

administrator

Das Magazin für professionelle System- und Netzwerkadministration

Desktop-Virtualisierung

Im Test

**Wyse Mobile Cloud
PCs und WSM 4.0**

10

Im Test

**KAMP Virtual-Core
Customer Cloud**

16

Systeme

**Neuerungen in Hyper-V 3.0
unter Windows Server 8**

28

Workshop

**Open Source-
Virtualisierung mit Qemu 1.0**

36

Know-how

**WAN-Optimierung
vs. RDP-Beschleunigung**

70



BUILT FOR THE FUTURE. READY NOW.

Microsoft Private Cloud-Lösungen

In Zukunft werden Sie Ihr Rechenzentrum kostengünstiger betreiben müssen.

Nehmen Sie eine Private Cloud-Lösung, bei der nicht jede virtuelle Maschine einzeln abgerechnet wird.

Jetzt mehr erfahren auf **Microsoft.de/readynow**



Auf der Jagd

Liebe Leser,

mit dem neuen Hyper-V 3.0 bläst Microsoft zur Aufholjagd auf den Platzhirsch VMware. Mit im Fokus: große Umgebungen à la Private Cloud und Serverfarmen. Dabei hat VMware bereits Ende letzten Jahres mit vSphere 5 vorgelegt. So unterstützt die aktuelle Version 5 nun 1 TByte an Arbeitsspeicher und 32 virtuelle CPUs pro VM. Ebenso viele Kerne soll Hyper-V 3.0 unter Windows Server 8 unterstützen, dazu 512 GByte RAM und 16 TByte große virtuelle Festplatten. Zudem sollen Administratoren ihre virtuellen Server in Hyper-V 3.0 wesentlich leichter zwischen Hosts replizieren können.

Ein Exportvorgang ist nicht mehr nötig, asynchrone Replikationsvorgänge lassen sich im laufenden Betrieb von virtuellen Servern durchführen. Was Sie im neuen Microsoft-Hypervisor 3.0 erwartet, lesen Sie in unserem Artikel ab Seite 28.



Auf der Jagd der etwas anderen Art befinden sich organisierte Hacker, die es auf wertvolle Unternehmensdaten abgesehen haben. Der aktuelle Trend hin zu mobilen Geräten – am besten noch das private Smartphone – macht es ihnen dabei leicht. Ebenso der nach wie vor in vielen Unternehmen fehlende Sinn für IT-Sicherheit. Geht es nach dem Willen der Europäischen Union, sollen Firmen, die ihre IT-Sicherheit vernachlässigen, künftig ordentlich zur Kasse gebeten werden. Die Strafe soll “abschreckend” wirken und bis zu zwei Prozent des Jahresumsatzes betragen. Auch soll es eine Meldepflicht für Hacker-Angriffe geben.

Über die Hälfte der für eine Studie des Ponemon-Instituts befragten deutschen Unternehmen beklagten denn auch Datenverluste allein auf mobilen Endgeräten. Gravierend dabei: Lediglich 55 Prozent der Befragten hätten überhaupt Sicherheitsrichtlinien für die Nutzung mobiler Geräte definiert. Während der letzten zwölf Monate hätten denn auch 57 Prozent der befragten Unternehmen einen Datenverlust durch die Nutzung von unsicheren mobilen Geräten zu beklagen gehabt. Einen Weg zu mehr Sicherheit, auch im mobilen Bereich, zeigt die Desktop-Virtualisierung auf. In unserem Workshop ab Seite 32 erfahren Sie, welche Sicherheits-Features das neue VMware View 5 mitbringt. In unserem Kurztest auf Seite 26 müssen die Cortado Printing Essentials beweisen, wie sie für Sicherheit bei den Ausdrucken sorgen – Smartphones sei dank.

Viel Spaß beim Lesen, Ihr

Daniel Richey

Daniel Richey
Stellv. Chefredakteur

Desktop-Virtualisierung

Im Test: NComputing L300 und vSpace



Was auf den ersten Blick aussieht wie ein ganz gewöhnlicher, recht formschöner Thin Client, ist auf den zweiten Blick ein interessantes Zusammenspiel von Hard- und Software.

Gemeinsam sind sie eine äußerst interessante, leistungsfähige und gleichzeitig kostengünstige Mischung aus Computer, virtuellem Desktop und Terminalserver. In unserem Test haben wir sowohl das Zugriffsgerät als auch die Management-Software unter die Lupe genommen und dabei festgestellt, dass lizenzrechtliche Einschränkungen seitens Microsoft die Freude an der Mini-VDI etwas trüben.

