfunktionen etwa für den Postfachzugriff sowie die Überwachungsprotokolle hat Microsoft ausgebaut. Sie können nun einfacher die Verwendung des Servers überprüfen, zum Beispiel für spätere Erweiterungen der Hardware. Zudem lassen sich Änderungen an der Exchange-Konfiguration mit Service Pack 2 jetzt besser im Auge behalten. Das Management der Überwachungsfunktionen ist durch eine grafische Oberfläche leichter geworden. Bisher mussten die meisten Administratoren dazu auf Cmdlets oder Zusatztools zurückgreifen. Mehr Informationen zu den verbesserten Überwachungsmöglichkeiten finden Sie unter [1] im Internet. Schemaerweiterungen, zum Beispiel für Zusatzprogramme für Exchange wie CRM-Systeme, sind jetzt leichter möglich und es treten keine Konflikte mehr auf, wenn verschiedene Programme gleiche Werte anlegen wollen. Exchange verwendet für den Zugriff auf das Active Directory den Treiber *Microsoft.Exchange.Data.Directory.dll*. Die meisten AD-Schemadefinitionen sind fest vorgegeben. Führt eine Anwendung eine Aktualisierung des Schemas von Active Directory durch, kommt bisher die Datei *App.config* zum Einsatz, was aber recht fehleranfällig ist. Der neue Treiber des SP2 ist hier zuverlässiger. Attribute lassen sich nun unabhängig von Schemaänderungen setzen. Ferner ist der Verweis auf Attribute, die nicht im Schema vorhanden sind, kein Problem. Außerdem ist der neue Treiber kompatibel zu Exchange Server 2010.

Für öffentliche Ordner lassen sich mit SP2 leichter Kontingente festlegen. Dazu stellt Microsoft das Cmdlet *Set-PublicFolder* mit erweiterten Möglichkeiten zur Verfügung. Eine Verwaltung der Kontingente in der

grafischen Oberfläche ist leider nicht möglich. Neben diesem Cmdlet hat Microsoft auch die Möglichkeiten der meisten anderen Befehle für die Verwaltungsshell erweitert. Mehr Informationen zur Syntax von *Set-PublicFolder* finden Sie unter [2]. Außerdem können Sie unter [3] auf eine ausführliche Hilfe zu den neuen Befehlen und Optionen für die Exchange-Verwaltungsshell zugreifen.

Installation nicht ohne Handarbeit

Vor der Installation des SP2 sollte Ihnen bewusst sein, dass sich das Service Pack nicht deinstallieren lässt. Microsoft empfiehlt, zunächst die Installation auf Client Access-Servern durchzuführen, in einem Netzwerk mit Essential Business Server 2008 daher zuerst auf dem Sicherheits-Server. Achten Sie darauf, dass eventuelle Zusatz-Konnektoren für Unified Messaging oder Faxdienste das neue Service Pack unterstützen und fragen Sie dazu vorher beim Hersteller nach.

Nach der Aktualisierung der Client Access-Server aktualisieren Sie die anderen Server im Netzwerk. Setzen Sie EBS 2008 ein, bietet sich die Reihenfolge Sicherheits-Server, Messaging-Server und schließlich Verwaltungs-Server an. Dieser enthält zwar keine Exchange-Komponenten, aber die Exchange-Verwaltungstools, die mit dem SP2 ebenfalls aktualisiert werden. Im herkömmlichen Netzwerk lautet die empfohlene Reihenfolge Client Access, Hub Transport, Mailbox, Unified-Messaging. Außerdem sollten Sie auf allen Servern zunächst das ServicePack 2 für Windows Server 2008 installieren.

Erhalten Sie während der Installation eine Fehlermeldung, dass Sie Windows-Installer 4.5 benötigen, laden Sie sich diesen von der Webseite [4] herunter und installieren Sie die Erweiterung. Starten Sie dann das Setup-Programm erneut. Achten Sie darauf, dass Serverlösungen, die Exchange-Dienste automatisch starten, dies nicht während der Installation tun, da diese für das Setup beendet sein müssen. Setzen Sie Sprachpakete für Unified-Messaging-Server ein, müssen Sie diese vor der Installation deinstallieren und anschließend aus den aktuellen SP2-Dateien mit *setup.com* wieder installieren, zum Beispiel mit

```
setup.com /AddUmLanguagePack:de-DE
/sourcedir:c:\ languagePacks
```

Sie finden die aktuellen Sprachdateien für Unified-Messaging auf der Internetseite [5]. Das Service Pack führt außerdem mit *PrepareAD* und *PrepareDomain* Änderungen am Schema durch.

Sonderfälle Essential Business Server und Forefront

Die Installation auf dem Messaging-Server in einem Essential Business Server-Netzwerk (EBS) oder wenn Sie Forefront Security für Exchange einsetzen, oder auch bei Small Business Server 2008, unterscheidet sich etwas von der Installation des Service Packs auf anderen Servern. Ist zusätzlich Forefront Security für Exchange installiert, müssen Sie die Security-Lösung vor der Installation des SP2 erst deaktivieren und anschließend wieder aktivieren. Achten Sie aber darauf, dass Ihre Forefront-Version kompatibel zum Service Pack ist. Ist sie das nicht, aktualisieren Sie zunächst Forefront und dann erst die Exchange-Server. Zur Installation des Service Pack 2 auf dem Messaging-Server im EBS-Netzwerk oder auf Mailbox-Servern mit Forefront gehen Sie am besten folgendermaßen vor:

1. Geben Sie *services.msc* in das Suchfeld des Startmenüs ein, um die Dienste-Steuerung zu starten.
2. Klicken Sie mit der rechten Maustaste auf den Dienst *FSCController* und stoppen Sie diesen, sofern er gestartet ist.
3. Durch das Beenden dieses Dienstes beenden sich nach einer Bestätigung auch die beiden Dienste Microsoft Exchange-Informationsspeicher und Microsoft Exchange-Transport.
4. Nun müssen Sie eine Eingabeaufforderung mit Administrator-Rechten öffnen. Klicken Sie dazu mit der rechten Maustaste auf "Start/Eingabeaufforderung" und wählen Sie "Als Administrator ausführen".
5. Wechseln Sie in das Verzeichnis "{systemdrive}\Program Files (x86)\Microsoft Forefront Security\Exchange Server".
6. Geben Sie den Befehl *FSCUtility.exe /disable* ein, um Forefront zu deaktivieren. Lassen Sie nach Abschluss die Befehlszeile geöffnet, Sie benötigen diese nach der Installation noch einmal.
7. Führen Sie mit einem Doppelklick auf *Setup.exe* die Installation des SP2 durch.
8. Nach abgeschlossener Installation wechseln Sie in der Befehlszeile in das Verzeichnis "{systemdrive}\Program Files (x86)\Microsoft Forefront Security\Exchange Server".
9. Geben Sie den Befehl *FSCUtility.exe /enable* ein, um Forefront wieder zu aktivieren.

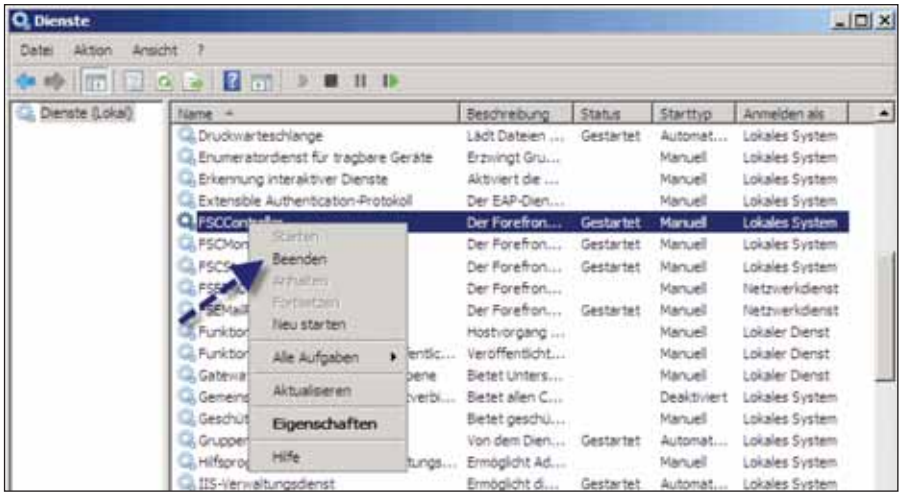


Bild 1: Beim Einsatz von Forefront Security für Exchange müssen Sie zunächst den Dienst für Forefront beenden

10. Starten Sie nach erfolgter Aktivierung die Systemdienste FSCController, MS Exchange-Informationsspeicher und MS Exchange-Transport. Sind noch andere auf "Automatisch" gestellte Exchange-Dienste nicht gestartet, fahren Sie diese manuell hoch.

Small Business Server 2008 erfordert Registry-Änderung

Installieren Sie das Service Pack unter SBS 2008, müssen Sie zunächst Erweiterungen in der Registry durchführen, da ansonsten die Installation mit einem Fehler abbricht. Navigieren Sie dazu zum Registry-Schlüssel "HKEY_LOCAL_MACHINE \ Software \ Microsoft \ SmallBusinessServer \ Exchange". Ist der Schlüssel nicht vorhanden, erstellen Sie diesen. Danach legen Sie unterhalb dieses Schlüssels den neuen DWORD-Eintrag "E12SP2READY" mit dem Wert 1 an. Mehr zu diesem Thema finden Sie auf der Support-Internetseite [6]. Nach der Installation des SP2 haben manche Clients mit Outlook 2007 Probleme mit dem Offline-Adressbuch. Diese lassen sich mit dem Befehl

```
Update-OfflineAddressbook {Name des
  Offline-Adressbuches}
```

in der Exchange-Verwaltungsshell des Servers beheben. Mehr zu diesem Fehler und dessen Behebung finden Sie auf der Internetseite [7].

