

# **i**Administrator

Das Magazin für professionelle System- und Netzwerkadministration

**Im Test:  
Vizioncore  
vFoglight Pro 6.0** 10

**Im Test:  
Kaviza VDI-in-a-Box** 16

**Systeme:  
Möglichkeiten von  
Virtual Desktop Infrastructures** 26

**Workshop:  
VMware ESX4 über die  
Kommandozeile verwalten** 30

**Know-how:  
Datenverluste in virtuellen  
Umgebungen vermeiden** 61

## Management virtueller Infrastrukturen



# Markenserver gibt's jetzt billiger!

[www.notebooksbilliger.de/server](http://www.notebooksbilliger.de/server)

**50 €  
Gutschein\***



Gutscheincode: itmktka

**Für Ihr individuelles Angebot und Ihren Gutschein  
erreichen Sie unser Consultingteam unter  
0331 73099 034**



\* Sichern Sie sich jetzt unser Sparangebot! Erstbesteller erhalten beim Kauf eines Servers einen Warengutschein im Wert von 50 Euro! Eine Barauszahlung ist nicht möglich. Gutschein kann nur telefonisch eingelöst werden. Angebot gilt solange der Vorrat reicht.

## Löwenbändiger gesucht

Liebe Leser,

die Hauptattraktion vieler Zirkusaufführungen ist zweifellos die Löwendressur. Majestätisch dirigiert der Dompteur den Tanz der Löwen mit kurzen Kommandos und seiner Peitsche. Als Ergebnis jahrelangen Trainings bewegt sich der König der Tiere wie an einem unsichtbaren Band geführt nach dem Willen des Dompteurs. Nun stellen wir uns einmal vor, die Löwen wären virtualisiert. Zunächst wüsste der Dompteur nicht mehr, wo sich seine Löwen gerade in der Manege aufhalten. Und wie viele es gerade sind, könnte der tapfere Mann nur erahnen. Zudem hätte er keine Peitsche. Diese Show wäre sicher auf eine ganz spezielle Art nervenaufreibend. Und Sie ahnen es sicher schon: Es gibt Parallelen zwischen unserem Dompteur und einem Systemadministrator.



Früher hockte jeder Server brav auf seinem Blech wie die Löwen in der Manege auf ihren Plätzen. Heute sind die Server in vielen Unternehmen virtualisiert und die Situation ähnelt oft unserer Metapher von oben. So erkennen auch immer mehr IT-Verantwortliche mit steigender Anzahl virtualisierter Server die Notwendigkeit einer guten Peitsche – passender Managementwerkzeuge. Dass sich mit diesen Tools nicht nur die alte Beherrschbarkeit wieder etablieren lässt, sondern die Vorteile der Virtualisierung so richtig zum Tragen kommen, diese Erkenntnis sickert allerdings nur sehr langsam ein. So gaben in einer Umfrage im Auftrag von CA 74 Prozent von 550 befragten IT-Verantwortlichen in Deutschland an, dass sie entweder gerade virtualisieren oder dies vorhaben. Nur 20 Prozent arbeiten jedoch mit einer automatischen Provisionierung, noch weniger, nämlich 14 Prozent, deprovisionieren automatisch. Im Ergebnis kommt diese Studie zu der Aussage, dass Unternehmen die Virtualisierung zwar bereits zur Kostensenkung in den Rechenzentren nutzen, allerdings wissen sie nach eigener Aussage oft nicht, wie sich virtualisierte Umgebungen automatisieren, verwalten und sichern lassen. Daher sind Unternehmen im Moment noch nicht in der Lage, die weit über Kostenersparnis und Serverkonsolidierung hinausgehenden Vorteile der Virtualisierung voll zu nutzen.

Unser Schwerpunkt im August zeigt diese Vorteile auf. Im Test bewiesen vFoglight (Seite 10) und das Virtualisierungsmodul für Ipswitch WhatsUp Gold (Seite 21), dass sich eine virtualisierte Infrastruktur heute genauso gut beherrschen lässt wie eine physikalische. Und als Schmankehl zeigen wir Ihnen eine der vielen neuen Möglichkeiten, die die Virtualisierung bietet, indem wir ab Seite 49 Notebooks für den Außendienst absichern. Viel Vergnügen beim Dressieren und Lesen, Ihr

John Pardey  
Chefredakteur

# NEU!

# V-locity™ 2

FÜR VMWARE UND HYPER-V

## Der einzige Weg zu maximaler I/O-Leistung auf virtuellen Servern

V-locity™ 2, der neue Disk Optimizer für virtuelle Umgebungen, überwindet die Barrieren zu maximaler Systemgeschwindigkeit und Effizienz. Seine leistungsstarke neue Technologie koordiniert die Optimierung von VMs ohne Ressourcenkonflikte.

### Nur V-locity 2 bringt Ihnen diese Vorteile

- Höchste Server-Geschwindigkeit und Verlässlichkeit auf jedem virtuellen OS.
- Längere Server-Betriebszeit.
- Maximale Effizienz des freien Speichers, wenn die Festplatte auf dynamisches Wachstum ausgelegt ist.
- Hervorragende Optimierungskompatibilität mit der Copy-on-Write-Technologie.
- Schnellere Leistung für Nutzer von Linked Clones/ Differencing Disks.

### Exklusive Features von V-locity 2

- IntelliWrite™, die Technologie zur Verhinderung von Fragmentierung. Verhindert die meiste Fragmentierung, bevor diese entsteht.
- InvisiTasking® Technology – koordiniert die Nutzung virtueller Ressourcen ohne Konflikte, 100 % im Hintergrund.
- Virtuelle Festplatten-Intelligenz – erkennt und konfiguriert automatisch Festplattentypen (z. B. Differencing Disks und Linked Clones) für verbesserte Optimierungsroutinen.
- Virtuelle Festplatten-Komprimierung – verkleinert virtuelle Festplatten, die freien Platz vergeuden würden.

Testen Sie V-locity gratis für 30 Tage: [diskeeper.com/v2](http://diskeeper.com/v2)

Oder fragen Sie telefonisch nach einem Preisangebot: +44 (0)1293 763406

© 2010 Diskeeper Corporation. Alle Rechte vorbehalten. Diskeeper, das Diskeeper-Logo, V-locity, das V-locity-Logo, IntelliWrite, InvisiTasking und das Diskeeper Corporation-Logo sind in den USA und/oder in anderen Ländern eingetragene Marken bzw. Marken, die im Eigentum der Diskeeper Corporation stehen. Alle anderen Marken und Markennamen stehen im Eigentum ihrer jeweiligen Inhaber.



# INHALT

IT-Administrator – Ausgabe August 2010

## Management virtueller Infrastrukturen

### Im Test: WhatsVirtual 1.0 für Ipswitch WhatsUp Gold



Mit über 70.000 verwalteten Netzwerken ist die Management-Software "WhatsUp Gold" weit verbreitet. Neu ist nun das Plug-In "WhatsVirtual" für den Zugriff auf virtuelle Serverumgebungen unter VMware. Ziel ist ein integriertes Monitoring und Management physischer und virtueller Systeme von einer Konsole aus. IT-Administrator hat untersucht, wie gut das mit dieser Erweiterung möglich ist, die der Hersteller bestehenden Nutzern zu recht geringen Update-Kosten anbietet.

Seite 21

### Linux-Systeme mit Spacewalk verwalten

Linux-Systeme von Hand zu verwalten, ist ab einer bestimmten Größe der Systemlandschaft zeitaufwendig und meist nicht sonderlich praktikabel. Mit dem Projekt Spacewalk entstand eine Open Source-Lösung, mit der sich Linux-Systeme an zentraler Stelle aus verwalten lassen. IT-Administrator stellt Ihnen das Programm vor und zeigt, welche Möglichkeiten es zur Software- und Patchverteilung bietet.



Seite 53



Server- und Systemmanagement



Clientmanagement



Storage



Sicherheit



Messaging

### Themenübersicht



Virtualisierung



Netzwerkmanagement



Job/Weiterbildung







Recht

### AKTUELL

- 06 News
- 09 **ITANet aktuell:** IT-Administrator-Workshop "Windows 7" am 21. September 2010 in Karlsruhe – Zugabe


### PRODUKTE

- 10  **Im Test:** Vizioncore vFoglight Pro 6.0  
Licht im virtuellen Nebel
- 16  **Im Test:** Kaviza VDI-in-a-Box  
Virtuelle Desktops aus der Dose
- 21  **Im Test:** WhatsVirtual 1.0 für Ipswitch WhatsUp Gold  
Virtuelles Management-Schnäppchen
- 25  **Im Kurzttest:** CoGen eBoostr 4.0  
Nachrüstbarer Turbolader

### PRAXIS

- 26  **Systeme:** Möglichkeiten von Virtual Desktop Infrastructures  
Nicht ohne mein Clientmanagement!
- 30  **Workshop:** VMware ESX4 über die Kommandozeile verwalten  
Steuerung per Tastendruck
- 35  **Workshopserie:** Logdaten mit Splunk auswerten und verwalten (1)  
Gesucht, gefunden
- 38  **Systeme:** Citrix XenClient Express für mobile Geräte  
Virtuell unterwegs
- 41  **Workshopserie:** Desktop-Management mit dem Microsoft Desktop  
Optimization Pack (3) – Letzte Rettung beim Systemabsturz
- 46  **Workshopserie:** Migration auf SharePoint 2010 (2)  
Umzug leicht gemacht
- 49  **Workshop:** Sichere Notebooks für den Innen- und Außendienst  
Reiseschutzversicherung
- 53  **Workshopserie:** Linux-Systeme mit Spacewalk verwalten (1)  
In den Weiten von Linux
- 57  **Workshop:** Laufwerke und NTFS-Rechte mit PowerShell 2.0 bearbeiten  
Die Platte in Griff
- 58 **Tipps, Tricks & Tools**

### WISSEN

- 61  **Know-how:** Datenrettung in virtuellen Umgebungen  
Reale Rettung virtueller Daten
- 63 **Buchbesprechung**  
"Unified Communication" und "Microsoft Exchange Server 2010"
- 64 **Website & Fachartikel online**

### RUBRIKEN

- 03 Editorial
- 05 Inhalt
- 23 Stellenmarkt
- 43 Seminarmarkt
- 65 Das letzte Wort
- 66 Vorschau, Impressum, Inserentenverzeichnis

## Vereinfachter Kampf gegen Datenlecks

**Blue Coat Systems** stellt seine neuen integrierten **Data-Loss-Prevention-Appliances** (DLP) vor. Die Geräte sollen Unternehmen umfassend und unkompliziert vor dem Verlust sensibler Daten schützen, die über das Netzwerk laufen. Besonderes Augenmerk hat der Hersteller nach eigenen Angaben auf die leichte Implementierbarkeit der Appliances gelegt. So soll innerhalb weniger Tage die Installation und Konfiguration, die Definition von Richtlinien, das Fingerprinting von Inhalten, die erste Überwachung und Kontrolle von Datenverkehr sowie Analyse von Vorfällen möglich sein. Über 600 unterschiedliche Dokumententypen werden dabei unterstützt. Die DLP-Appliances lassen sich über das Internet Content Adaption Protocol (ICAP) zudem mit Blue Coat Proxy-SG-Appliances verbinden. In diesem Fall ermöglicht es eine ProxySG-Apliance einer DLP-Apliance, auch SSL-verschlüsselten Verkehr wie Webmails zu inspizieren. Gleichzeitig kann sie dann als der Punkt agieren, an dem sensible Informationen blockiert, weitergeleitet oder verschlüsselt werden. ProxySG-Appliances können zudem umfassende Authentifizierungsdaten an DLP-Appliances weitergeben, so dass sich dort Richtlinien auch auf Benutzerbasis durchsetzen lassen. Die neuen DLP-Appliances sind in drei Modellen für 250, 5.000 oder 20.000 Benutzer verfügbar. Die Preise beginnen bei 12.000 Euro. (dr)

Blue Coat: [www.bluecoat.de/products/dlp/](http://www.bluecoat.de/products/dlp/)



Die DLP-Appliances von Blue Coat sollen sich besonders einfach im Netzwerk implementieren lassen

## Mehr Power für den E-Mailschutz

**SonicWALL** kündigt die beiden **E-Mail-security-Appliances ESA 3300** und **ESA 4300** an. Die Geräte verfügen über leistungsstärkere Prozessoren, erweiterten Speicher (2 GByte, 4 GByte) sowie eine optimierte RAID-Leistung (in der ESA 4300). Beide Geräte unterstützen dabei Flash-Speicher, der gewährleistet, dass im Falle eines Systemausfalls die Konfigurationsdateien vollständig wiederhergestellt werden können (SAFE-Modus). Die ESA 4300 bietet dank der zwei zusätzlichen Laufwerke die Möglichkeit, weitere Festplatten einzusetzen und damit die Speicherkapazitäten bei Bedarf zu erhöhen. Die ebenfalls verfügbare Email Security Virtual Appliance für virtualisierte Infrastrukturen beinhaltet die Firmware ES 7.2.2, die bereits Anfang des Jahres angekündigt wurde. Unternehmen haben damit laut Hersteller die Möglichkeit, ihre virtualisierten Umgebun-

gen frei zu skalieren und effizient zu verwalten. Für den E-Mailschutz erhalten alle Appliances nahezu in Echtzeit Informationen und Signatur-Updates aus dem SonicWALL GRID Network, um eine verbesserte Sicherheit zu gewährleisten. Weltweit sammelt und analysiert SonicWALL hierbei Millionen von Datenpunkten und untersucht zudem stets die Reputation des E-Mail-Absenders, der Inhalte, der Strukturen, Links, Bilder oder Anhänge. Die Preise für das Modell ESA 3300 beginnen bei 1.850 US-Dollar. Die Variante ESA 4300 ist ab 7.200 Dollar zu haben. (dr)

SonicWALL: [www.sonicwall.com/de](http://www.sonicwall.com/de)



Die SonicWALL-Appliances ESA 3300 und 4300 bieten mehr Rechenleistung und Arbeitsspeicher

## Zwei Wege zum Storage

**ALLNET** erweitert seine Produktpalette an **NAS-Netzwerkspeichern** um ein weiteres Modell für den professionellen Einsatz. Der **ALL60600 NAS** unterstützt neben dem NAS- auch den DAS-Modus (Direct Attached Storage) und lässt sich so direkt über den USB-Anschluss an einen PC anbinden. Das NAS-Gerät wird von einem 1,86 GHz schnellen Intel Celeron M-Prozessor angetrieben und verfügt über einen Systemspeicher von einem GByte. Neben zwei GBit-Netzwerkports mit Lastausgleich, Ausfallsicherung und 802.3ad-Linkaggregation verfügt das Gerät zusätzlich über vier Type A-USB-Ports und einen Type B-Port sowie über eine RS232-Schnittstelle zum Anschluss an eine USV zur Sicherstellung eines korrekten Shutdowns bei Stromausfall. Insgesamt erreicht der Netzwerkspeicher mit fünf internen SATA Festplatten eine Gesamtspeicherkapazität von bis zu 10 TByte (bestückt mit

fünf 2 TByte-Festplatten). Die in die Laufwerksschächte eingebauten Festplatten können als RAID 0, 1, 5, 6, 10 oder JBOD-System konfiguriert werden. Für rund 560 Euro ist der NAS-Server ab sofort erhältlich. (dr)

ALLNET: [www.allnet.de](http://www.allnet.de)



Das ALL60600 NAS lässt sich direkt sowie übers Netzwerk anschließen

## Datenschleuse in Netzwerk

**WatchGuard Technologies** erweitert seine Produktpalette um die **VPN-Appliance SSL 560**. Die neue Appliance richtet sich besonders an große Organisationen, in denen bis zu 500 verteilte und mobile Benutzer gleichzeitig auf das Firmennetz zugreifen. Dabei können die Nutzer über SSH und RDP auf ihre Desktops zugreifen. Dank einer einfachen Installation lässt sich die Appliance ohne besondere Fachkenntnisse aufsetzen und betreiben. Wizards führen den Benutzer dabei durch den Installationsprozess. Im Betrieb ist es grundsätzlich nicht erforderlich, die Appliance in andere Authentifizierungssysteme wie LDAP, Active Directory oder RADIUS zu integrieren. Das Gerät generiert vielmehr für mobile Endgeräte wie Firmen-Handys, Smart Phones oder PDAs Token und Einmalpasswörter auf SMS-Basis. Dennoch ar-

beitet die Appliance auch mit bereits bestehenden Authentifizierungssystemen wie LDAP, Active Directory oder RADIUS zusammen. Zudem ermöglicht das Gerät eine Überprüfung der Endgeräte inklusive Integritäts-Checks. Diese sollen laut Hersteller garantieren, dass alle angeschlossenen Endgeräte durch Firewalls geschützt sind und eine aktuelle Antiviren-Software läuft. Hierfür steht ein web-basierter Zugriffsklient zum Download zur Verfügung, so dass keine Vorinstallation von Clientsoftware nötig ist. Die Appliance bietet darüber hinaus auch erweiterten Access Client-Support für Microsoft XP, Vista und Windows 7 sowie einen Client-losen Modus. Für rund 9.100 Euro ist die Appliance erhältlich. (dr)

**WatchGuard:**

[www.watchguard.com/products/watchguard-ssl/overview.asp](http://www.watchguard.com/products/watchguard-ssl/overview.asp)



Bis zu 500 Nutzer können gleichzeitig über die VPN-Appliance SSL 560 von WatchGuard auf ihre Desktops zugreifen

## Kostenlos auf die TechEd 2010

Zur anstehenden **Microsoft TechEd 2010** in Berlin verlost IT-Administrator zwei **Karten im Wert von jeweils 1.895 Euro** (bei der Registrierung bis zum 31. August gilt ein um 200 Euro ermäßigter Preis). Vom 8. bis 12. November

erfahren Sie in 17 technischen Tracks das Neueste unter anderem zu Application-Server und Infrastructure, Cloud Computing, Virtualisierung, Windows, Office und SharePoint oder auch Sicherheit und Identity Management. Referenten sind erfahrene Microsoft-Experten, die Ihnen technische Tricks aufzeigen und einen Ausblick auf die künftigen Entwicklungen bei Microsoft geben. Um an der Verlosung teilzunehmen, senden Sie eine E-Mail bis zum 20. August an "redaktion@it-administrator.de" mit dem Betreff "TechEd 2010". Nutzen Sie die Gelegenheit und besuchen Sie die Expertenkonferenz kostenlos. (dr)

<http://europe.mstched.com/>



Gewinnen Sie zwei Freikarten zur TechEd 2010 in Berlin

## +++TICKER+++TICKER+++TICKER+++

**it-novum** stellt das Systemmanagement-Framework **IT-Cockpit** als **openITCockpit** unter GPLv2-Lizenz zur Verfügung. Das Framework basiert auf Nagios und ist modular erweiterbar. openITCockpit soll Nagios um einige Mehrwerte erweitern: Es lässt sich durch eine Web-Oberfläche konfigurieren, ist mandantenfähig und bietet vorintegrierte Open Source-Tools. openITCockpit unterstützt daneben Geschäftsprozesse durch applikationsübergreifende Integrationen in Ticketing-, CMDB- und Provisioning-Systeme. (dr)

[www.open-itcockpit.com](http://www.open-itcockpit.com)

**Trend Micro** präsentiert **Version 8.0** der **InterScan Messaging Security Virtual Appliance (IMSVA)**. Konzipiert als Hybrid-Lösung für gehostete E-Mailsicherheit integriert das Angebot In-the-cloud-Sicherheitstechnologien mit Security as a Service-Angeboten in einer VMware-kompatiblen virtuellen Appliance. Damit sollen sich bereits 90 Prozent der Spam-Nachrichten vor Eintreffen im lokalen Netz aussortieren lassen. Die Quarantäne von Nachrichten findet jedoch vor Ort statt, sodass Nutzer die Kontrolle über ihre E-Mails in jedem Fall behalten. Bei 100 Benutzern kostet der Dienst rund 31 Euro pro User. (dr)

[www.trendmicro.de](http://www.trendmicro.de)

**Infotrend** bringt das **SAS-Storage-Modell ESVA F60** auf den Markt. Das Gerät verfügt je nach Ausführung über vier beziehungsweise acht 8 GBit/s-FC-Anschlüsse und unterstützt 16 SAS-Platten mit einer Durchsatzrate von 6 GBit/s. Zusätzlich arbeitet das Speichersystem mit drei Höheneinheiten auch mit Solid State Disks (SSDs). Eine F60-Installation mit 16 6 GBit/s SSD-Festplatten kommt auf einen Einstiegspreis von insgesamt 41.425 US-Dollar. (dr)

[www.infotrend.com](http://www.infotrend.com)

**F-Secure** bietet seine mobile Sicherheitslösung **F-Secure Mobile Security 6** nun auch für Android-basierte Handys an. Die Suite soll vor bösartigen Apps und Webseiten schützen. Die zentrale Funktion hierfür ist die "Browsing Protection". Sie identifiziert Cloud-basiert, welche Internetpräsenzen sicher sind und blockiert laut Hersteller unsichere Webseiten. Zudem bietet die Software Anti-Virus, Firewall und Anti-Spyware. Für knapp 40 Euro ist das Schutzschild für Smartphones erhältlich. (dr)

[www.f-secure.de](http://www.f-secure.de)

### Kleine PCs mit großen Chips

CONCEPT International bietet zwei lüfterlose Mini-PCs an. Herzstück der Modelle miniPC 316i und 319i ist NVIDIAs hochperformanter ION-Grafikchip, der auch eine ruckelfreie Darstellung von Full-HD Inhalten gewährleistet. Verbunden mit Intels 1,6 GHz ATOM Prozessor, der keinen Lüfter benötigt, beziehungsweise Intels Doppelkernprozessor mit 1,9 GHz (miniPC 319i), eignen sie sich laut Hersteller besonders für den Einsatz im Digital Signage-Umfeld. Dank der Verwendung von Flash-ROMs oder SSDs als Speichermedium befinden sich zudem keine beweglichen Teile in den miniPCs, was einen wartungsfreien und langlebigen Betrieb gewährleisten soll. Für eine maximale Bildschirmauflösung von 2.560 x 1.600 Bildpunkten hat der Hersteller digitale DVI- und HDMI-Monitoranschlüsse verbaut. Daneben verfügen die Geräte über vier USB 2.0- sowie einen seriellen Port. Zur Kommunikation in Netzwerken stehen außerdem ein GBit-Ethernet-Anschluss und wahlweise ein 802.11a/b/g WLAN- oder UMTS-Modul zur Verfügung. Als Betriebssysteme kommen Windows XP Professional, Windows 7 und Windows embedded zum Einsatz. Der miniPC 316i mit 1,6 GHz Intel ATOM (N270) Prozessor, 2 GByte Arbeits- und 32 GByte SSD Flash-Speicher sowie Windows XP Professional-Lizenz ist für 595 Euro zu haben. (dr)

CONCEPT: [www.concept.biz/de/minipcs.html](http://www.concept.biz/de/minipcs.html)



Die miniPCs von CONCEPT arbeiten lüfterlos und beinhalten einen NVIDIA-Grafikchip

### Desktopverteilung mit Red Hat

Red Hat ergänzt mit Enterprise Virtualization (RHEV) 2.2 sein Portfolio für die Server- und Desktop-Virtualisierung. Die neue Version kann virtuelle Maschinen sowohl unter Windows als auch Linux hosten und verwalten. Die mit Version 2.2 eingeführte Red Hat Enterprise Virtualization für Desktops ermöglicht es dabei, Virtual Desktop Infrastrukturen (VDI) aufzubauen. Hierfür steht ein webbasierter Connection Broker zur Verfügung, mit dem die Benutzer Zugang zu ihren gehosteten, virtuellen Desktops erhalten. Auch Features wie Templating, Thin Provisioning und Desktop-Pooling sind dabei möglich. Mit dem Release 2.2 stellt RHEV eine hohe Skalierbarkeit zur Verfügung und kann Gast-Systeme mit bis

zu 16 virtuellen CPUs und 256 GByte Speicher pro virtueller Maschine unterstützen. Das Release bietet zusätzlich neue Konvertierungs-Fähigkeiten für virtuelle Maschinen mit einem V2V-Tool, das eine automatisierte Konvertierung von virtuellen Maschinen unter VMware oder Xen für den Einsatz unter RHEV erlaubt. Zur weiteren Vereinfachung der Verlagerung von Images virtueller Maschinen zwischen verschiedenen Umgebungen werden der Import und Export von Images und Templates im Open Virtualization Format (OVF) unterstützt. Ab sofort ist das Release 2.2 verfügbar. Die Preise für das RHEV Server Starter Kit beginnen bei rund 3.000 US-Dollar. (dr)

Red Hat: [www.de.redhat.com/virtualization/rhev/server/](http://www.de.redhat.com/virtualization/rhev/server/)

### Netzwerkschutz mit Rollenverteilung

Astaro veröffentlicht das Astaro Security Gateway in Version 8. Die UTM-Lösung ist als Appliance oder Software erhältlich und richtet sich sowohl an kleine und mittelständische als auch große Unternehmen. Unternehmen können mit dem Security Gateway die Netzwerkaktivitäten von Mitarbeitern nachvollziehen, die in entfernten Niederlassungen sitzen, sowie den Internet Traffic von ausgewählten Ländern blockieren. Das Security Gateway verfügt mit Version 8 nun über eine neue Benutzeroberfläche, die die Aufgabenverwaltung erleichtern soll. So zeigt eine neue Suchfunktion beispielsweise alle mit der Abfrage des Administrators verwandten Menüpunkte automatisch an. Über eine Multi-Role Administration lassen sich außerdem Zugriffsrechte für verschiedene Administratoren festlegen, während das Configuration Change Auditing folgerichtig aufzeigt, wer welche Konfigurationsänderungen vorgenommen hat. Das Security Gateway ermöglicht daneben die Migration zur IPv6-Adressierung und zeigt Status und Aktivitätshistorie von Remote-Mitarbeitern über die Funktion "VPN Activity

Reporting". Ab sofort ist Version 8 auf dem Markt verfügbar, die Preise für die Software liegen für 100 Nutzer im "Full Guard"-Bundle bei 3.450 Euro. Für bestehende Astaro-Kunden ist das Upgrade auf Version 8 kostenfrei. (dr)

Astaro: [www.astaro.com/de-de/produkte/astaro-security-gateway-software-appliance](http://www.astaro.com/de-de/produkte/astaro-security-gateway-software-appliance)



Das Astaro Security Gateway 8 ist als Soft- und Hardware verfügbar

# IT-Administrator-Workshop "Windows 7" am 21. September 2010 in Karlsruhe

## Zugabe

ITANet Workshop-Partner:  
**matrix42**

von John Pardey

Die überwältigende Nachfrage nach unserem August-Workshop zu Windows 7 hat uns veranlasst, zu diesem für unsere Leser sehr wichtigen Thema einen zusätzlichen Termin anzubieten. Diesmal findet der Workshop, der sich intensiv mit den Herausforderungen und Aufgaben der Migration zu Windows 7 beschäftigt, am 21. September in Karlsruhe statt.

**D**ie Umstellung auf Windows 7 wird von den IT-Verantwortlichen in den Unternehmen aus verschiedenen Gründen ins Auge gefasst. Auf der einen Seite bietet der neue Microsoft-Client im Zusammenspiel mit dem Server 2008 R2 eine ganze Reihe von Features, die die Produktivität und Effizienz der IT steigern können, andererseits ist das "Auslassen" dieser Client-Generation vor dem Hintergrund des auslaufenden XP-Supports für viele Unternehmen keine Option.

Letztendlich sind die Gründe für einen Umstieg nicht von Belang, wenn es für die IT-Verantwortlichen und Administratoren darum geht, die Migration zu planen und durchzuführen, warten auf alle die gleichen Aufgaben und Herausforderungen. Unser Workshop soll helfen, die Klippen dieses Projektes zu umschiffen und Migration und Rollout möglichst reibungslos abzuwickeln.

### Migration bedarf genauer Planung

Vor der tatsächlichen Umstellung der Endanwender auf Windows 7 steht natürlich eine gründliche Vorbereitung und Planung. Doch auch wenn sich schon jetzt herauskristallisiert hat, dass Windows 7 deutlich einfacher zu handhaben ist als sein wenig geliebter Vorgänger Vista, wis-


sen die Dozenten unseres Workshops doch von einigen Hürden auf dem Weg zum Windows 7-Netzwerk zu berichten.

So müssen sich die IT-Abteilungen Aufgaben wie etwa der Profilmigration stellen. Auch eine genaue Untersuchung der Applikationen auf ihre Windows 7-Tauglichkeit ist unumgänglich und verbunden mit der Frage, wie mit nicht-kompatiblen Anwendungen verfahren wird. Hier bietet die Virtualisierung einige mögliche Vorgehensweisen, aber auch eine Strategie mit einem Windows XP/7-Parallelbetrieb ist denkbar. Und da kein direktes Upgrade auf Windows 7 von XP möglich ist, stellt sich zudem die Frage, wie die Benutzerprofile zu migrieren sind – zu allen diesen Themen geben unsere Workshopexperten den Teilnehmern wertvolle Tipps und Hinweise zu bewährten Vorgehensweisen.

### Der Rollout von Windows 7

Sind die Planungen abgeschlossen und alle Kompatibilitätsfragen geklärt, geht es daran, Windows 7 im Unternehmen zu verteilen. Dabei wendet sich unser Workshop zunächst der Frage zu, wie Windows 7 für die automatische Softwareverteilung vorbereitet werden muss. Nachdem der Client derart vorbereitet wurde, steht dann die tatsächliche Verteilung an und die Frage, wie

sich beispielsweise die virtuellen Festplatten, die Windows 7 bietet, dabei nutzen lassen. Und natürlich ist so ein Rollout kaum ohne Tool-Unterstützung zu realisieren, weshalb wir im Workshop beispielhaft die Rollout-Unterstützung durch das MS System Center betrachten.

Somit will unser Workshop-Nachmittag helfen, den Umstieg auf Windows 7 so einfach wie möglich zu gestalten, indem er den Teilnehmern geeignete Vorgehensweisen vermittelt und zudem mögliche Werkzeuge des Rollouts untersucht. Wir freuen uns auf jeden Fall, Sie in Karlsruhe zu begrüßen. 

**iläNet**  
Die System und Netzwerk User Group

#### Die Agenda des Workshops

**13.00 Uhr:** Begrüßung

**13.05 Uhr:** Herausforderungen der Windows 7-Migration

- Hardwareauswahl
- Anwendungen portieren
- Parallelbetrieb mit Windows XP
- Migration der Benutzerprofile

*Dozenten: Thorsten Christoffers und Thomas Wegener, Berater, sepago GmbH, Köln*

**14.30 Uhr:** Kaffeepause

**14.45 Uhr:** Lösungen für die Windows 7-Migration:  
Empirum Client Life Cycle Management

*Dozent: Roland Schäfer, matrix 42 AG*

**15.30 Uhr:** Rollout von Windows 7

- Vorbereitung der Verteilung
- Automatische Installation
- Virtuelle Festplatten nutzen
- Unterstützung durch MS System Center

*Dozenten: Thorsten Christoffers und Thomas Wegener, Berater, sepago GmbH, Köln*

**17.30 Uhr:** Ende des Workshops

**Ort:** Der Blaue Reiter Designhotel,  
Amalienbadstr. 16, 76227 Karlsruhe

**Teilnahmegebühren:**

Für IT-Administrator Abonnenten kostenlos.

**Anmeldung bis zum 15. September unter**  
[www.it-administrator.de/workshops/](http://www.it-administrator.de/workshops/)

**Workshop "Windows 7" am**  
**21. September 2010 in Karlsruhe**



**Im Test: Vizioncore vFoglight Pro 6.0**

# Licht im virtuellen Nebel

von Jürgen Heyer

Umgebungen mit hundert und mehr virtuellen Maschinen unter VMware Virtual Center sind heutzutage keine Seltenheit mehr. Mit der zunehmenden Größe wird es jedoch immer schwieriger, das Zusammenspiel aller Systeme mit der gemeinsamen Nutzung der verfügbaren Ressourcen zu überwachen. Hilfreich ist dann ein Tool wie vFoglight von Vizioncore, um schleichende Lastzunahmen oder auch ein ungewöhnliches Verhalten einzelner Gastsysteme rechtzeitig zu erkennen. Wie gut das funktioniert, wollte IT-Administrator genauer wissen.

**E**in Ende des Wachstums der virtuellen Umgebungen in den Unternehmen ist nicht in Sicht. Viele Firmen betreiben mittlerweile auch schon mehr als eine Virtualisierungsfarm. Wer auf den Marktführer VMware setzt, hat in einer produktiven Umgebung meist VMware Virtual Center (vCenter) im Einsatz. vCenter ermöglicht eine Lastverteilung und meldet auftretende Probleme sowie Performanceengpässe. Allerdings reichen die von vCenter gelieferten Informationen nicht aus, um beispielsweise bei einem auftretenden Engpass sicher zu erkennen, ob es sich um ein generelles Problem durch das Anlegen zu vieler VMs handelt, ob eine allgemeine Lastzunahme dafür verantwortlich ist oder ein Gastsystem allein der Verursacher ist und warum. Vor allem unterstützt vCenter den Administrator nicht bei der Analyse durch zusammenhängende Informationen, da es nicht in ein Gastsystem hineinschauen kann. Auch die VMware-Boardmittel stoßen beim Betrieb mehrerer vCenter schnell an Grenzen. Jedes vCenter ist dann vom Administrator als Insel getrennt zu betrachten.

Hier setzt vFoglight Pro 6.0 an und bietet eine übergreifende Leistungs- und Zustandsüberwachung auch über mehrere vCenter hinweg. Durch einen Blick auf die Dienste in einer VM ist es möglich, den Grund und die Auswirkungen auf den

Ressourcenverbrauch schneller zu erkennen. Außerdem hilft es bei der Erkennung wenig genutzter Ressourcen; drohende Engpässe werden durch Trendanalysen früher sichtbar. Weiterhin erlaubt vFoglight eine Kapazitätsplanung für Erweiterungen sowie geplante Migrationen und macht die Kosten transparent.

vFoglight ist ein Ableger des für den Enterprise-Einsatz konzipierten Applikationsüberwachungstools Foglight. Dieses wurde von der Softwareschmiede Quest, zu der Vizioncore gehört, entwickelt. vFoglight besteht letztendlich aus dem Foglight-Kernmodul inklusive einer Virtualisierungserweiterung. vFoglight-Anwender können durch zusätzliche Erweiterungen, Cartridges genannt, das Produkt zu Foglight aufrüsten. Ebenso kann ein Unternehmen, das Foglight nutzt, durch die Ergänzung mit den Virtualisierungscartridges auch seine virtuellen Umgebungen überwachen.

## Bei der Installation kommt es auf den richtigen Agenten an

Für den Test installierten wir den vFoglight Pro 6.0 Management-Server auf einem eigenständigen Windows 2008 Server. Der Management-Server kann im sogenannten Stand-alone-Modus arbeiten, weiterhin im Hochverfügbarkeitsmodus, was eine externe Datenbank voraussetzt, sowie als Windows-Dienst, was wir in un-

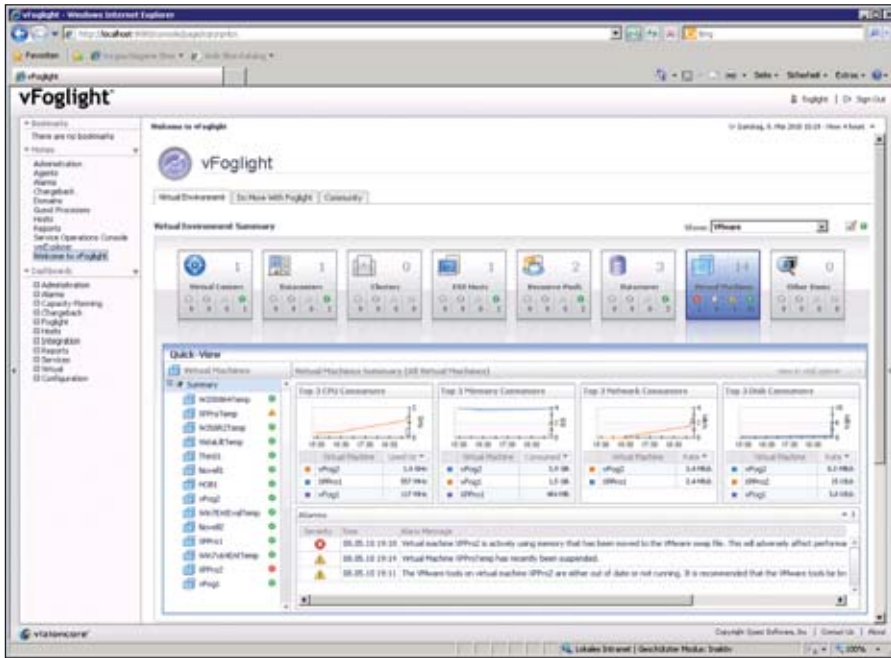
serer Testumgebung nutzten. vFoglight kommt mit einer integrierten MySQL-Datenbank, unterstützt aber auch als externe Datenbank MySQL, Oracle und MS SQL Server 2003/2008. Bei einer externen Datenbank kann diese auf einem Server unter Windows 2003/2008 Server, Red Hat Enterprise Linux 5.3, IBM AIX 5.3, HP-UX 11i v2 oder Solaris 10 laufen. Unbedingt zu beachten sind die allgemeinen Hardwareanforderungen (Kasten "Systemvoraussetzungen"), die in einer 64-Bit-Umgebung einen aktuellen Hochleistungsserver voraussetzen. In einer Multi-Tier-Umgebung mit getrennter Datenbank sollten der Management-Server mindestens 8 GByte und der Datenbank-Server 6 GByte RAM besitzen.

Management-Server mit 64 Bit-Betriebssystem:  
Quadcore-Prozessor 2,4 GHz, 12 GByte RAM,  
120 GByte Plattenkapazität auf schnellen Festplatten  
(10.000 U/min). Management-Server mit 32 Bit-  
Betriebssystem: Quadcore-Prozessor, 4 GByte RAM,  
120 GByte Plattenkapazität auf schnellen Festplatten  
(10.000 U/min). Betriebssystem Windows  
2003/2008 Server, SLES 9/10, Oracle Unbreakable  
Linux 5, RHEL 4/5/5.3 oder Solaris 9/10.

Der Agent Manager auf überwachten Maschinen verursacht durchschnittlich 4,8 Prozent CPU-Last und benötigt durchschnittlich 180 MByte Plattenkapazität.

### Systemvoraussetzungen





**Bild 1:** Mit unterschiedlichen Ansichten visualisiert vFoglight den aktuellen Zustand der virtuellen Umgebungen recht eindrucksvoll

Bei der Installation wird ein Web-Server mit eingerichtet, da die Konsole als Java-Programm im Browser läuft. Hier fällt auf, dass der Monitor mindestens 20 Zoll groß sein sollte, bei der von uns genutzten Auflösung mit 1.920 x 1.080 Punkten reichte diese in der Höhe noch nicht aus, um den Gesamtüberblick auf der Willkommens-Seite ohne Schiebepalken darzustellen.

Als Testumgebung diente uns ein Virtual Center vSphere 4.0 auf einem weiteren Windows 2008 Server. Das vCenter wiederum griff auf einen ESX4i-Server zu, auf dem mehrere VMs liefen. Mit der neuen Version 6.0 hat sich das Agentenkonzept geändert, Vizioncore spricht hier von der Middleware. Auf jedem auch intern zu überwachenden Client, also auch auf den VMs, ist der so genannte "Agent Manager" zu installieren. Der Agent Manager übernimmt die Kommunikation mit dem Management-Server und ist quasi ein Schirm für die diversen Agenten, die auf den Clients benötigt werden, um unterschiedliche Prozesse, Dienste et cetera abzufragen. Welche Agenten ein Administrator verteilt, hängt davon ab, was er überwachen möchte.

