IT-ADMINISTRATOR.DE

02/2009

€ 12,60 ISSN 1614-2888

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

Rechenzentrumsausstattung und -überwachung

LANCOM

Network Connectivity · Wireless LAN

. . . connecting your business

Made in Germany

Sie denken weiter. Kann Ihre Technik das auch?

Mit **VPN-Lösungen von LANCOM** kennt Ihr Business keine Grenzen. Effektiv und sicher vernetzen Sie alle Standorte Ihres Unternehmens – weltweit. Ob das Lager um die Ecke, das Home Office des Außendienstlers oder die Filiale im Ausland – Niederlassungen und mobile User sind mit wenigen Clicks voll eingebunden. In Mittelstand und Großkonzern, in Behörden und Institutionen. Zuverlässig, einfach und absolut sicher. **Über alle Breitbandanschlüsse, WLAN oder UMTS**. Für Sprache und Daten.

CeBIT
HANNOVER
3.– 8.3.2009
HALLE 13
STAND C34

Professionelle **VPN Gateways**, **Router** und **Clients** vom deutschen Marktführer. Exzellenter Service, kostenlose Updates und Investitionsschutz inklusive.

LANCOM Systems

www.lancom.de

EDITORIAL

IT-Fabrik

Liebe Leser,

es ist 9 Uhr an diesem 5. Februar 2014, als Systemadmin Matthias H. sich im Rechenzentrum eincheckt und seine 8-Stunden-Schicht antritt. Monoton summen Heerscharen von Servern im Duett mit der Lüftung. Matthias H. sitzt gebeugt über eine kleine Instrumententafel, die ihm den Zustand des kompletten RZs anzeigt. Alle Lampen sind heute grün. Die Lampen sind immer grün, seit vor drei Jahren die selbstheilenden Betriebssyteme eingespielt wurden. Alle 15 Minuten muss Matthias H. den "Life-Button" drücken um dem RZ zu signalisieren, dass er noch wohlauf ist. Den Höhepunkt einer ereignislosen Schicht bildet das kurze Aufflackern zahlreicher LEDs, die ein automatisches Switchover von 75 Servern ankündigen. Um 17 Uhr endet die Schicht.

Nun, liebe Leser, ganz so monoton wie bei unserem kleinen Blick in die Zukunft dürfte Ihr Arbeitsplatz auch in fünf Jahren nicht aussehen. Doch "IT-Fabrik", "RZ-Automatisierung" oder "Orchestration" sind nach Meinung führender Analysten der Schritt in Richtung Industrialisierung der IT. Dass aber solche RZs, die bei Bedarf automatisch Ressourcen – Storage, Rechenleistung oder neue Applikationen – bereitstellen oder selbstständig auf Sicherheitsereignisse reagieren, sogar in weniger als fünf Jahren Realität sein könnten, zeigt Ihnen unsere Februar-Ausgabe.

Insbesondere unser Test des "Bladelogic Operations Manager" ab Seite 12 führt eindrucksvoll vor Augen, was RZ-Werkzeuge der neuesten Generation leisten. Der Hersteller verspricht, dass sich der Zeitaufwand für die von seiner Lösung übernommenen Aufgaben im RZ um satte 97 Prozent reduziert. Die Frage, ob dieser Wert nun 97, 98 oder nur 96 Prozent beträgt, lässt auch unser Test unbeantwortet. Dass sich jedoch ein beeindruckender Grad an IT-Industrialisierung schon heute erreichen lässt, führt Ihnen nicht nur dieser Beitrag, sondern auch ein Blick auf Citrix' neue Lösung "Workflow Studio" ab Seite 42 vor Augen, mit der sich komplette Abläufe in der IT automatisieren lassen.

Doch keine Angst: Langweilig wird Ihnen bestimmt auch in der Zukunft nicht! Denn es rücken andere Skills in den Mittelpunkt Ihrer Tätigkeit, wie etwa der Artikel zum Monitoring (Seite 52) aufzeigt: Auch in Zukunft müssen Administratoren beispielsweise festlegen, welche Indikatoren der jeweiligen Ressourcen überwacht werden sollen und daraus eine Planung für die Zukunft ableiten. Dies kann Ihnen kein Werkzeug abnehmen. Viel Vergnügen beim Lesen, Ihr

John Pardey
Chefredakteur IT-Administrator

Schmidt's LogInventory

keep IT simple

www.loginventory.com

INHALT

IT-Administrator – Ausgabe Februar 2009

Rechenzentrumsausstattung und -überwachung

Im Test: Toolhouse Toolstar*testWIN 1.35

Sporadische Hardwarefehler sind in der Regel schwer zu finden, vor allem wenn sie nur selten auftreten und nicht reproduzierbar sind. Toolstar*testWIN bietet die Möglichkeit, jegliche Hardware unter Windows gezielt und auf Dauer zu testen, um so einem vermuteten Fehler schneller auf die Schliche zu kommen. IT-Administrator hat einige Systeme intensiv mit dem Tool geprüft, um sich einen Eindruck von der Software zu verschaffen.

Seite 20

iSCSI-SAN und Virtualisierung

Ein hervorstechendes Merkmal bei der Virtualisierung ist die Migration: Ein Gastsystem lässt sich im laufenden Betrieb von einem physikalischen Server auf einen anderen unterbrechungsfrei verschieben. Muss der Administrator einen Server zu Wartungs- oder Erweiterungszwecken herunterfahren, werden die laufenden virtuellen Maschinen auf einen anderen Server verschoben, um dort ihren Dienst ohne Unterbrechung zu verrichten. Dazu ist jedoch ein SAN Voraussetzung. Unser Workshop zeigt, wie Sie iSCSI-SANs einsetzen, um das Potenzial der Virtualisierung voll zu entfalten.

Seite 36

Anomaly Detection-Lösungen

Die Leistungsfähigkeit von Software ist immer dann gefährdet, wenn Anomalien und Unregelmäßigkeiten innerhalb der Netzwerk-Infrastruktur auftreten. Eine Herausforderung für jeden Systemadministrator ist es, den Überblick zu behalten. Hier haben sich Werkzeuge zur Erkennung von Unregelmäßigkeiten, sogenannte "Anomaly Detection"-Lösungen, bewährt. Sie versprechen eine Kontrolle der Verhaltensänderungen in Echtzeit. In diesem Beitrag gehen wir auf die Grundlagen dieses Frühwarnsystems ein und skizzieren, auf welche Unregelmäßigkeiten diese reagieren.

Seite 60

Speicher-Sixpack

QNAP bringt mit dem **TS-639 Pro Turbo NAS** einen Netzwerkspeicher auf den Markt, der sich sowohl als **NAS** als auch als **iSCSI-Zielserver** einsetzen lässt. Dabei steht eine Thin Provisioning-Funktion zur Verfügung, die es erlaubt, Kapazitäten in einem iSCSI-LUN unabhängig von der physischen Volumenkapazität zuzuweisen. Das Gerät verfügt über sechs Festplatteneinschübe. Jeden dieser Slots kann der Storage-Admin mit einer SATA I/II-Platte mit maximal 1,5 TByte Speicherkapazität bestücken, womit dem System nominell **bis zu 9 TByte** zur Verfügung stehen. Im Regelfall wird sich der zur Verfügung stehende Speicherplatz je nach Wahl des RAID-Modus jedoch verringern. Das Gerät unterstützt neben dem JBOD-Modus RAID 0, 1, 5, 5+ Spare und 6. Die Magnetspeicher lassen sich im laufenden Betrieb wechseln. Eine volumenbasierte 256-Bit-AES-Verschlüsselung schützt Daten vor unbefugtem Zutritt. Fünf USB- und zwei eSATA-Ports machen den Speicher nach außen hin erweiterbar, während unter der Haube ein Intel-Prozessor mit 1,6 GByte und 1 GByte DDRII-RAM für die nötige Rechenleistung sorgen. Der Preis des plattformunabhängigen Systems hängt von der Größe der verbauten Harddisks ab. Mit sechs Platten à 500 GByte kostet das NAS rund 1.260 Euro, während die Maximal-Bestückung mit 1,5-TByte-Platten mit 1.850 Euro zu Buche schlägt. *(ln)*

QNAP: www.qnap.com/de/

Das "TS-639 Pro Turbo NAS" lässt sich auch als iSCSI-Zielserver einsetzen

Der Wireless N-Router "DIR-655" von D-Link bindet USB-Geräte drahtlos an

Drahtlose USB-Anbindung

D-Link ermöglicht mit seiner SharePort-Technologie Nutzern des Wireless N GBit-Routers **DIR-655** nun den **drahtlosen Zugriff auf USB-Drucker, -Scanner und -Multifunktionsgeräte** im Netzwerk, inklusive deren erweiterten Funktionsumfang. Die USB-Geräte lassen sich dank dieser Technik nun direkt an den Wireless N-Router anschließen und von jedem Ort im Netzwerk aus ansteuern. Die zugehörige Software, die auf den angebundenen Desktop-PCs und Notebooks im WLAN beziehungsweise LAN installiert werden muss, zeigt die verfügbaren USB-Geräte auf den Clients an. Der USB-Port des Routers DIR-655 wird dann zu den jeweiligen PCs und Notebooks getunnelt, sodass eine Vielzahl von Funktionen der USB-Geräte für den jeweiligen Nutzer ebenso verfügbar sind wie über eine direkte USB-Anbindung. Der Einsatz eines USB-Hubs ermöglicht es zudem, mehrere Geräte in das Netzwerk einzubinden. Unterschiedliche USB-Geräte können dabei parallel von verschiedenen Benutzern verwendet werden. Das Firmware-Upgrade und die dazugehörige D-Link SharePort-Software für das Modell DIR-655 stehen ab sofort zum kostenfreien FTP-Download bereit. *(dr)*

D-Link: www.dlink.de,
ftp://ftp.dlink.de/dir/dir-655/driver_software/

Berichtswesen leicht gemacht

FileMaker bietet seine Datenbankanwendung **FileMaker Pro** in Version 10 an. Mit der Software lassen sich **Datenbanken** erzeugen sowie aus Quelldaten **Berichte anfertigen** und optisch darstellen. Veränderungen an diesen Quelldaten können dabei nun direkt während der Arbeit in der Berichtsansicht vorgenommen werden. Die Aktualisierungen erscheinen automatisch in der Datenbank, ohne dass die Benutzer hierfür die Ansichten wechseln müssen. In Version 10 speichert die Datenbanklösung durchgeführte Suchen zudem automatisch und ermöglicht es, diese Suchlogiken unter einem eigenen Namen abzulegen. Sogenannte **Script Trigger** lösen bestimmte Skripte entweder in Abhängigkeit des Nutzerverhaltens oder nach Ablauf festgesetzter Zeitlimits automatisch aus. Ähnlich einem Tabellenkalkulations-Makro kann spezifiziert werden, dass ein FileMaker-Skript zeitbestimmt abläuft und einen Vorgang automatisiert. So greift ein Script Trigger beispielsweise dann, wenn der Nutzer im Browse-Modus oder Suchmodus in ein bestimmtes Feld klickt oder einen Ansichtsmodus verlässt. In FileMaker Pro 10 sind zwölf vorgefertigte Script Trigger enthalten – fünf objektbasierte und sieben layoutbasierte. Die Software läuft auf Windows- und Mac-Rechnern und ist ab sofort erhältlich. Für die Pro-Variante beträgt der Preis 349 Euro. *(dr)*

FileMaker: www.filemaker.de/products/fmp/

Protokollführer für den Admin

BalaBit IT Security bringt Version 3.0 seiner **syslog-ng Premium Edition** (PE) auf den Markt. Das **Netzwerkmanagement-Werkzeug** ermöglicht es, sämtliche Status-, Fehler-, Alarm- und sonstigen Syslog-Meldungen von Servern und Netzwerkkomponenten im Unternehmensnetz zu sammeln, zu übertragen und zentral abzuspeichern. In der neuen Version speichert syslog-ng PE nun die Log-Nachrichten auch in **verschlüsselten und mit einem Zeitstempel versehenen Binärdateien** ab. Des Weiteren ist die Software in der Lage, Teile von Log-Meldungen auszutauschen. Dabei kann sie sowohl Textfragmente automatisch suchen und ersetzen als auch bestimmten Feldern einer Syslog-Nachricht einen festgelegten Wert zuweisen. Das sogenannte "Log-Message-Rewriting" nutzen Administratoren häufig in Verbindung mit dem Parsen von Nachrichten. Teil der Premium Edition ist der syslog-ng-Agent für Windows-Systeme. Das Tool erlaubt es, alle Informationen aus einem lokalen Windows-Ereignisprotokoll auszulesen und in eine unternehmensweite Syslog-Infrastruktur einzubinden. In Version 3.0 hat der Hersteller die Konfigurationsoberfläche des Windows-Agenten nun überarbeitet. So lässt sich die Software jetzt auch über einen Domänencontroller über Gruppenrichtlinien verwalten. Neben den Ereignisprotokollen von Windows XP und dem Windows Server 2003 unterstützt der Syslog-Agent nun außerdem das XML-basierte Ereignisprotokoll von Windows Vista und des Windows Server 2008 – sowohl in den 32-Bit- als auch in den 64-Bit-Versionen. Erhältlich ist die neue Version ab sofort. Für fünf Log-Quellen liegt der Einstiegspreis bei 385 Euro. *(dr)*

Die "syslog-ng Premium Edition 3.0" speichert Log-Daten nun auch verschlüsselt ab

Balabit IT Security: www.balabit.com/network-security/syslog-ng/central-syslog-server/

Mit zwei Bildschirmen wartet das "ThinkPad W700ds" von Lenovo auf

Notebook mit Doppelbildschirm

Lenovo bringt mit dem Modell **ThinkPad W700ds** ein Notebook auf den Markt, das über **zwei Bildschirme** verfügt. Während der erste Bildschirm Notebook-üblich aufgeklappt wird, lässt sich der zweite an der Seite bei Bedarf herausziehen. Damit richtet sich das Gerät überwiegend an Nutzer, die viel mit Grafiken arbeiten müssen. Hierfür bietet das Notebook auch ein **Grafiktablett** vor der Tastatur sowie auf Wunsch einen Farbkalibrator. Im Gerät verrichtet ein Intel Mobile Quad Core-Prozessor seinen Dienst, während NVIDIA Quadro FX mobile-Grafikprozessoren für die Bildausgabe sorgen. Zudem ist die mobile Workstation mit bis zu 8 GByte DDR3-RAM und einer Auswahl an Solid State Disks sowie traditionellen Festplatten mit bis zu 960 GByte Gesamtspeicherplatz erhältlich. Bei Bedarf lassen sich die Festplatten als RAID betreiben. Die Sicherheits-Features beinhalten einen optionalen Fingerabdruckleser, einen Smartcard-Reader und Festplatten mit Full-Disk-Encryption. Ab 4.529 Euro ist der mobile Rechner auf dem Markt zu haben. *(dr)*

Lenovo: www.lenovo.de

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

Die freie Linux-Distribution **openSUSE** ist in Version 11.1 erhältlich. Das Betriebssystem ist die erste vollständig mit openSUSE Build Service entwickelte Linux-Distribution. Dies soll einen transparenten Entwicklungsprozess in enger Zusammenarbeit mit der Community ermöglichen. Neu in Version 11.1 ist unter anderem der zugrunde liegende Kernel 2.6.27.7, der eine Vielzahl an Geräten und Webcams besser unterstützt. Daneben ist der Desktop KDE nun in Version 4.1.3 an Bord. openSUSE 11.1 ist ab sofort verfügbar. *(dr)*

www.opensuse.org

IBM bietet gemeinsam mit **Topalis** den Microsoft-freien, Linux-basierten virtuellen Desktop **Virtual Enterprise Remote Desktop Environment** (VERDE) an. Das Angebot besteht aus der Linux-Distribution Ubuntu für den Desktop sowie der IBM Open Collaboration Client Solution Software (OCCS) mit Lotus Symphony, IBM Lotus Notes und weiteren Lotus-Applikationen. Für eine 1.000-Benutzer-Umgebung beträgt der Preis 49 Euro pro User. *(dr)*

www.ibm.de

Von **Net at Work** kommt Version 6.5 des Spam- und Malware-Blockers **NoSpamProxy** auf den Markt, den der Hersteller erstmals mit dem Filter des Herstellers Commtouch ausgestattet hat. Der Torwächter arbeitet mit der "Recurrent Pattern Detection" (RPD). Nachrichten, die innerhalb weniger Minuten millionenfach auf der ganzen Welt verteilt werden, enthalten mit hoher Wahrscheinlichkeit Spam oder Viren und werden von der Engine unmittelbar geblockt. Die Verwaltung der Sicherheitslösung erfolgt über Microsoft Management Console (MMC) vom Server oder PC aus. Die Software läuft auf Windows Server 2003 und 2008 und ist für 25 User zum Preis von 575 Euro erhältlich. *(ln)*

www.nospamproxy.de

Die **science + computing ag** veröffentlicht Version 2.3 ihrer Systemmanagementsoftware **scVENUS.** Der Hersteller will darin vor allem die Unterstützung von Windows-Systemen verbessert haben. Unter anderem erlaubt das Werkzeug nun auch das Patchmanagement und ermöglicht es dem Admin, Benutzer und Gruppen in einem Active Directory anzulegen und zu verwalten. Auch Änderungen in der Registry und an Dateiattributen sollen sich in Windows-Umgebungen nun einfacher gestalten. Diese Maßnahmen lassen sich auch von der Powershell aus aufrufen und auf mehreren Rechnern gleichzeitig ausführen. Weitere Features wie der "Job-Log-Browser" sollen die Dokumentation der vorgenommenen Änderungen erleichtern. Die Verwaltungs-Suite kostet pro Rechner 25 Euro. Zusätzlich ist für jede Funktion extra zu zahlen. Softwareverteilung etwa schlägt mit 75 Euro zu Buche, Monitoring gibt es zum Preis von 50 Euro. *(ln)*

www.science-computing.de

Flexibles Backup für unterwegs

Mit **PresSTORE Backup2go** stellt **Archiware** eine Datensicherungslösung für mobile Mitarbeiter vor. Dabei hat der Hersteller einkalkuliert, dass die Rechner nicht immer eine Verbindung zum Unternehmensnetz besitzt. So startet die Software automatisch, sobald der Client wieder Zugang zum Firmennetz hat. Damit ist die **Clientkomponente der Backup-Lösung** für die Sicherung der Daten verantwortlich und kontaktiert von sich aus die entsprechenden Server. Sollte die Verbindung während eines Sicherungsprozesses unterbrochen werden, führt die Software das Backup automatisch beim nächsten Kontakt zum Firmen-LAN fort. Obwohl die Anwender dabei eine gewisse Kontrolle über die Software besitzen, kann der Administrator auch zentrale Sicherungsrichtlinien festlegen. Besonders sensible Daten können zudem **verschlüsselt abgespeichert** und damit nur vom entsprechenden Arbeitsplatz aus gelesen werden. Die Verbindung lässt sich dabei über Intra- oder Internet aufbauen. An Betriebssystemen werden auf Server- und Clientseite Windows 2000 und XP sowie Mac OS X 10.6 und verschiedene Linux-Distributionen unterstützt. Die Software ist ab sofort auf dem Markt und kostet für 20 zu sichernde Arbeitsplätze 500 Euro. *(dr)*

Archiware: www.archiware.com/index.php?hp=468

Verschlüsselung im Handumdrehen

Für große Umgebungen, die auf **Ethernet-WAN-Verbindungen** setzen und in denen Daten zügig **verschlüsselt** werden sollen, bietet **SafeNet** den **Ethernet Encryptor 10G** an. Damit richtet sich der Hersteller an sicherheitssensible Bereiche, bei denen Daten über Ethernet-WAN-Strecken an andere Standorte übertragen werden. Die Durchsatzrate soll dabei trotz Ver- und Entschlüsselung 10 GBit/s betragen. Als Verfahren kommt AES-256 auf **Layer 2-Ebene** zum Einsatz. Damit sind beispielsweise auch IP-Adressen selbst geschützt. Für eine gegenseitige Authentifizierung der Geräte untereinander sowie den notwendigen Schlüsselaustausch sorgen X.509-Zertifikate mit einem öffentlichen Schlüssel nach RSA-2048. Ein Out-of-Band-Ethernet-Anschluss sowie eine RS-232-Konsole ermöglichen den Wartungszugang, auch wenn der direkte Link ausgefallen ist. Mittels SNMP v3 ist zudem eine grundlegende Überwachung der Appliances möglich. Erhältlich ist der Encryptor ab sofort. Die Preise liegen bei 58.000 Euro. *(dr)*

Der "Ethernet Encryptor 10G" von SafeNet verschlüsselt Breitbanddaten über Ethernet-WAN

SafeNet: www.safenet-inc.com/solutions/enterprise_data_protection.asp

Mini KVM-Weiche

Daxten stellt einen neuen **2-Port KVM-Switch** für den SOHO-Sektor vor. Der **SCOUTmicro DVI** erlaubt die Steuerung und das Umschalten zweier USB-Rechner mit DVI-Schnittstellen über nur ein Tastatur-, Monitor und Maus-Set. Dabei sind die Anschlusskabel für die Rechnerkonsolen und die DVI-Schnittstellen bereits im Switch integriert. Eine an der Gerätefront eingerichtete DVI-Schnittstelle sowie zwei USB-Ports stellen die Einbindung einer lokalen Bedienkonsole sowie einer digitalen Videoquelle sicher. Somit eignet sich die KVM-Weiche besonders für Einsatzbereiche, bei denen die Arbeit mit hochauflösenden Videodarstellungen auf mehreren Computern auf nur einen Arbeitsplatz konsolidiert werden soll. Die maximal mögliche Auflösung beträgt 1.920 mal 1.080 Punkte. Den Strom bezieht der Switch direkt über die angeschlossenen Computer, sodass keine externe Versorgung benötigt wird. Für 75 Euro ist das Gerät ab sofort erhältlich. *(dr)*

Daxten: www.daxten.de

Vierfach-Speed

Mit Modell 12200 stellt **QLogic** einen **Infiniband-Switch** vor, der Daten im QDR-Modus (Quad Data Rate) überträgt und so nominell bis zu **40 GBit/s** erreicht. Der Switch verfügt über 36 Ports und ist für den **Einsatz in einem kleineren Cluster** gedacht. Alternativ sorgt er als Edge-Switch innerhalb größerer Umgebungen für eine erhöhte Skalierbarkeit. Die Netzwerkkomponente soll sich zudem durch einen geringen Energieverbrauch auszeichnen, der laut Angaben des Herstellers je nach Auslastung zwischen 85 und 264 Watt beträgt. Stromversorgung und Lüfter sind redundant ausgelegt. Das Gerät lässt sich mit der "InfiniBand Fabric Suite"-Software (IFS) verwalten. Mithilfe von Konfigurations-Assistenten soll es IT-Verantwortlichen dabei möglich sein, auch große Infiniband-Umgebungen mit nur wenig Zeitaufwand zu installieren. Der Edge-Switch gehört zur aktuellen Linie von Blade- und Edge-Servern von QLogic. Diese basiert auf dem neu entwickelten TrueScale-ASIC-Prozessor, der für Latenzzeiten von unter 150 ns sorgen soll. Das für den Rack-Einbau konzipierte, eine Höheneinheit messende Gerät ist ab 10.000 US-Dollar erhältlich. *(ln)*

QLogic: www.qlogic.com

Der Infiniband-Switch 12200 von QLogic verfügt über 36 Ports und überträgt 40 GBit/s

iadministrator

Live-Workshops 2009

Jetzt Plätze sichern und anmelden!

1 München

Exchange 2007

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

ausgebucht

2 Frankfurt/Eschborn

Netzwerksicherheit

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

anschließend, am 02. und 03. April 2009:

Data Center Security

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

3 Berlin

Storage-Lösungen für virtualisierte Server

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

am darauffolgenden Tag, dem 29. Mai 2009:

Storage-Virtualisierung

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

4 Heidelberg

Hochverfügbarkeit von Diensten und Applikationen

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

5 Hamburg

E-Mail-Management

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

anschließend, am 01. und 02. Oktober 2009:

SPAM

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

6 Böblingen

Virtualisierte Infrastrukturen

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

7 München

Open Source im Mittelstand

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

anschließend, vom 25. bis 27. November 2009:

IT-Security-Workshop

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

IT-Administrator Trainings-Partner: GeNUA

IT-Administrator Trainings-Partner: fast lane

ITANet Schirmherrschaft: REALTECH

ITANet – Die System und Netzwerk User Group

Mehr Infos und Anmeldeformulare zu den Veranstaltungen unter

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

oder per E-Mail an info@itanet.de

IIR Forum "Storage", 1. bis 4. Dezember 2008, Hamburg

Speicherkenner auf großer Fahrt

von Lars Nitsch

Zum achten Mal lud IIR Technology zum jährlichen Storage-Forum nach Hamburg, um Trends und Entwicklungen auf dem Speichermarkt aufzuzeigen und neue Technologien näher zu beleuchten. Schwerpunkte der diesjährigen Tagung waren neben der allgegenwärtigen Virtualisierung vor allem eine Übersicht über effiziente Archivierungsmethoden sowie die immer drängendere Frage nach der Compliance. In einer gelungenen Mischung aus Expertenvorträgen und praktischen Beispielen aus den unterschiedlichsten IT-Abteilungen konnten die rund 80 Teilnehmer ihr Fachwissen auffrischen und scheuten sich nicht, die Hersteller mit der einen oder anderen kritischen Frage zu behelligen.

Wer während der Vorträge einen Blick aus den Fenstern des Tagungssaals "Elbkuppel" warf, konnte nicht selten ein riesiges Containerschiff oder einen imposanten Tanker den Hamburger Hafen durchkreuzen sehen. Große Themen waren es dann auch, die der Ausrichter IIR Technology auf die Agenda für das insgesamt achte Storage-Forum gesetzt hatte: Storage-Technologien wie Virtualisierung, Archivierung, Datenmanagement, Compliance, Backups und nicht zuletzt Green IT sollten in drei Vortragstagen und einem eintägigen Seminar zur Sprache kommen und mit den Teilnehmern diskutiert werden.

Die großen Drei: Deduplizierung, Virtualisierung, Netzwerkkonsolidierung

In seiner Keynote zeigte Norbert Deuschle vom Storage Consortium drei große Trends auf: Ein großes Einsparpotenzial gerade in wirtschaftlich klammen Zeiten biete die Kapazitätsoptimierung, die von den meisten Herstellern unter dem Stichwort "Deduplizierung" vermarktet wird. Redundante Daten werden dabei durch einen Pointer ersetzt und sind so nur einmal auf dem Datenspeicher vorhanden. Firmen stünde somit im Regelfall zwischen zehn- und 30-mal mehr Speicherplatz zur Verfügung. Zu einer besseren Ausnutzung der vorhandenen Ressourcen soll auch die Storage-Virtualisierung beitragen. Hier lautet das Kennwort "Thin Provisioning", das Anwendern nur bei Bedarf aus einem gemeinsamen Pool neuen Plattenplatz zuteilt und auf diese Weise jedes einzelne Speichermedium effizienter mit Daten belegt. Als drittes In-Thema nannte Deuschle die Netzwerkkonsolidierung. So sei es vielfach simpler Platzmangel im Rechenzentrum, der die Reduzierung der physikalischen Architektur erfordere. Ein vielversprechender Ansatz sei hier die Fibre Channel over Ethernet-Technologie (FCoE), die allein die Menge der benötigten Kabel und Switches um einen bedeutenden Faktor vermindern würde.

In Sichtweite des Hamburger Hafens trafen sich die Teilnehmer zum IIR Forum "Storage"

Die Grenzen der Compliance

Die Tatsache, dass die Archivierung von Geschäftsvorgängen im Interesse eines jeden Unternehmens liegt, hat sich in kleinen und mittelständischen Betrieben mittlerweile herumgesprochen. Selbst Hersteller von Archivierungslösungen mussten beim Thema Compliance in einer Diskussion mit den Teilnehmern allerdings zugeben, dass den gesetzlichen Anforderungen meist nicht zu hundert Prozent entsprochen werden könne. Allein die Tatsache, dass eingehende E-Mailnachrichten eigentlich sofort unverändert archiviert werden müssten, stellt die meisten IT-Abteilungen vor logistisch und technisch oft unüberwindliche Hürden. Wie etwa Rudolf Ennikl, Systemadministrator bei der österreichischen Voestalpine-Gruppe, betonte, wandern alte Mails erst nach einem bestimmten Zeitraum ins Archiv. Von dort seien zwar sogar einzelne Nachrichten mit wenigen Klicks wieder herstellbar. Eine Unveränderlichkeit der Daten vor der Archivierung sei aber nicht gewährleistet.

Von alten Schinken und dicken Platten

Zwischen einschnürenden Gesetzen und grauer Theorie gab es jedoch stets auch viel Praxiserfahrungen aus dem Admin-Alltag zu hören. Schon ob der unglaublichen Datenmengen beeindruckte hier der Vortrag von Dr. Bernd Reicher vom Leibniz-Rechenzentrum in München. Das Rechenzentrum ist als Dienstleister für die Bayerische Staatsbibliothek tätig und zeichnet dort unter anderem für die elektronische Langzeitarchivierung von Schriften des 16. Jahrhunderts verantwortlich. Fortschrittliche Scan-Roboter sorgen laut Reicher für ein tägliches Datenvolumen von rund 500 GByte. Insgesamt belaufe sich allein der Datenbestand dieser Scans derzeit auf rund 87 TByte. Für Dr. Dirk Düllmann vom CERN in Genf dürfte sich selbst diese Größenordnung im Bereich "Peanuts" bewegen. Die Datenmengen, die im Teilchenbeschleuniger LHC anfallen, erfordern gewaltige Lösungen: Sämtliche NAS-Server des Forschungszentrums verfügen auf mehr als 20.000 Festplatten über eine Speicherkapazität von 10 PByte, während die auf Band abgelegten Daten sogar 30 PByte umfassen. Dies ist für die Zukunft laut Düllmann aber noch lange nicht ausreichend, die einzige Lösung sieht der Forscher hier in durch Hochgeschwindigkeitsnetze verbundenen Grid-Strukturen.

Fazit

Ob Sagenhaftes aus dem Reich der Petabytes, Alltägliches aus dem Arbeitsablauf einfacher Admins oder viel Hintergrundwissen rund um die neuesten Speichertechnologien – das IIR Forum "Storage" 2008 überzeugte durch den anregenden Mix verschiedenster Inhalte. Wer von der Theorie in die Praxis wollte, hatte an zwei Tagen zudem die Möglichkeit, sich auf der kleinen Ausstellungsfläche mit den Produkten verschiedener Storage-Anbieter auseinanderzusetzen.

Im Test: BMC Bladelogic Operations Manager

Rundumpflege für Server

von Jürgen Heyer

Mit der kürzlich übernommenen Firma Bladelogic und deren Lösung "Bladelogic Operations Manager" adressiert BMC in erster Linie größere Unternehmen und Rechenzentren mit mindestens dreistelligen Serverstückzahlen. Der Operations Manager präsentiert sich dabei als überaus mächtiges Werkzeug für ein Server-Lifecycle-Management, um Administratoren bei oft ungeliebten, zeitintensiven und häufig wiederkehrenden Pflege- und Kontrollaufgaben zu entlasten. Der Zeitaufwand für Tätigkeiten wie das Ausrollen von Installationen sowie Compliance- und Konsistenzprüfungen auf vielen Servern lässt sich mit diesem Werkzeug von mehreren Stunden Dauer auf wenige Minuten reduzieren, wie die Lösung im Testlabor des IT-Administrator unter Beweis stellte.

Die IT-Verantwortlichen in Rechenzentren mit mehreren hundert oder gar mehreren tausend Servern stehen vor der fast unlösbar erscheinenden Aufgabe, alle Systeme mit einem kleinen Administratorenteam gleich zuverlässig zu betreuen und stets auf aktuellem Stand zu halten. Während es für die Verteilung einer Software oder deren Update noch diverse Produkte zur Unterstützung gibt, ist es beispielsweise weitaus schwieriger zu kontrollieren, ob ein bestimmter Registry-Schlüssel auf allen Systemen auf einen bestimmten Wert gesetzt ist.

Weitere in derartigen Umgebungen typische Aufgabestellungen sind etwa:

- Ein System muss bei der Installation mittels einer Sicherheitspolicy nicht nur vor Angriffen gehärtet werden; auch sollte eine Prüfung sicherstellen, ob diese Parameter auch drei Monate später noch entsprechend gesetzt sind, nachdem andere Abteilungen womöglich ebenfalls mit Administrationsrechten den Server genutzt haben.
- Veränderte Einstellungen müssen schnell wieder geändert werden.
- Es gilt die Verantwortung zu klären für das Anlegen oder Löschen eines Benutzers auf mehreren hundert Servern, wenn diese nicht unter einem Verzeichnisdienst laufen.
- Der Zeitrahmen für den Wechsel eines SSH-Schlüssels nach personellen Wechseln muss klar sein.
- Administratoren- und Root-Passwörter sind regelmäßig zu ändern.

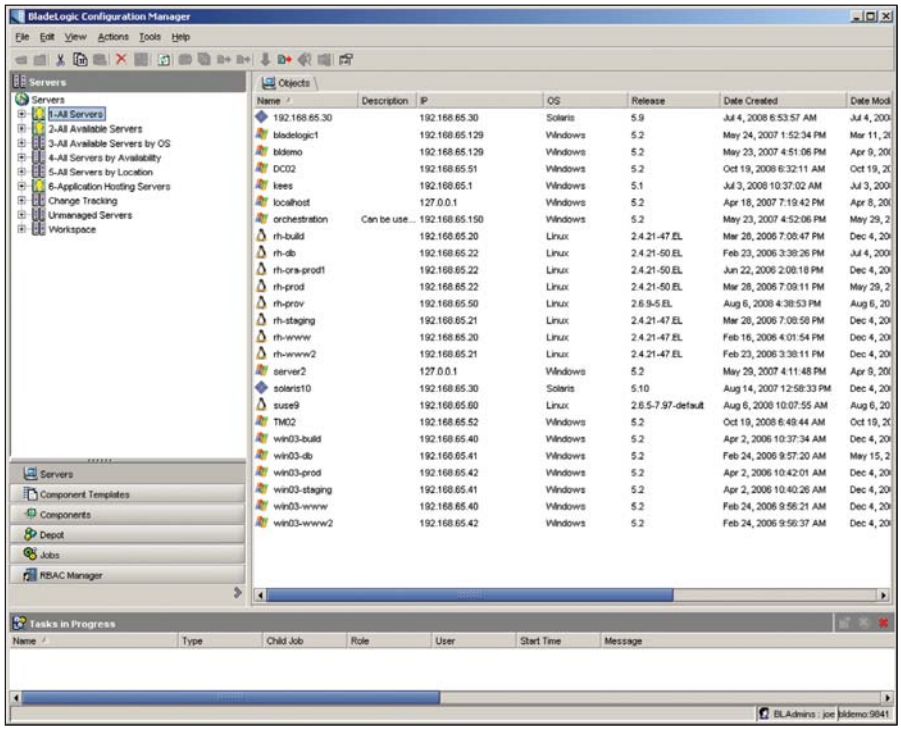


Bild 1: Die Smart Groups werden automatisch gefüllt und sorgen für eine übersichtliche Auflistung der Objekte

Anspruchsvolle Installation und Konfiguration

Der Bladelogic Operations Manager (BOM) ist kein Werkzeug, das schnell out-of-the-box installiert ist. Vielmehr empfiehlt es sich, mit dem Hersteller zusammen ein Betriebskonzept zu erarbeiten, welches dann umgesetzt wird, und für die Ersteinrichtung sowie Grundkonfiguration einige Tage Unterstützung einzukaufen. Auch wir haben uns für den Test eine vir-

tuelle Umgebung vorbereiten lassen und waren zudem bei einer größeren Kundeninstallation vor Ort dabei, um den Ablauf verfolgen zu können.

Modularer Aufbau

Der Operations Manager besteht aus Modulen zur Inventarisierung, Compliance-Prüfung, Softwareverteilung und zum Patchmanagement, zur Systeminstallation sowie zur Erstellung von Berichten und Analysen. Damit deckt er die typischen Aufgaben für ein umfassendes Lifecycle-Management ab. Die meistgenutzte, zentrale Konsole ist dabei der "Configuration Manager" mit der gesamten Benutzer- und Jobverwaltung. Eine zweite Konsole, der "Provisioning Manager", dient zur Installation neuer Server.

Die zentrale Komponente bildet das sogenannte "Depot", bestehend aus einem Datenbank- sowie einem Fileserver. Eine Installation ist sowohl unter Linux (Red Hat, Novell SLES) als auch unter Windows 2000/2003 Server möglich. Hinsichtlich der Datenbank werden Oracle sowie SQL unterstützt. Die Datenbank ist eine CMDB und enthält sämtliche Informationen über alle Jobs und Aufträge, die gesamte Inventarisierung, Vergleiche und so weiter. Der Fileserver ist für die Speicherung sämtlicher Installationspakete, Hotfixes und Skripte zuständig. Da bei einem Ausfall eines dieser beiden Systeme der gesamte BOM brachliegt, sind sie idealerweise als Cluster zu installieren.

Hochsicheres Konzept der Steuerung mit Agenten

Die gesamte Steuerung und Bedienung der Umgebung erfolgt über einen oder auch mehrere "Application Server" (APS). Je nach Konzept sind auf den APS die benötigten Bedienkonsolen installiert, außerdem kommunizieren sie mit den Agenten auf den Clients, also den zu überwachenden Servern. Die Agenten belegen nur wenige MByte Platz und verhalten sich absolut passiv, was bedeutet, dass sie nie von sich aus Verbindung mit einem APS aufnehmen. Vielmehr übernimmt ausschließlich der APS die aktive Rolle. Das bedeutet auch, dass der BOM für ein Systemmonitoring, bei dem die Agenten bei auftretenden Fehlern oder Ereignissen diese selbstständig weitergeben müssen, nicht geeignet ist. Unter Sicherheitsaspekten ist diese Arbeitsweise sehr von Vorteil, denn so ist der Kommunikationsaufbau klar geregelt und ein gehackter Client kann nicht verwendet werden, um weiter in Richtung Depot vorzudringen. Weiterhin erfolgt die gesamte Kommunikation zwischen APS und Agent über einen einzigen Port, sodass bei einem Betrieb über Firewalls hinweg auch nur dieser eine Port geöffnet werden muss. Der Datenaustausch erfolgt über das proprietäre "Protocol 5", ein TLS-basierendes Protokoll mit selbstsignierten Zertifikaten.

Ein APS kann durchaus 1.000 und mehr Agenten verwalten, es können sich aber auch mehrere APS parallel oder netzsegmentweise die Arbeit teilen. Wird mit mindestens zwei APS gearbeitet, lassen sich diese redundant konfigurieren, sodass bei einem Ausfall der verbleibende alle Agenten bedient. Jeder Agent wiederum lässt sich über eine IP-Adressbeschränkung so konfigurieren, dass er nur die Anfragen von bestimmten Application Servern akzeptiert.

Neben der oben beschriebenen Datenbank, die die aktuellen Arbeitsinformationen enthält, ist für das Reporting eine zweite einzurichten, was auf dem gleichen Datenbankserver erfolgen kann. Reportaufträge wiederum werden auf einem APS ausgeführt und in die Reportdatenbank geschrieben. Die Resultate können über eine Webseite abgerufen werden, hierzu wird standardmäßig ein Tomcat-Webserver eingerichtet.