Service Pack 2 und Cluster

Der Ablauf zur Installation auf einem Cluster ist generell folgender (eine ausführliche Anleitung finden Sie auf der Internetseite [8]):

1. Stellen Sie sicher, dass der passive Knoten keine Ressourcen verwaltet und bereit zur Installation ist. Verschieben Sie dazu die Ressourcen eventuell auf einen anderen Knoten.
2. Achten Sie darauf, dass Überwachungsprogramme wie OpenView, Tivoli oder MOM nicht aktiv auf dem Server Aktionen durchführen.
3. Starten Sie den Dienst für die Remoteregistrierung neu.
4. Starten Sie in der Befehlszeile den Befehl *Setup /m:upgrade* aus den Service Pack 2-Installationsdateien.
5. Starten Sie den Knoten neu.
6. Melden Sie sich nach dem Neustart an und öffnen Sie die Exchange-Verwaltungsshell. Halten Sie den Clusterknoten mit dem Befehl *Stop-ClusteredMailboxServer* an.

Danach beginnt mit der Aktualisierung des aktiven Knotens der kritische Teil:

1. Verschieben Sie in der Exchange-Verwaltungsshell des passiven Knotens die Clusterressourcen vom aktiven Knoten auf einen passiven Knoten, den Sie bereits auf das SP2 aktualisiert haben. Dazu steht der Befehl *Move-ClusteredMailboxServer* zur Verfügung:
```
Move-ClusteredMailboxServer
  {Servername} -TargetMachine
  NODEB -MoveComment "Update zu SP2"
```
2. Anschließend aktualisieren Sie den eigentlich geclusterten Exchange-Server auf das SP2. Verwenden Sie dazu den Befehl *Setup /upgradecms*.
3. Danach führen Sie auf dem Knoten die Schritte eins bis fünf durch, die Sie bereits bei der Aktualisierung des passiven Knotens durchgeführt haben.

Installation auf Domänencontrollern

Mit dem neuen Service Pack lässt sich Exchange Server 2007 jetzt auch auf Domänencontrollern mit Windows Server 2008 R2 installieren. Dazu verwenden Sie die Installationsdateien des Service Pack 2 für eine komplette Neuinstallation. Beachten Sie dazu aber die Hinweise des Exchange-Entwicklerteams auf der Webseite [9]. Selbst wenn alle Domänencontroller im Netzwerk mit Windows Server 2008 R2 installiert sind, kann es Probleme mit Exchange Server 2007 geben, auch dann, wenn Sie das Service Pack 2 installieren. Generell ist Windows Server 2008 R2 allerdings bereits für Exchange Server 2010 und den zahlreichen Änderungen bei der Authentifizierung optimiert. An Details interessierte Administratoren können die Hilfedatei des Service Pack 2 gesondert von der Internetseite [10] herunterladen.

Mittlerweile bietet Microsoft auch das erste Updaterollout für das Service Pack 2 an. Sie sollten also nach der Installation des SP2 noch die etwa 40 MByte große Erweiterung installieren, die einige Patches enthält. Eine genaue Auflistung der Änderungen und den Download finden Sie unter [11]. *(ln)*

Links

[1] Postfachzugriffsüberwachung mit Exchange Server 2007
http://technet.microsoft.com/de-de/library/ee221156.aspx

[2] Syntax zu Set-PublicFolder
http://technet.microsoft.com/de-de/library/aa998596.aspx

[3] Exchange Server 2007 Service Pack 2 Shell-Hilfe
www.microsoft.com/downloads/details.aspx?familyid=AB3523A9-D502-420D-9719-9373FA2427BA&displaylang=de

[4] Windows Installer 4.5
http://support.microsoft.com/kb/942288

[5] Exchange Server 2007 Service Pack 2 Unified Messaging Language Packs
www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=735518c5-acb1-4f9d-a973-80695dd0913e#tm

[6] Tipps für die Installation auf SBS 2008
http://support.microsoft.com/?scid=kb;en-us;973862&x=10&y=13

[7] Fehlerbehebung bei Problemen mit Outlook 2007
http://blogs.msdn.com/dgoldman/archive/2006/11/27/Error-0x80190194-when-using-an-outlook-2007-client-to-download-a-web-distribution-enabled-oab.aspx

[8] Anleitung zu SP2-Installation in geclusterten Umgebungen
http://technet.microsoft.com/en-us/library/bb676320.aspx

[9] SPP auf Server 2008-Domänencontroller installieren
http://msexchangeteam.com/archive/2009/09/15/452494.aspx

[10] Hilfe-Datei für Exchange Server 2007 SP2
www.microsoft.com/downloads/details.aspx?FamilyID=85c5ef71-6a1f-4eb0-9ff3-3feee6057e96&DisplayLang=de

[11] Updaterollup 1 für Service Pack 2
http://support.microsoft.com/?kbid=971534

Prozessoptimierung durch Logon-Skripte (2)

Mailsignatur nach Maß

von Sascha Giebelhausen

Im ersten Teil unserer Workshopserie haben wir verdeutlicht, wie Logon-Skripte durch das Lesen von Daten aus dem Active Directory Prozesse einfach automatisieren. Dabei hat sich gezeigt, dass die auf Basis von VB-Skript erstellten Logon-Skripte eine überzeugende kostenlose Alternative zu kommerzieller Software von Drittanbietern sind. Im zweiten Teil des Workshops gehen wir darauf ein, wie Sie über Logon-Skripte E-Mailsignaturen erzeugen und den Anwendern zuweisen.

Die Mailsignatur wird mit Hilfe von Active Directory-Attributen generiert. Wie Sie die enthaltenen Informationen vor der Generierung auslesen und prüfen müssen, haben wir bereits erklärt. Die Mailsignaturen bestehen in dem hier beschriebenen Fall aus der normalen Mailsignatur für neue Mails (lang) und aus der Antwortsignatur (kurz). Die normale Mailsignatur setzt sich im Groben aus folgenden Bausteinen zusammen: Verabschiedung, Mailanschrift, Postanschrift, Ruf- und Faxnummern, Pflichtangaben des Unternehmens, Veranstaltungen/Lesungen und Mailinformationen.

Die Antwortsignatur dagegen enthält nur den Verabschiedungs-Baustein. Die mit diesem Skript erstellten Signaturen gelten für Text-E-Mails (unter Office 2003 werden HTML- und RTF-Signaturen automatisch erstellt).

Gesetzliche Anforderungen beachten

Wichtig ist bei Signaturen generell, dass seit dem 1. Januar 2007 das "Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister" (EUHG) gilt. Es besagt, dass die Pflichtangaben für Firmen nun auch für die elektronische Post mitgeliefert werden müssen. Diese Pflichtangaben müssen Umsatzsteuernummer, Amtsgericht und Geschäftsführer enthalten.

Natürlich lassen sich auch bei der Mailsignatur verschiedene Bausteine ein- oder ausblenden. Zusätzlich besteht die Möglichkeit, anhand der Zugehörigkeit zu Gruppen oder Organisationseinheiten verschiedene Pflichtangaben für Unterneh-

```
Set objSysInfo = CreateObject("ADSystemInfo")
strquery = "LDAP://" & objSysInfo.Username
Set objuser = GetObject(strquery)

strfirstname = objuser.givenname
strname = objuser.sn
straccount = objuser.samaccountname
strmail = objuser.mail
strcompany = objuser.Company
strphone = objuser.TelephoneNumber
strfax = objuser.FaxNumber
straddress = objuser.streetaddress
strzip = objuser.postalcode
strcity = objuser.l
strmobile = objuser.TelephoneMobile
strweb = objuser.wwwhomepage
stroffice = objuser.physicaldeliveryofficename

Set objShell = CreateObject("WScript.Shell")
Set objFSO = CreateObject
   ("Skripting.FileSystemObject")
RegKey = "HKEY_CURRENT_USER\Software\Microsoft\
   Office\11.0\Common\General"
RegKey = RegKey & "\Signatures"
objShell.RegWrite RegKey , "Signatures"
UserDataPath =
   ObjShell.ExpandEnvironmentStrings("%appdata%")
FolderLocation = UserDataPath &"\Microsoft\
   Signatures\"
newsignature = FolderLocation & "XYZ GmbH (lang).txt"
answersignature = FolderLocation & "XYZ GmbH
   (kurz).txt"

Set objFile = objFSO.CreateTextFile(newsignature,True)
objFile.Close
Set objFile = objFSO.OpenTextFile(newsignature, 2)

objfile.write vbCrLf
objfile.write "Mit freundlichen Grüssen / With kind
   regards" & vbCrLf
objfile.write vbCrLf
objfile.write strfirstname & " " & strname & vbCrLf
objfile.write strmail & vbCrLf
objfile.write vbCrLf
objfile.write strcompany & vbCrLf
objfile.write straddress & vbCrLf
objfile.write strzip & " "& strcity & vbCrLf
objfile.write "Tel. " & Strphone & vbCrLf
If strmobile <> "" Then objfile.write "Mobil " &
   Strmobile & vbCrLf
objfile.write "Fax " & strfax & vbCrLf
objfile.write strweb & vbCrLf
objfile.write vbCrLf
objfile.write "UST-ID-Nr.: …" & vbCrLf
objfile.write "Amtsgericht …" & vbCrLf
objfile.write "Geschäftsführer: …" & vbCrLf
objfile.write vbCrLf
IF strevent<> "" Then objfile.write strevent & vbCrLf
objfile.write
   "************************************************
   ********" & vbCrLf
objfile.write "Der Inhalt dieser E-Mail ist aus-
   schließlich für den bezeichneten Adressaten be-
   stimmt. Wenn Sie nicht der vorgesehene Adressat
   dieser E-Mail oder dessen Vertreter sein sollten,
   so beachten Sie bitte, dass jede Form der Kenntnis-
   nahme, Veröffentlichung, Vervielfältigung oder Wei-
   tergabe des Inhalts dieser E-Mail unzulässig ist.
   Wir bitten Sie, sich in diesem Fall mit dem Absen-
   der der E-Mail in Verbindung zu setzen." & vbCrLf
objfile.write "This e-mail and any files transmitted
   with it are confidential and intended solely for
   the use of the individual or organization to whom
   they are addressed. Should you not be the intended
   addressee of this e-mail or his or her representa-
   tive, please note that publication, replication of
   the contents by any means or further communication
   of the content is not permissible. Should you have
   received this e-mail in error, please notify the
   sender." & vbCrLf
objFile.Close

Set objFile =
   objFSO.CreateTextFile(answersignature,True)
objFile.Close
Set objFile = objFSO.OpenTextFile(answersignature, 2)

objfile.write vbCrLf
objfile.write "Mit freundlichen Grüssen / With kind
   regards" & vbCrLf
objfile.write vbCrLf
objfile.write strfirstname & " " & strname & vbCrLf
objFile.Close
```

Listing 1: Erstellen einer Mailsignatur aus Bausteinen aus dem Active Directory

men aus einer vorgegebenen Liste zu importieren. Diese Option kommt meist dann zum Einsatz, wenn das Active Directory durch mehrere Firmen genutzt wird. Sie können aber ebenso vorgegebene Adress- oder Kontaktinformationen einer Vermittlung, einer Sammelrufnummer, des Vorgesetzten oder der Sekretärin aus einer Liste auslesen. In dieser Liste muss dann nur die Zuordnung zwischen der Organisationseinheit oder der Gruppe enthalten sein.