Funktionserweiterungen des Management-Servers erfolgen durch die Installation der schon erwähnten Cartridges. Cartridges enthalten zusätzliche Funktionalitäten, aber auch Komponenten wie neue Agenten. Damit vFoglight nun eine virtuelle Umgebung überwachen kann, sind auf dem Management-Server die "Cartridge for VMware" und zwei Cartridges mit VMware-Agentenkomponenten zu installieren und zu aktivieren. Damit stehen die Grundfunktionalität und zwei Agenten für die Abfrage des vCenter zur Verfügung. Die Agenten wiederum sind auf einen Server mit Agent Manager zu verteilen und die Anmeldeinformationen auf dem vCenter einzutragen. Im Falle der Grundinstallation läuft dies glücklicherweise etwas einfacher ab, da diese standardmäßig die Einrichtung des Management Servers, der Datenbank und des VMware Infrastructure Agents auf einem System umfasst, so dass wir im Test nur die Anmeldedaten eingeben mussten. Da wir aber auch einige VMs intern überwachen wollten, mussten wir anschließend aus vFoglight die Installationspakete für die Agent Manager (32 und 64 Bit) herunterladen und auf den

gewünschten VMs installieren, damit wir aus vFoglight heraus die eigentlichen Agenten verteilen konnten.

### Eindrucksvolle Visualisierung

Auf den ersten Blick verständlich und zugleich intuitiv bedienbar präsentiert sich die ausladende vFoglight-Konsole. Die bei Administratoren standardmäßig eingestellte Startseite "Welcome to vFoglight" zeigt eine Zusammenfassung der gesamten virtuellen Umgebung unter anderem mit der Anzahl der Virtual Center, Data Center, Datastores, VMs und Angabe des Status mit vier Farben (grün, gelb, orange, rot). Ein Unterfenster namens "Quickview" visualisiert den aktuellen Stand und als Kurvendiagramm die Historie der vier wichtigsten Ressourcen CPU-Last, Netzwerk-I/O, Disk-I/O und Speichernutzung. Sobald der Betrachter intuitiv auf ein Objekt klickt, wird dieses vergrößert dargestellt beziehungsweise das Quickview-Fenster inhaltlich angepasst. Um mehr über einen Alarm zu erfahren, reicht es, auf das entsprechende farbige Symbol zu klicken. Unterhalb des Quickview-Fensters befindet sich ein Fenster namens "FAQts" mit vorbereiteten Abfragen, um sich beispielsweise die VMs mit der höchsten CPU-Last oder die Datastores entsprechend des noch freien Speichers auflisten zu lassen.

Die Navigationsleiste auf der linken Seite teilt sich standardmäßig in die drei Rubriken "Bookmarks", "Homes" und "Dashboards". Die Rubrik Dashboards beinhaltet alle Einstiegsansichten und ist damit der wichtigste Bereich für die Navigation. Der Inhalt der anderen beiden Rubriken lässt sich durch den Benutzer anpassen, um schneller zu häufig benötigten Ansichten zu kommen. Standardmäßig beinhaltet das Dashboard bei einem Administrator elf Rubriken, die wiederum eine Vielzahl an Unteransichten beinhalten. Gerade am Anfang muss sich der Administrator erst etwas orientieren und sollte die diversen Menüpunkte einmal durchklicken, um einen ersten



Eindruck vom Gesamtumfang des Werkzeugs zu erhalten. Insgesamt bietet das Programm außergewöhnlich viele Möglichkeiten zur individuellen Anpassung der Konsole sowohl hinsichtlich des Stils als auch der Menüstruktur.

Der Menüpunkt "vmExplorer" ermöglicht dem Administrator eine genaue Analyse einzelner VMs. Das Registerblatt "Monitor" liefert eine Vielzahl an Werten zum Speicherverbrauch, CPU-Last sowie Platten- und Netzwerk-I/O. Gut ist, dass die meisten Werte mit einer Historie kommen, so dass sich schnell erkennen lässt, ob sich in der letzten Zeit etwas geändert hat. Das Register "Storage" konzentriert sich auf die Platten-I/O-Werte getrennt für jeden Datastore. Auch ermittelt vFoglight das wöchentliche Wachstum und errechnet daraus, wann die Platte voll ist. Ob das realistisch ist, muss ein Administrator natürlich individuell bewerten, aber Trends werden so sichtbar. Das Register "Processes" ist nur gefüllt, wenn auf der VM der Agent Manager mit dem so genannten GuestProcessAgent installiert ist. Dann liefert vFoglight die CPU-Last der einzelnen Dienste. Zeigt also beispielsweise eine VM in vFoglight in der Übersicht eine ungewöhnlich hohe Last an oder wird gar ein Alarm ausgelöst, so kann der Administrator hier nachschauen, ob ein bestimmter Dienst auf der VM dafür verantwortlich ist. Er muss nicht zwischen verschiedenen Administrationswerkzeugen springen, sondern kann alles mit einem Tool erledigen. Genauso detailliert wie die Gastsysteme analysiert vFoglight die ESX-Hosts und liefert diverse Diagramme (Historie und aktuelle Werte) zur Netzwerk-, RAM-, CPU- und Plattenspeicherauslastung. Auch hier ist es möglich, sich die Last der einzelnen Prozesse anzeigen zu lassen.

Geradezu in Erstaunen versetzte uns die Art und Weise, wie sich vFoglight selbst überwacht. Eine eigene Rubrik liefert dem Administrator genaue Informationen, wie es um den Management-Server selbst und die eigene Applikation bestellt

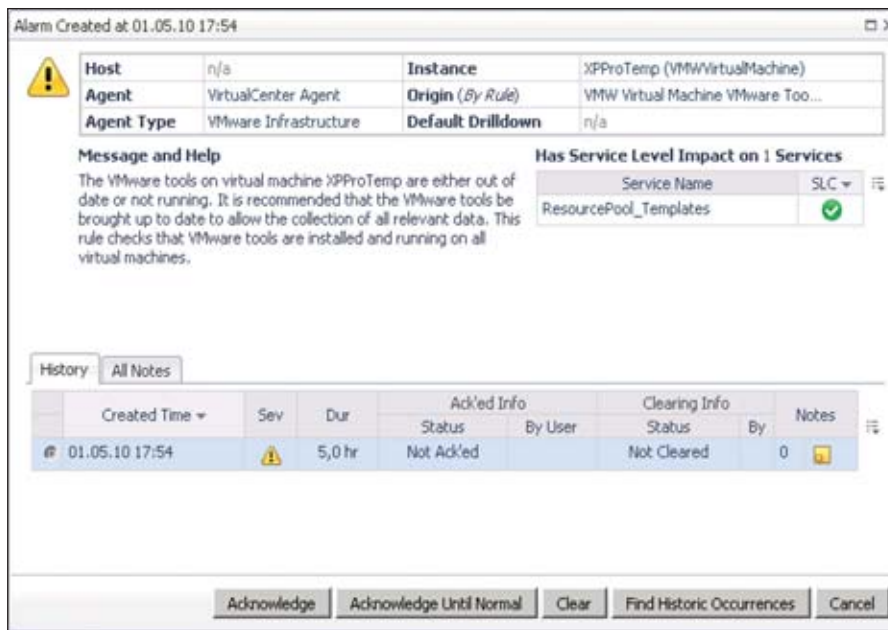


Bild 2: Ein intuitiver Klick auf ein Alarmsymbol reicht aus, um mehr über den Grund zu erfahren

ist. Unter anderem stehen Diagramme zur genutzten Datenbank (MySQL, Oracle), zu Java, zur Regelarbeit sowie Werte zu den Datenbankgrößen zur Verfügung. Allerdings bedarf es einiger Erfahrung, diese Diagramme zu interpretieren.

### Komplexe Regeln für die Alarmierung

vFoglight bietet eine Vielzahl an vorkonfigurierten Alarmen. Nichtsdestotrotz ist es natürlich wichtig, das gesamte Gerüst an die individuellen Gegebenheiten anzupassen. Dazu enthält vFoglight ein umfangreiches Regelwerk, in dem individuell die Bedingungen definiert werden können, wann benachrichtigt wird und auf welche Weise. Neben den üblichen, einfachen Regeln, die bei der Überschreitung von Schwellwerten benachrichtigen, lassen sich auch komplexe verzweigte Regeln erstellen, bei denen Zustand und Abhängigkeit von unterschiedlichen Parametern und verschiedenen Quellen einbezogen werden.

Prinzipiell gibt es einfache Regeln, die drei Zustände (Fire, Undefined, Normal) kennen und komplexe Regeln mit fünf Schweregraden (Undefined, Fatal, Critical, Warning, Normal). Weiterhin gibt es Da-

ten-, Zeit- und Ereignis-gesteuerte Regeln. Regeln lassen sich auch mit einem Scheduler koppeln, um Prüfungen zu bestimmten Zeiten durchführen zu können. Auch kann eine Regel auf Wunsch erst dann einen Alarm auslösen, wenn mehrfache Prüfungen zu einem entsprechenden Resultat geführt haben. Positiv ist, dass vFoglight bereits mit einem umfangreichen Regelwerk geliefert wird, so dass ein Administrator hier nicht sofort einsteigen muss. Sobald aber Anpassungen notwendig sind, ist vorher eine umfassende Einarbeitung erforderlich. Wir haben den Eindruck gewonnen, dass das gesamte Regelwerk sehr mächtig, aber auch ebenso komplex ist. Die Mailbenachrichtigung erfolgt per SMTP-Mail (optional SMTPS), wobei sich für verschiedene Alarme unterschiedliche Mailadressen hinterlegen lassen. Ebenso kann vFoglight SNMP-Traps an ein übergeordnetes Managementsystem verschicken. Neben Benachrichtigungen veranlasst vFoglight auf Wunsch die Ausführung von lokalen oder entfernten Kommandoaufrufen oder ruft ein Skript auf.

Recht interessant und durchdacht ist das Scheduler-Konzept: So gibt es innerhalb von vFoglight eine bereits gefüllte Sche-

dulerliste mit typischen Zeitabläufen, die ein Administrator nach Belieben erweitern kann. Zu jedem Eintrag gibt es eine Reche-  
teliste, wer diesen ausführen darf. Bei der Erstellung von Re-  
geln oder auch Berichten kann deren Ausführung nun mit einem  
vorhandenen Planungseintrag verknüpft werden.

Ebenfalls ein sehr komplexes Thema für den fortgeschrittenen  
Administrator ist die Möglichkeit, mit eigenen Skripten zu  
arbeiten. Dies wird in erster Linie benötigt, falls die mitge-  
lieferten Cartridges und Agenten bestimmte Informationen  
von einer überwachten Maschine nicht liefern können. Die  
Ausführung übernimmt der so genannte Script Agent. Ein  
Administrator kann Skripte in einer beliebigen Sprache schrei-  
ben (Batchdateien, Visual Basic, Shell-Skripte), die dieser Agent  
ausführt. Um deren Resultate zu erfassen, liest der so genannte  
"vFoglight collector" von der Standardausgabe (stdout) und lei-  
tet die Daten an den Agent Manager weiter, der diese dann an  
den Management-Server übergibt. Daneben besitzt vFoglight  
eine interne Scriptsprache, die für Abfragen oder auch für die  
Erstellung von Regeln zum Einsatz kommt.

### Abrechnen, berichten und planen

Falls in einem Unternehmen eine interne Abrechnung der von  
der IT bereitgestellten Ressourcen erfolgen soll, kann vFoglight  
die entsprechende Nutzung erfassen und unterstützt dazu zwei  
Modelle namens TFR (Tiered Flat Rate) und MRU (Measured  
Resource Usage). Bei TFR sind entsprechend der genutzten  
VM-Größen (CPU, Speicher, Storage) Typen festzulegen, die  
feste Kosten verursachen. Die laufenden VMs müssen nun  
noch einem TFR-Typ zugewiesen werden, schon kann vFoglight  
die Nutzung erfassen und daraus einen Abrechnungsreport er-  
stellen. Beim MRU-Modell sind Gesamtkosten und Laufzeit  
eines ESX-Servers zu hinterlegen, woraus sich die monatlichen  
Kosten ergeben. Über eine Gewichtung der Ressourcen er-  
mittelt vFoglight nun, welcher Kostenanteil auf jede auf einem  
Host laufende VM entfällt. Hier sind sowohl eine Vollkosten-  
als auch eine Teilkostenkalkulation möglich.

Um bei Migrationen oder vor einer Verlagerung von Res-  
ourcen im Vorfeld die Machbarkeit abschätzen zu können,  
besitzt vFoglight ein Modul zur Kapazitätsplanung. Bei einer  
abstrakteren Planung beispielsweise für einen neuen Host er-  
stellt der Administrator ein Szenario und gibt dabei entspre-  
chende Werte für CPU, RAM, Netzwerk und Storage vor.  
Dann ordnet er diesem Szenario die existierenden VMs zu,  
für die er dieses System plant, und kann nun aufgrund der in  
der Vergangenheit gesammelten Daten sehen, inwiefern der  
Leistungsbedarf die gesetzten Planwerte einhält oder über-  
schreitet. Alternativ ordnet der Administrator in einem Sze-  
nario mehrere VMs einem existierenden Host zu, um zu prü-  
fen, ob diese VMs alle gemeinsam auf dem Host laufen  
könnten. Der Vorteil der Kapazitätsplanung von vFoglight ge-

Kostenlos für  
IT-Administrator-Abonnementen  
und ice:2010-Teilnehmer



# Workshop in Lingen

Windows 7  
am 13. August 2010

## Die Agenda:

13.00 Uhr: Begrüßung

13.05 Uhr: Herausforderungen der Windows 7-Migration

- > Methoden der Automatisierung
- > Anwendungen portieren
- > Parallelbetrieb mit Windows XP
- > Migration der Benutzerprofile

Dozenten: Thorsten Christoffers und Thomas Wegener,  
Berater, sepago GmbH, Köln

14.30 Uhr: Kaffeepause

14.45 Uhr Partnernvortrag:

Client-Lifecycle-Management:

Automatisiert zu Windows 7 wechseln

- > Vorbereitungen, Aufgaben und Herausforderungen vor dem Betriebssystemwechsel
- > Risiken vermeiden mit dem Windows 7 Kompatibilitätscheck
- > Windows 7 automatisiert installieren
- > Beispielhaftes Migrationsszenario im Netzwerk

Dozent: Gerd Conrad, Baramundi Software AG

15.30 Uhr: Rollout von Windows 7

- > Vorbereitung der Verteilung
- > Automatische Installation
- > Virtuelle Festplatten nutzen
- > Unterstützung durch MS System Center

Dozenten: Thorsten Christoffers und Thomas Wegener

17.30 Uhr: Ende des Workshops

**Termin:** 13. August 2010

**Ort:** it.emsland, Halle 31, Kaiserstraße 10b, 49809 Lingen

**Uhrzeit:** 13.00 bis ca. 17.30 Uhr

**Teilnahmegebühren:**

Für IT-Administrator-Abonnementen und ice:2010-Teilnehmer kostenlos.

Mehr Infos hierzu auch unter [www.ice-lingen.de](http://www.ice-lingen.de).

**Anmeldeschluss: 09. August 2010**

**Mehr Infos und Anmeldeformulare unter**  
[www.it-administrator.de/workshops/](http://www.it-administrator.de/workshops/)





genüber einer manuellen Planung auf dem Papier besteht darin, dass vFoglight tatsächlich die bisherigen Lastkurven der VMs addiert. Sollen nun auf einem System mehrere VMs mit starken Lastschwankungen arbeiten, die aber ihre Spitzen zu unterschiedlichen Zeiten haben, so kann vFoglight die resultierende Summe in der Vergangenheit genau ermitteln und so eine Aussage für die Zukunft treffen. Eine Planung auf dem Papier ist viel ungenauer, da ein Administrator hier von allen Lastspitzen ausgehend diese addieren müsste.

Sehr umfangreich ist das in vFoglight integrierte Reporting. Das Programm bietet bereits eine Vielzahl an Vorlagen, darüber hinaus kann der Administrator weitere Vorlagen erstellen. Neben der Definition der eigentlichen Abfrage kann der Zeitabschnitt frei gewählt werden, um eine Auswertung beispielsweise über vier Stunden oder auch zwei Tage zu fahren. Genauso lässt sich die Granularität festlegen, also die gewünschten Zeitschritte. Die Reporterstellung kann mittels der beschriebenen Scheduler automatisiert werden, wobei die Ausgabe als PDF-, XLS- oder XML-Datei erfolgt. Auch ein automatischer Versand

per E-Mail ist möglich. Eine Testfunktion hilft dem Administrator bei der Überprüfung, ob ein erstellter Report auch das gewünschte Resultat bringt.

### Durchdachte Benutzerverwaltung

vFoglight besitzt ein umfassendes Rollenkonzept zur Verwaltung der Benutzerrechte. Dabei kann ein Administrator Benutzer und Gruppen innerhalb von vFoglight anlegen oder eine Anbindung per LDAP an einen Verzeichnisdienst (Active Directory, Sun Java Systems Directory Server, OpenLDAP und Novell eDirectory) einrichten und dort angelegte Benutzer und Gruppen nutzen. Bei der Installation von vFoglight werden zudem ein interner Benutzer mit Administrationsrechten sowie eine Handvoll Gruppen angelegt, die nicht gelöscht werden können. Die eigentliche Rechtevergabe erfolgt über Rollen (unter anderem Administrator, Cartridge Developer, Console Operator), in denen die Detailrechte auf verschiedene Objekte und Ansichten innerhalb von vFoglight festgelegt sind. Über eine Rollenzuweisung an eine Gruppe, in der sich wiederum ein oder mehrere Benutzer befinden, werden die Rechte letztendlich zugeordnet. Entsprechend

der Rolle sehen die Benutzer nur einen Teil des Navigationsmenüs.

Jeder Benutzer kann zudem eine bevorzugte Startseite festlegen, um entsprechend seiner Aufgabe an einer passenden Stelle in die Konsole einzusteigen, und Lesezeichen zu häufig genutzten Seiten festlegen. Wie bei Windows selbst lässt sich der kom-

#### Produkt

Managementsoftware für virtuelle Umgebungen.

#### Hersteller

Vizioncore  
www.vizioncore.com

#### Preis

vFoglight Pro wird pro Socket der ESX-Server lizenziert und kostet pro CPU 587 Euro. Enthalten sind ein Jahr Support und Subskription. Bei drei Jahren Support kostet die Lizenz 752 Euro.

#### Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Installation	7
Intuitivität der GUI	9
Detailgrad und Umfang	9
Alarmierung und Reporting	8
Dokumentation	8

#### Dieses Produkt eignet sich

**optimal** für große bis sehr große virtuelle Umgebungen auch mit mehreren vCenter und einigen hundert VMs.

**bedingt** für mittelgroße virtuelle Umgebungen mit nur einem vCenter und einer überschaubaren Anzahl an VMs. Hier ist eine genaue Abschätzung des Aufwands für die Konfiguration und den Betrieb von vFoglight gegenüber dem Nutzen erforderlich.

**nicht** für Umgebungen, die bei der Virtualisierung nicht auf VMware setzen oder die kein vCenter betreiben.

**Vizioncore vFoglight Pro 6.0**



Bild 3: Sehr gut gelungen und informativ ist die Übersicht aller wichtigen Leistungsdaten einer virtuellen Maschine

plette Seitenstil hinsichtlich der Farben anpassen. Weiterhin ist es möglich, eine oder mehrere Seiten direkt über die Favoriten des benutzten Browsers zu verlinken. Nach Anklicken eines solchen Links erscheint zuerst die Anmeldeseite von vFoglight und anschließend die gewünschte Seite. Letztendlich ist es kein Problem, bei der Nutzung von vFoglight durch verschiedene Supportgruppen (First Level, Second Level) in einem größeren Unternehmen die jeweiligen Ansichten optimal zu konfigurieren, wobei jeder Benutzer hier auch selbst tätig werden kann.

### Fazit

Im Test präsentierte sich vFoglight Pro 6.0 als überaus mächtiges und umfassendes Management- und Überwachungstool für virtuelle Umgebungen, bei dem der Mehrwert mit wachsender Größe der Umgebung ebenfalls zunimmt. Sinnvoll ist ein Einsatz beim Betrieb ab etwa zehn ESX-Servern in einem Virtual Center und mehr als hundert virtuellen Maschinen bis hin zu sehr großen Netzwerken mit mehreren vCenter-Installationen, Hunderten von Hosts und Tausenden von virtuellen Maschinen. vFoglight überwacht alle denkbaren Dienste, liefert eine fast schon erschlagende Vielzahl an Performancewerten mit Überwachung von Schwellwerten, wertet die Verfügbarkeit als Nachweis für Service Level Agreements aus, erlaubt eine Kapazitätsplanung und ermöglicht die Erstellung von Reports für eine Nutzungsabrechnung. Durch eine breite Betriebssystemunterstützung sowohl beim Management-Server als auch bei den Agenten ist vFoglight nicht nur für die Windows-Welt geeignet, sondern auch für heterogene Umgebungen.

Ein Administrator sollte allerdings wissen, dass auf ihn gerade am Anfang umfassende Konfigurationsarbeiten zukommen, um zum einen alle benötigten Informationen abzufragen und die ganze Oberfläche auf die eigenen Belange anzupassen. Zum anderen müssen die gelieferten Datenmengen für einzelne Anwendergruppen sinnvoll beschränkt werden. Dies erfordert, dass sich jemand eingehend mit vFoglight beschäftigt sowie am besten diverse Schulungen belegt, um die Lernkurve zu beschleunigen und die Wichtigkeit der diversen Funktionen schneller abschätzen zu können. Immerhin hat vFoglight seinen Ursprung in dem Enterprise-Produkt Foglight von Quest und ist entsprechend komplex, so dass sich gerade die Einführung schnell eine Zeit lang als Vollzeitjob entpuppen kann.

Erfreulich umfangreich und übersichtlich ist die Dokumentation, die Gesamtkomplexität aber macht es schwierig, sich nur durch deren Studium einzuarbeiten. Auch für uns war es unmöglich, im Test alle möglichen Funktionen einzurichten und anzuschauen, dazu erwies sich vFoglight als zu mächtig. Wer allerdings die Hürden der Einarbeitung und Konfiguration am Anfang überwunden hat, wird später auf vFoglight nicht mehr verzichten wollen. (jp)



Kostenlos für  
IT-Administrator-Abonnementen

# iläNet

## Workshop in Karlsruhe

Windows 7  
am 21. September 2010

### Die Agenda:

13.00 Uhr: Begrüßung

13.05 Uhr: Herausforderungen der Windows 7-Migration

- > Methoden der Automatisierung
- > Anwendungen portieren
- > Parallelbetrieb mit Windows XP
- > Migration der Benutzerprofile

Dozenten: Thorsten Christoffers und Thomas Wegener,  
Berater, sepago GmbH, Köln

14.30 Uhr: Kaffeepause

14.45 Uhr – Partnervortrag:

Lösungen für die Windows 7 Migration:  
Empirum Client Life Cycle Management

ITANet Workshop-Partner:

**matrix42**

Dozent: Roland Schäfer, Matrix42 AG

15.30 Uhr: Rollout von Windows 7

- > Vorbereitung der Verteilung
- > Automatische Installation
- > Virtuelle Festplatten nutzen
- > Unterstützung durch MS System Center

Dozenten: Thorsten Christoffers und Thomas Wegener

17.30 Uhr: Ende des Workshops

**Termin:** 21. September 2010

**Ort:** Der Blaue Reiter Designhotel,  
Amalienbadstraße 16, 76227 Karlsruhe

**Uhrzeit:** 13.00 bis ca. 17.30 Uhr

**Teilnahmegebühren:**

Für IT-Administrator-Abonnementen kostenlos.

**Anmeldeschluss: 15. September 2010**

**Mehr Infos und Anmeldeformulare unter**  
[www.it-administrator.de/workshops/](http://www.it-administrator.de/workshops/)



**Im Test: Kaviza VDI-in-a-Box**

# Virtuelle Desktops aus der Dose

von Thomas Bär

Die Virtual Desktop Infrastructure (VDI) soll so ziemlich jedes Problem der Administration bei der Bereitstellung von Arbeitsumgebungen lösen – so suggerieren es die Hersteller. Richtig ist allerdings auch, dass VDI ein deutliches Mehr an Infrastruktur benötigt, ehe auch nur ein einziger Desktop für die Anwender zur Verfügung steht. Kaviza will beweisen, dass das Verteilen virtueller Desktops weder kompliziert noch teuer sein muss. IT-Administrator hat das Desktop-Rollout mit VDI-in-a-Box im Testlabor ausprobiert.

Ort werden direkt in Richtung des Serverraums verlagert. Die bekannten Erfahrungen bezüglich der Anforderungen aus dem Terminal-Server-Umfeld können dabei nicht 1-zu-1 auf VDI angewendet werden. Während beispielsweise ein herkömmlicher 32-Bit Windows-Terminalserver mit 4 GByte RAM bis zu 40 gleichzeitige Terminalsitzungen ohne Probleme bietet, sind es – je nach Server-Hardware – bei den meisten VDI-Lösungen deutlich weniger, da komplett eigenständige Betriebssysteme vorgehalten werden.

Kaviza gibt in Bezug auf die Auslastung zirka fünf bis acht gleichzeitige User/Desktops pro virtuellem Core an. Ein Template mit Windows XP als Betriebssystem kommt üblicherweise mit 512 MByte Arbeitsspeicher gut aus. Für Windows 7 müssen mindestens 1 GByte angerechnet werden. Zusätzlich benötigt die Kaviza-Appliance selbst 512 MByte des physikalischen Arbeitsspeichers und die zugrunde liegende Hypervisor-Software darf mit einem bis maximal 3 GByte Speicherbedarf kalkuliert werden. Um beispielsweise zehn gleichzeitige Windows XP-Desktops mit VMware ESXi4 zu betreiben, ist eine Maschine mit mindestens 6,5 GByte Arbeitsspeicher erforderlich.

**H**inter Kaviza stehen namhafte Unternehmen, die sich vor einigen Jahren mit der Zielsetzung, eine einfachere VDI-Umgebung bereitstellen zu können, zusammaten: Hewlett Packard und IBM. Im April dieses Jahres beteiligte sich zudem Citrix mit einem strategischen Investment an Kaviza. VDI-in-a-Box (VDIB) arbeitet als virtuelle Maschine auf Hypervisor-Basis und bietet alles, was für den Aufbau einer VDI-Umgebung notwendig ist. Durch das Hinzufügen weiterer Server ist VDIB sehr einfach skalierbar, was das professionelle Einsatzfeld der Software noch einmal unterstreicht. Für Administratoren in kleineren und mittleren Unternehmen besonders hervorzuheben ist die Fähigkeit von VDIB, auch ohne zusätzliches SAN-Storage eine VDI-Umgebung bereitstellen zu können. Zum Zeitpunkt des Tests war Kaviza VDIB ausschließlich in VMware ESX 3/4-Umgebungen einsatzfähig. Die Unterstützung für Xen, nebst HDX-Protokoll, ist mit Version 3.0 in das Produkt eingeflossen. Die Integration in Umgebungen mit Microsoft Hyper-V steht bereits fix in der Roadmap der Entwickler und wird inoffiziell für das vierte Quartal 2010 avisiert.

## Probleme herkömmlicher VDI

Die größte Hürde bei der Einführung von VDI sind üblicherweise die hohen Anforderungen an die Serversysteme, Netzwerkkomponenten und die Leistungsfähigkeit des Storage-Subsystems. Die Einsparungen bei den Leistungsanforderungen beim Client-Computer vor

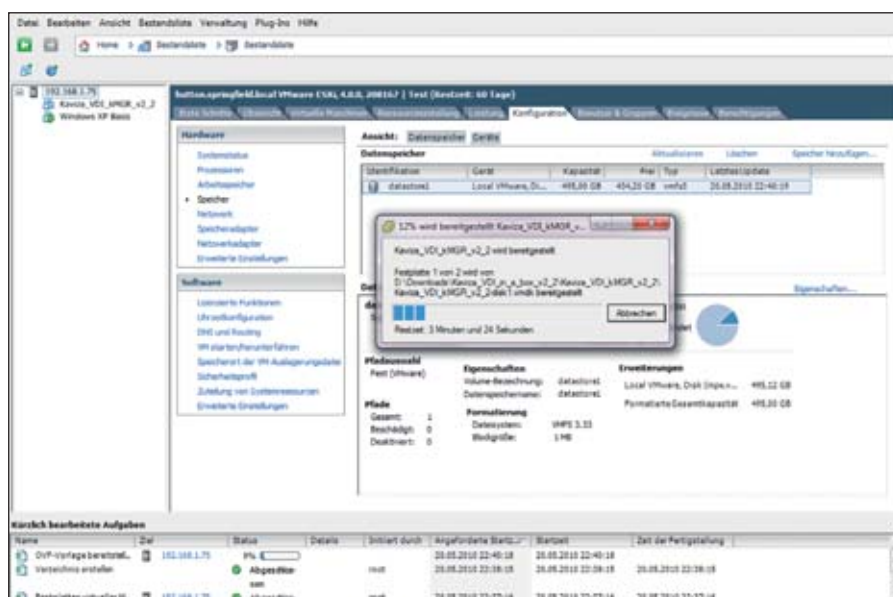


Bild 1: Nach der Installation von ESXi ist lediglich die Kaviza-VM zu importieren und eine IP-Adresse festzulegen. Der Einrichtungsaufwand ist dank der vorinstallierten VM sehr einfach



VDI erfordert zudem, dass die komplette Arbeitsumgebung des Benutzers, bestehend aus Betriebssystem, Applikationen und Benutzerprofil, zentral im Storage-System gespeichert werden. Neben den erhöhten Anforderungen in Bezug auf den Speicherplatz und die damit verbundenen höheren Kosten ist die Geschwindigkeit des Speichersystems von Bedeutung. Im Modell von VDI werden alle Interaktionen über das Storage-System abgewickelt. Die höheren Anfangsinvestitionskosten sind häufig ein großes Hindernis für VDI-Projekte. Das hier vorgestellte System "Kaviza" reduziert die Anforderungen auf eine möglicherweise günstigere Infrastruktur wie VMware ESXi und einfachere Standard-Hardware.

### Die Technik hinter Kaviza

Abstrakt betrachtet liefert Kaviza alle notwendigen Komponenten, die für den Aufbau einer VDI-Umgebung erforderlich sind. Als Serversysteme kommen derzeit VMware ESX 3 oder 4 sowie VMware ESXi 3 oder 4 zum Einsatz. Auf diesen Hypervisor-Servern werden für die Benutzer Windows XP- oder Windows 7-VMs betrieben. Das Erstellen, Organisieren und Zuweisen der virtuellen Maschinen übernimmt der Kaviza Management Server (kMGR), der ebenfalls als VM auf einem der ESX-Systeme läuft. Auf jeder VM für Anwender residiert der so genannte Kaviza Desktop Agent (kDA), der für die komplette Kommunikation mit dem kMGR zuständig ist. Die virtuellen Arbeitsumgebungen werden dabei nicht individuell pro Benutzer erstellt, sondern auf Basis eines einheitlichen Templates zur Laufzeit von Kaviza generiert. Alle Metadaten einer virtuellen Arbeitsumgebung, wie beispielsweise zugewiesene CPUs oder Arbeitsspeicher, aber auch das Betriebssystem oder Applikationen, werden durch das Template erstellt. Die Templates selbst werden aus ganz normalen virtuellen Maschinen, die auf dem Hypervisor-System generiert wurden, in ein "Working Desktop" überführt. Aus Sicht der Administration sinkt somit der Aufwand bei der Bereitstellung von Applikationen, Betriebssystemen, Patch-



Bild 2: Die Kaviza VDI-in-a-Box-Weboberfläche ist sehr leicht zu bedienen. Dank der Integration in LDAP-Verzeichnisdienste ist die Verwendung eines Microsoft Active Directory möglich.

Management oder der Bereitstellung von Antivirus-Pattern. Anstelle zahllose Umgebungen auf den neuesten Stand zu bringen, gilt es lediglich, die Desktop-Vorlage für die nächste Generation aufzubereiten. Gleichzeitig reduzieren Templates den Speicherbedarf auf dem Storage-System, da lediglich eine einzige Vorlage vorgehalten werden muss. Erst bei Aktivierung der virtuellen Desktops (VMs) wird der Speicherplatz tatsächlich angefordert.

Kaviza Server (kMGR) lassen sich als alleinstehende Server einrichten oder in einem Verbund betreiben. Unabhängig davon, ob es sich um einen einzelnen Server oder eine Gruppe von Servern handelt, wird eine Konfigurationseinheit als "Kaviza Grid" bezeichnet. Der Vorteil eines Grids mit mehreren Servern liegt auf der Hand: einerseits ist so eine bessere Verteilung der Systemlast (Load Balancing) gegeben. Andererseits sinkt die Abhängigkeit von einem einzelnen Server – fällt eine Maschine im Verbund aus, so sind Benutzer in der Lage, sich durch Neuansmeldung auf einem neuen System aufzuschalten. Sämtliche Konfigurationseinstellungen, Images und Templates werden zwischen den Grid-Servern automatisch repliziert.

### Einfache Installation

Die Einrichtung von Kaviza VDIB gestaltet sich sehr einfach. Der Hersteller bietet neben der kostenlosen Testversion für 30 Tage in Form einer virtuellen Maschine einige PDF-Dokumente in englischer Sprache an, die die Installation und die ersten Schritte in der Software be-

schreiben. Die Installation ist mit Hilfe der Unterlagen zwar problemlos möglich, doch darf der IT-Verantwortliche einige Male im PDF-Dokument von Seite zur Seite springen und ist zudem über einige Einträge im Sinne eines "fehlerhaften Verweises" in der Dokumentation verwundert. Sehr positiv indes: In rund zwei bis drei Stunden verfügt der Administrator über eine komplett ausgebaute Testumgebung für VDI.

Der erste Schritt der Inbetriebnahme von Kaviza besteht im Aufbau einer VMware ESX-Umgebung. Ist diese bereits vorhanden, so ist lediglich die rund 495 MByte große Virtual Appliance von Kaviza mithilfe eines Virtual Center Clients (VCC) auf einen ESX-Host zu importieren – ein Vorgang, der je nach Geschwindigkeit des Systems lediglich einige Minuten an Zeit in Anspruch nimmt. Kaviza ist in der Standardauslieferung auf DHCP eingestellt. Soll eine feste IP-Adresse verwendet werden, so ist mithilfe von VI in der Konsole die Einstellung in "/etc/network/interfaces" anzupassen. Alternativ ist eine IP-Adressreservierung anhand der MAC-Adresse möglich. Alle weiteren Einstellungen geschehen ausschließlich über die einfach und funktionell gehaltene Weboberfläche.

Bei der Erstanmeldung wurden wir im Test von einem Konfigurations-Assistenten begrüßt, der uns Schritt für Schritt durch die wichtigsten Einstellungen begleitete. In Kombination mit den PDF-Dokumenten sind auch diese Einrich-

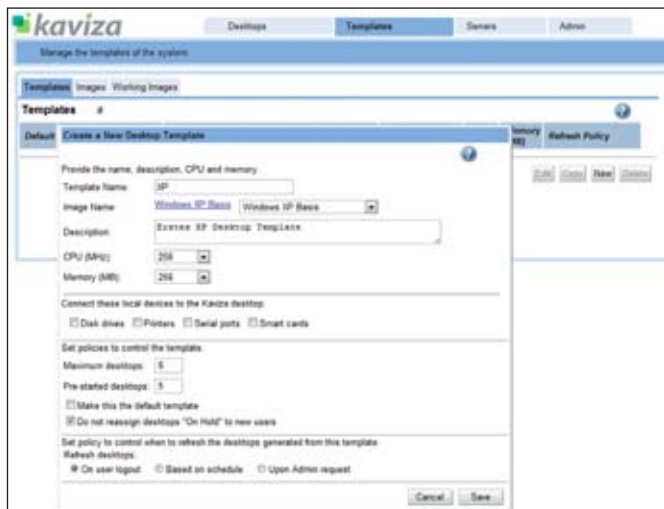


Bild 3: Bei der Anlage eines neuen Desktop Templates wird neben dem Betriebssystem und der darin installierten Software auch die rechnerische MHz-Performance und der Anteil am RAM zugewiesen

tungsschritte kein Hexenwerk und innerhalb weniger Minuten erledigt. Im ersten Schritt des Konfigurations-Assistenten wird ein neues "Kaviza Grid" angelegt. Danach entscheidet der Administrator, ob die Kaviza-Umgebung in einem Active Directory/LDAP-Verzeichnisdienst betrieben wird oder die Kaviza-interne Benutzerdatenbank verwendet werden soll. Zur Nutzung eines Verzeichnisdienstes sind lediglich die Nennung des entsprechenden DCs und die Eingabe eines administrativ entsprechend ausgestatteten Kontos erforderlich. Im abschließenden Konfigurationsschritt ist festzulegen, wie die ESX-Server angesteuert werden sollen: Über den VMware VCenter-Client oder über den lokalen Virtual Center-Client. Da das Kaviza-Grid die typischen Hochverfügbarkeitsfunktionalitäten von VMware wie VMotion, HA oder DRS nicht verwendet, ist der lokale Zugriff in kleineren Installationen in der Regel die richtige Antwort. Nach Beantwortung dieser Frage ist die Kaviza-Installation sofort nutzbar.

### Die ersten virtuellen Desktops

Nach der Einrichtung des Grids standen uns die vier Hauptmenü-Befehle von Kaviza namens Desktops, Templates, Servers und Admin zur Verfügung. Da zu diesem Zeitpunkt noch kein einziger virtueller Desktop erzeugt war, ließen sich folge-

richtig kaum Kommandos nutzen. Die erste Erstellung eines Desktops geschieht typischerweise durch die Übernahme einer bereits vorhandenen virtuellen Maschine mit Windows XP- oder Windows 7-Betriebssystem aus der ESX-Umgebung. Kaviza unterstützt offiziell kein Windows Vista, da es jedoch auf derselben Sysprep-Technik aufsetzt wie

Windows 7, dürfte sich auch Windows Vista theoretisch als Betriebssystem mit Kaviza VDIB nutzen lassen.

VDIB bringt bezüglich der VMs, die in Images umgewandelt werden sollen, sehr genaue Anforderungen mit. Daher empfiehlt es sich, diese VMs speziell für die Kaviza-Nutzung neu anzulegen. Der Titel der virtuellen Maschine darf keinerlei Umlaute oder länderspezifische Sonderzeichen enthalten, es dürfen keinerlei Snapshots angelegt und die VM darf unter keinen Umständen seit ihrer Erstellung umbenannt worden sein. Zudem ist die Größe der virtuellen Festplatte laut Dokumentation auf 50 GByte limitiert und es ist auch nur eine einzige virtuelle Festplatte pro VM zulässig. In der Testumgebung wurde ein virtuelles Windows XP installiert, auf den aktuellen Patch-Stand gebracht und mit weiterer Software, etwa einem PDF-Reader, ausgestattet.

Anschließend folgte die Überführung der virtuellen Maschine in ein sogenanntes "Working Image". Nach der Installation eines lokalen Kaviza-Clients auf unserer virtuellen Maschine, die in der Rolle des lokalen Administrators durchzuführen ist, war Kaviza in der Lage, die Maschine direkt über die Weboberfläche "fernzusteuern". Dabei wurde ein RDP-Zugriff auf

die jeweilige VM initiiert – sollte es dabei einmal zu Schwierigkeiten kommen, da beispielsweise der von Kaviza automatisiert ausgeführte SysPrep-Vorgang scheitert, so ist ein Aufschalten über die ESX-Konsole ebenfalls jederzeit möglich.

Da sich Working Images auch aus bestehenden Images von Kaviza erzeugen lassen, haben wir im Test zunächst ein Image mit einer Basis-Installation angelegt und mit VDIB als "Image" gespeichert. Dank kurzer und selbsterklärender Hinweisdiagnostik wird der Administrator dabei vor Fehlentscheidungen bewahrt. Beispielsweise informiert die Software, was genau beim Speichervorgang eines Working Images in ein Image passiert: Die virtuelle Maschine verschwindet aus der Übersicht in der ESX-Umgebung und das Image wird anschließend primär aus Kaviza heraus bearbeitet.

### Mit Working Images, Images und Templates arbeiten

Aus dem Working Image mit dem installierten Kaviza-Agent wird durch die Speicherung ein normales Image, das sich für die Zuordnung als Template für Benutzer eignet. In unserer Testumgebung haben wir das Basis-Image anschließend erneut als Grundlage für ein Working Image genutzt und mit entsprechender Office-Software ausgestattet. Ein Wor-

Es wird auch in Zukunft viele Umgebungen geben, in denen Terminalserver für viele Benutzer die optimale Arbeitsumgebung in Bezug auf Kosten/Nutzen-Faktor darstellen. Der eigenständige PC mit einer eigenen Betriebssysteminstallation, Grafikkbeschleuniger, lokaler RAID-Verbund hat als Workstation ebenfalls eine "feste Heimat". VDI ist eine ergänzende Technologie die die Vorteile der Terminalserver-Technik mit den Vorzügen eines Fat Client-PCs in ganz eigener Art und Weise kombiniert. Somit ist VDI eine weitere Möglichkeit der Desktop-Bereitstellung, die mit den anderen beiden Varianten koexistiert. Sinkende Preise für Serverhardware, insbesondere Arbeitsspeicher und Storage, werden die Bereitschaft VDI zu nutzen, sicherlich steigern.