Seite 21

Aufbau einer VDI-Umgebung mit VMware View 5



Nach dem durchschlagenden Erfolg der Server-Virtualisierung verabschieden sich mehr und mehr Unternehmen auch im Desktop-Bereich vom einzelnen Rechner mit lokal installiertem Betriebssystem. Zur Verwirklichung einer Virtual Desktop Infrastructure bietet VMware mit View eine eigene Lösung an, die mit der Ende 2011 erschienenen Version 5.0 eine erneute Optimierung erfahren hat. In diesem Beitrag stellen wir die einzelnen Elemente des Produkts vor und gehen auf die wichtigsten Punkte ein, die im Rahmen einer (Teil-)Umstellung auf virtuelle Desktops zu beachten sind. Nicht zuletzt beleuchten wir das Zusammenspiel mit vSphere und den Einsatz von Thin Clients.

Seite 32

AKTUELL

06 News

PRODUKTE

- 10**  **Im Test: Wyse Mobile Cloud PCs und WSM 4.0**
Mit der Desktop-Virtualisierungslösung WSM 4.0 positioniert sich Wyse als Experte in Sachen Cloud-basiertes Client Computing. IT-Administratoren hat sich angeschaut, was die Systeme taugen und wie das Management per WSM funktioniert.
- 16**  **Im Test: KAMP Virtual-Core Customer Cloud**
Wenn die gängigen Cloud-Modelle eine Nummer zu groß sind, dem steht mit dem Ansatz von KAMP eine Alternative zur Verfügung. Wir haben uns im Test angesehen, ob die Trennung von Cloud-Ressourcen und Cloud-Steuerung im Alltag zu überzeugen weiß.
- 21**  **Im Test: NComputing L300 und vSpace**
Das interessante Zusammenspiel von Hard- und Software ermöglicht es Unternehmen, auch im ganz kleinen Rahmen, etwa für Schulungsräume, auf VDI zu setzen. In unserem Test haben wir sowohl das Zugriffsgerät als auch die Management-Software unter die Lupe genommen.
- 26**  **Im Kurztest: Cortado Personal Printing Essentials**
Die Cortado Personal Printing Essentials sollen mittels Authentifizierung am Drucker für Sicherheit sorgen. IT-Administratoren hat im Rahmen eines Kurztests untersucht, wie die Lösung funktioniert.

PRAXIS

- 28**  **Systeme: Neuerungen in Hyper-V 3.0 unter Windows Server 8**
Mit der neuen Version Hyper-V 3.0 im kommenden Windows Server 8 versucht Microsoft den Sprung an die Virtualisierungsspitze. In diesem Beitrag lesen Sie, welche Neuerungen auf Sie warten.
- 32**  **Systeme: Aufbau einer VDI-Umgebung mit VMware View 5**
Zur Verwirklichung einer Virtual Desktop Infrastructure bietet VMware mit View eine eigene Lösung an, die mit Version 5.0 eine erneute Optimierung erfahren hat. In diesem Beitrag stellen wir dessen Funktionen vor und beleuchten das Zusammenspiel mit vSphere.
- 36**  **Workshop: Virtualisierung mit QEMU 1.0**
Beim Thema Desktop-Virtualisierung fällt den meisten Administratoren die Produktpalette von VMware oder das VirtualBox-Projekt ein. Doch mit QEMU gibt es eine Alternative, die für ihre gute Ausführungsgeschwindigkeit bekannt ist.
- 42**  **Workshop: Zentrale Datensicherung mit Bacula**
Die Datensicherheit und -sicherung werden von Administratoren oft stiefmütterlich behandelt. Doch es gibt professionelle Lösungen wie Bacula, mit denen Sie dieses leidige Thema endlich ad acta legen können.
- 46**  **Workshop: Neuerungen in Citrix XenDesktop 5.5 und Provisioning Services 6.0**
Die neue Version 5.5 von Citrix XenDesktop konzentriert sich primär auf die Optimierung des Bedienkomforts. Doch auch unter der Haube bringen die Provisioning Services 6.0 Verbesserungen bei der Verwaltung der Desktop-Images mit sich.

52 **Workshop: Administration von Windows Server 8 mit dem Server-Manager**

Microsoft integriert in Windows 8 Server vor allem zahlreiche Neuerungen. Der neue Server erlaubt, auch ohne Zusatztools über den Server Manager mehrere Server zu verwalten. Das Werkzeug wurde komplett überarbeitet und zu einer Zentrale der Administration gemacht.

57 **Workshop: Aufbau einer Testumgebung mit VMware Workstation**

Die Neuinstallation von Software oder das Durchführen von Updates im Netzwerk ist oft genug ein kleines Glücksspiel. Wie sich unangenehme Überraschungen durch eine praxisnahe virtuelle Testumgebung auf Basis von VMware Workstation vermeiden lassen, beschreiben wir in diesem Workshop.

62 **Systeme: Fortgeschrittene Methoden des IT-Projektmanagements (2)**

Arbeiten verschiedene Menschen gemeinsam auf eine Sache hin, sind nicht selten soziale Konflikte programmiert. Damit Sie als Projektleiter souverän mit zwischenmenschlichen Problemen umgehen können, geben wir Ihnen passende Konfliktmanagementwerkzeuge an die Hand.