Automatische Erweiterung der Outlooksignatur

Da in den meisten Unternehmen nicht jeder Anwender ein Mobiltelefon oder ein eigenes Fax erhält, muss diese Besonderheit über eine Abfrage abgefangen werden. Dafür müssen Sie prüfen, ob das Active Directory-Attribut "TelephoneMobile" oder "FaxNumber" ausgefüllt ist. Ist dies der Fall, fügen Sie in die Textdatei der Mailsignatur einfach eine zusätzliche Zeile für die Mobilfunk- und/oder Faxnummer ein. Häufig soll auch innerhalb einer Mailsignatur auf Veranstaltungen wie Messen oder Vorlesungen aufmerksam gemacht werden. Um mit einer manuellen Änderung an der Signatur nicht den Anwender oder den Administrator zu belasten, ist auch hierfür ein Logon-Skript einsetzbar. Es reicht vorerst eine Textdatei zur Pflege der Veranstaltungen aus. Diese muss das Logon-Skript dann nur auslesen und die entsprechende Information in die Signatur einarbeiten.

Implementierung des Skriptes

Vor der Generierung der Mailsignatur sollten Sie alte Signaturen manuell oder via Skript entfernen. Weiterhin müssen Sie vor der Aktivierung der neuen Signaturen noch diverse Registry-Schlüssel (hier für Office 2003; andere Versionen weichen unter Umständen ab) ändern. Das Skript zur Generierung sollte mindestens die folgenden Bausteine beinhalten:

- Auslesen der AD-Attribute
- Setzen von Registrierungsschlüsseln
- Löschung alter Signaturen
- Erstellung der neuen Signaturen

Mit dem folgenden Skript lassen sich die Registrierungsschlüssel für das automatische Eintragen der neuen Signaturen ändern. Weiterhin wird dem Nutzer die Möglichkeit genommen, andere Signaturen auszuwählen und Word zum Verfassen von Mails zu nutzen.

```
Set objShell =
  CreateObject("WSkript.Shell")
objShell.RegWrite
  "HKEY_CURRENT_USER\Software\Micro-
  soft\Office\11.0\Common\MailSet-
  tings\NewSignature" , "XYZ GmbH
  (lang)"
objShell.RegWrite
  "HKEY_CURRENT_USER\Software\
  Microsoft\Office\11.0\Common\
  MailSettings\ReplySignature" ,
  "XYZ GmbH (kurz)"
objShell.RegWrite
  "HKEY_CURRENT_USER\Software\
  Microsoft\Office\11.0\Outlook\
  Options\Mail\EditorPreference" ,
  "65536", "REG_DWORD"
objShell.RegWrite
  "HKEY_CURRENT_USER\Software\
  Microsoft\Office\11.0\Outlook\
  Options\Mail\UseWordMail" , "0",
  "REG_DWORD"
```

Nach der Änderung der Registrierung können Sie dann mit dem Skript aus Listing 1 direkt die Dateien für die neuen Signaturen erstellen und befüllen. Zusätzlich müssen Sie zur Aktivierung und Zuweisung der Mailsignatur den in Listing 2 aufgeführten Quelltext ausführen. Dieser lässt sich auch dann anwenden, wenn ein Benutzer noch kein Mailprofil besitzt.

Fazit

Mit dem Einsatz der obigen Skripte ist es ohne Verwendung von Zusatzsoftware und mit wenig Aufwand möglich, aus Informationen aus dem Active Directory automatisch Signaturen zu generieren. Diese genügen den gesetzlichen Anforderungen und können flexibel auf spezielle Ereignisse hinweisen. Alle hier enthaltenen Beispieltexte, die in Textdateien abgelegt wurden, lassen sich auch mit einer Datenbank verwalten. Der Einfachheit halber haben wir in diesem Workshop darauf verzichtet. *(ln)*

```
Const HKEY_CURRENT_USER = &H80000001
strComputer = "."
dim Subkey
dim strKeyPath
dim strsubKeyPath
strSigName ="XYZ GmbH"
strProfile =""

If Not IsOutlookRunning Then
Set objreg = GetObject("winmgmts:" & "{impersonation-
   Level=impersonate}!\\" & strComputer &
   "\root\default:StdRegProv")
strKeyPath = "Software\Microsoft\Windows NT\" & "Cur-
   rentVersion\Windows " & "Messaging Subsystem\Profi-
   les\"
If strProfile = "" Then
objreg.GetStringValue HKEY_CURRENT_USER, strKeyPath,
   "DefaultProfile", strProfile
End If
myArraylong = StringToByteArray(strSigName&" (lang)" ,
   True)
myarrayshort = StringToByteArray(strSigName&" (kurz)"
   , True)
strKeyPath = strKeyPath & strProfile &
   "\9375CFF0413111d3B88A00104B2A6676"
objreg.EnumKey HKEY_CURRENT_USER, strKeyPath, arrPro-
   fileKeys
For Each subkey In arrProfileKeys
strsubkeypath = strKeyPath & "\" & subkey
objreg.SetBinaryValue HKEY_CURRENT_USER, strsubkey-
   path, "New Signature", myArraylong
objreg.SetBinaryValue HKEY_CURRENT_USER, strsubkey-
   path, "Reply-Forward Signature", myArrayshort
Next
Else
strMsg = "Please shut down Outlook before " & "running
   this Skript."
End If

Public Function StringToByteArray (Data, NeedNullTer-
   minator)

Dim strAll
strAll = StringToHex4(Data)
If NeedNullTerminator Then
strAll = strAll & "0000"
End If
intLen = Len(strAll) \ 2
ReDim arr(intLen - 1)
For i = 1 To Len(strAll) \ 2
arr(i - 1) = CByte ("&H" & Mid(strAll, (2 * i) - 1,
   2))
Next
StringToByteArray = arr
End Function

Public Function StringToHex4(Data)
Dim strAll
For i = 1 To Len(Data)
strChar = Mid(Data, i, 1)
strTemp = Right("00" & Hex(AscW(strChar)), 4)
strAll = strAll & Right(strTemp, 2) & Left(strTemp, 2)
Next
StringToHex4 = strAll
End Function
```

Listing 2: Aktivierung der Mailsignatur

Tipps zur PowerShell 2

Fernverwaltung mit der Kommandozeile

von Rolf Masuch

Zu Beginn der Fernadministration über die PowerShell 2 müssen Sie diese zunächst mit dem Befehl "winrm quickconfig" einrichten

Neben der besseren Unterstützung für das Active Directory stand bei der PowerShell v2 [1] die – in der ersten Version stark vermisste – Unterstützung des Remoting auf der Wunschliste vieler Administratoren. In diesem Workshop befassen wir uns näher mit der skriptgestützten Fernverwaltung von Servern von einem administrativen Arbeitsplatz aus.

Grundlage Windows Remote Management

Um in den Genuss der neuen Fernsteuerungsfunktionen zu kommen, benötigen Sie entweder Windows 7 oder Windows Server 2008 R2. Für die älteren Betriebssysteme Windows XP, Vista und Server 2003 inklusive R2 und auch Windows Server 2008 muss das "Windows Management Framework" [2] installiert sein. Neben der PowerShell v2 bringt dieses Framework, das in zehn Sprachen verfügbar ist, WinRM 2.0 und BITS 4.0 mit. Dabei ist WinRM die Microsoft-Implementierung des WS-Management-Protokolls [3]. Dies definiert als Simple Object Access Protocol (SOAP) den Informationsaustausch innerhalb einer IT-Infrastruktur. Die Implementierung von WinRM hat Microsoft als Webservice vorgenommen.

Zur Einrichtung der Kommunikation zwischen dem administrativen Rechner und den verwalteten Servern müssen Sie auf allen Systemen die PowerShell v2 installieren und starten und den Befehl *winrm quickconfig* eingeben. Dafür müssen Sie die PowerShell als Administrator starten. Falls Sie den Rechner noch nicht für die Fernverwaltung vorbereitet haben, wird der genannte Befehl die Startart des Dienstes WinRM auf "verzögerten automatischen Start" setzen, bei der Windows Firewall die notwendigen Ausnahmen konfigurieren und auf *HTTP://** den WinRM-Listener erstellen. Mit dem Cmdlet *get-service winrm* können Sie den Status des Dienstes überprüfen.