**VDI, Fat Client oder Terminalserver-Technik?**



# 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](http://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



king Image stellt somit eine aktuell in Bearbeitung befindliche virtuelle Maschine dar und ein Image ist eine fertig abgeschlossene virtuelle Maschine. Das Template wiederum ist die Zuordnung des Images mit weiteren Konfigurationsmerkmalen wie beispielsweise die rechnerische Zuweisung von CPU-Leistung und die Gewährung von zugeordnetem Arbeitsspeicher. Ob klassische RDP-Features, wie beispielsweise die Nutzung der Zwischenablage, der Zugriff auf Client-Laufwerke oder das automatische Mapping von Druckerzuordnungen, verwendet werden dürfen, wird ebenfalls im Template gesteuert.

Eine der wichtigsten Einstellungen im Template ist die Anzahl maximaler Desktops, die gleichzeitig durch Kaviza bereitgestellt, und die Anzahl bereits vorbereiteter Templates, sprich Desktops, die erzeugt und betrieben werden, auch ohne dass ein Anwender aktuell auf ihnen arbeitet. Je mehr vorbereitete Templates bereits im Vorfeld aktiv sind, desto schneller können sich Benutzer später anmelden. Ist beispielsweise nur ein einziges Template als "Prestart" eingetragen und ein Anwender hat sich vor kurzer Zeit angemeldet, so erhält der nächste Benutzer möglicherweise die Meldung, dass er noch einige Minuten auf seinen Desktop warten muss. Doch je höher der "Prestart"-Wert, desto mehr Ressourcen verwenden die Hypervisor-Server möglicherweise für nicht benutzte Desktops.

### Virtuelle Maschinen im Einsatz

Werden fünf Maschinen als "Prestart" eingetragen und das Dialogfenster bestätigt, so zeigt ein Blick in die Übersicht des VCC/vSphere-Client, was Kaviza VDIB im Anschluss vorbereitet: Nacheinander wird eine Maschine nach der anderen erzeugt, die Festplatten-Dateien kopiert und das System gestartet. Dass die Namen der VMs eher kryptischer Natur sind, ist kaum von Bedeutung, da in der Kaviza-Web-Oberfläche die Zuordnung zu Template und Benutzer leicht zu erkennen ist. Durch die Zuordnung einer OU im Ac-

tive Directory werden die vorbereiteten VMs auch in der AD-Struktur angezeigt. Welches Template für welche Benutzer oder welche Benutzergruppe vorgehalten wird, lässt sich im Menü "Admin" von Kaviza steuern – eine weitere Zuordnungsmöglichkeit wäre die Zuweisung von IP-Adressen zu Templates.

Der Zugriff auf den Desktop findet stets über die Web-Oberfläche statt. Von dort aus wird eine dynamische RDP-Sitzung auf die zugeordnete Maschine eingerichtet und die endgültige Anmeldung geschieht dann über den Windows-Dialog der VM. Danach steht dem Benutzer das Client-Betriebssystem mit seinen üblichen Fähigkeiten in einer RDP-Sitzung zur Verfügung. Die verschiedenen Übersichten in Kaviza zeigen dem Administrator in Echtzeit die Auslastung der VDI-Umgebung und den Status des Grids an. In "User Sessions" finden sich alle aktuell aktiven Sitzungen mit IP-Adresse, Name der virtuellen Maschine, Laufzeit und Name des angemeldeten Benutzers. Das Audit-Protokoll, das sich auch als CSV-Datei in jedes Tabellenkalkulationsprogramm exportieren lässt, umfasst alle Anpassungen in der Kaviza-Umgebung, An- und Abmeldungen und Statusveränderungen von virtuellen Maschinen nebst Zeitstempel und Benutzerangabe. Was genau mit einer virtuellen Maschine nach Abmeldung durch den Benutzer passiert, steuert der Administrator. Entweder wird der entsprechende "Desktop" gelöscht und durch eine neu vorbereitete VM ersetzt oder die Maschine wird "on hold" für die erneute Nutzung durch denselben Anwender vorgehalten. Ein einfacher Scheduler erlaubt die tägliche, wöchentliche oder monatliche Neuanlage von virtuellen Desktops.

### Fazit

Kaviza VDI-in-a-Box ist ohne Frage ein äußerst spannendes Produkt – verwandelt es doch eine Hypervisor-Installation auf Standard-Hardware in eine relativ leicht zu erstellende und unkompliziert zu bedienende VDI-Umgebung. Die Anleitung

beschreibt zwar alles, was für den Erstbetrieb notwendig ist, dennoch bleibt das Verlangen nach detaillierteren Informationen ungedeckt. Die Integration von VDIB in die verwendete IT-Management-Lösung ist sicherlich genau zu prüfen, da VDI ansonsten zu einer "Insellösung" werden würde. (dr)



#### Produkt

Software für den Aufbau einer VDI-Umgebung.

#### Hersteller

Kaviza  
www.kaviza.com

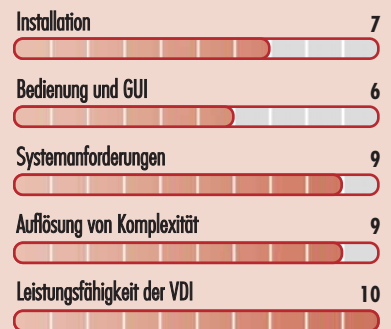
#### Preis

Bei 1-50 Desktops/Concurrent Users 95 Euro je Lizenz. Bis 100 gleichzeitigen Desktops 90 Euro und 61 Euro bei Abnahme eines 5.000+-Lizenz-Bundles. Die Kosten für Wartung und Support pro Jahr liegen zwischen 14 und 19 Euro pro Desktop.

#### Technische Daten

www.it-administrator.de/downloads/datenblaetter

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



#### Dieses Produkt eignet sich

**optimal** für kleinere und mittlere Firmen, die VDI nutzen wollen und ein gutes Preis-/Leistungsverhältnis suchen, ohne eine komplexe Serverumgebung vorzuhalten.

**bedingt** für kleinere und mittlere Firmen, die noch keine Standardisierung der Arbeitsumgebung umgesetzt oder keine Erfahrungen mit Terminalservertechnik gesammelt haben.

**nicht** für Firmen, die keine Hypervisor-Umgebung vorhalten oder über keinerlei Erfahrungen mit Virtualisierung verfügen.

**Kaviza VDI-in-a-Box**



# Im Test: WhatsVirtual 1.0 für Ipswitch WhatsUp Gold

## Virtuelles Management-Schnäppchen

von Jürgen Heyer

Mit über 70.000 verwalteten Netzwerken ist die Management-Software "WhatsUp Gold" weit verbreitet. Neu ist nun das Plugin "WhatsVirtual" für den Zugriff auf virtuelle Serverumgebungen unter VMware. Ziel ist ein integriertes Monitoring und Management physischer und virtueller Systeme von einer Konsole aus. IT-Administrator hat untersucht, wie gut das mit dieser Erweiterung möglich ist, die der Hersteller bestehenden Nutzern zu recht geringen Update-Kosten anbietet.

**M**it WhatsUp Gold ist Ipswitch recht erfolgreich im Markt für Netzwerkmanagement-Software unterwegs. Die Lösung überwacht nicht nur Server, sondern auch alle anderen Netzwerkkomponenten wie Router und Switches, sofern diese SNMP-Abfragen unterstützen. Bei Windows-Servern erfolgt die Kommunikation darüber hinaus mittels WMI. Integriert ist auch ein Anwendungs-Monitoring beispielsweise für Exchange, Microsoft SQL und Windows-Dienste. Diverse Erweiterungen (Flow Monitor, Flow Publisher, VoIP Monitor, Failover Manager), hier Plug-Ins genannt, bauen das Produkt um zusätzliche Funktionen aus. Mit der Version 14.2 kommt das Plug-In WhatsVirtual hinzu, das auch virtuelle Umgebungen auf Basis von VMware ESX sowie ESXi überwachen kann – und zwar sowohl die Hosts als auch die Gastsysteme. Für das Auslesen der Systeminformationen sowie der aktuellen Performedaten nutzt das Programm dann die VMware-API.

Ipswitch adressiert mit dieser Ergänzung in erster Linie bestehende WhatsUp-Nutzer, um die Funktionalität des Produkts zeitgemäß zu erweitern und so zu vermeiden, dass die Bestandskunden sich auf die Suche nach einem alternativen Management für ihre virtuelle Landschaft



Bild 1: In einem umfangreichen Report liefert WhatsUp Gold mit dem Plug-In WhatsVirtual alle wichtigen Performance-Daten sowie eine Liste der auf dem ESX-Host laufenden VMs

machen. Tatsächlich ist es nun prinzipiell möglich, das Werkzeug als zentrale Konsole für das Monitoring und Management sowohl der physischen als auch der virtuellen Systeme einzusetzen.

Entsprechend dem Schwerpunkt dieser Ausgabe haben wir uns bei diesem Test speziell auf die Erweiterung WhatsVirtu-

al konzentriert, weshalb unser Test primär Anwender des Basis-Produkts anspricht. Aber auch Administratoren, die dieses Produkt nicht einsetzen, erhalten einen Überblick über die generelle Funktionsweise. Zum Test stand uns die Version 1.0 von WhatsVirtual in Kombination mit WhatsUp Gold 14.2 zur Verfügung. Noch nicht nutzen konnten wir die Version 2.0 des

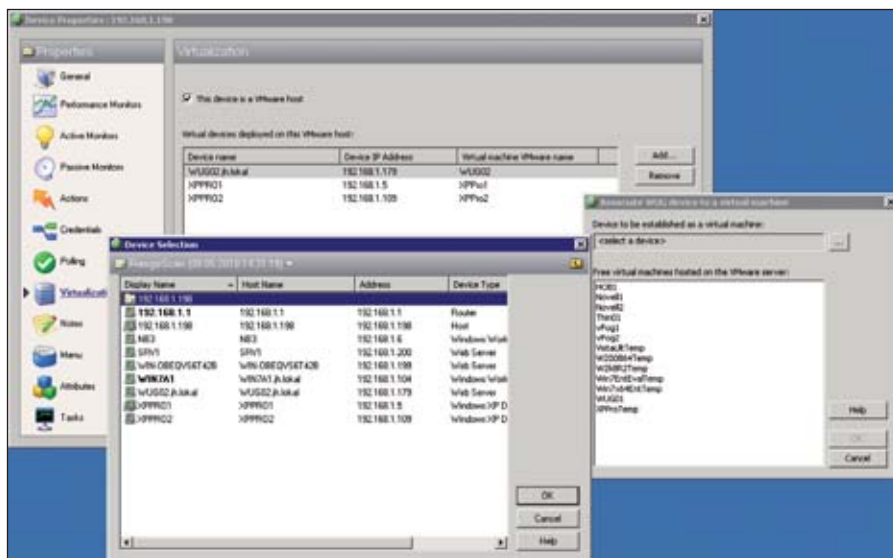


Bild 2: WhatsVirtual liefert automatisch eine Übersicht der VMs auf einem Host, die Zuordnung zu den mittels IP-Scan gefundenen Systemen ist aber manuell durchzuführen

Virtualisierungs-Plug-Ins, die aber zum Testzeitpunkt schon angekündigt war. Deren wichtigsten Neuerungen haben wir weiter unten zusammengetragen.

### Reibungslose Installation und Inbetriebnahme

Für den Test installierten wir WhatsUp Gold Premium 14.2 auf Windows 2008 Server. Das bereitgestellte Setup mit 392 MByte Größe, das nach einer Registrierung auch als voll lauffähige 30-Tage-Testversion heruntergeladen werden kann, umfasst unter anderem auch das Plug-In WhatsVirtual, so dass dieses nicht extra zu installieren ist. Während der Einrichtung sind kaum Abfragen zu beantworten, es lässt sich aber der Port des automatisch mit installierten Web-servers ändern. Als Datenbank lässt sich ein externer SQL-Server nutzen, alternativ installiert das Setup SQL 2005 Express und konfiguriert die notwendige Datenbankinstanz. Bei Nutzung eines externen SQL-Servers ist zu beachten, dass dieser in englischer Sprache installiert sein muss. Insgesamt erweist sich die Installation aber als geradlinig und unproblematisch.

Anschließend startet die WhatsUp Gold-Konsole mit einem Assistenten, der die SMTP-Mail-Konfiguration übernimmt und auch die Anmeldeinformationen abfragt, die später für den Zugriff auf die zu

überwachten Systeme benötigt werden. Da für die Abfrage vieler verschiedener Geräte auch entsprechend unterschiedliche Credentials benötigt werden, ist die Erfassung insofern recht geschickt gelöst, als dass alle diese Informationen in einer Liste eingetragen werden, wobei der Administrator für jeden Eintrag eine sinnvolle Bezeichnung hinterlegen kann. Insgesamt kennt WhatsUp Gold acht unterschiedliche Credential-Typen (SNMP v1, SNMP v2, SNMP v3, Windows, ADO, Telnet, SSH und VMware). Die Software arbeitet komplett agentenlos, so dass auf den überwachten Systemen nichts zu installieren ist. Vielmehr verschafft sie sich alle Informationen durch Remote-Abfragen eben mit Hilfe der genannten Anmeldeinformationen. Nachdem SNMP-Abfragen bei virtualisierten Systemen

nur ungenaue Werte liefern, nutzt WhatsVirtual für den Zugriff auf VMware-Hosts ab ESX 3.0 sowie ESXi 3.5i und höher die auf dem vSphere Web Services-SDK basierende VMware-API, um exakte Kennzahlen in Echtzeit auslesen zu können. Zusätzlichem Aufwand, der bei SNMP-Nutzung entstehen würde, weil VMware mit vSphere das SNMP-Modell geändert hat, geht der Hersteller so von vornherein aus dem Weg. Letztendlich ist der Zugriff über die API auch der bessere, weil zukunftsweisende Weg.

Der nächste Schritt der Inbetriebnahme beinhaltet eine Discovery-Phase, um im Netzwerk Komponenten und ihre IP-Adressen zu ermitteln. Das Programm versucht dabei, den Gerätetyp zu erkennen und ihm eine entsprechende Rolle (Drucker, Router, Server, VMware Host) zuzuweisen. Zusätzlich kann der Administrator bei jedem gefundenen Gerät stets die Eigenschaften manuell anpassen und ergänzen. Hier ordnet er zudem aus der Credential-Liste die passenden Anmeldeinformationen zu. Fehlen Letz-

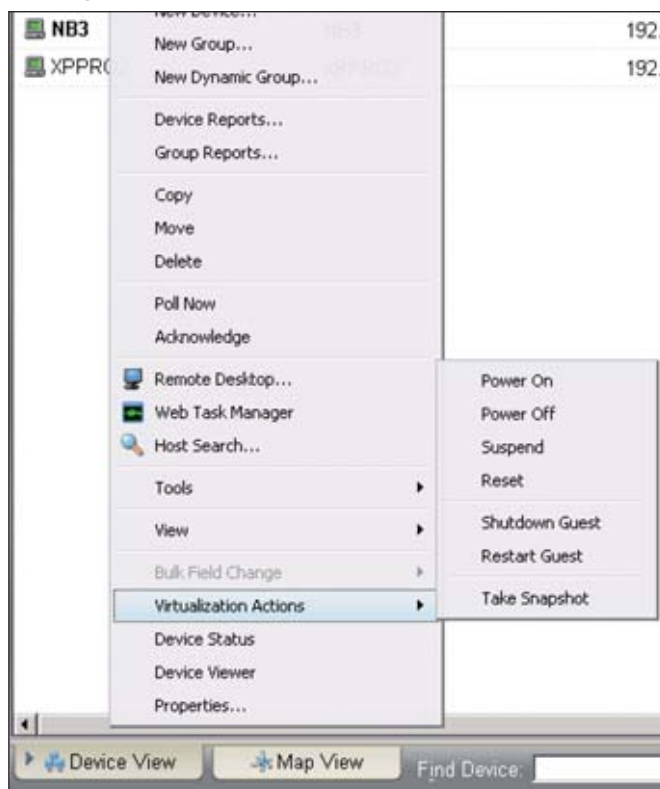


Bild 3: WhatsVirtual ermöglicht typische Aktionen zur Steuerung einer VM, so dass der VMware-Client hierzu nicht extra aufgerufen werden muss



tere noch, kann er diese Liste von hier aus direkt erweitern, was den Arbeitsablauf erleichtert.

### Manuelle Zuordnung von Host und Gast nötig

Das Ergänzen der Eigenschaften bei einem physischen und einem virtuellen Server unterscheidet sich nicht, da beide Typen prinzipiell gleich behandelt werden. Der Administrator kann unter anderem angeben, welchen Performance-Monitor (CPU, Festplatte, Speicher, LAN-Schnittstelle und Ping) er aktivieren will. Nur bei einem VMware-Host sind auf dem Registerblatt "Virtualization" zusätzliche Einträge erforderlich. Hintergrund ist, dass WhatsUp Gold bei einem Host zwar die Liste der aktuell dort laufenden VMs ausliest, aber die Zuordnung zwischen diesen und den über den IP-Scan gefundenen Systemen nicht automatisch vornehmen kann.

Vielmehr muss der Administrator über das genannte Registerblatt aus zwei Listen das mittels IP gefundene Gerät sowie eine freie (noch nicht zugeordnete) VM auswählen und zuordnen. Wer viele VMs betreibt, kann sich hier auf einige Arbeit freuen, wobei dies pro VM ein einmaliger Vorgang bleibt. Allerdings wiederholt er sich immer dann, sobald neue VMs in Betrieb genommen werden. Eine Zuordnung über die Seite der Eigenschaften eines Gastsystems ist übrigens nicht möglich, diese muss immer über den Host erfolgen, was den Ablauf etwas umständlicher als notwendig gestaltet.

Wer bisher aufmerksam mitgelesen hat, dem dürfte auffallen, dass noch an keiner Stelle das VMware Virtual Center erwähnt wurde. Tatsächlich ist es so, dass zum aktuellen Zeitpunkt die Version WhatsVirtual 1.0 das vCenter noch nicht direkt unterstützt. Dies bedeutet im Detail, dass eine Änderung der Zuordnung zwischen einem Host und den darauf laufenden Gastsystemen nicht automatisch erkannt wird. Vielmehr ist es notwendig, die Zuordnungen durch einen erneuten Netzwerkscan zu aktualisieren, damit die Inhalte der genutzten dynamischen Gruppen angepasst werden. Glückli-

Bild 4: Für jeden ESX-Host liefert WhatsVirtual eine detaillierte Übersicht über den Ressourcenbedarf der darauf laufenden VMs

cherweise lässt sich dieser Prozess automatisieren, so dass sichergestellt ist, dass es zumindest in regelmäßigen Abständen zu einer Aktualisierung dieser Informationen kommt. Mit Version 2.0 sollen dann vCenter und vMotion in vollem Umfang Unterstützung erfahren, um Verlagerungen von VMs innerhalb einer Farm in Echtzeit verfolgen zu können. Angekündigt sind auch ein High Availability Support, um Verlagerungen aufgrund von Hardware- oder Betriebssystemausfällen besser nachvollziehen zu können, sowie das komplette Management virtueller Cluster.

Über die Konsole kann der Administrator grundlegende Aktionen (Ein- und Ausschalten, Suspend, Reset, Snapshot erstellen) für VMs veranlassen, so dass es nicht notwendig ist, hierfür den vSphere-Client zu starten. Zusätzliche Möglichkeiten ergeben sich dadurch, dass sich derartige Aktionen über einen Scheduler auch automatisieren oder regelmäßig wiederholen lassen. Es ist also beispielsweise möglich, in Verbindung mit WhatsUp Gold einzelne VMs gezielt herunterzufahren oder zu starten, wenn sie nicht rund um die Uhr benötigt werden. Ebenso lassen sich bei Bedarf regelmäßig Snapshots erzeugen. Auch kann der Nutzer eine Aktion mit einer Bedingung koppeln, um beispielsweise eine VM herunterzufahren, wenn deren Auslastung unter einen bestimmten Wert fällt – was auf einen Leerlauf schließen lässt.

### Anschauliche und detaillierte Host-Informationen

Bezüglich der VMs liefert WhatsUp Gold erst einmal prinzipiell die gleichen Infor-

mationen wie bei einem physischen Server. Bei Betriebssystem-spezifischen Abfragen muss die Software nicht unterscheiden und dies funktioniert auch schon ohne das WhatsVirtual Plugin. Allerdings kommen zu den bereits vorhandenen Leistungs-Monitoring-Reports für physische Server noch weitere Workspace-Reports für die physischen VMware-Host-Server und die darauf laufenden VMs hinzu. So liefert der Virtual Host List-Report eine Übersicht über die Host-Server und die darauf laufenden VMs. Weitere Ansichten zeigen die aktuelle Konfiguration mit den entsprechenden Versionsnummern an sowie die Nutzungsdaten für CPU, Arbeitsspeicher und Netzwerkanbindung. Das Plug-In liefert den aktuellen Wert sowie Minimal- und Maximalwert, den Durchschnitt und ein Verlaufsdigramm, so dass sich auch Änderungen recht gut beobachten lassen. Ein Administrator kann so auf einen Blick die Auslastung der Hardware schnell erkennen.

**Log.in consultants**

**Log-into success – join the Team!**  
Für unser junges motiviertes Team suchen wir weitere

**Junior Consultants/Consultants**

Wir bieten Ihnen spannende und innovative SBC- und Virtualisierungsprojekte sowie attraktive Entwicklungschancen.

Interessiert?  
Dann freuen wir uns auf Ihre Bewerbung unter [job@loginconsultants.de](mailto:job@loginconsultants.de).

[www.loginconsultants.de](http://www.loginconsultants.de)



Für den Plattenspeicher des Hosts zeigt WhatsUp Gold den Füllgrad absolut sowie prozentual an. Zudem liefert das Programm für einen Host eine genaue Übersicht, welche der VMs welche Ressourcen beansprucht, um so leichter die Auslastung und die Verteilung zu erkennen. Dies umfasst mehrere Listen aller VMs auf einem Host mit ihrem Zustand (Online, Suspended, Powered Off) und deren CPU-, RAM-, Plattenspeicher- und Netzauslastung als aktuellen Wert, Spitzenwert der letzten Stunde sowie Stundendurchschnitt.

Bei Verlaufsdiagrammen wählt WhatsUp Gold standardmäßig ein Zeitfenster von vier Stunden, der Bereich lässt sich aber hinsichtlich Start- und Endzeit jederzeit frei definieren. Auch für die Darstellungsart stehen verschiedene Modi zur Verfügung (unter anderem Linien, Balken und Flächen in 2D und 3D). Das Werkzeug kommt mit einer beeindruckenden Vielzahl an bereits vorbereiteten Ansichten und Reports, die ein Administrator ohne weitere Vorarbeit nutzen kann. Selbstverständlich kann er darüber hinaus auch eigene Ansichten und Reports erzeugen. Recht intuitiv erweist sich in diesem Zusammenhang die gesamte Bedienung, da die verschiedenen Ansichten konsequent miteinander verlinkt sind. So kann der Nutzer beispielsweise in der VM-Übersicht eines Hosts auf einen Eintrag klicken und kommt so direkt auf die Geräte-spezifische Ansicht der jeweiligen virtuellen Maschine.

Was wir bei WhatsVirtual vermissen, sind Simulationsmöglichkeiten für Szenarien, um dem Administrator beim Betrieb mehrerer Hosts Hinweise zu geben, welche VMs sich aufgrund ihres Lastverhaltens gut auf einem Host gemeinsam betreiben lassen. Auch liefert die Software keine Wachstumsprognosen, um aufgrund der historischen Lastentwicklung vorherzusagen, wann ein Host an seine Lastgrenzen stoßen dürfte beziehungsweise wann eine Erweiterung sinnvoll sein dürfte. Hier ist jedoch zu berücksichtigen, dass sich WhatsVirtual mit Version 1.0 quasi noch


in der Einführungsphase befindet und schon in der nächsten Version größere Funktionserweiterungen zu erwarten sind.

Vorteilhaft ist, dass das Plug-In eine Integration mit dem WhatsUp Gold Alert Center beinhaltet. Dies erlaubt es dem Administrator, für ESX-Hosts und VMs ebenso wie für die physischen Maschinen Warnungen und Eskalationsstufen zu definieren sowie Schwellwerte zu konfigurieren, um sich beim Überschreiten benachrichtigen zu lassen. So kann das Management-Tool bei einem unternehmensweiten Einsatz die Informationen aus der gesamten Infrastruktur erfassen und bietet somit eine zentrale Konsole für die Verwaltung aller Geräte und Komponenten im Netz sowie eine übergreifende Alarmierung.

### Fazit

Mit der Ergänzung WhatsVirtual befindet sich Ipswitch auf dem richtigen Weg, um die Netzwerkmanagement-Software WhatsUp Gold sinnvoll und zeitgemäß zu erweitern. Nun ist es auch möglich, VMware ESX/ESXi-Hosts mit zu überwachen sowie die Beziehungen zwischen den Hosts und den virtuellen Gastsystemen zu verwalten. Noch nicht unterstützt wird allerdings VMware Virtual Center, so dass sich entsprechende Bewegungen von VMs innerhalb einer Farm nur mit einer gewissen Verzögerung durch einen erneuten Netzwerkscan nachvollziehen lassen. Mit der Version 2.0, die bereits angekündigt ist, soll der vCenter-Support allerdings kommen.

Administratoren, die bei ihrer Netzwerküberwachung bereits auf WhatsUp Gold setzen, sollten sich für die Verwaltung ihrer virtuellen Umgebung unter VMware dieses neue PlugIn genauer ansehen. Damit ist es möglich, physische und virtuelle Systeme sowie ESX-Hosts über alle Ansichten und Reports hinweg gleichermaßen nebeneinander zu überwachen, zu steuern und bei Ausfällen oder Schwellwertüberschreitungen eine Alarmierung zu veranlassen.

Sehr interessant ist in diesem Zusammenhang auch der Preis, denn Ipswitch verlangt für das Plug-In nur 1.270 Euro, unabhängig davon, wie groß die Umgebung ist. Käufer der 1.0-Version erhalten das Upgrade auf 2.0 kostenlos. Damit ist die Erweiterung für Bestandskunden auf jeden Fall weitaus interessanter als der Blick auf ein anderes, zusätzliches Produkt zum Management und Monitoring der virtuellen Landschaft. (In) 

#### Produkt

Erweiterung zum Monitoring und Management von virtuellen Umgebungen unter VMware.

#### Hersteller

Ipswitch  
<http://de.whatsupgold.com>

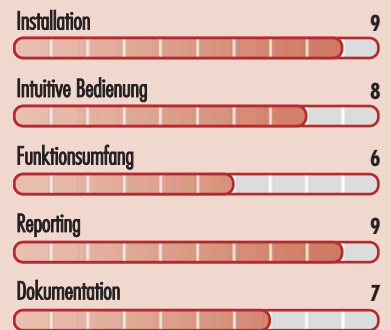
#### Preis

Das Plug-In WhatsVirtual kostet einmalig 1.270 Euro, unabhängig von der Größe der überwachten Umgebung.

#### Technische Daten

[www.it-administrator.de/downloads/datenblaetter](http://www.it-administrator.de/downloads/datenblaetter)

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



#### Dieses Produkt eignet sich

**optimal** als preisgünstige Erweiterung für (teilweise) virtualisierte Umgebungen, in denen bereits WhatsUp Gold eingesetzt wird.

**bedingt** für Umgebungen, in denen WhatsUp Gold nicht zum Einsatz kommt, da dieses dann erst eingeführt werden muss. In solch einem Fall empfiehlt sich zuerst ein Vergleich mit anderen Produkten für das Management virtueller Umgebungen.

**nicht**, falls ein Unternehmen nicht auf eine Virtualisierung mit VMware setzt.

**WhatsVirtual 1.0 für Ipswitch WhatsUp Gold**



**Im Kurztest: CoGen eBoostr 4.0**

# Nachrüstbarer Turbolader

von Sandro Lucifora

Die Cache-Technik ReadyBoost ist mittlerweile von Windows 7 und Vista gut bekannt. Hierbei werden die sonst auf der Festplatte abgelegten Systemdaten auf schnellere Flash-Speicher – etwa USB-Sticks – ausgelagert. Durch die im Vergleich zum Magnetspeicher wesentlich schnelleren Zugriffszeiten erreicht Microsoft eine deutliche Geschwindigkeitssteigerung. eBoostr 4.0 ist ein Windows-Utility, das die ReadyBoost-Funktion unter XP und Windows Server bereitstellt. Ob der Rechner mit dem Tool auch wirklich durchstartet, haben wir in einem Test für Sie herausgefunden.

**I**n unserem Test konzentrierten wir uns auf den Einsatz unter Windows Server 2008 (32 Bit) und Windows Server 2003 (64 Bit). Unter 2008 laufen ein File- und MS SQL-Server, der Windows 2003-Server beherbergt den VMware Server 2.0 mit zwei virtuellen Maschinen. Beide Umgebungen sind jeweils mit 4 GByte Hauptspeicher ausgerüstet.

Die Installation war schnell erledigt. Im Test verwendeten wir zwei USB-Sticks: einen mit FAT32 formatierten 2 GByte-Speicher und einen 1 GByte-Stick mit NTFS. Die eBoostr-Funktion, ein neues Laufwerk als Cache-Speicher hinzuzufügen, prüft zunächst, ob das angeschlossene Gerät geeignet ist. Die Voraussetzung dafür ist ein USB 2.0-Stick mit mindestens 256 MByte freiem Speicher und einer Lesegeschwindigkeit von 2,5 MByte/s. Nachdem die Software die Flash-Speicher akzeptiert hatte, haben wir auf den Sticks jeweils die größtmögliche Cachespeicher-Datei angelegt.


Nach dem Start des Werkzeugs erschien uns der Zugriff subjektiv erst einmal nicht schneller. Nach kurzer Betriebszeit jedoch konnten wir objektiv eine Leistungssteigerung messen. Es beansprucht einfach etwas Zeit, bis die Daten vom Festplatten in den USB-Cache verlagert werden. Über die Prioritäten-Liste haben wir bestimmte Anwendungen gezielt beschleunigt. So

konnten wir neben den Instanzen des MS SQL-Servers auch dem VMware-Server einen Turbo verpassen. Parallel dazu haben wir in der Ausschluss-Liste unnötige Dateien vom Zwischenspeichern ausgeschlossen. Nach vier Wochen durchgehendem Betrieb konnten wir eine Leistungssteigerung von über 70 Prozent feststellen. Komplexe SQL-Queries wurden teilweise um bis zu 80 Prozent schneller ausgeführt als mit ausgeschaltetem Cache-Speicher – dabei haben wir vorher natürlich immer wieder auch den SQL-Cache gelöscht und die Instanz neu gestartet. Der Start des Internet Explorer 7 beschleunigte sich von zwölf auf acht Sekunden.

Außer auf den Servern haben wir eBoostr unter Windows XP 32 Bit mit 4 GByte Hauptspeicher getestet. Windows 32 Bit kann maximal 3 GByte Hauptspeicher adressieren und lässt so 1 GByte des Test-PCs ungenutzt. Der Hersteller verspricht, mit eBoostr auch den "versteckten Speicher" als Cache nutzen zu können. Auf dem Arbeitsplatz konnten wir auf diese Weise zum Beispiel den Start von Adobe Photoshop CS3 um bis zu acht Sekunden beschleunigen und die Arbeit mit großen Bilddaten verlief insgesamt flüssiger.

## Fazit

Unser Praxis-Test hat ergeben, dass eBoostr funktioniert. Dabei zeigte nicht

nur der Software-eigene Performance-Test eine Steigerung, sondern auch wir konnten mit objektiven Messungen sehr schnell einen Unterschied feststellen. Nicht nur Windows Server bekommt mit dem Utility einen Turbo verpasst, gerade bei 32-Bit-Systemen erweist sich das Tool als äußerst hilfreich. (In) 

### Produkt

Software zur Beschleunigung von Windows, die ausgelagerte Dateien auf einen USB-Stick zwischenspeichert.

### Hersteller

CoGen Media – [www.eboostr.com](http://www.eboostr.com)

### Preis

30 Euro für die PRO-Version

### Technische Daten

[www.it-administrator.de/downloads/datenblaetter](http://www.it-administrator.de/downloads/datenblaetter)

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

Aufwand der Konfiguration **9**



Umsetzung **8**



Handhabung **10**



Zuverlässigkeit **10**



Kosten-/Nutzen **8**



**CoGen eBoostr 4.0**



Quelle: aris - Fotolia.com

# Möglichkeiten von Virtual Desktop Infrastructures Nicht ohne mein Clientmanagement!

von Martin Kuppinger

Desktop-Virtualisierung ist ein Hype-Thema in der IT. Doch mit der technischen Bereitstellung von wenigen standardisierten Images ist es nicht getan. In diesem Artikel beschäftigen wir uns mit den Vor- und Nachteilen von Virtual Desktop Infrastructures und erklären Ihnen, warum sich erst im Zusammenspiel mit dem Client Lifecycle Management, also klassischen Systemmanagement-Funktionen, die Anforderungen der meisten IT-Umgebungen sinnvoll bedienen lassen – in einer Kombination von virtuellen und anderen Desktops.

**V**DI (Virtual Desktop Infrastructures) sind die Software-Lösung, mit der die Infrastruktur für die Bereitstellung von virtuellen Desktops geschaffen wird. Virtuelle Desktops zeichnen sich zunächst dadurch aus, dass sie als ein Image definiert sind, welches sich als virtuelle Maschine auf einem Hypervisor ausführen lässt. Diese Images werden zentral auf Servern bereitgestellt. Dabei erfolgt typischerweise eine Aufteilung in mehrere Elemente – Betriebssystem, Anwendungen und die benutzerspezifischen Profile werden getrennt. Dieses Splitting sorgt für weniger Speicherbelastung. Außerdem lassen sich Änderungen leichter auf die einheitlichen Teile von Images anwenden.

## **VDI wird als Allheilmittel verkauft**

VDIs sollen durch die Virtualisierung von Desktops zu einfacheren Umgebungen führen. Das zentrale Management der Desktops erhöht – so das Mar-

keting der entsprechenden Anbieter – deren Verfügbarkeit und erleichtert das Management. Benutzer könnten von unterschiedlichen Systemen aus auf ihre virtuellen Desktops zugreifen und diese beispielsweise auch vom Heimarbeitsplatz aus nutzen. Außerdem sollen VDIs durch die zentrale Bereitstellung und das zentrale Management die Sicherheit der Arbeitsumgebungen erhöhen. Diese Argumente sind jedoch alle nicht neu. Die meisten davon wurden bereits schon für das Client Lifecycle Management, also den Client-bezogenen Teil des Systemmanagements mit Softwareverteilung und anderen Funktionen, hervorgehoben. Außerdem wurden sie für die Terminaldienste ins Feld geführt. Doch VDIs lösen, soviel schon vorab, keineswegs alle Probleme in allen Anwendungsfällen.

## **Probleme bei der Anbindung mobiler Nutzer**

Interessant wird es bei der Frage, wie die Nutzer die Desktops verwenden können. Die derzeit übliche Zugriffsform sind Remote Desktop-Protokolle, also die gleichen Standards, die auch für den Zugriff

auf Terminaldienste verwendet werden. Dabei läuft der Desktop auf dem Server, während die Präsentationsschicht auf dem Client abgebildet wird. Die Anbieter von VDIs haben in den vergangenen Monaten intensiv daran gearbeitet, die Einschränkungen wie das Zusammenspiel mit lokalen Anwendungen und Geräten oder die Darstellung von Videos und Flash zu optimieren. Dennoch muss sich jeder darüber im Klaren sein, dass dieser Ansatz im Vergleich zur lokalen Ausführung des Desktops immer funktionale Einschränkungen haben wird.

Darüber hinaus hat der Ansatz zur Folge, dass der Zugriff eine Verbindung zum Server voraussetzt. Im Umkehrschluss heißt dies, dass diese Variante für mobile Benutzer nicht geeignet ist. Dort, wo keine zuverlässige Verbindung möglich ist, also beispielsweise auf Reisen, funktioniert das Konzept schlicht nicht. Die VDI-Anbieter sind inzwischen dabei, dieses Problem durch andere Deployment-Varianten zu adressieren, bei denen das Image auf einem lokalen Hypervisor ausgeführt wird. Diese Variante sieht das Streaming des Images zu Be-



ginn der Session vor – was eine relativ große Bandbreite und eine intelligente Bereitstellung des Images erfordert, um die Wartezeiten zu reduzieren. Auch hier gilt also im Regelfall, dass mobile Benutzer außen vor sind.

Die neuesten Ansätze wollen mobile Anwender mit synchronisierten Images versorgen, die ebenfalls auf einem lokalen Hypervisor ausgeführt werden, dort aber nach einmaliger Installation persistent sind. Änderungen müssen für das Roaming der Images auf andere Clients und das zentrale Management mit den zentralen Images in der VDI synchronisiert werden – auch das ist eine Herausforderung.

Letztlich bedeutet dies, dass VDIs zum heutigen Stand ein nur unwesentlich besseres Ergebnis für den Endanwender liefern als Terminaldienste. Und besser ist das Ergebnis eigentlich nur, weil die Protokolle bei VDIs bereits erweitert wurden. Citrix beispielsweise will aber die Funktionalität für die bei den Terminaldiensten verwendeten Protokolle beim nächsten Release wieder auf den gleichen Stand bringen. Derzeit lassen sich diverse Anwendungsszenarien mit VDIs nicht sinnvoll abdecken. Dazu zählen anspruchsvolle grafische Anwendungen ebenso wie der bereits erwähnte mobile Benutzer.

### Steigende Komplexität

An dem Versprechen, Desktops einfach bereitzustellen, müssen sich VDIs messen lassen. Wie bei allen vergleichsweise neuen technischen Ansätzen ist hier noch viel Bewegung im Markt. Der aktuelle Trend ist die Integration verschiedener Virtualisierungs-Ansätze und die Reduzierung der Anzahl an Management-Schnittstellen. Gemeinsame Schnittstellen für das Management der virtuellen Server und der virtuellen Desktops finden sich bei immer mehr Anbietern. Grundsätzlich gilt, dass es im Bereich dieser Schnittstellen durchaus noch Luft nach oben gibt. Die Kom-

plexität der Umgebungen sollte nicht unterschätzt werden.

Dabei fokussieren sich die VDI-Anbieter heute üblicherweise auf das Management der Images selbst, teilweise mit einer grundlegenden Unterstützung für die Erstellung von individualisierten Images und Funktionen für die Steuerung von wesentlichen Profileinstellungen. Im Vergleich zu den etablierten Lösungen im Bereich des Client Lifecycle Managements gibt es aber doch erhebliche Unterschiede bezüglich der Leistungsfähigkeit für die effiziente und nachvollziehbare Erzeugung und Anpassung einer größeren Zahl von Images und ihrer Befüllung mit Software ebenso wie der Anpassung von Konfigurationseinstellungen. Darauf haben die Anbieter aber zumindest insofern reagiert, als dass eine wachsende Zahl der VDIs über Schnittstellen zu Client Lifecycle Management-Lösungen verfügt und Hersteller wie beispielsweise Citrix oder Kaviza hier auf Partnerschaften setzen.

### Herausforderung für das Rechenzentrum

Nicht unterschätzt werden sollte zudem die Lastverlagerung ins Rechenzentrum. Zahlen von Citrix gehen davon aus, dass sich auf aktueller Server-Hardware pro System rund 125 virtuelle Desktops hosten lassen – im Vergleich zu 500 Sessions mit Terminaldiensten. Ein deutlich anderes Bild ergibt sich beim lokalen Deployment, wo Citrix von bis zu 5.000 Benutzern ausgeht, an die Desktops geliefert werden können. Hier dürfte der Engpass aber oft ohnehin eher auf der Seite des Netzwerks als beim Server liegen.