Installation

Die gesamte Installation läuft so ab, dass zuerst der Datenbankserver konfiguriert wird. Dies geschieht über einige Skripte, die die benötigten Tabellen anlegen. Der Fileserver benötigt keine spezielle Vorbereitung außer dem Anlegen einer Freigabe und der Installation des Agenten. Dann ist der APS wahlweise auf einem Linux- oder Windows-Server einzurichten, wobei bei der Installation der Ort der Datenbank sowie derjenige der Freigabe abgefragt werden. Handelt es sich um einen Windows-Server, kann die Konsole des Configuration Managers direkt auf dem Server aufgerufen werden. Besser ist es aber, die Konsole (zusätzlich) direkt am Arbeitsplatz zu installieren und sich dann zu einem APS zu verbinden.

Für Compliance-Prüfungen sollten IT-Verantwortliche anschließend diverse Template-Skripte importieren, ebenso einen Standard-Content, um die ersten Ordner und Ordnungskriterien einzuspielen. Die Reporting-Funktionen können später installiert werden, wenn die zentralen Komponenten laufen. Gleiches gilt für das Provisioning zur Bestückung neuer Server über PXE.

Insgesamt erweist sich die gesamte Installation als kein Hexenwerk, sie ist auch im Handbuch ausreichend beschrieben. Dennoch sollten IT-Verantwortliche ernsthaft in Erwägung ziehen, diese einem erfahrenen Spezialisten von BMC zu überlassen, um nichts zu vergessen und eine stabile Umgebung zu gewährleisten.

Einstieg in die Arbeit

Nach der Installation präsentiert sich dem Administrator ein erfreulich übersichtlicher Desktop des Bladelogic Configuration Managers. Die Ansicht gliedert sich in die Bereiche Server, Komponen-

Application Server:
2 x Xeon/2 GHz, 2 GByte RAM, SLES 9/10, RHEL 3.0/4.0 oder Windows 2000/2003 Server

File Server:
Aktuelle Hardware, 200 GByte Plattenkapazität

Datenbankserver:
Aktuelle Hardware, Datenbank Oracle 9i/10 oder MS SQL Server 2000/2005

Systemvoraussetzungen

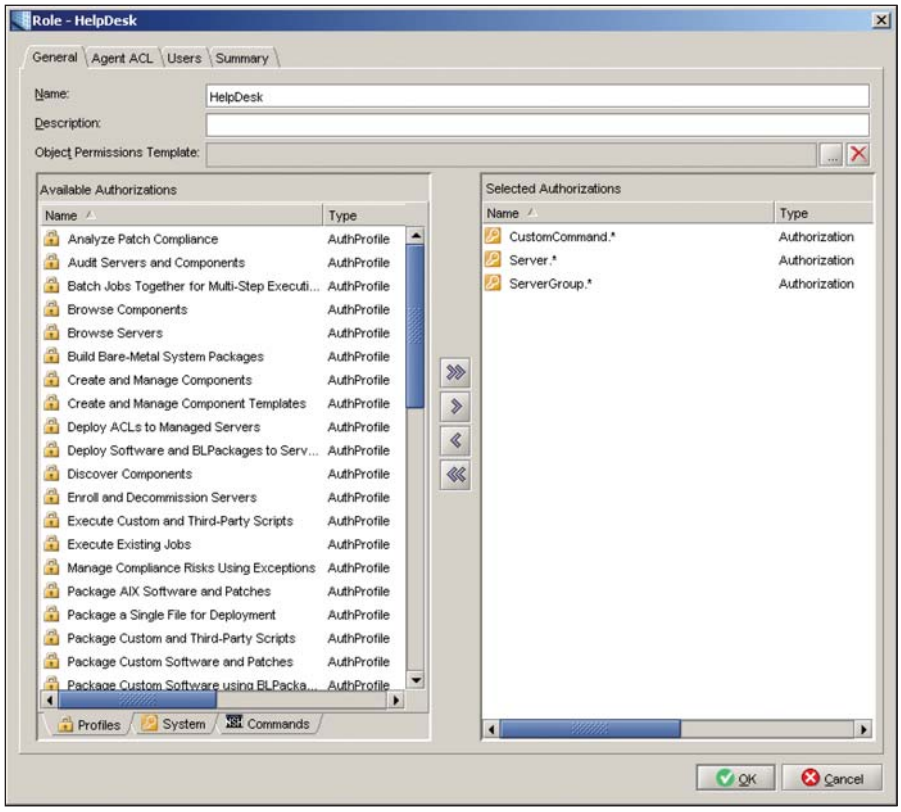


Bild 2: Zur einfacheren Zuweisung lassen sich Rechte für verschiedenste Aktionen über Profile zusammenfassen, typische Profile sind bereits angelegt.

ten, Komponentenvorlagen, Depot, Jobs und RBAC-Manager (Benutzer-, Gruppen- und Rechteverwaltung). In den Komponentenvorlagen sind die Definitionen und Kriterien für die weiter unten angesprochenen Vergleiche und Compliance-Prüfungen hinterlegt. Das Depot enthält alle Pakete zur Verteilung, Skripte und Hotfixes.

Über Jobaufträge ordnet der Administrator nun Objekte aus dem Depot oder auch eine Komponentenvorlage einem oder mehreren Servern zu, um dort ein Paket zu installieren, ein Skript auszuführen oder Einstellungen und Parameter abzufragen. Die gesamten Abläufe sind angesichts der Vielzahl der Möglichkeiten und Kombinationen erfreulich intuitiv gestaltet, und nach relativ wenig Einarbeitung gelingen im Test die ersten erfolgreichen Installationen sowie Abfragen.

Die meisten angelegten Objekte besitzen Eigenschaftsfelder (Properties), die teilweise automatisch gefüllt werden, zum Beispiel bei einem Server mit der IP-Adresse und dem installierten Betriebssystem. Teilweise lassen sich die Objekte aber auch vom Administrator zur Sortierung und Gruppierung verwenden, indem er die zuständige Abteilung oder den Aufstellort hinterlegt. Es lassen sich zudem weitere Properties nach Bedarf selbst anlegen. Wichtig sind die Properties zum einen, um Informationen zum Objekt zu speichern und zum anderen, um in Verbindung mit den sogenannten "Smart Groups" diese automatisch zu füllen. Eine Smart Group ist ein mit einer Filterbedingung verknüpfter Ordner. Die Filterbedingung bestimmt, welche Objekte darin automatisch zusammengefasst werden, beispielsweise alle Server der Abteilung X, alle 64-Bit-Linux-Systeme, alle Jobs für Linux-Systeme oder alle Pakete für Office-Installationen. Es ist nicht möglich, ein Objekt manuell einer Smart Group hinzuzufügen oder daraus zu entfernen, dies geschieht allein anhand der vorgegebenen Filterbedingungen. Smart Groups sind mit Abstand das wichtigste Werkzeug zur Sortierung der aufgenommenen Server, angelegten Vorlagen und erstellten Jobs.

Mehrseitige Assistenten führen durch die meisten Arbeitsabläufe und fragen die benötigten Daten ab. Trotzdem sind die Eingabemöglichkeiten oft so vielfältig, dass eine umfassende Einarbeitung und viel Übung für ein zielstrebiges Arbeiten erforderlich sind. Um beispielsweise einen Compliance-Job zu realisieren, sind zuerst die Compliance-Vorgaben als Komponenten-Vorlage anzulegen. Dann lassen sich bei der Jobanlage durchaus auch mehrere Vorlagen aufnehmen und dedizierten Servern oder auch einer Server Smart Group zuweisen und wahlweise sofort oder zeitgesteuert ausführen.

Granulare Benutzerverwaltung

Der Bladelogic Configuration Manager besticht durch eine überaus granulare Benutzer- und Rechteverwaltung, die aller-

Aus einer Shell entstanden

Entstanden ist der Operations Manager ursprünglich aus der sogenannten Network Shell (NSH), die auf einer Unix Z Shell (Zsh) basiert und um Netzwerkfunktionen sowie eigene Befehle zum Absetzen von Kommandos für mehrere Rechner erweitert wurde. Die NSH ist gleichzeitig das Kommandozeilen-Interface und es ist theoretisch möglich, alle Aktivitäten über die NSH zu steuern, ohne überhaupt eine Konsole zu verwenden. Zum Skripten in der NSH stehen typische Linux-Werkzeuge wie sed, uname und awk zur Verfügung. Auch die über die grafische Konsole veranlassten Aktivitäten werden letztendlich in NSH-Skripte und -Kommandos umgesetzt und als solche ausgeführt.

Interessant ist dabei, dass es keinerlei Rolle spielt, welches Betriebssystem auf dem Client läuft – die NSH steht auch auf Windows-Systemen zur Verfügung. Dabei können in Skripte Kommandos integriert werden, die im Command-Interpreter von Windows lokal am Client ausgeführt werden sollen. Das NEXEC-Kommando sorgt dabei für den Befehlsaufruf. Die resultierenden Ausgaben können wiederum in den Skripten weiterverarbeitet werden, sofern sie in der Standardausgabe landen. Letztendlich ist die NSH ein überaus mächtiges Instrument, welches allerdings gute Skriptkenntnisse verlangt. Hier erleichtert eine gewisse Erfahrung im Umgang mit UNIX oder Linux die Einarbeitung.

Sie suchen eine Internet-Adresse?

1&1 bietet doppelte Chancen bei der Domainauswahl!

Neu!

Neue Domains sichern …

Bei 1&1 gibt's Internet-Adressen für mehr als 30 Endungen und jetzt NEU: intelligente Alternativ-Vorschläge, falls Ihre Wunsch-Domain schon vergeben ist.

… oder Domain-Marktplatz nutzen:

Ihre Wunschdomain ist bereits registriert? Vielleicht wird sie in unserer Domain-Datenbank mit über 14 Mio. Internet-Adressen zum Verkauf angeboten!

Infos unter: www.1und1.info

.de-Domain jetzt 3 Monate für 0,– €!*

Aktion nur noch gültig bis 28.02.2009!

* Aktion bis 28.02.2009: 1&1 Domain mit .de-Domain 3 Monate für 0,– €/Monat, danach z. B. 1&1 Domain mit .de-Domain 0,49 €/Monat. Einmalige Einrichtungsgebühr 9,60 €. Mindestvertragslaufzeit 24 Monate. Preise inkl. MwSt.

Beratung und Bestellung:

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

www.1und1.info

MEMBER OF united internet

1&1

dings auch entsprechend komplex ist. In einem ersten Schritt sind die benötigten Benutzer anzulegen und Rollengruppen zuzuordnen. Eine Kopplung mit einem Microsoft Active Directory ist möglich, wird allerdings in der Praxis kaum verwendet, da hier deutlich weniger Benutzer benötigt werden, als in einer größeren Firmenumgebung angelegt sind.

Befindet sich ein Benutzer in verschiedenen Rollengruppen, kann er zwischen diesen wechseln, ohne sich dazu neu anmelden zu müssen. Einer Rollengruppe sind nun detaillierte Rechte auf die verschiedensten Objekte zuzuweisen (Windows-Software. Linux-Software, Verteiljobs, Depotordner), und dies wiederum für unterschiedliche Tätigkeiten (erstellen, modifizieren, lesen et cetera). Weiterhin lassen sich Autorisierungprofile für typische Operationen (zum Beispiel Server browsen, Software und Pakete auf Server verteilen, existierende Jobs ausführen) definieren, die die Einzelrechte entsprechend zusammenfassen. Diverse Beispiele sind bereits angelegt.

Sollen nun mehrere Administratorengruppen jeweils nur bestimmte Servertypen betreuen können, so lässt sich dies entsprechend einrichten. Ebenso können einem Helpdesk ganz dedizierte Rechte zum Ausführen bereits vorbereiteter Skripte und Jobs zugewiesen werden. Zu empfehlen ist hier auf jeden Fall eine vorausgehende Planung, um die Rechtestruktur im jeweiligen Unternehmen der Arbeitsweise und der Aufgabenteilung anzupassen. Unserem Eindruck nach dürfte es kaum eine Konstellation geben, die sich nicht abbilden ließe.

Der Zugriff vom Application Server über die Agenten auf die zu überwachenden Systeme erfolgt über ein Benutzer-Mapping. Hierzu wird bei der Agenteninstallation am Client eine Benutzerzuordnung hinterlegt und bei Bedarf aktualisiert, sodass beispielsweise der Bladelogic-Administrator BLAdmin an einem Windows-Client stets als Administrator oder bei Linux-Systemen als Root zugreift.

Vergleichender Live-Zugriff

Absolut beeindruckend sind die Möglichkeiten des Operations Managers zum Live-Zugriff. Bei den meisten Management- und Inventarisierungstools wird der Client in bestimmten Abständen über den Agenten ausgelesen und die Informationen in eine Datenbank geschrieben. Der Administrator kann dann nur auf die dort abgelegten Informationen zugreifen. Dies ist beim BOM völlig anders. Hier greift der Administrator praktisch transparent auf die Clients zu, um sich dort die aktuellen Informationen zu holen. Möchte er wissen, welche Hotfixes installiert sind, liest der Agent dies aktuell aus. Genauso kann der Administrator das Dateisystem des Clients komplett browsen, die Windows-Registry sowie Konfigurations- und Logdateien öffnen und auch editieren.

Weiterhin ermöglicht der BOM einen Vergleich zwischen mehreren Clients, um beispielsweise zu prüfen, ob wichtige Registry-Einstellungen identisch sind, ein bestimmtes Verzeichnis existiert oder ein Softwarepaket installiert ist. So lassen sich Unterschiede schnell ermitteln. Weiterhin erstellt das Programm auf Wunsch Snapshots von bestimmten Einstellungen. Auch diese lassen sich mit Live-Systemen vergleichen und der Administrator kann prüfen, ob beispielsweise einmal eingestellte Sicherheitseinstellungen, die er als Snapshot gespeichert hat, auch nach einiger Zeit noch so unverändert aktiv sind. Mit der Ermittlung von Unterschieden lassen sich dann Installationspakete verknüpfen, die die gefundenen Abweichungen ändern und die Werte des Live-Systems anpassen. Bei einigen Versuchen zeigt es sich, dass Abweichungen sicher gefunden und auf Wunsch auch korrigiert werden. Die Kunst besteht allenfalls darin, für einen Vergleich erst einmal die Kriterien festzulegen, also eine geeignete Komponentenvorlage zu definieren, die vorgibt, was verglichen werden soll. Ein pauschaler Vergleich von Systemen mit der Aufgabe, einfach alles aufzuzeigen, was unterschiedlich ist, ist ebenso unsinnig wie unrealistisch.

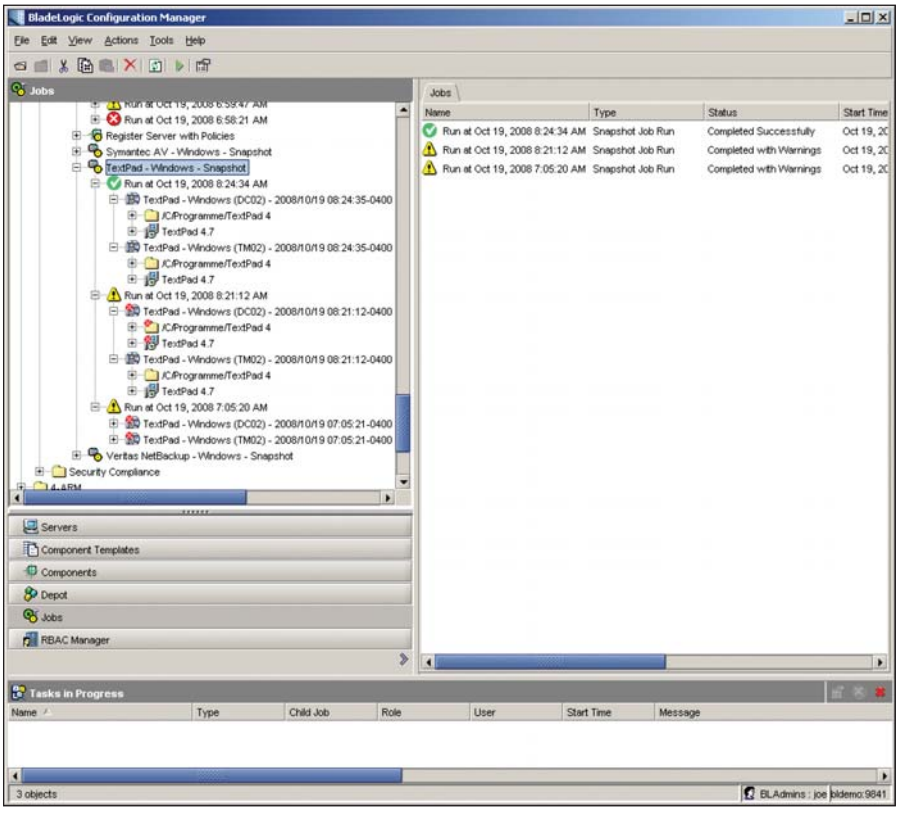


Bild 3: Beim Vergleich von aktuellen Systemen mit einem Snapshot zeigt das Programm übersichtlich die Abweichungen auf

Sie wollen einen Hightech-Server?

1&1 ist 1. Klasse!

1&1 bietet leistungsstarke Hightech-Server für höchste Ansprüche. Mit extrem schnellen AMD Prozessoren, unbegrenztem Inklusive-Traffic und umweltschonender Stromversorgung. IT-Profis haben die Wahl zwischen Root- und Windows-Servern (ganz neu mit: Windows Web Server 2008). Und wer die Leistung eines eigenen Servers bequem per Full-Service nutzen will, wählt den 1&1 Homepage-Server. Alle drei Server-Typen gibt's in nebenstehenden Leistungsklassen.

Supergünstig in 2009 starten!

1&1 SERVER L64

Der Einstiegs-Server mit hohem Leistungsanspruch!

ab **79,99** €/Monat*

Dual-Core AMD Opteron™ Prozessor, 250 GB Software RAID.

1&1 SERVER XL64

Gesteigerte Performance für anspruchsvolle Anwendungen! Dual-Core AMD Opteron™ Prozessor, 500 GB Software RAID.

ab ~~99,99~~ €/Monat*

3 Monate für 0,– €!*

Aktion nur noch gültig bis 28.02.2009!

1&1 SERVER XXL64

Hightech-Konfiguration für Profis! Quad-Core AMD Opteron™ Prozessor, 750 GB Hardware RAID.

ab ~~149,99~~ €/Monat*

3 Monate für 0,– €!*

Aktion nur noch gültig bis 28.02.2009!

1&1 SERVER 4XL64

Unerreichtes Preis-/Leistungsverhältnis!
2 x Quad-Core AMD Opteron™ Prozessor, 3 x 750 GB Hardware RAID 5.

ab ~~299,99~~ €/Monat*

3 Monate für 0,– €!*

Aktion nur noch gültig bis 28.02.2009!

Das komplette Server-Angebot, auch die 1&1 Virtual-Server, finden Sie im Internet.

* Aktion bis 28.02.2009: 1&1 Server XL64, 1&1 Server XXL64 oder 1&1 Server 4XL64 3 Monate für 0,– €/Monat, danach 1&1 Server XL64 99,99 €/Monat, 1&1 Server XXL64 149,99 €/Monat oder 1&1 Server 4XL64 299,99 €/Monat. Einmalige Einrichtungsgebühr 99,– €. Mindestvertragslaufzeit 12 Monate. 1&1 Server L64 79,99 €/Monat – einmalige Einrichtungsgebühr 99,– € bei einer Mindestvertragslaufzeit von 12 Monaten (alternativ: 0,– € Einrichtungsgebühr bei einer Mindestvertragslaufzeit von 24 Monaten). Preise inkl. MwSt.

Beratung und Bestellung:

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

www.1und1.info

MEMBER OF united internet

1&1

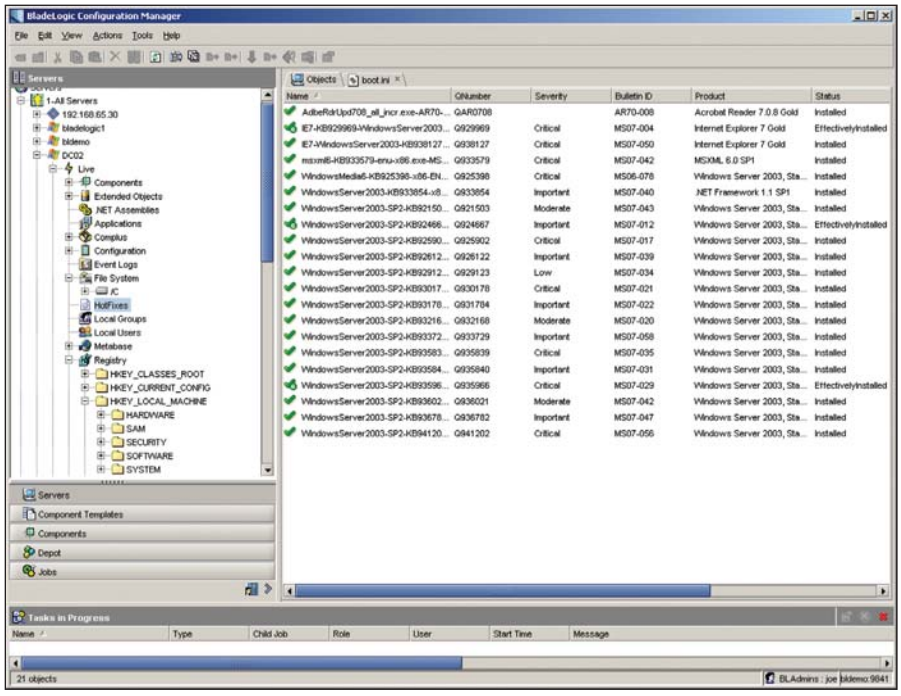


Bild 4: Über den Live-Zugriff auf einen Server kann sich ein Administrator schnell einen Eindruck vom Zustand eines Systems verschaffen

Neben direkten Vergleichen zum Aufzeigen von Unterschieden kann der Configuration Manager auch Compliance-Prüfungen durchführen, um festzustellen, ob bestimmte Vorgaben eingehalten werden. Ein Beispiel soll den Unterschied zwischen einem Vergleich und einem Compliance-Check aufzeigen: Bei einem Vergleich der vorgeschriebenen Passwortlänge zwischen zwei Systemen lässt sich als Ergebnis nur ermitteln, ob die Einstellungen identisch oder unterschiedlich sind. Ist der Wert aber auf beiden Systemen mit vier Zeichen viel zu kurz eingestellt, fällt dies beim Vergleich gar nicht auf, da identisch. Bei einer Compliance-Prüfung dagegen lässt sich eine minimale Passwortlänge vorgeben, sodass sinnvollerweise Systeme mit kürzerer Vorgabe auffallen, aber nicht, wenn am System eine noch größere Länge eingestellt ist. Hat ein Unternehmen nun bestimmte Compliance-Vorgaben einzuhalten, kann der Administrator diese als Komponentenvorlage definieren und alle Systeme regelmäßig dagegen prüfen. Weiterhin ist es möglich, Verstöße gegen die Compliance-Vorgaben über sogenannte "Remediation Packages" manuell oder automatisch zu korrigieren. BMC liefert diverse Compliance-Vorlagen mit, die unter anderem auf Empfehlungen für Sicherheitseinstellungen von CIS (Center for Internet Security), NSA und NIST basieren.

Provisionierung leicht gemacht

Für ein komplettes Lifecycle-Management übernimmt der Operations Manager die Installation neuer Server, die Installation von Softwarepaketen und auch das Patchmanagement. Neuinstallationen erfolgen dabei über eine eigene Konsole, den "Provisioning Manager". Bei den Installationsprozessen hat BMC nichts komplett Neues erfunden, sondern orientiert sich an den Möglichkeiten, die die Betriebssystemanbieter vorsehen. Linux- und Windows-Installationen starten mittels PXE-Boot. Je nachdem, ob mehr Windows- oder Linux-Systeme zu installieren sind, kann der Administrator vorgeben, ob neue Systeme, die sich beim PXE-Server melden, standardmäßig mit Gentoo oder WinPE 2.0 gebootet werden. Die MAC-Adresse erscheint dann im Provisioning Manager, damit der Administrator dieser einen Installationsauftrag zuweisen kann.

Entsprechende Konfigurationspakete lassen sich über den Provisioning Manager sehr komfortabel zusammenstellen, der Manager erstellt daraus die entsprechenden Steuerdateien (*unattend.txt*, AutoYast-Datei). Selbstverständlich können Pre- und Post-Jobs eingebunden werden, um gegebenenfalls die Hardware vorzukonfigurieren oder auch nach der Betriebssysteminstallation weitere Pakete aufzubringen. Im Test funktionierte die Installation weitgehend problemlos und es gelang, Server unter SLES 10, Windows 2003 Server 32 Bit sowie Windows 2008 Server 64 Bit aufzusetzen. Bei AIX- und Solaris-Systemen setzt der Provisioning

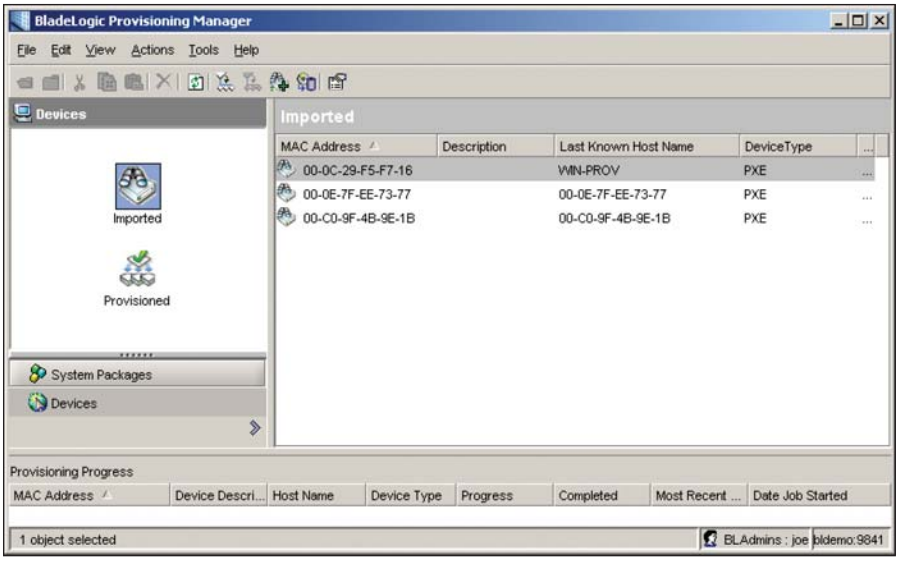


Bild 5: Dank PXE melden sich neue Systeme mit ihrer MAC-Adresse und können nun mit einem Systempaket installiert werden

Manager auf die in dem Umfeld üblichen Werkzeuge NIM und Jumpstart.

Umfassendes Reporting

Berichte und Analysen werden über ein Web-Portal bereitgestellt. In der Rubrik "Quick Reports" findet der Administrator eine Vielzahl an vorbereiteten Berichten, die mitgeliefert werden. Über die Funktion adhoc-Reports kann er mittels eines Assistenten eigene Berichte zusammenstellen. Die Berichte liefern auch Informationen über ausgeführte Jobs, um beispielsweise statistische Informationen zu durchgeführten Compliance-Prüfungen zu erhalten. Die Resultate können als CSV-, HTML- oder PDF-Dokument gespeichert und auch per Mail verschickt werden.

Produkt

Programm zur Datacenter Automation, Softwareverteilung, zum Patchmanagement, für Compliance-Prüfungen, Provisionierung und Fernadministration.

Hersteller

BMC Software
www.bmc.com

Preis

Die Lizenzierung erfolgt ohne Basispreis ausschließlich über die Anzahl der gemanagten Systeme mit entsprechender Mengenstaffelung.

IT-Verantwortliche, die den Einkauf der Bladeogic-Lösung planen, können mit Kosten von 1.200 Euro pro zu verwaltendem Client rechnen.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Installation	7
Bedienung	8
Funktionsumfang	9
OS-übergreifender Einsatz	9
Dokumentation	8

Dieses Produkt eignet sich

optimal für Umgebungen mit mehreren hundert oder gar mehreren tausend Servern, sowohl in homogenen Umgebungen als auch beim Einsatz unterschiedlicher Betriebssysteme.

bedingt für mittelgroße Netzwerke. Hier ist zu prüfen, ob sich Investition, Ausbildung der Administratoren und Grundaufwand für die Erstellung der Aufträge rechnen.

nicht für kleine Netze mit wenigen Servern. Hier rechnet sich der Betriebsaufwand nicht.

BMC Bladelogic Operations Manager

Fazit

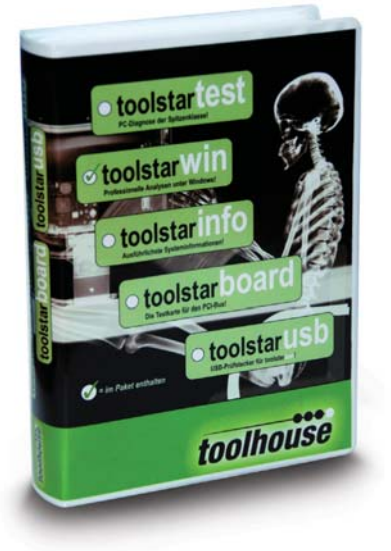
Wer das erste Mal mit dem Bladelogic Operations Manager konfrontiert wird, den machen die Versprechungen von BMC, beim Management vieler Server durchschnittlich 97 Prozent der Zeit einsparen zu können, erst einmal sehr skeptisch. Nach eingehender Betrachtung können wir diese Aussage jedoch bestätigen und es gibt zudem diverse Referenzen mit entsprechenden realen Erfahrungen. Letztendlich steigt der Umfang der möglichen Einsparungen mit der Anzahl der Server.

IT-Manager sollten sich allerdings darüber im Klaren sein, dass sie mit der Einführung einer solch leistungsfähigen Managementlösung nicht in dem Maße ihr Administratorenteam verkleinern können. Vielmehr lassen sich mit dem Einsatz einer derartigen Software mit dem gleichen Team mehr Systeme pflegen und so ein zukünftiges Wachstum bewältigen. Außerdem können Überprüfungen vor allem in Hinblick auf Konsistenz und Compliance realisiert werden, die vorher vom Aufwand her überhaupt nicht darstellbar waren. So lässt sich sehr effizient der Qualitätsstandard signifikant steigern, was den eigentlichen Vorteil der Software ausmacht.

Zu beachten ist, dass der Operations Manager nicht die Aufgabe des Monitorings übernehmen kann. Da die Agenten grundsätzlich passiv arbeiten, ist für die Weitergabe von plötzlich auftretenden Fehlern und für die Überwachung der Verfügbarkeit ein zusätzliches Produkt einzusetzen. *(jp)*

Im Test: Toolhouse Toolstar*testWIN 1.35

Dauertest auf Bit und Byte



von Jürgen Heyer

Sporadische Hardwarefehler sind in der Regel schwer zu finden, vor allem wenn sie nur selten auftreten und nicht reproduzierbar sind. Toolstar*testWIN bietet die Möglichkeit, jegliche Hardware unter Windows gezielt und auf Dauer zu testen, um so einem vermuteten Fehler schneller auf die Schliche zu kommen. IT-Administrator hat einige Systeme intensiv mit dem Tool geprüft, um sich einen Eindruck von der Software zu verschaffen.

Die im bayerischen Pfaffenhofen an der Ilm ansässige Firma Toolhouse hat sich auf Testsoftware und Diagnosekarten für PCs, IPCs, Notebooks und Server spezialisiert. Hinzu kommen noch Programme zur Datenrettung sowie zum Kopieren und Löschen von Festplatten. Die angebotene Diagnosekarte ist dann sinnvoll, wenn ein System schon bei der Initialisierung Schwierigkeiten hat. Bei der Testsoftware hat Toolhouse zwei Werkzeuge im Portfolio: "Toolstar* testOS" liefert der Hersteller auf einem bootfähigen USB-Stick aus, um Systeme unabhängig vom Betriebssystem testen und analysieren zu können. Das zweite Programm, "Toolstar*testWIN 1.35", welches wir in diesem Test eingehend untersucht haben, eignet sich für Systeme, auf denen Windows installiert ist und läuft. Aufgrund dieser Voraussetzungen ist der Einsatzbereich zwar nicht so breitbandig wie bei den anderen Tools, dafür wird aber nicht nur die Hardware analysiert und getestet, sondern auch das Betriebssystem.

Programmstart ohne Installation

Wie es sich für eine Testsoftware gehört, lässt sie sich ohne vorherige Installation starten. Das Programm selbst besteht aus einer gut 4 MByte großen EXE-Datei sowie einem kleinen INI-File, in dem die Programmeinstellungen hinterlegt sind. Es ist problemlos möglich, beide Dateien auf einen USB-Stick zu kopieren und von dort aus aufzurufen. Hinzu kommen gegebenenfalls noch Skriptdateien für selbst definierte Dauertests.

Die Benutzeroberfläche präsentiert sich sehr aufgeräumt mit drei Fenstern. Das Fenster "Hauptelemente" erlaubt einen Blick auf drei kompakte Systemübersichten mit den wichtigsten Informationen, Ergebnisberichten und abgespeicherten Dauertests. Ein zweites Fenster listet thematisch alle Elemente auf, die sich mit

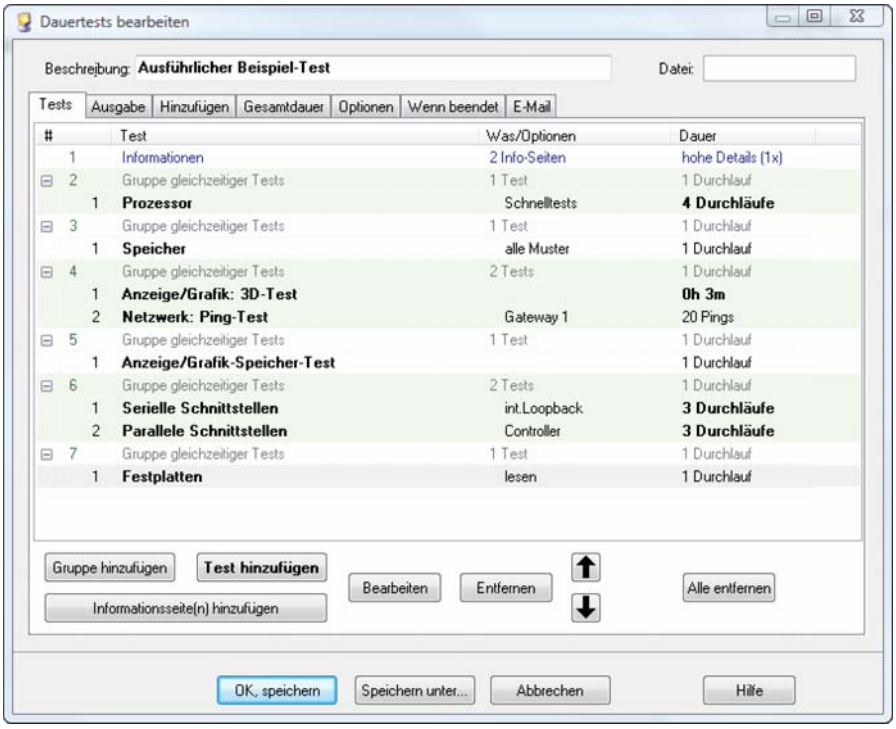


Bild 1: Dauertests lassen sich intuitiv zusammenstellen und laufen je nach Bedarf sequenziell oder auch parallel ab

dem Tool untersuchen lassen. Hier gibt es die drei gefilterten Ansichten "Alles", "Infos" und "Tests", außerdem ist eine Suche beziehungsweise Filterung nach einem eingegebenen Begriff möglich. Das ist vor allem dann sinnvoll, wenn Sie nach einem Test oder einer Information suchen, das Gesuchte aber aufgrund der Vielfalt an Optionen nicht auf Anhieb finden. Das dritte und größte Fenster liefert die Ergebnisse für das gewählte Thema. Bei der Ergebnisanzeige sind die Resultate häufig blockweise gegliedert, wobei Sie jeden Block individuell auf- und zuklappen können. Das hat den Vorteil, dass Sie als Betrachter nicht sofort mit endlos langen Informationen überschüttet werden. Vielmehr können Sie schrittweise vorgehen, um das zu finden, was Sie eigentlich interessiert. Insgesamt ist es trotz der vielen ermittelten Informationen kein Problem, gezielt etwas Bestimmtes zu finden.

Darüber hinaus hat der Anwender die Möglichkeit, diverse Programmeinstellungen anzupassen, wie die Inhalte der kompakten Systemübersichten, das Design der Benutzeroberfläche, den Umgang mit Skriptdateien für Dauertests, den Umfang an externen Tools, die sich direkt aufrufen lassen, und die E-Maileinstellungen für den Versand von SMTP-Mails.

Parallele Dauertests

Toolstar*testWIN ermöglicht es, praktisch alle Komponenten des Systems zu testen. Dazu ist eine Vielzahl an individuellen Tests integriert, wie beispielsweise diverse CPU-Tests (Kern, FPU, MMX, SSE, Cache), weiterhin Speicher-, Grafik- und Audiotests. Diese geben einen guten Überblick über den Systemzustand und dauern in der Regel nur einige Sekunden. Dies ermöglicht eine zügige Erstanalyse, außerdem lassen sich lastunabhängige Fehler so bereits frühzeitig feststellen. Je nach Art des Tests liefert das Programm entweder die Information, ob der Test bestanden wurde, oder entsprechende Messwerte. Beim Festplattentest bezüglich Oberfläche und Geschwindigkeit erhält der Anwender neben einigen Werten zusätzlich eine Grafik. Ein Tastaturtest ist ebenfalls integriert, um alle Tasten auf Funktion prüfen zu können.

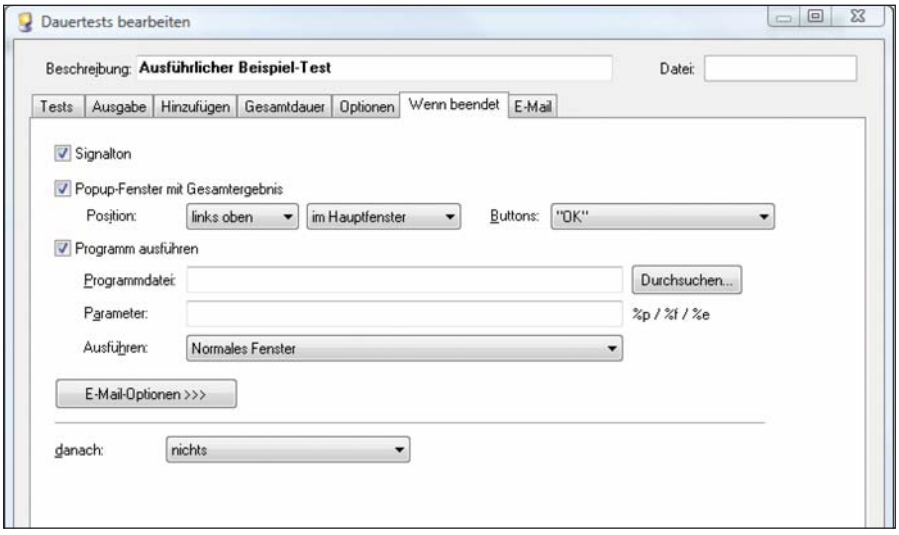


Bild 2: Es stehen verschiedene Möglichkeiten zur Verfügung, um das Ende eines Tests zu signalisieren

Um nun ein System gezielt über einen längeren Zeitraum oder in Hinblick auf eine permanente Belastung zu testen, erlaubt das Programm die Einrichtung von Dauertests. Die Möglichkeiten zur Definition dieser Dauertests sind beeindruckend. Vom Prinzip her lassen sich alle vorhandenen individuellen Tests zu automatisch ablaufenden Dauertests kombinieren. Die einzelnen Tests müssen dabei nicht zwingend sequenziell ablaufen, der Administrator kann auf Wunsch eine parallele Ausführung veranlassen. Hierzu legt er bei der Dauertest-Definition eine oder mehrere Gruppen gleichzeitiger Tests an und bestimmt dann, welche Einzeltests innerhalb der Gruppe ablaufen sollen.