Die Cmdlets für die Fernsteuerung

Für die Verwaltung entfernter Rechner stehen Ihnen nun die Cmdlets und Befehle des Zielsystems zur Verfügung. Sollten Sie dabei versehentlich ein Programm mit einer grafischen Oberfläche starten, läuft der Prozess zwar an, aber die GUI steht Ihnen nicht zur Verfügung. Sollte das passieren, brechen Sie den Befehl mit "STRG+C" ab, um zur Shell des eigenen Rechners zurückzukehren. Befehle, die Sie in Ihrer lokalen Shell eingeben, werden gesammelt und komplett zum Zielsystem übertragen. Das Zielsystem gibt die Ausgaben der Cmdlets zurück, sobald sie verfügbar sind. Objekte werden dabei in XML umgewandelt und übertragen. Ihnen stehen die Cmdlets *Invoke Command, New PSSession, Enter PSSession, Exit PSSession, Get PSSession, Import PSSession* und *Export PSSession* zur Verfügung.

Das einfachste Cmdlet ist *Invoke Command*. Damit wird direkt die Eingabe zum über den Schalter *-Computername* angegeben Rechner umgeleitet. Natürlich können Sie auch eine Liste von Namen angeben. Dann kommen die Befehle auf allen angegebenen Rechnern zur Ausführung. Sollten Sie diesen Schalter vergessen, wird das Cmdlet lokal ausgeführt. Wenn Sie keinen weiteren Schalter angegeben haben, reagiert jedes Cmdlet wie gewohnt interaktiv und gibt Ihnen sofort die Ausgabe vom entfernten Rechner zurück. Dies beinhaltet auch eventuelle Fehlermeldungen. Mit dem Schalter *-Credential* haben Sie die Möglichkeit, andere Anmeldedaten an den entfernten Rechner zu übermitteln. Diese müssen aber Mitglied der Gruppe der Administratoren des Zielsystems sein.

In Kombination mit dem Cmdlet *New-PSSession* ist es möglich, die Informationen zum Zielsystem und die notwendigen Anmeldedaten in einer Variablen zu kombinieren. Diese Variable kann dann im Cmdlet *Invoke command* über den Schalter *-Session* übergeben werden. Das sieht dann so aus:

```
C:\PS>$s = new-pssession -computername server02
  -credential
  domain01\user01
C:\PS> invoke-command -session $s
  -scriptblock {get-culture}
```

Die gleiche Methodik können Sie bei den anderen Cmdlets aus der PSSession-Familie anwenden. Während Sie mit *New PSSession* die eigentliche Session erzeugen, können Sie mit *Get PSSession* alle Sessions der aktuellen Shell ermitteln, um sich dann mit *Enter PSSession* auf eine der zurückgegebenen Sessions zu verbinden. Sie verlassen diese wieder mit dem Cmdlet *Exit PSSession*.

Eine Sonderrolle kommt den letzten beiden Cmdlets *Import PSSession* und *Export PSSession* zu. Mit diesen können Cmdlets zwischen Sessions übertragen werden. Dabei ist zu beachten, dass die Session, aus der importiert wird, geöffnet bleiben muss. Hier ist der zusätzliche Schalter *-AsJob* zu empfehlen. Mehr Informationen gibt Ihnen die Hilfe der PowerShell mit dem Befehl *get help about_Jobs*.

Fazit

Das Thema Remoting ist in Version 1 der PowerShell dem Standpunkt "To ship is to choose" zum Opfer gefallen. Die Entwickler in Redmond hatten einfach keine Zeit mehr, diese Funktion einzubauen. Mit Version 2 wurde diese Lücke nun geschlossen. Die Entscheidung, die Implementierung auf Basis des WS-Managements Standards vorzunehmen, erleichtert die Integration in bestehende Windows-Umgebungen. Bei der Arbeit mit diesen Cmdlets gilt es aber, die Übersicht zu bewahren, um sich nicht zwischen den verschiedenen Sessions zu verzetteln. Um dies zu vermeiden, hilft ein gelegentlicher Blick auf die Eigenschaft "PSComputerName" der jeweiligen Session. *(ln)*

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.

Links

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

[2] Windows Management Framework
http://support.microsoft.com/kb/968929/

[3] Spezifikation des WS-Management Protokolls (DMTF)
http://go.microsoft.com/fwlink/?linkid=73965

Tipps & Tricks ohne Gewähr

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

Microsoft Windows

Wir nutzen unter **Windows 7** den Ordner **"Computer"** regelmäßig, um auf unsere Festplatten und Netzlaufwerke zuzugreifen. Für mich als Admin wäre es dabei hilfreich, wenn ich auch andere **Verknüpfungen zu Programmen und Dateien** hier ablegen könnte, die ich oft benötige. Gibt es hierfür eine Möglichkeit?

Sie können den Ordner "Computer" auch um eigene Verknüpfungen bereichern. Gehen Sie hierfür mit dem Dateiexplorer in das Verzeichnis "C:\Benutzer\{Benutzername}\AppData\Roaming\Microsoft\Windows\Network Shortcuts" und kopieren Sie Ihre gewünschten Verknüpfungen in diesen Ordner. Um jedoch auf das Verzeichnis zugreifen zu können, müssen Sie zunächst die Option aktivieren, versteckte Dateien und Ordner anzuzeigen. Dies erreichen Sie über den Menüpunkt "Extras / Ordneroptionen / Ansicht". Aktivieren Sie nun in der Liste unter "Versteckte Dateien und Ordner" die Option "Ausgeblendete Dateien, Ordner und Laufwerke anzeigen". Nachdem Sie Ihre Verknüpfungen im Verzeichnis abgelegt haben, erscheinen diese auch im Ordner "Computer". Entfernen können Sie diese, indem Sie sie aus dem Verzeichnis löschen oder unter "Computer" mit der rechten Maustaste anklicken und auf "Löschen" gehen. *(dr)*

Unter **Windows 7** fällt es relativ schwer, zwischen **geöffneten und geschlossenen Ordnern** zu unterscheiden, da sich die **Icons** ähneln. Gibt es eine Möglichkeit, die Ansicht im Dateiexplorer deutlicher zu gestalten?

Sie können über eine einfache Registry-Änderung die Icons der Ordner anpassen, so dass sich geschlossene und geöffnete Verzeichnisse deutlich voneinander unterscheiden. Starten Sie hierfür den Registry-Editor mit dem Befehl *regedit* und bestätigen Sie die Sicherheitsabfrage der Benutzerkontensteuerung. Nun öffnen Sie den Schlüssel "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons" und klicken mit der rechten Maustaste in das rechte Fenster. Gehen Sie nun auf den Menüpunkt "Neu / Zeichenfolge" und nennen Sie den neuen Wert vom Typ "REG_SZ" "4". Nun öffnen Sie den Wert mit einem Doppelklick und tragen `C:\Windows\System32\Shell32.dll,-137` ein. Damit werden die geöffneten Ordner mit einem neuen Symbol – in diesem Fall einem Stern – gekennzeichnet. Sie können auch andere Zahlen als die 137 verwenden. Um auch die geschlossenen Ordner anders zu kennzeichnen, legen Sie einfach einen neuen Wert mit dem Namen "3" an. Um die Original-Windows-Einstellung wieder herzustellen, löschen Sie die Werte. *(dr)*

Linux

Wenn ich **openSUSE 11.2** das erste Mal auf einem **x86-System boote**, erhalte ich eine **Fehlermeldung** vom Typ "err 11". Woran liegt das und was kann ich hier tun?

Es scheint ein Produktionsfehler von openSUSE 11.2 in der Box-Version zu sein, der die angesprochenen x86-Rechner mit 32 Bit betrifft. Dabei erscheint beim ersten Bootvorgang eine Fehlermeldung. Um nun weiterarbeiten zu können, drücken Sie die Return-Taste und geben Sie *Linux* ein. Bestätigen Sie diese Eingabe mit einem erneuten Return, anschließend sollte das System ohne Probleme starten. Dieser Fehler sollte auch nur beim ersten Bootvorgang des Betriebssystems auftreten. *(dr)*

Opera

Auf den öffentlich zugänglichen Internet-Terminals eines meiner Kunden ist als Browser **Opera 10** installiert. Mein Kunde hätte nun gerne, dass das Browserfenster bei **Nichtbenutzung des Rechners zurück zur Homepage** springt. Kann ich diese Einstellung mit Bordmitteln vornehmen oder muss ich hierzu auf Zusatztools oder selbst geschriebene Skripte zurückgreifen?

Wie Konkurrent Firefox auch, verfügt Opera in den neueren Versionen über eine erweiterte Konfiguration, die Sie nicht über die GUI, sondern über die Eingabe von *about:config* in der Adresszeile erreichen können. Hier begeben Sie sich nun in der Rubrik "Special" zum Eintrag "Go Home Time Out". An dieser Stelle lässt sich festlegen, nach wie vielen Sekunden der Inaktivität die Anzeige zur gesetzten Homepage zurückspringt. *(ln)*

Wie bei den meisten Browsern lässt sich mittlerweile ja auch bei Opera über die Eingabe der Tastenkombination "STRG+F" ein Suchfeld zum **Durchsuchen der aktuell angezeigten Webseite** aufrufen. Ich habe gehört, dass man diese Suche aber auch direkt über das **multifunktionale Suchfeld** in der Menüleiste vornehmen kann. Dies funktioniert bei mir aber nicht auf Anhieb, was gilt es hier zu beachten?

Um das Multifunktionssuchfeld auch zur Suche nach Textbausteinen auf der aktuell geöffneten Webseite zu nutzen, ist zunächst eine Änderung in den erweiterten Einstellungen nötig. Navigieren Sie nach der Eingabe von *about:config* unter der Rubrik "User Prefs" zum Eintrag "Use Integrated Search", setzen Sie dort ein Häkchen und klicken Sie auf "Speichern". Sobald Sie jetzt in dem Multifunktions-Suchfeld Buchstaben eingeben, markiert der Browser die Fundstellen farbig im Dokument. Die erste Übereinstimmung wird dabei grün hervorgehoben, alle weiteren in Gelb. *(ln)*

CITRIX

Über die **Verwaltungswerkzeuge** von Citrix lässt sich zwar die gesamte **XenServer-Umgebung administrieren**. Aber was ist mit der **Automatisierung oder Zeitsteuerung von Aufträgen**? Der Hersteller verweist da auf das Workflow Studio, das mit Sicherheit auch eines der besten Werkzeuge für diese Arten von Aufgaben ist, aber leider in der kostenfreien Version des XenServer nicht zur Verfügung steht.