Diese Zahlen machen deutlich, dass der Schritt hin zu VDIs zwangsläufig bedeutet, dass der Aufbau und die Verwaltung einer hoch skalierbaren Server-Infrastruktur Pflicht ist. Ohne vorher die Hausaufgaben bei der Server- und Storage-Virtualisierung gemacht zu haben, werden sich kaum erfolgreich VDIs aufsetzen lassen. Und selbst dann ist zu be-

achten, dass VDIs mit zentral ausgeführten Desktops unter dem Aspekt der erforderlichen Server-Hardware und damit der Kosten durchaus kritisch zu betrachten sind.

### Die Alternativen: Lokale Desktops und Terminaldienste

Es ist keineswegs so, dass sich die Herausforderungen nicht auch mit etablierten Ansätzen angehen ließen. Lokale Desktops können Netzwerk-Verantwortliche mit Client Lifecycle Management-Lösungen durchaus im Griff behalten. Natürlich gibt es hier Grenzen – lokale (zumindest temporäre) Konfigurationsänderungen oder die größere Hardware-Vielfalt sind hier zu nennen. Terminaldienste können ebenfalls zentral Desktops bereitstellen. Das funktioniert durchaus gut, auch wenn es in einer Multi-User-Umgebung ebenso einige Einschränkungen gibt wie durch die Remote Desktop-Protokolle.

Dennoch ist der Wert dieser Ansätze nicht zu unterschätzen. Terminaldienste sind etabliert und es gibt sehr viele erfahrene Dienstleister ebenso wie unzählige Add-On-Tools dafür. Lokale Desktops bieten letztlich die größte Flexibilität für Benutzer. Dies sollte nicht vergessen werden – gerade mit Blick auf die anspruchsvolleren Benutzergruppen, die spezielle Anwendungen oder eine größere Flexibilität bei der Konfiguration

- Ist genügend Erfahrung für das Management der Server-Backends bei VDIs vorhanden?
- Ist die Verantwortung geregelt für das, was innerhalb der Images geschieht?
- Passen die Anwendungsszenarien überhaupt zum aktuellen Stand der VDI-Lösungen (mobile Benutzer, komplexe Applikationen)?
- Was wird das Unternehmen in Zukunft überhaupt noch selbst für die IT bereitstellen?
- Funktionieren weitere Elemente wie Endpoint Security Management, Contract Management, License Management oder Konfigurationsmanagement?

Das sollten Sie bei VDIs beachten





### Ansätze zur Desktop-Bereitstellung im Vergleich

	Management	Deployment	Runtime	Desktop-Zugriff	Mobile Nutzung
<b>Desktop Virtualization mit Remote Desktop</b>	Server	Server	Server	Remote Desktop Protocol (RDP, ICA, ...)	Online
<b>Desktop Virtualization mit lokalem Image</b>	Server	Lokal, beim Start oder synchronisiert	Lokal	Lokal	Online und Offline (bei Synchronisierung)
<b>Terminal Services</b>	Server	Server	Server	Remote Desktop Protocol (RDP, ICA, ...)	Online
<b>Lokale Installation</b>	Lokal (oft mit zentralen Tools)	Lokal	Lokal	Lokal	Online und Offline

ihrer Desktop-Umgebungen benötigen oder zumindest einfordern. Übersehen werden darf weiterhin nicht, dass es immer mehr zu verwaltende Zielumgebungen gibt. Andere Betriebssysteme wie Mac OS X und Linux und zusätzliche Geräteklassen wie Smartphones oder das iPad sollten beim strategischen Blick auf das Desktop-Management nicht ignoriert werden.

#### Effektives Management von Desktops ist gefragt

Neben der Heterogenität an Zielumgebungen ist die Vielfalt der Verwaltungsfunktionen nicht zu unterschätzen, die abgedeckt werden muss. Mit dem Management der VDI selbst und der Images ist es nicht getan – und auch

die Unterstützung bei der Erstellung von Images reicht nicht aus. Es wird auf längere Sicht bei virtuellen Desktops die Notwendigkeit geben, in bestimmten Situationen Anwendungen in das Image zu installieren oder es zu deinstallieren – vor allem für die Benutzer mit etwas spezielleren Anforderungen. Einiges lässt sich zwar zentral reaktivieren, zum Teil bis hin zum Patch-Management. Aber wenn es darum geht, Anwendungen flexibel bereitzustellen, spielt die klassische Softwareverteilung weiterhin eine Rolle, trotz der Anwendungs- und Desktop-Virtualisierung (siehe Kasten “Anwendungs- und Desktop-Virtualisierung im Zusammenspiel”).

Noch offensichtlicher wird dies bei Themen wie der Inventarisierung und dem Lizenz-Management ebenso wie beim Asset- und Contract-Management. Diese Funktionen werden durch VDIs heute noch nicht abgedeckt. Hier braucht es also weiterhin die ergänzenden Werkzeuge aus dem Client Lifecycle Management. Aber selbst wenn es um die effiziente Erstellung einer etwas größeren Zahl von Images geht, haben diese ihren Platz.

#### Die Strategien der Anbieter

So ist es nicht verwunderlich, dass die meisten Anbieter im Client Lifecycle Management-Markt inzwischen in der einen oder anderen Form VDIs unterstützen – und einige Anbieter bereits konkrete Partnerschaften mit VDI-An-

bietern haben. Die Schweizer Brainware AG unterstützt derzeit Funktionen wie die Inventarisierung, das Lizenzmanagement und ein zentralisiertes Patchmanagement, aber auch die Softwareverteilung in virtualisierten Umgebungen. In der Pipeline sind weitere Funktionen wie die automatische Erzeugung von virtuellen Desktops und die Paketierung von virtuellen Anwendungen, integriert mit den standardmäßigen Paketierungsfunktionen. Zudem steht das Management von Thin Clients, also der Schicht unterhalb von Client-Hypervisoren, auf der

Eine immer wieder gestellte Frage ist die nach dem Zusammenhang zwischen Desktop- und Anwendungsvirtualisierung. Die Anwendungsvirtualisierung liefert paketierte Anwendungen, die in einer Art “Sandbox” auf dem Client ausgeführt werden. Das funktioniert heute mit vielen, aber noch nicht mit allen Anwendungen. Unter dem Effizienzgesichtspunkt ist die Anwendungsvirtualisierung insbesondere für die Bereitstellung von Applikationen interessant, die nur zeitweise und nur von begrenzten Benutzergruppen benötigt werden. Programme, die ohnehin jeder benötigt, lassen sich effizienter direkt in das Image installieren. Außerdem ist immer daran zu denken, dass auch die Anwendungsvirtualisierung mit Funktionen für die Paketierung von Anwendungen, das Lizenzmanagement und die Inventarisierung integriert werden muss, um die Anforderungen von Anwenderunternehmen abzudecken – sie kann also ebenso wenig isoliert vom Client Lifecycle Management betrachtet werden wie die Desktop-Virtualisierung.

VDIs werden im Zusammenspiel mit dem Cloud Computing zukünftig an Bedeutung gewinnen. Die Möglichkeit, sowohl komplette Images als auch virtualisierte Anwendungen von externen Anbietern zu beziehen und die Erstellung ebenso wie das Management der Desktops zu externalisieren, ist dabei sowohl für MSPs (Managed Service Providers) von größeren Unternehmen sowie für Dienstleister im KMU-Umfeld interessant. Die Lieferung vollständiger Systeme mit Branchen- und Office-Lösungen beispielsweise für Handwerker ist nur ein Beispiel. Mit wachsenden Bandbreiten und fortschreitender Reife von VDI-Technologien werden hier wohl schnell entsprechende Geschäftsmodelle umgesetzt werden.

#### VDIs und die Cloud



#### Anwendungs- und Desktop-Virtualisierung im Zusammenspiel





**PROFILE  
MIGRATOR**  
by sepago®

#### Ihr Vorteil

- hohe Business-Kontinuität
- Benutzereinstellungen bleiben erhalten
- kein zusätzlicher Aufwand für den User Help Desk
- reine Freude über den neuen Desktop



## Migrieren Sie Benutzereinstellungen!

**Nutzen Sie Profile Migrator für eine vereinfachte Migration auf...**

- Windows 7
- Windows Server 2008 (R2)
- 64-Bit-Betriebssysteme
- virtuelle Desktops und Server



**DOWNLOAD  
TRIAL-VERSION**



WEITERE INFORMATIONEN UNTER

**[www.profilemigrator.com](http://www.profilemigrator.com)**

oder Telefon +49 [0]221-801 93 95-12

Roadmap. Matrix42 bietet für die VDIs von Citrix und Kaviza jeweils eine Desktop Virtualization Suite an. Im Mittelpunkt stehen dabei Portale für IT-Shops, über die die Benutzer die erforderlichen IT-Dienste anfordern können und anschließend die spezifische virtuelle Umgebung erhalten. Dazu gehören Funktionen wie die Erstellung von virtuellen Images, die Sicherung der Profilinformatoren und die Softwareverteilung und Inventarisierung.

FrontRange Solutions (ehemals Enteo) hat noch für 2010 ein Release angekündigt, in dem klassische und virtualisierte Umgebungen vollständig integriert verwaltet werden können. CA hat seinen IT Client Manager um die Unterstützung für virtuelle Anwendungen erweitert. Für die Erstellung und Verwaltung solcher Applikationen gibt es ebenfalls Werkzeuge. Auch hier geht es also darum, die Verwaltung von physischen und virtuellen Desktops in einem System zu integrieren. Symantec hat in seine Endpoint Virtualization Suite zwar einige Funktionen wie das Lizenzmanagement und die flexible Bereitstellung von Anwendungen integriert, aber noch keine engere Integration mit seinen Altiris-Produkten für das Client Lifecycle Management umgesetzt – hier sind die weiteren Entwicklungen mit Spannung abzuwarten.

Auch Quest fokussiert sich derzeit noch eher auf die VDI selbst als auf die Integration mit dem Client Lifecycle Management. Baramundi hat bereits einige Funktionen im Bereich der Softwareinstallation und des Patch-Managements verfügbar. In Planung sind erweiterte Dienste für das Management von Images und die Integration des Patch-Managements mit den Master-Images.

### **Client Lifecycle Management als strategisches Kernelement**

Die generelle Stoßrichtung der Client Lifecycle Management-Anbieter ist klar: Sie möchten sich als die zentrale Schicht für das Desktop-Management positionieren – und VDIs als eine Deployment-Option sehen. Das macht durchaus Sinn, da die meisten Unternehmen auf längere Sicht noch Terminaldienste und lokal installierte Desktops nutzen werden und ein integriertes Management über alle Desktops hinweg damit eine Grundanforderung bleibt. Dies gilt besonders für die Inventarisierung und das Lizenzmanagement, aber auch für die erforderliche Flexibilität bei der Konfiguration von virtuellen Desktops über ein paar Standard-Images hinaus.

Daher ist davon auszugehen, dass – wie einige der Hersteller-Roadmaps schon zeigen – relativ schnell weitere Schnittstellen zu VDIs in den Client Lifecycle Management-Produkten zu finden sein werden. Abzuwarten bleibt, ob VDI-Anbieter vermehrt solche Hersteller akquirieren, um die Funktionalität der VDIs zu erweitern und eine vollständige, integrierte Lösung anbieten zu können.

### **Fazit**

Heißt das alles nun, dass VDIs eigentlich (noch) überflüssig sind? Sicher nicht. Richtig ist vielmehr, dass IT-Verantwortliche den taktischen Nutzen von VDIs durchaus kritisch betrachten müssen und die Lösung auch strategisch nur ein (zunehmend wichtiges) Element bei der Bereitstellung und dem Management von Desktops ist. Im Laufe der Zeit werden immer mehr Desktops auf Hypervisoren ausgeführt werden.

Ohne das adäquate Management dieser Umgebung selbst und der damit einhergehenden langjährigen Migrationsphase hin zu einer vollen VDI-Infrastruktur werden sich aber die Effizienzvorteile, die VDIs in vielen Szenarien bieten, nicht nutzen lassen. Daher ist eine Entscheidung über VDIs nicht nur eine rationale – nämlich welcher Teil der Desktops sich heute und in naher Zukunft wirklich effizient dadurch abdecken lässt – sondern es sollte stets über die Integration mit dem Client Lifecycle Management nachgedacht werden. (In)



## VMware ESX4 über die Kommandozeile verwalten

# Steuerung per Tastendruck

von Dennis Zimmer

Spätestens bei der Automatisierung, Fehlersuche oder tiefgehenden Sicherheitseinstellungen ist der Weg über die Kommandozeile unumgänglich. Das ist im VMware-Umfeld nicht anders und jeder Administrator sollte zumindest ein Grundverständnis der Befehlszeile haben. In diesem Workshop gehen wir auf die wichtigsten Kommandozeilenmöglichkeiten und Werkzeuge wie VMware vMA, vCLI, PowerCLI und natürlich die lokale Konsole ein. Außerdem erhalten Sie ein Verständnis vom Aufbau der Dateisysteme und den wichtigsten VMware-spezifischen Dateien.

**D**ie ersten Erfahrungen mit der Kommandozeile sammelt ein Administrator schon während und auch nach der Installation des VMware ESX Servers. Allerdings unterscheiden sich ESX und ESXi in dieser Beziehung deutlich voneinander, da weder die Anpassungsmöglichkeiten während der Installation noch die spätere Kommandozeile bei ESXi sehr umfangreich sind. Sie können allerdings mit einem kleinen Trick – der keinen offiziellen Support von VMware genießt – auch unter ESXi auf die lokale Kommandozeile gelangen, wie Sie später sehen werden.

Allgemein ist zu sagen, dass VMware immer mehr Funktionalität in der grafischen Oberfläche und in den Tools vCLI und PowerCLI unterbringt, um die lokale Kommandozeile überflüssig zu machen. Dies ist in weiten Teilen auch gelungen, allerdings ist vor allem beim Troubleshooting immer noch der Weg über die lokale Konsole einzig zielführend. Beispiele hierfür wären die Protokolldateien und Konfigurationssoftware der VMware HA-Funktion. Ein weiterer Aspekt ist die Geschwindigkeit und Einfachheit, mit der Sie an viele Daten über die lokale Konsole gelangen, wie etwa *esxtop* zur Überwa-



ESX und ESXi hören bei Bedarf auch auf die Kommandozeile

chung der Leistung und Leistungspässe oder der schnelle Zugriff auf die Vielzahl der Protokolldateien. Der mit Abstand wichtigste Aspekt der lokalen Kommandozeile ist allerdings, dass diese immer funktioniert – selbst wenn Sie die Netzwerkverbindung zum ESX-Host verloren haben. Dies gilt bei physikalischen Ausfällen des Netzwerks, Fehlkonfigurationen oder bei Problemen mit den Management-Agenten (*hostd*, *vpax*), wodurch ein Zugriff über vSphere Client, vCLI oder PowerCLI nicht mehr möglich ist. Daher sollten Sie in jedem Fall noch wissen, wie Sie grundlegend das Netzwerk auf dem ESX-Host überprüfen können.

### Die Kommandozeile von ESX und ESXi

Die Befehlszeile des ESX-Servers lässt sich lokal an der Serverkonsole oder über das Remote Management der Server mittels iLO, DRAC oder iRMC sowie IP-basierten KVM-Lösungen nutzen. Dies ist als normaler Benutzer sowie als root-Benutzer möglich. Sehen Sie nur ein Bild mit Servername und IP-Adresse, können Sie mit Alt-F1 und Alt-F6 zwischen den Konsolen wechseln und gelangen mit Alt-F12 auf die VM-Kernel-Ausgabe. Die Verbindung über SSH (PuTTY) ist mit einem normalen Benutzerkonto bereits nach der Installation möglich, mit root nur



durch eine Anpassung der Datei `/etc/ssh/sshd_config`, indem Sie den Eintrag "PermitRootLogin yes" setzen. Allerdings stellt die deaktivierte root-Anmeldung über SSH auch eine Sicherheitsmaßnahme dar, daher sollten Sie die Beschränkung belassen und bei mangelnden Rechten besser `su` oder `sudo` verwenden.

Auch unter ESXi ist der direkte Konsolenzugriff möglich, allerdings finden Sie sich hierbei nur in einer BIOS-ähnlichen Oberfläche mit wenigen Verwaltungsmöglichkeiten wieder. Möchten Sie über die Kommandozeile mehr einsehen, bleibt nur der inoffizielle Weg über die erste Konsole (Alt-F1) und der Eingabe von `unsupported`. Danach gelangen Sie durch Eingabe des root-Passworts in die eigentliche Kommandozeile. Um SSH freizuschalten, sollten Sie sich gut mit dem Linux Editor `vi` auskennen und die Datei `/etc/inetd.conf` anpassen, indem Sie die Zeile "`#ssh`" suchen und das Rautezeichen entfernen. Die Änderungen werden anschließend mit `:wq` geschrieben. Den Neustart des SSH-Dienstes lösen Sie mit dem Befehl `services.ssh restart` aus. Alternativ können Sie den `inetd` komplett starten, indem Sie mit dem Befehl `ps aux | grep inetd` nach dem `inetd`-Prozess suchen und die entsprechende Prozess-ID angeben: `kill -HUP {PID}`. Das ermöglicht Ihnen beispielsweise neben der Nutzung von SCP auch SFTP. Wem dies zu umständlich ist, kann das ESX-System auch komplett neu starten.

Grundsätzlich lassen sich alle Befehle ohne Angabe von Parametern ausführen. Sie erhalten entweder direkt die Standardausgabe oder die Hilfetexte des Befehls. Zur weiteren Unterstützung können Sie die Befehlshilfe `{Befehl} --help` oder die Manpages nutzen über `man {Befehl}`. Die Kommandos zur ESX-Wartung und deren Einsatzgebiet:

- `esxcli`: Storage- und Multipathing
- `esxcfg-advcfg`: Advanced Settings
- `esxcfg-mpath`: Multipathing-Verwaltung
- `esxcfg-nas`: NFS-Verwaltung

- `esxcfg-nics`: Verwaltung der physikalischen Netzwerkkarten
- `esxcfg-rescan`: Rescan der SAN-HBA
- `esxcfg-volume`: Datastores
- `esxcfg-vswitch`: Virtuelle Netzwerke
- `esxcfg-vswif`: Service Console (Management-Adapter)
- `esxupdate`: Patchverwaltung
- `vmkfstools`: vmdk-Festplattendateien
- `vmware-cmd`: Virtuelle Maschinen
- `esxtop`: Systemressourcen
- `vdif`: Anzeige der Festplatten

Einer der Hauptgründe, auf die Konsole zu wechseln, ist neben der Nutzung von `esxtop` die Ansicht der Protokolldateien. Alle wichtigen Protokolldateien sind unterhalb von `"/var/log"` und `"/var/log/vmware"` zu finden:

- `messages`: Konsolenmeldungen
- `vmkernel`: Meldungen des VM-Kernel
- `vmkwarning`: Extrakt aus `vmkernel` nur mit Warnungen und Fehlern
- `vmware/hostd.log`: ESX Host-Agent (Verwaltungsschnittstelle des VM-Kernel)
- `vmware/vpx/vpxa.log`: Meldungen des vCenter-Agents
- `vmware/esxcfg-firewall.log`: Firewall-Protokoll
- `vmware/aam`: Protokolldateien von VMware HA

### vCLI in Betrieb nehmen

Die vCLI (früher Remote CLI) [1] bietet die Möglichkeit, von einem beliebigen PC im Netzwerk des ESX-Hosts oder des vCenters auf diesen über den SDK-Port (Standard 443) zuzugreifen. Beachten Sie dabei die unterstützten Betriebssysteme der eingesetzten vCLI-Version, da diese Liste nicht sonderlich umfangreich ist. So werden etwa die aktuellsten Red Hat-Systeme oder Windows 7 nicht unterstützt. Dies bedeutet allerdings nicht, dass die Software unter diesen Betriebssystemen nicht funktioniert, sondern nur, dass kein offizieller Support durch VMware besteht.

Die Installation läuft sehr einfach ab. Unter Windows wird dabei zusätzlich Active Perl mitinstalliert, da die vCLI komplett in Perl entwickelt wurde. Die

Installationsdateien finden Sie später unter "ProgramFiles(x86) \ VMware \ VMware vSphere CLI \ bin" bei Windows-Systemen mit 32 Bit und unter "ProgramFiles \ VMware \ VMware vSphere CLI \ bin" unter 64 Bit-Windows. Unter Linux muss die heruntergeladene Datei mit `tar xzvf` entpackt und mit `./vmware-install` installiert werden. Damit die Installation reibungslos funktioniert, muss unbedingt auf die richtige Perl Version (5.8) und die folgenden Paketversionen geachtet werden:

- Crypt: SSLey (0.51) [Crypt::SSLeay]
- Data-Dumper (2.102) [Data::Dumper]
- MethodMaker (2.0.8) [Class::MethodMaker]
- XML-LibXML (1.60) [XML::LibXML]
- libwww-perl (5.805) [LWP]

Die Befehle finden Sie anschließend unter `"/usr/bin"`, wenn kein anderes Installationsverzeichnis ausgewählt wurde. Hier ein Überblick der wichtigsten vCLI-Befehle:

- `esxcli`: Storage und Multipathing
- `svmotion.pl`: Storage vMotion
- `vicfg-advcfg.pl`: Advanced Settings
- `vicfg-mpath.pl`: Multipathing
- `vicfg-nas.pl`: NFS-Verwaltung
- `vicfg-nics.pl`: Verwaltung der physikalischen Netzwerkkarten
- `vicfg-ntp.pl`: NTP-Server-Verwaltung
- `vicfg-rescan.pl`: Rescan der SAN-HBA
- `vicfg-volume.pl`: Datastore-Verwaltung
- `vicfg-vswitch.pl`: Verwaltung von virtuellen Netzwerken
- `vifs.pl`: Verwaltung der Datastores
- `vihostupdate.pl`: Patchverwaltung
- `vmkfstools.pl`: vmdk-Festplattendateien
- `vmware-cmd.pl`: Virtuelle Maschinen
- `resxtop.pl`: Remote esxtop Befehl (nur Linux)

Im Unterschied zu den lokalen Befehlen müssen Sie bei den vCLI-Befehlen die Verbindung zum vCenter oder dem ESX-Host angeben:

```
{vCLI Kommando} -server {Server}
                -username {Benutzer} -password
                {Pass} {Optionen}
```

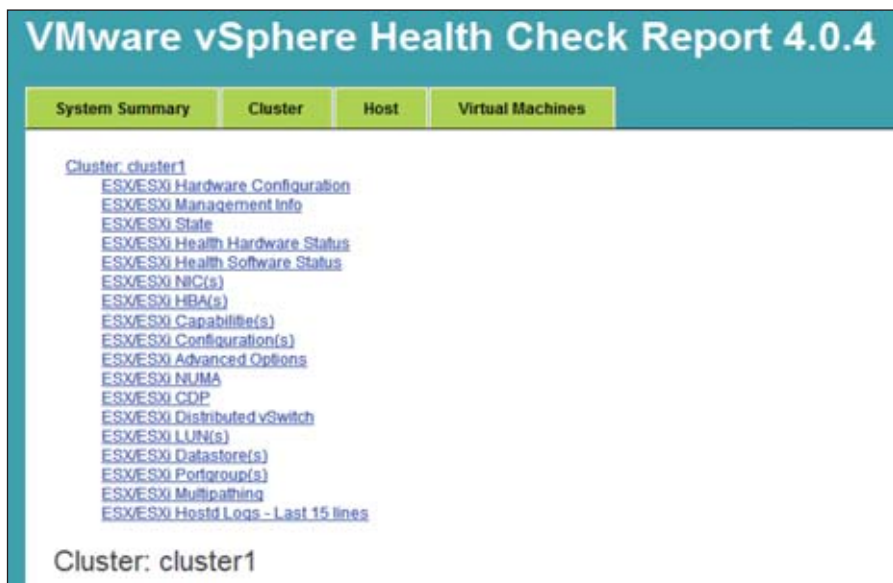


Bild 1: Der vSphere-Healthcheck gibt Auskunft über das Befinden einzelner ESX/ESXi-Komponenten

```
esxcfg-mpath.pl -server ESX1
               -username root -password vmware -l
```

Melden Sie sich am vCenter an, müssen Sie im Kommando den gewünschten ESX-Host mitgeben:

```
{vCLI Kommando} -server {Server}
                 -username {Benutzer} -password
                 {Pass} -vihost {ESX-Host aus Sicht
                 des vCenter} {Optionen}
```

Um die Anmeldung zu vereinfachen, können Sie Umgebungsvariablen setzen, die von der vCLI ausgelesen werden und im Handbuch nachzulesen sind [2] (etwa VI\_SERVER, VI\_USERNAME, VI\_PASSWORD). Ein praktisches Health Check-Skript, das mit vCLI eingesetzt werden kann, finden Sie zudem unter [3].

### Der virtuelle Management-Assistent

Der “virtual Management Assistant” (vMA) zentralisiert als Appliance mit SDK-Zugriff die Administration der virtuellen Infrastruktur über das Netzwerk und kann über SSH verwaltet werden. Dies gilt allerdings hauptsächlich für die Tätigkeiten, die normalerweise über die lokale Servicekonsole stattfinden würden und nicht über den vSphere-Client. Der vMA [4] lässt sich als virtuelle Appliance

im vCenter importieren. Sobald diese startet, können Sie bereits erkennen, dass es sich um eine Linux-VM unter Red Hat 5.2 handelt, die unter anderem die vCLI mit allen Anforderungen enthält. Zum kompletten Start müssen Sie jedoch noch die Netzwerkkonfiguration und das Passwort für vi-admin hinterlegen. Es bestehen die gleichen Befehle und Nutzungsmöglichkeiten wie beim Einsatz der vCLI für Linux und darüber hinaus Konfigurationsmöglichkeiten zum Single-Sign-On am vCenter oder ESX sowie zur zentralen Protokollierung. Die Dokumentation mit Anleitung finden Sie unter [5].

Die erste Anmeldung erfolgt mit dem Benutzer vi-admin und dem von Ihnen während der Installation eingegebenen Passwort. Um den Benutzer vi-user einzurichten, mit dem Sie zumeist arbeiten sollten, müssen Sie lediglich ein Passwort vergeben: `sudo passwd vi-user`.

Um die zentrale Anmeldung via VI Fastpath zu den ESX-Hosts und dem vCenter einzurichten, müssen Sie für jeden Server mit `sudo vifp addserver {ESX/vCenter}` die Anmeldung angeben (root Passwort) und mit `sudo vifpinit {ESX/vCenter}` den Zugang aktivieren. `vifp listservers` zeigt die eingetragenen Serversysteme an. Danach können Sie in der vifpinit-Sitzung eines

ESX-Hosts jeden vCLI-Befehl nutzen, also etwa `vifg-mpath -l`. Sind Sie an einem vCenter angemeldet, müssen Sie noch den Parameter “--vihost” mitgeben: `esxcfg-mpath -l --vihost {ESX-Host}`. Befinden Sie sich nicht in der vifpinit-Sitzung, so können Sie den Befehlen mit “--server” einfach den ESX-Host mitgeben: `vifg-mpath --server {ESX Host} -l`.

Die Möglichkeit der zentralen Protokollierung nennt sich “vilogger” und ist ebenso wie die VI Fastpath-Anmeldung sehr schnell eingerichtet. Hierfür verbinden Sie den vilogger enable-Befehl mit dem Server und der Protokolldatei:

```
vilogger enable -server {ESX-Host}
               -logname {Protokolldatei}
```

Ab diesem Zeitpunkt finden Sie die betroffenen Protokolldateien im Verzeichnis mit dem Hostnamen unterhalb von “/var/log/vmware”. Möchten Sie diese Funktion abschalten, rufen Sie einfach den gleichen Befehl mit “disable” auf:

```
vilogger disable -server {ESX-Host}
                -logname {Protokolldatei}
```

Da immer wieder Aktualisierungen für den vMA erscheinen, sollten Sie sich die beiden folgenden Befehle merken, um auf neue Updates zu prüfen (`sudo vima-update scan`) oder diese einzuspielen (`sudo vima-update update`).

### Mit PowerCLI und PowerShell arbeiten

Das Kommandozeileninterface PowerCLI [6] benötigt eine installierte PowerShell [7]. Außerdem existiert noch eine Erweiterung für den Update-Manager, den Sie unter [8] finden. Damit die PowerCLI richtig starten kann, also die VMware-Snap-ins zur Verwaltung von vSphere geladen werden können, müssen die Sicherheitsregeln der PowerShell etwas aufgeweicht werden mit dem Befehl `Set-ExecutionPolicy RemoteSigned`. Danach ist ein Laden der Snapins mit `add-psnapin vmware.vimautomation.core` oder einfach `add-`



# Bestellen Sie jetzt das IT-Administrator Sonderheft II/2010!

180 Seiten Praxis-Know-how  
rund um das Thema

## Active Directory

zum Abonnenten-Vorzugspreis\* von

# nur € 24,90!

\* IT-Administrator Abonnenten erhalten das Sonderheft II/2010 für € 24,90. Nichtabonnenten zahlen € 29,90. IT-Administrator All-Inclusive Abonnenten "zahlen" für Sonderhefte nur € 19,90 - diese sind im Abonnement dann automatisch enthalten. Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

[www.it-administrator.de/kiosk/sonderhefte/](http://www.it-administrator.de/kiosk/sonderhefte/)



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

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

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

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

Ich zahle  per Bankeinzug

Firma: \_\_\_\_\_

Geldinstitut: \_\_\_\_\_

Name, Vorname: \_\_\_\_\_

Kto.: \_\_\_\_\_ BLZ: \_\_\_\_\_

Straße: \_\_\_\_\_

oder  per Rechnung

Land, PLZ, Ort: \_\_\_\_\_

Datum: \_\_\_\_\_

Tel: \_\_\_\_\_

Unterschrift: \_\_\_\_\_

E-Mail: \_\_\_\_\_

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

So erreichen Sie unseren Vertrieb, Abo- und Leserservice:

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

Diese und weitere Aboangebote finden Sie auch im Internet unter [www.it-administrator.de](http://www.it-administrator.de)



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

ITA 0810

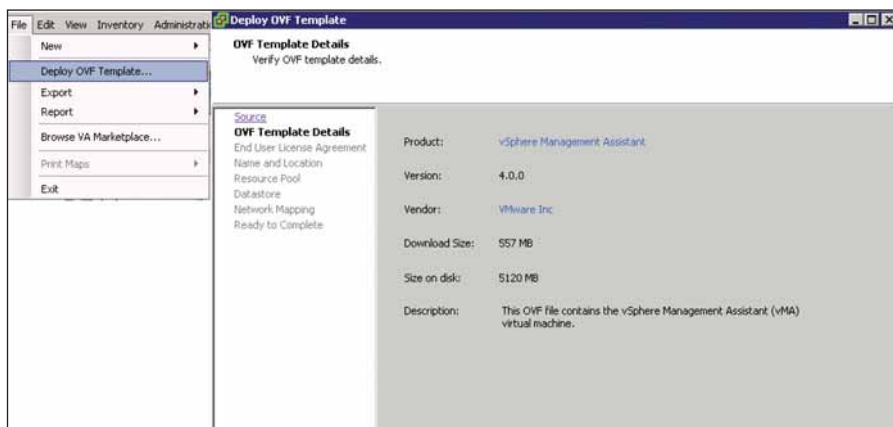


Bild 2: Nach dem Import der virtuellen vMA-Appliance steht der Assistent zur Verfügung

`pssnapin vmware*` möglich und es stehen Ihnen über 200 neue PowerShell-Cmdlets zur Verfügung, die Sie sich mit `Get-Command -Module vmware*` auflisten lassen.

Die Anmeldung am vCenter oder dem ESX-Host geschieht über `Connect-VIServer` mit Benutzername und Passwort, den Windows-Anmeldedaten oder den so genannten PowerShell-Credentials

```
Connect-VIServer {vCenter} -User {Benutzer} -Password {Passwort}
```

oder

```
Connect-VIServer {vCenter} -Credential (Get-Credential),
```

wobei das Passwort im Anmeldedialog einzugeben ist. Funktioniert die Anmeldung nicht, obwohl Namensauflösung und Benutzerdaten passen, kann es sein, dass vCenter entweder nicht auf dem Standardport läuft. Verwenden Sie in diesem Fall den Parameter `“-Port {Portnummer}”`. Möglicherweise ist auch ein Proxy im Internet Explorer hinterlegt. In diesem Fall kann der Befehl `Set-PowerCLIConfiguration -Proxy-Policy NoProxy` Wunder wirken.

Aufgrund der Vielzahl der Cmdlets verzichten wir an dieser Stelle auf eine Auflistung und verweisen auf den Artikel unter [9] und auf die mitgelieferte Hilfe von VMware zur PowerCLI, die Sie im In-

stallationsverzeichnis `“%ProgramFiles \ VMware \ Infrastructure \ vSphere PowerCLI \ VICore Documentation \ vSphere PowerCLI Cmdlets Reference.chm”` finden. Ansonsten erhalten Sie zu jedem Befehl die Hilfe mittels `Get-Help` in der PowerShell-Sitzung, also etwa `Get-Help Get-VM`. Die Möglichkeiten der PowerCLI gehen dabei sehr weit und reichen von einfachen Befehlen wie

```
Get-VM | Get-CDDrive | Set-CDDrive -NoMedia
```

zum Setzen aller CD-ROM-Laufwerke auf dem Client-Device zu etwas komplexeren wie

```
foreach ($vm in (get-view -viewtype virtualmachine)) {($VM.Guest.Disk | Select @{N="Name";E={$VM.Name}},DiskPath, @{N="Capacity(MB)";E={[math]::Round($_.Capacity/1MB)}}, @{N="Free Space(MB)";E={[math]::Round($_.FreeSpace/1MB)}}, @{N="Free Space %";E={[math]::Round(((100 * $_.FreeSpace)/($_.Capacity)),0)}}) | Format-Table}
```

oder enorm umfangreichen Healthcheck-Skripten, die jeder Administrator im Einsatz haben sollte. Diese – beispielsweise `vCheck` – finden Sie unter [10]. Vergessen Sie dabei nicht, nach getaner Arbeit die Verbindung zum ESX oder vCenter Server mit `Disconnect-VIServer` zu trennen.

## Fazit

VMware betreibt einiges an Aufwand, um die Kommandozeilenmöglichkeiten zu optimieren und die Werkzeuge nicht nur lokal auf der Konsole, sondern vor allem über das Netzwerk mit Linux- oder Windows-Arbeitsstationen vollständig zu ermöglichen. Dies befähigt den Administrator, von überall aus dem Netzwerk die Fehlersuche und die Automatisierung durchzuführen und diese auch zu automatisieren. Wenn Sie mehr über die Kommandozeilenmöglichkeiten, die PowerCLI und die Fehlersuche auf der Kommandozeile von VMware ESX 4 erfahren wollen, lohnt sich ein Blick in das Buch `“VMware ESX4”`, das der Autor dieses Workshops gemeinsam mit Bertram Wöhrmann und weiteren Autoren veröffentlicht hat [11]. (dr)

- [1] **Download von vCLI**  
[www.vmware.com/support/developer/vcli/](http://www.vmware.com/support/developer/vcli/)
- [2] **Umgebungsvariablen, die von der vCLI ausgelesen werden**  
[www.vmware.com/pdf/vsphere4/r40\\_u1/vsp\\_40\\_u1\\_vcli.pdf](http://www.vmware.com/pdf/vsphere4/r40_u1/vsp_40_u1_vcli.pdf)
- [3] **Health Check-Skript für den Einsatz mit vCLI**  
<http://communities.vmware.com/docs/DOC-9842>
- [4] **vMA-Download**  
[www.vmware.com/go/vma](http://www.vmware.com/go/vma)
- [5] **vMA-Dokumentation mit Anleitung**  
[www.vmware.com/support/developer/vima/vima40/doc/vma\\_40\\_guide.pdf](http://www.vmware.com/support/developer/vima/vima40/doc/vma_40_guide.pdf)
- [6] **PowerCLI**  
[www.vmware.com/go/powercli](http://www.vmware.com/go/powercli)
- [7] **Microsoft PowerShell**  
<http://support.microsoft.com/kb/968929>
- [8] **Update-Manager**  
<http://communities.vmware.com/community/vmtm/vsphere/automationtools/powercli/updatesmanager>
- [9] **Beitrag “Angriff der Power-Skripte” im IT Administrator 01/2009**  
[www.it-administrator.de/magazin/heftarchiv/artikel/51690.html](http://www.it-administrator.de/magazin/heftarchiv/artikel/51690.html)
- [10] **Health-Skripte**  
[www.virtual.net/featured-scripts/vcheck/](http://www.virtual.net/featured-scripts/vcheck/)
- [11] **VMware ESX4**  
[www.galileocomputing.de/2179](http://www.galileocomputing.de/2179)

Links





## Logdaten mit Splunk auswerten und verwalten (1)

# Gesucht, gefunden

von Holger Sesterhenn

Angesichts der erdrückenden Menge an Logdaten sind IT-Administratoren kaum mehr in der Lage, mit manuellen Methoden oder selbst entwickelten Skripten Events und Sicherheitsmeldungen zeitnah aufzubereiten und auszuwerten. Folglich finden Analysen oft nur im Nachhinein statt – was mit Risiken verbunden ist. Wie Sie mit Splunk den Überblick behalten, zeigt Ihnen diese Workshopserie.



Quelle: Scot Maxwell – Fotolia.com

**W**as den meisten IT-Abteilungen fehlt, sind geeignete Werkzeuge, um mit Logdaten von bis zu mehreren GByte pro Tag effizient arbeiten zu können. Darüber hinaus fehlt der integrative Ansatz – die Möglichkeit, alle Logdaten an einem zentralisierten Punkt zu erfassen, nahezu in Echtzeit zu durchsuchen, zu visualisieren, zu archivieren und bei Anomalien einen Alarm zu versenden. Betrachten wir den typischen Ablauf einer Fehlersuche. Das Monitoringtool, zum Beispiel Nagios, meldet ein Problem. Sie melden sich über die Konsole des fehlerhaften Systems an und beginnen, mit `grep`, `tail -f` oder ähnlichen Kommandos Logdateien auf Auffälligkeiten hin zu durchforsten

Da Sie den Zeitpunkt nur grob kennen, quälen Sie sich durch Millionen von Log-Events. Dabei sind die Chancen, gleich auf dem ersten System fündig zu werden, recht gering. Sie weiten die Suche auf die Kommunikationspartner des vermuteten Systems aus, müssen dazu Logdaten unterschiedlicher Formate interpretieren und benötigen extrem viel Zeit, Wissen und Erfahrung, um den Auslöser des Problems zu finden. Am Ende haben Sie einige Indizien entdeckt, exportieren die betreffenden Logzeilen und schicken diese dem Applikationsverantwortlichen zur weiteren Analyse zu. Leider hat dieser keinen Administrationszugriff auf sämtliche OS-

Logs und kommt daher wieder auf Sie zurück. Die Iteration beginnt von vorne. Angesichts dieser wiederkehrenden Erfahrungen wird deutlich, welche Funktionen eine umfassende Logverwaltung mitbringen sollte:

- Erfassung von Logdaten beliebiger Betriebssysteme, Anwendungen, Netzwerkgeräte, Sicherheitslösungen oder auch JMX- und J2EE-Stack Traces in Echtzeit.
- Vordefinierte Dashboards, Suchen, Reports, Alerts und Korrelationen.
- Skalierbare, flexible und verteilbare Systemarchitektur, die lauffähig auf allen gängigen OS ist.
- Performante, skalierbare Indexierung.
- Langzeit-Speicherung inklusive signaturbasiertem Integritätsschutz.
- Anreicherung der Logdaten mit Zusatzinformationen wie etwa Benutzer- und CMDB-Daten.
- Intelligente und verteilte Suchfunktionen (Boolean-, Field-, Statistical-, Pattern- und Subsearches).
- Erkennen von Anomalien und Trends.
- Automatisierte Überwachung und Benachrichtigung.
- Custom-Dashboards für unterschiedliche Nutzer (Management, Auditoren, Sysadmins et cetera).
- Rollen- und Rechtekonzept inklusive Integration eines Verzeichnisdienstes (MS AD/LDAP).

- Integration mit anderen Verfügbarkeits-, Monitoring-, Incident Management- und Trouble Ticketing-Systemen wie Nagios, BMC Remedy, Cisco Works, HP Service Desk oder IBM Tivoli.