Sowohl für den Gesamtablauf als auch für jede Gruppe und jeden Test kann der Administrator festlegen, wie oft, wie lange oder bis zu welcher Fehleranzahl diese durchgeführt werden sollen. Bei Multiprozessorsystemen können Sie zudem jedem Test eine CPU zuordnen. Der Test kann gleichzeitig mehrfach ablaufen, bis zu 32 CPUs lassen sich so ansprechen, sofern Windows dies unterstützt. Damit ist Toolstar*testWIN im Serverumfeld, wo häufig Mehrprozessorsysteme zum Einsatz kommen, gut geeignet.

Das Resultat des Tests kann die Software in eine Datei schreiben oder an eine bestehende anhängen, wahlweise im HTML-Format. Um die Einstellungen später nachvollziehen zu können, lässt sich einem Testprotokoll eine Systemübersicht mit dreierlei Umfang voranstellen. Statt vorher alle Informationen zu erfassen, kann ein Test die Gesamtdauer, den Ausgabedateinamen und Infos zum PC oder zum Tester abfragen. Dies erleichtert die spätere Zuordnung bei häufig wiederkehrenden Tests. Ist der Test abgeschlossen, kann dies das Programm durch einen Signalton melden, ein Pop-Fenster einblenden, ein Programm ausführen und/oder eine Mail per SMTP verschicken.

Auf Wunsch verschickt das Programm nicht erst beim Abschluss des Gesamttests, sondern bei Auftreten des ersten Fehlers eine Mail. Das erleichtert die Überwachung vor allem bei der Suche nach sporadischen Fehlern, da es regelmäßiges Nachsehen erspart. Vorteilhaft ist, dass die Konfiguration für jeden Dauertest in eine eigene Datei geschrieben wird. So lassen sich Tests problemlos weitergeben und mehrfach parallel einsetzen, indem Sie einfach die Testdateien mitkopieren.

Detaillierte Informationen über das Windows-System

Toolstar*testWIN liefert neben Informationen zur Hardware überaus viele

Details zur Windows-Konfiguration, wie einige nachfolgende Beispiele zeigen. So liefert das Programm Zusammenhänge wie beispielsweise eine Treiberliste bezogen auf die einzelnen Geräte. Beim Anklicken eines Treibers springt das Programm in den Gerätebaum und zeigt alle dazugehörigen Geräte- sowie Treiberdetails an.

Bei einem Notebook lassen sich genaueste Informationen zum Akkustatus und -zustand auslesen, also die vorgesehene Kapazität, die Kapazität bei voller Ladung und die durch Abnutzung verlorene Kapazität. Angezeigt wird zudem der aktuelle Leistungsverbrauch, der beispielsweise bei einer Änderung der Bildschirmhelligkeit variiert.

Ein Zähler für die Shared DLLs gibt Auskunft darüber, wie viele Programme eine DLL nutzen. Welche Programme das sind, verrät das Tool dann allerdings nicht. Bei der Diensteübersicht liefert das Programm auf einen Blick mehr Informationen als die Windows-eigene Diensteverwaltung. Statt jeden Eintrag öffnen zu müssen, zeigt Toolstar*testWIN für alle Dienste die interne Bezeichnung, den Dienstetyp, das Verhalten bei einem Fehler und den genauen Pfad auf einer Seite an. Am Fuß der Übersicht lässt sich zudem über eine Verknüpfung die Windows-Diensteverwaltung starten, um bequem Änderungen vornehmen zu können.

Sehr informativ ist die Auflistung der Zuordnung bekannter Dateiendungen mit den verknüpften Aktionen wie Öffnen oder Wiedergabe. Das Programm zeigt zusätzlich den Pfad zur ausführenden Datei an. Recht übersichtlich werden die Rubriken der Ereignisanzeige dargestellt, sodass die Meldungen besser lesbar sind als mit dem Windows-Bordmittel. Vorteilhaft ist, dass die gesamten Inhalte der Meldungen einsehbar sind, ohne jede einzeln öffnen zu müssen. Eine farbige Schrift unterscheidet zwischen Informationen, Warnungen und Alarmen.

Natürlich lassen sich sehr viele dieser Informationen auch mit Windows-Bordmitteln auslesen. Der Anwender muss hierzu aber auf diverse Tools zugreifen und an mehreren Stellen nachsehen, während Toolstar*testWIN alles aus einer Hand liefert und zugleich übersichtlicher aufbereitet.

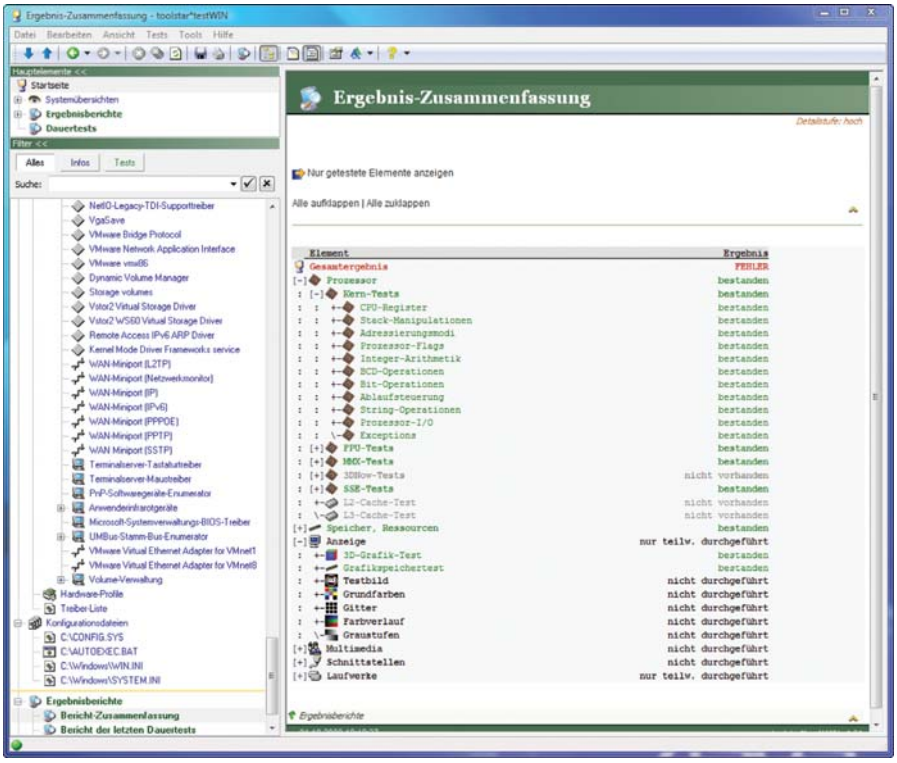


Bild 3: Das Programm listet die Resultate eines Tests übersichtlich auf und signalisiert Fehler durch rote Einträge

Ändern der Einstellungen über eine einzige Oberfläche

Neben dem reinen Auslesen von Informationen und der Durchführung von Tests erlaubt Toolstar*testWIN weiterhin das recht einfache Ändern diverser Einstellungen. Dies umfasst beispielsweise die Parameter der Eingabegeräte, also die Mausgeschwindigkeit, das Aktivieren eines Mausschattens und einer Zeigerspur sowie die Zeitintervalle beim Klicken. Komfortabel ist, dass sich aus dem Tool heraus gleich der entsprechende Bereich der Systemsteuerung öffnen lässt.

Bezüglich der Verwendung des Internet Explorers ermöglicht das Programm eine einfache Änderung der Farbeinstellungen für den Hintergrund sowie besuchte und nicht besuchte Links. Allerdings zeigt sich hier noch etwas Optimierungsbedarf. Es sind nämlich nicht alle notwendigen Einstelloptionen vorhanden, damit eventuelle Farbänderungen auch tatsächlich greifen. Hierzu sind im Internet Explorer selbst zusätzlich einige Parameter zu ändern. Darauf angesprochen, will der Hersteller dies im nächsten Update ergänzen. Das Löschen der Historie der eingegebenen URLs funktioniert dagegen einwandfrei. Bezüglich weiterer Interneteinstellungen ermöglicht das Programm einen schnellen Zugriff auf Parameter, die an sich fast unbekannt sind, aufgeteilt in neun Rubriken wie Zugriff, Browsen, Sicherheit, Java und Multimedia.

Toolstar*testWIN listet alle Autostart-Einstellungen auf und erlaubt es, einzelne abzuwählen. So lassen sich mit wenigen Mausklicks lästige Programme abschalten, die sonst beim Booten immer mitstarten. Zudem ist es möglich, installierte Software zu deinstallieren. Dazu zeigt eine lange Liste alle installierten Programme sowie Hotfixes beziehungsweise Service Packs an. Mit Vorsicht zu genie-

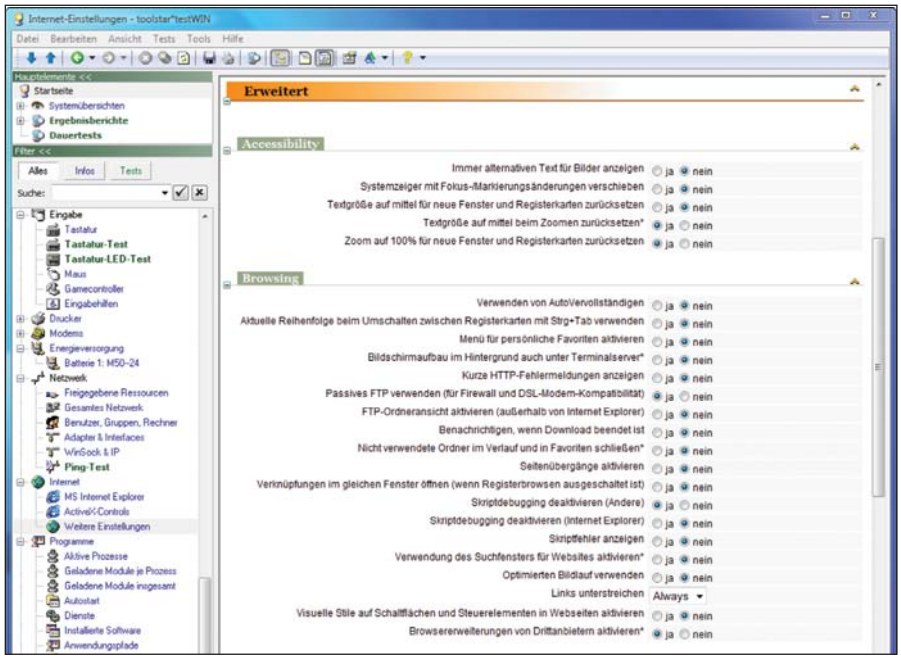


Bild 4: Neben Tests und dem Auslesen von Informationen erlaubt das Tool auch die Anpassung vieler Einstellungen

ßen ist die Möglichkeit, dass sich statt einer Deinstallation auch ein Eintrag aus dieser Liste löschen lässt. Die Folge ist, dass sich das Programm dann nicht mehr über die Systemsteuerung deinstallieren lässt. Toolstar*testWIN erlaubt es ferner, die Windows-Konfigurationsdateien *(Config.sys, autoexec.bat, boot.ini, win.ini und system.ini)* einzusehen und zu editieren. Ein Zugriff auf die Registry ist allerdings nicht vorgesehen.

Neben der Anzeige des Inhalts des CMOS-RAMs ermöglicht das Tool auch das Sichern und Wiederherstellen der Inhalte. Diese werden dazu in eine Datei geschrieben. Neben dem CMOS-RAM kann das Programm den Bootsektor sichern und wiederherstellen. Ändern lassen sich weiterhin die Eigenschaften der Anzeige, hier bietet das Programm einige Parameter mehr zur Änderung an als das Windows-Bordmittel. Ebenso lässt sich der Bildschirmschoner konfigurieren.

Alles in allem sind die Einstellungen sehr vielfältig, auch wenn einige Parameter mehr den Spieltrieb anregen dürften, als dass sie wirklich wichtig sind. Aber das Programm zwingt ja niemanden dazu, irgendwelche Desktopfarben zu ändern. Allerdings ist es nicht vorgesehen, den Stand der editierbaren Einstellungen zu speichern, um diesen dann wiederum auf mehreren Systemen anzuwenden und so schnell eine einheitliche Konfiguration zu erhalten.

Um die externen Schnittstellen genauer zu testen, bietet Toolstar optional ein sogenanntes Techpack an, bestehend aus einem seriellen und einem parallelen Prüfstecker sowie einer Test-CD und einer Test-DVD. Letztere sind komplett beschrieben, um zu prüfen, ob sie auch tatsächlich von der ersten bis zur letzten Spur ausgelesen werden können. Mit speziellen Bitmustern lassen sich zudem Lesefehler aufdecken. Neben dem Techpack ist noch ein optionaler USB-Prüfstecker erhältlich.

Fazit

Toolstar*testWIN überzeugt durch umfassende und sorgfältig zusammengetragene Möglichkeiten zum Ermitteln vieler Systeminformationen, bietet umfassende Testmöglichkeiten und die Änderung diverser Einstellparameter. Eine wertvolle Hilfe beim Aufdecken von sporadischen Fehlern sind auf jeden Fall die individuell konfigurierbaren Dauertests, um gezielt bestimmte Komponenten zu stressen beziehungsweise länger unter Hochlast zu betreiben. Nur an wenigen Stellen sehen wir noch etwas Optimierungspotenzial. Hierzu ist festzustellen, dass der Hersteller das Produkt kontinuierlich weiterentwickelt. Wichtig ist zu beachten, dass Toolstar*testWIN ein laufendes Windows voraussetzt, andernfalls ist Toolstar*testOS mit selbstbootendem USB-Stick einzusetzen. *(ln)*

Produkt
Tool zum Testen der Hardware und des Betriebssystems unter Windows.

Hersteller
Toolhouse
www.toolhouse.de

Preis
Toolstar*testWIN kostet 229 Euro. Interessant sind auch Bundles, die verschiedene Tools des Herstellers beinhalten.

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

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

Installation	10
Bedienung	9
Funktionsumfang	8
Übersichtlichkeit der GUI	8
Dokumentation	6

Dieses Produkt eignet sich

optimal zum Test unterschiedlichster Hardware in kleinen und mittleren Umgebungen, sofern Windows installiert ist und läuft.

teilweise zum Test unterschiedlichster Hardware in größeren Umgebungen, sofern Windows installiert ist und läuft.

nicht zum Test von Geräten, die mit einem anderen Betriebssystem als Windows konfiguriert sind oder wenn aufgrund eines Fehler Windows nicht mehr gestartet werden kann.

Toolstar*testWIN 1.35

Die kompakte IT-Administrator-Heftsammlung

mit den Ausgaben 01/08 bis 12/08 im PDF-Format auf CD

Sie sind bereits IT-Administrator-Abonnent?
Dann erhalten Sie die Jahres-CD 2008 jederzeit für nur € 37,90.

Sie möchten Abonnent werden und die Jahres-CD 2008 gleich mitbestellen? Abonnieren Sie noch heute das günstige Schnupperabo und bestellen Sie die Jahres-CD für nur € 37,90 dazu.

Sie möchten nur die Jahres-CD 2008? Für € 49,90 erhalten Sie die kompakte IT-Administrator-Heftsammlung.

www.it-administrator.de

administrator Das Magazin für professionelle System- und Netzwerkadministration

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

☐ **Ja**, als bestehender IT-Administrator-**Jahresabonnent** (auch ermäßigt) möchte ich die Jahres-CD 2008 zum **Sonderpreis von € 37,90** inklusive Versand und 19% MwSt. bestellen.

☐ **Ja**, ich möchte das **Schnupperabo (= 6 Ausgaben)** des IT-Administrator zum **Vorzugspreis von € 37,80** inkl. Versand und 7% MwSt (€ 41,70 im Ausland) mit **50% Rabatt** auf den Preis der Einzelausgabe testen. Mir ist bekannt, dass das Schnupperabo frühestens nach Erhalt der 6. Ausgabe kündbar ist. Wenn ich mich nicht innerhalb von 10 Tagen nach Erhalt des 6. Hefts melde, erhalte ich **12 x im Jahr** den IT-Administrator zum Jahrespreis von € 135,- inkl. Versand und 7% MwSt (€ 150,- im Ausland). Ich kann das anschließende Jahresabonnement jederzeit kündigen. Das Geld für bezahlte und noch nicht gelieferte Hefte erhalte ich zurück.

☐ **Ja**, ich möchte die **Jahres-CD 2008 zum Sonderpreis von € 37,90** inklusive Versand und 19% MwSt. zu meinem Abonnement dazubestellen.

☐ **Ja**, ich möchte **nur die Jahres-CD 2008 zum Preis von € 49,90** inklusive Versand und 19% MwSt. bestellen.

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: Kto.: BLZ:

oder ☐ per Rechnung

Datum: Unterschrift:

Firma:

Name, Vorname:

Straße:

Land, PLZ, Ort:

Tel:

E-Mail:

ITA 02209

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

Spannende Software zum Testen inklusive

Im Test: Servicetrace ServiceTracer

SLAs messen, nicht schätzen!

von Jürgen Heyer

Wer genaue Informationen zur Verfügbarkeit einer Netzwerkverbindung oder einer Applikation benötigt, kann auf ein zuverlässiges Mess- und Monitoring-Werkzeug nicht verzichten. Dies gilt sowohl für die Überwachung an sich, als auch für den Nachweis zur Einhaltung von SLA-Verträgen oder für den eigenen Wunsch zur Darstellung und Verbesserung einer IT-Dienstleistung. Die Monitoring-Software ServiceTracer zeigte im IT-Adminstrator-Test, wie sie diese Aufgaben bei gleichzeitig erfreulich geringem Personalaufwand übernimmt.

In der heutigen IT ist es durchaus üblich, die Verantwortlichkeit für eine bestimmte Dienstleitung auf mehrere Schultern zu verteilen oder Teile einer Gesamtdienstleistung mittels Outsourcing an externe Vertragspartner zu übergeben. Dies beginnt beispielsweise damit, dass Server und vor allem externe Netzwerkverbindungen bei entsprechenden Providern angemietet werden. Hierbei werden stets Verträge und SLAs (Service Level Agreements) abgeschlossen, die auch Aussagen zur garantierten Verfügbarkeit beinhalten. Ein Dienstleistungsangebot setzt sich meist aus mehreren Modulen zusammen, bestehend aus angemieteten Diensten und eigenen Bausteinen, die womöglich noch von unterschiedlichen Abteilungen betrieben werden.

Bild 1: Das Alerting Dashboard informiert den Administrator kompakt über aktuelle Alarme und Probleme

Die resultierende Dienstleistung ist nur dann verfügbar, wenn alle einzelnen Module korrekt arbeiten. Sobald nun eine Störung auftritt (ist etwa eine Netzwerkverbindung unterbrochen, ein Webportal nicht mehr verfügbar oder reagiert eine Applikation nicht mehr), ist es wichtig, dieses Fehlverhalten möglichst schnell zu entdecken, wichtige Personen zügig zu alarmieren und die exakte Ursache zeitnah zu ermitteln, um letztlich die End-to-End-Verfügbarkeit wiederherzustellen. Weiterhin geht es bei SLA-Verträgen darum, deren Einhaltung nachzuweisen, da andernfalls unter Umständen Vertragsstrafen fällig werden.

Modulare Überwachung

Derartige Aufgaben übernimmt die modular aufgebaute Software ServiceTracer der fast gleichnamigen deutschen Firma Servicetrace. Im Rahmen dieses Tests haben wir uns neben dem zentralen TraceManagement-Server mit den Modulen zum Netzwerk- und Applikations-Monitoring eingehender beschäftigt, weiterhin bietet Servicetrace Module zum Monitoring von Servern und SAP-Installationen an.

Eine Umgebung zur Netzwerk- und Applikationsüberwachung besteht aus einem TraceManagement-Server, mindestens einem NetworkTracer sowie mindestens einem ServiceTracer-Client. Je nach Aufgabenstellung kann der TraceManagement-Server auch als NetworkTracer arbeiten und zugleich ServiceTracer-Client sein. Der TraceManagement-Server stellt die Zentrale von ServiceTracer dar, läuft dediziert im RZ und beinhaltet das Datawarehouse, die Webservices, die zentrale Steuereinheit (Control Center), das Reporting und das Alerting.

Das Modul NetworkTracer überwacht die durchgängige Netzwerkqualität beispielsweise von der Firmenzentrale zu allen externen Lokationen oder auch die Erreichbarkeit eines Portals von verschie-

denen Stellen im Internet. Ein ServiceTracer-Client prüft die Funktion einer Applikation, indem er sich quasi wie ein Anwender verhält und Eingaben auf einem System simuliert.

Reibungslose Installation

Obwohl Servicetrace eine deutsche Firma ist, die allerdings auch in Russland und Indien programmieren lässt, ist die gesamte Software ebenso nur in Englisch verfügbar wie die Dokumentation. Der Hersteller empfiehlt als Basis für den TraceManagement-Server einen englischen Windows 2003 Server mit IIS sowie einen englischen MS SQL-Server 2005. Die Testumgebung konfigurierten wir entsprechend, wobei Servicetrace für die korrekte Einrichtung der genannten Grundvoraussetzungen eine Checkliste liefert. Die eigentliche Installation des TraceManagement-Servers benötigt nur sehr wenige Eingaben wie das Installationsverzeichnis und einen Lizenzschlüssel. Sehr vorteilhaft ist hierbei, dass das Setup die SQL-Datenbank komplett inklusive aller Tabellen, der benötigten SQL-Benutzer und deren Rechten vollautomatisch anlegt. In der Regel übernimmt Servicetrace die Erstinstallation beim Kunden und verbindet dies gleich mit einer entsprechenden Einweisung.

Nach der Installation folgt eine einfache Grundkonfiguration. ServiceTracer ist mehrmandantenfähig, damit beispielsweise ein Provider mehrere Kunden sauber getrennt verwalten kann. Nach dem Anlegen eines Kunden ("Customer") sind die verschiedenen Aufgaben (Überwachung der Applikationen und Netzwerkverbindungen) sowie die beteiligten Clients, die Lokationen und die Stationen mit ServiceTracer-Clients zu definieren. Durch eine hierarchische Struktur ergibt sich dabei eine recht eingängige Übersicht über den gesamten Systemaufbau. Zu jeder Aufgabe lassen sich individuelle Servicezeiten mit Vertragszeitraum sowie geplante Nichtverfügbarkeiten (Downtimes) eintragen. Der Vertragszeitraum ist insofern wichtig, als sich beispielsweise im Laufe der Zeit die Servicezeiten ändern können. Geplante Ausfallzeiten wiederum dürfen sich nicht negativ auf die ermittelte Verfügbarkeit auswirken. All diese Angaben spielen bei der Erstellung der Reports und der gesamten Auswertung eine große Rolle, da in erster Linie die Verfügbarkeit während der Servicezeit das entscheidende Kriterium für die Einhaltung einer SLA ist. In den grafischen Berichten sind Zeitabschnitte, die eine geplante Nichtverfügbarkeit enthalten, andersfarbig hinterlegt, um dies auch zu visualisieren.

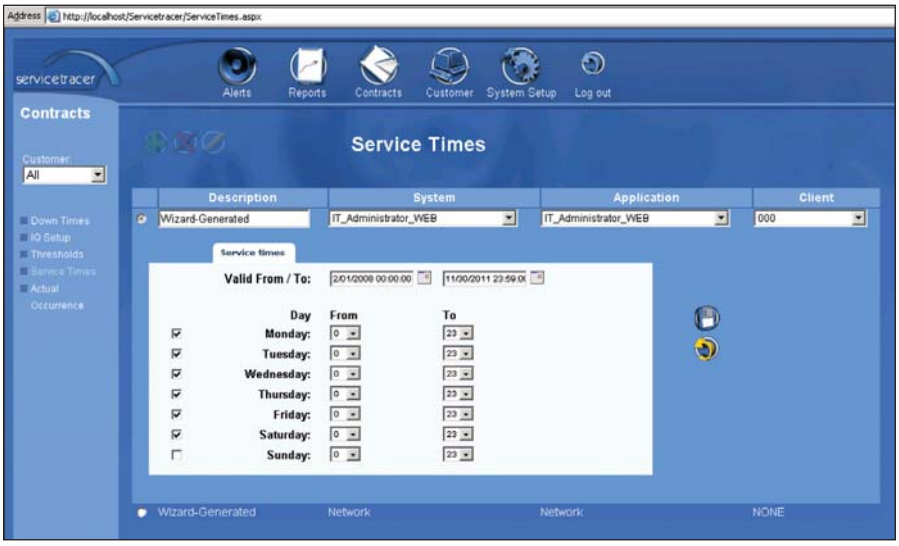


Bild 2: Erst die Berücksichtigung der Service-Zeiten und der Vertragslaufzeit ermöglicht das Erstellen aussagekräftiger und korrekter Reports

TraceManagement-Server:
Empfohlen Windows 2003 Server (englisch), .NET-Framework, IIS Webserver, Microsoft SQL-Server 2005 (englisch)

NetworkTracer und ServiceTracer-Client:
Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP (32/64 Bit), Windows Server 2000, Windows Server 2003 (32/64 Bit)

Systemvoraussetzungen

Bezüglich einer hohen Verfügbarkeit des TraceManagement-Servers ist in erster Linie darauf zu achten, dass die SQL-Datenbank möglichst verfügbar ist und regelmäßig mit den datenbankeigenen Mechanismen gesichert wird. Ist der TraceManagement-Server einmal für externe NetworkTracer beziehungsweise ServiceTracer-Clients nicht verfügbar, so arbeiten diese eigenständig weiter, speichern die Messdaten lokal und aktualisieren dann, wenn die Verbindung wieder klappt, den TraceManagement-Server. So ist sichergestellt, dass die Messungen auch vollständig dokumentiert sind.

Zentrale Agenten-Steuerung

Mittels des Control Centers steuert der TraceManagement-Server sämtliche NetworkTracer sowie ServiceTracer-Clients. Von hier aus lassen sich neue Aufträge einstellen und Änderungen vornehmen. Im Hinblick auf die Systemsicherheit ist die Kommunikation so gestaltet, dass nicht der TraceManagement-Server auf alle externen Systeme zugreift, da dies eine entsprechende Menge offener Webservices erfordern würde.

Vielmehr stellt der TraceManagement-Server über einen Webservice die entsprechenden Aufträge und Kommandos bereit, die die externen Systeme dort abholen. So ist nur ein System vom Zugriff her abzusichern. Bei der Fernsteuerung eines Clients macht sich diese Arbeitsweise allerdings in einer geringen Trägheit bemerkbar.

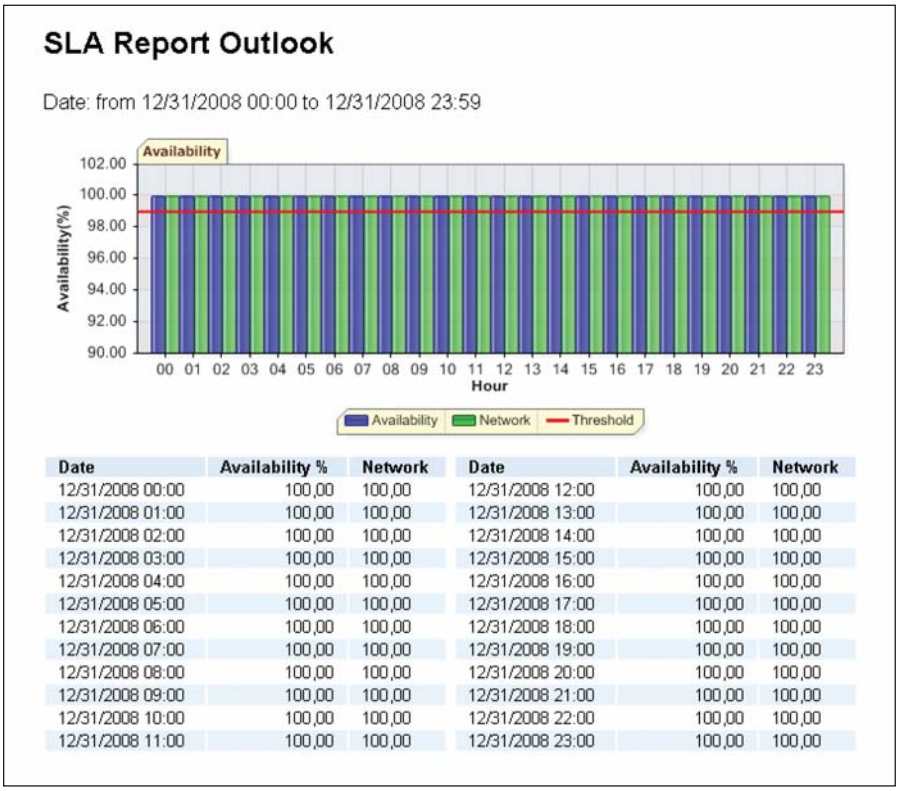
Netzwerk-Monitoring mit Fehlerisolation

Das Monitoring von Netzwerkstrecken übernimmt der sogenannte Network-

Tracer, der im einfachsten Fall mit auf dem TraceManagement-Server installiert wird und von dort aus die Erreichbarkeit verschiedener IP-Adressen, zum Beispiel die Router in externen Lokationen oder auch Systeme mit bestimmten Applikationen, regelmäßig prüft. Weitere NetworkTracer können auf anderen Systemen mitinstalliert werden, wenn beispielsweise eine komplexe und vermaschte Umgebung zu überwachen ist. Da der NetworkTracer als Dienst im Hintergrund läuft und wenig Last erzeugt, sind keine Konflikte mit anderen Applikationen zu befürchten.

Beim Anlegen einer Messung lässt sich neben einer Zieladresse auch eine Backup-Adresse eintragen, weiterhin ist die Tracemethode anzugeben, gegebenenfalls der gewünschte Port, der maximal zulässige Timeout und das Prüfintervall. Bei den Tracemethoden stehen zehn unterschiedliche Möglichkeiten (Ping, TCP-Ping, FTP-, HTTP-, HTTPS-, SMTP-, POP3-, IMAP-Request, TCP-Port-Check und Traceroute) zur Verfügung, sodass individuell bedarfsorientiert geprüft werden kann. Um die Anzahl der Datensätze sinnvoll zu reduzieren, lassen sich mehrere Messungen zu einem Output in Form eines Datenbankeintrags zusammenfassen.

Um bei negativen Resultaten die Fehlerquelle schneller eingrenzen zu können, verfügt der NetworkTracer über ein spezielles Feature, den optional aktivierbaren "Error Trace". Für einen Error Trace lassen sich weitere Ziele eintragen, die ebenfalls mit den oben genannten Methoden adressiert werden können. Der Error Trace wird nur abgearbeitet, wenn die Hauptmessung fehlschlägt und liefert dann weitere Analysedaten. Beispielsweise nutzen größere Firmen aus Redundanzgründen für ihren Internetzugang mehrere Provider und haben mehrfache Netzwerkanbindungen. Ein Error Trace kann nun alle Übergabepunkte prüfen, um zu ermitteln, ob einer der Provider ein Problem hat. Ebenso kann der Administrator bekannte IP-Adressen, die auf dem Weg der eigentlich zu vermessenden End-to-End-Verbindung liegen, ansprechen, um so die fehlerhafte Strecke einzugrenzen.



Date	Availability %	Network	Date	Availability %	Network
12/31/2008 00:00	100,00	100,00	12/31/2008 12:00	100,00	100,00
12/31/2008 01:00	100,00	100,00	12/31/2008 13:00	100,00	100,00
12/31/2008 02:00	100,00	100,00	12/31/2008 14:00	100,00	100,00
12/31/2008 03:00	100,00	100,00	12/31/2008 15:00	100,00	100,00
12/31/2008 04:00	100,00	100,00	12/31/2008 16:00	100,00	100,00
12/31/2008 05:00	100,00	100,00	12/31/2008 17:00	100,00	100,00
12/31/2008 06:00	100,00	100,00	12/31/2008 18:00	100,00	100,00
12/31/2008 07:00	100,00	100,00	12/31/2008 19:00	100,00	100,00
12/31/2008 08:00	100,00	100,00	12/31/2008 20:00	100,00	100,00
12/31/2008 09:00	100,00	100,00	12/31/2008 21:00	100,00	100,00
12/31/2008 10:00	100,00	100,00	12/31/2008 22:00	100,00	100,00
12/31/2008 11:00	100,00	100,00	12/31/2008 23:00	100,00	100,00

Bild 3: Eine gute Grafik sagt mehr als tausend Worte: Keine Probleme mit Outlook

Bilderkennung zur Applikations-Steuerung

Während ein NetworkTracer für die Überwachung von Netzwerkverbindungen zuständig ist, übernimmt ein ServiceTracer-Client die Prüfung von Applikationen auf einem System und meldet die Resultate an den TraceManagement-Server. Der Client läuft als Dienst auf dem System und emuliert quasi einen Benutzer mit seinen Eingaben. Diese Emulation erfolgt skriptgesteuert, wobei sich der Ablauf über das Tool "STC Eagle" und dessen Assistenten ähnlich wie bei einem Makrorekorder schrittweise zusammenklicken lässt. Bei Verwendung des Assistenten generiert dieser automatisch das Skript. Abgesehen davon ist die verwendete Skriptsyntax relativ einfach und orientiert sich an Basic, sodass eine Einarbeitung nicht übermäßig schwierig ist.

Um die Steuerung der Applikationen möglichst universell und systemunabhängig zu gestalten, bedient sich STC Eagle einer automatischen Muster- beziehungsweise Bilderkennung. Das Tool verhält sich letztendlich analog zu einem Benutzer, der mit seinen Augen ein Icon oder anderes Objekt sucht und anklickt oder ein Feld markiert und Zeichen eingibt.

Beim Start der Aufzeichnung legt der Administrator erst einmal fest, welche Aktionen (Mausbewegungen, Tastatureingaben, Bildsuche) berücksichtigt werden sollen. Angenommen, eine Applikation wird über eine Verknüpfung auf dem Desktop gestartet, markiert er das entsprechende Icon und legt noch einen Suchbereich für das markierte Objekt fest. Hier ist etwas Erfahrung notwendig, damit möglichst nur ein kleiner Bereich abgesucht werden muss und das Objekt trotzdem mit großer Sicherheit gefunden wird. Um die Suche zu vereinfachen und zu optimieren, führt STC Eagle eine Bildtransformation durch, bei der es die Grafik auf die Kontraste reduziert und die Farbe herausnimmt. Für eine optimierte Erkennung lässt sich der Schwellwert für den Kontrast verändern, eine Prüfmög-

Bestellen Sie jetzt das zweite IT-Administrator Sonderheft

180 Seiten Praxis-Know-how rund um Exchange 2003/2007 + Tools-CD

zum Abonnenten-Vorzugspreis* von

nur € 29,90

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

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

IT administrator
Das Magazin für professionelle System- und Netzwerkadministration

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

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

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

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

Ich zahle ☐ per Bankeinzug

Geldinstitut:

Kto.: BLZ:

oder ☐ per Rechnung

Datum:

Unterschrift:

Firma:

Name, Vorname:

Straße:

Land, PLZ, Ort:

Tel:

E-Mail:

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

ITA 0209

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

lichkeit für die Erkennungszuverlässigkeit hilft bei der Abstimmung. Durch dieses Verfahren kann das Tool beispielsweise unterschiedliche Desktophintergründe ignorieren, und die Erkennung ist unabhängig von der verwendeten Farbeinstellung.

Anschließend legt der Administrator fest, wo auf die gefundene Grafik geklickt werden soll,und führt diese Aktion dann auch im Assistenten durch, sodass wie im vorliegenden Fall die Applikation gestartet wird. Auf der Oberfläche der Applikation markiert er wieder einen eindeutigen Grafikabschnitt sowie einen dazugehörigen Suchbereich. Wichtig ist es, beispielsweise bei einem Webseitenaufruf ein Objekt zu wählen, welches erst ziemlich zum Schluss erscheint, denn dessen Erkennung ist für STC Eagle das Zeichen, dass dieser Schritt abgeschlossen ist und der nächste gestartet werden kann. Optional misst das System die Zeiten für die einzelnen Schritte, um Performanceschwankungen aufzeichnen zu können. Auf diese Art und Weise wird ein kompletter Ablauf per Assistent zusammengeskriptet. Die zweifache Bilderkennung garantiert, dass die Steuerung genau mit der Verarbeitungsgeschwindigkeit Schritt hält. Plötzlich auftretende Popups von anderen Applikationen werden übrigens erkannt, sodass sie den Erkennungsvorgang und damit den Ablauf nicht behindern.

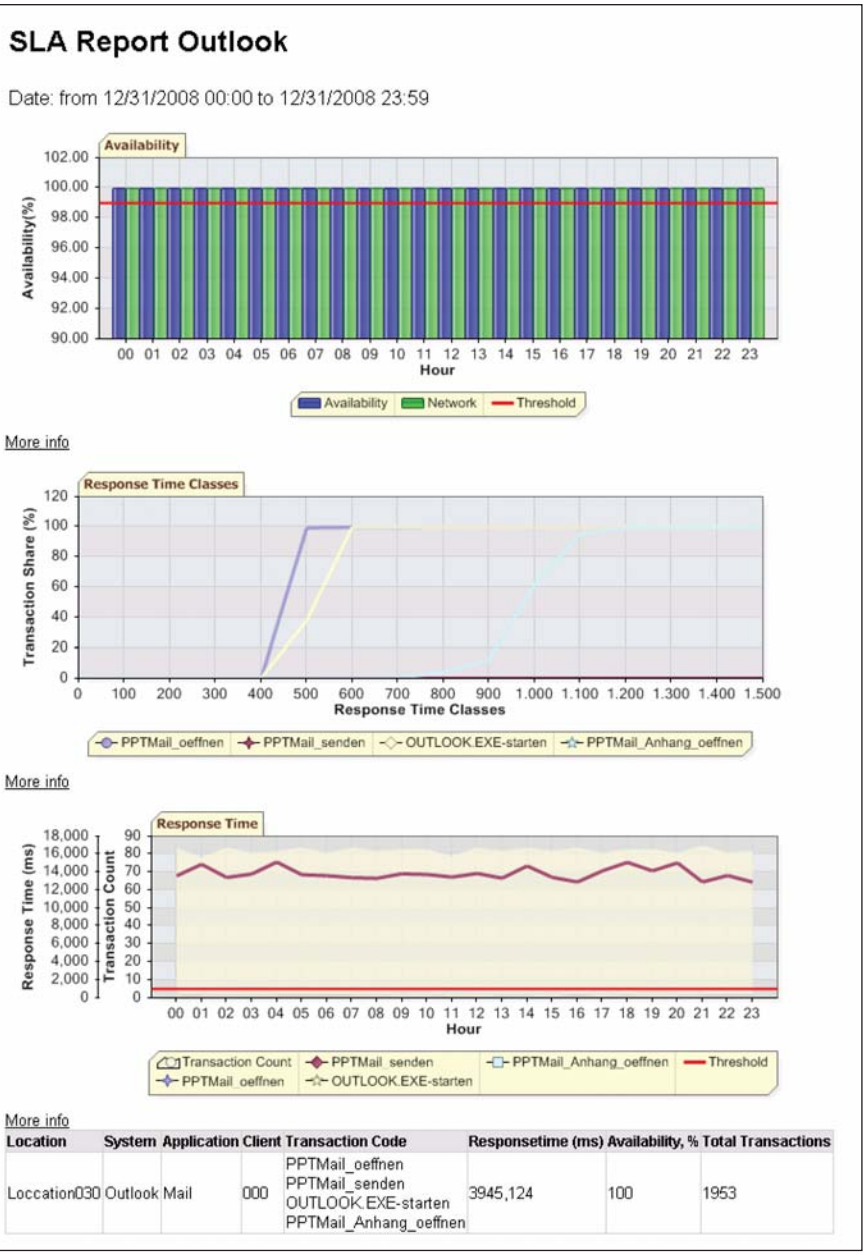


Bild 4: Die kompletten Kennzahlen einer Applikation im Überblick

Ist das Skript fertiggestellt, wird es mit einem Zeitplan verknüpft, sodass es vollautomatisch läuft. Zusätzlich zu dem Zeitplaner lässt sich mittels eines Workflows definieren, welche Aktionen beispielsweise bei Fehlschlagen des Ablaufs ausgeführt werden sollen. So lässt sich neben dem Absetzen von Alarmmeldungen auch ein anderes Skript starten.