Eine sehr pragmatische Alternative hierzu finden Sie im Installationsordner des Citrix XenCenter in Form des XE-Kommandozeilenbefehls. Dieser Befehl kann in einer Kommandozeile oder auch in einer beliebigen Batch- oder Scriptdatei verwendet werden, um Aktionen auf den XenServern auszuführen. Die Parameter sind hierbei die gleichen, wie sie auch auf der Konsole des XenServers selbst verwendet werden könnten. So ermöglicht etwa der Befehl

```
xe -s {Servername oder -IP} -u root
  -pw {Passwort des root} vm-list
```

das Anzeigen aller virtueller Systeme auf dem XenServer inklusive ihrer uuids (Eindeutigen Kennungen). Das Herunterfahren einer VM könnte somit über den Befehl

```
xe -s {Servername oder -IP} -u root
  -pw {Passwort des root} vm-shut-
  down uuid={Eindeutige Kennung der
  Ziel-VM}
```

herbeigeführt werden. Durch diese Befehle und Kombinationen hieraus lässt sich somit ein vollständiges Scripting der Umgebung realisieren. Weitere Informationen zu den Befehlen finden sich unter: *http://docs.vmd.citrix.com/XenServer/5.5.0/1.0/en_gb/reference.html#cli* *(Acocon/jp)*

Die **Citrix NetScaler-Appliance** komprimiert keine Informationen, die vom Backend-Server bereits komprimiert wurden. Wie können wir daher **Kompressions-Tasks** vom Backend-Server auf Citrix NetScaler übertragen?

Es ist mit Hilfe weniger manueller Schritte möglich, die Aufgabe der Datenkompression vom Backend-Server auf NetScaler zu übertragen. Damit lassen sich Ressourcen für Client Requests auf den Backend-Servern freischaufeln. Geben Sie folgenden Befehl ein, um eine Rewrite-Aktion zu generieren. Sie entfernt den Accept-Encoding-Header aus dem Client-Request, bevor der Request an den Backend-Server geschickt wird:

```
add rewrite action "no_svr_cmp" de-
  lete_http_header "Accept-Encoding"
```

Der Server geht nun aufgrund des fehlenden Accept-Encoding-Header im Request davon aus, dass der Client eine Kompression nicht unterstützt. Als Resultat schickt der Server unkomprimierte Inhalte. Starten Sie anschließend folgenden Befehl, um eine Rewrite-Policy für die Client-Requests zu generieren:

```
add rewrite policy "no_svr_cmp" true
  "no_svr_cmp"
```

Folgender Aufruf aktiviert die Richtlinie global:

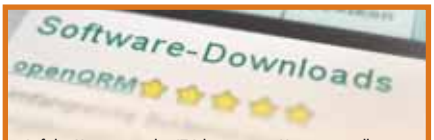
```
bind rewrite global " no_svr_cmp" 1
  NEXT -type REQ_DEFAULT
```

Darüber hinaus ist es möglich, diese Policy auch für virtuelle Server zu aktivieren. *(Citrix/dr)*

Tools

Es kommt immer wieder vor, dass der Computer selbst auf die einfachsten Befehle **träge reagiert**. Der erste Blick fällt wahrscheinlich auf die **Festplatten-LED**, um festzustellen, ob die Disk beschäftigt ist. Doch nicht immer ist diese LED am Rechner sichtbar, etwa bei Remote-Verbindungen. Hier hilft das Tool **DiskLED** weiter.

DiskLED ist eine kleine Windows-Anwendung, die in der Taskleiste angezeigt wird und flackert, wenn auf die Festplatte zugegriffen wird. Was DiskLED im Grunde tut, ist in regelmäßigen Abständen einen spezifischen Leistungsindikator abzufragen und den aktuellen Wert grafisch anzuzeigen. Das Schöne daran ist, dass es nicht auf die Festplattendaten beschränkt ist. DiskLED kann so konfiguriert werden, die Daten jedes beliebigen Leistungsindikators anzuzeigen. Leider ist ein LED-Display nur für das Anzeigen von Aktivitäten geeignet. Beim Umgang mit



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

vielen anderen Indikatoren ist eine andere Visualisierungs-Methode erforderlich. DiskLED hat hierfür einen zweiten Display-Modus, in dem die Auslastung auf einer Skala von 0 bis 100 angezeigt wird, ähnlich wie im Task-Manager bei der CPU-Auslastung. Bei Verwendung von Remote-Protokollen wie RDP oder ICA versucht man im Allgemeinen Bildschirm-Updates auf ein Minimum zu reduzieren. Aus diesem Grund ist die Häufigkeit, mit der DiskLED die Anzeige aktualisiert, frei konfigurierbar. *(Sepago/dr)*

Weitere Infos zu dem Tool finden sich unter http://blogs.sepago.de/tools/category/diskled/

Derzeit prägen zwei Entwicklungen viele IT-Landschaften: Virtualisierung und der zunehmende Einsatz von Consumer-Produkten in Netzwerken von Unternehmen. Beide Trends haben ihre Ursache in der Notwendigkeit, Kosten zu reduzieren. Und beide bergen dieselbe Gefahr: Sie setzen das Sicherheitsniveau von Unternehmensnetzwerken deutlich herab. Es gibt nur wenige **Sicherheitslösungen**, die in virtuellen Umgebungen laufen, und diese sind teuer und kompliziert zu verwalten. Wer solche Lösungen einsetzt, muss seine Anforderungen an die Sicherheit einschränken – und erhöht so die Verwundbarkeit seines Netzwerks. Genau das Gleiche gilt für den Einsatz von Consumer-Produkten in Unternehmensnetzwerken. Eine Alternative bietet die professionelle, aber kostenlose **Essential Firewall Edition** des Astaro Security Gateway.

Als frei verfügbare Edition des Astaro Security Gateway bietet die Essential Firewall die gleiche, einfach zu bedienende graphische Benutzeroberfläche und ist sowohl als **Software** als auch als **Virtual Appliance** erhältlich. Die Software bietet Anwendern folgende Features:

- Netzwerkdienste: Statisches Routing, Bridging, DNS-Server und -Proxy, DynDNS, DHCP-Server und -Relay, NTP-Unterstützung, QoS.
- Netzwerksicherheit: Stateful Packet Inspection Firewall sowie Network Address Translation (DNAT/SNAT/Masquerading).
- Fernzugriff: PPTP und L2TP über IPSec-Unterstützung.
- Protokollierung/Berichte: Vollständige Protokollierung auf lokaler Festplatte, Abfragen, Such- und Sortierfunktion, Live Logs, Echtzeitberichte für Hardware, Netzwerknutzung und -sicherheit, tägliche Gesamtberichte.
- Verwaltung: Webbasierte Oberfläche in lokaler Sprache, Setup Wizard, Backup & Restore der Konfiguration, Administrator-Benachrichtigungen, SNMP-Unterstützung, zentrale Verwaltung über Astaro Command Center (ebenfalls kostenlos). *(jp)*

Quelle: www.astaro.com/de/essential_firewall

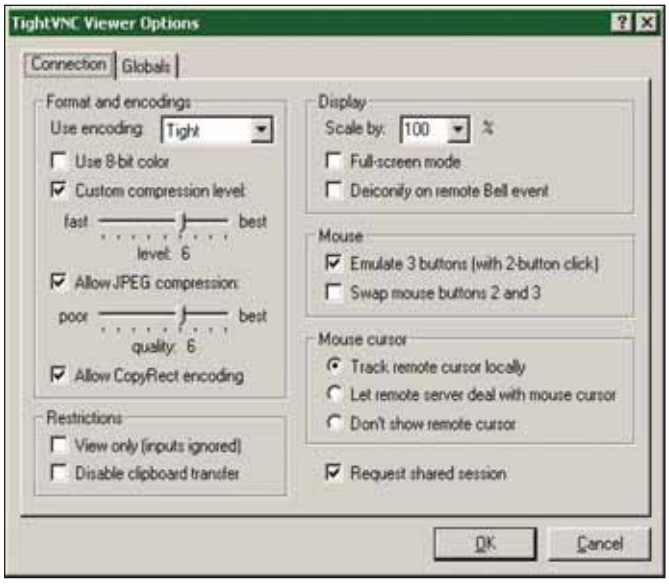
Die **Fernwartung** von Anwender-PCs ist gerade für Supporter, die auch entfernte Nutzer – etwa in Home Offices oder Außenstellen – betreuen, ein absolutes Muss. Werkzeuge hierfür bieten sich dem Administrator in großer Zahl an, besonderer Beliebtheit erfreuen sich dabei VNC-Werkzeuge. Wer nun allerdings Fernsupport über "dünne" WAN-Strecken leisten muss, der wird zu schätzen wissen, wenn das benutzte Werkzeug die Bandbreite durch Komprimierung der Grafik schont und so erlaubt, auch **im WAN zügig Support** zu leisten.