66 **Tips, Tricks & Tools**

WISSEN

70 **Know-how: WAN-Optimierung vs. RDP-Beschleunigung**

Virtuelle IT-Umgebungen liegen auch im Desktop-Bereich im Trend. Die Anwender kämpfen aber nicht selten mit Performance-Problemen. Abhilfe versprechen WAN-Optimierer und RDP-Beschleuniger. Unser Artikel zeigt die Vor- und Nachteile dieser beiden Techniken auf.

74 **Recht: Die acht Gebote des Datenschutzes: Eingabekontrolle (4)**

Durch die Eingabekontrolle muss nachträglich überprüfbar sein, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt wurden. Wie Sie dies rechtskonform sicherstellen, lesen Sie im vierten Teil unserer Artikelreihe.

78 **Know-how: Als Opa Admin war: HP-85**

79 **Buchbesprechung** "Professionelles Mac OS X-Client-Management" und "OS X Lion und UNIX, 6. Auflage"

80 **Website & Fachartikel online**

RUBRIKEN

- 03 Editorial**
- 04 Inhalt**
- 81 Das letzte Wort**
- 82 Vorschau, Impressum, Inserentenverzeichnis**

Kostenlos für
IT-Administrator-Abonnenten

iläNet

Workshop in Frankfurt / Eschborn

Virtualisierung im Client-Management am 31. Mai 2012

Die Agenda:

13:00 Uhr: Begrüßung

13:15 Uhr: Virtualisierung des Desktops

- Erfolgsfaktoren von VDI-Projekten: Methoden, Werkzeuge und Kompetenzen
- VDI vs. Client-seitige Virtualisierung (XenDesktop, Hyper-V 3.0)
- Integration mobiler Geräte

Dozent: Nico Lüdemann, acocon GmbH, Bielefeld

14:45 Uhr: Kaffeepause

15:00 Uhr: Partnervortrag:

Consumerization of IT – Wahn oder Wirklichkeit?



Dozent: Matthias Wessner, Login Consultants

15:45 Uhr: Virtualisierung von Anwendungen und Profilen

- Anwendungs- und Präsentationsvirtualisierung
- Virtualisierte Benutzerprofile
- Zusammenspiel der vorgestellten Virtualisierungstechnologien im Rahmen einer Desktop-Strategie

Dozent: Nico Lüdemann, acocon GmbH, Bielefeld

17:30 Uhr: Ende des Workshops

Ort:

Fast Lane Institute for Knowledge Transfer GmbH,
Ludwig-Erhard-Straße 3, 65760 Frankfurt / Eschborn



Uhrzeit: 13.00 bis 17.30 Uhr

Teilnahmegebühren:

Für IT-Administrator-Abonnenten kostenlos.

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

Anmeldeschluss:

23. Mai 2012

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

Neues in XenDesktop 5.5 und Provisioning Services 6.0



Mit Version 5.5 von XenDesktop setzt Citrix die Entwicklung der hauseigenen Infrastruktur-Lösung zur Bereitstellung virtueller Desktops fort. Brachte der Vorgänger 5.0 tiefgreifende Änderungen an der Architektur mit sich, konzentriert sich die neue Version

primär auf die Optimierung des Bedienkomforts. Doch auch unter der Haube bringen die Provisioning Services 6.0 Verbesserungen bei der Verwaltung der Desktop-Images mit sich. IT-Administrator stellt Ihnen die Neuerungen vor.

Seite 46

Fortgeschrittene Methoden des IT- Projektmanagements (2)



Wo gehobelt wird, fallen Späne: Dieses Sprichwort beschreibt die Realität in Projektteams bisweilen recht treffend. Kommen Menschen mit unterschiedlicher Kompetenz und Persönlichkeit zusammen, um gemeinsam auf eine Sache hinzu-

arbeiten, sind nicht selten soziale Konflikte vorprogrammiert. Damit diese Ihr Projekt nicht lahmlegen und Sie als Projektleiter künftig souverän mit zwischenmenschlichen Problemen umgehen können, geben wir Ihnen passende Konfliktmanagementwerkzeuge an die Hand.

Seite 62

Link-Codes

Unsere Link-Codes ersparen Ihnen mühsame Tipparbeit bei langen URLs



NAS zur freien Bestückung

LaCie liefert den Netzwerkspeicher **5big Network 2** nun auch **ohne Festplatten** aus und stellt die Bestückung der fünf Laufwerksschächte dem Nutzer frei. Bei Verwendung von 3 TByte-Platten lässt sich das NAS mit 15 TByte ausstatten. Ebenso ist ein Mischbetrieb mit unterschiedlichen HD-Größen möglich. Das ohne Magnet-speicher ausgelieferte Modell soll so den Einsatz des NAS flexibel gestalten: Festplatten lassen sich nach Bedarf einsetzen – das Gerät erstellt dann automatisch den entsprechenden RAID-Modus. Außerdem wartet der Speicherwürfel mit den RAID-Modi 5 und 6 auf, die für automatischen Datenschutz auf Hardware-Ebene sorgen. Fällt eine Festplatte aus, kann der Nutzer

diese einfach austauschen, ohne das Gerät ausschalten zu müssen. Auch die Verwendung als iSCSI-Zielserver stellt laut Hersteller kein Problem dar. Nutzer können Datensicherungsvorgaben für mehrere Linux-, PC- und Mac-Workstations festlegen und so sicherstellen, dass alle Daten an einem Speicherort verwahrt werden. Das NAS-System ist mit Apples Time Machine sowie Windows 7 Backup kompatibel. Dazu unterstützt es aufgrund des Dual-LAN-Anschlusses Datentransferraten von bis zu 70 MBit/s, womit LaCie eine hohe Geschwindigkeit der Datensicherung im ganzen Unternehmen gewährleisten will. Ac-