Im Test zeigte sich, dass die Erstellung solcher Prüfszenarien mit die zeitaufwendigste Arbeit ist. Vorteilhaft ist, dass einmal erstellte Abläufe dann durchaus auf mehreren ServiceTracer-Clients ohne weitere Anpassung fehlerfrei funktionieren, auch wenn die Systeme nicht absolut identisch aufgebaut sind. Bei einem Update der gesteuerten Applikation (etwa von MS Office 2003 auf 2007, von IE6 auf IE7) hängt es immer davon ab, wie groß die Änderungen an der Oberfläche sind, ob Anpassungen erforderlich sind oder nicht.

Vielseitiges Reporting

Äußerst vielseitig ist das Reporting gestaltet, und es gibt mehrere Möglichkeiten, die Messresultate einzusehen. Einen groben, aber sehr schnellen Einblick gewährt das der Alarmierung zugeordnete Dashboard. Das sogenannte "General Dashboard" zeigt dabei die Verfügbarkeiten sowie Antwortzeiten grafisch und als Ampelstatus auf.

Das "Alerting Dashboard" dagegen signalisiert aktuelle Alarme. Diese können auch verschickt werden, wobei ServiceTracer dies via SMTP, SNMP-Trap und SMS unterstützt. Wann ein Alarm vorliegt, kann der Administrator für jeden Prüfjob individuell festlegen und sowohl für eine Warnung als auch für einen Fehler entsprechende Schwellwerte (Antwortzeiten oder prozentuale Verfügbarkeiten) vorgeben.

Sinnvoll ist auch die Möglichkeit festzulegen, dass erst bei mehreren fehlgeschlagenen Messungen alarmiert wird. So lassen sich unnötige Fehlalarme aufgrund einzelner fehlgeschlagener Messungen vermeiden. Genauso lassen sich Alarme auf Statusänderungen beschränken, damit bei einem länger andauernden Fehler nicht ständig alarmiert wird.

Produkt
Programm zum Netzwerk- und Applikations-Monitoring.

Hersteller
Servicetrace
www.servicetrace.de

Preis
Einstiegs-Bundles werden ab 15.000 Euro angeboten.

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

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

Installation	9
Bedienung	7
Funktionsumfang	8
Übersichtlichkeit der GUI	8
Dokumentation	6

Dieses Produkt eignet sich

optimal für Windows-Umgebungen und Firmen, die viele zeitkritische Netzwerkverbindungen und/oder Applikationen betreiben. Optimal ist ServiceTracer weiterhin einsetzbar, wenn in Windows-Umgebungen Verfügbarkeiten im Rahmen von SLAs nachzuweisen sind.

bedingt in heterogenen Umgebungen, da der ServiceTracer-Client ebenso wie der NetworkTracer als Betriebsplattform ein Windows-System voraussetzt. Zugriffe auf Nicht-Windows-Systeme sind aber möglich.

nicht für Unternehmen, die weder zeitkritische Applikationen betreiben noch wichtige End-to-End-Verbindungen unterhalten oder die gänzlich auf Windows-Systeme verzichten wollen.

Servicetrace ServiceTracer

Das eigentliche Reporting bereitet die Daten für eine Bereitstellung im HTML- und PDF-Format auf. Das Layout der Auswertungen kann dabei individuell auf die Wünsche des Providers abgestimmt und mit entsprechenden Logos versehen werden, sodass der Endkunde dann ansprechend aufbereitete Auswertungen erhält. Dass bei der Erstellung der Reports nach Servicezeiten und entsprechend der Vertragslaufzeit gefiltert wird sowie eventuelle geplante Downtimes berücksichtigt werden, wurde weiter oben schon erwähnt.

Eine Besonderheit ist, dass in die Reports auch externe Daten eingebunden werden können. Gibt es also beispielsweise noch ein anderes Auswertungswerkzeug, so können die Daten in ServiceTracer importiert werden, um dann einen umfassenden Report mit einheitlichem Aussehen zu erzeugen. Hierzu ist nur einmalig ein Importprofil anzulegen, welches dann immer wieder verwendet werden kann. Insgesamt lässt sich das gesamte Reporting so weit automatisieren, dass die komplette Auswertung zeitgesteuert erfolgt und dann beispielsweise als PDF-Datei dem Endkunden automatisch per Mail zugestellt wird. Nach der erstmaligen Einrichtung sind außer bei Änderungen keine regelmäßigen manuellen Eingriffe notwendig.

Fazit

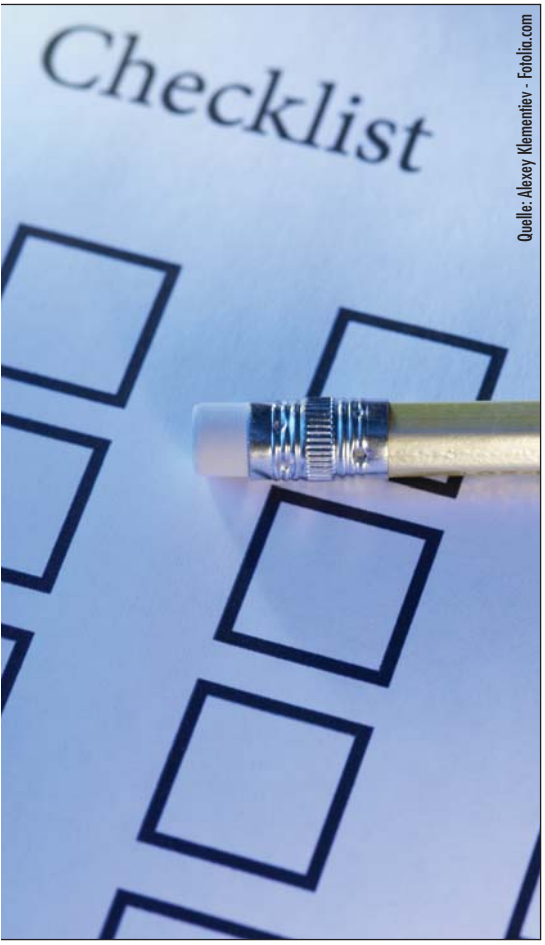
Im Test erwies sich ServiceTracer als sehr vielseitig und effizient einsetzbares Werkzeug, das auf einen sehr hohen Automatisierungsgrad hin konzipiert ist. Vor allem überzeugen die speziellen Funktionen wie das Durchführen von ergänzenden Messungen im Netzwerk, wenn die Hauptmessung fehlschlägt. Recht zuverlässig arbeitet auch die implementierte Bilderkennung. Nach einer Einweisung und Basisinstallation durch den Hersteller ist eine schnelle Lernkurve zu erwarten, da die meisten Arbeiten assistentengestützt durchgeführt werden können. Programmierkenntnisse sind zwar von Vorteil, aber nicht unbedingt erforderlich, und eine Einarbeitung in die Basic-ähnliche Programmierung dürfte recht schnell gelingen. *(jp)*

Netzwerkrichtlinien mit Windows Server 2008 (1)

Sicherheit per Checkliste

von Thomas Joos

Ein neues Sicherheits-Feature im Windows Server 2008 stellt der Netzwerkzugriffsschutz namens "Network Access Protection" dar. Über diesen können Unternehmen anhand entsprechender Richtlinien sicherstellen, dass nur solche Clients Zugang zum Firmennetz erhalten, die bestimmten Sicherheitskriterien genügen. IT-Administrator stellt Ihnen den Einsatz von NAP in einem dreiteiligen Workshop vor.



Quelle: Alexey Klementiev - Fotolia.com

Die Network Access Protection überprüft, ob alle Sicherheitsanforderungen auf den Clients eingehalten werden

Die für die Network Access Protection (NAP) erforderliche Client-Software ist in Vista und Windows Server 2008 bereits enthalten, während für Windows XP SP2 oder Windows Server 2003 eine separat zu installierende NAP-Client-Software angeboten wird. Im Service Pack 3 für Windows XP ist dieser Client ebenfalls integriert. Mit den zugehörigen Richtlinien kann zum Beispiel ein NAP-Server feststellen, ob Remote-PCs, die über ein VPN Verbindung zum Firmennetz herstellen möchten, die Sicherheitsrichtlinien des Unternehmens einhalten. Trifft dies nicht zu, lehnt der VPN-Server die Verbindung ab. Genauso ermittelt der Netzwerkzugriffsschutz, ob ein im LAN befindlicher Computer die gesetzten Sicherheitskriterien erfüllt und gewährt oder verweigert ihm damit den Zugang zum Firmennetz. Auch DHCP-Server, Switches und Terminalserver unterstützen diese Funktion. Auf der TechNet-Seite unter [1] erhalten Sie interessante Infos direkt von den NAP-Entwicklern aus erster Hand.

Patch-Kontrolle und sichere IP-Adressvergabe

Durch den Einsatz von NAP lässt sich feststellen, ob Sicherheits-Patches aufgespielt sind und ob der Computer durch Antiviren- sowie Antispyware-Programme geschützt wird. Erfüllt ein Client diese Kriterien nicht, weist NAP ihn ab oder leitet ihn in eine eingeschränkte Umgebung um, wo er zunächst aktualisiert wird. Dort können Clients von einem FTP- oder WSUS-Server Updates herunterladen und aufspielen, um ihre Sicherheitskonfiguration auf den neuesten Stand zu bringen und so die definierten Zugangsvoraussetzungen zu erfüllen.

Durch die DHCP-Adressvergabe können DHCP-Server Richtlinien für Integritätsanforderungen immer dann erfordern, wenn ein Computer versucht, im Netzwerk eine IP-Adresskonfiguration zu leasen oder zu erneuern. Mithilfe der 802.1X-Erzwingung weist ein Netzwerkrichtlinienserver (Network Policy Server, NPS) über NAP einen 802.1X-basierten Zugriffspunkt (einen Ethernet-Switch oder einen drahtlosen Zugriffspunkt) an, für den 802.1X-Client so lange ein eingeschränktes Zugriffsprofil zu verwenden, bis eine Reihe von Korrekturfunktionen ausgeführt wurden. Die 802.1X-Erzwingung bietet einen sicheren eingeschränkten Netzwerkzugriff für alle Computer, die auf das Netzwerk über eine 802.1X-Verbindung zugreifen.

Microsoft plant derweil, Forefront Client Security direkt mit der neuen Netzwerkzugriff-Schutzfunktion von Windows Server 2008 zu verbinden. Dabei kann der NAP-Server feststellen, ob ein Client mit den aktuellen Antiviren-Updates versorgt ist und basierend auf diesen Informationen eine Netzwerkrichtlinie anwenden, die den Client entweder isoliert oder gar nicht erst mit dem Netzwerk kommunizieren lässt. Außerdem wird in diesem Fall eine automatische Aktualisierung veranlasst. Stellt Forefront Client Security auf einem Client einen Virus fest, kann der NAP-Server diesen PC vom Netzwerk im laufenden Betrieb isolieren. Durch diesen neuen Sicherheitsmechanismus können ungeschützte Clients nicht mehr ein ganzes Netzwerk verseuchen. Damit NAP

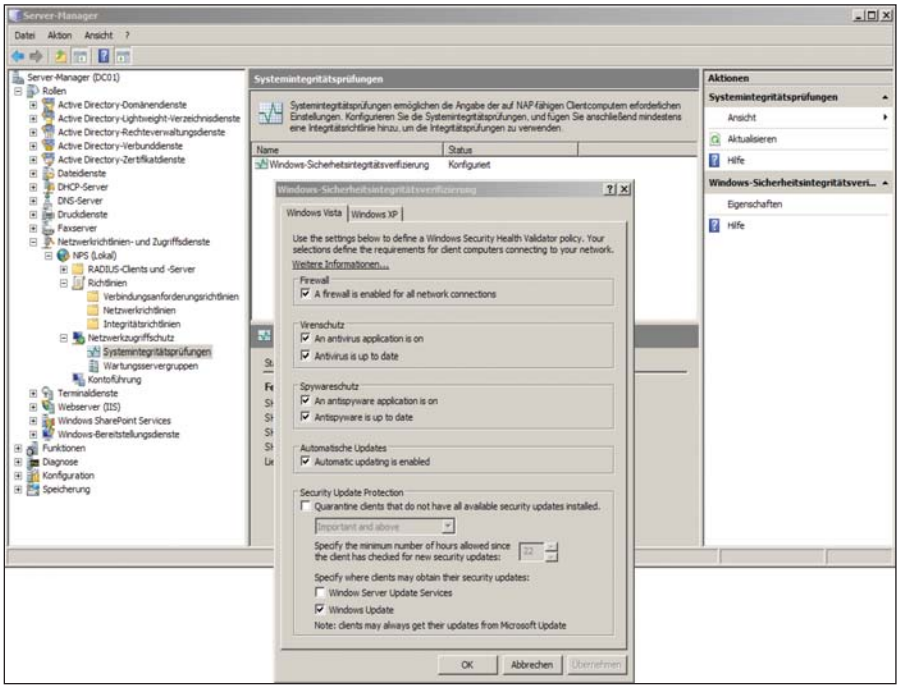


Bild 1: Mit NAP im Windows Server 2008 werden Clients vor der Netzwerkverbindung auf eine sichere Konfiguration hin überprüft

eingesetzt werden kann, muss nicht das ganze Netzwerk auf Windows Server 2008 umgestellt werden, ein Mischbetrieb mit Windows Server 2003 ist ohne Weiteres möglich.

Terminalserver absichern

NAP unterstützt nicht nur Domänencomputer, sondern auch Computer, die nicht Mitglied einer Domäne sind. Neben der NAP-Funktionalität bietet ein Netzwerkrichtlinien- und Zugriffsserver auch die Remote-Einwahl. Die Remote Authentication Dial-In User Service (RADIUS)-Funktion des Windows Server 2008 ersetzt den Internet Authentication Service (IAS) von Windows Server 2003. NAP können Sie auch in Windows Server 2003-Domänen nutzen, allerdings muss der Netzwerkrichtlinienserver (Network Policy Server, NPS) unter Windows Server 2008 laufen. Grundsätzlich ist NAP eine Weiterentwicklung der Network Access Quarantine aus dem Windows Server 2003. Damit der Zugriff eines PCs überprüft werden kann, findet folgender Vorgang statt:

1. Ein Client-PC will sich mit dem Netzwerk verbinden.
2. Als Nächstes generiert der Client ein Statement of Health (SoH). Der NAP-Client weiß, wie er das System untersuchen muss und kann einen Bericht erstellen, der an den Netzwerkrichtlinien-Server übergeben wird.
3. Dieser Server entscheidet auf Basis der zentralen Richtlinie, ob das Statement of Health gültig ist oder nicht.
4. Auf Basis dieses Ergebnisses wird eine Richtlinie verwendet, die den Zugriff gestattet oder nicht.

Sie können für die NAP-Infrastruktur ungeschützte Bereiche von DMZs und geschützte Bereiche unterscheiden. In den geschützten Bereichen stehen zum Beispiel Ihre Datei- oder Exchange-Server. In der DMZ könnte dagegen ein WSUS-Server oder der DHCP-Server stehen. Der ungeschützte Bereich bleibt von der NAP vollkommen unberücksichtigt. Wichtig ist hier die Art und Weise, wie der Zugriff auf das Netzwerk stattfindet. Clients können sich per VPN einwählen, auf ein Terminalserver-Gateway zugreifen oder sich mit dem Netzwerk verbinden. Findet die Verbindung über das Hausnetzwerk statt, benötigt ein Client zunächst eine IP-Adresse von einem DHCP-Server. Dieser Zugriff sollte also gestattet werden. Nicht konforme Clients können sogar am Beziehen einer DHCP-Adresse gehindert werden. Auch der Zugriff per WLAN lässt sich über NAP steuern. Ein Client, der nicht konform ist, sollte aber Gelegenheit haben, zumindest auf den WSUS-Server zuzugreifen.

Funktionsweise der Richtlinien

Netzwerkrichtlinien (Network Policies) steuern den Netzwerkzugriff von Clients basierend auf Integritätsrichtlinien (Health Policies), die wiederum auf den Systemintegritätsprüfungen (System Health Validators, SHVs) aufbauen. Nachdem Sie über die Systemintegritätsprüfungen konfiguriert haben, welche Bedingungen ein NAP-konformer Client erfüllen muss, legen Sie mit den Integritätsrichtlinien fest, ob ein Client NAP-konform ist oder nicht. Das bedeutet, ein Client muss erst bestimmte Bedingungen erfüllen – zum Beispiel die Installation aktueller Patches oder eines Virenschutzes. Meldet er diesen Zustand und erfüllt damit die Systemintegritätsrichtlinie, ist er NAP-konform. Erfüllt er die Bedingungen in den Systemintegritätsprüfungen nicht, ist er nicht NAP-konform und darf entweder gar nicht oder nur eingeschränkt mit anderen Rechnern kommunizieren, bis die Systemintegritätsprüfungen erfüllt sind. Die Netzwerkrichtlinien steuern wiederum, was mit NAP-konformen beziehungsweise nicht NAP-konformen

Bild 2: Auf den Computern werden Meldungen angezeigt, ob eine Netzwerkverbindung auf Basis der Richtlinien erlaubt oder verweigert wird

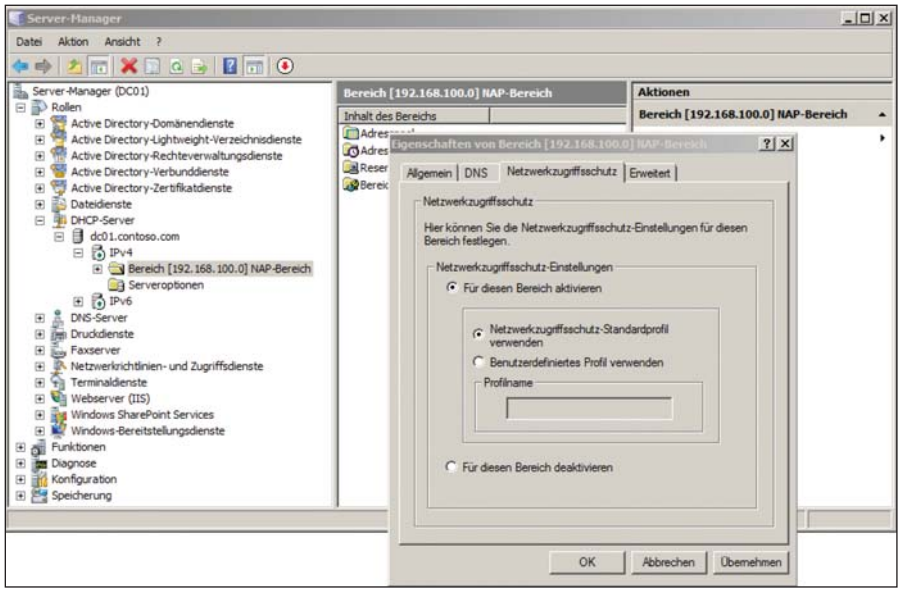


Bild 3: Über den Server-Manager aktivieren Sie den Netzwerkzugriffsschutz für einen DHCP-Bereich

Clients im Netzwerk passieren soll und welchen Zugriff diese erhalten dürfen. Die NAP-Infrastruktur basiert daher auf den drei Pfeilern

- Systemintegritätsprüfungen (System Health Validators)
- Integritätsrichtlinien (Health Policies)
- Netzwerkrichtlinien (Network Policies)

Verwenden Sie IPSec, erhalten NAP-konforme Clients ein Zertifikat und können anschließend mit anderen Rechnern über IPSec kommunizieren. Entspricht ein Client nicht den Richtlinien, erhält er auch kein Zertifikat und kann mit anderen IPSec-geschützten Computern nicht kommunizieren. Für das Ausstellen dieser Zertifikate ist der NAP-Server zuständig. Eine eigene PKI (Public Key Infrastructure) benötigen Sie für diese Funktion nicht unbedingt. Die Komponente in der Network Access Protection, die dieses Zertifikat ausstellt, trägt die Bezeichnung "Health Registration Authority" (HRA) – bei den Zertifikaten handelt es sich um standardmäßige X.509-Zertifikate.

Der Client sendet also seine Anforderung an die IPSec Enforcement Component und verwendet dazu entweder HTTP oder HTTPS (dies lässt sich über die Gruppenrichtlinien steuern). Diese sendet dann das Statement of Health des Clients (SoH) an die HRA, welche wiederum die Anfrage an den Netzwerkrichtlinienserver (Network Policy Server, NPS) weiterreicht. Dieser gibt nun die Information an den HRA zurück, ob der Client konform ist oder nicht und verweist den Client falls nötig an die Wartungsserver – etwa einen Server mit WSUS 3.0, von dem der Client aktuelle Patches beziehen kann. Ist der Client NAP-konform, teilt die HRA ein Zertifikat zu. Ist der Client nicht konform, erhält er kein Zertifikat, sondern die Anforderung, sich mit dem Wartungsserver zu verbinden. Der Client sendet in diesem Fall eine Update-Anforderung an den Wartungsserver. Nach der Aktualisierung sendet der Client erneut seinen SoH an den HRA.

Abgeschottete Netzbereiche nutzen

IEEE 802.1x ist ein Standard zur Authentifizierung in Netzwerken und stellt eine Möglichkeit dar, nicht konforme Clients vom Produktivnetz zu trennen. Der Standard beschreibt die Zuordnung von zwei logischen Ports (Controlled, Uncontrolled) zu einem physikalischen Port. Der physikalische Port leitet die empfangenen Pakete zunächst an den "Uncontrolled Port". Der "Controlled Port" kann nur nach erfolgreicher Authentifizierung erreicht werden. Nicht konforme Geräte werden durch das 802.1x-Gerät (zum Beispiel einen Switch) blockiert oder in ein spezielles virtuelles LAN (VLAN) verschoben.

Bei externen Verbindungen über eine RAS- oder VPN-Einwahl wählen sich PCs über das Internet oder per DFÜ ins Netzwerk ein und können auch hier auf ihre

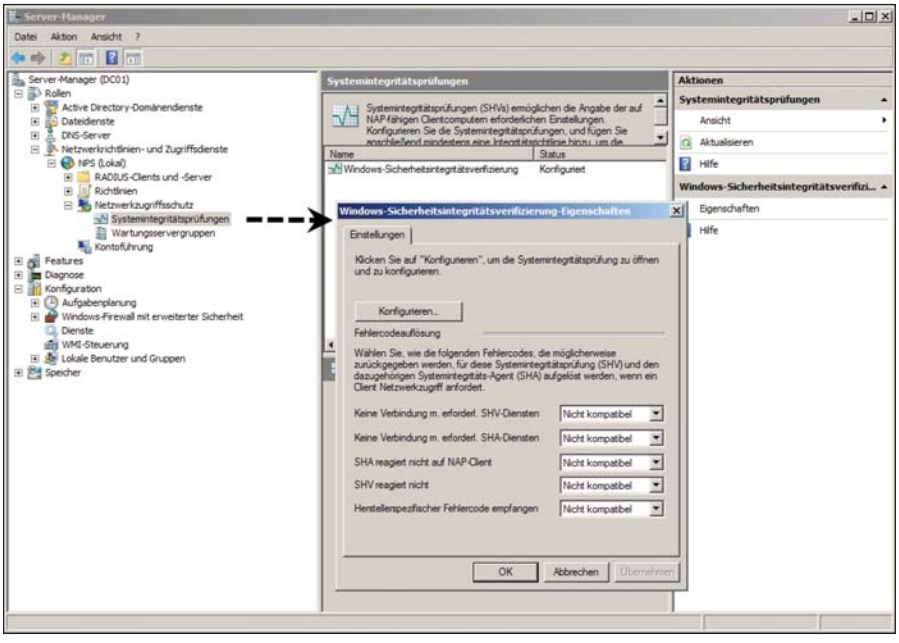


Bild 4: Beim Konfigurieren der Sicherheitsintegritätsverifizierung legen Sie fest, welche Fehlercodes als Nichtkompatibilität gedeutet werden

NAP-Konformität überprüft werden. Unter Windows Server 2003 stand für diese Funktion noch die Quarantäne-Lösung zur Verfügung. Diese wurde mit dem Windows Server 2008 durch NAP ersetzt und ist nun deutlich effizienter und leichter zu konfigurieren. Auch Terminalserver-Gateways unterstützen NAP. Ein TS-Gateway verbindet mehrere Terminalserver über HTTP/RDP-Kommunikation mit dem Internet. Diese Funktion ist neu in Windows Server 2008.

Weitere Möglichkeiten, Rechner zu isolieren, liegen im Bereich von DHCP. Nicht konforme NAP-Clients können am Beziehen einer IP-Adresse durch einen DHCP-Server gehindert werden. Alternativ erhalten die Clients spezielle IP-Adressen und kein Standardgateway. DHCP-Server unter Windows Server 2008 haben bei der Konfiguration eines Bereiches für die Verwaltung von NAP eine zusätzliche Registerkarte, über welche Sie die NAP-Unterstützung aktivieren können.

Auch das Cisco-Pendant zur Microsoft Network Access Protection mit der Bezeichnung "Cisco Network Admission Control" (NAC) arbeitet mit NAP zusammen. Es gibt gemeinsame Produkttests und die Entwicklung findet Hand in Hand statt. Sie können in NAP-Lösungen damit auch NAC-Komponenten von Cisco integrieren und umgekehrt. Der NAP-Client in Windows Vista unterstützt so auch Cisco NAC und Sie müssen Sie keinen zusätzlichen Client installieren. Neben Cisco unterstützen auch zahlreiche andere Unternehmen NAP, dazu gehören Nortel oder Juniper. Eine ausführliche Liste finden Sie auf der Microsoft-Seite zu NAP unter [2]. Ausführliche Informationen zur NAP/NAC-Interoperabilität bietet zudem ein Microsoft-Whitepaper unter [3]. Die Interoperabilität zu Cisco sieht folgendermaßen aus:

1. Der Client sendet sein Statement of Health (SoH) an den Cisco Secure Access Control Server (ACS)
2. Der ACS sendet das SoH an den Netzwerkrichtlinienserver (Network Policy Server) weiter. Dabei wird das Host Credential Authorization Protocol (HCAP) verwendet.
3. Auf Basis der Richtlinien des NPS wird der Zugriff des Clients gesteuert.

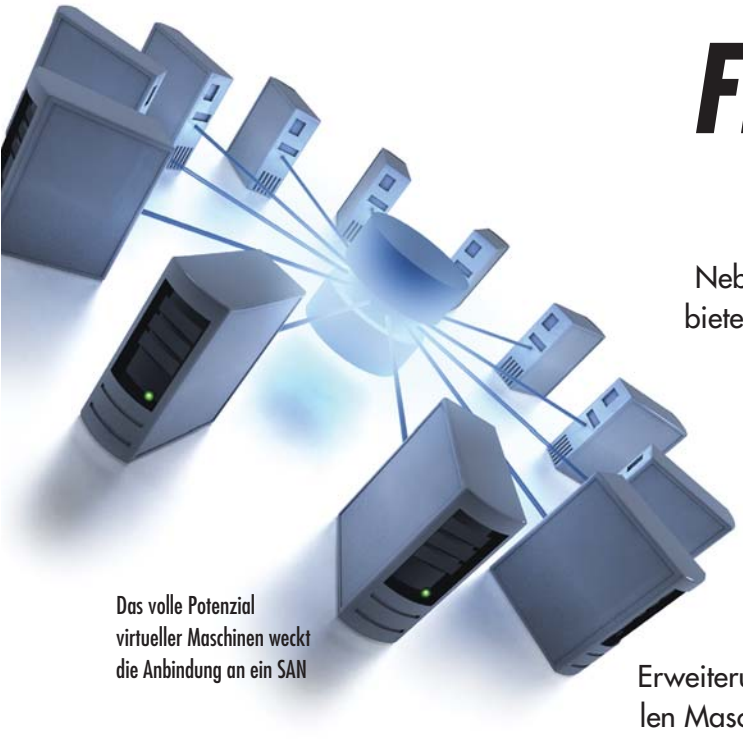
Damit sind die NAP-Einstellungen erledigt. Im zweiten Teil unserer Workshopserie zeigen wir Ihnen, wie Sie NAP einführen und testen und den DHCP-Server unter Windows Server 2008 für die Network Access Protection konfigurieren. Außerdem gehen wir im Weiteren auf die VPN-Konfiguration für den sicheren Netzwerkzugriff ein. *(dr)*

Links

[1] **Entwicklerinfos zu NAP im TechNet-Blog**
http://blogs.technet.com/nap

[2] **Microsoft-Webseite zu NAP**
www.microsoft.com/nap

[3] **Whitepaper über NAP/NAC-Interoperabilität**
http://download.microsoft.com/download/c/1/2/c12b5d9b-b5c5-4ead-a335-d9a13692abbb/TNC_NAP_white_paper.pdf



Das volle Potenzial virtueller Maschinen weckt die Anbindung an ein SAN

iSCSI-SAN und Virtualisierung

Fliegende Wechsel

von Thomas Weyergraf

Neben der besseren Auslastung vorhandener Serverressourcen bietet Virtualisierung vor allem eine logische Trennung zwischen Gastsystem und zugrunde liegender Hardware. Virtuelle Maschinen werden erzeugt, betrieben, heruntergefahren und unter Umständen wieder gelöscht, ohne den zugrunde liegenden Server zu beeinträchtigen. Ein hervorstechendes Merkmal ist dabei die Migration: Ein Gastsystem lässt sich im laufenden Betrieb von einem physikalischen Server auf einen anderen unterbrechungsfrei verschieben. Muss der Administrator einen Server zu Wartungs- oder Erweiterungszwecken herunterfahren, werden die laufenden virtuellen Maschinen auf einen anderen Server verschoben, um dort ihren Dienst ohne Unterbrechung zu verrichten. Dazu ist jedoch ein SAN Voraussetzung. Der folgende Workshop zeigt, wie Sie iSCSI-SANs einsetzen, um das Potenzial der Virtualisierung voll zu entfalten.

Zu den beiden Open Source-Lösungen Xen und KVM sind bereits einige Artikel im IT-Administrator erschienen, die beide Konzepte erklären und dem Anwender die ersten Schritte ermöglichen. Zudem steht eine zweiteiliger Artikel mit einer praktischen Einführung in iSCSI unter Linux zur Verfügung. Im Kasten "Ressourcen" am Ende dieses Beitrags sind alle Artikel aufgeführt, die im IT-Administrator erschienen sind und auf die dieser Workshop aufbaut.

Performant nur im SAN

Die Vorteile eines unterbrechungsfreien Betriebs und die dynamische Auslastung vorhandener Serverressourcen bei Lastspitzen, indem virtuelle Maschinen abhängig von der durch sie erzeugten Last auf physikalische Server verteilt werden, liegen auf der Hand. Will der Administrator das Potenzial, das Migration bietet, ausnutzen, ist der Einsatz eines SANs unausweichlich. Der Grund dafür ist recht einfach: Allen virtuellen Maschinen – im Folgenden kurz VM genannt – wird sowohl von Xen als auch von KVM Festplattenspeicher zugewiesen. Um eine VM von einem Server auf einen andern zu migrieren, muss auf beiden Servern die Festplatte der VM über den gleichen Device-Eintrag erreichbar sein.

Ein Beispiel: Konfigurieren Sie eine VM, die auf der Partition "/dev/sda5" arbeitet, und migiriert diese auf einen anderen Server, erwartet die VM ihre Daten dort ebenfalls unter "/dev/sda5". Bei statischen Partitionen, wie im Beispiel, schlägt dies normalerweise fehl – mit "/dev/sda5" wird auf beiden Systemen nicht die gleiche Partition angesprochen. Die Virtualisierungslösung erwartet eine "einheitliche Sicht" auf den Speicher.

Verwenden Sie für die VM Dateien anstelle von Block-Devices, ist die Lösung recht einfach: Die Dateien mit den VM-Daten können auf einem NFS-Share abgelegt werden, der auf allen Servern im jeweiligen Dateisystem gleich gemountet wird. Sinnvoll ist dies jedoch allenfalls bei VMs, die keine hohe IO-Last erzeugen, denn dateibasierte VMs sind in der Regel schlichtweg nicht performant genug. Der Ausweg besteht in einem SAN, welches Festplattenkapazität zur Verfügung stellt und dabei allen beteiligten Servern netzweit eine gleiche Adressierung bereitstellt.

iSCSI und die Alternativen

Im Folgenden betrachten wir iSCSI, jedoch ist dies nicht die einzige Möglichkeit. Alternativ bieten sich Fibre Channel (FC-AL)-Lösungen an, oder gar Cluster-Dateisysteme. Während FC-AL eine ausgereifte, schnelle und auch verbreitete Möglichkeit darstellt, sind Cluster-Dateisysteme derzeit noch etwas exotischer und weniger weit verbreitet. FC-AL ist mit vergleichsweise hohen Kosten verbunden,

vor allem wenn Ausfallsicherheit mittels Storage-Switches hergestellt werden soll.

iSCSI hat eine ganze Reihe von Vorteilen: Es verwendet kostengünstige Ethernet-Infrastrukturen und lässt sich mit Linux-Bordmitteln aus Open Source-Komponenten aufbauen. Zukünftig steigende Anforderungen an die Leistung lassen sich durch dedizierte iSCSI-Storagehardware, etwa von EMC oder IBM, befriedigen. Reicht die Bandbreite von gegenwärtigen Ethernet-Verbindungen nicht aus, bietet sich Infiniband an. Es existieren iSCSI-Protokollstacks, die über Infiniband arbeiten. Im Linux-Umfeld sind diese sogar ebenfalls als Open Source lizenzkostenfrei erhältlich.

Bandbreitenplanung ist das halbe Leben

Bevor Sie mit der Implementierung eines SANs zur Unterstützung der Virtualisierung und insbesondere der VM-Migration beginnen, sind ein paar grundsätzliche Überlegungen sinnvoll. Für den Normalbetrieb einer VM reicht es, die Netzwerkverbindungen für das iSCSI-SAN dergestalt auszulegen, dass die Bandbreite ausreichend dimensioniert ist, um die Transferrate des Festplattensubsystems aufnehmen zu können. Bei großen RAID-Arrays werden Transferraten von mehreren 100 MByte/s erreicht. Eine einzelne GBit-Verbindung reicht dazu nicht mehr aus. 10-GBit-Ethernet ist derzeit nur vereinzelt zu finden und in Serversystemen noch kein Ausstattungsstandard. 10-GBit-Switche sind zudem noch exorbitant teuer.

Infiniband ist – insbesondere bei kleinen Switchen – im deutlichen Kostenvorteil, jedoch muss auch hier jeder Server mit einem Infiniband-Adapter ausgerüstet werden, was ebenfalls die Kosten nach oben treibt. Einen kostengünstigen Ausweg gibt es jedoch: "Link Aggregation", also das Zusammenfassen mehrerer physikalischer Ethernet-Verbindungen zu einer logischen. Diese logische Verbindung bietet im Idealfall die kumulierte Bandbreite aller eingesetzten Ethernet-Verbindungen.

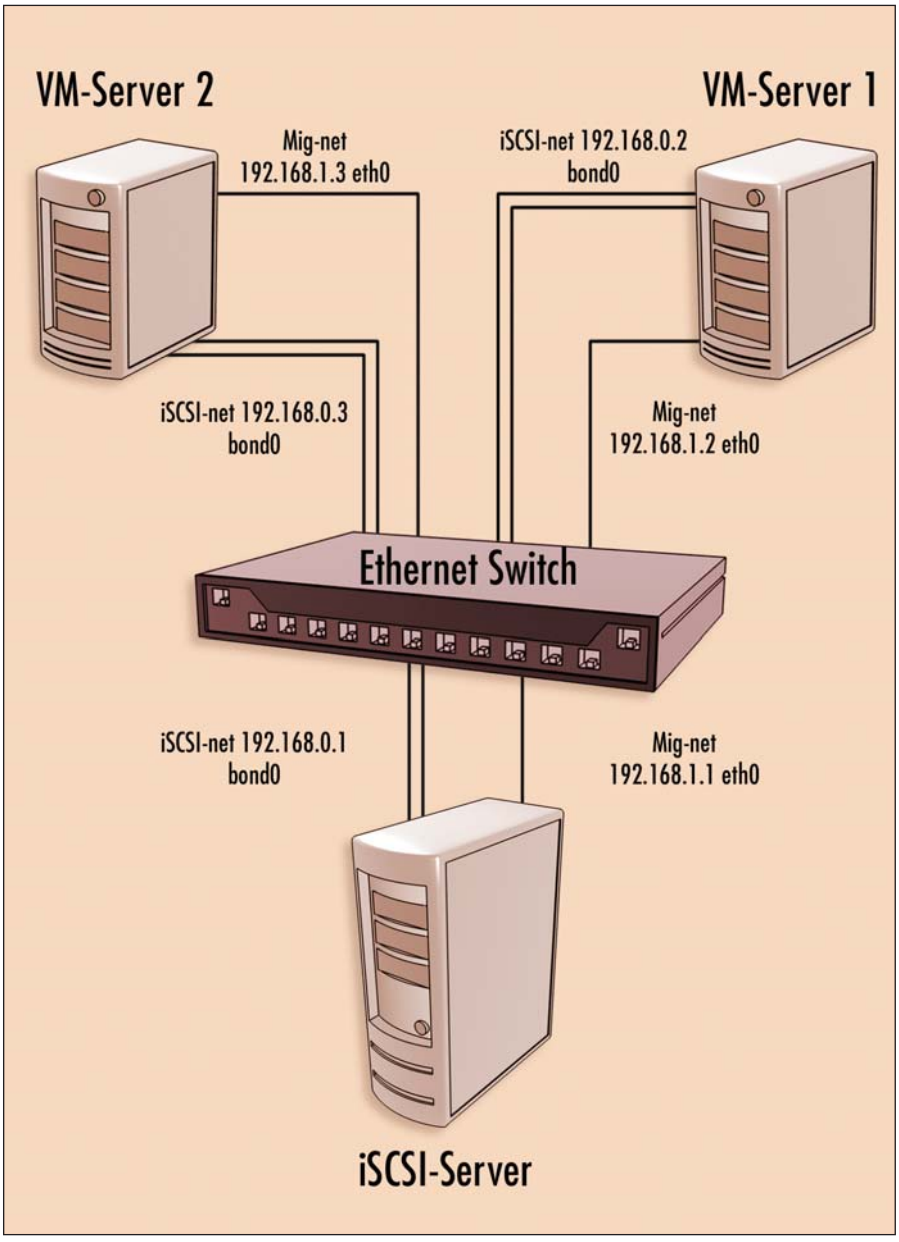


Bild 1: Im Beispielnetzwerk sind die Virtuellen Maschinen über einen Switch mit dem iSCSI-Server verbunden

Die Bedeutung der Bandbreite steigert sich vor allem dann, wenn VMs migriert werden. Bei der Migration fallen unter Umständen erhebliche Datenmengen an. Neben Verwaltungsdaten muss der komplette von der VM benutzte Hauptspeicher übertragen werden – Größenordnungen von mehreren GByte sind nicht unüblich. Es ist ein weitverbreiteter Irrtum, dass während dieses Hauptspeichertransfers die VM nicht weiterarbeiten kann – das wäre fatal, denn ein Transfer mehrerer GByte dauert etliche Dutzend Sekunden. Einem Anwender, der mit der VM arbeitet, würde dies sofort auffallen.