### Log-Management für die gesamte IT-Landschaft

Der Mehrwert von Log-Management-Lösungen besteht in der zentralen Erfassung, Indexierung und Speicherung von Logdaten sowie der Bereitstellung von Such- und Analysemöglichkeiten. Wesentlich dabei ist, dass Log-Management-Lösungen im Gegensatz zu SIEM-Lösungen auf aufwändiges Parsen und Normalisieren von Logda-

Splunk wird als proprietäres Softwarepaket angeboten. Als **Freeware-Version** darf der registrierte Nutzer 500 MByte pro Tag ohne zeitliche Beschränkung auswerten. Somit eignet sich die Software auch hervorragend zum Testen für Einsteiger.

Splunk ist für alle gängigen Betriebssysteme verfügbar: Solaris 9, 10 (x86, SPARC), Linux Kernel Vers 2.6.x (x86: 32/64 Bit), FreeBSD 6.1 / 6.2 (x86: 32/64 Bit), Windows 2003 (32/64 Bit), Windows 2008, XP und Vista. Die Hardware-Minimalanforderungen für unsere Testinstallation von etwa 50 GByte je Tag zu indexierendem Logvolumen und drei parallelen Anwendern lassen sich mit einem Standard-Server von der Stange problemlos abbilden.

**Splunk-Lizenzen und Systemvoraussetzungen**



ten verzichten und stattdessen auf eine teilweise oder vollständige Indexierung des Logtextes setzen. Für dieses Verfahren hat sich der Terminus “Universal Indexing” durchgesetzt. IT-Search-Lösungen sind auf hohe Datendurchsätze getrimmt und speichern Logdaten mit Kompressionsraten bis zu einem Faktor 3:1 in sogenannte “Indexed Flatfiles”. Sie verwenden keine Datenbanken zum Ablegen der Informationen und arbeiten somit schemalos. Stattdessen werden die Logdaten in der Regel in einem offenen Format (GZIP) gespeichert und signiert, um Manipulationssicherheit zu gewährleisten.

Einige dieser Lösungen sind in der Lage, wiederkehrende Muster in Logdaten zu erkennen und beherrschen dabei eine Volltextindexierung in Echtzeit (zum Beispiel ArcSight Logger, LogLogic oder Splunk). Bei fast allen Universal-Indexing-Lösungen können Sie mehr oder weniger intelligent mit den Suchergebnissen interagieren. Splunk bietet auf diesem Sektor eine derzeit marktführende Technologie. Das Ajax-basierte Web2.0-GUI ermöglicht Drill-Downs, Zoom-Funktionen auf der Zeitachse, Trendanalyse und das Erkennen von Spikes oder Anomalien in bester Manier. Statistiken, Grafiken und andere praktische Werkzeuge ermöglichen es in kürzester Zeit, die Nadel im Heuhaufen zu finden.

Das Vorgehen nach Handbuch gestaltet sich dabei einfach, und bereits drei Minuten später präsentiert sich das Web2.0-GUI per Zugriff auf <http://mysplunkhost:8000> als aufgeräumte Umgebung – dem sogenannten Splunk Launcher (Bild 1).

Wenn Sie Splunk verwenden, nutzen Sie sogenannte Splunk Apps. Das sind verschiedene Sichtweisen auf die Logdaten, die durch Rollen und Rechte gesteuert werden können. Anders ausgedrückt sind Apps Zusammenstellungen von Suchen, Event-Typen, Metadaten, Views und Dashboards sowie Reports, die auf einer Splunk-Instanz laufen. Sie dienen dazu, Erscheinungsbild und Inhalte den Nutzerbedürfnissen entsprechend anzupassen. So kann zum Beispiel eine App zur Analyse des Webdatenverkehrs eingesetzt werden und eine andere für E-Mail, ERP-Daten, Finanztransaktionen, Datenbank-Umgebungen oder auch IT-Security-Systeme. Apps werden innerhalb der Splunk-Community zahlreich und oft kostenfrei angeboten, so dass Sie für viele Themenbereiche passend vorkonfigurierte Apps finden dürften.

## Zweigeleisige Architektur

Werfen wir einen Blick auf das Architekturkonzept. Splunk bietet einen mehrdimensionalen Ansatz und will den

Administrator dabei unterstützen, alle notwendigen Verarbeitungsschritte flexibel und funktional umzusetzen. Grundsätzlich unterscheidet die Splunk-Architektur zwei Funktionen: Indexierung und Suche. Im ersten Schritt werden die als Text eingelesenen Daten von einem “Indexer” analysiert und indiziert. Über Suchanfragen können Sie die indizierten Daten analysieren und deren Ergebnisse als einfache Tabelle oder in Diagrammform darstellen lassen. Indexierung und Analyse lassen sich auf der gleichen Plattform ausführen oder bei steigenden Anforderungen auf verschiedene physikalische Systeme verteilen. Sogenannte “Search Heads” verteilen dann die Anfragen und führen deren Ergebnisse wieder auf einem System zusammen. Dies ermöglicht auch bei sehr großen Datenmengen effiziente Analysen.

Sie haben die Möglichkeit – im einfachsten Fall über das Web-GUI per Drag and Drop – eigene Apps zu erstellen, vorgefertigte Anwendungen mit wenigen Mausklicks zu installieren oder mit Hilfe weniger, Text- und XML-basierter Konfigurationsdateien, umfangreiche Applikationen zu entwickeln. Je nach verwendeter Plattform werden auch systemspezifische Applikationen als vordefinierte Datenquellen und Beispiele zur Verfügung gestellt (“Splunk> Windows” und “Splunk> \*nix”). Eigene Datenquellen werden durch den Administrator in der Regel über das Web-GUI konfiguriert. Das System erstellt die notwendigen Konfigurationsdateien automatisch. Für weitergehende Anpassungen lassen sich diese Konfigurationsdateien (*inputs.conf*) dann erweitern und optimieren.

## Allzweckwaffe Universal Indexing

Universal Indexing indiziert alle Arten von Logdaten, jeden Term, jedes Ereignis von allen Quellen in Echtzeit, ohne dabei Datenbanken zu verwenden, Konnektoren zu benötigen oder benutzerdefinierte Parser für proprietäre Anwendungen voraussetzen. Administratoren ist es damit möglich, in Analogie zu einer



Bild 1: Beim Start bietet der Splunk Launcher eine erste Hilfestellung



Internetsuchmaschine nach beliebigen Mustern, Wörtern oder Wortgruppen zu suchen (Bild 2). Sämtliche in Splunk verarbeiteten Daten werden dabei in Paketen ("chunks") zu rund 10 KByte durch die "Universal Pipeline" geschleust. Im ersten Schritt teilt das System die Daten in "Events" auf. Diese sind in der Regel durch einen Zeilenvorschub getrennt. Über Einstellungen in der Konfigurationsdatei *props.conf* lassen sich mehrere Zeilen zu einem Event zusammenfassen ("Multiline events").

Im Zuge der Indexierung werden Events in einzelne Abschnitte ("segments") aufgeteilt. Diese Segmentierung erfolgt auf Grund definierter Trennzeichen ("breaking characters") und weiterer Regeln wie der maximalen Zeichenanzahl pro Segment. In der Datei *segmenters.conf* lassen sich die Trennzeichen und Regeln beeinflussen. Einzelne Segmente bilden sogenannte Terme, die im Index abgelegt werden. Durch Zusammenfassung von Termen zu komplexeren Ausdrücken, die ihrerseits zum Index hinzugefügt werden, erhalten Sie eine Flexibilität, die zum Beispiel beim Eingeben eines Suchausdrucks im "Type-Ahead"-Stil genutzt werden kann. Geben Sie etwa zuerst nur eine zweistellige Zahl ein, so kann dies als Wert eines Feldes oder auch als das erste Oktet einer IP-Adresse interpretiert werden. Durch Eingabe weiterer Zeichen schränkt das System die Ergebnismenge immer weiter ein, bis zum Schluss nur noch eine mögliche Antwort angezeigt wird.

```

Source & host capture: 384:5] ICMP PING [**]
[Classification: Misc activity] [Priority: 3]
05/04-16:23:26.195793 10.2.1.48 -> 10.2.1.222
ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:52296 Seq:4 ECHO
source= /var/log/snort/alert - host= virt2:cardholder:cardholder-dest
sourcetype= snort_alert_log - | linecount= 5 -


Automatically discovered fields
05/04/09 11:51:26.224713 5] ICMP PING [**]
[Classification: Misc activity] [Priority: 3]
05/04-11:51:26.224713 10.2.1.48 -> 10.2.1.222
ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:47447 Seq:4 ECHO
ID= 0 - | ttl= 20 - | TOS= 0x0 - | TTL= 64 - | bytes_in= 84 - | category= Misc activity - |
dest_ip= 10.2.1.222 - | generator_id= 1 - | name= ICMP PING - | proto= ICMP - | severity= 3 - |
signature= 384 - | signature_rev= 384 - | time= 11:51:26 -

And user-defined fields
  
```

Bild 2: Beim Universal Indexing werden alle Arten von Logdaten berücksichtigt und mit den Admin-Eingaben verknüpft

Ein zentraler Schritt im Zuge der Indexierung ist das Erkennen eines eindeutigen Zeitstempels innerhalb eines Events. Durch Auswertung regulärer Ausdrücke ist Splunk in der Lage, verschiedenste Formen von Zeitstempeln zu erkennen und als grundlegendes Normalisierungskriterium zu nutzen. Dabei werden selbst unterschiedliche Zeitzonen-Informationen erkannt und berücksichtigt. In einem weiteren Verarbeitungsschritt werden aus einem Event Schlüsselwert-Paare extrahiert, mit deren Hilfe Sie später bei der Datenanalyse schnell zum gewünschten Ergebnis kommen. Typische Trennzeichen sind zum Beispiel das Gleichheitszeichen und der Doppelpunkt. Der linke Teil dieser Wertepaare wird als Feld ("field") bezeichnet, das in einer spezifischen Suche oder bei der Erstellung statistischer Auswertungen genutzt werden kann. Jedes Event ist genau einer Datenquelle, einem Host, zugeordnet. In Kombination mit verschiede-

nen Indizes lässt sich dadurch ein detailliertes Zugriffsmodell entwickeln, das in Kombination mit einer teilweisen Anonymisierung von Daten den heutigen Anforderungen an Datenschutz und Vertraulichkeit gerecht wird. Das Ergebnis einer Suche lässt sich um Informationen anreichern, die im ursprünglichen Event nicht vorhanden waren, ohne das eigentliche Event zu verändern. Diese als "Metadaten" bezeichneten Informationen erlauben weitere komplexe Operationen bis hin zu einer statischen Auswertung von ursprünglich nicht zusammenhängenden Logdaten.

Lesen Sie im zweiten Teil unserer Workshopserie, wie Sie Splunk in der Praxis nutzen. (dr) 

Dipl.-Ing. (FH) Holger Sesterhenn, CISSP ist Consultant IT-Security bei IT-CUBE SYSTEMS, einem auf IT-Security spezialisierten Systemintegrator.

Bringt abends Arbeit mit nach Hause.

Und morgens Viren in die Firma.

**Mitarbeiter sind auch nur Menschen.** Da kann es passieren, dass ein privater USB-Stick Ihr ganzes Netzwerk lahmlegt. Oder dass wichtige Daten verloren gehen. Oder in falsche Hände geraten. Oder manipuliert werden. Schützen Sie sich davor!

- Kontrolle sämtlicher PC-Schnittstellen
- Schutz vor Datenbeschädigung und -verlust durch Unachtsamkeit oder Vorsatz
- Individuelle Justierbarkeit
- Für kleine, große und größte Netzwerke
- Über 4 Mio. Installationen
- Referenzen in hochsensiblen Branchen

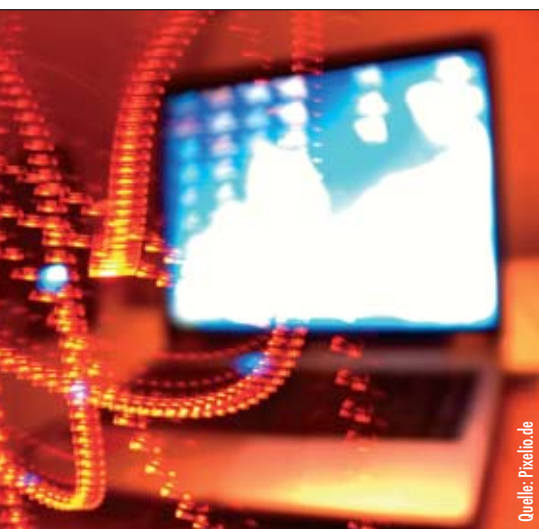
Informieren Sie sich jetzt!  
[www.deviceclock.de](http://www.deviceclock.de) oder wählen Sie die Nummer sicher: +49.2102.89211-0

**DeviceLock**  
 Proactive Endpoint Security

# Citrix XenClient Express für mobile Geräte Virtuell unterwegs

von Nico Lüdemann

Die Virtualisierung von Servern und Desktops im Rechenzentrum ist bereits seit einiger Zeit relativ leicht realisierbar. Problematisch hingegen war bisher die Bereitstellung virtualisierter Systeme an Offline-Geräten wie Notebooks – und genau an dieser Stelle greift Citrix nun mit Unterstützung von Intel mit dem XenClient an. Dieser Artikel verrät Ihnen, was der Typ-1-Hypervisor in Sachen Virtualisierung auf mobilen Endgeräten leistet und welchen Einfluss dies auf das Client-Management der Zukunft hat.



Quelle: Pixelio.de

**E**ine kurze, aber wichtige Vorbemerkung muss erfolgen, bevor wir in das Thema einsteigen: Der Artikel basiert auf dem Release Candidate [1] des XenClient Express, der noch kein finales Produkt darstellt und bei dem es im Einzelfall noch zu fehlerhaften Funktionen kommen kann. Zudem können erwähnte Features im finalen Produkt fehlen oder neue hinzukommen.

Beim XenClient handelt es sich um einen Client-Hypervisor, also um eine Lösung, die Sie dazu verwenden können, um virtuelle Maschinen direkt auf Ihrem Notebook oder PC laufen zu lassen. Hierdurch werden Sie beispielsweise in die Lage versetzt, mehrere Betriebssysteme – etwa Windows XP und Windows 7 – parallel auf Ihrem Endgerät nutzen zu können.

## Neue Möglichkeiten am Endgerät

Aber selbst wenn Sie hierfür keinen Bedarf haben sollten, bringt Ihnen die Virtualisierung auch nur eines Betriebssystems einen Vorteil: Sie können das OS von der darunterliegenden Hardware entkoppeln und es beispielsweise bei einem Wechsel Ihres Endgerätes einfach auf das neue Gerät “mitnehmen”. In Summe lässt sich also

sagen, dass Sie hierdurch ähnlich flexibel arbeiten können, wie Sie es vielleicht schon aus Ihrer XenApp- oder Xen-Desktop-Umgebung kennen, auf die Sie ja auch flexibel und unabhängig von Ihrem Endgerät über nahezu jede Netzwerkverbindung zugreifen können – aber mindestens eine Netzwerkverbindung benötigen. Wenn Sie mittels des XenClients Ihre virtuellen Umgebungen aber immer direkt bei sich haben, können Sie auch ohne eine Netzwerk-anbindung damit arbeiten – ein gewaltiger Vorteil für mobile Benutzer.

Nun ist die Idee des Betriebes von virtuellen Maschinen auf dem Endgerät nicht neu. Im Vergleich zu anderen Client-Hypervisoren setzt sich der XenClient jedoch durch eine bisher einzigartige Besonderheit ab – es handelt sich um einen sogenannten “Typ-1-Hypervisor”.

## Die Architektur eines Typ-1-Hypervisors

Der Kern des XenClient ist eine Bare-Metal-Installation auf der Basis des Open Source Xen-Hypervisors, der auch für das Server-Produkt Citrix XenServer verwendet wird. Wie den XenServer installieren Sie auch den XenClient direkt auf der Hardware des Endgerätes, ohne

dass vorher ein anderes Betriebssystem darauf installiert sein muss. Dieser Typ-1-Hypervisor unterscheidet sich insofern deutlich von den anderen am Markt befindlichen Lösungen etwa von Microsoft und VMware, die jeweils ein Betriebssystem für die Installation des Hypervisors voraussetzen.

Hieraus ergeben sich einige geänderte Architekturmerkmale: Zum einen können Sie so Ihre virtuellen Maschinen mit einem nur sehr geringen Overhead von etwa zwei bis sieben Prozent für die Virtualisierung betreiben – großartige Werte im Vergleich zu 15 bis 20 Prozent für die heute verfügbaren Typ-2-Hypervisoren. Das hieraus resultierende Plus an Leistung können Sie dann natürlich innerhalb der virtuellen Maschinen für Ihre Anwendungen nutzen oder eben einfach mehr virtuelle Systeme parallel betreiben, als es unter anderen Lösungen möglich wäre.

Doch der geringere Overhead bei der Virtualisierung ist noch nicht die einzige Besonderheit des Citrix XenClient. Auch bietet er die Möglichkeit, dass Sie den virtuellen Maschinen einen direkten Zugriff auf physikalische Komponenten wie Schnittstellen oder die Gra-



fikkarte geben können. Durch Letzteres erreichen Sie für die hierfür aktivierten VMs die volle Grafikleistung, die Sie auch mit einem nativ installierten System erreichen würden – das ist revolutionär für einen Hypervisor. Für spätere Versionen ist beispielsweise auch die direkte Adressierung von integrierten UMTS-Karten oder Kameras geplant. Bereits in der aktuellen Version können Sie direkt aus dem “leeren” XenClient, also ohne zuerst eine virtuelle Maschine erstellt zu haben, bereits WLAN-Karten nutzen, um auf das Netzwerk zugreifen zu können.

Die einzige kleine Krux bei dieser Technologie ist allerdings genau diese relativ starke Bindung an die Hardwareressourcen des Endgerätes. So setzt der XenClient für den Betrieb am Endgerät die vPro-Technologie von Intel voraus, über die etwa die Virtualisierung von CPU-Zugriffen (Intel VT) oder Komponenten-Zugriffen mittels Directed-I/O (Intel VT-d) realisiert wird. Auch die anderen Funktionen des XenClient Express wie die Sicherheitssteuerung, die Grafikbeschleunigung und die WLAN-Integration nutzen direkt die Schnittstellen und Komponenten der Intel vPro-Spezifikationen.

## Benutzeroberfläche und Administration

Die gesamte Benutzeroberfläche des XenClient ist wiederum ebenfalls in Form einer virtuellen Maschine, einer sogenannten Service-VM, realisiert. Diese wird automatisch mit dem XenClient installiert und auch direkt beim Booten des Endgerätes gestartet. Das heißt, dass Sie direkt mit dieser Oberfläche arbeiten können, sobald Sie den XenClient auf einem den Anforderungen entsprechenden Notebook oder PC installiert haben.

Neben der Anpassung von Systemkonfigurationen, wie etwa den bereits oben beschriebenen WLAN-Verbindungen, können Sie an dieser Stelle direkt neue virtuelle Maschinen erstellen und diese



Bild 1: XenClient erlaubt ein schnelles Wechseln zwischen den installierten virtuellen Maschinen

mittels einer DVD oder einer PXE-basierten Bereitstellung installieren. Nach der Installation des Betriebssystems können Sie virtuelle Maschinen wie ein lokales Betriebssystem nutzen und verwalten. Sollten Sie mehrere VMs installiert haben, können Sie einfach zwischen diesen umschalten.

Doch das ist noch nicht alles: Sie sollten in den virtuellen Maschinen auch die entsprechenden “XenClient-Tools” installieren, in denen nicht nur die optimierten Virtualisierungstreiber enthalten sind, sondern auch eine erweiterte Oberfläche – der “Citrix Receiver for XenClient”. Dieser erlaubt es Ihnen, mittels eines Menüs am oberen Rand des Bildschirms zwischen den VMs zu wechseln.

## Gesicherter Zugriff zwischen VMs

Was ist aber in dem Fall, wenn Sie eigentlich mit Ihrem virtuellen Windows 7 arbeiten möchten, weil Sie hierin beispielsweise die Aero-Funktion lieben, Ihre wichtigste Anwendung aber nur unter Windows XP läuft? Hier ermöglicht es XenClient, dass Sie nicht immer zwischen den beiden virtuellen Maschinen hin und her schalten müssen. Denn mit den XenClient-Tools lässt sich ein Toolset installieren, über das Sie beispielsweise Ihre Anwendung auf Ihrem Wind-

ows XP “veröffentlichen” können. Anschließend wird diese Anwendung auf Ihrem Windows 7 über das ebenfalls direkt mitgelieferte Citrix Dazzle zur Verfügung gestellt. Von hier aus können Sie es dann als Seamless-Anwendung nutzen. Dies bedeutet konkret, dass Sie das Anwendungsfenster Ihrer auf Windows XP installierten Anwendung in Ihrem Windows 7-Desktop eingeblendet bekommen und sie somit nahtlos parallel mit nativen Windows 7-Anwendungen nutzen können. Einzig ein farbiger Rahmen um das Anwendungsfenster zeigt an, dass sie aus einer anderen Umgebung bereitgestellt wird.

Diese Funktion ist nicht nur sehr hilfreich bei der Arbeit mit Anwendungen aus mehreren VMs, sie hat sogar sicherheitsrelevante Vorteile. Durch die Virtualisierung mittels eines Typ-1-Hypervisors und der engen Verdrahtung mit Intels vPro-Technologien wird bei dieser VM-übergreifenden Darstellung zwar der Grafikinhalt in einem Desktop konsolidiert, alle anderen Funktionen – wie etwa die Eingaben über Tastatur und Maus – bleiben jedoch über die jeweilige virtuelle Maschine eingegrenzt. So wäre es in unserem beschriebenen Szenario so, dass etwa ein unter Windows 7 installierter Keylogger keine Tastatureingaben erfass-

## Worüber Administratoren morgen reden

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

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

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

Jetzt einfach und kostenlos bestellen unter:



[www.it-administrator.de/newsletter](http://www.it-administrator.de/newsletter)

sen könnte, die in der Windows XP-Anwendung getätigt würden. Das Fenster der Anwendung befindet sich zwar rein optisch auf dem Windows 7-Desktop, aber in dem Moment, in dem in der Anwendung eine Eingabe erfolgt, wird diese mittels vPro direkt in der XP-VM durchgeführt und somit für den Schädling in der Win7-VM nicht sichtbar.

Genau diese Tatsache eröffnet für den XenClient natürlich weitere Anwendungsfälle – nicht nur der parallele Betrieb von virtuellen Maschinen mit unterschiedlichen Betriebssystemen auf einem Endgerät ist ein Einsatzszenario – auch der parallele Betrieb von VMs, die sich vielleicht nicht im Betriebssystem, sondern vielmehr in ihrem Sicherheitsniveau unterscheiden, ist ein valider und durchaus wichtiger Anwendungsfall. Dieses Szenario ist beispielsweise dann gegeben, wenn mobile Mitarbeiter auf ihren Notebooks neben ihrem “Arbeits-Images” auch ein “Private-Image” betreiben dürfen: Arbeiten in der Unternehmens-VM und abends im Hotel über die private VM Videos ansehen und im Internet surfen.

### Zentrale Verwaltung über den Synchronizer


Und an dieser Stelle schließt sich der Kreis. Denken Sie an das eben beschriebene Szenario, so wünschen Sie sich vielleicht eine weitere Funktion: Neben der reinen Betriebssystem-Installation von einer DVD würden Sie auch gerne zentral verwaltete Unternehmens-VMs im XenClient einsetzen und mit Hilfe einer Managementinfrastruktur verwalten.

Die hierfür zuständige Komponente ist der sogenannte “VM Synchronizer”. Bei ihm handelt es sich um eine virtuelle Appliance, welche Sie auf einem XenServer importieren und betreiben können. Anschließend können Sie auf Ihrem XenClient die Adresse dieses Systems angeben und dort hinterlegte virtuelle Maschinen – also beispielsweise Ihre stan-

dardisierten Unternehmens-VMs – herunterladen. Dies spart nicht nur Zeit, sondern verhilft Ihnen auch dazu, standardisierte virtuelle Systeme auf Ihren Endgeräten nutzen zu können. Speichert der Benutzer Daten in diesen VMs, kann der Synchronizer auch Daten zu Sicherungszwecken von VMs “zurückholen”.

### Fazit

XenClient Express stellt einen großen Durchbruch im Bereich der Desktop-Virtualisierung dar. Seine neuen Möglichkeiten der Bereitstellung von virtuellen Systemen auf einem Endgerät ohne die bisherigen Einschränkungen wie schlechte Schnittstellen und Komponenten-Unterstützung und mäßige Performance haben das Potenzial, die Verwaltung von (zunächst) mobilen Endgeräten zu revolutionieren.

Dies wird vielleicht noch nicht in den nächsten drei bis sechs Monaten und auch noch nicht mit der ersten Version des XenClient der Fall sein, aber spätestens dann, wenn die ersten Hardware-Hersteller direkt von Haus aus eine funktionale und stabile OEM-Implementation des XenClient mit ihren Geräten ausliefern, wird wahrscheinlich niemand mehr über eine native Installation des Betriebssystems nachdenken – mit sehr weitreichenden Auswirkungen auf den gesamten Bereich des Client-Computings. So werden sich auch in Themengebieten wie der initialen Bereitstellung von Betriebssystemen, der Standardisierung und zentralen Verwaltung von Unternehmenskonfigurationen oder dem zentralen Backup von Endgeräten mittels des XenClient neue Möglichkeiten auftun, die dann den Weg in die IT-Strukturen finden werden. (jp) 

[1] Release Candidate des XenClient Express

[www.citrix.com/English/ps2/products/feature.asp?contentID=2300346](http://www.citrix.com/English/ps2/products/feature.asp?contentID=2300346)

Links





## Desktop-Management mit dem Microsoft Desktop Optimization Pack (3)

# Letzte Rettung beim Systemabsturz

von Thomas Joos



Quelle: mipan - Fotolia.com

In unserer Workshopserie zum Microsoft Desktop Optimization Pack (MDOP) beschäftigen wir uns im dritten Teil mit dem Microsoft Diagnostic and Recovery Toolset in der Version 6.5. Das Toolset enthält verschiedene Werkzeuge, die bei der Systemdiagnose und der Analyse von Bluescreens helfen. Außerdem gehen wir näher darauf ein, wie Sie mit etwas Glück und einer Systemrettungs-CD auch in schweren Fällen eine Neuinstallation des OS vermeiden.

**D**as Microsoft Diagnostic and Recovery Toolset (DaRT) in der aktuellen Version ist vor allem für Windows 7 und Windows Server 2008 R2 optimiert. Setzen Sie im Unternehmen noch Windows Vista und Windows Server 2008 ein, können Sie die Version 6.0 von DaRT nutzen, die ebenfalls Bestandteil des MDOP 2010 ist. Zudem finden Sie die Tools des MDOP auch einzeln direkt auf der CD und können die Installationsdateien separat auf den Server kopieren. So benötigen Sie nicht immer den vollständigen MDOP-Datenträger. Die beiden zentralen Tools des DaRT sind der Assistent für die Absturzanalyse, ein Tool zur Untersuchung von Bluescreens, sowie der ERD-Commander (Emergency Recovery Disk), mit dem Sie eine Rettungs-CD für Windows Server 2008 R2 und Windows 7 erstellen können. Interessant ist, dass Sie auch den Assistenten für die Absturzanalyse auf eine solche Wiederherstellungs-CD integrieren können. Damit haben Sie die Möglichkeit, die Ursache für nicht startende Server direkt über die Rettungs-CD herauszufinden. Im folgenden Workshop gehen wir genauer auf die Möglichkeiten dieser beiden Tools ein.

### Bluescreens verstehen

Die Installation von DaRT führen Sie über die Installationsoberfläche des MDOP durch. Nach der Installation starten Sie die Tools über eine eigene Programmgruppe. Bestandteil von DaRT ist der Assistent für die Absturzanalyse. Einfach gesagt lassen sich mit dem Tool die Dump-Dateien von Bluescreens analysieren. Dazu greift das Tool auf die Free-ware Microsoft Debugging Tools for

Windows zurück und analysiert mit Hilfe dieses Werkzeugs die von Windows erzeugten Dump-Dateien. Die Debugging Tools müssen Sie getrennt zu DaRT herunterladen und installieren. Sie finden den kostenlosen und auch ohne MDOP lauffähigen Download auf der Seite [1]. Für Windows 7 und Windows Server 2008 R2 installieren Sie die Debugging Tools über das Windows 7 SDK, welches Sie auf der gerade genannten Webseite

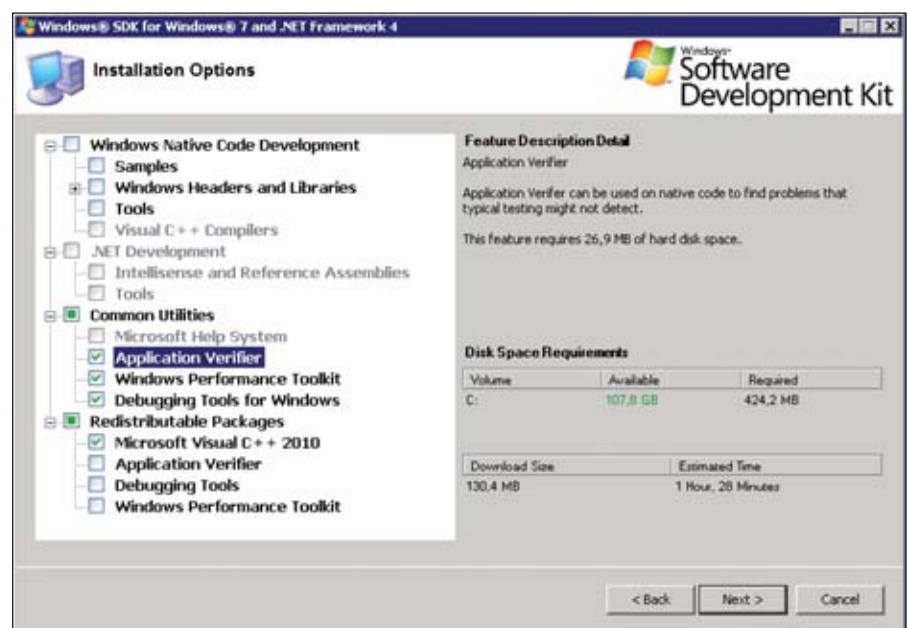


Bild 1: So installieren Sie die Microsoft Debugging Tools x64 als Teil des Windows 7 SDK



herunterladen können. Während der Installation wählen Sie einfach die Komponenten des SDK aus.

## Systemfehler mit dem Assistenten für die Absturzanalyse untersuchen

Windows Server 2008 R2 ist standardmäßig so eingestellt, dass nach einem Bluescreen automatisch der Rechner neu startet. Das hat den Vorteil, dass der Server recht schnell wieder zur Verfügung steht. Allerdings können Administratoren in diesem Fall die entsprechende Fehlermeldung nicht lesen. Tritt der Fehler bei jedem Start auf, verfängt sich der Computer somit in einer Endlosschleife. Die möglichen Einstellungen, wie sich Windows nach einem Bluescreen verhalten soll, finden Sie unter "Start / Systemsteuerung / System und Wartung / System / Erweiterte Systemeinstellungen". Klicken Sie im Bereich "Starten und Wiederherstellen" auf die Schaltfläche "Einstellungen". Über den Bereich "Systemfehler" lässt sich die Konfiguration vornehmen.

Zunächst sollten Sie das Häkchen "Automatisch Neustart" durchführen deaktivieren, wenn der Rechner im Bluescreen stehen bleiben soll. Im Bereich "Debuginformationen" wählen Sie über das Dropdown-Menü aus, welche Art der Informationen das Betriebssystem protokollieren soll. Am besten ist die Variante "Kleines Speicherabbild" geeignet, da andere Informationen eher verwirrend sind. Die hier protokollierten Informationen können Sie mit den Microsoft Debugging Tools oder dem Assistenten für die Absturzanalyse auslesen. Hier legen Sie zudem fest, in welchem Verzeichnis das Speicherabbild mit dem Fehler abgelegt werden soll. Um eine DMP-Datei mit den Tools zu analysieren, laden Sie diese ganz einfach in das Programm.

Die Microsoft Debugging Tools analysieren zusammen mit dem Assistenten für die Absturzanalyse die Protokolldatei, die Windows beim Auftreten des Bluescreens erzeugt hat. Der Inhalt lässt Rückschlüsse auf den Ursprung des Fehlers zu. Setzen Sie den Assistenten für die Fehleranalyse ein,

müssen Sie nicht die Debugging Tools starten, sondern den Assistenten. Zunächst wählen Sie aus, in welchem Verzeichnis das Werkzeug installiert ist. Auf der nächsten Seite entscheiden Sie, in welches lokale Verzeichnis der Assistent Daten ablegen soll.

Als Nächstes laden Sie die DMP-Datei des Bluescreens. Standardmäßig legt das Betriebssystem die Dateien im Verzeichnis "C:\Windows" als *memory.dmp* ab. Sie können den Pfad aber über den bereits beschriebenen Weg anpassen. Als Nächstes analysiert der Assistent für die Absturzanalyse die DMP-Datei und informiert über die Ursache des Bluescreens. Klicken Sie auf "Details", erhalten Sie mehr Informationen zum Bluescreen auf Basis der Debugging Tools.

## Bluescreen-Analyse mit Bordmitteln und nützlicher Freeware

Selbst wenn mit dem Assistenten für die Absturzanalyse die Untersuchung eines Systemfehlers wesentlich einfacher ist, lassen sich die Bluescreens ohne dieses Hilfsmittel nur mit den Debugging Tools untersuchen. Starten Sie dazu nach deren Installation die Debugging Tools über "Start / Programme / Debugging Tools für Windows / WinDbg". Über das Menü "File / Symbol File Path" tragen Sie am besten noch den Befehl

```
SRV*c:\websymbols*http://msdl.microsoft.com/download/symbols
```

ein. Dieser bewirkt, dass das Programm automatisch notwendige Ressourcen aus dem Internet in den Ordner "C:\Websymbols" herunterlädt, wenn diese für die Analyse benötigt werden. Eine ausführliche Anleitung zur Bluescreen-Analyse finden Sie auf der Seite [2].

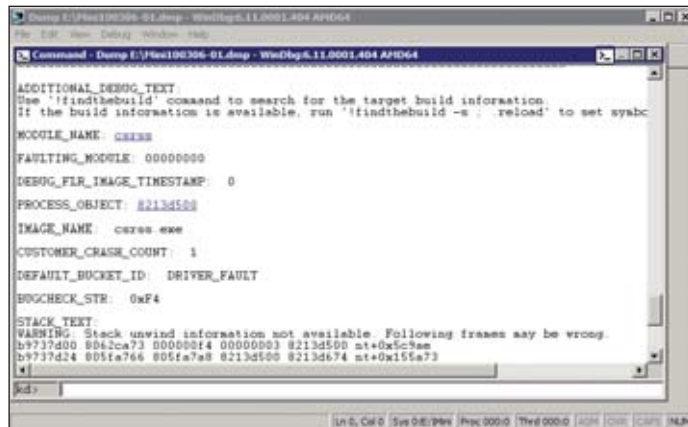


Bild 2: Mit den Microsoft Debugging Tools ist die Bluescreen-Analyse ohne den Assistenten für die Absturzursache möglich – wenn auch etwas komplizierter

Öffnen Sie eine Dump-Datei, also das Protokoll des Bluescreens, sehen Sie ein Fenster mit zwei Bereichen: "Command" und "Disassembly". Den meisten Anwendern reichen die Informationen unter Command. Die Daten unter Disassembly sind hauptsächlich für Programmierer gedacht, die Fehler in eigenen Anwendungen oder Treibern suchen. Interessant ist der Bereich "Bugcheck Analysis". Hier sehen Sie den Fehlercode, der sich sehr gut zur Recherche im Internet eignet. Durch die Eingabe des Befehls *!analyze -v* im Command-Fenster zeigen die Tools weitere Informationen an, die ebenfalls nützlich für die Recherche sind. In der Zeile "Probably caused by" sehen Sie die Datei, die vermutlich den Fehler verursacht hat. Über den Befehl *lm v m {Dateiname}* erhalten Sie weitere Informationen. Beachten Sie, dass Sie bei diesem Kommando den Dateinamen ohne Endung und direkt hinter "m", also ohne Leerzeichen, eingeben. Oft weist die Meldung einer bestimmten Datei auf einen Treiber-Fehler hin. Eine gute Möglichkeit, Absturz-Ursachen auf die Spur zu kommen, ist ferner die Software BlueScreenView, die Sie unter [3] kostenfrei herunterladen können. Mit der Software erhalten Sie weitere Informationen zu den Bluescreens und können so noch schneller die Fehler finden. Ein weiterer Vorteil des Tools ist zudem, dass Sie es nicht installieren müssen und es sich so von einem USB-Stick aus aufrufen lässt.



## Erstellen einer Rettungs-CD

Nach der Installation des DaRT steht auf dem Computer der ERD-Commander zur Verfügung. Mit diesem Werkzeug können Sie eine Rettungs-CD auf Basis von Windows PE 3.0 für Server mit Windows Server 2008 R2 und Windows 7 erstellen. Bei Windows PE 3.0 handelt es sich um eine Minimalversion von Windows 7, welche die Kernfunktionen des Betriebssystems enthält. Auch die Basisinstallationen von Windows 7 und Windows Server 2008 R2 basieren auf Windows PE 3.0. Während der Installation von Windows 7 lädt die Installationsroutine die Windows PE-Version auf der DVD über die Image-datei *boot.wim* im Verzeichnis "Sources". Auf dieser Basis kommt es dann zur Installation von Windows 7.

Zur Erstellung einer solchen Rettungs-CD starten Sie den ERD-Commander. Zunächst benötigen Sie eine Installations-DVD von Windows 7 oder Windows Server 2008 R2. Sie müssen zur Erstellung der CD das gleiche Betriebssystem verwenden, auf dem Sie den ERD-Commander ausführen. Von dieser DVD lädt der Assistent die notwendigen Daten zur Erstellung der CD. Im nächsten Schritt kopiert der Assistent die notwendigen Dateien auf den Computer. Auf der nächsten Seite können Sie auswählen, welche Tools Sie aus dem DaRT auf der Start-CD integrieren wollen. Generell ist zu empfehlen, dass Sie möglichst alle Tools verwenden, da diese nicht viel Speicherplatz benötigen.

Damit Sie den Assistenten für die Absturzanalyse über die Rettungs-CD verwenden können, müssen auf der CD auch die Microsoft Debugging Tools verfügbar sein. Dazu installieren Sie das Werkzeug zunächst am besten auf dem Rechner, auf dem Sie die Rettungs-CD erstellen. Wählen Sie nun beim Zusammenstellen des optischen Datenträgers den Assistenten für die Absturzanalyse als mit zu installierendes Tool aus, werden Sie in einem weiteren Fenster danach gefragt, wo sich die

Microsoft Debugging Tools befinden. Auf diesem Weg lassen sich diese Tools dann leicht auf der Rettungs-CD integrieren. Außerdem können Sie noch den System Sweeper auf der Rettungs-CD integrieren. Dieser kann befallene Computer von Viren befreien. Dazu können Sie die aktuellen Definitions-Dateien für das Tool herunterladen. Als Nächstes lassen sich noch zusätzliche Treiber in die Start-CD integrieren. Abschließend ist weiterhin die Integration eigener Tools oder Dateien in die ISO-Datei möglich. Die so erstellte ISO-Datei brennen Sie dann auf CD.

## Rettungs-CD des ERD-Commanders verwenden

Um die Rettungs-CD zu verwenden, booten Sie den Computer vom optischen Datenträger. Anschließend wählen Sie einige Optionen wie die Netzwerkanbindung und die Spracheinstellungen aus. Nach der Auswahl des Betriebssystems, das Sie auf dem Rechner reparieren wollen, können Sie über die Eingabeaufforderung mit den verschiedenen Tools arbeiten. Geben Sie zum Beispiel *explorer* ein, können Sie Dateien mit der CD kopieren. Über diese Anwendung können Sie die auf der CD integrierten Anwendungen leichter starten. Wählen Sie nach dem Booten die Option "Microsoft Diagnostic and Recovery Toolset" aus, öffnet sich ein neues Fenster mit den Tools, die Sie auf die Rettungs-CD integriert ha-

ben. Über diesen Bereich steuern Sie zudem die Netzwerkanbindung manuell, wenn kein DHCP-Server im Netzwerk vorhanden ist.