Nicht jedes NAS muss schwarz sein – LaCie bewirbt das „5big Network 2“ auch mit seinem außergewöhnlichen Design

tive Directory- und UPnP-Unterstützung ergänzen den Funktionsumfang des Netzwerkspeichers, der in der Variante ohne Festplatten knapp 300 Euro kostet. (In) LaCie: www.lacie.com

Linux-Kassenwart

SUSE hat das **Service Pack 2** für **SUSE Linux Enterprise Point of Service (POS) 11** veröffentlicht. Das System basiert auf Linux und ist für die spezifischen Anforderungen des **Einzelhandels** konzipiert. Es ermöglicht den Einsatz von Linux von der Kasse über den Filialserver bis hin zum Verwaltungsserver im Rechenzentrum. Die Lösung setzt dabei auf dem SUSE Linux Enterprise Server auf und kombiniert diesen mit handelspezifischen Zusatzmodulen,

die die Einrichtung einer POS- und Filialumgebung erleichtern. Sie soll so eine einfache, flexible und kostengünstige Implementierung, Verwaltung, Kontrolle und Aktualisierung der gesamten POS-Infrastruktur ermöglichen. Die Neuerungen des Service Pack 2 umfassen eine Full-Disk-Encryption auf Terminals für Daten- und Root-Partitionen. Zudem können Administratoren das integrierte Subscription Management Tool zur zentralen Verwaltung von Software-Updates

sowie Sicherheitsrichtlinien nutzen. Im Bereich der Verfügbarkeit bietet das Update Verbesserungen bei RAID1 auf Image-basierten Terminals. Die zugehörigen PXE-Images können nun auf jedem Terminal gespiegelt vorgehalten werden. Ferner ist es möglich, verschiedene Versionen an PXE-Bootimages vorzuhalten. Das Service Pack 2 steht im Rahmen einer bestehenden Subscription kostenfrei zur Verfügung. (dr)

SUSE: www.suse.com

Brillanter Flachmann

Mit dem **S271HL** aus der S1 Display-Serie bietet Acer einen **LCD-Bildschirm mit energieeffizienter und umweltverträglicher LED-Hintergrundbeleuchtung** an. Das Display ist 24 mm dünn und wird von einem glänzend schwarzen Rahmen umschlossen. Das Acer Adaptive Contrast Management soll für eine optimierte Darstellung extrem kontrastreicher und farbtintensiver Bilder in leuchtenden Farben mit einem dynamischen Kontrastverhältnis von bis zu 100.000.000:1 sorgen. Zudem will der Hersteller die Farbabstufung und Detaildarstellung erheblich gesteigert haben und reguliert das Kontrastverhältnis des Eingangssignals abhängig vom Bildinhalt dynamisch, um gestochen scharfe Bilddarstellung sicherzustellen. Damit sei der

Bildschirm eine geeignete Wahl etwa für die Bildbearbeitung oder CAD-Anwendungen, die eine hohe Präzision und eine außerordentlich feine Liniendarstellung nötig machen. Das Modell arbeitet mit der White LED Backlight-Technologie, die eine Herstellung der Displays ohne schädliche Substanzen wie Quecksilber oder Halogengase ermöglicht und gegenüber herkömmlichen LCDs mit vier Lampen für eine Reduzierung des Ener-



Soll bis zu 68 Prozent weniger Energie benötigen: Das Acer S271HL

gieverbrauchs um bis zu 68 Prozent sorgen soll. Für rund 209 Euro ist der Bildschirm erhältlich. (dr)