Die freie Software **TightVNC** hat sich genau auf diese Anforderung spezialisiert und liegt nun in der Version 1.3.10 vor. Darin haben die Entwickler einige Bugs entfernt und neue Features aufgenommen, so dass sich auf entfernte Rechner zugreifen lässt, um diese zu kontrollieren, zu supporten oder zu konfigurieren. Weitere Features des Werkzeugs sind:

- Dateitransfer zwischen Server und Rechner
- Konfigurierbare Kompressionsstufen
- Optionale Kompression von JPEGs
- Browserzugang per Java-Applet
- Unterstützt zwei Passwörter
- Sichere SSH-Verbindungen auf Unix-Rechnern
- Beschleunigung der Darstellung
- Echtzeiteinstellungen
- Unterstützt Loopbackverbindungen

Die Bedienung der Software gestaltet sich sehr einfach und sollte keinen Administrator vor unüberwindbare Hindernisse stellen. Sehr gut ist auch die Möglichkeit, die Übertragungsqualität individuell einzustellen. Unter Windows Vista läuft TightVNC derzeit jedoch nicht. *(jp)*

Quelle: www.tightvnc.com



Je nach Durchsatz der WAN-Verbindung kann der Administrator in TightVNC die Kompression der übertragenen Daten erhöhen oder senken, um jederzeit flott supporten zu können

Netzwerk-Monitoring für den Mittelstand

Netzwerkfehler auf dem Radar

von Thomas Timmermann

Die IT-Infrastruktur ist für mittelständische und kleine Unternehmen ein entscheidender Erfolgsfaktor. Um diese zu sichern, sind Virenscanner und Firewall heute Standard. Sie schützen jedoch nur vor Malware und Eindringlingen. Netzwerkleistung und -verfügbarkeit kann nur ein auf die Anforderungen abgestimmtes Monitoring gewährleisten. Worauf es hierbei ankommt, zeigen wir Ihnen in diesem Hintergrundbeitrag.

Individuelle Dashboards, WIN-GUI, Web-Interface, Mobile Interface: Zeitgemäße Monitoring-Tools überlassen die Wahl der Arbeitsumgebung dem User

Treten ungewöhnliche Aktivitäten auf, die von den Überwachungsparametern stark abweichen, kann dies bei einem permanenten Monitoring dem Netzwerk-Administrator nicht entgehen. Dies stellt eine zusätzliche und nicht zu unterschätzende Instanz im Sicherheitskonzept dar, die zur Früherkennung von beispielsweise Malware entscheidend beitragen kann. Der Einsatz eines geeigneten Netzwerk-Monitorings erspart den Verantwortlichen zudem wertvolle Zeit, die sie sinnvoll für andere Aufgaben einsetzen können. Wurde früher auf Insellösungen gesetzt, die einzelne Geräte oder Auslastungen umständlich überwachen, so behalten moderne, umfassende Lösungen das komplette Netz und die angeschlossene Umgebung permanent im Auge.

Die Lösung alarmiert sofort bei auftretenden Problemen oder Engpässen, und das über nahezu alle modernen Kommunikations-Tools. Schnell lassen sich so Fehlerquellen aufdecken und beseitigen. Die umfassende Transparenz der kompletten Umgebung senkt damit den Stressfaktor für jede IT-Abteilung stark. Sind die Überwachungsparameter richtig eingestellt und erfolgt keine Alarmierung, kann man davon ausgehen, dass alles in Ordnung ist. Darüber hinaus können der aktuelle Status und Detailinformationen jederzeit und nahezu von überall abgerufen werden.

Nicht zuletzt hilft Netzwerk-Monitoring dabei, Kosten einzusparen oder zu senken. Professionelle Monitoring-Systeme mit einem umfassenden Feature-Set sind zu einem attraktiven Preis-Leistungs-Verhältnis erhältlich und belasten das Budget der IT-Abteilung nur gering. Die erwähnte Zeitersparnis bedeutet auch finanzielle Einsparungen und somit ein weiteres Argument. Darüber hinaus führen die Möglichkeiten zur Optimierung von Netzwerken auf der Basis von langfristig gesammelten Ergebnissen und einer entsprechenden Trendanalyse oft zu einem weiteren, signifikanten Einsparpotenzial. So hilft beispielsweise die Ermittlung des tatsächlichen Bandbreitenbedarfs bei der gezielten Planung und Einteilung der Ressourcen. Die Einhaltung von Service Level Agreements (SLAs) kann zudem auf dieser Basis kontrolliert werden.

Grundlegende Funktionen

Bei der Wahl einer geeigneten Lösung steht der Verantwortliche vor der Frage, was das Monitoring leisten muss. Das Überwachen von Verfügbarkeit und Bandbreitenauslastung sind Kernfunktionen. Die gemessenen Ergebnisse werden dabei zuverlässig über gängige Protokolle erfasst und gespeichert. Dieser wichtige Vorgang ist die Grundlage für die im nächsten Schritt erfolgende Analyse. Dazu werden die gespeicherten Daten ausgewertet und in Form von Charts, detaillierten Berichten, Übersichten, Graphen und Listen aufbereitet. Eine langfristige Datenspeicherung und -auswertung lässt Trends erkennen, die eine Optimierung des Netzwerks anhand des tatsächlichen Bedarfs zulassen.

Im Vorfeld definierte Überwachungsparameter und Schwellenwerte liefern den Rahmen für die Alarmierung. Die Möglichkeit, Meldungen bei Überschreiten der festgelegten Werte oder bei Geräteausfällen über E-Mail, SMS, Instant Messaging, Syslog und SNMP Trap, HTTP Request oder Event log-Einträge empfangen sowie einsehen zu können, erlaubt dem Administrator maximale Mobilität. Dabei ist auch die Option wichtig, im Alarmfall eine EXE-Datei und darüber beispielsweise einen Reboot auszulösen.

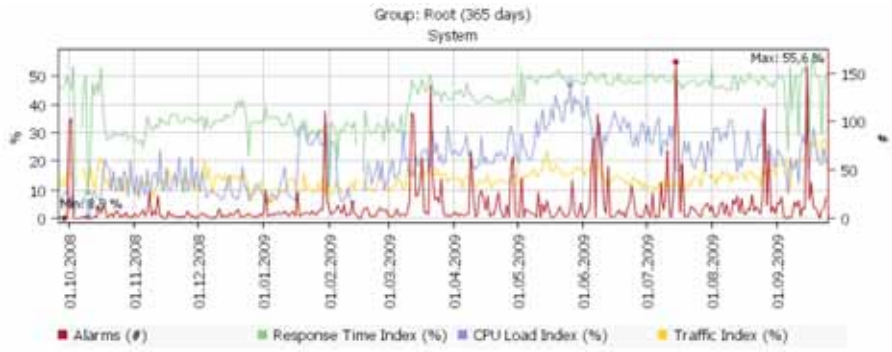


Bild 1: Behalten Sie die Daten auch über einen längeren Zeitraum im Auge, um Trends zu erkennen

Übersichtliche Ergebnisse

Für einen schnellen Einstieg in das Monitoring sind vorgefertigte Templates für gängige Hard- und Software-Produkte sehr hilfreich. Der Prozess an sich ist wahlweise automatisiert und/oder individualisiert einstellbar. Besonders praktisch für den Arbeitsalltag ist es, optional über die Möglichkeit eines Schnellüberblicks oder einer detaillierteren Expertenauswertung zu verfügen.

Eine visuell ansprechende und übersichtliche Aufmachung ist eine wichtige Grundlage für das Verständnis, was wirklich im Netz passiert. Sie ermöglicht den Überblick über den aktuellen Zustand mittels Graphen, Listen und Tabellen. Dabei ist der Detailgrad entscheidend: Die verschiedenen Anzeigemöglichkeiten sollten schnell und übersichtlich erreichbar sein wie etwa die Anzeige nach Stunden, Tagen oder Wochen. Des Weiteren ist es sinnvoll, die überwachten Geräte in Gruppen sortieren zu können und so übersichtlichere Anzeigen zu generieren.

Passende Kriterien definieren

Damit das Thema Monitoring im Unternehmen nicht aus dem Ruder läuft, ist es wichtig, die Kriterien und Anforderungen für das eigene Szenario im Vorfeld genau zu definieren. In der Praxis kann so beispielsweise eine Website auf ihre reine Verfügbarkeit hin überwacht werden. Gerade wenn eine Seite einen Shop beinhaltet, ist die Überwachung der Antwortzeit sinnvoll: Wie schnell ist die Webseite erreichbar? Im nächsten Schritt ist es interessant, nicht nur über die Startseite informiert zu sein, sondern auch über die angeschlossenen Unterseiten, Formulare und andere interaktive Elemente. Bei internationalen Web-Auftritten ist zudem die weltweite Verfügbarkeit der Webseite ein Kriterium. Wie schnell ist die Seite für den Nutzer in den USA, in Spanien oder in Japan zu öffnen?

Ein anderes essenzielles Thema ist die E-Mailkommunikation. Bei einem Ausfall sind heute viele wichtige Arbeitsprozesse blockiert. Das einfachste Überwachungsszenario sieht vor, die Verfügbarkeit von POP3 und des IMAP-Servers im Auge zu behalten. Immer wieder kann es vorkommen, dass E-Mails gar nicht oder nur verzögert ankommen. Hier kann die Überwachung der kompletten Ende-zu-Ende-Zustellung von E-Mails weiterhelfen. Dazu wird in regelmäßigen Abständen eine Test-E-Mail versendet und genau protokolliert. So ist die Überprüfung der Verfügbarkeit und der Performance des gesamten Übertragungsprozesses möglich.

Das sind nur zwei Beispiele für sinnvolle Maßnahmen im Rahmen von Netzwerk-Monitoring. Schnell ist eine Vielzahl von Sensoren eingerichtet, die aber auch genau so schnell eine unübersehbare Informationsflut liefern. So kann beispielsweise bei einem Switch mit 100 Ports jeder Port auf Bandbreite überwacht und protokolliert werden. Allerdings ist das nicht wirklich sinnvoll: In der Regel ist man ja nur an den Ports interessiert, die die meiste Bandbreite brauchen, und an den Ursachen dafür. Hier unterstützen als nützliches Feature sogenannte Toplists den Verantwortlichen. Diese überwachen via NetFlow oder Packet Sniffing den kompletten Switch, werten aber nur die verbrauchsstärksten Ports aus.