Migration des Arbeitsspeichers

Tatsächlich verwenden sowohl Xen als auch KVM ausgefeilte Mechanismen, um die Zeitspanne des eigentlichen Hauptspeichertransfers zu kaschieren. KVM geht dabei – grob vereinfacht – wie folgt vor: Zunächst startet die neue VM auf dem Zielserver und erhält die Anweisung, auf den Transfer zu warten. Die VM auf dem Quellserver loggt ab einem bestimmten Zeitpunkt alle Spei-

cherseiten (Pages), die nach diesem Zeitpunkt modifiziert wurden. Anschließend werden alle nicht modifizierten Pages übertragen. Die VM läuft dabei weiter. Ändert sich im Folgenden eine bereits übertragene Seite, loggt KVM diese ebenfalls. Nach dem Transfer erfolgt eine iterative Übertragung der Liste der modifizierten Pages. Dabei legt KVM erneut ein Zeitpunkt an, ab dem es weiter modifizierte Pages aufzeichnet. Sind alle Pages übertragen, wird die VM auf dem Quellserver gestoppt und deren Zustandsdaten auf den Zielserver übertragen. Anschließend startet die VM auf dem Zielserver und arbeitet an der Stelle weiter, wo sie auf dem Quellserver unterbrochen wurde.

Obwohl das genaue Migrationsverfahren sowohl bei KVM als auch bei Xen um einiges komplexer ist, als diese vereinfachte Darstellung suggerieren mag, wird jedoch eins klar: Der eigentliche Transfer des Hauptspeichers stellt kein allzu großes Problem dar. Trotzdem sollten Sie eine schnelle Netzwerkverbindung sicherstellen. Da insbesondere bei sehr aktiven VMs die iterativ abzuarbeitenden Listen modifizierter Pages von Durchlauf zu Durchlauf sehr groß werden können, während die Transfers laufen, kann der eigentliche Migrationsprozess recht lange dauern – auch wenn der Anwender davon nichts mitbekommt. Ist der Migrationsgrund beispielsweise ein drohender Hardware-Ausfall des Quellservers, will der Administrator schnell die VMs von der Maschine abziehen. In jedem Fall sorgt eine VM-Migration für eine Lastspitze auf dem Transfer-Netzwerk. Läuft iSCSI über das gleiche Netz, kann es zu Performance-Engpässen für den iSCSI-Betrieb kommen. Der Einsatz von getrennten Migrations- und Storagenetzwerken ist eine sinnvolle Konfiguration, mit der Sie das Problem umgehen.

1. Das Bonding-Modul beim Systemstart mit den richtigen Parametern laden
In */etc/modprobe.conf* hängen Sie folgende Zeile an:

```
alias bond0 bonding
```

2. Das Bonding-Device konfigurieren
Legen Sie die Datei */etc/sysconfig/network-scripts/ifcfg-bond0* an:

```
DEVICE=bond0
BONDING_OPTS="miimon=100 mode=0"
BOOTPROTO=none
NETWORK=192.168.0.0
IPADDR=192.168.0.1
NETMASK=255.255.255.0
BROADCAST=192.168.0.255
MTU=9000
ONBOOT=yes
```

3. Ethernet-Interfaces als Slave-Devices konfigurieren
Beispielsweise eth2 in */etc/sysconfig/network-scripts/ifcfg-eth2* dem Bond hinzufügen.

```
DEVICE=eth2
ONBOOT=yes
BOOTPROTO=none
HWADDR=DE:AD:BE:EF:AF:FE
MASTER=bond0
SLAVE=yes
```

Einrichten des Bonding

Link-Aggregation mittels Linux Bonding konfigurieren

Obwohl nicht notwendig, bietet Link-Aggregation eine kostengünstige Möglichkeit zur Leistungssteigerung, und wir richten es für unser Beispiel-Setup ein. Bild 1 zeigt unser Beispielnetzwerk: Zwei Server für virtuelle Maschinen, VM-Server1 und VM-Server2, hängen über einen Switch an einem iSCSI-Server. Zwischen den drei Systemen legen wir zwei Netzwerke an: eins für die Migration ("Mig-net") und eins für dem iSCSI-Transport ("iSCSI-net"). Das iSCSI-net besteht aus zwei Ethernet-Links, die mittels Bonding zu einer logischen Verbindung zusammengefasst sind (daher der Device-Name "bond0").

Das Migrationsnetzwerk besteht aus normalen Ethernet-Verbindungen, deren Konfiguration sich nicht von normalen Netzwerken unterscheidet. Im Kasten "Einrichten des Bonding" sind drei Schritte gezeigt, mit denen Sie unter Red Hat Enterprise Linux 5.2 (RHEL) oder Centos 5.2 Bonding einrichten. Zunächst wird das Bonding-Modul in der *modprobe.conf* geladen. Für jedes Bonding-Device müssen Sie eine entsprechende alias-Zeile eintragen, da für jedes Device ein Bonding-Modul geladen wird. Das Bonding-Device selbst konfigurieren Sie mit der Datei *ifcfg-bond0*. Bis auf die Zeile "BONDING_OPTS" entspricht die Konfiguration der einer normalen, statischen Ethernet-Karte. In der Zeile "BONDING_OPTS" stellen Sie mit "miimon=100" ein, dass die Ethernet-Interfaces alle 100 Millisekunden überprüfen sollen, ob der jeweilige Link noch aktiv ist. Damit lassen sich Unterbrechungen feststellen.

Mit der Option "mode=0" konfigurieren Sie das Bonding-Device in den "Balanced round-robin"-Modus. Die Datenübertragung wird dabei auf alle beteiligten Devices gleichmäßig verteilt und bei Ausfall eines Links wird mit den verbleibenden Devices weitergearbeitet. Der Linux Bonding-Treiber kennt insgesamt sechs verschiedene Modi. Allerdings bietet der Mode 0 eine Reihe von Vorteilen: Er ist der einzige Modus, bei dem schon eine einzige TCP- oder UDP-Verbindung von der aggregierten Bandbreite aller Interfaces profitieren kann. Bei anderen Modi steht zwar auch die Gesamtbandbreite zur Verfügung, allerdings kann eine Verbindung lediglich die Bandbreite eines Links verwenden. Darüber hinaus erfordert der Mode 0 keine besondere Unterstützung durch den Switch, wie etwa bei 802.3ad (Dynamic Link Aggregation, oft verwirrend als Port-Trunking bezeichnet).

Schließlich setzen Sie die MTU auf 9.000 hoch, um größere, unfragmentierte Ethernet-Frames übertragen zu können. Der Switch muss dies natürlich ebenso unterstützen wie die beteiligten Ethernet-Interfaces. Es reicht, die MTU für das Bonding-Device zu setzen, die beteiligten Interfaces werden automatisch mit eingestellt. Im dritten Schritt konfigurieren Sie die am bond0 beteiligten Interfaces. Im Beispiel fügen Sie eth2 mit der Zeile "Master=bond0" dem Bonding-Device hinzu. Analog lassen sich eth3 oder weitere Interfaces hinzufügen. Die Bonding-Kon-

figuration nehmen Sie auf allen beteiligten Systemen vor – dem iSCSI-Server sowie den beiden VM-Servern.

iSCSI-Devices anlegen und die Server anbinden

Die iSCSI-Konfiguration ist in der eingangs erwähnten Artikelserie ausführlich beschrieben, daher geben wir im Kasten "Konfiguration des Target" lediglich eine verkürzte Version der Target-Konfiguration ohne Authentifizierung wieder (auf eine entsprechende Konfiguration des OpenISCSI-Initiators verzichten wir aus Platzgründen).

Bei der Target-Konfiguration gibt es einen Unterschied zu den Beispielen in der iSCSI-Workshopreihe: Das exportierte Logical Volume "/dev/hydra/testlinux" stellen wir anstelle von "Type=fileio" als "Type=blockio" bereit. Damit wird der Buffercache auf dem iSCSI-Server umgangen und alle Operationen direkt auf dem exportieren Block-Device ausgeführt. Da die VMs eigene Betriebssysteme fahren, sorgen diese bereits für effektives Caching, um die Performance zu steigern. Abschließend verbinden Sie mit den in Schritt 2 gezeigten "iscsiadm"-Kommandos beide VM-Server mit dem iSCSI-Server.

1. iSCSI-Target in */etc/ietd.conf* anlegen

```
Target iqn.2007-01.de.it-administrator:
      storage:disk1
   Lun 0 Path=/dev/hydra/testlinux,
      Type=blockio
   #MaxConnections                    1
   InitialR2T                        No
   ImmediateData                    Yes
   #MaxRecvDataSegmentLength       8192
   #MaxXmitDataSegmentLength       8192
   MaxBurstLength                262144
   FirstBurstLength               65536
   #DefaultTime2Wait                  2
   #DefaultTime2Retain               20
   #MaxOutstandingR2T                 8
   #DataPDUInOrder                  Yes
   #DataSequenceInOrder             Yes
   #ErrorRecoveryLevel                0
   #HeaderDigest              CRC32C,None
   #DataDigest                CRC32C,None
   # various target parameters
   Wthreads                           8
```

2. Anbindung der beiden VM-Server an das iSCSI-Target (hier für einen Server wiedergegeben):

```
# iscsiadm -m discovery -t sendtargets  -p
   192.168.0.1:3260
# iscsiadm -m node -T iqn.2007-01.de.it-
   administrator:storage:disk1 -p
   192.168.0.1:3260 -l
```

3. Beispiel eines erzeugten iSCSI-Devicenodes in */dev/disk/by-path*:

```
 ip-192.168.0.1:3260-iscsi-iqn.2007-
   01.de.it-administrator:storage:disk1 ->
   ../../sdc
```

Konfiguration des Target

Die eingangs erwähnte "einheitliche Sicht" stellt der Device-Mapper von Linux her: Im Verzeichnis */dev/disk/by-path* befindet sich ein Link, der die IQN-basierte iSCSI-Adresse auf das lokale Device zeigen lässt. Im Beispiel hat das System die iSCSI-Platte lokal als "sdc" angebunden – das mag auf dem zweiten Server davon abweichen, wenn er eine andere Anzahl oder Konfiguration lokaler Platten hat. Wichtig ist lediglich, dass der auf der iSCSI-IQN basierende Link auf beiden Servern gleich und damit migrationstauglich ist.

VM-Migration mit KVM und Xen

Die Migration der VMs ist in den beiden Virtualisierungslösungen KVM und Xen unterschiedlich. Im Folgenden beschreiben wir ausführlich die Migration mittels KVM, da die vorliegende Dokumentation zu KVM derzeit ausgesprochen spärlich und teilweise inkorrekt ist. KVM basiert auf dem Open Source-Systememulator "Qemu". Dieser wird durch das KVM-Projekt um die benötigte Funktionalität erweitert, die es ihm ermöglicht, VMs mit minimalem Overhead zu betreiben. Aus Sicht des Administrators bleibt die Benutzerschnittstelle von Qemu weitgehend erhalten.

Qemu bietet bei einer laufenden VM die Möglichkeit, in einen sogenannten "Monitor" zu wechseln, über den unter anderem auch die Migration durchgeführt wird. Üblicherweise startet Qemu ein grafisches Frontend, das als Display für die VM fungiert und sich entweder VNC oder der SDL-Grafikbibliothek bedient. In diesem Fenster lässt sich mittels "Alt-2" auf die Monitorkonsole und mit "Alt-1" zurück zur grafischen Ausgabe der VM schalten. Auf Desktopsystemen bietet das hinreichenden Komfort, für den Serverbetrieb ist der interaktive Umgang mit der grafischen Konsole zu umständlich. KVM erlaubt, den Monitor auf einen per telnet erreichbaren Port umzubiegen, was die Bedienung hinsichtlich Migration vereinfacht. In Kasten "Live-Migration mit KVM und iSCSI" sind die drei Schritte zur Migration einer KVM-VM aufgezeigt.

KVM-Kommandozeilen können mitunter verwirrend lang werden, da eine Vielzahl von Konfigurationsoptionen zur Verfügung steht. Die Kommandozeilen im Kasten entstammen bis auf einige kosmetischen Änderungen einer realen Produktionsumgebung.

Schritt 1: Starten der VM auf VM-Server1

```
# kvm -smp 2 -m 4096 -monitor
  tcp:127.0.0.1:3333,server,nowait
-net nic,macaddr=DE:AD:BE:EF:01:04,
  model=e1000
-net tap,script=/etc/qemu-ifup
-drive index=0,media=disk,if=ide,cache=off,
  file=/dev/disk/by-path/
  ip-192.168.0.1:3260-iscsi-iqn.2007-
  01.de.it-administrator:storage:disk1
-vnc :1 -daemonize
```

Schritt 2: Starten der Empfangs-VM auf VM-Server2

```
# kvm -smp 2 -m 4096 -net
  nic,macaddr=DE:AD:BE:EF:01:04,model=e1000
-net tap,script=/etc/qemu-ifup
-drive index=0,media=disk,if=ide,cache=off,
  file=/dev/disk/by-path/
  ip-192.168.0.1:3260-iscsi-iqn.2007-
  01.de.it-administrator:storage:disk1
-vnc :1 -daemonize
-incoming tcp:192.168.0.3:4444
```

Schritt 3: Starten der Migration

```
# telnet localhost 3333
Trying 127.0.0.1...
Connected to localhost.localdomain
  (127.0.0.1).
Escape character is '^]'.
QEMU 0.9.1 monitor - type 'help' for more
  information
(qemu) migrate tcp:192.168.0.3:4444
(qemu) quit
```

Live-Migration mit KVM und iSCSI

Zunächst startet das Kommando in Schritt 1 eine VM mit zwei Prozessoren und 4 GByte Speicher. Mit der Option "-monitor[...]" wird der eingebaute Qemu-Monitor in unserem Beispiel auf Port 3333 des Hostsystems (127.0.0.1) umgeleitet. Die beiden Zeilen "-net[...]" konfigurieren den Netzwerkzugang der VM. In der Zeile, die mit "-drive[...]" beginnt, erfolgt die Festplattenkonfiguration via iSCSI. Beachten Sie bitte, dass hier die netzweit gültige IQN-basierende Adresse des iSCSI-Speichers angegeben wird. Mittels "-vnc :1" aktivieren Sie den in Qemu eingebauten VNC-Server, sodass sich netzweit mittels VNC-Client direkt auf die grafische Konsole der VM zugreifen lässt. Schließlich sorgt "-daemonize" dafür, dass die VM als Hintergrundprozess startet.

Um die VM erfolgreich zu migrieren, starten Sie auf dem VM-Server2 zunächst die "Empfangs-VM" und weisen sie an, auf die Migration zu warten. Die Kommandozeile entspricht der auf VM-Server1, auch hier wird über die gleiche netzweite IQN-basierende Adresse auf den iSCSI-Storage zugegriffen. Lediglich eine neue Option ist hinzugekommen: Mit "-incoming" weisen Sie die VM an, auf der Adresse 192.168.0.3 an Port 4444 auf Migrationsdaten via TCP zu warten. Derart gestartet, macht diese VM erst mal nichts außer warten.

Im letzten Schritt wird auf VM-Server1 mit dem Kommando "telnet localhost 3333" in den Monitor der VM gesprungen, entsprechend der "-monitor"-Option im ersten Schritt. Der Monitor selbst meldet sich mit dem "(qemu)"-Prompt. Das Kommando "migrate tcp:192.68.0.3:4444" weist die VM an, mit der Migration zu beginnen. IP-Adresse und Port müssen mit den im zweiten Schritt angegebenen Parametern für "-incoming" übereinstimmen.

Die Migration dauert eine Weile, nach Abschluss meldet sich der Monitor erneut mit dem "(qemu)"-Prompt und Sie können ihn mit "quit" beenden. Danach ist der KVM-Prozess auf VM-Server1 beendet und die VM erfolgreich auf VM-Server2 migriert.

Aus Platzgründen verzichten wir auf eine ausführliche Darstellung der Migration unter Xen. Im Prinzip läuft diese wie folgt ab: Zunächst ist der Xen-Daemon zu aktivieren und auf Netzbetrieb zu konfigurieren. Die Optionen sind in der Manpage "xend-config.sxp(5)" beschrieben – im Wesentlichen muss "xend-relocation-server" enabled werden sowie ein "xend-relocation-port" und die "xend-relocation-address". Natürlich muss xend auf beiden VM-Servern aktiviert und vor allem der xend-relocation-port gleich sein. Die zu migrierende Xen-VM muss sich des iSCSI-Storages in gleicher Weise bedienen wie im KVM-Beispiel, also als Block-Device mit der "by-path" IQN-Adresse angesprochen werden. Der "disk"-Eintrag in der Konfiguration der VM sieht dann etwa wie folgt aus:

```
disk = ['phy:/dev/disk/by-path/
  by-path/ip-192.168.0.1:3260-iscsi-
  iqn.2007-01.de.it-administrator:
  storage:disk1,xvda,w' ]
```

Laufen auf beiden VM-Servern die xend-Instanzen, startet der Administrator auf VM-Server1 mit 'xm create..." die VM. Die eigentliche Migration führen Sie unter Xen mit dem folgenden Kommando durch:

```
xm migrate –live VM-{Zielserver-
  Hostname}
```

Fazit

Mit Linux-Bordmitteln ist es durchaus möglich, eine komplette Virtualisierungs-Infrastruktur aufzusetzen, die bei entsprechender Auslegung der zugrunde liegenden Hardware auch hohen Anforderungen gerecht werden kann. Der Einsatz von iSCSI empfiehlt sich, da es sich um einen offenen Standard handelt, der zudem auf vorhandener Netzwerkinfrastruktur aufsetzt. Auf solche Grundlagen gestellt, funktioniert Live-Migration von VMs in den beiden Virtualisierungsansätzen Xen und KVM problemlos.

Im Betrieb zeigte KVM jedoch einige Instabilitäten bei der Live-Migration mit neueren KVM-Versionen, die dem gegenwärtigen Entwicklungsstand geschuldet sind – die KVM-Entwickler bauten zum Entstehungszeitpunkt des Artikels die KVM-Infratruktur massiv um. Wenn Sie diese Zeilen lesen, sollte sich die Lage allerdings wieder beruhigt haben – auf umfangreiche Tests sollten Sie dennoch nicht verzichten.

Ein Wort zur Sicherheit ist in diesem Zusammenhang geboten: Während KVM prinzipiell die Möglichkeit bietet, die Migration durch einen SSH-Tunnel zu verschlüsseln, überträgt Xen die VM unverschlüsselt. Das Migrationsnetz sollte daher ein von der Außenwelt isoliertes Netz sein. Das Gleiche gilt für iSCSI – auch hier werden die Daten unverschlüsselt übertragen, sodass das iSCSI-Netz ebenfalls sorgfältig abgeschottet werden muss, um Datenklau zu verhindern. *(jp)*

Ressourcen

[1] **"Arbeitsweise und Konfiguration von Xen (1)"** in IT-Administrator 2/2007

[2] **"Arbeitsweise und Konfiguration von Xen (2)"** in IT-Administrator 3/2007

[3] **"Kernel-based Virtual Machine for Linux einrichten"** in IT-Administrator 09/2007

[4] **"Xen-Infrastrukturen effektiv verwalten"** in IT-Administrator 01/2008

[5] **"Virtualisierungstechnologien im Vergleich"** in IT-Administrator 01/2008

[6] **"iSCSI unter Linux einrichten (1)"** in IT-Administrator 06/2008

[7] **"iSCSI unter Linux einrichten (2)"** in IT-Administrator 07/2008

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

Citrix Workflow Studio

Manuell war gestern

von Nico Lüdemann

Das Workflow Studio von Citrix ist eine Automatisierungslösung für IT-Prozesse. Es ermöglicht die Zusammenstellung, Integration und Abstimmung von regelbasierten Workflows in einer Citrix-Infrastruktur und auch von Drittanbietern. Mit diesem grafischen Konfigurations- und Verwaltungswerkzeug können Administratoren Technologiekomponenten einfach über Workflows miteinander verknüpfen und eine dynamische Bereitstellungsplattform realisieren. IT-Administrator zeigt, wie Sie IT-Infrastrukturen mit dem neuen Werkzeug gestalten.

Nach der ursprünglichen Ankündigung des Workflow Studio (WFS) im Frühjahr 2008 hat es nach vielen Monaten unterschiedlicher Tech-Preview- und Betaphasen nun einen stabilen Zustand erreicht, der die wahren Möglichkeiten dieses Produkts erkennen lässt. Es steht Ihnen nunmehr eine einheitliche Orchestrationsoberfläche zur Verfügung, die eine effiziente Verwaltung einer dynamischen Rechenzentrumsumgebung ermöglicht.

Alles basiert auf der PowerShell

Im Kern besteht das WFS aus zwei Komponenten – der WFS "Console" und der WFS "Runtime". Bei der Console handelt es sich um eine grafische Oberfläche, mit der Sie neue Workflows erstellen sowie vorhandene Workflows bearbeiten oder ausführen können. Die zweite Komponente Runtime erlaubt, Ihre erstellten Workflows später auf dem gewünschten System ausführen zu können.

Beide Komponenten setzen hierbei als Basis das .NET Framework 2.0 und die Microsoft PowerShell 1.0 voraus, wodurch schnell ersichtlich wird, auf welcher Plattform die erstellten Workflows abgearbeitet werden – das WFS ist eine grafische Oberfläche für PowerShell-Skripte, die Sie in der Console komfortabel erstellen, bearbeiten und debuggen können.

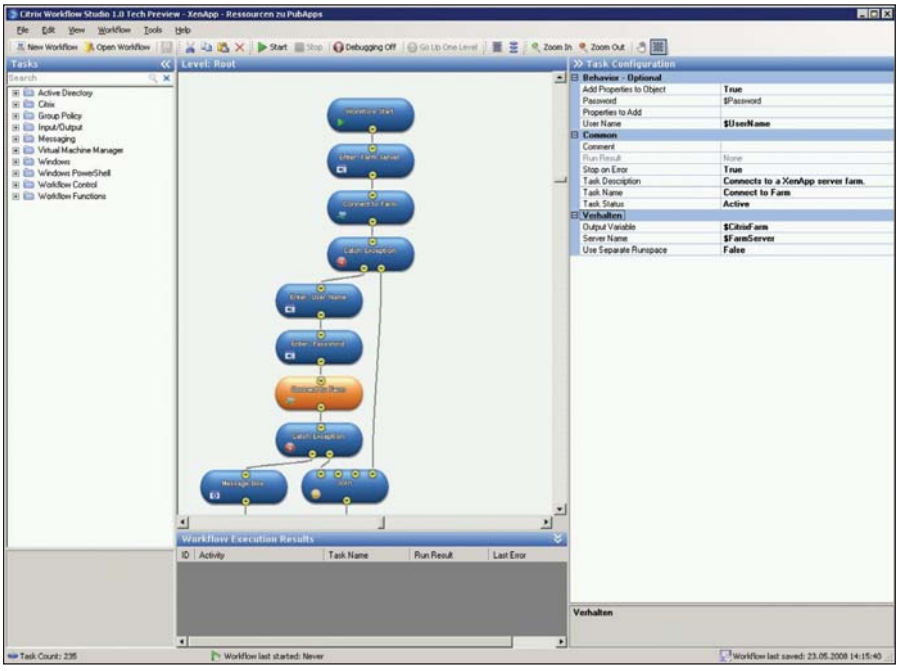


Bild 1: Das Workflow Studio ermöglicht die Verwaltung von RZ-Abläufen in einer grafischen Oberfläche

Automatisierung per Mausklick

Die Optik der Konsole ist grob mit Microsoft Visio zu vergleichen, da Sie auch hier die gewünschten Aktionsobjekte ("Tasks") aus einer Liste von zur Verfügung stehenden Objekten auf der linken Fensterseite auswählen und auf die Arbeitsfläche ("Design Surface") ziehen können. Anschließend können Sie die so hinzugefügten Tasks markieren und ihre Eigenschaften in der entsprechenden Konfigurationsbox ("Configuration Pane") auf der rechten Seite des WFS-Fensters bearbeiten.

Durch einfache Verknüpfungen zwischen Tasks steuern Sie den zeitlichen Ablauf Ihres Workflows. Natürlich können Sie an dieser Stelle auch Abfragen, Ausgaben oder Fallunterscheidungen einsetzen, um geplante Workflows in der notwendigen Komplexität abbilden zu können. Auch die Nutzung von Variablen ist selbstverständlich möglich, was

Bild 2: Mit wenigen Eingaben ist ein neuer Task erstellt, der die Grundlage der Automatisierung bildet

Ihnen eine "harte Codierung" etwa von Serveradressen oder Kennwörtern erspart. Sie können beispielsweise alle notwendigen Werte über Eingabeboxen zum Start eines Workflows abfragen, um ihn beliebig häufig für alle benötigten Varianten einsetzen zu können. Auch das Auslesen von Systeminformationen und das automatische Befüllen von Variablen mit den so gewonnenen Informationen ist möglich.

Sobald Ihr Workflow erstellt ist, können Sie ihn über den Start-Button in der Symbolleiste der Konsole starten. Am unteren Fensterrand der WFS Console finden Sie ein Dialogfeld, in dem Sie die Ergebnisse ("Execution Results") eines laufenden Workflows nachvollziehen können, was Ihnen insbesondere im Fall von Debugging-Aktionen als sehr hilfreich auffallen wird. Hier finden Sie Informationen über jeden Workflow-Schritt, wobei jeweils die aktive Task auch optisch durch ein Blinken hervorgehoben wird. Haben Sie diese Arbeitsumgebung erst einmal verinnerlicht, werden Sie sich schnell darin zurechtfinden und zeitnah Ergebnisse herbeiführen können.

Die Produktfamilie des Citrix Delivery Center enthält:

- Citrix XenServer: Plattform zum Management von Servervirtualisierung im Rechenzentrum
- Citrix NetScaler: Lösung zur Bereitstellung von browserbasierten Unternehmensanwendungen und Websites
- Citrix XenApp: Citrix' Presentation Server-Produktlinie unter neuem Namen
- Citrix XenDesktop: Das Virtual Desktop Infrastructure (VDI)-System stellt individuelle virtuelle Windows-Desktops bereit

Citrix Delivery Center-Strategie

Integration auch mit anderen Produkten

Im Bezug auf den gesamten Funktionsumfang des WFS wird Ihnen hierbei positiv auffallen, dass die Elemente der Aktionsobjekte erweitert werden können. So lassen sich beispielsweise Aktionsbibliotheken ("Task Library") für weitere Citrix-Produkte oder auch Produkte von Drittanbietern in das WFS integrieren und anschließend mitnutzen. Für einige Microsoft-Produkte sind die Task Libraries sogar direkt mit enthalten – etwa für das Windows-Management, das Active Directory oder den VirtualMachine Manager.

An dieser Stelle zeigt sich somit nun der große Vorteil der PowerShell-Technologie unter dem WFS: Sofern Sie ein gewünschtes Produkt über die PowerShell ansteuern und konfigurieren können, geht dies prinzipiell auch über das WFS. Es gibt somit keine Gründe mehr, warum ein aktuelles Produkt nicht integrierbar sein sollte. Aber selbst in dem Fall, dass etwa für ein älteres Produkt keine PowerShell-Unterstützung gegeben sein sollte, können Sie es im WFS greifen – so lassen sich etwa auch "normale" PowerShell- oder Command-Skripte aus einem Workflow heraus aufrufen. Spätestens auf diesem Weg sollten Sie jedes Produkt "automatisierbar" machen können – nur vielleicht nicht ganz so schön und übersichtlich, wie es bei den Produkten mit fertigen Task Libraries der Fall ist.

Anwendungsfälle im Überblick

Besonders interessant wird das WFS in dem Moment, in dem Sie ein wenig über den Tellerrand blicken und sich die möglichen Anwendungsfälle verdeutlichen. Der erste und einleuchtendste Anwendungsfall ist hierbei natürlich die Automatisierung von regelmäßigen Standardtätigkeiten wie die Erstellung eines neuen Benutzers oder einer virtuellen Maschine,

Bild 3: Eine große Auswahl an vorbereiteten Aufgaben beschleunigt die Erstellung eines Workflows

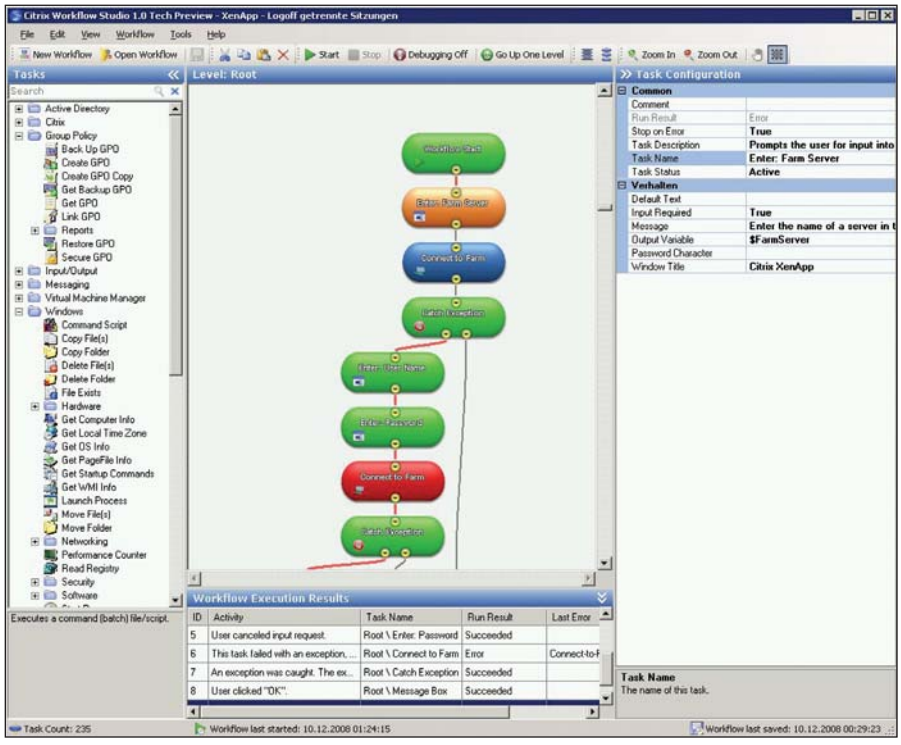


Bild 4: Die Resultate eines ausgelösten Workflows zeigen deutlich aufgetretene Fehler an

die automatisierte Anpassung der Einstellungen einer veröffentlichten Anwendung oder das Beenden von getrennten Sitzungen. Zu diesem Punkten muss nicht viel gesagt werden, und der Nutzen eines Werkzeuges wie dem WFS wird Ihnen hierbei schnell deutlich werden.

Aber es gibt noch mehr: Ein zweites Einsatzgebiet in Ihrem Unternehmen könnte die Standardisierung von Konfigurationsaufgaben sein – nicht primär zum Zweck der Automatisierung, sondern zum Zweck der Standardisierung. Stellen Sie sich einmal vor, dass Sie einen Workflow entworfen haben, der etwa die Installation eines Servers in Ihrem Netzwerk beschreibt und durchführt. Sofern Sie diesen umfassend und ausreichend genug entwerfen – also beispielsweise inklusive der Installation aller notwendigen Updates und Tools auf den Systemen (Stichworte: bginfo, Virenscanner) – könnten Sie ab diesem Zeitpunkt sicher sein, dass alle neu installierten Server in Ihrem Unternehmen Ihrem einheitlichen Standard entsprechen. Unterschiedlich große C-Partitionen oder individuelle Namensgebungen gehören damit der Vergangenheit an. Alle Systemeinstellungen wären standardisiert. Gleiches könnte natürlich auch für den Aufbau von Datenbanksystemen, Mailservern oder des kompletten Active Directory gelten. Die Möglichkeiten sind durch die erweiterbaren Tasks nahezu unbegrenzt und die Vorteile im Hinblick auf Konzepttreue und Dokumentation sind ebenfalls schnell erkennbar.

Ein dritter – womöglich noch weniger offensichtlicher – Anwendungsfall ist die Energieoptimierung in Ihrem Rechenzentrum. Stellen Sie sich auch hier einmal vor, dass Sie in der Lage wären, komplexe Abläufe entwerfen und ausführen zu können, die etwa im Rahmen einer umfassenden Virtualisierungsstrategie über alle Virtualisierungsebenen hinweg prüfen, welche Ihrer Serverressourcen zu einem bestimmten Zeitpunkt tatsächlich benötigt werden. Alle überschüssigen Ressourcen würden einfach bei Bedarf ab- oder wieder angeschaltet. So könnten beispielsweise in der Nacht alle laufenden virtuellen Systeme per XenMotion- oder VMotion-Technologien auf wenige XenServer- oder ESX-Hosts konsolidiert werden. Die freien Hosts könnten zur Energieeinsparung abgeschaltet oder in den Ruhezustand versetzt werden. Sobald später eine entsprechenden Systemlast auf den laufenden Systemen erkannt würde, könnten abgeschaltete Hosts wieder hochgefahren und die laufenden virtuellen Maschinen wieder auf diese verteilt werden.

Wenn das für Sie nach Zukunftsmusik klingt, lassen Sie sich von den Möglichkeiten des WFS überraschen, denn eben genau Szenarien dieser Art sind denkbar und werden in einigen Umgebungen auch schon erfolgreich umgesetzt. Wie schon bei den anderen Anwendungsfällen gilt auch hier, dass der Phantasie (und einem Stück weit dem Spieltrieb) keine Grenzen gesetzt sind. So salopp dies jedoch auch jetzt für Sie klingen mag – die Ergebnisse einer solchen Lösung können Ihnen in Ihrem Rechenzentrumsbetrieb bares Geld sparen.

Vorlagen für viele Standard-Workflows

Äußerst erfreulich ist in diesem Zusammenhang, dass Sie bei der Erstellung von neuen Workflows oder dem Experimentieren mit neuen Ideen bereits auf eine breite Basis von vorhandenen Vorlagen zurückgreifen können, die Ihnen für viele der Standardanwendungen bereits eine Lösung bieten. So steht Ihnen beispielsweise eine Vorlage zur Verfügung, mit deren Hilfe Sie einen XenApp-Workflow erstellen können, über den Benutzer, Gruppen und Server zu einer veröffentlichten Anwendung hinzugefügt werden können. Zwei weitere sehr nützliche Vorlagen lassen Sie etwa in Ihrer XenApp-Farm getrennte Benutzersitzungen abmelden oder Anwendungen aktivieren beziehungsweise deaktivieren. Auch für weitere Citrix-Produkte wie den XenServer, den Provisioning Server oder den Netscaler existieren entsprechende Vorlagen, die Sie für die Weiterentwicklung oder einfach die Ideensammlung nutzen können.

Um ein Gefühl für die Integration von Drittanbieter-Produkten in das WFS zu

bekommen, sollten Sie auch einen Blick auf die Vorlagen aus dem Bereich Active Directory oder Windows-Management werfen – hier finden Sie etwa sehr anschauliche Beispiele für das Zurücksetzen eines Benutzerkennworts oder den Neustart von beendeten Diensten. Auch diese Vorlagen können Sie natürlich nach Belieben mit eigenen Tasks oder Workflow-Schritten erweitern.

Die Community als Workflow-Lieferant

Doch was ist, wenn Sie Ihren gewünschten Workflow nicht erfolgreich zum Laufen bekommen oder die gesuchte Vorlage noch nicht existiert? Wie bei vielen anderen Produkten kann auch beim WFS eine Lösung die Suche im Internet sein. Bereits jetzt gibt es frei verfügbare oder kostenpflichtige Workflows im Internet, die den Funktionsumfang des Basispakets deutlich erweitern.

Im Bezug auf freie Workflows sei Ihnen hierbei insbesondere das "Citrix Developer Network" [1] ans Herz gelegt, in dem es einen eigenen Download-Bereich für das WFS gibt. Hier können Sie vorhandene Workflows frei herunterladen oder eigene Workflows der Community zur Verfügung stellen. Auf diese Weise werden Ihnen in naher Zukunft viele gute Workflows für den Einsatz zur Verfügung stehen.

Fazit

Das Citrix Workflow Studio stellt die Abrundung der Delivery Center-Strategie dar, da Sie hierdurch schlussendlich die Vielzahl der Lösungen und Produkte unter einer einheitlichen Oberfläche automatisieren können. Insbesondere die Möglichkeit, auch Standard-Windows- und Active-Directory-Einstellungen und -Komponenten verwalten zu können, bietet Ihnen ein hohes Maß an Integration und Leistungsumfang, das Sie im Rahmen einer ernsthaften Automatisierungsstrategie benötigen.

Durch die Integration mit weiteren Produkten und der schnell wachsenden Community wird sich das Produkt bald großer Unterstützung erfreuen. Nicht zuletzt aus diesen Gründen wird sich das Workflow Studio als nahezu unbegrenzt skalier- und einsetzbar erweisen. Da Sie es beliebig durch eigene PowerShell-Skripte oder sonstige externe Programmaufrufe erweitern können, liegen Ihren Ideen keine Steine mehr im Weg.

Selbst wenn Sie bereits andere Produkte für Prozess- oder Konfigurationsautomatisierungen einsetzen, sollten Sie also einen Blick auf das Workflow Studio wagen und es vielleicht einmal anhand einiger kleiner Workflows testen. *(jp)*

Links

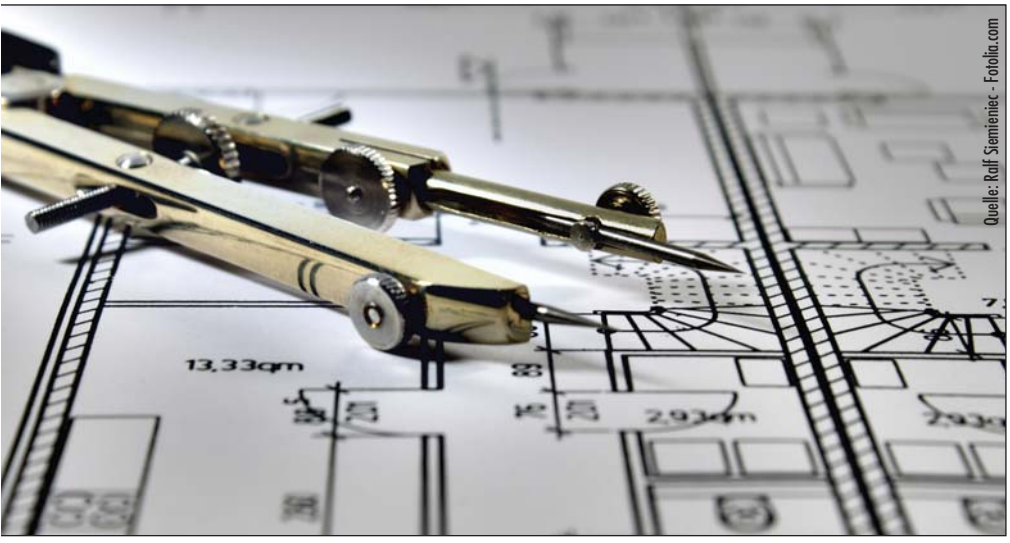
[1] Citrix Developer Network
http://community.citrix.com/cdn/

Migration auf den Small Business Server 2008

Sorgenfreier Umzug

von Thomas Joos

Mit Small Business Server 2008 steht die neue Version von Microsofts beliebter Software-Suite für kleine Unternehmen zur Verfügung. Doch da auf dem Server oft die wichtigsten Daten des Unternehmens liegen, will eine Migration auf die neue Version sorgfältig durchgeführt werden. Wie Sie erfolgreich Stolpersteine vermeiden, zeigen wir Ihnen in diesem Workshop.