Acer: www.acer.de

IT-Dokumentation kann auch Spaß machen

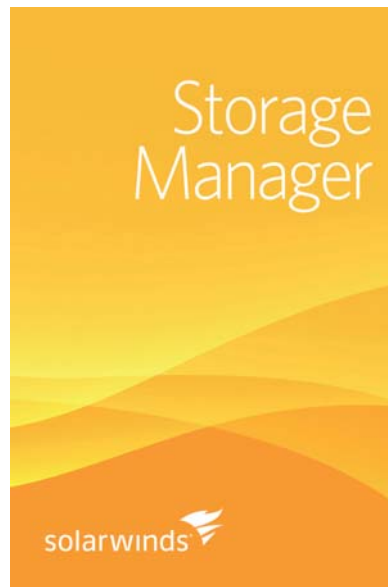
itelio gibt den Startschuss für **Release 6.0 von Docusnap**. Das **Dokumentationswerkzeug** kommt nun auch mit Microsoft SharePoint, den Internet Information Services und Hyper-V zurecht und verfügt in der neuen Version über eine **erweiterte Berechtigungsanalyse**, die auf SharePoint ausgeweitet wurde und neue grafische Darstellungsformen beinhaltet. Das optionale Modul liest die Berechtigungen von Windows-PCs auf Basis von NTFS- und Freigabeberechtigungen aus und bietet diverse Funktionen für die Analyse, etwa die Inventarisierung und Visualisierung von Vererbungsblockern oder die Ausgabe von effektiven Rechten für selektierte Benutzer und Gruppen. Die Software erstellt nun zudem einen Soll/Ist-Abgleich von installierten Lizenzen. Dabei lassen sich laut Hersteller jegliche Lizenzmodelle abbilden, egal

ob die Lizenzierung nach Geräten, Benutzern, Prozessoren oder Prozessorkernen erfolgt. Ein weiterer Bestandteil der Software ist die Inventarisierung von SNMP-Komponenten – neu ist hierbei die Unterstützung von SNMP in Version 3. IT-Konzepte wie Notfallpläne oder Betriebshandbücher lassen sich im aktuellen Release jetzt direkt per Drag & Drop in der Benutzeroberfläche von Docusnap erstellen. Weitere Neuerungen betreffen einheitliche Layout-Stile für alle Ausgabedokumente und eine Hierarchie zur Organisation von Dokumenten. Der Preis von Docusnap richtet sich nach der Anzahl der inventarisierten Rechner und der verwendeten Module. 25 überwachte Stationen etwa schlagen inklusive einem Bundle der wichtigsten Module mit rund 475 Euro zu Buche. (In)

itelio Docusnap: www.docusnap.de

Herstellerübergreifender SAN-Betreuer

SolarWinds bringt mit **Storage Manager 5.2** die neueste Version seiner **Software zur Speicherverwaltung** auf den Markt. Das Überwachungstool unterstützt im neuen Release mehr als zehn Storage-Hersteller und über 25 Arrays, darunter mit den Serien Compellent, Equal-Logic und PowerVault MD30/32/36 sämtliche von Dell angebotenen SAN-Systeme. Die neue Ausgabe der Management-Lösung bietet Nutzern laut SolarWinds umfangreiche Detailansichten, die über den Funktionsumfang der von den Storage-Herstellern mitgelieferten Management-Tools hinausgehen. So verfügt die Software nun auch über Zielansichten für Blockspeicher (Fibre Channel, iSCSI LUN) und File Storage Shares (NFS). IT-Administratoren sollen so in die Lage versetzt werden, mögliche Konflikte sowohl auf der Virtualisierungs- als auch auf der Speicherseite einfacher zu erkennen und sie mit zusätzlichen Leistungskennzahlen für HP EVA, IBM SVC und IBM DS 6/8K Speicher-Arrays schneller zu lösen. Frei konfigurierbare Diagramme zeigen Speicher- und Leistungstrends an, umfangreiche Alarm-Funktionen sollen frühzeitig auf Probleme hinweisen. Zu den weiteren Funktionen zählen Speicherleistungsüberwachung und Hotspot-



SolarWinds hat für Version 5.2 des Storage Manager die Liste der unterstützten SAN-Arrays erneut erweitert

Isolierung. Die Speicherkapazitätsplanung erfasst automatisiert Prognose-Daten und soll Hochrechnungen ermöglichen, wann eine bestimmte Speicherkapazität erreicht wird. Nicht zuletzt übernimmt das Werkzeug die automatische Zuordnung von virtuellen Maschinen zu physischem Speicher. Storage Manager 5.2 ist ab sofort erhältlich. Die Lizenzierung richtet sich nach der Anzahl der verwalteten Festplatten. Der Einstiegspreis für 25 Disks beträgt 2.440 Euro. (In)

SolarWinds: www.solarwinds.com/products/storage-management/

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

Nach der Veröffentlichung einer iOS-App und eines Web-Clients bringt **FastViewer** nun auch eine **Android-Anwendung** für seine gleichnamige Remote- und Fernwartungs-Software heraus. Die App erlaubt neben der Teilnahme an einer Web Session auch aktives Arbeiten – so ist es zum Beispiel möglich, einen Rechner fernzusteuern und Eingaben über die Tastatur vorzunehmen. Ebenfalls lassen sich mit der Anwendung Videos von Webcams empfangen und das eigene Videobild übertragen. Eine Chat-Funktion rundet die App in Sachen Wortmeldungen ab. Das Remote-Tool steht ab sofort kostenlos auf den Webseiten von Google Play zum Download bereit. (In)