Neben den Spezialtools des DaRT enthält die Rettungs-CD die Standard-Software zur Systemwiederherstellung, wie die Eingabeaufforderung, die Reparatur des Bootmanagers und die Systemwiederherstellung. Außerdem ist auf der CD ein Lösungs-Assistent integriert. Dieser stellt Ihnen einige Fragen nach dem auf dem Computer auftretenden Problem und schlägt Ihnen dann entsprechende Lösungsmöglichkeiten vor. Die Umgebung ist multitaskingfähig, Sie können also mehrere Programme gleichzeitig ausführen. Im Kasten "Alle Tools des DaRT" finden Sie eine komplette Liste der zur Verfügung stehenden Werkzeuge.

## So erstellen Sie zur Systemrettung einen bootfähigen USB-Stick

Anstatt die ISO-Datei auf CD zu brennen, können Sie alternativ einen bootfähigen Flash-Stick verwenden, von dem Sie den Computer in das mit dem ERD-Commander erstellte Rettungs-Menü booten können. Gehen Sie dazu folgendermaßen vor:

1. Verbinden Sie den USB-Stick am besten mit einem Windows 7-Computer. Sie benötigen für den Betrieb das Befehlszeilentool *Diskpart*.

## SEMINARMARKT

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

[www.it-administrator.de/seminarmarkt](http://www.it-administrator.de/seminarmarkt)

**Log.in**  
consultants

Von Profis entwickelte  
High-Level-Trainings!

- ✓ Server-Based Computing
- ✓ Virtualisierung
- ✓ Softwaremanagement
- ✓ Herstellerunabhängig
- ✓ Praxisorientiert

Jetzt buchen!

[www.loginconsultants.de](http://www.loginconsultants.de)



Über das DaRT stehen Ihnen folgende Werkzeuge standardmäßig zur Verfügung:

**ERD-Registrierungs-Editor:** Dieses Tool ermöglicht die Bearbeitung des Windows-Systems, auf dem Sie den Datenträger gebootet haben. Die Bedienung entspricht dem ganz normalen Registry-Editor in Windows.

**Kennwort zurücksetzen:** Mit diesem Werkzeug können Sie lokale Kennwörter auf dem Computer zurücksetzen. Dazu wählen Sie über ein Dropdown-Menü bequem das Konto aus und setzen ein neues Kennwort.

**Absturzanalyse:** Dieser Bereich startet den bereits behandelten Assistenten für die Absturzanalyse über die Microsoft Debugging Tools.

**Datei wiederherstellen:** Mit diesem Tool startet ein sehr umfangreiches Suchfenster, mit dem Sie gelöschte Dateien retten können.

**Datenträger-Commander:** Das Tool ermöglicht umfassende Reparaturen am Datenträger und dem Master Boot Record (MBR).

**Datenträger-Löschung:** Mit diesem Tool können Sie Daten von Festplatten löschen. Zusätzlich bietet das Werkzeug die Option, Daten in vier Überschreib-Vorgängen endgültig zu löschen, so dass sich diese nicht mehr wiederherstellen lassen.

**Computerverwaltung:** Hierüber starten Sie die Computerverwaltung, die auch im normal gestarteten Windows zur Verfügung steht. Sie können Systeminformationen abrufen, die Ereignisanzeigen lesen, Dienste und Treiber konfigurieren und Festplatten mit der Datenträgerverwaltung konfigurieren. Die Ereignisanzeigen funktionieren auf Servern, die Mitglieder einer Domäne sind. Wir haben diese Funktion auf Servern mit Windows Server 2008 R2 als Domänencontroller und auf Servern mit Exchange Server 2010 getestet. Alle Daten lassen sich problemlos auslesen. Zusätzlich steuern Sie über die Computerverwaltung die Systemdienste des Rechners. Wenn also ein Systemdienst den Server zum Absturz bringt, können Sie diesen über die Computerverwaltung deaktivieren und dann den Server starten.

**Explorer:** Mit dem Explorer lassen sich Dateien kopieren, auch im Netzwerk. Der Umgang entspricht dem herkömmlichen Windows-Explorer.

**Hotfix-Deinstallation:** Macht ein System nach der Installation eines Patches Probleme, können Sie mit diesem Programm bequem Hotfixes vom Computer deinstallieren.

**SFC-Überprüfung:** Mit dieser Software reparieren Sie defekte Systemdateien. Das Tool scannt dazu die Systemdateien und setzt diese bei einem Problem automatisch wieder in Stand.

**Suchen:** Hierüber können Sie nach bestimmten Dateien auf dem Computer oder im Netzwerk suchen.


**Autonomer System Sweeper:** Dieses Tool entfernt Viren und andere Schadsoftware vom Rechner. Sie können die Definitions-Dateien nach dem Start aktualisieren, so dass diese bei jedem Scanvorgang auf dem neuesten Stand sind.

2. Starten Sie eine Befehlszeile über das Kontextmenü im Administratormodus.
3. Starten Sie die Festplattenverwaltung in der Befehlszeile mit *Diskpart*.
4. Geben Sie *list disk* ein.
5. Tippen Sie den Befehl *select disk {Nummer des USB-Sticks}* ein.
6. Nun folgt das Kommando *clean*.
7. Geben Sie *create partition primary* ein.
8. Der Befehl *active* aktiviert die Partition, was für den Bootvorgang nötig ist.
9. Formatieren Sie den Datenträger mit *format fs=fat32 quick*.
10. Geben Sie den Befehl *assign* ein.
11. Beenden Sie Diskpart mit *exit*.

Kopieren Sie den Inhalt der erstellten ISO-Datei in das Stammverzeichnis des USB-Sticks. Auf diesem Weg deponieren Sie beliebig weitere Tools auf den Speicher-Riegel und können diese verwenden, wenn Sie den Computer starten. Dazu müssen Sie lediglich die Eingabeaufforderung starten und mit *explorer* den Explorer. Über diesen können Sie dann auch per Doppelklick Tools starten. Die ISO-Datei entpacken Sie entweder als Archiv, zum Beispiel mit 7-Zip [4]. Es gibt zudem Werkzeuge, die ISO-Dateien direkt als CD-Laufwerk in Windows einbinden können. Allerdings sind diese nicht immer legal, da sie sich zur Erstellung von Raubkopien einsetzen lassen. Legale Programme hierzu sind zum Beispiel IsoBuster [5] oder Virtual CloneDrive [6].

Verbinden Sie den USB-Stick mit dem Computer und stellen Sie im BIOS oder dem Bootmenü ein, dass der Rechner vom Flash-Speicher bootet. Nun sollten Ihnen verschiedene Laufwerke zur Verfügung stehen, unter anderem alle lokalen Partitionen des PCs – das gilt auch für CD- oder DVD-Laufwerke. Das Dateisystem des USB-Sticks lädt Windows ebenfalls, so dass Sie Daten zwischen den lokalen Festplatten und dem USB-Stick kopieren können. Außerdem lassen sich auf dem Stick beliebige weitere portable Tools installieren. Unter [7] und [8] finden Sie dazu eine Vielzahl von Er-

weiterungen. Ebenso findet die komplette Microsoft Sysinternals-Suite [9] auf dem externen Speicher Platz, da sämtliche Tools ohne Installation laufen. Bei Wikipedia [10] finden Sie zusätzliche Informationen und Links zu portablen Anwendungen.

Im vierten und letzten Teil unserer Workshopserie widmen wir uns einem weiteren mächtigen Werkzeug des MDOP: Dem System Center Desktop Error Monitoring. Dieses Tool überwacht die Fehler aller Anwendungen und des Betriebssystems und listet die entsprechenden Meldungen an einer zentralen Stelle auf. In unserem Workshop erklären wir, wie Sie mit der Software bereits proaktiv für eine reibungslose Produktivumgebung sorgen. (In) 

- [1] **Microsoft Debugging Tools for Windows**  
[www.microsoft.com/whdc/devTools/debugging](http://www.microsoft.com/whdc/devTools/debugging)
- [2] **Anleitung zur Analyse von Bluescreens mit den Debugging Tools**  
[www.microsoft.com/whdc/devtools/debugging/debugstart.mspx](http://www.microsoft.com/whdc/devtools/debugging/debugstart.mspx)
- [3] **BlueScreenView**  
[www.nirsoft.net/utils/blue\\_screen\\_view.html](http://www.nirsoft.net/utils/blue_screen_view.html)
- [4] **ISO-Entpacker 7-Zip**  
[www.7-zip.org](http://www.7-zip.org)
- [5] **IsoBuster**  
[www.isobuster.com](http://www.isobuster.com)
- [6] **Virtual CloneDrive**  
[www.slysoft.com/de/virtual-clonedrive.html](http://www.slysoft.com/de/virtual-clonedrive.html)
- [7] **Portable App Directory**  
<http://portableapps.com/apps/>
- [8] **Pendrivelapps**  
[www.pendrivelapps.com](http://www.pendrivelapps.com)
- [9] **Windows Sysinternals**  
[www.sysinternals.com](http://www.sysinternals.com)
- [10] **Wikipedia-Artikel zu portabler Software**  
[http://de.wikipedia.org/wiki/Portable\\_Software/](http://de.wikipedia.org/wiki/Portable_Software/)
- [11] **SystemRescueCd**  
[www.sysresccd.org](http://www.sysresccd.org)
- [12] **Ultimate Boot CD**  
[www.ultimatebootcd.com](http://www.ultimatebootcd.com)

## Alle Tools des DaRT



## Links



Professionelles Ressourcenmanagement mit PRTG

# Effizient virtualisieren auf Basis von Netzwerk-Monitoring

**Die Virtualisierungstechnologie gewinnt für Unternehmen zunehmend an Bedeutung – insbesondere betrifft dies IT-Abteilungen, die unter erhöhtem Budgetdruck stehen. Energie- und Hardwarekosten steigen, da Rechenzentren mit ihren Ressourcen oft an ihre Grenzen stoßen. Virtualisierung kann dazu beitragen, Kosten einzusparen. Um die zuverlässige Performance sicherzustellen, ist es ratsam, ein professionelles Netzwerk-Monitoring zu integrieren.**

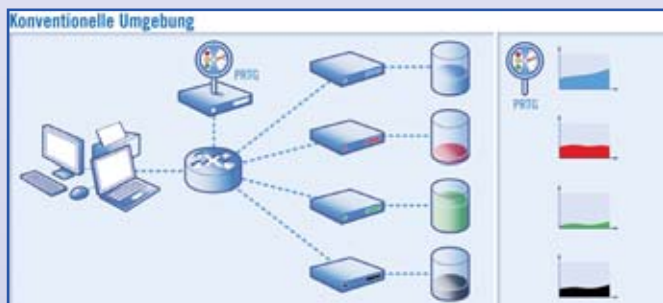
Viele IT-Anwendungen unterliegen hinsichtlich ihrer Nutzung starken zyklischen Schwankungen, da sie unregelmäßig in täglichen, wöchentlichen, monatlichen oder gar jährlichen Rhythmen genutzt werden. In einer nicht-virtualisierten Umgebung müssen für diese Schwankungen zu jeder Zeit sämtliche Kapazitäten bereitgestellt werden, um die maximalen Anforderungen erfüllen zu können. Gegebenenfalls sind sogar zusätzliche Investitionen in Rechen- und Speicherleistung erforderlich.

Servervirtualisierung ermöglicht eine dynamische Zuweisung von Rechenleistung und Speicherplatz, um Verbrauchsspitzen einzelner Applikationen abzufangen. Bei hoher Beanspruchung kann eine Anwendung so Ressourcen von anderen Applikationen nutzen, die zu diesem Zeitpunkt ungenutzt zur Verfügung stehen. Die Energie- und Hardwarekosten sinken, während die Kapazität der Rechenzentren steigt.

## Dynamische Ressourcenzuweisung

Virtualisierung befreit Applikationen somit von den Einschränkungen, die ihnen ein physikalischer Server auferlegt. Sie erlaubt den Betrieb mehrerer Applikationen auf einem einzelnen oder einer ganzen Reihe von Servern und stellt so einer Applikation die Ressourcen eines ganzen Netzwerks bereit. In der Praxis funktioniert dies jedoch nur dann, wenn ein schnelles und hochgradig zuverlässiges Netzwerk die physikalischen Server verbindet. Schließlich können schon geringe Einbußen in der Übertragungsgeschwindigkeit zu hohen Leistungseinbrüchen führen.

Um eine dynamische Zuweisung von Rechen- und Speicherkapazitäten zu erreichen, ist der Einsatz einer zuverlässigen Netzwerküberwachungslösung wie PRTG Network Monitor sinnvoll. Die intuitiv zu bedienende Software überwacht kritische Punkte des Netzwerks in Echtzeit und sammelt zentral Informationen zur Analyse



Jede Applikation befindet sich auf einem eigenen physikalischen Server mit angeschlossenem Speicher



Drei Anwendungen laufen in einer virtuellen Umgebung und teilen sich die Ressourcen des physikalischen Servers

der Ressourcenauslastung. Damit können Netzwerkverantwortliche langfristige Trends erkennen, vorausschauend planen und so Engpässen rechtzeitig vorbeugen.

PRTG bereitet zudem die Netzwerkdaten auf und stellt sie anschaulich in Graphen dar. Dabei reagiert PRTG bereits auf kleinste Änderungen im Netzwerkverkehr genauso wie auf Fehlfunktionen von Geräten oder Applikationen. Die Software kann so bei Störungen eines Servers oder seiner Netzwerkanbindung die zuständige IT-Abteilung sofort benachrichtigen, sodass diese umgehend reagieren und schlimmere Folgen verhindern kann.

## PRTG: Trends erkennen – Kapazitäten einplanen

Bereits in der Planungsphase zur Virtualisierung gibt PRTG Network Monitor Aufschluss über die zu erwartenden Leistungsansprüche der einzelnen Applikationen. Anhand von Langzeitanalysen kann der Anwender Trends sowie Lastspitzen erfassen und auf Basis dieser Informationen die erforderlichen Ressourcen bedarfsgerecht einplanen. Auch während des Betriebs gewährleistet PRTG die lückenlose Überwachung virtualisierter Umgebungen. Bei Server-Beeinträchtigungen alarmiert die Software den zuständigen Mitarbeiter umgehend.

**PAESSLER®**

**Paessler AG**

Burgschmietstraße 10

D-90419 Nürnberg

Tel.: +49 (911) 7 39 90 30,

Fax: +49 (911) 7 39 90 31

**E-Mail:** info@paessler.com

**URL:** www.de.paessler.com

**Ansprechpartner:**

Dorte Winkler



## Migration auf SharePoint 2010 (2)

# Umzug leicht gemacht

von Thomas Bär



Quelle: pixelio.de

Im ersten Teil unserer Workshopserie zeigten wir verschiedene Wege der Migration zu Sharepoint 2010 auf. Dabei eignet sich die In-Place-Migration nur für Infrastrukturen, die bereits für die neue Version von Microsofts Intranetwerkzeug vorbereitet sind. Doch unabhängig von der gewählten Variante sind weitere Arbeiten notwendig, um auch die Daten zu migrieren. Im abschließenden Teil unserer Workshopserie zeigen wir, wie der Import und Export der SharePoint-Daten reibungslos vonstattengeht. Und für den Fall, dass die Bordmittel nicht ausreichen, werfen wir noch einen Blick auf nützliche Drittanbietertools.

**D**ie beiden gangbaren Wege einer Migration zu SharePoint 2010 sind – wie in Teil 1 ausführlich dargestellt – die direkte Aktualisierung (In-Place-Migration) und das Anhängen der Inhaltsdatenbank. Beide bringen spezielle Voraussetzungen mit sich, die Sie auf jeden Fall genau prüfen sollten.

### Sichern und Wiederherstellen von Webseiten

Ganz gleich, welche Umzugsvariante für Sie in Betracht kommt, Sicherungen müssen Sie in jedem Fall zuvor anlegen. Im Idealfall erproben Sie das Einspielen der Sicherungen auf anderen Serversystemen im Vorfeld. Das Kommando für das Erstellen eines Backups einer ganzen SharePoint-Website lautet beispielsweise:

```
stsadm.exe -o backup -url
http://{Sitename} -filename {Pfad
mit Dateiname} -backupmethod full
```

Ist die Sicherungsdatei bereits vorhanden und soll überschrieben werden, verwenden Sie den Parameter “-overwrite”. In kleineren Umgebungen dauert dieses Backup lediglich einige Minuten. Regelmäßig über den Scheduler gestartet, ist eine Sicherung der Websites mit *stsadm.exe* somit leicht eingerichtet. Im Zusammenspiel mit den Volumenschattenkopien (VSS) in Windows ist auf einem ausreichend dimensionierten Windows-Fileserver eine Wiederherstellung unterschiedlicher Stände über einige Tage hin möglich. Wie bei allen anderen Backup-Aufgaben ist und bleibt die Übertragung der Sicherungsdateien auf ein Bandmedium mit unterschiedlichen Sicherungsgenerationen das Mittel der Wahl für ein ordentliches Backup.

### Wiederherstellung einer Website

Um eine über diesen Weg erzeugte Datei wieder einzuspielen, ist lediglich ein einziges Kommando erforderlich:

```
stsadm.exe -o restore -overwrite
-url http://{Sitename} -filename
{Pfad mit Dateiname}
```

Sofern Sie die Option “overwrite” verwenden, werden alle seit der Erstellung des Backups angelegten und modifizierten Elemente der Webanwendung überschrieben. Bereits mit diesem Einzeiler ist der Administrator in der Lage, unerwünschte Änderungen in SharePoint komplett rückgängig zu machen.

### Notfall-Wiederherstellung

Mithilfe von *stsadm.exe* ist die Wiederherstellung einer Webseite auch auf einem anderen Server möglich. Wird gleichzeitig die Domänenstruktur verlassen, spricht die Sicherung auf einer SharePoint-Installation in einer anderen Active Directory-Umgebung eingespielt, so müssen Sie die entsprechenden Rechte manuell ändern. Beispielsweise muss der Webanwendungs-Administrator neu festgelegt werden. So-



fern es sich nur um kleinere Installationen handelt, ist ein Nachpflegen der Accounts von Hand sicherlich akzeptabel, ansonsten helfen Skripte weiter. Eine Übernahme von Benutzern ist mittels `stsadm -o migrateuser` möglich, damit neue Anmeldenamen und die Informationen aus dem Benutzerprofilspeicher wieder zusammenpassen. Mit dem Befehl `stadm.exe -o restore` und der Option “-restoreconfigurationdatabase” führen Sie eine Wiederherstellung in einer anderen Serverumgebung durch.

## Export und Import innerhalb einer Version

Für einen Umzug innerhalb einer SharePoint-Version ist der Aufwand relativ gering. Neben der Zusammenführung von Websites ist dies mitunter dann nützlich, wenn das Ziel des Exports beispielsweise ein unter x64-Windows betriebener SharePoint 2007 ist, der über eine In-Place-Migration anschließend auf die neueste Version aktualisiert werden soll. Ein Import und Export von Version 2007 zu Version 2010 führt jedoch zu einer Fehlermeldung. Der Inhalt des virtuellen SharePoint-Papierkorbs geht bei dieser Über-

tragung generell verloren. Anstelle der bereits benannten Befehloptionen “Restore” und “Backup” kommen hier “Import” und “Export” zum Einsatz. Um einen Export einer Webseite auf einem Server durchzuführen, ist das Kommando

```
stsadm -o export -url {Sitename}
      -filename {Pfad mit Dateiname}
```

erforderlich. Auf einem anderen Server wird die Datei mit dem Befehl

```
stsadm -o import -url {Sitename}
      -filename {Pfad mit Dateiname}
```

eingespielt. Sollte die Seite auf dem neuen Server nicht existieren, so erscheint eine entsprechende Fehlermeldung. Diese Webseite kann entweder über die grafische Oberfläche der Zentraladministration angelegt werden. Schneller und per Skript umsetzbar ist das Anlegen der Zielwebseite mit dem Kommando:

```
stsadm -o createsite
      -url {Sitename}
      -owneremail {E-Mailadresse}
      -ownerlogin {Domäne\User}
```

## Über die Grenzen der Bordmittel hinaus

Ohne Frage liefert Microsoft bereits eine beachtliche Anzahl von Werkzeugen und Dokumentationen für Umzüge und Migration in der SharePoint-Produktfamilie mit. Mit steigender Komplexität der eingerichteten Sites steigt der administrative Aufwand jedoch mit an. Dabei muss es sich nicht einmal um eine sehr große Anzahl unterschiedlicher Server handeln: Sollen die verschiedenen Teamwebseiten von Abteilungen innerhalb des Unternehmens auf einen anderen Server übertragen werden, so ist häufig eine exakte terminliche Planung erforderlich. Kaum ein Administrator wird gewillt sein, jedes Mal einen Script-Job zu starten und das Resultat manuell zu prüfen. Professionelle Lösungen wie der “Migration Manager for SharePoint” von Quest Software bieten sich für derlei Vorhaben an.

In einer recht einfach gehaltenen Maske geben Sie bei Quest die Quelle und das Ziel an und richten – sofern erforderlich – eine neue Datenbank in diesem Zug mit ein. Um Detailfragen, wie beispielsweise unterschiedliche Patch-Stände der Server, müssen Sie sich bei Verwendung dieser Software-Lösung nicht kümmern. Egal, ob von SharePoint Portal Server 2003 zu Microsoft Office SharePoint Server 2007, SharePoint Services zu SharePoint Services oder Services zu einer großen SharePoint-Server-Installation: Der “Migration Manager for SharePoint” von Quest Software verarbeitet die Umstellungen. Besonders bei einem Wechsel eines 2003er SharePoint-Servers auf eine aktuellere Version sind die automatisierten Umstellungen eine große Hilfe. Ältere Templates, auf denen das Design und die Funktionalität basieren, werden durch einen so genannten “Post-Processing Web Part Wizard” übernommen und angepasst.

Äußerst angenehm für Administratoren sind die Jobs im Migration Manager. Diese lassen sich über einen einfachen Sche-

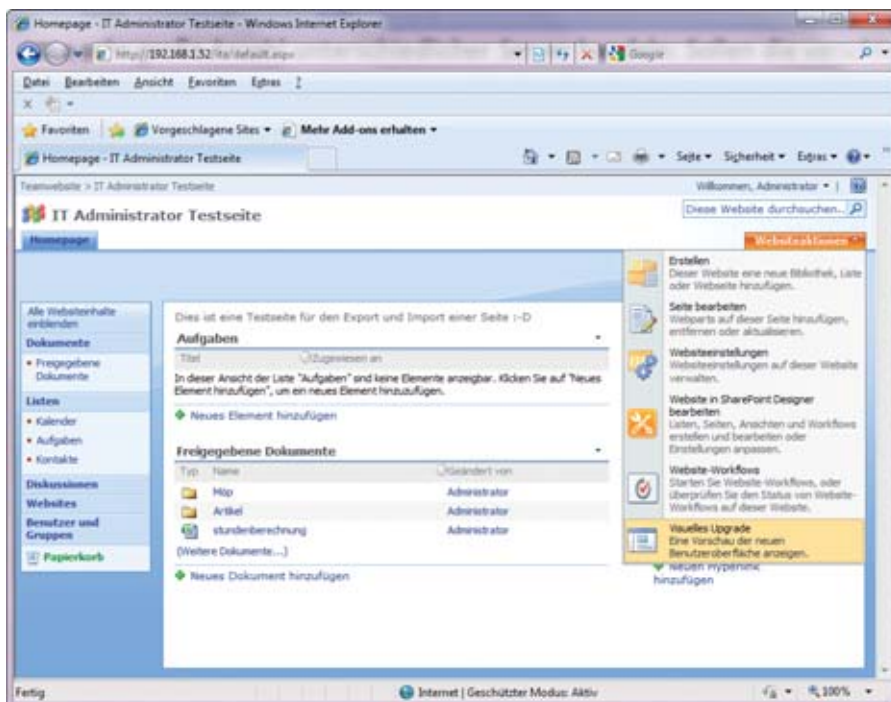


Bild 1: Nach der Installation verhalten sich die SharePoint-Seiten weitgehend wie ihre Vorgänger, bis das Visual Upgrade ausgeführt wird



duler zu einer bestimmten Zeit starten und auf Wunsch wiederholen, was die Abbildung einer "dynamischen Weitermigration" ermöglicht. Sollten auf Ursprungs-Sites neue Inhalte generiert werden, lassen sich diese auf den neuen SharePoint übertragen. Anstelle jeden einzelnen Auftrag immer wieder über das Interface manuell einzutragen, bietet sich der Import einer zuvor definierten Excel-Datei mit den Job-Details an.

Neben Migrations- und Umzugsvorhaben eignet sich die Quest-Software zudem für das so genannte "DB Splitting". Die aktuelle Empfehlung für Microsoft SharePoint 2007 in Bezug auf die Datenbankgröße liegt zwischen 60 und 100 GByte. Theoretisch ließen sich zwar bis zu 16 TByte in einer einzigen Microsoft SQL-Datenbank ablegen, doch vor dem Hintergrund der Backup- und Restore-Geschwindigkeit sind solche Dimensionen bei aktuellen Durchsatzraten der Netzwerke kaum praktikabel. Wird eine einzelne "Site Collection" zu groß, lässt sich diese mit Quest-Mitteln aus der einen Datenbank in eine andere "umziehen". Wie bei allen Vorgängen dieser Art informiert die "Pre-Migration Analysis" den Administrator über die zu erwartende Dauer des Vorgangs und die Datendimensionen, die bewegt werden müssen.

Der Vollständigkeit halber sei erwähnt, dass der "Migration Manager for SharePoint" von Quest nur eine von mehreren Lösungen aus dem Portfolio des Herstellers ist.

Der "Site Administrator for SharePoint" ist eine optimierte Administrationsoberfläche für die SharePoint-Technologie. Mit dieser Software ist es möglich, eine SharePoint-Installation, wie jedes andere Microsoft-Produkt, über die "Microsoft Management Console" (MMC) zu verwalten. Warum Microsoft nicht selbst eine Implementierung für seine eigene Administrationskonsole vornimmt, bleibt rätselhaft. Für die Übernahme von "öffentlichen Ordnern" aus Exchange-Installationen zu SharePoint bietet Quest einen Migrationshilfe, wie auch für die Übernahme von Lotus Notes-Installationen.

Das Security Management des Site Administrators unterstützt Administratoren zudem bei


der Beantwortung weiterführender Fragen wie "Worauf hat ein bestimmter Benutzer eigentlich überhaupt Zugriff?" oder "Wo befinden sich möglicherweise doppelte Inhalte?". Ein Reporting über eine gesamte SharePoint-Farm, ein mit Bordmitteln gänzlich unmögliches Unterfangen, rundet einen positiven Gesamteindruck der Quest-Software ab. Pünktlich zum offiziellen Erscheinungstermin des neuen SharePoint Server 2010 im Juni 2010 veröffentlichte Quest den "Migration Manager for SharePoint" für Umzüge von der 2003er hin zur aktuellen 2010er-Version. (dr) 



Bild 2: Nach Ausführung des Visual Upgrades ist die Umstellung auf SharePoint 2010 abgeschlossen



## Lesen Sie den IT-Administrator als E-Paper

Testen Sie kostenlos und unverbindlich die elektronische IT-Administrator Leseprobe auf [www.it-administrator.de](http://www.it-administrator.de).

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

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

[www.it-administrator.de/magazin/epaper](http://www.it-administrator.de/magazin/epaper) 



# Sichere Notebooks für den Innen- und Außendienst

## Reiseschutz- versicherung

von **Andreas Roscher**

Viele Unternehmensnotebooks wechseln ständig zwischen externen VPN-Zugängen und dem internen Firmennetz hin und her. Soll das System den beiden unterschiedlichen Nutzungsarten gerecht werden – etwa mit den gewohnten Anwenderrechten im internen Netz und flexibler Wahl des Netzzugangs im Außendienst – bietet sich eine Dualbetriebssysteminstallation an. Dabei ist die Anforderung hinsichtlich der Sicherheit dieses Rechners natürlich sehr hoch, vor allem wenn wichtige Daten mit dem Anwender auf Reisen gehen. Diese Daten lassen sich nur über eine Verschlüsselung absichern. In diesem Workshop führen wir Sie Schritt für Schritt durch die Bespielung und Verschlüsselung des Notebooks am Beispiel Windows 7 und zeigen zudem Ansatzpunkte zur Automatisierung auf.



Mobile Mitarbeiter sollten auf die Sicherheit achten – auch auf die ihres Notebooks

**W**indows 7 bietet in der Ultimate Version die Möglichkeit einer Laufwerksverschlüsselung mit dem Programm BitLocker. BitLocker benötigt eine primäre Partition zum Booten, um auf die verschlüsselte Windows-Partitionen zuzugreifen. Damit mal die eine und mal die andere Windows-Bootpartition angesprungen werden kann, stellen wir den Windows-Bootpartitionen noch eine Managementpartition voran. Auf dieser Partition befindet sich auch die Software, die es erlaubt, jede der beiden Windows-Installationen mit Hilfe einer nicht-bootbaren USB-Festplatte (oder USB-Stick) erneut in Betrieb zu nehmen. Aus diesem Ansatz heraus ergibt sich das Partitionierungsschema (Kasten "Partitionierungsschema").

### Partitionierung einrichten

Die Managementpartition enthält ein minimales Linux aus der OMA-Distribution. Sie können aber auch per Hand ir-

gendem Linux auf die erste primäre Partition legen und den Bootmanager passend einrichten. Da Windows nicht in der Lage ist, von erweiterten Partitionen zu booten und die Verteilung des unverschlüsselten Windows eine primäre Partition benötigt, die dann um eine weitere primäre Partition ergänzt werden muss, bleibt uns vorerst nur der Ausweg, das zweite Windows auf eine USB-Festplatte zu legen (Kasten "Partitionierung mit USB-Festplatte").

Die Windows-Installation liegt als unverschlüsseltes Partitionsimage vor und wird noch vor dem ersten Booten von Windows automatisch auf die gewünschte Größe von Laufwerk C ausgedehnt. Die Laufwerke D und E werden als leere NTFS-Dateisysteme formatiert. Noch vor dem ersten Booten von Windows nutzen wir das Laufwerk D, um die Installationsquellen der Softwarepakete dort abzulegen. So ist das Notebook schon beim ersten

Typ	Laufwerk	Größe	Funktion
Primary	-	0,4 GByte	Managementpartition
Primary	S:	1,5 GByte	1. Windows 7-Bootpartition
Primary	S:	1,5 GByte	2. Windows 7-Bootpartition
Logical	C:	20,0 GByte	Windows 7 Nr. 1
Logical	D:	30,0 GByte	Windows 7 Nr. 1
Logical	C:	20,0 GByte	Windows 7 Nr. 2
Logical	D:	30,0 GByte	Windows 7 Nr. 2
Logical	E:	120,0 GByte	Plattenrest

Partitionierungsschema





Typ	Laufwerk	Größe	Funktion
Primary	-	0,4 GByte	Managementpartition
Primary	S:	1,5 GByte	1. Windows 7-Bootpartition
Primary	C:	20,0 GByte	Windows 7 Nr. 1
Logical	D:	30,0 GByte	Windows 7 Nr. 1
Logical	D:	30,0 GByte	Windows 7 Nr. 2
Logical	E:	120,0 GByte	Plattenrest
<b>USB-Platte</b>			
Primary	-	0,4 GByte	Managementpartition
Primary	S:	1,5 GByte	2. Windows 7-Bootpartition
Primary	C:	20,0 GByte	Windows 7 Nr. 2

## Partitionierung mit USB-Festplatte



```

echo BITLOCKER = DRIVE C + D ===== CONFIG RUN
REM -rk or -Recoverykey
REM -sk or -Startupkey
REM -rp or -RecoveryPassword

c:
cd \windows\system32

set PROG=cscript manage-bde.wsf
IF EXIST manage-bde.exe set PROG=manage-bde

echo ++ %PROG% -status c:
      %PROG% -status c:

echo ++ wait for windows ... ping -n 20 localhost
ping -n 20 localhost > c:\windows\Temp\omaping.log

set DRIVE=a
echo .. EXIST e:\bitlocker ?
IF %DRIVE%==a (
  IF EXIST e:\bitlocker set DRIVE=e
)
IF %DRIVE%==a (
  echo .. EXIST f:\bitlocker ?
  IF EXIST f:\bitlocker set DRIVE=f
)
IF %DRIVE%==a (
  echo .. EXIST g:\bitlocker ?
  IF EXIST g:\bitlocker set DRIVE=g
)
IF %DRIVE%==a (
  echo .. EXIST h:\bitlocker ?
  IF EXIST h:\bitlocker set DRIVE=h
)
IF %DRIVE%==a (
  echo .. EXIST i:\bitlocker ?
  IF EXIST i:\bitlocker set DRIVE=i
)
IF %DRIVE%==a (
  echo .. EXIST j:\bitlocker ?
  IF EXIST j:\bitlocker set DRIVE=j
)
IF %DRIVE%==a (
  echo .. EXIST k:\bitlocker ?
  IF EXIST k:\bitlocker set DRIVE=k
)
IF %DRIVE%==a (
  echo .. EXIST l:\bitlocker ?
  IF EXIST l:\bitlocker set DRIVE=l
)
IF %DRIVE%==a (
  echo .. EXIST m:\bitlocker ?
  IF EXIST m:\bitlocker set DRIVE=m
)

IF %DRIVE%==a (
  echo .. EXIST n:\bitlocker ?
  IF EXIST n:\bitlocker set DRIVE=n
)
IF %DRIVE%==a (
  echo .. EXIST o:\bitlocker ?
  IF EXIST o:\bitlocker set DRIVE=o
)
IF %DRIVE%==a (
  echo .. EXIST p:\bitlocker ?
  IF EXIST p:\bitlocker set DRIVE=p
)
IF %DRIVE%==a (
  echo .. EXIST q:\bitlocker ?
  IF EXIST q:\bitlocker set DRIVE=q
)

IF NOT EXIST %DRIVE%\bitlocker GOTO END
IF EXIST %DRIVE%\bitlocker echo .. FOUND
%DRIVE%\bitlocker
Echo

REM windows 7 is not amused about keys in sub
directories !!
REM set RKOPT=%DRIVE%\bitlocker
REM set SKOPT=%DRIVE%\bitlocker
REM windows 7 erlaubt keine Schlüssel in Unterver-
zeichnissen

set RKOPT=%DRIVE%\
set SKOPT=%DRIVE%\

set LOGF=%DRIVE%\bitlocker\c.log
echo .. LOGFC %LOGF%
%PROG% -on C: -rk %RKOPT% -sk %SKOPT% -rp > %LOGF%
%PROG% -status c: > %LOGF%

set LOGF=%DRIVE%\bitlocker\d.log
echo .. LOGFD %LOGF%
%PROG% -on D: -rk %RKOPT% -sk %SKOPT% -rp > %LOGF%
%PROG% -protectors -disable D: > %LOGF%
%PROG% -status d: > %LOGF%

:END
IF NOT EXIST %DRIVE%\bitlocker ( echo ERROR: No bit-
locker key drive found
echo ERROR: %DRIVE%\bitlocker is the wrong default
name
echo ERROR: We search from e:\bitlocker up to t:\bit-
locker to find your USB device
pause )

echo BITLOCKER = DRIVE C + D ===== CONFIG END

```

## Listing 1: Nachbehandlungsprozedur



Booten einsatzbereit für den mobilen Nutzer, da es sich selbständig zu Ende installiert und die geplante Verschlüsselung der Laufwerke im Alleingang vornimmt. Laufwerk E bleibt hier unverschlüsselt, um den Datenaustausch zwischen den beiden verschlüsselten Windows-Systemen zu ermöglichen. Zwingend ist das aber nicht, da hierfür auch ein anderer Datenträger wie etwa ein USB-Stick zum Einsatz kommen könnte oder Sie verschlüsseln einfach alle Partitionen und ein Datenaustausch zwischen den beiden Windows-Installationen ist nur möglich, wenn der Computer am Firmennetz hängt. Letztendlich entscheidet die Security-Policy Ihrer Firma, welche der hier beschriebenen technischen Möglichkeiten zur Anwendung kommt.

Im Folgenden zeigen wir die Details des Deployments. Selbstverständlich können Sie statt BitLocker auch eine andere Software zur Partitionsverschlüsselung einsetzen. Als Name für das Deployment wählen wir "Windows\_ultimate\_bitlocker\_2x". Unter diesem Namen hinterlegen wir alle Einstellungen, um letztendlich nur noch den Namen des Rechners und diesen Deployment-Namen auszuwählen, wenn ein neues Notebook erstmalig im Firmennetz gespielt wird.