Sorgfältig geplant passt sich der Small Business Server 2008 gut ins Netzwerk ein

Der erste Schritt bei der Migration auf den Small Business Server 2008 ist die Durchführung einer vollständigen Datensicherung des bestehenden Small Business Servers. Bevor Sie Ihre Daten sichern, sollten Sie zudem sicherstellen, dass sich auf dem Server keinerlei Viren befinden. Scannen Sie daher sicherheitshalber nochmals alle Verzeichnisse durch. Anschließend führen Sie mit Ihrer herkömmlichen Datensicherung ein vollständiges Backup des Servers durch. Haben Sie ein Image-Programm zur Hand und verfügen Sie über ausreichend Platz, ist es sicherlich auch sinnvoll, alle Partitionen des Servers zusätzlich zu spiegeln. In der Linksammlung zu diesem Artikel finden Sie ein Whitepaper [1], das Sie durch die Sicherung des Servers führt. Überprüfen Sie nach der Sicherung, ob diese fehlerfrei ist. Zusätzlich bietet es sich an, die wichtigsten Verzeichnisse – etwa die Dateiablagen der Benutzer und Abteilungen – auf eine externe Festplatte zu kopieren. Auch eine zusätzliche Sicherung der Exchange-Datenbanken sowie eventuell vorhandener SQL-Datenbanken ist sinnvoll.

Bestehende Systeme für die Migration aktualisieren

Nachdem Sie Ihren Server gesichert haben, müssen Sie sich an die notwendigen Vorbereitungen machen. Der erste Schritt besteht darin, alle benötigten und aktuellen Sicherheitspatches und Service Packs zu installieren. Viele Produkte, auch SBS 2008, gehen bei der Installation über eine Vorgängerversion davon aus, dass das Produkt aktuell ist. Außerdem bieten vor allem viele Service Packs Verbesserungen im Bereich der Migration. Wichtig ist zunächst die Installation des Service Pack 1 für Small Business Server 2003, sofern diese noch nicht erfolgt ist. Am schnellsten überprüfen Sie die Installation, indem Sie in der Registry zum Schlüssel "HKEY_LOCALMACHINE \ SOFTWARE \ Microsoft \ SmallBusinesServer \ ServicePackNumber" navigieren. Der Wert muss an dieser Stelle mit "0x00000001" hinterlegt sein. In diesem Fall ist das Service Pack ordnungsgemäß installiert.

Setzen Sie bereits die R2-Version des Small Business Server 2003 ein, entfällt dieser Test, da hier das Service Pack 1 schon installiert ist. Fehlt das Service Pack, sollten Sie es vor der Migration zunächst installieren. Sie finden den Link zum Download unter [2]. Der nächste Schritt gilt auch für die R2-Version des SBS 2003: Die Installation von Service Pack 2 für Windows Server 2003 [3]. Ob dieses bereits installiert ist, stellen Sie fest, indem Sie die Eigenschaften des Arbeitsplatzes auf dem Desktop aufrufen oder *winver* in das Feld "Ausführen" des Startmenüs eingeben. Fehlt das Service Pack 2 für Windows Server 2003, installieren Sie es bitte nach. Unter Umständen gibt es im Netzwerk Probleme nach der Installation des Service Packs. Die notwendigen Informationen dazu finden Sie im KB-Artikel 936594 der Microsoft-Knowledgebase unter [4].

Auch das Service Pack 2 für Exchange Server 2003 sollte auf dem Server installiert sein. Um das zu überprüfen, rufen Sie die Verwaltungsoberfläche von SBS 2003 auf und navigieren zu "Erweiterte Verwaltung / {Name der Exchange-Organisation} / Server. Auf der rechten Seite des Fensters finden Sie im Bereich "Serverversion" die Information, ob das Service Pack installiert ist. Wenn nicht, installieren Sie es nach. Zusätzlich müssen Sie sicherstellen, dass das SP1 für Microsoft Core XML Services (MSXML) 6.0 installiert ist. Rufen Sie dazu die Eigenschaften der Datei

MSXML6.dll im Verzeichnis "Windows \ System32" auf. Auf der Registerkarte "Version" muss die Dateiversion 6.10.1129.0 oder höher hinterlegt sein. Falls nicht, installieren Sie das Service Pack 1 [5] für diese Komponente.

Überprüfen Sie anschließend, ob das .NET-Framework 2.0 auf dem Server installiert ist. Dieses finden Sie wieder in der Systemsteuerung unter "Software". Hier muss das .NET-Framework 2.0 als installiertes Programm auftauchen. Wenn nicht, installieren Sie auch diese Software [6] nach. Stellen Sie außerdem sicher, dass das Service Pack 2 für Microsoft SQL Server Management Studio Express installiert ist. Dieses Programm finden Sie ebenfalls in den Links unter [7]. Wählen Sie die 32-Bit-Version, da SBS 2003 nicht als 64-Bit-Software verfügbar ist. Das Express-Studio lässt sich jedoch nicht installieren, wenn bereits die Vollversion für SQL Server 2005 vorhanden ist. In diesem Fall können Sie diesen Schritt überspringen.

SharePoint Services migrieren

Nutzen Sie auf Ihrem Server bereits die SharePoint Services 3.0, müssen Sie bei der Migration einiges beachten, da die direkte Migration nicht möglich ist. Die notwendigen Hinweise dazu finden Sie unter [8]. Standardmäßig sind auf einem Small Business Server 2003 die SharePoint Services 2.0 mitinstalliert. Diese lassen sich auf den SBS 2008 migrieren. Aber auch hier müssen Sie einige Punkte beachten: Zunächst sollten Sie sicherstellen, dass das Service Pack 3 für die SharePoint Services 2.0 auf dem Server installiert ist. Am schnellsten stellen Sie dies fest, indem Sie die Systemsteuerung starten und auf "Software" klicken. Wählen Sie anschließend "Microsoft SharePoint Services 2.0" aus und klicken Sie auf "Klicken Sie hier, um Supportinformationen zu erhalten". Überprüfen Sie, ob es sich um die Version 11.0.8173.0 handelt. Sollte das nicht der Fall sein, laden Sie das Service Pack [9] herunter und installieren es.

Nach erfolgter Installation testen Sie, ob die Intranetwebseite "CompanyWeb" ordnungsgemäß aktualisiert wurde. Rufen Sie dazu in der Programmgruppe "Verwaltung" den Link "Sharepoint-Zentraladministration" auf. Klicken Sie nach dem Start auf die Konfiguration für die virtuellen Server. Die CompanyWeb-Seite muss die Version 6.0.2.8165 haben, dann ist sie auf dem richtigen Stand. Sollte dies bei Ihnen nicht der Fall sein, können Sie die Seite manuell aktualisieren. Starten Sie dazu eine Befehlszeile und wechseln Sie mit dem Befehl

```
cd /d \Programme\Gemeinsame
  Dateien\Microsoft Shared\Web Server
  Extensions\60\Bin
```

in das Verzeichnis mit dem notwendigen Tool. Geben Sie dann den Befehl

```
stsadm -o upgrade -forceupgrade -url
  http://companyweb
```

ein. Nach der Aktualisierung müssen Sie den IIS neu starten. Geben Sie dazu den Befehl *iisreset* in der Befehlszeile ein oder starten Sie am besten den Server neu, damit alle Änderungen neu geladen werden.

Notwendige Netzwerkanpassungen

Damit Sie auf einem Server den SBS 2008 betreiben können, muss die Internetanbindung über eine Hardware-Firewall oder einen DSL-Router erfolgen. Der Router ist dann die Zwischenstelle zwischen Internet und internem Netzwerk. Diese Konfiguration ist ohnehin Standard für eine sichere Internetanbindung im Unternehmen. Setzen Sie die Premium Edition von Small Business Server 2003 ein, müssen Sie auch für die Aktualisierung des ISA Server 2004 noch einiges beachten, doch dazu später mehr.

Für die Durchführung der Migration empfiehlt Microsoft, dass nur ein Netzwerkadapter auf dem Server aktiv ist. Von diesem Adapter aus muss der Server den Router erreichen können. Verwenden Sie mehrere Netzwerkkarten im Server, deaktivieren Sie diese für die Durchführung der Migration. Nach Abschluss des Vorgangs lassen sich diese wieder in das System einbinden. Rufen Sie anschließend in der Programmgruppe "Verwaltung" die Serververwaltungskonsole auf. Klicken Sie auf "Internet und E-Mail" und dann auf "Verbindung mit dem Internet herstellen". Stellen Sie sicher, dass die Anbindung optimal funktioniert.

Bestehen Probleme, weisen Sie dem SBS-Server eine zusätzliche IP-Adresse im Bereich 192.168.x.1 zu und ändern Sie auch die IP-Adresse des Routers entsprechend im Laufe der Migration. Setzen Sie ein VPN auf dem SBS-Server ein, deaktivieren Sie diese Funktion während der Migration. Beim ISA-Server 2004 stellen Sie zudem sicher, dass das Service Pack 3 [10] installiert ist. Rufen Sie anschließend die ISA-Verwaltung auf. Diese befindet sich in einer eigenen Programmgruppe. Navigieren Sie zu den Firewall-Richtlinien und öffnen Sie die Eigenschaften der Regel "SBS Protected Networks Access Rule". Wechseln Sie nun auf die Registerkarte "Protokolle", klicken Sie auf die Schaltfläche "Filterung" und wählen Sie "RPC-Protokoll konfigurieren" aus. Entfernen Sie den Haken bei der Option "Strikte RPC-Einhaltung konfigurieren". Dieser Schritt ist notwendig, damit der Migrationsassistent später alle notwendigen Schritte durchführen kann, zum Beispiel den DCOM-Verkehr und Verbindungen per RPC.

Aktive Directory und Exchange vorbereiten

In der Domäne des SBS dürfen keine Domänencontroller auf einem Windows 2000-Server vorhanden sein. Ist das bei Ihnen der Fall, müssen Sie diese Domänencontroller vor der Migration aus dem Netzwerk entfernen. Standardmäßig befindet sich nach der Installation von SBS 2003 der Betriebsmodus der Domäne und der Gesamtstruktur im Windows 2000-Modus. Zwar sollte dieser ohnehin schnell umgestellt werden, da erst im Windows Server 2003-Modus alle Funktionen von Windows Server 2003 verfügbar sind, aber diesen Schritt übergehen viele Administratoren. Für die Migration auf den Small

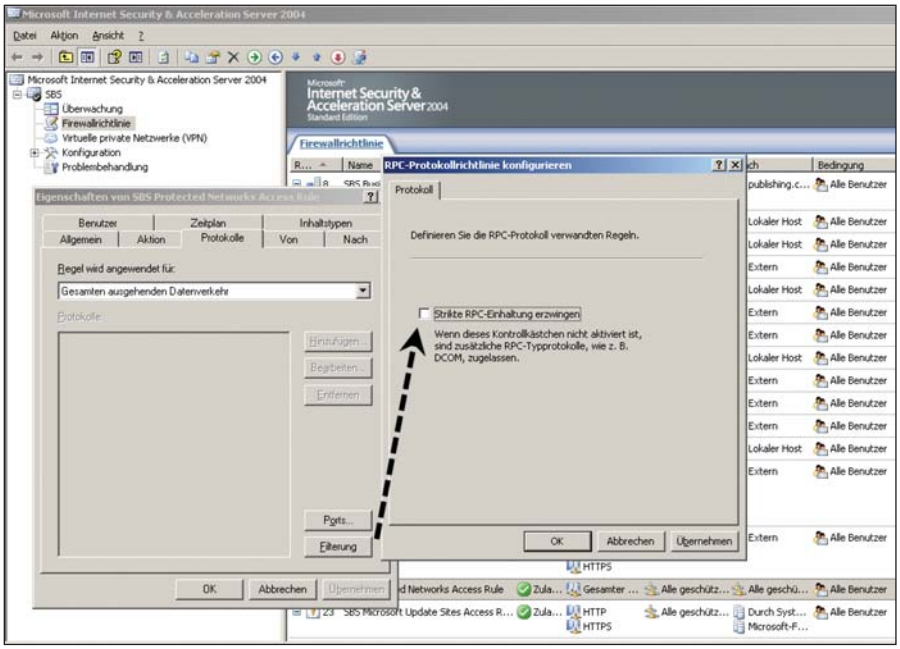


Bild 1: Die strikte RPC-Einhaltung muss auf dem ISA-Server deaktiviert sein, damit die Migration funktioniert

Business Server 2008 ist der Schritt jedoch notwendig.

Gemischtes Active Directory

Ein Active Directory lässt sich unter verschiedenen Betriebsmodi betreiben, standardmäßig befindet sich das Active Directory nach der Installation im gemischten Modus. In diesem Modus können neben den Windows Server 2003-Domänencontrollern parallel auch noch Windows NT 4.0-Domänencontroller betrieben werden. Um diese Funktionsebene zu ändern, klicken Sie in der Serververwaltungskonsole unter "Erweiterte Verwaltung" auf das Snap-in "Active Directory-Benutzer und -Computer" und dann mit der rechten Maustaste auf die Domäne und wählen die Option "Domänenfunktionsebene heraufstufen". Im anschließenden Fenster können Sie den Modus auswählen, den Sie aktivieren wollen. Sie erhalten dabei eine Warnung, dass die Umstellung des Modus nicht mehr rückgängig gemacht werden kann. Nach Bestätigen dieser Meldung wird die Funktionsebene heraufgestuft. Den Server müssen Sie danach nicht neu starten. Domänen mit dem Small Business Server 2003 ziehen daraus zwar keine besonderen Vorteile, da die neuen Funktionen hauptsächlich für die Zusammenarbeit von verschiedenen Domänen gedacht sind. Dennoch ist die Heraufstufung sauberer, da so das Small Business Server-Netzwerk eine einheitliche Struktur aufweist und später nicht irgendwelche Funktionen fehlen.

Die Funktionsebene der Gesamtstruktur können Sie mithilfe des Snap-ins "Active Directory-Domänen und -Vertrauensstellungen" heraufstufen. Sie finden dieses Verwaltungsprogramm über "Start / Programme / Verwaltung / Active Directory-Domänen und -Vertrauensstellungen". Klicken Sie mit der rechten Maustaste auf den Menüpunkt und wählen Sie die Option "Gesamtstrukturfunktionsebene heraufstufen". Dies funktioniert jedoch erst, wenn die Domänenfunktionsebene heraufgestuft ist. Wählen Sie auch hier den Modus "Windows Server 2003" aus und klicken Sie auf die Schaltfläche "Heraufstufen". Auch nach der erfolgreichen Heraufstufung der Gesamtstruktur ist es nicht notwendig, die Domänencontroller neu zu starten. Anschließend stehen die neuen Funktionen wie SID-History, universale Gruppen und gesamtstrukturübergreifende Vertrauensstellungen zur Verfügung.

Letzter Check vor der Migration

Nachdem Sie alle Vorbereitungen getroffen haben, können Sie mit dem Small Business Best Practices Analyzer (BPA) überprüfen, ob sich der Server in einem ordentlichen Zustand befindet, um auf SBS 2008 migriert zu werden. Entfernen Sie vor der Migration alle Fehler, die das Tool findet. Microsoft stellt den Analyzer kostenlos unter [11] zur Verfügung. Installieren Sie das Tool am besten direkt auf dem SBS-Server und starten Sie es nach der Installation. Stellen Sie sicher, dass der Server dabei eine Verbindung zum Internet hat und lassen Sie das Tool zunächst nach Aktualisierungen suchen. Microsoft stellt ständig neue Regeln zur Verfügung, die der BPA an dieser Stelle herunterladen und verwenden kann. Wählen Sie als Nächstes die Option "Start a scan" auf der linken Seite des Fensters. Der Vorgang dauert bis zu mehreren Minuten. Über den Link "View a report of this Best Practices scan" zeigt das Tool alle Probleme an und macht teils auch Lösungsvorschläge. Neben dem BPA sollten Sie natürlich auch die Standard-Diagnosetools "netdiag", "dcdiag" und "repadmin" durchführen, welche die Netzwerkkonfiguration und das Active Directory im Netzwerk auf Fehler untersuchen. Eine exakte Anleitung dazu finden Sie in den Ausgaben 07 bis 09/2007 des IT-Administrator.

Auch die Exchange-Komponente des SBS-Servers sollten Sie vor der Migration erst optimieren. Führen Sie am besten auch hier vorher eine Datensicherung sowie eine Offline-Defragmentierung der Exchange-Datenbanken durch. Etwa durch das Verschieben von Benutzern zwischen Postfachdatenbanken oder auch die normale Arbeit mit dem Exchange-Server wachsen Datenbankdateien ständig an. Auch nach einem Reparaturvorgang ist es unerlässlich für die Datenbankdateien, eine Offline-Defragmentierung durchzuführen. Diese dauert bei entsprechender Datenbankgröße oft stundenlang, aber nur dadurch ist sichergestellt, dass die Datenbankdateien nach einer Reparatur voll funktionsfähig sind. Während der Offline-Defragmentierung

löscht Exchange leere und, falls noch vorhanden, korrupte Seiten aus den Datenbanken. Für die Offline-Defragmentierung muss die Bereitstellung der Datenbanken aufgehoben oder der Informationsspeicherdienst beendet sein. Um die Defragmentierung durchzuführen, starten Sie das Werkzeug "Eseutil" mit der Option "/d" und dem Pfad zur Datenbank. Das Tool legt vor dem Defragmentierungsvorgang eine temporäre Kopie der Datenbankdatei an, die es defragmentiert und nach dem Vorgang wieder zurückkopiert. Die Temporärdateien werden auf dem Laufwerk angelegt, auf dem Sie Eseutil aufrufen. Aus diesem Grund sollte der Datenträger genug Platz bieten, also mindestens das Doppelte der Exchange-Datenbanken.

Steht nicht genug Platz zur Verfügung, kann Eseutil im Notfall keine Datenbank defragmentieren oder reparieren. Die einzige Alternative ist das langwierige Kopieren der Datenbank- und Eseutil-Dateien auf einen anderen Computer. Die Syntax in der Befehlszeile für eine Offline-Defragmentierung lautet zum Beispiel:

```
eseutil /d C:\Programme\Microsoft\
  Exchange-Server\Mailbox\First Stora-
  ge Group\Mailbox Database.edb
```

Hat Eseutil mit der Defragmentierung begonnen, öffnet es die Datenbank und legt eine Kopie an. Dabei werden auch automatisch defekte Bereiche der Datenbank gelöscht. Durch diese Option können Sie also korrupte Datenbanken wieder reparieren oder nach einer Reparatur überprüfen. Wird die Defragmentierung durch Herunterfahren des Servers unterbrochen, kann es sein, dass die temporär angelegte Datenbankdatei noch nicht über die Originaldateien kopiert wurde. Lokalisieren Sie dann die Temporärdatenbank und kopieren Sie diese über die Originaldateien.

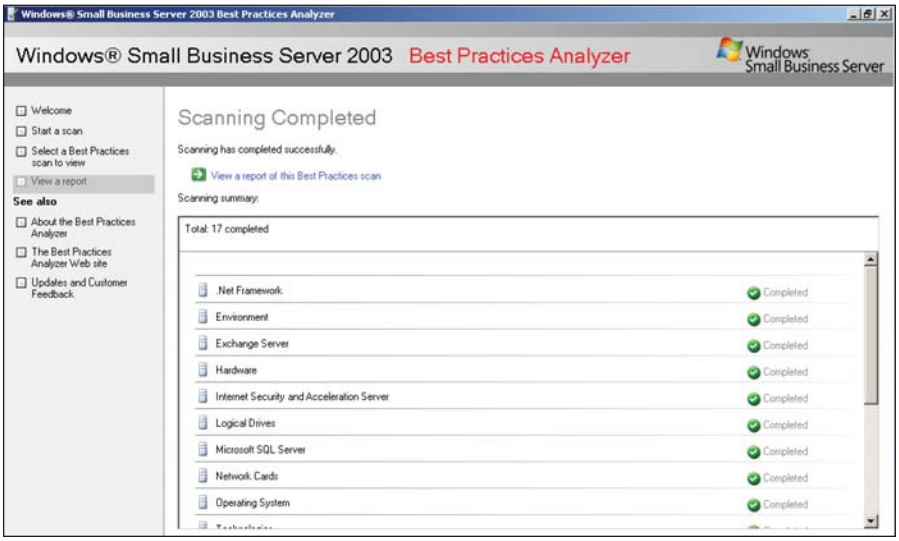


Bild 2: Gibt der Best Practices Analyzer grünes Licht, steht es gut um die Voraussetzungen zur Migration

Zeit für den Umzug

Nachdem Sie nun alle Migrationsvorbereitungen getroffen haben, legen Sie die SBS 2008-DVD in das Laufwerk des Servers. Anschließend startet der Assistent die Installationsoberfläche. Innerhalb der Tools stellt SBS 2008 ein spezielles Migrationswerkzeug zur Verfügung, das Sie nun starten. Unter Umständen erhalten Sie dabei eine Fehlermeldung. Die Lösung dieses Problems wird in einem speziellen KB-Artikel unter [12] beschrieben. Lassen Sie im Rahmen des Assistenten auch eine Antwortdatei erstellen, wie vom Tool vorgeschlagen. Eine Migration von SBS 2003 auf die Version 2008 benötigt in jedem Fall eine Antwortdatei – ohne diese bricht der Installationsassistent ab. Speichern Sie die Antwortdatei mit dem Namen *sbsanswerfile.xml* ab und starten Sie nach der Durchführung des Assistenten den Server neu.

Die Installation von SBS 2008 erfolgt im Migrationsmodus auf einer getrennten Maschine. Der gleiche Server lässt sich leider nicht verwenden, da SBS 2008 64-Bit-Hardware voraussetzt und SBS 2003 nur als 32-Bit-Software verfügbar ist. Aus technischen Gründen lässt sich eine 32-Bit-Version von Windows nicht direkt auf 64 Bit aktualisieren, das gilt auch für SBS 2003/2008. Installieren Sie also während der Migration SBS 2008 auf dem Zielserver. Der Quellserver ist der Server mit SBS 2003. Im Rahmen der Migration nimmt der Installationsassistent den neuen Server in die Domäne des SBS 2003-Servers mit auf. Achten Sie aber darauf, dass der Quellserver – also der Server unter Small Business Server 2003 – spätestens nach 21 Tagen aus dem Netzwerk entfernt werden muss. Nach 21 Tagen fährt der Quellserver ansonsten ständig automatisch herunter und trägt entsprechende Fehlermeldungen im Eventlog ein. Der Installationsassistent verschiebt außerdem alle Betriebsmasterrollen (FSMO) auf den neuen Server, der dabei auch zum globalen Katalog konfiguriert wird. Die DHCP-Funktion übernimmt der Assistent ebenfalls vom Quell- auf den Zielserver. Nachdem die Installation auf dem Zielserver gestartet ist, führt ein Assistent durch die einzelnen Schritte und weist auch auf eventuelle Probleme und Fragen hin.

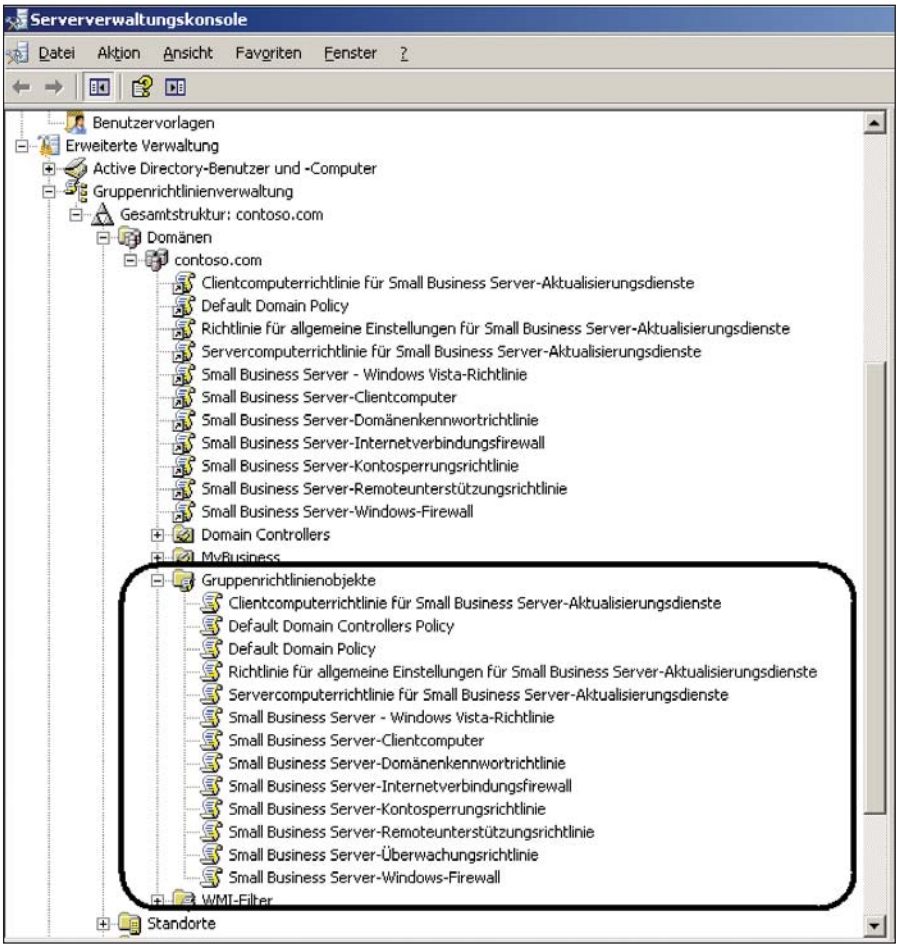


Bild 3: Über die Serververwaltungskonsole lassen sich GPOs exportieren und sichern

Gruppenrichtlinien und Exchange-Daten übernehmen

Zwar überträgt der Installationsassistent so gut wie alle Einstellungen vom alten auf den neuen Server und schlägt über Assistenten auch Problemlösungen vor, allerdings beachtet der Server nicht alles. Haben Sie zum Beispiel die Anmeldeskripte in SBS 2003 angepasst, übernimmt der SBS 2008 diese nicht immer automatisch. Sichern Sie diese Skripte daher vorher und binden Sie sie nachträglich wieder ordnungsgemäß ein. Sie finden diese auf dem Quellserver im Verzeichnis "\\localhost \ sysvol \ {DomainName}.local \ scripts". Auch die Gruppenrichtlinieneinstellungen übernimmt der Assistent nicht immer sauber, zumindest wenn Sie diese nachträglich manuell geändert haben. Am besten nehmen Sie die Einstellungen nach der Migration manuell neu vor und löschen vor der Migration die Gruppenrichtlinienobjekte. Alternativ exportieren oder sichern Sie die Einstellungen über die Serververwaltungskonsole. Die Verwaltung der SBS-Richtlinien finden Sie in der Konsole über "Erweiterte Verwaltung / Gruppenrichtlinienverwaltung / Gesamtstruktur / Domänen / {Name der Domäne} / Gruppenrichtlinienobjekte".

Überprüfen Sie nach der Installation auch die verschiedenen Konnektoren für den Mailversand. Stellen Sie sicher, dass Exchange die neuen Konnektoren von Exchange Server 2007 nutzt, nicht die des alten Servers. Löschen Sie am besten alle Konnektoren vom alten Server. Verwenden Sie den POP3-Konnektor von SBS 2003, deaktivieren Sie diesen und konfigurieren Sie die neue Version des Programms auf dem SBS 2008. Verschieben Sie auch die Postfächer vom alten auf den neuen Server. Öffnen Sie dazu die Exchange-Verwaltungskonsole auf dem neuen Server und navigieren Sie zu "Empfängerkonfiguration / Postfach". Klicken Sie nun mit der rechten Maustaste auf das Postfach, das Sie verschieben wollen, und wählen Sie den Befehl "Postfach verschieben" aus. Haben Anwender in Outlook Posteingangsregeln definiert, die im Postfach gespeichert werden, müssen Sie noch eine Besonderheit beachten: Ein Exchange 2000/2003-Server lässt für die Posteingangsregeln im Postfach eine Gesamtgröße von 32 KByte zu. Ist diese Größe überschritten, lässt sich das entsprechende Postfach nicht verschieben. In diesem Fall können Sie das Postfach über die Exchange-Verwaltungsshell bewegen. Verwenden Sie dazu den Befehl

```
Move-Mailbox {Benutzername} -TargetDa-
  tabase First Storage Group\Mailbox
  Database -IgnoreRuleLimitErrors.
```

Sie können auch mehrere Postfächer markieren und diese in einem Rutsch verschieben. Auf der ersten Seite des Assistenten wählen Sie den Server, die Speichergruppe und die Postfachdatenbank aus, in die Sie die Postfächer verschieben wollen. Beim Verschieben von zahlreichen Postfächern werden erhebliche Mengen an Transaktionsprotokollen geschrieben. Auch bei Servern mit genügend Festplattenplatz kann so schnell die Kapazitätsgrenze erreicht werden. Vor allem beim Verschieben über Nacht blüht dadurch einem Administrator am nächsten Tag eine Überraschung, wenn der Verschiebevorgang abgebrochen wurde, da die Transaktionsprotokolle die Festplatten überfüllt haben.

Um diesem Problem aus dem Weg zu gehen, sollten Sie entweder nicht zu viele Postfächer auf einmal verschieben, dafür sorgen, dass genügend Festplattenplatz verfügbar ist oder in den Eigenschaften der beteiligten Speichergruppen die Umlaufprotokollierung aktivieren, damit immer der gleiche Satz an Transaktionsprotokollen zum Einsatz kommt. Bei Abschluss dieses Vorgangs wird das Postfach zunächst auf den Zielserver kopiert und danach mit dem Quellpostfach verglichen. Erst dann wird das Quellpostfach gelöscht. Es besteht bei diesem Vorgang zu keiner Zeit irgendeine Gefahr des Datenverlustes, da das Quellpostfach bis zum Schluss vorhanden ist. Auch wenn Sie den Verschiebevorgang abbrechen, gehen keine Daten verloren. Während dieses Vorgangs können betroffene Exchange-Benutzer natürlich nicht mit ihrem Postfach arbeiten.

Startet der Benutzer nach dem Verschiebevorgang sein Outlook wieder, verbindet sich Outlook mit seinem alten Server und erhält die Information, dass das Postfach umgezogen ist. Outlook trägt automatisch den neuen Server in seine Einstellungen ein. Sie müssen lediglich dafür sorgen, dass der Quell-Exchange-Server zur Verfügung steht, wenn verschobene Benutzer ihr Outlook starten. Nach der ersten Verbindungsaufnahme mit dem neuen Exchange-Server wird auf den alten Server nicht mehr zugegriffen. Auf der nächsten Seite des Assistenten legen Sie die Optionen fest, wie mit Postfächern verfahren werden soll, die defekte Nachrichten enthalten. Sie können entweder in diesem Fall das komplette Postfach überspringen oder eine Anzahl Nachrichten einstellen, die beim Übertragen übergangen werden dürfen, wenn diese fehlerhaft sind. Achten Sie beim Verschieben darauf, dass die Größe der Postfächer nicht irgendwelche Grenzwerte auf dem Zielserver überschreitet. Ist ein Postfach zu groß, wird dieses nicht auf den Zielserver verschoben, bleibt aber auf dem Quellserver erhalten.

Auf der nächsten Seite legen Sie fest, wann der Exchange-Server mit dem Vorgang beginnen soll. Sie können das Verschieben der Postfächer entweder sofort starten oder einen Zeitpunkt angeben, zu dem der Vorgang automatisiert stattfinden soll. Abhängig von der Größe der Postfächer dauert der Vorgang unterschiedlich lange. Zum Abschluss wird Ihnen der Status für jedes einzelne Postfach angezeigt. Überprüfen Sie nach dem Verschieben auch das Anwendungsprotokoll der Ereignisanzeige auf Fehler. Achten Sie vor allem auf Meldungen der Quelle "Exchange Migration". Auch die öffentlichen Ordner müssen Sie auf den neuen Server migrieren, die entsprechende Anleitung dazu finden Sie im Link am Ende des Artikels.

Migration abschließen

Neben den hier beschriebenen Schritten sollten Sie noch überprüfen, ob die SharePoint-Daten korrekt übernommen wurden und unter Umständen nacharbeiten. Wenn Sie sicher sind, dass der neue Server funktioniert, sollten Sie erst einige Tage damit arbeiten. Vor Ablauf der 21-Tage-Frist müssen Sie jedoch den Domänencontroller auf dem SBS 2003 herabstufen sowie Exchange Server 2003 deinstallieren. Beachten Sie hier auch die Workshops in den Ausgaben 05 und 06/2008 zu den Besonderheiten des primären Exchange-Servers. Der alte Quellserver lässt sich nach der Migration auch als zusätzlicher Server in das SBS-Netzwerk integrieren. Die entsprechenden Informationen dazu finden Sie unter [13]. Eine ausführliche englische Anleitung zur Migration können Sie ebenfalls bei Microsoft unter [14] herunterladen. *(dr)*

Links

[1] SBS 2003 sichern
http://go.microsoft.com/fwlink/?LinkId=27140

[2] SBS 2003 Service Pack 1
http://go.microsoft.com/fwlink/?LinkId=46690

[3] SP2 für Windows Server 2003
http://go.microsoft.com/fwlink/?LinkId=98932

[4] Netzwerkprobleme nach Installation von SP2 für Windows Server 2003
http://support.microsoft.com/kb/936594

[5] Microsoft Core XML 6 SP1
http://go.microsoft.com/fwlink/?LinkId=87548

[6] .NET Framework 2.0
http://go.microsoft.com/fwlink/?LinkId=104397

[7] Microsoft SQL Server Management Studio Express Service Pack 2
http://go.microsoft.com/fwlink/?LinkId=104395

[8] Migration von WSS 3.0 zu SBS 2008
http://go.microsoft.com/fwlink/?LinkId=115335

[9] SP3 für SharePoint 2.0
http://go.microsoft.com/fwlink/?LinkId=101615

[10] ISA 2004 SP3
http://go.microsoft.com/fwlink/?LinkId=104551

[11] SBS Best Practices Analyzer
http://go.microsoft.com/fwlink/?LinkId=113752

[12] Probleme mit dem SBS 2008-Migrationstool
http://go.microsoft.com/FWLink/?LinkID=118672

[13] Zusätzlicher Server im SBS 2008-Netzwerk
http://go.microsoft.com/fwlink/?LinkId=104875

[14] Migrationsanleitung zu SBS 2008
www.microsoft.com/downloads/details.aspx?FamilyID=95e4863e-bb59-4a66-9fee-9874e8903888&displaylang=en

Weitere Informationen

[15] Service Pack 1 für das .NET Framework 2.0
www.microsoft.com/downloads/details.aspx?familyid=79BC3B77-E02C-4AD3-AACF-A7633F706BA5&displaylang=en

[16] Service Pack 2 für Exchange Server 2003
http://go.microsoft.com/fwlink/?LinkId=98933

[17] Öffentliche Ordner zu SBS 2008 verschieben
http://go.microsoft.com/fwlink/?LinkId=117339

Tools zur grafischen Aufbereitung von Monitoring-Daten

Ein Bild sagt mehr als tausend Mails

von Dr. Michael Schwartzkopff

Ein gutes Monitoring aufzubauen und die gewonnenen Daten regelmäßig auszuwerten, ist ein Muss für jeden Netzwerk-Administrator. Die Überwachung alarmiert nicht nur bei aktuellen Ausfällen, sondern gibt dem Administrator – durch die Aufzeichnung der historischen Werte – auch Kennzahlen für die Planung an die Hand. Wenn diese Werte auch noch grafisch aufbereitet werden, hilft das in Budgetverhandlungen oder bei der Darstellung der Leistung der Administratoren ungemein. In diesem Artikel stellen wir Ihnen geeignete Tools vor und beweisen den Mehrwert grafisch aufbereiteter Monitoring-Daten anhand von Beispielen aus der Praxis.

Allgemein hat sich die Auffassung durchgesetzt, dass eine Überwachung der Server die tägliche Arbeit der IT-Abteilung sinnvoll unterstützt. Falls ein Server Probleme macht, entdeckt der Administrator diesen Fehler und nicht erst ein Benutzer. Im Idealfall behebt der Betreuer den Fehler so schnell, dass andere nichts davon mitbekommen. Es hat so den Anschein, dass die IT wunderbar funktioniert. Das klappt aber nur, wenn ein gutes Monitoring die Server überwacht, die Alarmierung hinreichend schnell ist und der Administrator "immer" verfügbar ist.

Monitoring ≠ Reporting

Eine reine Überwachung, die den aktuellen Status nur mit den Werten "rot", "gelb" und "grün" darstellt, hat den Nachteil, dass keine echte Historie verfügbar ist. Der Klassiker für die Netzwerküberwachung "Nagios" [1] kennt den aktuellen Zustand jedes einzelnen Servers und Dienstes. Die Vergangenheit speichert Nagios als Zeitpunkt des Wechsels zwischen verschiedenen Zuständen. Im Nachhinein kann der Administrator nachvollziehen, dass ein Dienst von "OK" auf "Warnung" gewechselt hat. Informationen über die tatsächlichen Werte, die diesen Wechsel ausgelöst haben, geschweige denn auf alle Werte, die zwischen solchen Wechseln liegen, hat er allerdings nicht. Dieses Vorgehen spart zwar sehr viel Speicherplatz, verwirft aber auch sehr viele wertvolle Informationen, die dem Administrator im Notfall helfen könnten, ein Problem schnell zu lösen, das sich über längere Zeit aufgebaut hat, aber nicht bemerkt wurde.

Ein typisches Beispiel hierfür ist der Plattenplatz. Üblicherweise füllt sich eine Platte nur langsam im Laufe der Zeit. Sind die Warnungsschwellen bei "80 Prozent voll" und kritisch bei "95 Prozent voll" definiert, erhält der Administrator zwar eine entsprechende Meldung, hat aber keinen Zugriff auf eine Historie. Diese könnte ihm Aufschluss geben, über welchen Zeitraum sich das Problem aufgebaut hat (wie schnell – mit welcher Rate – sich die Platte aktuell füllt und wie viel Zeit noch bleibt, bis das Problem katastrophale Ausmaße annimmt). Der Administrator, der in solchen Momenten üblicherweise überlastet ist, kann nicht entscheiden, ob er sich sofort um das Problem kümmern muss oder ob das Problem noch Zeit bis zum Nachmittag hat.