Wahl der richtigen Lösung

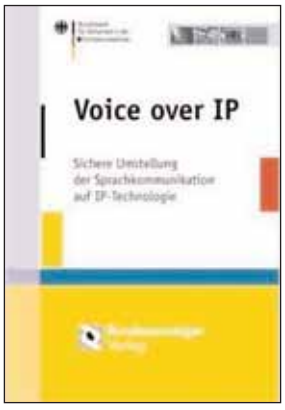
Netzwerk-Monitoring-Software sollte einfach zu installieren sein. Sie sollte über eine intuitiv zu bedienende Benutzeroberfläche verfügen, die flexibel und konfigurierbar ist. Idealerweise kann der User dabei zwischen Varianten wie Web-, Windows- und Mobile-Interface wählen. Eine automatische Netzwerkerkennung nach Installation ist Stand der Technik und darf nicht fehlen.

Netzwerke sind eine äußerst heterogene IT-Landschaft mit unterschiedlichsten Geräten und Softwarelösungen. Eine ideale Monitoring-Lösung sollte die meisten gängigen Protokolle wie beispielsweise SNMP, WMI, Packet Sniffing, NetFlow, HTTP oder FTP beherrschen, um aktuellen wie auch kommenden Anforderungen gerecht zu werden. Eine Frage, die den Entscheidungsprozess zudem wesentlich beschleunigen kann, lautet: Ist eine aktuelle Testversion sofort verfügbar und ist diese zur Evaluierung uneingeschränkt nutzbar? Wichtig in diesem Zusammenhang ist auch, ob die IT-Abteilung sie danach direkt mit allen bereits vorgenommenen Einstellungen in den Produktivbetrieb übernehmen kann.

Eine übersichtliche, einfach aufgebaute Lizenzierung sowie eine Preispolitik ohne versteckte Kosten schafft Transparenz. Eine einfache und kostengünstige Upgrade-Möglichkeit bei steigenden Anforderungen bietet Zukunftssicherheit. Das Stichwort an dieser Stelle ist "Mitwachsen". Eine geeignete Lösung ist in der Lage, über ein einfach durchzuführendes Upgrade an die neuen Anforderungen angepasst zu werden. Nicht zuletzt ist ein erreichbarer kompetenter Support vom Hersteller in der jeweiligen Landessprache ein nicht zu unterschätzender Faktor. *(dr)*

Thomas Timmermann ist Manager Sales & Marketing bei der Paessler AG.

Voice over IP



Die meisten Administratoren merken erst bei der Lektüre von Büchern wie "Voice over IP" vom Bundesamt für Sicherheit in der Informationstechnik (BSI), wie viele Aspekte die Sicherheit bei VoIP-Anwendungen berührt. Das Büchlein ist mit etwa 170 Seiten zwar recht dünn, konzentriert sich aber ausschließlich auf die Absicherung der Kommunikationsinfrastruktur. Zielgruppe sind erfahrene Administratoren oder technisch orientierte CIOs, die sich vor der Einführung von VoIP im Unternehmen über alle Risiken informieren wollen. Der Ton klingt ein wenig nach Beamtendeutsch. Das verwundert nicht weiter, wenn man weiß, dass das Buch unter der Federführung des BSI steht und das Ergebnis einer Studie zur Sicherheit von Voice over IP ist.

Die Autoren vermeiden durch die Konzentration auf den Sicherheitsfokus langwierige Grundlagenerklärungen. Das erste Kapitel befasst sich zwar mit den Komponenten einer VoIP-Infrastruktur, aber schon hier orientieren sich die Autoren in Richtung Sicherheit. In den folgenden Kapiteln liefert das Buch ein sinnvolles Gerüst, wie eine fundierte Bewertung und Umsetzung von VoIP-Sicherheit aussehen könnte. Nach der Bedrohungsanalyse werden mögliche Sicherheitsmaßnahmen aufgezählt. Derart vorbereitet, geht es mit dem Netzdesign weiter. Die gut erklärten NAT-Konzepte fallen dabei ins Auge, hier werden die Unterschiede und ihre Bedeutung für VoIP mit Grafiken unterlegt. Weiter geht es mit den Rahmenbedingungen und gesetzlichen Vorschriften. Ein Kommunikationsmittel, über das sensible Daten transportiert werden, muss natürlich entsprechenden Regulatorien genügen. Gerade hier wird das Buch den Erwartungen allerdings nicht gerecht – die knapp zwei Seiten mit Verweisen auf das Fernmeldegeheimnis und Datenschutz hätten sich die Autoren auch sparen können. Nützlicher sind die Einsatzszenarien, in denen sowohl die grundlegende Struktur des VoIP-Netzwerks beschrieben als auch per Checkliste mögliche Bedrohungen und Sicherheitsmaßnahmen aufgelistet werden.

Fazit: Abgesehen vom sehr schwachen Kapitel mit den gesetzlichen Bestimmungen erfüllt das Buch die Erwartungen. Angelehnt an die IT-Grundschutzkataloge werden die Bedrohungen und mögliche Maßnahmen kurz, aber ausreichend beschrieben. *Elmar Török*

Autor:	Bundesamt für Sicherheit in der Informationstechnik BSI
Verlag:	Bundesanzeiger Verlag
Preis:	32 Euro
ISBN:	978-3-89817-539-1
Bewertung:	★★★½☆

Der Mac im Unternehmen

Während sich die schicken Rechner von Apple früher auf den kreativen Bereich konzentrierten, scheinen die Grenzen mittlerweile aufzuweichen. Autor Steffen Hellmuth leistet in seinem Buch "Der Mac im Unternehmen" weitere Überzeugungsarbeit für die Akzeptanz von Mac und Co. Sein Buch ist eine, stellenweise kuriose, Mischung aus Hands-On für Administratoren und betriebswirtschaftlicher Betrachtung. Den Anfang machen Pro und Contra-Vergleiche von Mac- und Windows-Welt. Hellmuth bemüht sich um Objektivität, aber natürlich ist die Vorliebe des Autors für Apple deutlich spürbar. Dieses erste Kapitel sorgt beim Leser eigentlich für den falschen Eindruck: es geht hier im Prinzip um einen Crash-Kurs für Windows-Admins. Immer wieder werden Einstellungsdialoge und typische Einsatzszenarien von Vista und OS X gegenübergestellt. Das hat allerdings keinen Besser/Schlechter-Vergleich zum Ziel, sondern soll dem Windows-Admin zeigen, wie diese Aufgaben beim Mac zu lösen sind.

Der Schwerpunkt des Buchs liegt auf dem Umgang mit Macs als Clients in einem Netzwerk. Dass dabei auch Office-Software und Programme zur Bildbearbeitung erwähnt werden, gehört zum etwas uneinheitlichen Gesamtbild. Wichtiger sind die Kapitel, in denen das Clientmanagement mittels eingebauter Tools oder Software von Drittherstellern beschrieben wird. Oft greift der Autor auch typische Prozeduren wie das Backup auf und zeigt anhand von Bordmitteln, wie der Mac damit umgeht. Das letzte Kapitel ist vollständig der Fehlersuche gewidmet. Gerade Admins, die ihre Hauptbeschäftigung in der Windows-Welt haben, finden hier sehr viele Hinweise, um einen Mac möglichst schnell wieder flott zu bekommen, vom eingebauten Texteditor über die Systemdienste bis hin zur Datenrettung.

Fazit: Steffen Hellmuth gebührt ein dickes Lob für die zahlreichen Hands-On-Infos. Administratoren, die sich zum ersten Mal mit einem Mac beschäftigen, erhalten einen gut geschriebenen Crash-Kurs. Auf die Investitionsanalyse pro Mac hätte der Autor allerdings verzichten können. *Elmar Török*

Autoren:	Steffen Hellmuth
Verlag:	Mandl&Schwarz
Preis:	34,80 Euro
ISBN:	978-3-939685-15-9
Bewertung:	★★★★☆

www.codeplex.com
Fundgrube

Die von Microsoft seit 2006 betriebene Hostingplattform codeplex.com soll teambasiertes Arbeiten an quelloffenen Anwendungen unterstützen und die so erstellten Projekte allen Interessenten zur Verfügung stellen. Diese konzeptionelle Nähe zum Open Source-Gedanken sowie die direkte Konkurrenz zum etablierten sourceforge.net ist vielen Vertretern der GNU Public License ein Dorn im Auge – vor allem, weil Microsoft die Verwässerung des Open Source-Lizenzmodells vorgeworfen wird. Doch unbeschadet dieser Debatte stellt codeplex dem Administrator mittlerweile eine ganze Reihe von interessanten Werkzeugen zur Verfügung.

Dazu stellt die Website den dort tätigen Entwicklern zunächst einmal eine ganze Reihe von Werkzeugen zur Verfügung, um Team-basiertes Arbeiten zu ermöglichen, wie etwa ein Wiki, eine Versionsverwaltung und einen Bug-Tracker. So entstanden seit 2006 rund 10.000 Softwareprojekte. Dabei ist der Schwerpunkt entwicklerseitig zweifellos bei den Microsoft-eigenen Entwicklungswerkzeugen wie das .NET-Framework oder ASP.NET.

Aber wie eingangs erwähnt, ist codeplex.com durchaus auch eine lohnenswerte Fundgrube für den Systemadministrator. So wird der Exchangeverantwortliche beispielsweise mit dem "CatchAllAgent" versorgt, der es erlaubt alle eingehenden Mails, die an unbekannte Adressaten gerichtet sind, an eine dezidierte Adresse weiterzuleiten. Eine Funktion, die weder Exchange 2007 noch 2003 erlauben und die wir Ihnen in einer unserer kommenden Ausgaben noch ausführlich vorstellen werden. Hochinteressant sind sicher auch eine ganze Reihe von Hyper-V-Verwaltungstools oder eine PowerShell-Management-Bibliothek für Hyper-V. So richtig aus dem Vollen schöpfen kann der Sharepoint-Verantwortliche: codeplex.com listet für dieses Stichwort annähernd 1.000 Entwicklungsprojekte – von der Sharepoint-Programmierung über die Verwaltung bis hin zu Lernprogrammen.