www.fastviewer.de

AppSense stellt die von **AppSense Labs** entwickelte neue Technologie **StrataApps** vor. Diese unterstützt Unternehmen dabei, neben der IT-Effizienz auch die Anwenderproduktivität zu verbessern. Wenn ein Anwender eine App installiert, die nicht von der Unternehmens-IT zentral bereitgestellt wird, müssen IT-Manager sicher sein, dass Compliance-Probleme auf dem Zielgerät verhindert werden und sie einen Bericht hinsichtlich des Installationserfolgs erhalten. Mit StrataApps können Anwender selbst ausgewählte Apps herunterladen und installieren, ohne Probleme zu verursachen oder etwas an der Systemkonfiguration zu ändern. StrataApps steht als kostenloser Download zur Verfügung. (dr)

www.appsense.com

TeamViewer gibt die Verfügbarkeit von **TeamViewer 7 für Mac** bekannt. Die Software ermöglicht Cross-Plattform-Kommunikation zwischen Windows- und Linux-Rechnern, Macs sowie iOS- und Android-basierten Geräten. Dabei wird die Einrichtung von Online-Meetings für bis zu 25 Teilnehmer unterstützt. Sowohl in Online-Meetings als auch in Fernwartungssitzungen besteht in der neuen Mac-Version jetzt die Möglichkeit der Videoübertragung. Ferner eignet sich TeamViewer 7 für den Mac für Einsätze in den Bereichen Remote Support und Desktop Sharing. TeamViewer 7 für Mac ist ab sofort verfügbar und läuft auf Mac OS X Systemen ab Version 10.4, inklusive OS X "Lion". Für die professionelle Nutzung sind Lizenzen zu einmaligen Kosten ab 499 Euro erhältlich. (dr)

www.teamviewer.com

FCS Fair Computer Systems hat den Hardware-verschlüsselten USB-Stick **Store O'Crypt** mit einem neuen, kostenfreien Feature ausgestattet. Durch die Integration der Plattform **PortableApps.com** in die Launcher Anwendung von Store O'Crypt lassen sich ab sofort portable Anwendungen (wie der portable Mozilla Firefox Browser) ganz einfach auf den Stick laden, dort installieren und in der sicheren und abgeschlossenen Umgebung des Sticks betreiben. Die persönlichen Programmeinstellungen wie Bookmarks und Favoriten bleiben auf dem Stick erhalten, unabhängig vom verwendeten Host-PC. Der USB-Stick ist derzeit in den Größen 4 und 8 GByte für 31 beziehungsweise 55 Euro erhältlich. (dr)

www.fair-computer.de

Bonjour durch die Luft

Aerohive Networks stellt ein neues **Gateway** vor, das die Apple Zero-Configuration-Networking Technologie Bonjour unterstützt. Damit werden Services wie Airprint und Airplay unabhängig von der zugrundeliegenden Topologie im gesamten Netzwerk nutzbar. Das neue **Bonjour-Gateway** wird als **Software-Upgrade** für bestehende Kunden oder als **separate Plattform** für Anwender von anderen drahtlosen oder kabelgebundenen Netzwerken bereitgestellt. Als nicht-routbares Layer 2-Protokoll unterliegt Bonjour der Einschränkung, dass es nicht einfach über Subnetze hinweg arbeitet. Um dieses Problem zu lösen, hat Aerohive die Bonjour-Unterstützung über das gesamte Netzwerk hinweg und

unabhängig von der Basistopologie in die Produktpalette integriert. Das Gateway ermöglicht somit etwa Airprint von Geräten mit iOS im gesamten Netzwerk. Das Gateway behandelt dabei lediglich die Service-Ankündigungen und nicht den Service selbst, so dass die existierenden Sicherheitsregelungen im Unternehmen erhalten bleiben und das Gateway nicht zum Durchsatz-Engpass wird. Das Aerohive Bonjour-Gateway ist für Beta-Tests im zweiten Quartal dieses Jahres verfügbar und soll voraussichtlich in der Mitte des Jahres kostenfrei ausgeliefert



Die Aerohive Access Points unterstützen künftig das Netzwerkprotokoll Bonjour

werden. Das günstigste Aerohive-Modell AP 110 kostet rund 400 Euro. (dr)

Aerohive: www.aerohive.com

Domino-Schutz

Norman ergänzt den Business-Virenschutz **Norman Endpoint Protection** (NPRO) um ein Plug-In für den **E-Mail-Scan von IBM Lotus Domino**. MailScan für Lotus Domino wird über die zentrale Administrations- und Konfigurations-Konsole Norman Endpoint Manager als Bestandteil der Virenschutzlösung konfiguriert und verwaltet. Das Plug-In ermöglicht das Scannen aller in der Notes Mail.Box-Datenbank eingehenden E-Mails, auch die zwischen Notes-Anwendern intern verschickten, auf virulente Anhänge. Zusätzlich können Anhänge, zum