### Erste Laufwerksverschlüsselung

Nachdem Sie die Linux-Partition gespielt haben und das Partitionierungsschema umgesetzt ist, wird Windows auf der dritten primären Partition installiert. Lassen sich Windows Nr.1 und Linux über das Bootmenü des Bootmanagers von Linux alternativ booten, kann unter Windows die Laufwerksverschlüsselung aktiviert werden. Per Voreinstellung verlangt BitLocker ein TPM-kompatibles BIOS. Wir wollen uns aber gegen einen separaten USB-Stick autorisieren. Nach dem Anmelden als Administrator rufen Sie dazu das Programm *gpedit.msc* auf. Mit der Maus geht es dann in den Zweig "Computerkonfiguration / Administrative Vorlagen / Windows

Komponenten / BitLocker Laufwerksverschlüsselung / Systemsteuerungssetup: Erweiterte Startoptionen aktivieren". Nachdem Sie dies aktiviert haben, ist kein TPM-kompatibles BIOS mehr erforderlich. Für die vollautomatische Bespielung ist der notwendige Mausklick jedoch ungünstig. Verpackt in ein Softwarepaket erledigen wir das mit dem Laden einer Registry-Datei:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\
Policies\Microsoft\FVE]
"EnableNonTPM"=dword:00000001
"UsePIN"=dword:00000002
"UsePartialEncryptionKey"=
dword:00000002
```

Somit besteht das fertige Softwarepaket "windows7\_bitlocker\_allow\_usb" aus einer Datei mit den Keys und einer Nachbehandlungsprozedur (*regedit /S bitlocker\_allow\_usb.reg*).

Das noch unverschlüsselte Pärchen aus den Laufwerken S und C bringen wir einmalig manuell mit Hilfe der Windows-DVD auf den Weg. Für das Erstellen von Laufwerk S muss vor dem Booten von der Windows-DVD die neue BitLocker-Boot-Partition zur aktiven Partition werden. Damit davon auch wirklich gebootet werden kann, müssen Sie

die Windows-Bootdateien auf die neue Boot-Partition kopieren. Nach dem Booten mit der Windows-DVD gibt es einen ersten Reparaturanlauf und einen Neustart. Erst danach kommt es zur Anzeige einer wiedergefundenen Windows 7-Installation. Jetzt können Sie auf der DVD die Systemstartreparatur wählen. Nach einem weiteren Neustart bootet Windows von der kleinen Partition und fährt die Installation auf der großen Partition hoch. Nun sind alle Voraussetzungen für die BitLocker-Laufwerksverschlüsselung erfüllt. Nach der erfolgreichen Aufteilung von Windows in eine Boot- und eine Root-Partition sichern Sie beide Partitionen in dem noch unverschlüsselten Zustand als Partitionsimages und können diese so für das Rollout aller Notebooks verwenden.

Per Mausklick ließe sich nun die Laufwerksverschlüsselung des ersten Windows aktivieren. Da wir jedoch diesen Schritt immer wieder neu und automatisiert ausführen möchten, wenn ein Notebook neu bespielt wird, nutzen wir die entsprechenden Befehle in einem Softwarepaket. Das Softwarepaket "winzall\_bitlocker\_drive\_encryption\_4\_usb\_on\_h\_2\_drive\_c+\_d" besteht nach Fertigstellung nur aus einer Nachbehandlungsprozedur (Siehe Listing 1).

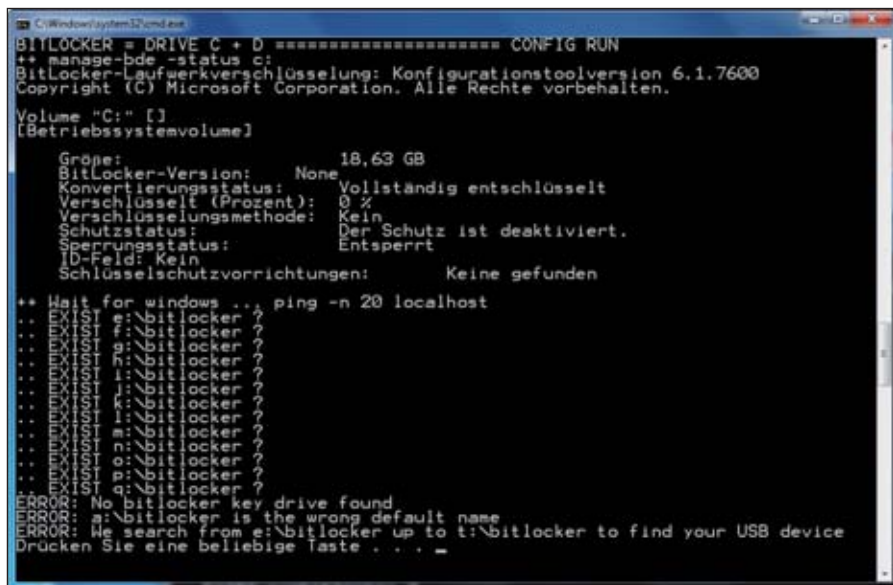


Bild 1: Die Verschlüsselung bricht ab, falls BitLocker das erwartete USB-Laufwerk nicht findet

Arbeiten heißt für Sie zusammenarbeiten?  
Persönliche Weiterentwicklung?  
Vereinbarkeit von Beruf und Familie?



Wir nehmen Sie mit auf den sepago way of work and life zu spannenden Projekten!

Alles was Sie mitbringen müssen ist...



...echte Leidenschaft für IT!

Prüfen Sie uns auf Herz und Nieren und finden Sie heraus, ob wir der passende Weggefährte für Ihren nächsten Karriereschritt sind:



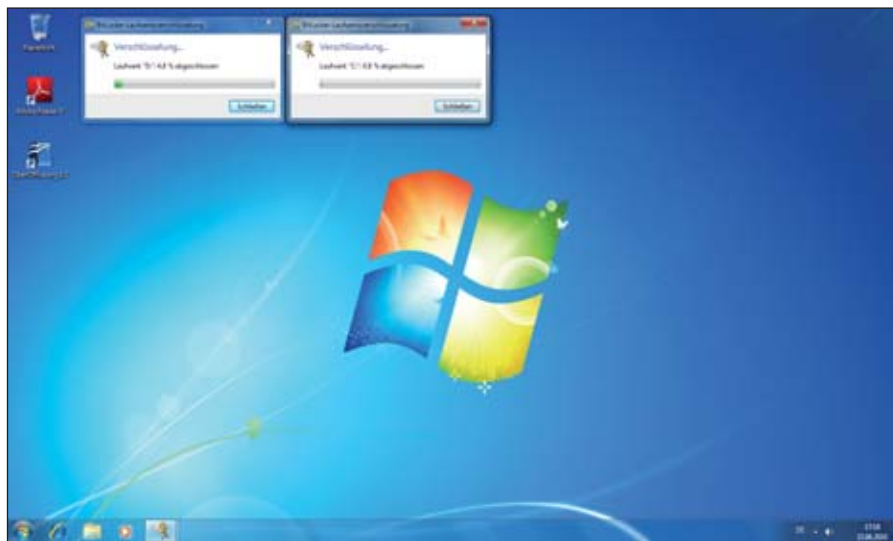


Bild 2: Während Windows noch die Daten verschlüsselt, kann der Anwender schon arbeiten

Auf einem beliebigen Laufwerk befindet sich der USB-Stick. Damit dieser auch sicher durch Windows gefunden wird, legt die Prozedur mit Hilfe des Programms *ping* eine kleine Verschnaufpause ein. Spätestens, wenn der Client nach dem Bespielen das zweite Mal bootet, muss ein USB-Stick eingesteckt sein, damit die Key-Dateien für den Bootzugriff dort abgelegt werden können. Fehlt der USB-Stick oder wird auf dem USB-Stick das Verzeichnis "bitlocker" nicht gefunden, bricht das Deployment ab (Bild 1).

In dem Verzeichnis findet sich in der Datei *c.log* auch das automatisch erzeugte Passwort. Damit ist zur Not noch ein Login möglich, wenn der Stick einmal verloren geht. Wo die Datei *c.log* sicher abzulegen und zu verwalten ist, muss wieder die Security-Policy Ihrer Firma entscheiden. In dem hier vorliegenden Fall hat die Bespielung "Windows\_ultimate\_bitlocker\_2x" folgende nachzuspielende Softwarepakete:

```
0_cygwin_1.5.24_2_oma_sshd_4_xpsp3_2
003_vista_win7
win0all_acrobat_reader_9.0_msi
win0all_open_office_311_msi
win0all_windows_firewall_allow_ping_
and_ssh_cmd
windows7_bitlocker_allow_usb
winzall_bitlocker_drive_encrypti-
on_4_usb_on_h_2_drive_c+_d
```

Die Komplettbespielung von "Windows\_ultimate\_bitlocker\_2x" stellt in wenigen Minuten alle Partitionen her (S, C, D und E). Beim ersten Booten erhält der Rechner seine Identität (Computernamen, SID), beim zweiten Booten werden die restlichen Aufgaben erledigt (Arbeitsgruppe und alle vier Softwarepakete). Die eigentliche Verschlüsselung läuft nach dem dritten Booten im Hintergrund ab. Nach dem dritten Booten ist eine Anmeldung möglich und es kann auch gearbeitet werden, während die Verschlüsselung noch läuft (Bild 2). Wie weit schon verschlüsselt ist, verrät das Programm *manage-bde.wsf* über die Option "-status".

Sobald die Verschlüsselung angelaufen ist, kommt beim nächsten Neustart die Stunde der Wahrheit. Das Booten der Windows-Partition funktioniert nur noch mit eingestecktem USB-Stick. Es darf also auch während der Verschlüsselung ein Neustart erfolgen. Die Verschlüsselung wird dann beim nächsten Neustart fortgesetzt.

### Zweite Laufwerksverschlüsselung


Sobald die Verschlüsselung auf der internen Platte gelaufen ist, kann die automatische Verschlüsselung auf der externen Platte anlaufen. Das geht in der

vorgestellten Konfiguration nur durch die Auswahl des Windows auf der externen Platte, wenn das Notebook sich beim Booten mit dem Bootloader der Managementpartition meldet. Automatisieren lässt sich der komplette Ablauf nur, wenn die beiden Windows-Pärchen auf die interne Platte kommen.

Dazu muss das doppeläufige Windows-Paar aus Boot- und Root-Partition umgestellt werden. Statt der Kombination aus primärer und primärer Partition erstellen Sie eine Kombination aus primärer und sekundärer Partition. Da in unserem Fall beide Laufwerke als Partitionsimages gesichert sind, lässt sich problemlos für die Bespielung diese Partitionierung wählen, obwohl der Abzug der Windows-Root-Partition ursprünglich von einer primären Partition erfolgt ist.

Als Bootmanager auf der Managementpartition kann Lilo oder GRUB zur Anwendung kommen. GRUB können Sie in der Version 0.97 oder 1.98 einsetzen. Ob beim GRUB von der Möglichkeit Gebrauch gemacht wird, beim Booten Partitionen zu verstecken, ist wieder eine Frage der Security-Policy. Die verlangt vielleicht auch noch ein extra Passwort für den Bootmanager.

### Fazit

Der Einsatz einer unverschlüsselten und frei gestaltbaren Bootpartition mit einem frei wählbaren Bootmanager ist die Grundlage, um mit dem Rest des Computers jede Art von Verschlüsselung zu betreiben, die die Security-Policy einer Firma als Anforderung definiert. Die Konfiguration lässt sich dann noch so weit automatisieren, dass sich der Anwender sogar selbstständig immer wieder mit einem verschlüsselten Notebook versorgen kann. Die Kosten gehen damit automatisch in den Keller, da Notebooks nie mehr zu Administrationszwecken eingesammelt werden müssen. Für den IT-Verantwortlichen gilt dann das Motto: "Aus den Augen, aus dem Sinn". (jp) 

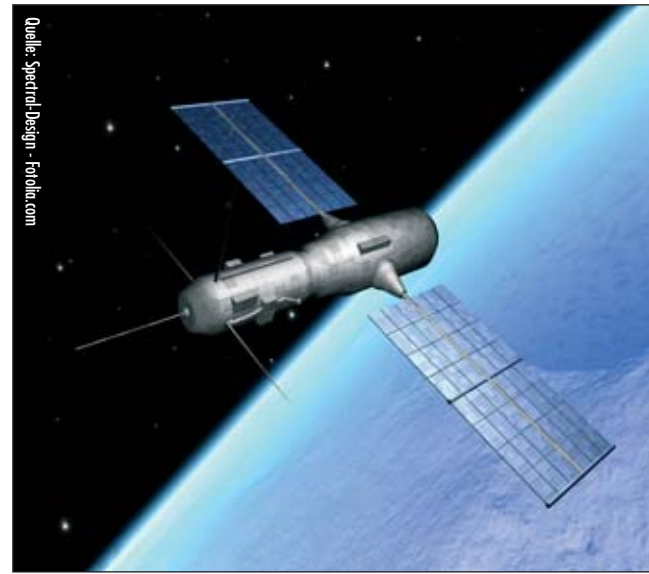


## Linux-Systeme mit Spacewalk verwalten (1)

# In den Weiten von Linux

von Thorsten Scherf

Linux-Systeme von Hand zu verwalten, ist ab einer bestimmten Größe der Systemlandschaft zeitaufwendig. Mit dem Projekt Spacewalk entstand eine Open Source-Lösung, mit der sich Linux-Systeme an zentraler Stelle aus verwalten lassen. IT-Administrator stellt Ihnen das Programm vor und zeigt, welche Möglichkeiten es zur Software- und Patchverteilung bietet.



**F**olgendes Szenario dürfte jedem Administrator bekannt vorkommen: Der Mailserver, der für die externe Mailkommunikation zuständig ist, hat ein Sicherheitsproblem. Zum Glück ist Hilfe in Form eines Update-Paketes schon vorhanden. Nur ist dieses Paket nicht nur auf einem einzelnen System, sondern auf einer Vielzahl von Systemen einzuspielen. Anstatt die neue Software umständlich auf den einzelnen Maschinen zu installieren, bietet es sich an, dies von zentraler Stelle aus zu erledigen. Genau das ist eine der Aufgaben von Spacewalk [1], der Open Source-Variante von Red Hats Network Satellite Server. Darüber lassen sich nicht nur Software-Pakete, sondern auch einzelne Konfigurationsdateien auf Linux-Systeme verteilen. Auch die Installation von neuen Systemen ist problemlos möglich, die Funktionsweise dabei einfach.

### Kanalbasierte Paketverteilung

Damit ein System auf die Spacewalk-Ressourcen zugreifen kann, muss sich dieses zuerst auf dem Server registrieren. Hierfür kommt entweder eine Kombination aus Benutzernamen und Passwort zum Einsatz oder ein sogenannter Aktivierungsschlüssel, der im

Vorfeld auf dem Spacewalk-Server erzeugt wurde. Das Linux-System erscheint nach erfolgreicher Registrierung auf der grafischen Weboberfläche des Spacewalk-Servers. Existieren bereits weitere Ressourcen auf dem Server, so können Sie diese nun dem System zuweisen. Zu den Ressourcen, die üblicherweise in Kanälen sortiert sind, zählen beispielsweise Software-Pakete oder Konfigurationsdateien. Ein System besitzt immer genau einen Basiskanal mit optionalen Unterkanälen. Der Basiskanal enthält dabei das RPM-basierte Betriebssystem, beispielsweise Red Hat En-

terprise Linux, Fedora oder CentOS. In den Unterkanälen befinden sich zusätzliche, vom Betriebssystem unabhängige Software-Pakete wie die Red Hat Cluster-Suite oder der 389-Directory-Server. Spacewalk ist dabei auch in der Lage, bestehende Kanäle zu klonen oder komplett neu zu erzeugen. Somit haben Sie eine sehr genaue Kontrolle über den Software-Stack, den Sie über Spacewalk anbieten. Mit Hilfe der Konfigurationskanäle verteilen Sie die entsprechenden Konfigurationsdateien für Ihre Software-Pakete. Spacewalk hält dabei auch ältere Versionen Ihrer Da-

by the apache and tomcat users. From within the specified tree path, a kernel should be available at "/images/pxeboot/vmlinuz" and an initrd image should be available at "/images/pxeboot/initrd.img". For instance, if you have media located on the Spacewalk server at: /var/distro-trees/rhel-5-server/ you would specify that path as your Tree Path value which would check for a kernel and initrd here: /var/distro-trees/rhel-5-server/images/pxeboot/

Create Kickstart Distribution

Distribution Label\*: fedora-12-i386

Tree Path\*: /var/distros/fedora-12-i386

Base Channel\*: Fedora 12 i386

Installer Generation\*: Fedora

Kernel Options:

Post Kernel Options:

Create Kickstart Distribution

Bild 1: Die Kickstart-Verteilung hilft Bare-Metal-Systemen auf die Beine

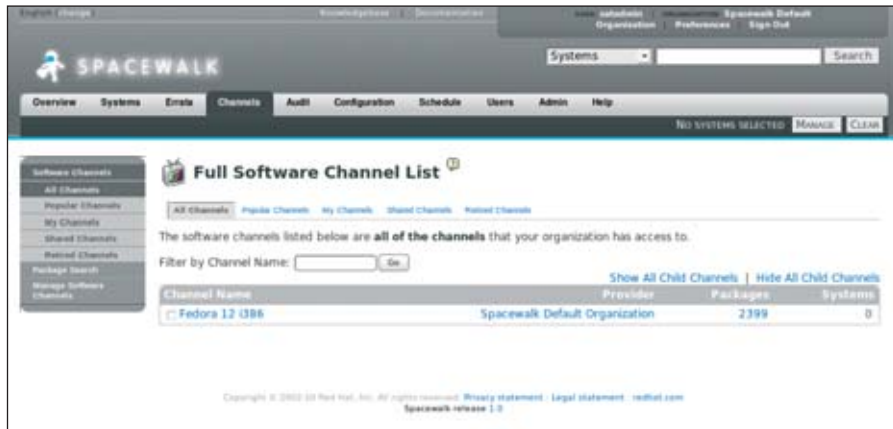


Bild 2: Die Software-Pakete werden über Kanäle bereitgestellt

teien vor, so dass Sie zu einem beliebigen Zeitpunkt zu einer älteren Version einer Konfigurationsdatei "zurückrollen" können.

Die Installation der gewünschten Software-Pakete oder Konfigurationsdateien aus diesen Kanälen erfolgt entweder vom Ziel-System aus oder zentral über die Spacewalk-Weboberfläche. Damit die Installation bei einer Vielzahl von Systemen nicht zur Qual wird, können Sie Ihre Systeme dabei in logische Gruppen einsortieren und die Installation einer Ressource dabei auf diese Gruppe anwenden. Beispielsweise bietet es sich an, alle Mailserver an die Spacewalk-Gruppe "Mail-Server" anzubinden. Kommt nun eine neue Version Ihrer Mailserver-Software heraus, so weisen Sie Spacewalk einfach an, das Update auf diese Gruppe anzuwenden. Alle Systeme, die Mitglied der Gruppe sind, erhalten das Software-Update somit automatisch. Die Installation erfolgt dabei standardmäßig im Poll-Verfahren – das heißt, Client-Systeme fragen nach einem festgelegten Zeitintervall (standardmäßig alle vier Stunden) auf dem Server nach, ob nach der letzten Abfrage neue Aktionen für das System definiert wurden. Ist dies der Fall, so führt Spacewalk diese aus.

Alternativ hierzu können Sie die Installation von Software-Paketen sowie andere Aktionen auch direkt im Push-Ver-

fahren anweisen. Über das Jabber-Protokoll stehen hierbei Client-System und Spacewalk-Server ständig miteinander in Kontakt. Sobald Sie eine neue Aktion definieren, führt Spacewalk diese unmittelbar auf dem Client aus. Die Kommunikation erfolgt jedoch nach wie vor vom Client zum Server, was für entsprechende Zugriffsregeln auf der Firewall sehr wichtig ist. Eine Liste der freizuschaltenden Netzwerkports liefert [2].

Zu den angesprochenen Aktionen zählt übrigens nicht nur die Installation von Software-Paketen oder Konfigurationsdateien, auch beliebige Kommandos führen Sie bequem über den Spacewalk-Server auf Ihren einzelnen Systemen aus. Haben Sie beispielsweise eine neue Konfigurationsdatei für Ihren Mailserver erstellt und auf das System verteilt, so ist natürlich ein Neustart des Servers notwendig, damit dieser die neuen Konfigurationsanweisungen einliest. Anstatt sich nun also auf jedes einzelne System einzuloggen oder mit for-Schleifen zu arbeiten, um dann den gewünschten restart-Befehl auf den Systemen auszuführen, erfolgt die Anweisung einfach wieder über eine zentrale Stelle – den Spacewalk-Server.

Auch die Installation von neuen Bare-Metal-Systemen gestaltet sich recht einfach. Spacewalk hält hierfür entsprechende Installationsdateien – die sogenannten Kickstart-Trees – bereit.

Über ein Bootmedium, beispielsweise eine CD, ein USB-Stick oder eine PXE-fähige Netzwerkkarte, stellen Sie dann den Kontakt zum Server her. Über welchen Server die Installation erfolgen soll, erfragt der sogenannte First-Stage-Installer. Dieser ist Teil des Installationsmediums. Die restliche Installation erfolgt dann über den Second-Stage-Installer. Dieser befindet sich auf dem Spacewalk-Server und wird zu Beginn einer Installation auf das Client-System übertragen. Soll die Installation komplett automatisiert erfolgen, können Sie dem Bootmedium direkt den Speicherort einer sogenannten Kickstartdatei mit angeben. Hierbei handelt es sich um eine Art Antwortdatei, die sämtliche Eigenschaften des zu installierenden Systems beschreibt, also beispielsweise Partitionierung, Software, Sprach- und Firewall-Einstellungen. Natürlich können Sie eine solche Kickstartdatei auf dem Spacewalk-Server erstellen und dem Bootmedium dann den entsprechenden Link zur Datei mitteilen.

Spacewalk ist in der Lage, jede RPM-basierte Distribution zu verwalten. Dabei besteht sogar die Möglichkeit, Client-Systeme in unterschiedlichen Organisationen zu betreiben. Über das Webinterface können Sie diverse Organisationen erstellen und diesen eine bestimmte Anzahl von System-Entitlements zuweisen. Die Entitlements sind an ein Zertifikat gebunden, das Spacewalk bei der Installation automatisch generiert. Den einzelnen Organisationen lassen sich dann Benutzer hinzufügen. Findet die Registrierung eines Clients nun mit einem Benutzeraccount aus einer bestimmten Organisation statt, so wird dieses System auch dieser Organisation zugewiesen. Meldet sich ein Benutzer aus der Organisation mit seinem Account über das Webinterface am Spacewalk-Server an, sieht er auch nur die Systeme aus der eigenen Organisation. Das ist praktisch, falls Sie mehrere Abteilungen betreuen und die Systeme aus den einzelnen Abteilungen getrennt verwal-



ten möchten. Sie weisen diese einfach unterschiedlichen Organisationen zu, die Sie im Vorfeld erzeugt haben.

## Installation mit Datenbank

Die Spacewalk-Installation erfolgt wahlweise auf einem Red Hat Enterprise (RHEL), CentOS [3] oder Fedora-Linux [4]. Die einzelnen Repositories enthalten dabei die entsprechenden Pakete für die einzelnen Distributionen. Beachten Sie, dass Spacewalk eine aktuelle Java Runtime ab der Version 1.6.0 benötigt. Hier bietet sich beispielsweise das quelloffene `openjdk` an, das bereits Bestandteil von Fedora ist. Setzen Sie RHEL oder CentOS ein, erhalten Sie über das zusätzliche Software-Repository EPEL (Extra Packages for Enterprise Linux) [5] Zugang zu dem Paket. Neben dem Java-Paket gehört eine Oracle-Datenbank 10g zum Pflichtumfang einer Spacewalk-Installation. Im einfachsten Fall steht Ihnen mit Oracle XE eine kostenlose Version der Datenbank zur Verfügung. Den Einsatz einer quelloffenen Datenbank treiben die Entwickler momentan voran. Hier hat sich PostgreSQL als beste Alternative zu Oracle herausgestellt. Wann genau die Unterstützung hierfür offiziell verfügbar ist, steht momentan noch nicht fest. Daher hilft ein regelmäßiger Blick auf die aktuelle Roadmap [6] oder die entsprechenden Mailinglisten [7] weiter.



Bild 3: Unter der Benutzerverwaltung können Sie die angelegten User sowie deren Rollen festlegen

## Oracle XE installieren

Haben Sie das entsprechende Repository-RPM für Ihre Distribution installiert, geht es als Erstes an die Installation der Oracle Express-Datenbank. Diese können Sie kostenfrei unter [8] herunterladen. Achten Sie darauf, dass Sie die Version 10.2.0.1 verwenden. Neben der eigentlichen Datenbank benötigen Sie auch die Pakete "oracle-instantclient-basic" und "oracle-instantclient-sqlplus". Anschließend installieren Sie die Pakete mittels yum:

```
# yum localinstall -nogpgcheck
  oracle-xe-univ*.rpm \
  oracle-instantclient-basic*.rpm
  oracle-instantclient-sqlplus*.rpm
```

Bevor es an die Konfiguration der Datenbank geht, sollten Sie sicherstellen, dass Ihr Rechnernamen in der Datei

`/etc/hosts` auf die richtige IP-Adresse zeigt, ansonsten gibt es später Probleme mit der Oracle Listener-Konfiguration. Benutzen Sie die folgenden Parameter zur Konfiguration:

```
HTTP port for Oracle Application
Express: 9055
Database listener port: 1521
Password for SYS/SYSTEM: {password}
Start at boot: y
```

Der Standard-HTTP-Port für die Oracle Express-Anwendung (8080) ist bereits durch den Applikationsserver Tomcat belegt, deswegen müssen Sie hier zwingend einen alternativen Port wählen. Damit Sie mit der Datenbank arbeiten können, ist schließlich noch die Listener-Konfiguration über die Datei `/etc/tnsnames.ora` durchzuführen:



Virtualization World, orts- und zeitgleich mit SNW Europe und Datacenter Technologies, bietet die Möglichkeit an 100 verschiedenen Konferenz-Sessions teilzunehmen, unvoreingenommene herstellereutrale Updates über die neuesten IT-Standards von SNIA Europe zu erhalten, praxisorientierten Übungen teilzunehmen, über 50 IT-Experten zu treffen und mit über 1000 Kollegen aus ganz Europa zu networken.

Kostenloser Eintritt für IT Manager und Channel Partner mit folgendem **Promo-Code: M14V10\***

**www.virtualizationworld.net**



**VIRTUALIZATION  
WORLD**

26. - 27. Oktober 2010  
Congress Frankfurt









\* Die Anmeldung gewährt Ihnen Eintritt für alle 3 Events



```

cat >> /etc/tnsnames.ora << 'EOF'
XE =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS =
        (PROTOCOL = TCP)(HOST = localhost)
        (PORT = 1521))
      )
    (CONNECT_DATA =
      (SERVICE_NAME = xe)
    )
  )
EOF

```

Abschließend folgen noch einige Konfigurationen an der Datenbank. Hierfür melden Sie sich mit Hilfe der Client-Anwendung sqlplus an der Datenbank an und legen als Erstes den Benutzer namens "spacewalk" an, der in unserem Beispiel das Passwort "spacewalk" zugewiesen bekommt:

```

# sqlplus 'sys@xe as sysdba'
SQL> create user spacewalk identi-
fied by spacewalk default table-
space users;
SQL> grant dba to spacewalk;
SQL> quit

```

In der Standardkonfiguration lässt die Oracle Express-Datenbank nicht mehr als 40 gleichzeitige Verbindungen zu, was für den Betrieb unter Spacewalk nicht ausreicht. Mit den folgenden Anweisungen erhöhen Sie diesen Wert auf 400 mögliche Verbindungen:

```

# sqlplus spacewalk/spacewalk@xe
SQL> alter system set processes =
400 scope=spfile;
SQL> alter system set
_optimizer_filter_pred_pullup"=
false scope=spfile;
SQL> alter system set
_optimizer_cost_based_transforma-
tion"=off scope=spfile;
SQL> quit

```

Anschließend starten Sie die Datenbank mit dem Kommando `# /sbin/service oracle-xe restart` neu.

## Setup über Konfigurationsdateien

Im nächsten Schritt installieren Sie den eigentlichen Spacewalk-Server. Hierzu ist zwingend das passende Spacewalk-Repository einzurichten wie zuvor beschrieben. Unter `"/etc/yum.repos.d/"` sollte sich eine Datei `spacewalk.repo` befinden, die auf das richtige Repository verweist. Die Installation selbst stoßen Sie dann mit folgendem Befehl an:

```
# yum install spacewalk-oracle
```

Da dieses Paket von allen anderen Spacewalk-Paketen abhängt, lädt der Paketmanager diese automatisch herunter und installiert sie. Die Konfiguration der Anwendung erfolgt dann entweder manuell über ein interaktives setup-Tool oder einfach durch die Angabe einer Antwortdatei als Option zum setup-Tool. Diese Antwortdatei enthält alle notwendigen Informationen, die zur Konfiguration der Spacewalk-Anwendung notwendig sind. Die Datei könnte beispielsweise so aussehen:

```

admin-email = root@localhost
ssl-set-org = Tuxgeek Org
ssl-set-org-unit = Tuxgeek OU
ssl-set-city = Essen
ssl-set-state = NRW
ssl-set-country = DE
ssl-password = spacewalk
ssl-set-email = root@localhost
ssl-config-sslvhost = Y
db-backend=oracle
db-user=spacewalk
db-password=spacewalk
db-sid=xe
db-host=localhost
db-port=1521
db-protocol=TCP
enable-tftp=Y


```

Die Antwortdatei übergeben Sie dem setup-Tool dann wie folgt:

```
# spacewalk-setup --disconnected
--answer-file=antwortdatei
```


Die Konfiguration kann einige Zeit in Anspruch nehmen, da nun auch die Da-

tenbank-Tabellen eingerichtet werden. Das setup-Tool startet abschließend alle notwendigen Dienste. Ein manueller Neustart aller Dienste ist über das Tool `/usr/sbin/rhn-satellite` möglich. Die abschließende Konfiguration ist bereits über das Spacewalk-Webinterface durchzuführen. Rufen Sie hierfür bitte die URL `http://spacewalk.server.tld` in Ihrem Webbrowser auf. Neben Kontaktinformationen ist hier nun beispielsweise auch das Passwort für den Spacewalk-Administrator zu setzen.

Lesen Sie im zweiten Teil dieser Workshopserie, wie Sie die Software-Kanäle für die Paketverteilung einrichten. (dr) 

*Thorsten Scherf ist Senior Consultant bei Red Hat EMEA in Stuttgart.*

- [1] **Spacewalk Projektseite**  
<http://fedorahosted.org/spacewalk>
- [2] **Spacewalk Netzwerk-Ports**  
<http://magazine.redhat.com/2008/09/30/tips-and-tricks-what-tcpip-ports-are-required-to-be-open-on-an-rhn-satellite-proxy-or-client-system/>
- [3] **RHEL5, CentOS5 Spacewalk Server Repository RPM**  
<http://spacewalk.redhat.com/yum/1.0/RHEL/5/i386/spacewalk-repo-1.0-2.el5.noarch.rpm>
- [4] **Fedora12 Spacewalk Server Repository RPM**  
<http://spacewalk.redhat.com/yum/1.0/Fedora/12/i386/spacewalk-repo-1.0-2.fc12.noarch.rpm>
- [5] **EPEL Repository**  
<http://download.fedoraproject.org/pub/epel/5/i386/epel-release-5-3.noarch.rpm>
- [6] **Spacewalk Roadmap**  
<http://fedorahosted.org/spacewalk/roadmap>
- [7] **Spacewalk Mailingliste**  
[www.redhat.com/spacewalk/communicate.html#lists](http://www.redhat.com/spacewalk/communicate.html#lists)
- [8] **Oracle XE Software Pakete**  
[www.oracle.com/technology/software/products/database/xe/htdocs/102xelinsoft.html](http://www.oracle.com/technology/software/products/database/xe/htdocs/102xelinsoft.html)



Links



# Laufwerke und NTFS-Rechte mit PowerShell 2.0 bearbeiten

## Die Platte in Griff

von Rolf Masuch

**F**ür Arbeiten im Dateisystem bietet die PowerShell zwei neue, schnelle Alternativen: die Cmdlets *Get-ACL* und *Set-ACL*. Mit ihnen lassen sich die gesetzten Berechtigungen auf Ordnern und Dateien überprüfen und neu schreiben. Auch die Arbeit über das Netzwerk wird von ihnen ohne große Umstände ermöglicht. Die Darstellung der Berechtigungsinformationen als kryptische Zeichenkette über das Attribut "SDDL" oder in Form einer Liste über das Attribut "Access" bietet ausreichend Möglichkeiten zur automatisierten Verarbeitung oder der verständlichen Darstellung für den Benutzer.

Grundsätzlich unterstützen die beiden Cmdlets die Provider "Filesystem" und "Registry". Weiterhin bieten sie den Parameter "-UseTransaction", um die aktuelle Aktion in eine Transaktion mit einzuschließen. Den Zugriff auf entfernte Dateisysteme über den Parameter "-Computername" unterstützen die beiden Cmdlets jedoch nicht. Alternativ können Sie ein verbundenes Netzwerklaufwerk verwenden oder direkt den UNC-Pfad der gewünschten Datei angeben. So gibt Ihnen der Befehl `get-acl \\nyc-dc1\e$temp` als Ergebnis den Pfad zum abgefragten Objekt zurück sowie eine Tabelle mit den Informationen Path, Owner und Access. Um diese als formatierte Liste zu erhalten, übergeben Sie den genannten Befehl mit der Pipeline an das Cmdlet `format-list` oder kurz `fl`. Der Befehl `get-acl \\nyc-dc1\e$temp | fl` zeigt Ihnen neben den bereits genannten Informationen zusätzlich die Informationen Group, Audit und Sddl ("Security Descriptor Definition Language") an.

Möchten Sie mehrere Objekte – zum Beispiel mehrere Dateien – überprüfen, emp-

fehlt es sich, sich nur ausgewählte Informationen zurückgeben zu lassen. Dies erreichen Sie mit Hilfe des Cmdlets `select-object`. Auf mehrere Server angewendet sieht das Skript beispielsweise so aus:

```
Get-Content e:\temp\server.txt | %
{ get-acl \\$_\C`$\windows\*.log |
  select-object Pspath, Sddl |
  format-list }
```

Da das \$-Zeichen von der PowerShell als Anfangszeichen einer Variable interpretiert wird, sollten Sie es für die Verwendung in einer Pfadangabe mit dem sogenannten Backtick (`) oder dem Accent Grave maskieren.

### Rechte setzen

Wie auch schon das Cmdlet *Get-ACL* benötigt *Set-ACL* ein Objekt und die gewünschten Rechte, die auf diesem Objekt gesetzt werden sollen. Der einfachste Weg ist es, die Rechte von einem bestehenden Verzeichnis zu kopieren:

```
Get-ACL E:\ACL\Source | Set-ACL
  \\Server01\E`$\Data\Target
```

Doch steckt in genau dem Lösungsansatz häufig das Problem: Welcher Ordner hat denn bereits die richtig gesetzten Rechte? Für einen schnellen Vergleich verwenden Sie das Cmdlet *Compare-Object*:

```
$acl1 = get-acl e:\temp\source
$acl2 = get-acl \\nyc-dc1\e`$\
  temp\target
compare-object $acl1.sddl $acl2.sddl
  -IncludeEqual
```

Beachten Sie, dass das Cmdlet *Compare-Object* keine Ausgabe liefert, wenn Sie oh-

ne den Parameter "-IncludeEqual" arbeiten. Schwieriger wird es, wenn Sie keine Referenzobjekte oder -Ordner haben beziehungsweise keinen Zugriff darauf. Ein ACL-Objekt bietet über die Methode "SetSecurityDescriptorSddlForm" die Möglichkeit, eine neue ACL zu schreiben. Entweder haben Sie die benötigte Information bereits früher mit dem Befehl

```
$acl.sddl | Out-File d:\temp\Tar-
  getSDDLFiles\sddlFoldersource.txt
```

gesichert oder Sie setzen sie anhand der Informationen aus der MSDN selbst zusammen [1-3]. Falls Sie die Referenz-SDDL in Form einer Textdatei gesichert haben, schreibt Ihnen das folgende Skript

```
$acl2 = get-acl \\nyc-dc1\e`$\
  temp\target
$sourcesddl = get-content
  d:\temp\TargetSDDLFiles\sddlFol-
  dersource.txt
$acl2. SetSecurityDescriptorSddlForm($sourcesddl)
```

die ACL wie gewünscht neu. (dr)



[1] Die Security Descriptor Definition-Sprache  
[http://msdn.microsoft.com/en-us/library/aa379567\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa379567(VS.85).aspx)

[2] ACE-Zeichenketten erklärt  
[http://msdn.microsoft.com/en-us/library/aa374928\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa374928(VS.85).aspx)

[3] Die Security-Klasse auf MSDN  
<http://msdn.microsoft.com/de-de/library/system.security.accesscontrol.directorysecurity.aspx>

Links





Tipps & Tricks ohne Gewähr

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



Ich nutze **Windows 7** und möchte das für mich unnötige **Protokollieren von Ereignissen** im Betriebssystem gerne dauerhaft **deaktivieren**. Wie kann ich das am besten tun?

Um unter Windows 7 keine Ereignisse mehr festzuhalten, müssen Sie eine kleine Änderung in der Registry vornehmen. Starten Sie hierfür den Registry-Editor mit dem Befehl

**regedit**

und gehen Sie zum Schlüssel "HKEY\_LOCAL\_MACHINE/Software/Microsoft/WBEM/CIMOM". Dort finden Sie die beiden Werte "Logging" und "EnableEvents" vom Typ REG\_SZ. Tragen Sie für beide Werte die Zahl "0" ein, bestätigen Sie die Änderung mit "OK" und starten Sie das Betriebssystem neu. Anschließend speichert Windows nicht mehr, was geschehen ist. Allerdings fehlt Ihnen damit auch diese Möglichkeit, um eventuelle Fehler im System nachvollziehen zu können. (dr)

Unter **Windows 7** nutze ich regelmäßig den **Taskmanager**, um die Prozesse und Speicherauslastung im Blick zu behalten. Diesen jedes Mal mit "STRG + ALT +

Entf." zu starten ist jedoch relativ umständlich. Wie kann ich den **Taskmanager** in die **Superbar** integrieren?

Um den Taskmanager bequem über die Superbar starten zu können, führen Sie einen Rechtsklick auf den Desktop aus und wählen im Kontextmenü den Punkt "Neu / Verknüpfung". Im nun geöffneten Fenster tragen Sie den Pfad zum Taskmanager ein: "C:Windows\System32\taskmgr.exe" sowie den Namen für die Verknüpfung, zum Beispiel "Taskmanager". Mit einem Klick auf "Fertig stellen" legen Sie Ihre neue Verknüpfung an und können diese über das Kontextmenü "An Taskleiste anheften" in die Superbar integrieren. (dr)

Wenn ich mir unter **Windows 7** einen Überblick über das System verschaffen will, geht dies nur relativ umständlich über die **Systemsteuerung**. Dabei möchte ich mir jedoch den Weg über die einzelnen Unterpunkte gerne sparen und wünsche mir eine **umfassende Übersicht**, die mir auf einen Blick alle relevanten Daten verrät. Muss ich dafür auf ein **Drittanbietertool** zurückgreifen oder bietet das Betriebssystem selbst auch eine solche Übersicht?

Sie müssen für den allumfassenden Überblick nicht zwingend ein Drittanbietertool nutzen. Windows 7 bietet ebenfalls eine Gesamtübersicht über das laufende System. Um diesen sogenannten "God mode" zu aktivieren, ist nicht ein-

mal eine Änderung am OS vonnöten. Starten Sie einfach den Windows Explorer und tragen Sie oben in der Adresszeile "shell::{ED7BA470-8E54-465E-825C-99712043E01C}" ein. Daraufhin erhalten Sie alle Daten und Möglichkeiten der Systemsteuerung in einem Fenster. Es bietet sich natürlich an, diese Adresse als Verknüpfung auf dem Desktop zu speichern, um das Fenster künftig mit einem Mausklick zu öffnen. (dr)

Ich möchte gerne auf einigen Rechnern **Windows Vista** installieren, dies jedoch aus **Performance-Gründen per USB-Stick** tun. Ist dies möglich und falls ja, wie?

Ohne weiteres ist eine Installation von Windows Vista über einen USB-Stick nicht möglich. Sie können jedoch den Stick formatieren und partitionieren und anschließend den Inhalt der Installations-CD draufkopieren. Schließen Sie hierfür den USB-Stick am Rechner an und führen Sie nacheinander zunächst die Befehle

```
diskpart
select {Bezeichnung des USB-Sticks, etwa disk 1}
clean
create partition primary
select partition 1
active
format fs=fat32
assign
exit
```

auf der Kommandozeile aus. Nun kopieren Sie den Inhalt der Setup-CD mit `xcopy d:\*.* /s/e/f e:\` auf den Stick – in der Annahme, dass Ihr CD-Laufwerk den Buchstaben “D” und der Stick “E” trägt. Jetzt müssen Sie nur noch sicherstellen, dass Ihr Rechner vom USB-Stick bootet und Sie können Windows installieren. (dr)



Auf einem unserer Rechner läuft **Outlook 2007 unter Windows Vista**. Wenn der Mail-Client versucht, sich mit unserem Exchange Server 2003 zu verbinden, kommt es zur Fehlermeldung “0x8004011D” mit dem **Hinweis, der Server sei nicht erreichbar**. Von anderen Clients aus besteht aber kein Problem mit der Verfügbarkeit des Exchange-Servers, die Synchronisation der restlichen Postfächer klappt tadellos. Es scheint, als liege der Fehler bei Windows Vista. Können Sie dies bestätigen und wenn ja, wie lässt sich diese Problematik aus der Welt schaffen?

Wie Sie schon vermuten, tritt das von Ihnen beschriebene Fehlverhalten nur dann auf, wenn Sie mit einem Vista-Client und Outlook 2007 auf den Exchange Server 2003 zugreifen wollen. Dies liegt daran, dass manche Anfragen, wie etwa der Exchange-Informationsspeicherdienst (Microsoft Exchange Information Store), versuchen, über den TCP-Port 1723 eine Verbindung zum Server aufzubauen. Vista hat Port 1723 jedoch ausschließlich für auf PPTP beruhende VPN-Verbindungen reserviert. Die Windows-Firewall überwacht dies und unterbindet jeden anderslautenden Kontakt. Umgehen können Sie dieses Problem nur, wenn Sie diese Kontrolle auf PPTP-Traffic ausschalten. Öffnen Sie dazu zunächst die Kommandozeile, und zwar mit Administrator-Rechten. Geben Sie dann den Befehl