Ein wenig in dieser Fundgrube zu stöbern lohnt sich also auf jeden Fall. Auch wenn das eigentliche Suchen auf der Seite komfortabler sein könnte, denn eine strukturierte Übersicht der Projekte nach Themen sucht der Besucher vergeblich. Über die Tagcloud und die Suchfunktion ist zwar jedes Projekt auffindbar, aber eine Kategorisierung – um etwa unter "Netzwerk" und dort unter "Monitoring" nach einer Auswahl von Tools zu suchen, wie von sourceforge.net bekannt – fehlt leider. *(jp)*

Codeplex hat einige wertvolle Fundsachen zu bieten

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

Die Bedeutung von Kennzahlen in der IT-Sicherheit

Gesetzliche Anforderungen und eigene Unternehmens-Regeln machen diverse Vorgaben zur Informationssicherheit. Bei der Ermittlung des aktuellen Sicherheitszustandes einer Infrastruktur und bei der längerfristigen Planung spielen Kennzahlen eine wichtige Rolle. Allerdings bleiben diese ohne ständige Aktualisierung und genaue Überprüfung ein zahnloser Tiger. In unserem Fachartikel gehen wir darauf ein, wie die regelmäßige und automatisierte Ermittlung der wichtigsten Kennzahlen die IT-Security erhöht.
www.it-administrator.de/themen/sicherheit/fachartikel/69336.html

Anwenderbericht: Clientmanagement bei der Playcom GmbH

Mit ihren 50 Mitarbeitern zählt die Playcom Software Vertriebs GmbH sicher nicht zu den großen Konzernen. Doch in seiner Branche gehört der Großhändler von Computer- und Videospielen zu den Top-3-Anbietern. Unser Anwenderbericht zeigt, welchen Herausforderungen sich das Unternehmen beim Management der Clients gegenübergestellt sieht und welche Tools der Händler zur automatisierten Installation von Betriebssystemen und Software sowie zur Remote-Wartung einsetzt.
www.it-administrator.de/themen/server_client/fachartikel/69337.html

Checkliste zur Rechenzentrums-Sicherheit

Gebäudesicherheit, Klimatisierung, Effizienz, Skalierbarkeit, Störungsmanagement – dies sind nur einige der Kriterien, die bei der Konzeption eines sicheren Rechenzentrums Beachtung finden müssen. Es bedarf eines ganzheitlichen Konzepts, um eine den Bedürfnissen entsprechende Sicherheit zu gewährleisten. Um die eigenen Ansprüche besser evaluieren zu können, stellen wir eine Checkliste zur Rechenzentrums-Sicherheit bereit.
www.it-administrator.de/themen/sicherheit/fachartikel/69338.html

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

»Im Arbeitsalltag ist Problemlösungskompetenz gefragt«

Benedikt Kiesenhofer (21) arbeitet beim österreichischen Beratungsunternehmen Software Quality Lab als Software-Tester und IT-Administrator. Das Unternehmen optimiert für seine Kunden die Effizienz, Qualität und Sicherheit im Bereich der Software-Entwicklung und der IT-Prozesse. An vier Standorten wird für diese Aufgaben eine kleine, aber feine IT-Infrastruktur bereitgehalten, die Benedikt Kiesenhofer gemeinsam mit einem Kollegen administrativ betreut.

Welche Ausbildung haben Sie gemacht?

Ich habe eine Ausbildung an der höheren Lehranstalt für Kommunikations- und Mediendesign im oberösterreichischen Freistadt erfolgreich abgeschlossen. Anschließend folgte die Weiterbildung zum ISTQB Certified Tester.

Warum sind Sie IT-Administrator geworden?

Schon in meiner Jugend habe ich privat kleinere Netze aufgebaut und diese individuell auf die Benutzer abgestimmt. Ich trage gerne die Verantwortung für die Infrastruktur eines Unternehmens. Erst wenn diese stabil ist, wird ein wirtschaftlich effizientes Handeln möglich.

Welche IT-Umgebung betreuen Sie aktuell?

In unserem kleinen Zwei-Mann-Team bin ich Software-Tester und IT-Administrator in Personalunion. Wir betreuen die Infrastruktur an vier Standorten in Langenstein, Linz, Wien und Graz. Aktuell sind wir für sieben feste sowie mehrere virtuelle Server verantwortlich und betreuen auch unsere VoIP-Installation. Darüber hinaus schauen wir nach den Arbeitsplätzen von aktuell 13 Mitarbeitern. Da unser Unternehmen momentan auf Expansionskurs ist, wird deren Zahl aber demnächst wohl auf 15 bis 16 Mitarbeiterplätze anwachsen.

Welches Netzwerk- und Systemmanagement setzen Sie ein?

Wir verwalten unsere Clients mit den integrierten Tools der eingesetzten Microsoft-Produkte. Für die virtualisierten PCs und Server setzen wir auf VMware.

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

Die größte Herausforderung ist es, Tag für Tag alle Kollegen zufrieden zu stellen. Es kommen täglich neue Herausforderungen auf mich zu, die gelöst und umgesetzt werden müssen. Hier ist Problemlösungskompetenz gefragt.

Geburtstag: 14.03.1988
Familienstand: ledig
Hobbys: HiFi, Autos, private Netzwerke, Kochen

Benedikt Kiesenhofer, IT-Administrator

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Wir werden am Standort Linz demnächst in ein neues Bürogebäude umziehen. Dort müssen wir dann die IT-Infrastruktur neu einrichten. Zudem ist die Einführung eines neuen ERP-Systems geplant.

Was macht Ihnen an Ihrem Job am meisten Spaß?

Jeder Tag birgt neue Herausforderungen. So gilt es auch, Probleme, die selten oder vielleicht sogar nur einmal auftreten, zufrieden stellend zu lösen. Dazu müssen Erweiterungen an der Unternehmensinfrastruktur geplant und umgesetzt werden. Kein Tag ist wie der andere.

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

Routinearbeiten, wie das Führen von Listen, Aufzeichnungen oder Dokumentationen sind nicht so mein Fall, müssen aber erledigt werden.

Was tun Sie für Ihre Fort- und Weiterbildung?

So oft es möglich ist, besuche ich Kurse und Seminare. Informationsquellen sind aber auch diverse Fachzeitschriften, Blogeinträge oder Newsletter sowie unsere Software-Quality-Days.

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

Im Rahmen eines Projekts habe ich eine Datenbank zerschossen. Die Wiederherstellung war dafür meine Strafarbeit.

Was war Ihr größter Erfolg als IT-Administrator?

Das ist eigentlich mein momentaner Job, denn als relativer Anfänger darf ich hier bereits als eigenständiger IT-Administrator arbeiten. Im Rahmen dieser Tätigkeit habe ich die Teilverantwortung für die geschäftskritische Infrastruktur. Darauf bin ich stolz.

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

Es ist mir noch kein Fall untergekommen, den ich in diese Kategorie einordnen kann. Schwere Fehler sollten von einem gut konfigurierten System auch gar nicht zugelassen werden. Dafür bin ich ja da.

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

Intern ist das die Expansion des Unternehmens und der dazugehörenden Infrastruktur. Extern sind das in meinen Augen die Themen Virtualisierung und Sicherheit.

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 2/10 erscheint am 5. Februar 2010

Schwerpunktthema:

Sicherheit von Webservern und -applikationen

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

Unsere Ausgabe im **März** steht unter dem Schwerpunkt **Rechenzentrumsausstattung**.
In unserer Test-Rubrik nehmen wir die Tandberg Virtual Tape Library unter die Lupe. In einem unserer Workshops lesen Sie außerdem, wie Sie Hyper-V-Umgebungen fernwarten.

Als Schwerpunkt im **April** folgt dann das Thema **Desktop-Virtualisierung**.

***Im Test:* Webapplication-Firewall phion airlock**

***Workshop:* Webserver Apache absichern**

***Workshop:* DNS-Fehler finden und beheben**

***Workshop:* Schwachstellen in PHP**

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

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

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

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

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

Autoren dieser Ausgabe
Petra Adamik, Thomas Bär, Sascha Giebelhausen, Thomas Gronenwald, Ulli Hankeln, Jürgen Heyer, Thomas Joos, Sandro Lucifora, Rolf Masuch, Henning Scherf, Thomas Timmermann, Elmar Török

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

Es gilt die Anzeigenpreisliste Nr. 7 vom 01.11.2009

LAC/2008

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

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

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

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

Erscheinungsweise
monatlich

Bezugspreise
Einzelheftpreis: € 12,60
Jahresabonnement Inland: € 135,-
Studentenabonnement Inland: € 67,50
Jahresabonnement Ausland: € 150,-
Studentenabonnement Ausland: € 75,-
Jahresabonnement Inland mit Jahres-CD: € 144,84
Studentenabonnement Inland mit Jahres-CD: € 77,34
Jahresabonnement Ausland mit Jahres-CD: € 159,84
Studentenabonnement Ausland mit Jahres-CD: € 84,84
E-Paper-Einzelheftpreis: € 9,45
E-Paper-Jahresabonnement: € 99,-
E-Paper-Studentenabonnement: € 49,50
Jahresabonnement-Kombi mit E-Paper: € 168,-

(Studentenabonnements nur gegen Vorlage einer gültigen Immatrikulationsbescheinigung)

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

Internet
www.it-administrator.de

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
80802 München

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

(zugleich Anschrift aller Verantwortlichen)

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

Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

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

ISSN
1614-2888

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

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

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

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

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

INSERENTENVERZEICHNIS
Die Ausgabe enthält eine Teilbeilage der Firma ppedv.

Das IT-Administrator Komplettprogramm!!!

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

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

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

Als bestehender Jahresabonnent können Sie hier upgraden:

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

Oder Sie sind Neukunde? Hier können Sie bestellen:

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

www.it-administrator.de

Heinemann Verlag
Im Dialog mit Spezialisten.

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

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

LANCOM

. . . connecting your business

Made
in
Germany

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.

INNOVATIONSPREIS-IT
2009
mittelstand
STORAGE | NETZWERKE

LANCOM OAP-310agn

CeBIT
HANNOVER
2.–6.3.2010
HALLE 13
STAND C28

LANCOM
Systems

www.lancom.de