Beispiel .exe-Dateien oder Wildcards, also Platzhalter-Dateibezeichnungen wie *.exe, pauschal geblockt und Trust- oder Blocklist-Einträge für bestimmte Absender-Mailadressen angelegt werden. Das Plug-In unterstützt dabei den E-Maildienst der Collaboration-Plattform von IBM ab Version 8.0.1 bis einschließlich der aktuellen Version 8.5.3 und wird an künftige Versionen angepasst. Es wird mit dem Update auf NPRO 9.01 ausgeliefert und kann ohne Aufpreis genutzt werden, sofern NPRO Advanced lizenziert ist. Weitere Verbesserungen in Version 9.01 betreffen die Per-

formance von On-demand- und On-access-Scanner durch die Integration von Whitelisting. Ein neues Scan- und Hashing-Verfahren beschleunigt manuelle Scans und verringert die Systembelastung. Die Verwendung von Wildcards und Verzeichnisnamen beim Mini-Filter soll die Exclude-List-Optionen verbessern. Außerdem hat Norman die Einstellungsmöglichkeiten in der Scan-Ausschlussliste auf Verzeichnisse einschließlich der Wildcards ausgedehnt. Für 46 bis 50 Clients kostet der Virenschutz 1.268 Euro pro Jahr. (dr)

Norman: www.norman.de

Rundum-Sicher-Paket

Blue Coat Systems präsentiert sein neues **Unified-Security-Angebot**. Dieses ermöglicht Unternehmen, Mitarbeiter und deren Geräte in beliebigen Netzen vor Gefahren aus dem Web zu schützen. Das Angebot umfasst **Global Threat Defense**, **Universal Policy** und **Unified Reporting** von Secure Web Gateway-Appliances bis hin zum Cloud-basierten **Blue Coat Security Service**. Universal Policy gibt Unternehmen dabei die Möglichkeit, globale Richtlinien zu erstellen, die einem Nutzer nahtlos über alle Netzwerke und Geräte hinweg folgen. Die Funktion einer Richtlinie pro Benutzer baut auf der Policy-Engine auf, die akti-

onsbasierte Policies sowie fein abgestufte Steuerungsmöglichkeiten von Web-Anwendungen und deren Operationen zur Verfügung stellt. Dank Unified Reporting erhalten Administratoren einen ganzheitlichen Einblick in das gesamte Web- und Nutzerverhalten. So soll das Reporting beispielsweise kontinuierlich bedrohliche Aktivitäten im Netzwerk und auf infizierten Systemen von Endanwendern iden-

tifizieren und so eine schnelle Behebung sowie forensische Analyse ermöglichen. Global Threat Defense, Universal Policy und Unified Reporting für die Blue Coat Unified-Security-Lösung sind ab sofort verfügbar. Die Preise beginnen bei 5.000 Euro für eine Web-Security-Appliance und 17 Euro für einen Benutzer des Blue Coat Web Security Services. (dr)

Blue Coat: www.bluecoat.de



Das Unified-Security-Angebot von Blue Coat schützt über die Cloud sowie Web Gateway-Appliances des Herstellers

Vollgas für Daten

Die **LSI Corporation** stellt mit **Nytro** eine neue Reihe von Produkten vor. Diese verbinden **PCIe Flash-Technologie** mit einer Caching- und Management-Software und sollen so die Performance von Applikationen beschleunigen. In diesem Portfolio bietet die **LSI Nytro WarpDrive**-Karte dazu Kapazitäten von 200 GByte bis 3,2 T-Byte mit MLC oder SLC Flash-Speicher im Zusammenspiel mit den LSI SAS Controller ICs. Dabei erweitert die Software **LSI Nytro XD** die PCI-Karte um eine Caching-Funktion zur Beschleunigung von Applikationen in SAN- und DAS-Umgebungen. Nytro XD cacht häufig zugegriffene Daten auf dem PCIe Flash-Speicher, was Latenzzeiten reduziert und nach Herstellerangaben im Vergleich zu Speichersystemen auf Festplattenbasis eine bis zu 30 mal höhere Leistung bietet.



Dank Flash-Speicher on board beschleunigen die neuen Nitro-Karten von LSI den Datenfluss im SAN oder bei DAS

Für kleinere Umgebungen oder Stand alone-Server bietet die **LSI Nytro MegaRAID**-Karte eine einfache und kostengünstige Beschleunigung von durch SAS verbundenen DAS-Speicher. Diese Karte bewegt Daten zwischen integriertem Flash-Speicher und Festplatten. Das Portfolio der LSI Nytro-Reihe wird ab sofort an OEM-Kunden ausgeliefert und soll im zweiten Quartal erhältlich sein. Empfohlene Verkaufspreise für Nytro WarpDrive-Karten starten ab 6.600 US-Dollar, Nytro XD ist ab 9.400 Dollar erhältlich und Nytro MegaRAID-Karten werden ab 1.699 Dollar angeboten. (jp)