Eine Aufzeichnung aller Messdaten ist allerdings auch in Zeiten billiger TByte-Festplatten weder sinnvoll noch machbar. Alleine die Auswertung einer sehr langen und detailreichen Historie übersteigt die Rechenleistung der üblichen Prozessoren. Ein kurzes Rechenbeispiel in einem kleinen Netz mit 50 überwachten Hosts und fünf Diensten pro Host, die alle fünf Minuten abgefragt werden, zeigt, dass 300 KByte pro Stunde oder zirka 10 GByte in fünf Jahren zusammenkommen. Diese Datenmenge kann zwar noch abgespeichert werden, aber keine der üblichen Managementstationen kann sie in normaler Zeit auswerten, um zum Beispiel aktuelle Grafiken darzustellen.

Um der Datenflut Herr zu werden, setzen die meisten Netzwerkmanagement-Programme auf sogenannte "Round Robin Datenbanken" (RRDB). Sie speichern die Daten nur für einen kurzen Zeitraum in hoher Auflösung. Zusätzlich werden Mittel- und Extremwerte für weiter zurückliegende Zeiträume abgelegt. Je weiter das Datum zurückliegt, desto größer werden die Zeiten, über die gemittelt wird. Diese Datenspeicher sind ein guter Kompromiss zwischen Genauigkeit und Datenflut.

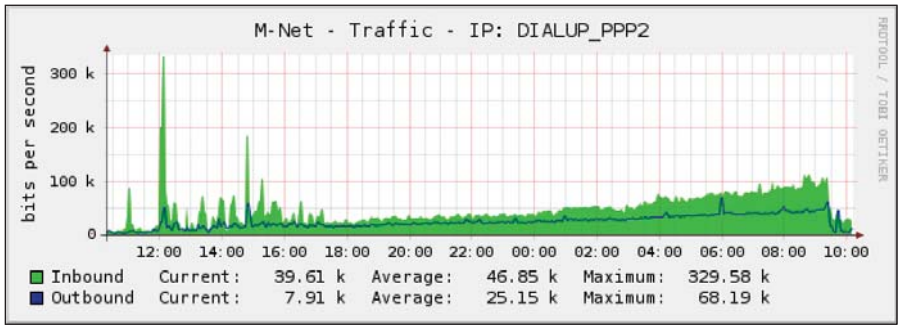


Bild 1: Die MRTG-Grafik der Auslastung der Internet-Anbindung lässt den exponenziellen Anstieg sowohl des eingehenden als auch des ausgehenden Verkehrs leicht erkennen

Werkzeuge für die grafische Aufbereitung

Das bekannteste Werkzeug für die Überwachung des Netzwerks ist Nagios. Leider zeichnet es die gemessenen Werte nicht selbst auf, sondern bietet nur eine Schnittstelle, mit der externe Programme dies erledigen können. Dabei nutzten alle Programme RRDtool [2], den Nachfolger des bekannten "Multi Router Traffic Grapher" (MRTG) [3]. Der Administrator ist selbst dafür verantwortlich, die RRDB für die langfristigen Berichte anzubinden oder eigene Messungen dafür anzustellen.

Das Programm RRDtool bietet die Schnittstelle für die vollständige Verwaltung von RRDBs. Mit *create* legen Sie eine neue Datenbank an. Natürlich müssen Sie schon beim Erzeugen der Datenbank wissen, wie groß sie werden soll und ab welchem Zeitpunkt die Mittelwertbildung einsetzt. Üblich sind genaue Werte, die 1,5 Tage zurückreichen, ein Mittelwert über sechs Messungen (also eine halbe Stunde) für den Wochenrückblick, ein 2-Stunden-Mittel für den letzten Monat und der Tagesdurchschnitt für den Jahresrückblick. Natürlich kann sich die Datenbank, falls gewünscht, auch noch Maxima und Minima pro Messpunkt merken. Die Datenbank füttern Sie mit *update* mit neuen Werten und mit *fetch* werden diese wieder ausgelesen. Eine Datensicherung beziehungsweise das Rückschreiben erledigen Sie mit *backup* und *restore*. Das Beste am RRDtool ist aber, dass sich auf Zuruf – mit dem Befehl *graph* – aus den gespeicherten Werten ansprechende Grafiken erstellen lassen.

Ist es Ihnen zu mühsam, den Befehl mit allen seinen Kommandos und Optionen zu lernen, hilft ein fertiges Werkzeug [4] für die Anbindung von RRD-tool an Nagios. Alternativ existieren auch grafische Frontends wie Cacti [5] oder Munin [6] für die RRDBs, die Sie über die Web-Oberfläche einrichten können. Diese erleichtern Ihnen die Konfiguration, führen selbstständig Messungen durch und speichern die Werte in der RRDB. Je nach Konfiguration werden die gemessenen Werte auch als Grafik exportiert, die wiederum mit dem Webserver ausgeliefert werden. So können einfach Rollenmodelle implementiert werden, bei denen die Administratoren die Datensammlung konfigurieren können und die Operatoren (oder Manager) nur einen lesenden Blick auf die erzeugten Grafiken werfen dürfen.

Wichtig ist, dass die Historie grafisch aufbereitet zur Verfügung steht, um mit einem Blick wichtige Trends zu erkennen. Die Darstellung ist deshalb so wichtig, weil der Mensch ein optisches Lebewesen ist und Zusammenhänge besser visuell erfassen kann als intellektuell über den Inhalt einer entsprechenden Warnmeldung des Monitoring-Systems.

Wenn der Administrator jeden Tag den Zustand seines System mit einem kurzen Blick auf die grafische Darstellung überprüft, werden ihm nach einiger Zeit auch kleine Abweichungen vom üblichen Verhalten sofort auffallen und er kann dem möglichen Problem auf den Grund gehen, bevor das Monitoring Alarm schlägt.

Beispiele aus der Praxis

In diesem Abschnitt haben wir einige Beispiele für die grafische Darstellung von gravierenden Fehlern in Netz gesammelt und möchten sie im Folgenden einzeln besprechen.

Datenflut

Der Datenverkehr des Internetanschlusses wird mit dem Klassiker MRTG aufgezeichnet. Aller eingehender Verkehr wird grün dargestellt, aller ausgehender Verkehr als blaue Linie. Beim morgendlichen Blick auf die Auswertung um 9.30 Uhr beschleicht den Administrator ein kurzer Anflug von Panik, denn es zeigt sich ein exponenzieller Anstieg des Verkehrs über die Nacht. Da eine kurze Extrapolation der Daten ergibt, dass spätestens am nächs-

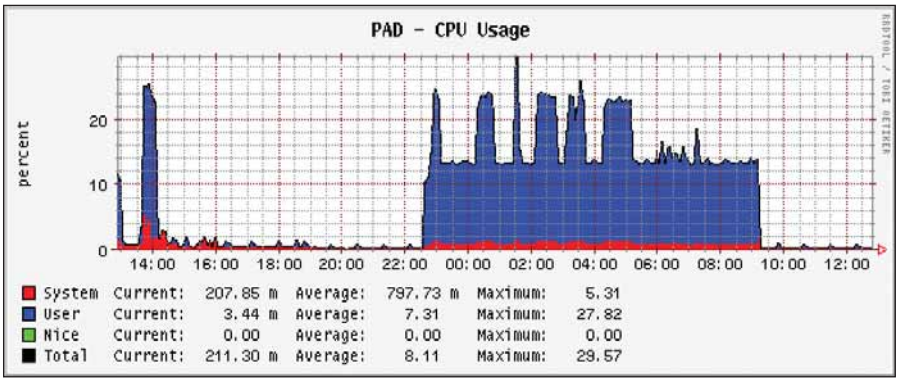


Bild 2: Die Grafik zeigt auf einen Blick, wie die andauernden Verbindungsversuche der Wörterbuchattacke gegen einen offen SSH-Port eine erhöhte CPU-Last erzeugen

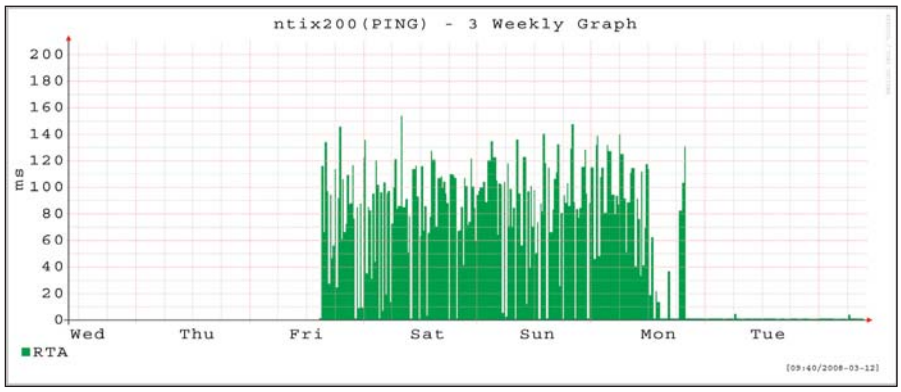


Bild 3: Nach dem Einrasten des Ethernet-Steckers in der Buchse des Servers normalisieren sich die Paketlaufzeiten

ten Abend die Leitung dicht gewesen wäre, bleibt noch genügend Zeit, das Problem genau zu analysieren und entsprechend zu reagieren.

Die Untersuchung zeigt, dass ein falsch konfiguriertes Gerät im Netz einer Außenstelle versucht hat, eine Verbindung zum zentralen Remote-Management-System aufzubauen. Nach dem Aufbau der Verbindung prüfte das Gerät jedes Mal, ob die Verbindung etabliert ist. Im Fehlerfall baute das Gerät die Verbindung neu auf. Der Fehler bestand darin, dass die Prüfung der Verbindung immer fehlschlug und beim Aufbau der neuen Verbindung die alte nicht abgebaut wurde. Über die Zeit versuchte der Rechner also mehrere Hundert Remote Management Sessions aufzubauen. Als Reaktion unterbindet der Administrator, dass die Firewall Verkehr vom betroffenen Rechner weiterleitet und sorgt dafür, dass dieser zudem mit ICMP "Host unreachable" abgewehrt wird. Danach kann der Administrator in aller Ruhe die Außenstelle unterrichten und Gegenmaßnahmen einleiten. Das Problem wurde erkannt und gelöst, obwohl der Verkehr auf der Leitung noch weit von allen Schwellwerten entfernt war.

Rumpelstilzchen-Angriffe

Ein beliebtes Ziel von Angreifern sind offene SSH-Ports. Dort versuchen sie, Passwörter von Benutzern durch plumpes Ausprobieren herauszufinden. Die entsprechenden Verbindungen verursachen natürlich eine hohe Prozessorlast, besonders wenn die Prozessoren in Netzwerkkomponenten nicht besonders leistungsfähig sind. Mit iptables lassen sich solche Angriffe leicht über die Limitierung der Anzahl der Verbindungen verhindern.

In machen kommerziellen Appliances gibt es allerdings keine Möglichkeit einer solchen Begrenzung. Wie Sie in Bild 2 erkennen, ist die Auslastung der CPU einer Firewall ab 22.30 Uhr bis kurz nach 9.00 Uhr des folgenden Tages erhöht. Die Kontrolle der Logfiles bestätigt den Verdacht auf eine sogenannte Rumpelstilzchen-Attacke, bei der wahllos Passwörter für verschiedene Benutzernamen durchgetestet wurden. Das Besondere an dieser Attacke ist die ungewöhnlich lange Dauer von über elf Stunden. Normalerweise sind diese Angriffe kürzer, wie auch gegen 14.00 Uhr zu erkennen. Leider lässt diese Appliance keine anderen Möglichkeiten als die Einschränkung der Absenderadressen zu, was jedoch in diesem Fall nicht möglich war. Auf der anderen Seite belasten die Angriffe die CPU auch nicht so stark, dass eine Einschränkung der Funktion zu erkennen ist. Deshalb wird in diesem konkreten Fall auf eine Reaktion verzichtet.

Einstecken hilft

Der folgende Fall zeigt, dass kleine Ursachen, die mit einem Handgriff zu beheben sind, manchmal große Auswirkungen haben können: Nach dem Aufbau einer Netzwerküberwachung zeigen sich bei einem Server im Netz extrem lange Paketlaufzeiten. Bei anderen Rechnern, die am selben Switch angeschlossen sind, liegen die Laufzeiten bei unter 2 ms. Bei diesem Rechner liegen sie um die 100 ms, ein Phänomen, das zuerst nicht erklärt werden kann. Auch die üblichen Sprüche ("schlechte Implementation des Netzwerk-Stacks im Betriebssystem") helfen nicht wirklich bei der Suche nach der Ursache. Erst eine Kontrolle der Verbindung vor Ort zeigt, dass der Stecker am Server nicht ganz eingerastet ist. Nach dem "Klick" gehen die Werte für die Laufzeit auf die üblichen Werte zurück.

Mailserver-Update

Gute grafische Berichte dienen auch dazu, den Erfolg Ihrer Arbeit zu dokumentieren. Im folgenden Fall wurde der Mailserver auf den neuesten Stand gebracht. Der Administrator führte sowohl eine neue Version von SpamAssassin ein als auch Greylisting zur Abwehr unerwünschter Spam. Der Erfolg lässt sich am deutlichsten in Bild 4 verfolgen: Die Gesamtzahl der Verbindungsversuche

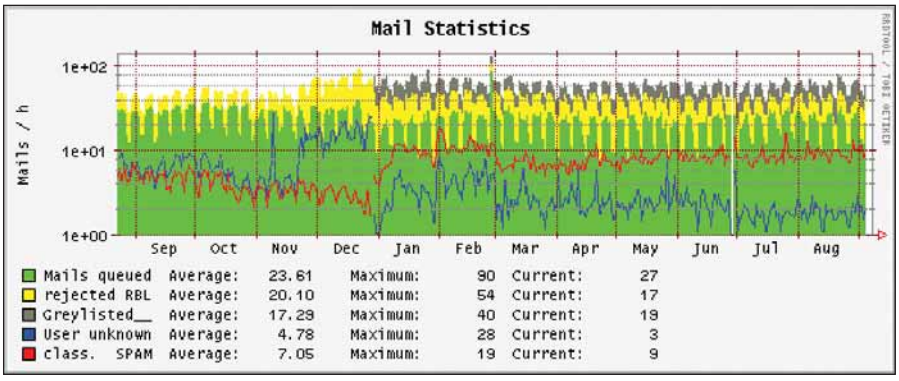


Bild 4: Die grafische Darstellung der Arbeit eines Mailservers zeigt, dass sich nach dem Update der Software die Erkennungsrate schlagartig verbesserte und die Benutzer fast keine unerwünschten E-Mails erhalten

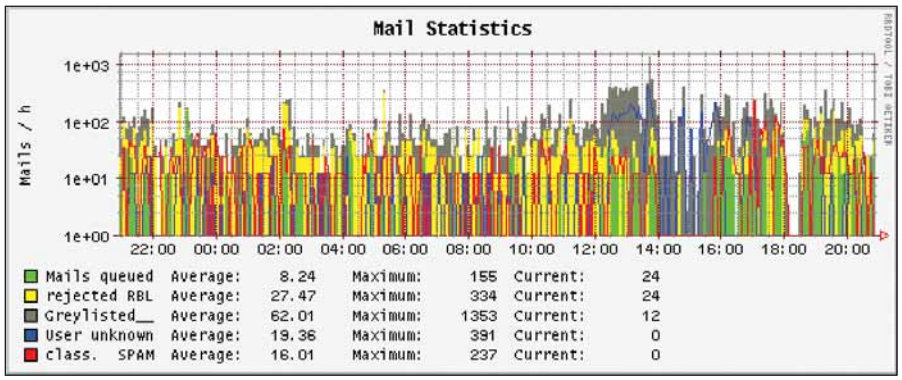


Bild 5: Die Grafik zeigt eindrücklich die Entwicklung des Spam-Aufkommens und den Erfolg entsprechender Gegenmaßnahmen

blieb über den Zeitpunkt der Veränderungen Ende Dezember ungefähr konstant. Auffallend ist eine deutliche Verbesserung der Erkennungsrate von SpamAssassin (rote Linie) um den Faktor 3 von 3 auf 10 pro Stunde. Die Rate der tatsächlich ausgelieferten Mails (grüne Kurve) verringerte sich im gleichen Maße. Die objektiv gemessene Verbesserung spiegelte sich auch im subjektiven Gefühl der Benutzer wieder.

Spuren eines Joe-Jobs

Ein Alptraum für jeden Mailadministrator ist eine Lawine von Mails, gegen die er sich nicht wehren kann. So etwas kann passieren, wenn ein Spammer die Absenderadresse fälscht. Der Mailserver leitet dabei alle Rückmeldungen über Spamversand oder nicht existente Postfächer an den eigenen Mailserver weiter. Ein Vorgehen, das auch als subtile Art von Angriff verwendet werden kann. Daher sollten Meldungen von Virenscannern nie an den scheinbaren Absender der Mail gesendet werden.

In Bild 5 (die Skala ist logarithmisch) sind per Realtime Blacklist (Spamhaus) abgelehnte Verbindungsversuche (gelb), per Greylisting vertröstete Verbindungsversuche (grau), von SpamAssassin verworfene Mail (rot) und tatsächlich ausgelieferte Mail (grün) dargestellt. Der blaue Graph stellt alle Mails dar, die an einen nicht vorhandenen User geliefert wurden.

Ab kurz nach 12 Uhr steigt zuerst das Greylisting von 60 auf etwa 300 pro Stunde (Faktor 5) an. Kurz darauf steigen auch die Versuche, einem unbekannten Benutzer eine Mail zu senden. Die Werte stabilisieren sich erst wieder, als der Administrator um 16:00 Uhr Gegenmaßnahmen ergeift (User anlegen und Mails an "/dev/null" weiterleiten).

In diesem Fall war der Angriff folgenlos, da der Mailserver mit genügend Reserven ausgelegt war und die wenigen hundert Mails pro Stunde keine ernsthafte Bedrohung darstellten. Anders würde das aussehen, wenn der Mailserver normalerweise am Kapazitätslimit arbeitet und dann noch die fünffache Menge von E-Mails verarbeiten soll. Aber mit einem guten Berichtswesen sollte man auch die CPU-Auslastung protokollieren und frühzeitig Maßnahmen ergreifen, falls der Server Schwächen zeigt. *(jp)*

Links

[1] **Nagios-Homepage**
www.Nagios.org

[2] **RRDtool Download**
http://oss.oetiker.ch/RRDtool

[3] **Multi Router Traffic Grapher**
www.mrtg.org

[4] **Nagios Grapher**
www.pnp4Nagios.org/pnp/start
www.Nagiosforge.org/gf/project/Nagiosgrapher
sourceforge.net/projects/Nagiosgraph

[5] **RRDtool-basiertes grafisches Fornend Cacti**
www.cacti.net

[6] **RRDtool-basierte Monitoringlösung Munin**
http://munin.projects.linpro.no

Exchange Server 2007

Postfachexport per PowerShell

von Robert Lindermeier

Das mächtige Tool ExMerge wird seit der Version Exchange 2007 nicht mehr von Microsoft unterstützt. ExMerge ist ein sehr nützliches Tool für den Exchange-Administrator, erlaubt es doch den Export von Postfachinhalten bis hin zum "Bereinigen" von Postfächern. Es gibt zwar im Internet einige Anleitungen, wie Sie ExMerge trotzdem noch zur Zusammenarbeit mit Exchange 2007 bewegen können, aber auf diese Möglichkeit möchten wir hier nicht weiter eingehen. Insbesondere sei darauf hingewiesen, dass ExMerge auf PST-Dateien mit maximal 2 GByte beschränkt ist. Wie so vieles wurden die Funktionen des Tools direkt in die Exchange-Verwaltungsshell verpackt. In diesem Workshop stellen wir daher den Ex- und Import eines Postfachinhalts über die PowerShell nach.

Der Ex- und Import setzt folgende Punkte voraus:

- Der Vorgang wird auf einer 32-Bit-Workstation mit installiertem Outlook 2003 oder 2007 durchgeführt.
- Der Benutzer, der den Vorgang ausführt, muss Exchange-Administrator mindestens auf dem Exchange 2007 Server sein, gegen den der Vorgang läuft.

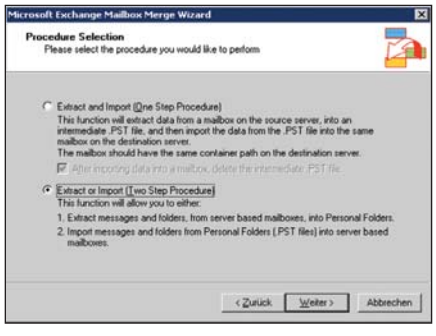


Bild 1: ExMerge findet unter Exchange 2007 keine Unterstützung mehr

Hier stellt sich schon der erste Unterschied zur Benutzung von ExMerge heraus, bei dem Sie zwingend vollen Postfachzugriff (Send As und Receive As) benötigen. Um nun ein Postfach zu exportieren, öffnen Sie die Exchange-Verwaltungsshell, um das Cmdlet "Export-Mailbox" hierfür zu benutzen. Die Syntax sieht wie folgt aus:

```
Export-Mailbox -Identity {Postfacha-
  liasname} -PSTFolderPath {Pfad zur
  PST-Datei}
```

Den Postfach-Aliasnamen entnehmen Sie den Eigenschaften des Postfachs. Der Befehl hierfür lautet beispielsweise

```
Export-Mailbox -Identity "robertl"
  -pstfolderpath "D:\E-Mail-Export"
```

Bevor die Verwaltungsshell den Befehl ausführt, müssen Sie noch den Hinweis bestätigen, dass der Vorgang sehr viel Zeit in Anspruch nehmen kann. Während des Exports zeigt die Verwaltungsshell den aktuell bearbeiteten Ordner an, inklusive der gelöschten Objekte aus dem Papierkorb. Dies erklärt am Ende auch, warum die PST-Datei meist bedeutend größer ist als die eigentliche Postfachgröße. Lassen Sie sich auch nicht von der Meldung "Die Nachrichten werden verschoben" irritieren, die Nachrichten werden tatsächlich nur exportiert und nicht gelöscht.

Mit ExMerge ist es möglich, mehrere Postfächer gleichzeitig beziehungsweise nacheinander zu exportieren. Auch mit der Verwaltungsshell besteht diese Möglichkeit. Nutzen Sie hierfür einfach die

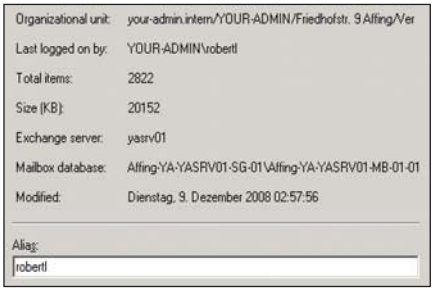


Bild 2: In den Postfacheigenschaften finden Sie den Aliasnamen, den Sie für den Umzug benötigen

Skriptmechanismen, indem Sie eine Liste von Postfächern – etwa die Postfächer einer bestimmten Datenbank – ausgeben und diese in das Export-Mailbox-Cmdlet einleiten. Das Kommando sieht beispielsweise so aus:

```
Get-Mailbox -Database {Name-des-
  Postfachspeicher} | Export-Mailbox
  -PSTFolderPath {Pfad zu PST-Dateien}
```

Nach erfolgreichem Export erhalten Sie eine detaillierte Ausgabe über den gesamten Vorgang sowie weitere Details wie Dauer, Postfachgröße und den Namen einer XML-Datei mit den gesamten Vorgangsdaten. Der Import-Befehl ist nahezu identisch und damit auch einfach auszuführen:

```
Import-Mailbox -Identity {Postfacha-
  liasname} -PSTFolderPath {Pfad zur
  PST-Datei}
```

Der Name der PST-Datei entspricht in diesem Fall, wie auch beim Export, dem Aliasnamen des Postfachs. *(dr)*

Robert Lindermeier ist Geschäftsführer und Inhaber von YOUR-ADMIN.

In jeder Ausgabe präsentiert Ihnen IT-Administrator Tipps und Tricks 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

Wenn ich Rechner unter Windows XP starte, kommt es manchmal vor, dass bei der Anmeldung kein **deutsches Tastatur-Layout** zur Verfügung steht. Das macht die Eingabe der Benutzerdaten schwierig, da das Passwort auch aus Sonderzeichen besteht. Die angeschlossene Tastatur selbst ist natürlich eine deutsche. Was kann ich hier tun?

Über eine Änderung in der Registry haben Sie die Möglichkeit, auch bei der Anmeldung an Windows für ein deutsches Tastatur-Layout zu sorgen, sollte dieses nicht vorhanden sein. Starten Sie hierfür den Registry-Editor mit dem Befehl

```
regedit
```

und gehen Sie zum Schlüssel "HKEY_USERS / .DEFAULT / Keyboard Layout / Preload". Dort finden Sie im rechten Fenster den Wert "1". Öffnen Sie diesen durch einen Doppelklick und tragen Sie den Wert "00000407" ein. Wenn Sie nun Ihren Rechner neu booten, sollte Ihnen bei der Anmeldung die deutsche Tastenbelegung zur Verfügung stehen. *(dr)*

Auf meinem Vista-Desktop prangt an allen Icons der bekannte **Verknüpfungspfeil**. Dies ist natürlich sinnig, da es sich um Verknüpfungen handelt. Dennoch würde ich diese Pfeile gerne entfernen, da es keinen Unterschied zwischen verlinkten und auf dem Desktop vorhandenen Dateien geben soll. Gibt es hierfür eine Möglichkeit?

Es ist ohne Schwierigkeiten möglich, die Verlinkungspfeile aus den Icon zu entfernen. Dann sehen Sie natürlich auf den ersten Blick nicht mehr, ob es sich um eine Verlinkung handelt. Gehen Sie in der Registry zum Schlüssel "HKEY_CLASSES_ROOT / lnkfile". Dort finden Sie den Wert "IsShortcut" auf der rechten Seite. Klicken Sie diesen Wert mit der rechten Maustaste an und benennen Sie diesen in "AriochIsShortcut" um. Beenden Sie nun den Registry-Editor und starten Sie Ihren Rechner neu. Anschließend sind die kleinen Pfeile verschwunden. *(dr)*

Wir nutzen ab und zu noch ein altes **16-Bit-Programm unter Windows XP**. Leider verursacht dieses im Speicher dann Probleme, was unter anderem zu Abstürzen führt. Können wir etwas hiergegen unternehmen?

Eine Möglichkeit wäre, das Programm nochmals explizit in einem getrennten Speicherbereich auszuführen. Legen Sie hierfür eine Verknüpfung zu der ausführbaren Datei der Software an. Klicken Sie nun mit der rechten Maustaste auf dieses Icon und gehen Sie zum Menüpunkt "Eigenschaften / Erweitert". Aktivieren Sie dort die Option "In getrenntem Speicherbereich ausführen". Starten Sie nun die 16-Bit-Applikation über diesen Link, sollte Windows sie in einem separaten Memory-Bereich ausführen und andere Programme dadurch nicht beeinträchtigen. *(dr)*

Wenn ich Programme oder Dateien auf meinem Windows-Rechner lösche, vergesse ich manchmal, den zugehörigen Link zum Beispiel auf dem Desktop mitzuentfernen. Klicke ich diesen nun versehentlich an, beginnt Windows, nach der verlinkten Datei zu suchen. Das nimmt jedoch unnötig Zeit in Anspruch und bringt nichts. Wie kann ich diese **Suchfunktion** ausschalten?

Sie können diese Suchfunktion, die durch ihr Taschenlampensymbol bekannt ist, deaktivieren. Starten Sie dazu den Registry-Editor und öffnen Sie den Zweig "HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ System". Dort legen Sie den Wert "NoResolveSearch" an, sofern er noch nicht existiert, und setzen ihn auf "1". Nun dürfte Windows nicht mehr nach "toten Links" auf Ihrem Desktop suchen. *(dr)*

Lotus software

Wir nutzen Lotus Notes 8 in unserem Netzwerk. Einige der Nutzer sollen den

Standard-Client starten können, während anderen Usern nur der **Basic-Client** zur Verfügung stehen soll. Dies lässt sich normalerweise auch über den Startparameter "-basic" regeln. Doch beim automatisierten Aufruf der Software durch eine Nutzeraktion geht das nicht. Was können wir hier tun?

Seit Version 8.0.2 können Sie dem Notes-Client auch über die Datei *Note.ini* mitgeben, ob er grundsätzlich als Standard- oder Basic-Ausführung starten soll. Denn es ist richtig, dass der Startparameter "-basic" nicht funktioniert, wenn die Nutzer etwa einen Mailto-Link anklicken und sich daraufhin der Client öffnet. Editieren Sie also die INI-Datei und fügen Sie die Zeile

```
UseBasicNotes=1
```

hinzu. Danach startet die Software nur noch in der Basic-Variante. *(dr)*

Auf unserem Domino-Server möchten wir mehrere Mailbox-Datenbanken **"mail.box"** nutzen. Doch leider verwendet der Server dann die ursprüngliche Datei nicht mehr, sondern nur noch "mail{n}.box". Wie lässt sich dieses Problem umgehen?

Einige Programme können Schwierigkeiten machen, wenn die Mailbox-Datenbank *mail.box* nicht mehr genutzt wird, sondern nur noch Datenbankdateien mit fortlaufender Nummerierung. Um dieses Problem aus der Welt zu schaffen, tragen Sie einfach die Zeile

```
Mail_Enable_Mailbox_Compatibility=1
```

in die Konfigurationsdatei *Note.ini* ein. Dadurch kommt auch die ursprüngliche Mailbox-Datei zum Einsatz. *(dr)*

Linux

Wie kann ich auf meinem Linux **mehrere Swap-Partitionen** gleichzeitig nutzen, damit etwa das Auslagern von Dateien schneller vonstatten geht?

Um mehrere Swap-Partitionen parallel über RAID zu nutzen, müssen Sie deren Prioritäten unter Linux angleichen. In der Datei */etc/fstab* finden Sie den Eintrag

```
/dev/hdx swap swap defaults,pri={Nummer} 0 0
```

Über die {Nummer} bestimmen Sie dabei, in welcher Reihenfolge die verschiedenen Partitionen genutzt werden sollen, sprich die Priorität. Setzen Sie nun zwei oder mehr Swap-Partitionen auf die gleiche Priorität, greift der Linux-Kernel quasi auf beide parallel zu. *(dr)*

Mozilla / Firefox

Ich habe mehrere E-Mail-konten und möchte gerne auch **verschiedene Instanzen von Thunderbird** mit unterschiedlichen Profilen auf meinem XP-Rechner nutzen. Doch leider lässt sich immer nur eine Instanz des Mailprogramms starten. Wie geht dies?

Sie können über eine Systemvariable auch mehrere Thunderbird-Instanzen ausführen und so etwa verschiedene Profile für Ihre Mailkonten gleichzeitig nutzen. Legen Sie hierfür die Systemvariable "MOZ_NO_REMOTE" an, indem Sie die Systemeigenschaften (etwa über einen Rechtsklick auf den Arbeitsplatz – "Eigenschaften") öffnen und unter dem Reiter "Erweitert" auf "Umgebungsvariablen" klicken. Nun klicken Sie unter "Systemvariablen" auf den Knopf "Neu" und tragen als Namen die zuvor genannte Variable ein. Um diese zu aktivieren, setzen Sie nun noch den Wert auf "1" und bestätigen Ihre Eingaben. Nun müssen Sie noch gegebenenfalls Ihr System neu starten, und Thunderbird lässt sich fortan in verschiedenen Instanzen aufrufen. *(dr)*

CITRIX

Was können wir auf unserem XenServer 5.0 tun, wenn bei der Konfiguration der Eigenschaften eines Netzwerkadapters in einer virtuellen Maschine die Meldung von Windows kommt, dass eine **zugewiesene IP-Adresse bereits im Netzwerk benutzt** wird?

Haben Sie eine XenConvert- oder V2XVA-Operation durchgeführt oder ein Netzwerk-Interface ohne Installation der XenServer Tools konfiguriert, meldet Windows, dass die Adresse, die Sie konfigurieren wollen, bereits einem anderen Netzwerk-Interface zugewiesen wurde. Das kann passieren, wenn ein Netzwerkgerät bereits konfiguriert und später entfernt wurde. In diesem Fall behält Windows die Konfiguration bei und generiert die Warnmeldung, obwohl der Netzwerkadapter aktuell nicht mehr im Netzwerk vorhanden ist. Um das Problem zu lösen, müssen Sie die Konfiguration für das inaktive Gerät entfernen. Geben Sie hierfür auf der Befehlszeile das Kommando

```
set devmgr_show_nonpresent_devices=1
  start devmgmt.msc
```

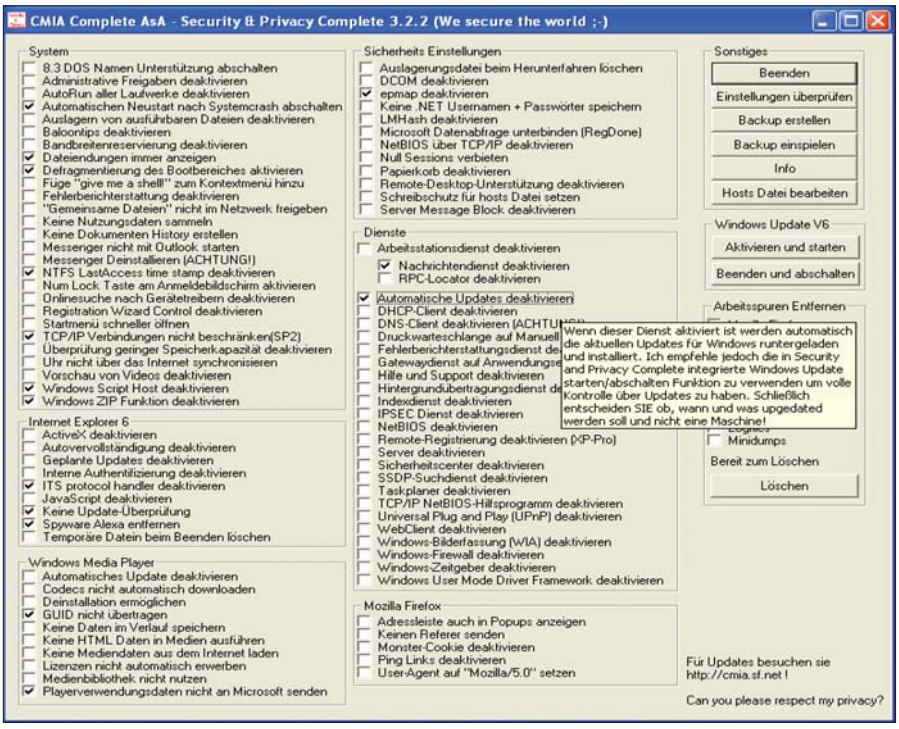
ein. Öffnet sich nun der Device Manager, klicken Sie auf "View / Show Hidden Devices". Im Menüpunkt "Network Adapters" wählen Sie anschließend die Netzwerkgeräte aus, die nicht länger im System präsent sind. Klicken Sie mit der rechten Maustaste auf die inaktiven Geräte und wählen Sie den Menüpunkt "Uninstall" aus. Starten Sie nach dem Entfernen der alten Geräte die virtuelle Maschine neu und rekonfigurieren Sie das Interface mit der gewünschten IP-Adresse. *(Citrix/dr)*

Tools

Bekanntermaßen bieten diverse Komponenten und Standardeinstellungen von Windows-Systemen Schadsoftware eine weit geöffnete Tür an. Das Werkzeug **Security & Privacy Complete 3.2.2** hilft, alle offenen Türen unter Verwendung einer einfachen GUI mit

Checkboxen zu schließen und darüber hinaus eine ganze Reihe sinnvoller Einstellungen in Sachen Geschwindigkeit und Privatsphäre zu treffen.

Mit der Version 3 (aktuell ist 3.2.2) verzichten die Entwickler dabei auf die Notwendigkeit des .NET-Frameworks und bieten dem Anwender eine echte Standalone-Lösung zum Schutz des Rechners an. Dabei lassen sich mit Security & Privacy Complete über hundert Einstellungen festlegen, auch solche, die Windows sonst dem Nutzer vorenthält, wie etwa die Deinstallation des Windows Messengers. In Sachen Systemsicherheit erlaubt das Tool etwa festzulegen, dass die Auslagerungsdatei beim Herunterfahren zu löschen ist oder auch den Schutz der hosts-Datei, die Angriffsziel zahlreicher Malware darstellt. Darüber hinaus bietet die Lösung die Aktivierung zahlreicher Einstellungen, um den Start und das Herunterfahren von Windows zu beschleunigen, unnötige Dienste dauerhaft abzuschalten sowie den Schutz der Privatsphäre bei der Nutzung des Internets. Zu finden ist Security & Privacy Complete unter http://cmia.backtrace.org/ *(jp)*



Nützliche Hinweise zu jeder Einstellung erleichtern die Arbeit mit Security & Privacy Complete 3.2.2

Mit **Login Virtual Session Indexer (Login VSI)** stellt das Beratungshaus " Login Consultants" ein plattformunabhängiges Benchmarkwerkzeug bereit. Das Werkzeug hilft IT-Verantwortlichen, die Leistungsfähigkeit von Hardwareplattformen in Terminalserver und Virtual Desktop-Infrastrukturen zu messen, um so Neuanschaffungen oder Änderungen der Infrastruktur besser planen zu können.

Die Version 1.0 von Login VSI steht nach einer Registrierung auf der Webseite kostenlos zur Verfügung. Login VSI erlaubt beispielsweise auch den Performance-Vergleich unterschiedlicher Storagesysteme, zeigt die Auswirkungen von Updates oder Hotfixes und erlaubt IT-Verantwortlichen den Vergleich unterschiedlicher Plattformen (beispielsweise VMware versus Hyper-V). Darüber hinaus deckt Login VSI noch zahlreiche weitere Felder wie etwa die Auswirkung einer Tuningmaßnahme ab und wird so zum unverzichtbaren Begleiter für jeden Administrator oder IT-Leiter, der mit der Planung von Terminalserverumgebungen betraut ist. *(jp)*

Quelle: www.loginconsultants.com

Mit dem **Offline Virtual Machine Servicing Tool 2.0** lassen sich virtualisierte Rechner aktualisieren, auch wenn diese aktuell offline sind. Das Werkzeug hilft Administratoren zudem, das Sicherheitsrisiko bei derartigen Updates zu minimieren.

Das Offline Virtual Machine Servicing Tool erlaubt die Aktualisierung von virtuellen Maschinen, die in einer Library des Microsoft System Center Virtual Machine Manager gespeichert sind, und eignet sich insbesondere für die Verwaltung von großen Infrastrukturen mit Hunderten oder Tausenden VMs.

Die neue Version 2.0 beinhaltet vor allem die Kompatibilität mit Hyper-V und System Center Virtual Machine Manager (SCVMM) 2008. Darüber hinaus werden die aktuellen Versionen von SCCM und WSUS unterstützt. Dabei automatisiert das Tool im Prinzip nur den Start einer solchen VM, leitet das Update (etwa mit WSUS) ein und fährt die VM dann wieder herunter, um sie – frisch gepatcht – wieder an ihrem ursprünglichen Ort zu speichern. Dabei lassen sich mit WSUS und SC Configuration Manager auch Updates von Drittanbietern einspielen. *(jp)*

Quelle: www.microsoft.com/downloads/details.aspx?FamilyId=8408ECF5-7AFE-47EC-A697-EB433027DF73&displaylang=en

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

Anomaly Detection-Lösungen

Frühwarnsystem für die Netzwerk-Performance

von Paul O´Reilly

Die Leistungsfähigkeit von Software ist immer dann gefährdet, wenn Anomalien und Unregelmäßigkeiten innerhalb der Netzwerk-Infrastruktur auftreten. Eine Herausforderung für jeden Systemadministrator ist es, den Überblick zu behalten. Hier haben sich Werkzeuge zur Erkennung von Unregelmäßigkeiten, sogenannte "Anomaly Detection"-Lösungen, bewährt. Sie versprechen eine Kontrolle der Verhaltensänderungen in Echtzeit. In diesem Beitrag gehen wir auf die Grundlagen dieses Frühwarnsystems ein und skizzieren, auf welche Unregelmäßigkeiten diese reagieren.