```
netsh advfirewall set global
statefulpptp disable
```

ein. Falls Outlook 2007 währenddessen geöffnet war, schließen Sie es und starten Sie es neu. Die Kommunikation mit dem Exchange Server 2003 sollte nun reibungslos funktionieren. Wenn Sie diese Aktion auf mehreren Clients durchführen müssen, sollten Sie darüber nachdenken, das Kommando in eine Gruppenrichtlinie einzubetten. Wie das geht, erklärt im Detail die Microsoft Knowledge Base im Artikel 939321. (ln)

An einen meiner Teamkollegen muss ich **besonders oft E-Mails** schreiben. Gibt es eine Möglichkeit, durch eine Verknüpfung auf dem Desktop direkt eine neue E-Mail zu erstellen, bei der **im Adressfeld der Empfänger bereits eingetragen ist**? Dies würde mir ein paar Klicks und etliche Tipparbeit ersparen.

Natürlich gibt es die Möglichkeit, Outlook 2007 mit einem speziellen Kommando dazu zu bewegen, eine neue, bereits voradressierte Nachricht zu generieren. Dieser Befehl lässt sich in einer Verknüpfung integrieren. Erstellen Sie dazu mit Rechtsklick auf den Arbeitsplatz eine neue Verknüpfung und geben Sie als Speicherort des Elements `“C:\Programme\Microsoft Office\office12\outlook.exe” /c ipm.note /m {E-Mailadresse des Empfängers}` ein. Vergessen Sie dabei keinesfalls die Anführungszeichen und achten Sie darauf, dass der Pfad auf einem englischen System (oder wenn Sie das Verzeichnis manuell geändert haben natürlich anders) anders lauten muss. Für Outlook 2003 gilt im Prinzip das gleiche Kommando, allerdings lautet das entsprechende Verzeichnis nicht “Office 12”, sondern “Office 11”, so dass Sie auch in diesem Fall den Pfad anpassen müssen. Geben Sie der Verknüpfung nun noch einen Namen und in Zukunft öffnen Sie mit einem Doppelklick die voradressierte E-Mail, die Sie jetzt nur noch mit einem Betreff und Inhalt auffüllen müssen. (ln)



## Tools

Die Bereitstellung von **virtualisierten Anwendungen mit App-V** aus dem Hause Microsoft stellt für viele Unternehmen eine sinnvolle Ergänzung der eigenen Virtualisierungs-Strategie oder der Terminal Server-Farmen dar. Das Werkzeug bietet die Anwendungsvirtualisierung als Teil des MDOP für Software Assurance-Kunden zudem kostenlos. Doch beim Management derart zur Verfügung gestellter Applikationen findet sich ein Haar in der Suppe: Es lässt sich mit Bordmitteln nichts über die tatsächliche Nutzung der Anwendungen in Erfahrung bringen. Diese sind jedoch entscheidend für die Steuerung und Optimierung der App-V-Infrastruktur

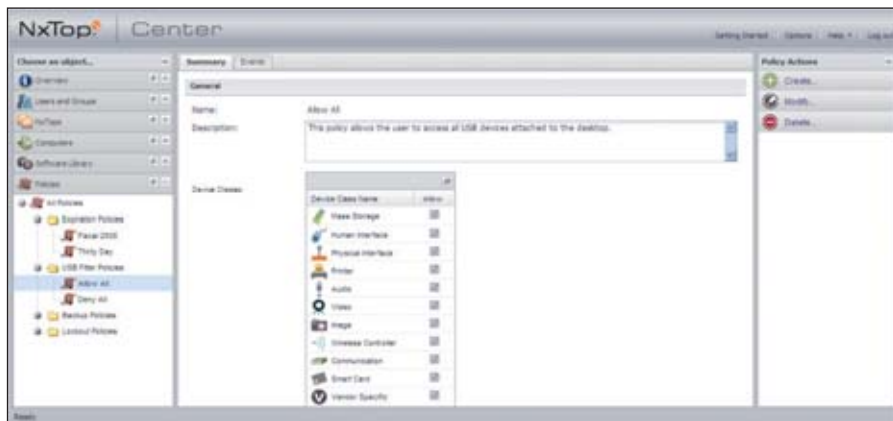
App-V beinhaltet natürlich eine Management-Konsole, mit deren Hilfe sich virtualisierte Applikationen bereitstellen, vorhandene konfigurieren und Berechtigungen setzen lassen. Eine Option, an die Informationen bezüglich der Nutzung zu kommen, ist die kostenlose Software **Microsoft Application Virtualization Dashboard**. Das Dashboard bezieht seine Daten direkt aus der App-V-Datenbank und stellt sie als vor-konfigurierte oder selbst definierte Berichte zur Verfügung. (jp)

Quelle: [www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=45a90ae8-6d09-4f9a-947b-a2d7fc80ba48](http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=45a90ae8-6d09-4f9a-947b-a2d7fc80ba48)

Das Mobile Computing birgt eine Reihe Herausforderungen. **Laptops sind unsicher** und gestohlene Laptops sind eine ernste Gefahr für Unternehmen, weil ver-

Viele weitere Tipps & Tricks sowie konkrete Hilfe bei akuten Problemen bekommen Sie auch im Internet bei unserem exklusiven Foren-Partner [administrator.de](http://administrator.de). Über 60.000 registrierte Benutzer tauschen dort in über 100 Kategorien ihre Erfahrungen aus und leisten Hilfestellung. So wie der IT-Administrator das proximate Fachmagazin für Administratoren ist [administrator.de](http://administrator.de) die Internetplattform für alle System- und Netzwerkadministratoren. [www.administrator.de](http://www.administrator.de)





Über das NxTop Center werden die virtualisierten Clients verwaltet

lorene Daten und Datenverlust erhebliche Compliance-Fragen darstellen. Bei herkömmlichen Desktop Management-Lösungen kommen Laptops in der Regel etwas zu kurz. Es ist schwierig und mit hohen Wartungs- und Upgrade-Kosten verbunden. Laptop Backup- und Recovery-Lösungen sind willkürlich, **Laptop-Management** benötigt viel Zeit und das Patch-Management für verschiedene Betriebssysteme und verschiedene Anwendungen ist umständlich und langsam. Eine mögliche Antwort auf diese Herausforderung sind **Bare Metal-Hypervisoren**, wie etwa der XenClient, den wir in dieser Ausgabe ausführlich vorstellen. Doch Citrix ist hier nicht allein unterwegs und so bietet das kostenlose **NxTop** sichere, kontrollierte Betriebssysteme in Form eines virtuellen Desktops auf jedem klassischen

Desktop-PC oder Laptop. Das Werkzeug besteht aus zwei Komponenten: der NxTop Engine und dem NxTop Center. NxTop erlaubt der IT-Abteilung, ein einzelnes Image eines Betriebssystems zu verteilen und es für ausgewählte oder alle Endbenutzer zu veröffentlichen. Das NxTop Center dient dabei als zentrale Managementinstanz. Für den Download der für bis zu fünf PCs freien Version ist lediglich eine kurze Registrierung erforderlich. (jp)  
Quelle: [www.virtualcomputer.com/download](http://www.virtualcomputer.com/download)

Die **Überwachung von Netzwerken** fällt schon in rein physikalischen Umgebungen nicht immer leicht. Gerade wenn es um

die **Auswertung von Latenzzeiten** geht, sind die Ergebnisse oft nicht eindeutig. Noch komplizierter gestaltet sich das **Messen dieser Verzögerungen in virtualisierten Umgebungen**.

Zur Lösung dieses Problems bietet VKernel mit **StorageVIEW** ein kostenloses Tool für VMware-Umgebungen an, das **die Hosts mit den größten Latenzwerten aufzeigt** und die dahinter stehenden virtuellen Maschinen identifiziert. In einer grafischen Übersicht listet die Software diejenigen fünf Hosts oder Pfade auf, die im Netzwerk mit der höchsten Verzögerungs-Rate zu kämpfen haben. Ein Klick auf den entsprechenden Eintrag enthüllt, welche virtuellen Maschinen betroffen sind und wie hoch der aktuelle Datendurchsatz ist. Ein weiteres Fenster zeigt die durchschnittliche Latenzzeit aller übrigen, in der Top-5-Aufstellung nicht enthaltenen Storage-Hosts an. Da vSphere selbst keine Informationen über NFS-Latenzzeiten gewährt, errechnet das Werkzeug diese aus über 20 anderen, von vSphere übermittelten Kennzahlen. Vor dem Download der schlanken Software ist eine Registrierung nötig. (In)  
Quelle: [www.vkernel.com/download/storage-view](http://www.vkernel.com/download/storage-view)

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/](http://www.it-administrator.de/downloads/software/)

**Download der Woche**



StorageVIEW identifiziert in VMware-Umgebungen die Speicher-Hosts mit den größten Latenzzeiten



# Datenrettung in virtuellen Umgebungen

## Reale Rettung virtueller Daten

von Holger Engelland

Virtualisierung bietet große Chancen, allen voran Flexibilität und Hardwareunabhängigkeit. Doch auch in virtuellen Umgebungen werden Daten letztendlich von Menschen auf Festplatten oder Bändern gespeichert. Die hohe Flexibilität und die Schnelligkeit, die per Mausklick Entscheidungen von großer Tragweite in den Speicherverwaltungen hervorrufen, schaffen damit auch neue Risiken. Ein Datenrettungsunternehmen berichtet über typische Fehler seiner Kunden.



**2**009 stieg die Zahl der Datenrettungs-Anfragen in virtualisierten Umgebungen bei den Datenrettern von Kroll Ontrack gegenüber dem Vorjahr um 58 Prozent. Über zwei Drittel davon waren Folgen von Anwenderfehlern. Häufigste Ursache sind dabei Fehlbedienungen. Bei traditionellen Systemen liegt der Anteil menschlichen Fehlverhaltens nur bei 26 Prozent gegenüber 74 Prozent technischem Versagen. Das zeigt, wie komplex es ist, virtuelle Umgebungen zu implementieren, zu managen oder zu migrieren. Bei virtualisierten Umgebungen liegen immer mehr kritische Informationen zentralisiert auf einem System. So ist der mögliche Schaden durch Datenverluste viel größer. Aber eine Datenrettung ist auch hier meistens noch möglich, denn wie in der herkömmlich digitalen Welt gilt auch in der virtuellen Umgebung: Erst nach Veränderung der Informationen in den Festplattensektoren sind Daten wirklich verloren.

### Szenarien des Datenverlustes in virtuellen Umgebungen

Die Ursachen der Datenverluste sind ebenso unterschiedlich wie bei herkömmlichen Systemen. Prinzipiell gilt, dass auch in der virtuellen Welt Informa-

tionen letzten Endes immer auf einer Festplatte oder einem Band gespeichert werden. Hardware-Unabhängigkeit bedeutet nicht, dass das Risiko des Datenverlustes durch Hardwareverlust ausgeschlossen ist. Auch neue Technologien nützen nichts, wenn – wie in der Praxis vorgekommen – ein Wassereintrich den überwiegenden Teil der Festplatten eines virtuellen Verbundes flutet und kein Backup vorliegt.

Viel entscheidender sind aber die Fehler durch Fehlbedienung beziehungsweise mangelhaftes Training. Hierbei handelt es sich nicht um fahrlässige oder überforderte Administratoren, sondern um Gefahren, die eine komplexe Technologie in sich trägt, wenn schnell und unter Zeitdruck Entscheidungen getroffen werden müssen. Bei Systemen des Virtualisierungsspezialisten VMware beispielsweise verteilen sich die Ursachen laut den Kroll Ontrack-Experten wie folgt:

- Hardware-/RAID-Probleme: 36 Prozent
- VMFS-Korruption: 20 Prozent
- gelöschte virtuelle Festplatten und/oder Snapshots: 18 Prozent
- VMFS-Re-Installation: 17 Prozent
- interne Korruption der virtuellen Festplatte: 9 Prozent.

### Szenario 1: Fehler im RAID

Ausfälle im RAID-System können verschiedene Ursachen haben. In einem Fall wurde aus Versehen eine intakte Festplatte aus dem virtuellen RAID-Bereich entfernt, der alle wichtigen SQL-Server in einem Krankenhaus hostete. Durch eine Reihe von Reparatur-Versuchen wie RAID-Rebuilds oder auch einer RAID-Initialisierung bei gleichzeitiger Überprüfung der Partition mittels Check Disk wurden nun die Data Stripes des RAID-Arrays weiter beschädigt. Der Fall stellte sich sehr kompliziert dar, da nicht nur Datenstrukturen zum Beispiel im VMFS (Virtual Machine File System)-Datensystem, sondern auch in SQL und sogar im NTFS selbst betroffen waren. Wesentlich war in diesem Fall die Wiederherstellung der Konfiguration der originären RAID-Konstellation.

Die Datenretter konnten dies durch eine Software-Simulation ohne den ursprünglichen Hardware-RAID-Controller erreichen, bei der die Data Stripes in der richtigen Reihenfolge über alle Festplatten neu angeordnet wurden. Die Experten verfügen auch über spezifische Tools zur Reparatur beschädigter VMFS-Dateisysteme und zur Kopie der



VMDK (Virtual Machine Disk)-Files. NTFS-Datenrettungs-Tools reparierten das NT-Datensystem und kopierten die SQL-Informationen, die dann in eine neue Datenbank überspielt wurden. Angesichts dieser aufwändigen Datenrettungsvorgänge ist es hierbei zwingend nötig, zuerst eine Sicherung des Status Quo mitsamt aller Beschädigungen der Datenstruktur vorzunehmen. Dann können anhand der Kopie über einen speziellen Recovery-Layer alle Rettungsarbeiten vorgenommen, dokumentiert und – sofern nötig – auch wieder zurückgenommen werden.

## Szenario 2: Gelöschte virtuelle Maschinen

Nicht selten kommt es vor, dass eine virtuelle Disk aus Versehen gelöscht wird. In einem Fall traf es dabei die Disk mit zwei virtuellen SQL-Datenbanken. Ein Backup war nicht vorhanden. Gelöschte Daten in VMFS sind eine besondere Herausforderung. Hier werden nämlich alle Verweise auf die Daten entfernt. Zum Glück werden die Home-Verzeichnisse der VMDK-Metadaten als zentrale Register nicht endgültig gelöscht – wie auch die Datei-Inhalte der besonders wichtigen Datei mit dem virtualisierten Dateisystem und den eigentlich gesuchten realen Daten. Die Datenrettungsingenieure können hier dann nach den noch auffindbaren VMDK-Dateien suchen. Einen kleinen Hinweis haben die Ingenieure bei ihrer Arbeit – vorausgesetzt sie beginnen sofort mit der Datenrettung: Sie müssen lediglich die freien und damit vermeintlich leeren Sektoren durchsuchen. Mit Hilfe von VMFS-Recovery-Tools lässt sich der Suchbereich auf den Unallocated Space des Volumes eingrenzen, um die gelöschte virtuelle Maschine zu finden. Aufwändig wird dies, weil VMDK-Files meist fragmentiert sind und alle Einzelteile mühsam wieder zum Ganzen zusammengesetzt werden müssen. Die Suche ist auch mit automatisierten Tools langwierig, da VMFS-Daten oft eine Dimension von über einer Milliarde Sektoren à 512 Byte

erreichen. Danach können aber die alten VMDKs in einem neuen VMDK-File wieder zusammengesetzt werden.

## Szenario 3: Formatierung und Reinstallation eines Volumens

Die versehentliche Neuformatierung eines Volumens virtueller Maschinen kann schwerwiegende Folgen haben. Das gilt insbesondere dann, wenn der Fehler nicht sofort bemerkt und eine Weile in einem so falsch neuformatierten System gearbeitet wird. In einem Fall wurde ein aktives VMFS-LUN versehentlich einem physikalischen Windows 2003-Server zugänglich gemacht und unter diesem als Datenplatte verwendet. Im NTFS wurden dadurch Datensätze neu geschrieben und damit die alten VMFS-Daten überschrieben. Nun war schnelle Hilfe notwendig: Auch hier wurden zuerst die neu beschriebenen NTFS-Daten ausgeblendet und im zweiten Schritt nur die noch nicht überschriebenen und nicht mehr sichtbaren VMDK-Strukturen gesucht. So ließen sich mit der rekonstruierten VMDK die Files wiederfinden und auslesen – sofern sie nicht schon überschrieben waren.


## Szenario 4: Quick initialised VMFS LUNs

Ebenso gefährlich kann es sein, ein VMFS-LUN an einem Windows Backup-Server zu betreiben und dabei die LUN nicht zu verstecken. Im Festplattenmanager lassen sich durch "Quick Initialising" auf dem Backup-Server mit einem Mausklick alle darunterliegenden Strukturen von VMFS für die ESX-Server unsichtbar machen. In einem Fall hatte ein Kunde ein SAN-System mit zehn ESX Production-Servern und 20 VMFS-LUNs mit je 500 GByte Speicher sowie einen Windows 2003 Server. Dieser diente in diesem System als Backup-Server, die 20 LUNs wurden dort im Direct Access Mode gemappt. Das ganze System beherbergte über 200 virtuelle Maschinen in einer unbekanntem Zahl von VMDKs.

Im konkreten Fall wurde am Windows Backup-Server eine neue Datenfestplatte eingebaut. Beim anschließenden Forma-

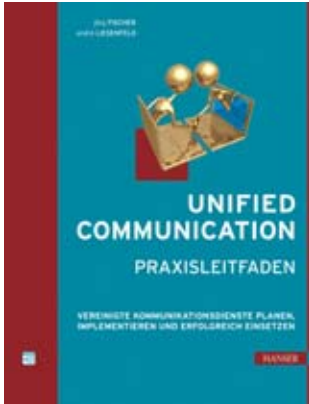
tieren musste zunächst ein "Quick Initialize" durchgeführt werden. Dabei waren nicht nur die eine neue Festplatte, sondern auch noch die 20 ESX-Volumes ausgewählt und mit dem Bestätigen auch sofort strukturell beschädigt. Die virtuellen Maschinen und der ESX-Server waren noch ansprechbar. Das Risiko, nach einem nun nötigen Reboot aber auch diese Daten endgültig zu verlieren, war groß, die VMFS-Volumes jedes ESX Servers wären nie wieder erkannt worden. Die ursprünglich vom Kunden anvisierte Lösung, einen neuen ESX-Server aufzusetzen und die Daten aller virtueller Maschinen und VMDKs auf neue LUNs zu überspielen, war zu aufwändig. Wesentlich eleganter war es hingegen, im laufenden Betrieb alle VMFS-LUNs mit modernen Datenrettungstechnologien reparieren zu lassen. Das bedeutet in diesem Fall die manuelle Rekonstruktion der gelöschten und zudem beschädigten VMFS-Frontend-Strukturen von 20 LUNs. Alle Daten konnten innerhalb von 24 Stunden gerettet werden. Gearbeitet wurde dabei über eine geschützte Internet-Verbindung, ohne dass Festplatten und Systeme ausgebaut werden mussten.

## Fazit

Administratoren können neben Schulungen und Sorgfalt zusätzlich im Vorfeld einiges tun, um auch einen möglichen Datenverlustfall einzugrenzen. Wer seine Strukturen gut dokumentiert und mit Bedacht virtuelle Speicherlandschaften anlegt, minimiert sein Risiko und kann im Ernstfall durch Rückgriff auf die Dokumentation die Wiederherstellung wesentlich vereinfachen oder auch erst ermöglichen. Zudem sollte man immer auch mit Weitblick in die Virtualisierung gehen. Die Infrastrukturen müssen Flexibilität, hohe Verfügbarkeit, Performance und Datensicherheit miteinander verbinden. Die Virtualisierungstechnologien bleiben eine verlockende und hervorragende Alternative; mit guter Planung auch ohne Weiteres sicher. (dr) 

*Holger Engelland ist Manager Data Recovery Engineering bei Kroll Ontrack.*

## Unified Communication



Beim Thema Unified Communication – kurz UC – gehen die Meinungen auseinander. So fängt es schon beim Namen an: Heißt es nun Communication oder Communications? Und

auch auf einer maßgeblicheren Ebene wird diskutiert, denn weder der Umfang noch die Komponenten von UC stehen zweifelsfrei fest. Laut Wikipedia wird UC mit der Integration von Kommunikationsmedien in einer einheitlichen Anwendungsumgebung definiert. Kein Wunder, dass das Thema für viele zu schwammig und dessen Nutzen unklar ist. Wer hier Klartext lesen will, sollte zum Buch "Unified Communication" von Jörg Fischer und André Liesenfeld greifen. Fischer, der schon mit seinem Titel "VoIP Praxisleitfaden" ein um-

fangreiches Thema umfassend beleuchtet hatte, enttäuscht auch beim noch weiter gefassten Aufhänger Unified Communications nicht. Der Ansatz der beiden Autoren ist wohlthuend methodisch und ganzheitlich. Im Mittelpunkt stehen nicht Kommunikationsstrukturen und Produkte, sondern grundsätzliche Fragen für den Leser: Warum könnte UC im Unternehmen sinnvoll sein? Welche Probleme lassen sich mit UC lösen? Oder, wie finde ich im Gespräch mit den Benutzern – Fischer und Liesenfeld nennen sie "die Kunden der Lösung" – heraus, ob es überhaupt Probleme gibt? Denn viele UC-Projekte scheitern schon lange, bevor überhaupt die Technik ins Spiel kommt, an den falschen Erwartungen von IT-Abteilung, Management und Endanwendern.

Die Autoren betonen mehrfach, wie wichtig es ist, sich im Vorfeld genaue Gedanken über die Ziele von UC zu machen. Return on Investment und Total Cost of Ownership spielen dabei eine große Rolle, aber nicht nur die einfach quantifizierbaren Werte wie "mehr

Zeit für Kundengespräche" oder "gesenkte Betriebskosten". Fischer und Liesenfeld wissen, dass UC die Kosten nicht unbedingt senkt, dafür aber die Erfahrung der Benutzer mit der Kommunikationstechnologie verbessert und so zu einer Erhöhung des "soft ROI" führt. Erst danach werden Funktionen von UC-Systemen beschrieben und echte Real Life-Einsatzmöglichkeiten genannt. Dabei zeigen die Autoren, dass sie viel Praxiserfahrung haben, und ergänzen den Text immer wieder mit Anekdoten und eigenen Beispielen.

Fazit: Die Autoren packen ein schwieriges und umfangreiches Thema sehr geschickt an. Der anfängliche, massive Fokus auf die Grundlagen hilft, bei der späteren Praxisplanung alle Aspekte zu beachten. Ein sehr empfehlenswerter Titel. *Elmar Török*

<b>Autoren:</b>	Jens Fischer; André Liesenfeld
<b>Verlag:</b>	Hanser
<b>Preis:</b>	49,90 Euro
<b>ISBN:</b>	978-3-446-41834-9
<b>Bewertung:</b>	★★★★★

## Microsoft Exchange Server 2010



In punkto Umfang mutet "Microsoft Exchange Server 2010" von Microsoft Press auf den ersten Blick recht harmlos an. Nach einem Blick auf die erste Seite wird der Irrtum klar: wenig Bilder, sehr kleine Schrift und

fast keine Seitenränder packen die knapp 650 Seiten voll mit geballten Informationen. Laut Autor William R. Stanek muss das auch so sein, denn gegenüber der Vorgängerversion 2007 hat sich bei Exchange 2010 so gut wie alles geändert. Um trotz-

dem ein – nach seiner Meinung – kompaktes Buch zu bekommen, setzt Stanek Grundlagen voraus und geht auf Basisanforderungen wie die Installation von Exchange nicht ein. Dennoch beschreibt das Buch die Hardware- und Strukturvoraussetzungen sowie die verschiedenen Editionen von Exchange Server 2010. Wen die eng bedruckten Seiten nicht abschrecken, der bekommt im Schnelldurchlauf die wesentlichen Rollen von Exchange-Servern und die Integration in Active Directory präsentiert. Entgegen der Ankündigung des Autors finden sich auch zwei Seiten zur Installation.

Ähnlich knapp geht es mit der Verwaltung von Exchange über PowerShell und die Verwaltungs-Shell weiter. PowerShell-Kommandos werden mit allen Optionen und Parametern kurz erklärt, leider nicht immer anhand eines Beispiels. Stanek versteht sein Handwerk und er weiß viel über Ex-

change, das ist klar. Doch sein auf das Minimum reduzierter Stil, zusammen mit der zwangsläufig etwas hölzernen Übersetzung macht das Lesen nicht gerade zum Vergnügen. Die positive Seite daran ist natürlich die phänomenale Menge an Wissen, die im Buch steckt. Es gibt eigentlich nichts, was ein Exchange Messaging-Admin nicht in den Kapiteln finden würde.

Fazit: Durch Format, Stil und Font nicht gerade angenehm zu lesen, aber voller Informationen zum Betrieb und zur Verwaltung von Microsoft Exchange Server 2010. Wer dieses Buch im Regal hat, braucht kein zweites über Exchange. *Elmar Török*

<b>Autoren:</b>	William R. Stanek
<b>Verlag:</b>	Microsoft Press
<b>Preis:</b>	39,90 Euro
<b>ISBN:</b>	978-3-86645-668-6
<b>Bewertung:</b>	★★★★★

# http://blog.dikmenoglu.de/ LDAP durch und durch

Was für andere Menschen Englisch, Französisch oder Deutsch ist, das ist für Yusuf Dikmenoglu nach eigener Aussage LDAP: Seine einzige Sprache. Dieses Statement zeugt von der Leidenschaft und Professionalität, mit der der Microsoft MVP an das Thema Verzeichnisdienste herangeht. Seit nunmehr vier Jahren bloggt der LDAP-Experte und erläutert dabei in einer bemerkenswerten technischen Tiefe die unterschiedlichen Aspekte des Protokolls – gewisse Vorkenntnisse durchaus vorausgesetzt. Dennoch schreibt Dikmenoglu seine Beiträge in klarer und verständlicher Weise, sodass die Informationen für die Leser den nötigen Nutzwert bieten – und nicht nur die Meinung des Bloggers wiedergeben, wie es in so vielen Blogs der Fall ist.

Besonderes Augenmerk legt der Experte dabei auf das Active Directory von Microsoft – als MVP auch wenig verwunderlich. Hierbei teilt Dikmenoglu seine Beiträge in zehn Kategorien ein: von der Administration über AD-PowerShell, Dokumentation, erweiterte Abfragen, Installation, Migration, Objektverwaltung, Replikation, Schema bis hin zur Wiederherstellung. Screenshots zeigen den Besuchern dann

auch gleich die Ergebnisse von durchgeführten Kommandos oder gesetzten Häkchen in den zahlreichen Fenstern eines Active Directory. Neben seinem Leib- und Magenthema geht der MVP auch auf das DNS sowie Gruppenrichtlinien, Netzwerke und Windows Server ein. Eine Volltextsuche hilft beim Finden eines gewünschten Themas. Diese zeigt jedoch alle gefundenen Artikel auf einer Seite nacheinander an und nicht, wie gewohnt, in einer Trefferliste. Dies – und die Tatsache, dass innerhalb einer Kategorie die Blogeinträge natürlich blogtypisch chronologisch aufgeführt sind – machen das Blog in Anbetracht der Fülle an Artikeln mitunter etwas unübersichtlich. Einen Abbruch tut dies dem Blog jedoch nicht.

Für Admins, die sich über den reinen Besuch der Seite auch mit Gleichgesinnten austauschen möchten, bietet Dikmenoglu eine Mailingliste. Über diese soll den Teilnehmern im Rahmen der Möglichkeiten Hilfestellung geboten werden, soweit dies mit ehrenamtlichen Mitgliedern möglich ist. Ein Blick in die einsehbare Historie der noch jungen Mailingliste zeigt, dass diese schon rege genutzt wird. Amtssprache: LDAP. Daran ändert übrigens auch die Tatsache nichts, dass die Besucher sich das Blog in 26 verschiedenen Stilen anzeigen lassen können. (dr)



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

**Management virtualisierter Infrastrukturen**  
Ziel der Desktop-Virtualisierung ist es, dem Nutzer einen Arbeitsplatz bereitzustellen, der nicht an physische Hardware gebunden ist. Produktivitätssteigerung und Kosteneinsparungen sind Vorteile dieses Ansatzes. Das Management virtualisierter Umgebungen stellt jedoch erhebliche Anforderungen an den Administrator. Im Online-Fachartikel gehen wir näher auf die Herausforderungen und die Umsetzung einer Strategie zur Desktop-Virtualisierung ein.  
[www.it-administrator.de/themen/virtualisierung/fachartikel/80993.html](http://www.it-administrator.de/themen/virtualisierung/fachartikel/80993.html)

**Anwenderbericht: Server-Virtualisierung bei der Dr. Peters Gruppe**  
Die Dr. Peters Gruppe betreibt als Anbieter geschlossener Fonds die größte deutsche Handelsflotte. Dabei legt das Unternehmen Wert auf höchste Sicherheit: Die Daten der Anleger müssen stets vor Verlust und unberechtigtem Zugriff geschützt sein. Die Zahl der Server ist in den letzten Jahren ständig gestiegen. Für eine höhere Ausfallsicherheit und einen verringerten Wartungsaufwand sorgte nun die Virtualisierung dieser Serverlandschaft. Wir stellen Ihnen auf unserer Webseite das Konzept der Umstellung vor.  
[www.it-administrator.de/themen/virtualisierung/fachartikel/80994.html](http://www.it-administrator.de/themen/virtualisierung/fachartikel/80994.html)

**Anwenderbericht: Verteiltes Engineering mit virtuellen Desktops**  
Der Pumpenhersteller LEWA setzt im Entwicklungsbereich auf Desktop-Virtualisierung: Auf diese Weise stellt das mittelständische Unternehmen komplette CAD-Arbeitsplätze über das Rechenzentrum bereit und bindet so alle internationalen Standorte an eine zentrale Engineering-Datenbank an. Dies führt zu schnelleren Entwicklungsprozessen, während gleichzeitig sichergestellt ist, dass geschäftskritisches Know-how die Firma nicht verlässt. In unserem Online-Beitrag setzen wir uns mit Aufbau und Verwaltung dieser Infrastruktur auseinander.  
[www.it-administrator.de/themen/virtualisierung/fachartikel/80995.html](http://www.it-administrator.de/themen/virtualisierung/fachartikel/80995.html)

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



Im Blog von Yusuf Dikmenoglu ist die Amtssprache LDAP

## »Cloud Computing als Herausforderung der Zukunft«

Stefan Roth ist beim Münchner Software-Unternehmen Meierhofer als Leiter der Systemadministration tätig. Die Firma liefert als Komplettanbieter ICT-Lösungen an Einrichtungen im Gesundheitswesen.

### Welche Ausbildung haben Sie gemacht?

Mein Studium habe ich als Diplom-Geograf abgeschlossen. Durch meine Begeisterung für alles, was mit Computern und Netzwerken zu tun hatte, habe ich dann einige Zeit als PC-Redakteur gearbeitet und über die Szene berichtet. Schließlich bin ich bei meinem jetzigen Beruf als Systemadministrator gelandet.

### Warum sind Sie IT-Administrator geworden?

Ich hatte immer schon Spaß am Umgang mit Computern, Netzwerken und der Technik im Allgemeinen. Aus diesem Grund habe ich mein Hobby dann irgendwann zum Beruf gemacht. Herausforderungen sind mir sehr wichtig und die gibt es in der IT unbegrenzt.

### Welche IT-Umgebung betreuen Sie aktuell?

Bei Meierhofer bin ich Leiter der Systemadministration. Wir arbeiten in einer fast reinen Microsoft-Umgebung, in der Windows 2003/2008 sowie Windows XP und 7 zum Einsatz kommen. Die Virtualisierung erfolgt mittels VMware ESX-Systemen. Aktuell betreuen wir in Deutschland, Österreich und der Schweiz insgesamt rund 350 Server, Workstations und Notebooks. Ergänzt wird dieser Gerätepark durch eine Vielzahl von Blackberrys und verschiedenen MDAs.

### Welches Netzwerk- und Systemmanagement setzen Sie ein?

Zur Überwachung unserer Systeme nutzen wir Nagios und den HP Operations Manager sowie Windows-Standardtools.

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

Den Kunden – sprich den Kollegen – immer professionell und freundlich weiterzuhelfen und dafür zu sorgen, dass der Betrieb des Unternehmensnetzwerkes störungsfrei rund um die Uhr gewährleistet ist.

### An welchem Projekt werden Sie in nächster Zeit arbeiten?

Zum einen steht die Domänen-Integration in der Schweiz an. Ein weiteres Projekt ist die Konsolidierung der VoIP-Umgebung in Österreich und der Schweiz. Generell



**Geburtsjahr:** 1965  
**Familienstand:** ledig  
**Hobbys:** unter anderem Rad fahren, Kanu fahren, Segeln und Skilanglaufen

Stefan Roth, IT-Administrator

müssen wir in unserer Systemlandschaft eine einheitliche Struktur schaffen und die Virtualisierung weiter ausbauen.

### Womit verwalten Sie Ihre virtuelle Umgebung?

Wir verwenden für das Management unserer virtuellen Umgebung vCenter/vSphere und sonstige Standardtools von VMware. Zur Sicherung der virtuellen Maschinen kommt VM Explorer von Trilead zum Einsatz. Als weiteren Helfer setzen wir FastSCP von Veeam ein.

### Was macht Ihnen an Ihrem Job am meisten Spaß?

Mir gefällt es, dass ich in meinem Alltag immer wieder mit neuen Herausforderungen und Problemen konfrontiert werde, die schnellstmöglich, aber kompetent und professionell gelöst werden müssen. Darüber hinaus habe ich Freude am Umgang mit Menschen – und den hat man als Administrator reichlich.

### Was tun Sie für Ihre Fort- und Weiterbildung?

Mein Arbeitgeber bietet gute Fortbildungsmöglichkeiten, die sehr praxisori-

entiert sind. Weitere Informationen hole ich mir ganz klassisch zum größten Teil aus Zeitschriften, Messebesuchen, Vorführungen, Teststellungen, Internet, internen Tests und Gesprächen mit Gleichgesinnten – wie viele meiner Kollegen auch.


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

Wo gearbeitet wird, werden Fehler gemacht. Und die IT arbeitet ständig, allerdings im Hintergrund, sodass dies vielen nicht auffällt. Einmal habe ich jedoch ein laufendes virtuelles Datenbanksystem ohne vorherige Sicherung auf einen anderen Host verschieben wollen. Leider ist dies nicht geglückt und die virtuelle Maschine war defekt. Mit viel Mühe und hohem Arbeitsaufwand konnten Maschine und letztendlich auch die Datenbank wiederhergestellt werden.

### Was war Ihr größter Erfolg als IT-Administrator?

Auf die Einführung von QM-, Terminal- und Helpdesk/ITIL-Systemen innerhalb von zwei Jahren bin ich wirklich stolz. Vor drei Jahren haben wir dann auch noch die komplette Virtualisierung einer DATEV-Umgebung aus einer Standalone-Variante heraus realisiert.

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

Cloud Computing wird in den nächsten Jahren für uns alle zur großen Herausforderung werden. Im Zuge dessen kommen dann auch zahlreiche andere Themen auf den Tisch. An vorderster Stelle steht in meinen Augen die Sicherheit. 

Das Interview führte Petra Adamik.

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

Was haben Sie zu sagen?

Die Ausgabe 9/10 erscheint am 6. September 2010

Schwerpunktthema:

# Messaging und Collaboration

Im Test: Signatur-Gateway enQsig

Einkaufsführer: Lösungen zur E-Mailarchivierung

Workshop: Loadbalancing für Exchange Server

Workshop: Open-Xchange Server 6 einrichten

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

Unsere Ausgabe im Oktober steht unter dem Schwerpunkt **Sicherheit für virtualisierte Infrastrukturen**. In unseren Tests nehmen wir unter anderem die "McAfee Total Protection for Virtualization" unter die Lupe. In der Praxisrubrik erfahren Sie außerdem, wie Sie sichere VLANs unter VMware einrichten.

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

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.



## IMPRESSUM

### Redaktion

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

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

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

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

### Autoren dieser Ausgabe

Petra Adamik, Thomas Bär, Holger Engelland,  
Jürgen Heyer, Thomas Joos, Martin Kuppinger,  
Sandro Lucifora, Nico Lüdemann, Ralf Masuch,  
Andreas Roscher, Thorsten Scherf, Elmar Török,  
Holger Sesterhenn, Dennis Zimmer

### Anzeigen

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

Es gilt die Anzeigenpreisliste  
Nr. 7 vom 01.11.2009

LAC/2008



### Produktion / Anzeigendisposition

Lightrays: Andreas Skrzypnik  
dispo@it-administrator.de  
Tel.: 089/4445408-88  
Fax: 089/4445408-99

### Druck

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

### Vertrieb

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

### Abo- und Leserservice

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

### Erscheinungsweise

monatlich

### Bezugspreise

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

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

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

### Verlag / Herausgeber

Heinemann Verlag GmbH  
Leopoldstraße 85  
80802 München  
Tel.: 089/4445408-0  
Fax: 089/4445408-99

(zugleich Anschrift aller Verantwortlichen)

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

Eingetragen im Handelsregister des  
Amtsgerichts München unter  
HRB 151585.

### Geschäftsführung / Anteilsverhältnisse

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

### ISSN

1614-2888

### Internet

www.it-administrator.de

### Urheberrecht

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

### Haftung

Für den Fall, dass in IT-Administrator unzutreffende  
Informationen oder in veröffentlichten Programmen,  
Zeichnungen, Plänen oder Diagrammen Fehler ent-  
halten sein sollten, kommt eine Haftung nur bei  
grober Fahrlässigkeit des Verlags oder seiner Mit-  
arbeiter in Betracht. Für unverlangt eingesandte  
Manuskripte, Produkte oder sonstige Waren über-  
nimmt der Verlag keine Haftung.

### Manuskripteneinsendungen

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

### So erreichen Sie den Leserservice

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

### Bankverbindung für Abonnenten

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

### So erreichen Sie die Redaktion

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

### So erreichen Sie die Anzeigenabteilung

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

DeviceLock	S. 37
Diskeeper	S. 04
IBM	S. 68
Log.in Consultants	S. 23, S. 43

notebooksbilliger.de	S. 02
Paessler	S. 45
sepag	S. 29, S. 51
SNW	S. 55

## INSERENTENVERZEICHNIS

Die Ausgabe enthält zwischen Seite 34 und 35 einen  
Beihälter der Firma IAIT (Institut zur Analyse von IT-  
Komponenten) sowie eine Gesamtheilage der Firma  
EUROFORUM sowie eine Teilheilage der Firma ppedv.

# Das IT-Administrator Komplettprogramm!!!

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

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

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



Als bestehender Jahresabonnent können Sie hier upgraden:

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

Oder Sie sind Neukunde? Hier können Sie bestellen:

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

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

# X. Neu definiert.

Bislang war die Sache ganz einfach: Wer mehr Rechenleistung braucht, z. B. für neue, speicherintensive Anwendungen, der muss eben mehr Server kaufen. Das Problem dabei: Mit der Zahl der Server wächst eher die Ineffizienz als die Leistung. Die meisten Server laufen heute nur mit 10% ihrer Kapazität.<sup>1</sup> Zum Glück haben die Entwickler von IBM dieses Problem gelöst. Die 5. Generation der Enterprise X-Architektur verfügt über leistungsstarke Intel® Xeon® 7500-Prozessoren. Vor allem aber kann man erstmals Speicher unabhängig vom Prozessor nachrüsten. Das Resultat: IBM eX5-Systeme können 6-mal mehr Speicher ansprechen als aktuelle x86-Server. Sie können damit rund 50% Lizenzgebühren und bis zu 97% der Speicherkosten sparen.<sup>2</sup>

Smarte Unternehmen brauchen intelligente Software, Systeme und Services. Also: Machen wir den Planeten ein bisschen smarter. Wie, erfahren Sie unter [ibm.com/systems/de/ex5](http://ibm.com/systems/de/ex5)



<sup>1</sup>Die McKinsey-Studie finden Sie hier: <http://www.datacenterknowledge.com/archives/2009/04/15/mckinsey-data-centers-cheaper-than-cloud/> <sup>2</sup>Vergleich eines IBM System x3850 X5 + MAX5 mit 96 DIMMs x 16 GB für insgesamt 1,5 TB Speicher gegenüber einem IBM System x3850 M2 mit 32 DIMMs x 8 GB = 256 GB. Vergleich von Lizenzgebühren auf Prozessorbasis für aktuelle Prozessorsysteme der Generation 4 mit 64 DIMMs gegenüber dem IBM System x3690 + MAX5. Bei Verwendung der IBM eXFlash-Technologie wäre es für einen Kunden nicht mehr erforderlich, zwei Einstiegserver und 80 JBODs zur Unterstützung einer Datenbankumgebung mit 240.000 IOPS zu kaufen, was einer Einsparung von 97% bei Server- und Speicher-Anschaffungskosten entspricht. IBM, das IBM Logo, ibm.com, X-Architecture und das Bildzeichen des Planeten sind Marken oder eingetragene Marken der International Business Machines Corp. in den Vereinigten Staaten und/oder anderen Ländern. Die komplette Liste der IBM Marken siehe unter: [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml). Intel, das Intel Logo, Intel Core, Intel Inside, das Intel Inside Logo, Xeon und Xeon Inside sind Marken oder eingetragene Marken der Intel Corp. oder ihrer Tochtergesellschaften in den Vereinigten Staaten und/oder anderen Ländern. © 2010 IBM Corp. Alle Rechte vorbehalten. O&M IBM IT 19/10