Um für ein reibungsloses Zusammenspiel von Anwendungen und Systemen zu sorgen und frühzeitig möglichen Problemen entgegenwirken zu können, sollte der vollständige Überblick über das Netz, insbesondere über das Verhalten des Datenflusses gegeben sein. Anomaly Detection-Lösungen wurden ursprünglich aus sicherheitsrelevanten Gründen für die IT-Sicherheitsverantwortlichen entwickelt und nicht im Hinblick auf die Stabilität und Leistung von Netzwerken im Unternehmen. Sie wurden traditionell zur Absicherung gegen Gefahren und Angriffe eingesetzt, wie etwa durch Würmer, Schadprogramme, DDOS (Distributed Denial of Service)-Attacken und andere unerwünschte Zugriffe auf das Netzwerk. Das führte in den letzten Jahren auch dazu, dass immer häufiger von der Netzwerkverhaltensanalyse oder Network Behaviour Analysis (NBA), die Rede ist.

Es liegt nahe, dass diese Art von Applikationen zum großen Teil durch IT-Security-Teams eingekauft werden, die die Anomaly Detection-Software oft als reine Sicherheitslösung betrachten. Doch abgesehen vom Sicherheitsaspekt liefern die Lösungen weit mehr als nur Schutz: Sie dienen auch als Frühwarnsystem für die Performance eines Netzwerks. Damit sind sie ein wichtiger Teil eines Network Performance Management-Ansatzes. Das Ziel ist es, Administratoren auf dem Weg zu optimal ausgelasteten und aufgebauten Netzwerkinfrastrukturen im Unternehmen zu unterstützen, um die uneingeschränkte Verfügbarkeit von Applikationen und ihre bestmögliche Leistung zu gewährleisten.

Eine derartige Lösung unterstützt Netzwerkadministratoren und gibt lückenlos Aufschluss über die End-User Response Time von Applikationen,VoIP-Metriken zur Qualitätssicherung, Beeinträchtigungen der Netzwerk- und Anwendungsperformance. Weiterhin lassen sich Leistungsprobleme in Appli-

Anomaly Detection ist ein performanceorientierter Ansatz für die Netzwerkverhaltensanalyse. Entsprechende Tools machen Unregelmäßigkeiten in Netzwerkverkehrsmustern mit den Anomalie-Erkennungsfunktionen sichtbar. Dabei dient beispielsweise die Cisco IOS NetFlow-Technologie als Datenquelle und liefert Informationen und Analysen in Echtzeit ebenso wie historische Daten für viele Hunderttausend Netzwerkverbindungen weltweit. Zusätzlich untersuchen die Anomalie-Erkennungsfunktionen die Verkehrsmuster in den NetFlow-Daten, die für alle Clients und Server im Netzwerk erfasst werden. Werden ungewöhnliche Verhaltensmuster entdeckt, dann informiert das Werkzeug die Netzwerkadministratoren etwa über ein Webportal, per E-Mail oder Trap-Funktion.

Anomaly Detection

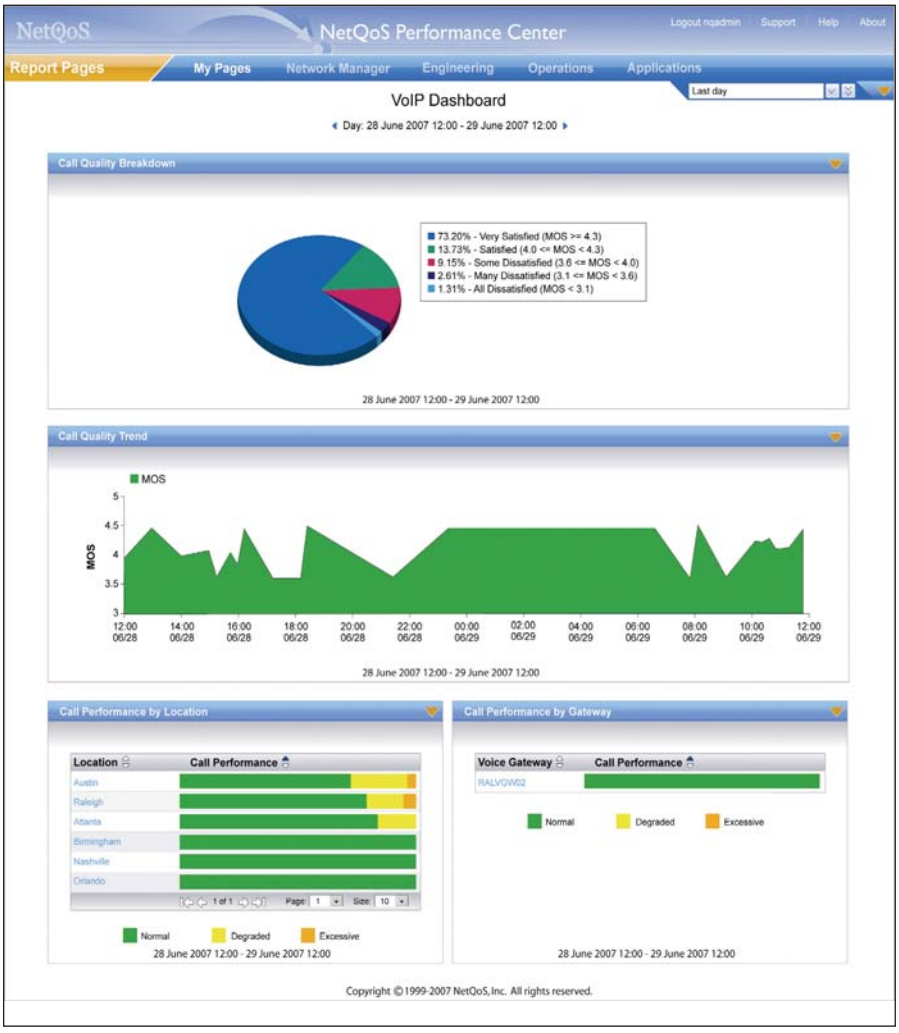
kationen, Servern und Netzwerken isolieren, die Bandbreiten von Applikationen und Benutzern ermitteln, um Kosten zu regulieren sowie Viren und DOS-Attacken identifizieren.

Brückenschlag zwischen Sicherheit und Netzwerk-Performance

Inzwischen wurden die Anomaly Detection-Lösungen weiterentwickelt, um sowohl den Anforderungen von Sicherheits- als auch Netzwerk-Performance-Teams gerecht zu werden. Sie liefern nicht nur frühzeitige Hinweise auf Sicherheitsbedrohungen oder Schwachstellen, sondern melden gleichzeitig, wenn User oder Anwendungen im Netz die Leistungsfähigkeit der gesamten Infrastruktur beeinträchtigen könnten. Unregelmäßigkeiten, die User an ihrem Arbeitsplatz wahrnehmen werden, indem beispielsweise Applikationen langsamer arbeiten.

Für den Netzwerkadministrator ist es entscheidend, dass er rechtzeitig über Anomalien informiert wird – idealerweise bevor das gesamte Netz in Mitleidenschaft gezogen wird. Er sollte auch in der Lage sein, die Auswirkungen auf die Antwortzeit von Applikationen zu ermitteln. Sie ist eine kritische Größe für die Beurteilung des Verhaltens der Software auf der Nutzerseite. Lösungen zur Anomalie-Erkennung haben sich als effizientes Werkzeug in Unternehmen bewährt, wenn sie die Funktionen zur Erkennung, Wirkungsanalyse und Fehlersuche in einem lückenlosen Workflow unterstützen.

Besonders hilfreich und wichtig sind die Details: Werden beispielsweise Host-Informationen zu einer erkannten Unregelmäßigkeit ohne die zugehörigen Schnittstellen und Router angezeigt, können wichtige Abhängigkeiten übersehen werden. Die Auswirkungen der Netzwerkunregelmäßigkeiten werden nicht im ganzen Ausmaß erkannt und die Fehlerbehebung wird erschwert. Da



Wie hier das "NetQoS Performance Center", informiert eine Anomaly Detection-Lösung auch über die Qualität des VoIP-Datenverkehrs

sie lediglich Veränderungen im Netzwerkverkehr sichtbar machen, kommen herkömmliche Network Behaviour Analysis-Lösungen schnell an ihre Grenzen.

Für die Erkennung von Unregelmäßigkeiten im Netzwerk stehen verschiedene Methoden und Datenquellen zur Verfügung. Häufig werden dabei der Datenverkehrsfluss und die Datenpakete analysiert. Mithilfe von Algorithmen untersuchen und profilieren sie die Verkehrsmuster für jeden Host (Client oder Server) im Netzwerk. Die Übersicht über diesen Netzwerkverkehr enthüllt verschiedene Anomalien – von Veränderungen bei den Pakettypen, die ein bestimmter Host über das Netzwerk versendet, bis hin zu Veränderungen im Umfang der Paketaussendungen. Jede dieser Veränderungen kann ein Warnzeichen für einen infizierten Host sein. Oder aber einfach ein Hinweis auf ein verändertes Nutzerverhalten, wenn auch nicht in schädlicher Absicht, das jedoch die Performance von Applikationen merklich beeinträchtigt.

Arten von Unregelmäßigkeiten

So könnte beispielsweise ein plötzlicher Anstieg des Paketvolumens bedeuten, dass ein Benutzer eine nicht erlaubte Applikation, beispielsweise eine Filesharing-Anwendung wie etwa Bit Torrent oder Kazaa benutzt. Eine solche Veränderung im Netzwerkverhalten richtet gewöhnlich nicht den gleichen

Schaden an wie beispielsweise ein Wurm oder ein Virus, kann aber durch die Belegung von Bandbreite und die Inanspruchnahme von Ressourcen die Bereitstellung von Applikationen behindern. Besondere Unregelmäßigkeiten, etwa auffällige Datenpakete bei Hosts, können ebenfalls ein Indiz für ein potenziell schädliches Verhalten sein. Solche Anomalien können auf eine unsachgemäß konfigurierte Anwendung hindeuten, die sich nachteilig auf die Performance auswirken kann, wenn Client-Anfragen nicht ordnungsgemäß bearbeitet werden.

Die Fragmentierung von Datenpaketen ist eine weitere Unregelmäßigkeit, die durch einen Fehler im Netzwerk verursacht werden kann. Solche Fehler oder Veränderungen der Netzwerkkonfiguration können ebenfalls zu einer Beeinträchtigung der Applikationsleistung führen. Werden beispielsweise Quellen von sogenannten "Nullrouten" entdeckt, können fehlerhafte Access Control Lists (ACLs) dafür verantwortlich sein. Die Überwachung des TTL-Bits im Netzwerkverkehr kann auch Routing-Schleifen sichtbar machen. Die Erkennung beider Verhaltensweisen spielt eine wichtige Rolle, um das Netzwerk ordnungsgemäß abzusichern und Applikationsdienste zeitnah bereitstellen zu können.

Weitere verdächtige Netzwerkaktivitäten sind fragmentierte Paketquellen, reine SYN-Paketquellen und eine hohe Paketstreuung. Diese Verhaltensweisen können auf Hacker hinweisen, die versuchen, Firewalls zu überwinden, oder auf das Vorhandensein von Viren und Würmern im Netzwerk. Ob schädlich oder nicht – derartige Verhaltensweisen können die Bereitstellung von Applikationsdiensten negativ beeinflussen. Das erhöhte Paketvolumen im Netzwerk führt dann letztendlich zu einer übermäßigen Belegung der Bandbreite, besonders wenn eine unerlaubte Anwendung stark genutzt wird.

Die Auswertung des Netzwerkverkehrs auf Anomalien ist ein logischer Ausgangspunkt und Teil eines Network Performance Management-Ansatzes. Auf Basis von weiteren Details über die Unregelmäßigkeiten bei den Antwortzeiten und der VoIP-Verbindungsqualität lassen sich die Ursachen der Anomalien und die betroffenen Ressourcen feststellen.

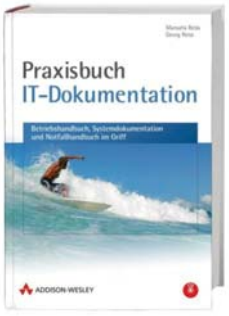
Fazit

Netzwerkfachleute verwenden das Performance-Management, um die Stabilität von Software-Anwendungen für den User am Desktop zu gewährleisten. Die Netzwerkverhaltensanalyse, Network Behaviour Analysis, ist dabei ein wichtiger Bestandteil. Ganz gleich, ob Anomalien im Netzwerkverhalten durch das Benutzerverhalten verursacht werden oder auf externe Angriffe wie etwa auf Hacker zurückzuführen sind: In jedem Fall ist es entscheidend, die möglichen Auswirkungen dieser Anomalien auf die Netzwerkressourcen und die Bereitstellung der Anwendungen zu kennen. Die schnelle Erkennung von Anomalien in Echtzeit ist ein effektives Mittel, um frühzeitig sowohl aus der Sicht des Sicherheitsfachmanns als auch des Netzwerkverantwortlichen gegenzusteuern.

NBA-Lösungen erkennen Anomalien im Netzwerkverkehr, sie liefern jedoch keine umfassenden Informationen. Daher ist es ratsam, Veränderungen im Netzwerk nicht isoliert zu betrachten. Auf Basis von weiteren, über den Host hinausgehenden Details lassen sich die Ursachen von Anomalien finden und frühzeitig beheben, bevor die Performance im Netzwerk beeinträchtigt wird. Ratsam ist es, Lösungen mit einem ausgereiften Network Performance Management-System zu koppeln, um das Verhalten des Netzwerks auch im Kontext mit zusätzlichen Analysen zu betrachten. *(ln)*

Paul O'Reilly ist Director of Sales bei NetQoS.

Praxisbuch IT-Dokumentation



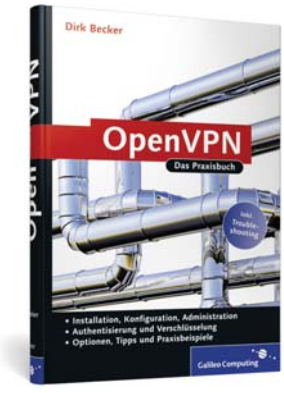
Mittlerweile enthalten zahlreiche gesetzliche Vorgaben mehr oder weniger exakte Anforderungen in puncto Dokumentation. So verwundert es nicht, dass die Autoren von "Praxisbuch IT-Dokumentation" schon auf den ersten Seiten eine Übersicht der gesetzlichen Standards mit Bezug zur IT-Dokumentation auflisten. Ob SOX, MaRISK oder GDPDU, Manuela und Georg Reiss gehen kurz auf Sinn und Zweck der Vorgaben ein und beschreiben, inwiefern Dokumentation etwas damit zu tun hat. Auf den folgenden Seiten stellt der unbedarfte Admin fest, dass Dokumentation nicht einfach nur Visio-Diagramme der Infrastruktur sind. IT-Dokumentation ist ein Fachgebiet für sich, mit eigener Terminologie und eigenen Standards und Nomenklaturen. Die Autoren geben sich reichlich Mühe, die Wichtigkeit der korrekten Begriffe wie "Konzept" und "Richtlinie" zu vermitteln. Das mag manchem haarspalterisch erscheinen, doch gerade wenn externe Stellen Audits durchführen, ist es absolut essenziell, dass sie die richtigen Dokumente mit dem richtigen Titel im richtigen Ordner finden.

Es liegt in der Natur der Sache, dass sich ein Buch über IT-Dokumentation nicht wie ein Thriller liest. Stellenweise geraten die Diskussionen über das Für und Wider der richtigen Notationsarten etwas zäh. Doch im Großen und Ganzen können Einsteiger in das Thema das Buch in einem Sitz durchlesen, ohne sich zu langweilen. Damit entsteht das notwendige Grundverständnis, ohne das keine funktionierende Struktur entwickelt werden kann. Dabei helfen auch die zahlreichen Mind-Map-Diagramme im Text. Ein entsprechender Viewer ist auf der beigelegten CD enthalten. Wer schon tiefer im Thema steckt, findet durch die extrem detaillierte Gliederung der Inhalte schnell die passenden Seiten zum Nachschlagen.

Fazit: Ein fokussiertes Buch mit methodischem Ansatz. In der beschriebenen Detailfülle passt es direkt auf große Unternehmen, Admins kleinerer Firmen müssen sich passende Teilbereiche zurechtschneiden. *Elmar Török*

Autor:	Manuela Reiss, Georg Reiss
Verlag:	Addison-Wesley
Preis:	39,95 Euro
ISBN:	978-3-8273-2681-2
Bewertung:	★★★★☆

OpenVPN



Das OpenVPN-Projekt ist seit Langem etabliert, stabil und für viele Plattformen verfügbar. Nur über eine zu einfache Konfiguration und Verwaltung hat sich vermutlich noch niemand beschwert, OpenVPN erfordert eine intensive Beschäftigung mit der Software und den Konzepten dahinter. Das Buch "OpenVPN" von Dirk Becker will dabei helfen. Auf 200 Seiten geht es um den Praxiseinsatz der VPN-Lösung. Ein relativ schmales Buch hat den Vorteil, dass es nicht von Anfang an durch schiere Größe abschreckt, und so stürzt sich der verschlüsselungswillige Leser vorbehaltlos in die Lektüre. Der Autor macht seine Sache schon auf den ersten Seiten sehr gut und erklärt kurz, woher OpenVPN kommt und was es an Vorgängerversionen und Alternativen gibt. Dann stellt er sein simuliertes Testnetzwerk vor, in dem die späteren Praxisbeispiele ablaufen werden. Der Ton ist kurz und prägnant, Erfahrung im Umgang mit Linux ist Pflicht, Netzwerkkenntnisse sowieso. Umso mehr überrascht es, gleich danach ein Kapitel mit dem Adam und Eva der Netzwerktechnologie zu finden, einschließlich OSI-Modell und, man glaubt es kaum, Bildern von BNC-Steckern und T-Stücken. Das sind zwar nur etwa 40 Seiten, die allerdings hätte sich der Verlag wirklich sparen können.

Danach besinnt sich Becker auf seine Qualitäten und beschreibt die Installation von OpenVPN und OpenSSL unter Linux und Windows. Zertifikate werden kurz erläutert und erzeugt, statische Schlüssel ebenfalls. Auch grafische Benutzeroberflächen stellt der Autor vor, allerdings sind die meisten nur zur Administration und nicht zur Konfiguration zu gebrauchen. Ohnehin rät Becker, in der Lernphase mit Konsole und Konfig-Dateien zu arbeiten. Solcherart vorbereitet, konfiguriert der Leser bald seine ersten VPN-Verbindungen zwischen Clients, Gateways und Netzen. Dieser Teil von "OpenVPN" nimmt den größten Platz ein und ist so praxisgerecht, wie man ihn sich nur wünschen kann. Blutige Anfänger ausgenommen dürfte jeder Admin damit klarkommen und nach kurzer Zeit den grundlegenden Umgang mit OpenVPN beherrschen. Danach gibt es noch ein Kapitel über Plug-ins zur Authentisierung und einige Tipps, unter anderem zum Umgang mit Zertifikaten und den Einsatz der Lösung mit normalen Benutzerrechten.

Fazit: Kurz, knapp und präzise gibt der Autor eine Anleitung für den Umgang mit OpenVPN. Einige Stellen könnten etwas ausführlicher sein, aber insgesamt passen der Detaillevel und die Tiefe der Erklärungen. *Elmar Török*

Autor:	Dirk Becker
Verlag:	Galileo Computing
Preis:	34,90 Euro
ISBN:	978-3-8362-1197-0
Bewertung:	★★★★☆

www.neogrid.de

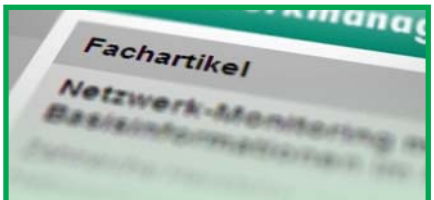
Reise durch die Zeit

Für die gezielte Suche nach Fachbegriffen bietet sich bereits eine Vielzahl an Portalen an, nicht zuletzt die Suchmaschinen selbst. Da müssen die einzelnen Seiten schon einen Mehrwert bieten, um aus der Menge herauszustechen. Diesen Ansatz verfolgt "neogrid.de" getreu dem Motto "Das innovative EDV-Lexikon". Hier wird den Besuchern nicht nur eine intelligent verlinkte Suche nach Fachbegriffen ermöglicht, sie machen auch eine Zeitreise in die Historie der IT – und dürfen zumindest an einem kleinen Ausblick in das Jahr 2015 teilhaben.

Was die Vergangenheit angeht, reicht die IT-Zeitreise auf neogrid.de bis ins Jahr 1646 zurück. Das mag die meisten überraschen, zählen doch 20 Jahre in der heutigen Computer-Branche bereits als historischer Zeitraum. Doch erblickte 1646 immerhin Gottfried-Wilhelm Leibniz das Licht der Welt – der Vater mechanischer Rechenmaschinen, die als Urahnen heutiger PCs und Server gelten. Auch lassen sich auch nur zu bestimmten Kategorien wie etwa Software, Hardware oder Programmiersprachen historische Entwicklungen anzeigen: AMD stieg 1975 in die Produktion von RAM-Bausteinen ein und der Firmenname IBM existiert schon seit dem Jahr 1924. Für Nutzer, die nicht ganz so weit in die Vergangenheit schweifen möchten, lässt sich der gewünschte Zeitraum per Drop-Down-Menü eingrenzen.

Natürlich ist der zeithistorische Ausflug nicht das Einzige, was das Informationsportal zu bieten hat. 28 Oberbegriffe listet neogrid.de auf seiner Startseite auf – darunter Mikrochip, Linux, Sicherheit oder Speichermedium – und bietet zu diesen Schlagwörtern Erläuterungen sowie zahlreiche thematisch verwandte Beiträge. Für eine alphabetische Suche steht zudem das Glossar zur Verfügung. Erst hier wird dem Besucher deutlich, wie viele Einträge zu EDV-Begriffen auf der Seite existieren – 14.289 sind es laut offizieller Zählung des Portals. Allerdings führen einige der Begriffe auch zu anderen, artverwandten Einträgen. Nicht zuletzt erlaubt eine Volltextsuche die Eingabe beliebiger Schlüsselwörter. Dass die Betreiber Nordamerika-Fans zu sein scheinen, beweist die Auswahl an Desktop-Hintergrundbildern. Hier stehen Landschaften aus verschiedenen Nationalparks und Städten der USA zum Download bereit. *(dr)*

Die Seite "neogrid.de" bietet interessante zeitgeschichtliche Fakten zur IT



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 mit den folgenden Links schon jetzt auf die Fachbeiträge zugreifen, noch bevor diese der Öffentlichkeit zur Verfügung stehen. Im Februar erfahren Sie auf unserer Webseite mehr zu diesen Themen:

Effizientes Netzwerkmanagement durch Physical Layer Monitoring

Traditionelles Monitoring ermöglicht dem IT-Verantwortlichen lediglich einen Einblick in die Protokollebene eines Netzwerks und setzt ein einwandfreies Funktionieren der physikalischen Ebene voraus. Doch gerade hier treten im Regelfall besonders viele Fehler auf. Lesen Sie in unserem Fachartikel, welche Vorteile ein Physical Layer Monitoring-System bietet.

www.it-administrator.de/themen/netzwerkmanagement/fachartikel/51750.html

Gezielt einkaufen – Managed Network Services

Immer komplexer werdende Netzwerkstrukturen ziehen einen stets steigenden Verwaltungsaufwand nach sich. Es stellt sich die Frage, ob wirklich jeder Teilbereich der IT-Umgebung im Haus geplant und verwaltet werden muss. Im Online-Beitrag erfahren Sie mehr über Managed Network Services und auf welchen Ebenen gezieltes Outsourcing Sinn macht.

www.it-administrator.de/themen/netzwerkmanagement/fachartikel/51751.html

Anwenderbericht: Wenn der Gabelstapler im WLAN funkt

Gerade in Logistikzentren und bei großen Lagerflächen bietet sich der kabellose Datentransfer an. Clients lassen sich flexibel einsetzen, während Mitarbeiter mit mobilen Telefonen über VoIP unternehmensweit zu erreichen sind. Wie eine solche Infrastruktur samt funkendem Gabelstapler aussehen kann, zeigen wir Ihnen am Beispiel eines Zulieferers für die Automobilindustrie.

www.it-administrator.de/themen/netzwerkausstattung/fachartikel/51752.html

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

»Kürzere Produktzyklen gehen zulasten der Qualität«

Bernhard Josko (55) arbeitet als IT-Ingenieur in einem Team von Administratoren bei der Informationstechnik der Bundesagentur für Arbeit. Das Nürnberger Systemhaus zählt mit über 167.000 vernetzten Arbeitsplätzen zu einer der größten IT-Landschaften in Europa und stellt bundesweit die Abwicklung aller Geschäftsprozesse der Agenturen für Arbeit und der ARGEn (Arbeitsgemeinschaften) sicher.

Welche Ausbildung haben Sie gemacht?

Von Haus aus bin ich gelernter Elektroniker. Durch Eigenengagement und interne Fortbildung kam ich dann zur IT-Administration.

Warum sind Sie IT-Administrator geworden?

Das war eigentlich ein Selbstläufer. Meinerseits bestand ein großes Interesse für die IT und ihre Zusammenhänge.

Welche IT-Umgebung betreuen Sie aktuell?

Ich bin in unserem Unternehmen in einem Team von Administratoren als IT-Ingenieur tätig. Zu unseren Aufgabengebieten gehören die Installation und die Inbetriebnahme von Lösungen sowie die Sicherung und die Überwachung von Exchange. Ich nehme dabei die Rolle des Überwachers ein. Wir arbeiten mit einer Vielzahl unterschiedlicher Server, die unter Windows 2003 und 2008 laufen. Zu unserem "Fuhrpark" gehören zudem Server, die mit verschiedenen Unix-Derivaten laufen. Insgesamt umfasst unsere Infrastruktur 9.200 Server und 167.000 Arbeitsplätze.

Welches Netzwerk- und Systemmanagement ist bei Ihnen im Einsatz?

In unser Netzwerk sind derzeit etwa 20.000 Netzwerkkomponenten integriert, davon rund 17.000 Switches und etwa 3.000 Router. Für die Überwachung und das Systemmanagement nutzen wir integrierte Werkzeuge der Betriebssysteme.

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

Das ist eindeutig die Komplexität des Netzwerks. Auf den Servern laufen in der Regel mehrere Applikationen. Damit die Prozesse im Alltagsbetrieb reibungslos funktionieren, müssen die Server miteinander verzahnt werden.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Neben dem Tagesgeschäft arbeite ich an einem Projekt zur Servicemodellierung.

Geburtstag: 03.01.1954
Familienstand: verheiratet
Hobbys: Technik, Handwerk

Bernhard Josko, IT-Administrator

Das wird mich in den nächsten Wochen in Anspruch nehmen.

Was macht Ihnen an Ihrem Job am meisten Spaß?

Die Vielfalt der Aufgaben, die ein Administrator zu erfüllen hat, macht die Arbeit nie langweilig. Da es sich zudem um eine anspruchsvolle und sehr abwechslungsreiche Tätigkeit handelt, besteht keine Gefahr, in Routinen zu verfallen.

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

Wie bei den meisten Administratoren gehören Reporting und Dokumentationen nicht zu meinen favorisierten Aufgaben.

Was tun Sie für Ihre Fort- und Weiterbildung?

Um auf dem Laufenden zu bleiben, mache ich Kurse bei verschiedenen Anbietern, vorausgesetzt ich habe die Zeit dazu. Weitere Informationen liefern externe Partner, Fachzeitschriften und natürlich das Internet.

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

Der hat nichts mit der IT zu tun. Ich spiele seit Jahren Lotto und noch nie hat's mit einem dicken Gewinn geklappt.

Was war Ihr größter Erfolg als IT-Administrator?

Das ist die Installation eines automatischen Alarmierungssystems (Alarm-Tool) per SMS, E-Mail oder Tickets (UHD), die unser Team gestemmt hat. Die besondere Herausforderung bestand darin, dass ein Alarm im Störungsfall von außen, beispielsweise aus den Agenturen für Arbeit, zur zuständigen Stelle innerhalb der BA-Informationstechnik gelangt.

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

Richtig dumme Anwender gibt es nicht. Anwender kennen sich meist mit der IT einfach nicht so gut aus. Ein Zwischenfall fällt mir aber doch ein: So hat ein Mitarbeiter den Stromverteilerschrank direkt hinter einer Tür platziert, und zwar genau so, dass der Türknauf stets die Not-Aus-Taste betätigte.

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

Die Kurzlebigkeit der Software und der Hardwareprodukte halte ich für eine große Herausforderung. Versionen ändern sich sehr schnell, Lebenszyklen werden kürzer. In diesem Zusammenhang befürchte ich für die nächsten Jahre leider auch einen Qualitätsverlust, den wir Administratoren wieder auffangen müssen.

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 3/09 erscheint am 2. März 2009

Schwerpunktthema:

Netzwerkmanagement und -inventarisierung

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

Im **April** ist unser Schwerpunkt **E-Mailmanagement** mit Workshops und Fachartikeln, unter anderem einem Test des neuen Kerio Mailservers, einem Workshop zur Administration von Zarafa, allen Neuheiten der Microsoft Windows Small und Essential Business Server 2008 sowie einer Anleitung zur richtigen Dokumentation eines E-Mailservers.

Als Schwerpunkt im Monat **Mai** folgt das Thema **Virtualisierung und Server-based Computing**.

Im Test: Citrix XenApp 5.0

Workshop: Sun ZFS durchleuchtet

Workshop: Performance-Monitoring mit Hyperic HQ

Workshop: Server-Tools für den Admin

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

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

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

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

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

Autoren dieser Ausgabe
Petra Adamik, Jürgen Heyer, Thomas Joos, Paul O'Reilly, Robert Lindermeier, Nico Lüdemann, Dr. Michael Schwartzkopff, Elmar Török, Thomas Weyergraf

Anzeigen
Anne Kathrin Heinemann, *Anzeigenleitung*
verantwortlich für den Anzeigenteil
kathrin@it-administrator.de
Tel.: 089/4445408-20
Es gilt die Anzeigenpreisliste Nr. 6 vom 01.01.2009

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

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

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

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

Erscheinungsweise
monatlich

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

(Studentenabonnements nur gegen Vorlage einer gültigen Immatrikulationsbescheinigung)

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

Internet
www.it-administrator.de

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
80802 München

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

(zugleich Anschrift aller Verantwortlichen)

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

Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

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

ISSN
1614-2888

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

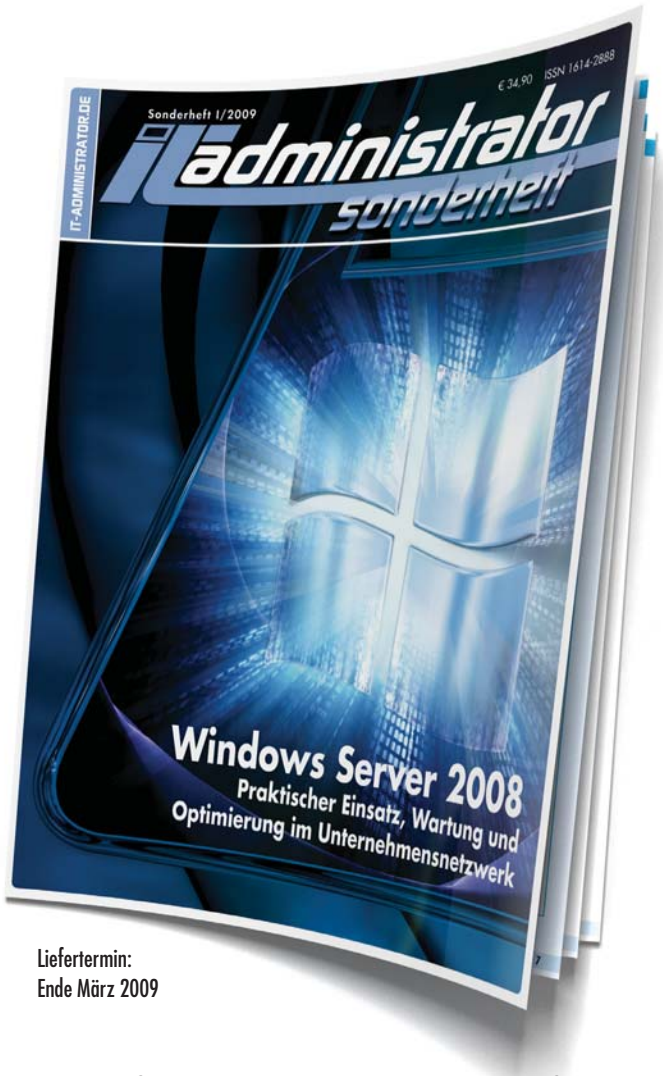
Bankverbindung für Abonnenten
Konto 174 966 462 bei der
Postbank Dortmund, BLZ 440 100 46
Kontoinhaber: Vertriebsunion Meynen

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

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

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

INSERENTENVERZEICHNIS



Liefertermin:
Ende März 2009

Bestellen Sie jetzt

das IT-Administrator

Sonderheft I/2009!

140 Seiten Praxis-Know-how
rund um den

Windows Server 2008

zum Abonnenten-Vorzugspreis* von

nur € 29,90!

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

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

administrator
Das Magazin für professionelle System- und Netzwerkadministration

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

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

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

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

Ich zahle ☐ per Bankeinzug

Geldinstitut:

Kto.: BLZ:

oder ☐ per Rechnung

Datum:

Unterschrift:

Firma:

Name, Vorname:

Straße:

Land, PLZ, Ort:

Tel:

E-Mail:

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

ITA 0209

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

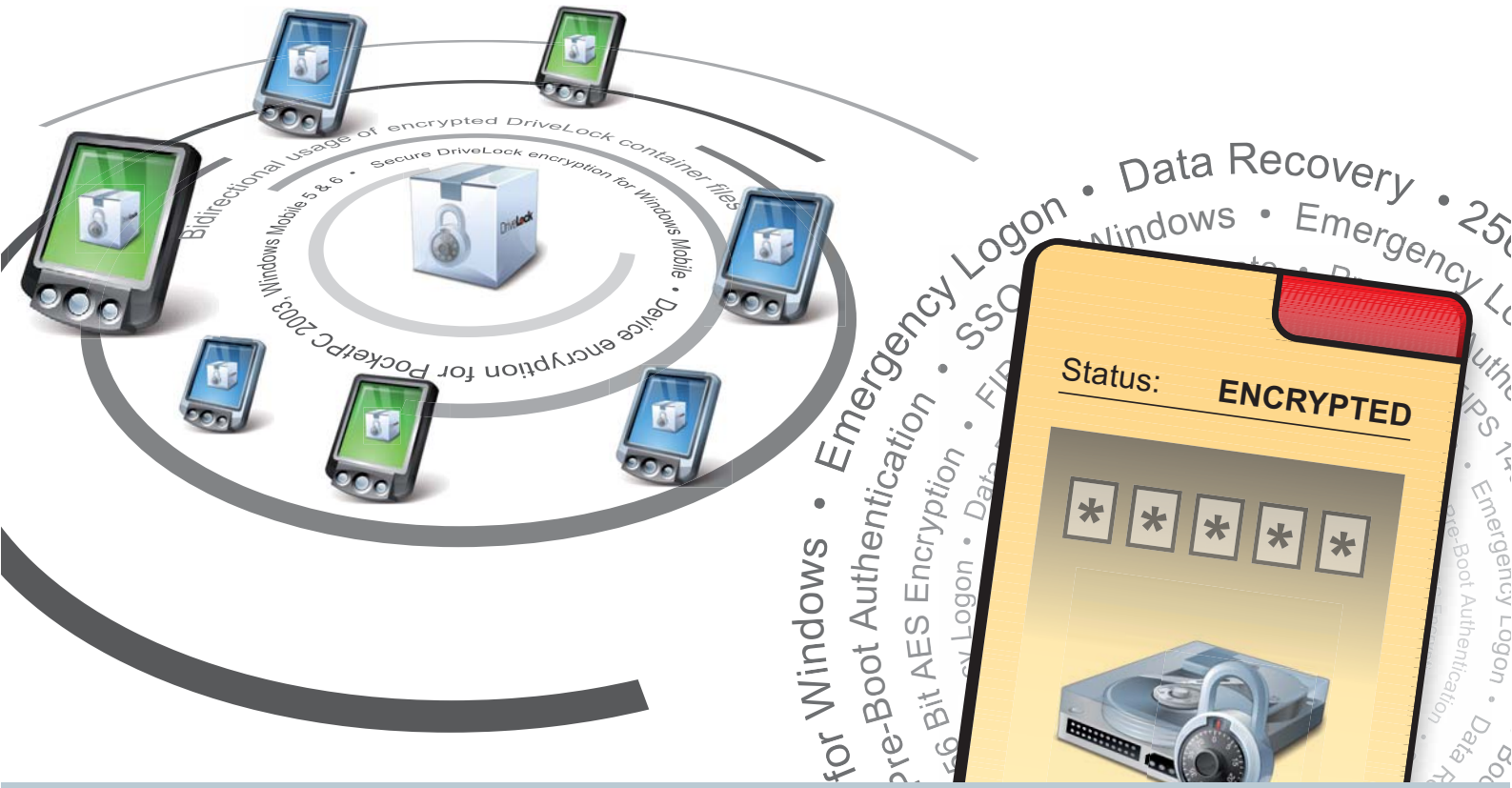
Heinemann Verlag
Leopoldstraße 85
D-80802 München
Tel: 089-4445408-0
Fax: 089-4445408-99
Geschäftsführung:
Anne Kathrin Heinemann
Matthias Heinemann
Amtsgericht München HRB 151585

DriveLock 5.5

Intelligente Kontrolle mobiler Geräte

» Daten. Sicherheit. Im Netzwerk. Unterwegs.

DriveLock 5.5



SICHERHEIT WIRD JETZT MOBIL. ODER ANDERS GESAGT: AUCH MOBILES WIRD SICHER. UND DRIVELOCK 5.5 SETZT HIER GANZ NEUE MASSSTÄBE:

- » VERSCHLÜSSELUNG FÜR WINDOWS MOBILE
- » ECHTE FULL DISK ENCRYPTION MIT SSO
- » VERBESSERTES UND INTUITIVES REPORTING
- » DEVICESCANNER FÜR DEN NETZWERK-SCAN

DriveLock bietet volle Datensicherheit bei USB-, WIFI- und anderen Geräten sowie vielen weiteren Applikationen für PCs im Netzwerk. Durch intelligente Anpassungen, Weiterentwicklungen und sinnvollen Add-ons wurde **DriveLock** inzwischen zum optimalen Rundum-Schutz für Netzwerke und sensible Firmendaten. Ein perfektes Praxis-Tool von CenterTools. Empfohlen und getestet von Fachblättern und erfolgreich eingesetzt bei vielen großen und kleinen Unternehmen Europas und Nordamerikas.

Aktuelle Referenzen, weitere Informationen und die aktuelle Testversion gibt es auf **www.drivelock.de**

Testen Sie das neue DriveLock. JETZT!

CenterTools