LSI: www.lsi.com

Hochglanz-Telefon

Gigaset bringt sein Telefon-Modell **SL910** mit **neuer Software** auf den Markt. Zu den Produktneuerungen gehört unter anderem die **automatische Bild-Übertragung aus Outlook-Kontakten** in das Adressbuch des Mobilteils. Gigaset hat außerdem die **Geschwindigkeit in der Bedienung** des Full-Touch-Telefons weiter beschleunigt. Auch steht jetzt die **SMS-Funktion** zur Verfügung. Als Full-Touch-Telefon verfügt das SL910 über einen berührungsempfindlichen Bildschirm, der kontextabhängig Bedienflächen zeigt. Dies können Zifferntasten sein und auch kleine elektronische Helfer im Stil der Apps, wie sie von Smartphones bekannt sind. Mit ihnen lässt sich das Bedienmenü individuell konfigurieren. Die neue Software-Version 03/2012 bietet die Möglichkeit, SMS mit bis zu 612 Zeichen zu versenden und zu empfangen. Beim Synchronisieren der Kontakte aus Outlook können jetzt auch Bilder mit übertragen werden. So kann das SL910H-Mobilteil sein hochwertiges Display für die Anrufer-Anzeige mit Bild – Picture-Clip genannt – zur Geltung bringen. Insgesamt speichert das interne Adressbuch bis zu 500 Einträge im beliebten vCard-Format, jeder mit bis zu acht Rufnummern. Die Verbindung zum PC wird über Bluetooth oder ein Mini-USB-Kabel hergestellt. Für 126 Euro ist das Telefon erhältlich. (dr)

Gigaset: www.gigaset.com



Das Gigaset SL910 überträgt nun auch Bilder bei der Outlook-Synchronisation

Ausfallsichere Faxumgebung

Ab sofort ist die neue **Version 5.90** der **Fax- und Unified Messaging-Lösung IXI-UMS** von **Servonic** erhältlich. Administratoren können in der neuen Version für die Rufnummernzuordnung und die LDAP-Suche drei weitere LDAP-Server angeben. Fällt ein LDAP-Server aus, wird automatisch der nächste genutzt. Dadurch ist gewährleistet, dass die UM-Funktionalität trotz eines oder mehrerer LDAP-Serverausfälle bestehen bleibt. Eine weitere Neuheit im Bereich Ausfallsicherheit ist die Festplattenüberwachung. So werden Benutzer informiert, falls ihre Festplatte voll ist. Darüber hinaus ist es in Version 5.90 möglich, einzelne OUs für die LDAP-Suche anzugeben. IT-Verantwortliche definieren, in welchen OUs die für den Austausch der UM-Nachrichten benötigten Informationen zu finden sind. Dies soll in großen Unternehmen mit umfangreichen Active

Directorys für eine deutliche Performance-Steigerung sorgen. Erhöhte Sicherheit und flexiblere Möglichkeiten bietet IXI-UMS 5.90 im Bereich der mobilen Abfrage. Das Enhanced Voice Package der neuen IXI-UMS Version unterstützt IMAPS: Der Benutzer greift unterwegs über eine verschlüsselte Verbindung auf seine Nachrichten im Microsoft Exchange 2010 oder 2007 zu. Der Administrator kann die Reihenfolge der Ansage beim Abfragen der UM-Nachrichten festlegen. Schließlich wartet die UMS-Lösung mit individuelleren Gestaltungsmöglichkeiten der Fax-Coverpage sowie erweiterten Faxmöglichkeiten auf. Abhängig von der Empfänger-Nummer werden unterschiedliche Fax-Deckblätter zur Faxnachricht hinzugefügt. Die neue IXI-UMS Version 5.90 ist ab 650 erhältlich. (dr)

Servonic: www.servonic.com

**Im Test: Wyse Mobile Cloud PCs und WSM 4.0**

Ein bisschen Cloud muss sein

von Dirk Srocke



Mit der Desktop-Virtualisierungslösung WSM 4.0 positioniert sich Anbieter Wyse als Experte in Sachen Cloud-basiertes Client Computing. Das umfasst mittlerweile nicht mehr nur klassische Thin Clients, sondern auch mobile Endgeräte. Dank eingebauter SSDs funktionieren die so genannten "Cloud PCs" auch ohne Anschluss an ein Firmennetz. IT-Administrator hat sich angeschaut, was die Systeme taugen, wie das Management per WSM funktioniert und welche Nutzungsszenarien sich anbieten. Dabei galt es, so manche Hürde zu nehmen.

Mit dem Cloud PC hat Wyse das Konzept des Thin Client ein wenig abgewandelt. In Reinform besitzt solch ein Cloud PC zwar weder Festplatte noch eigenes Betriebssystem, führt Applikationen aber dennoch selbst aus. Statt auf einem Server laufen Anwendungen also auf klassischer PC-Hardware. Das Betriebssystem-Image und provisionierte Applikationen werden allerdings auf Servern vorgehalten und per Netzwerk auf die Clients gestreamt. Somit erklärt sich dann auch der Name der Cloud PCs: Cloud steht für eine private Cloud, mit Technik für Streaming und Verwaltung von Betriebssystemabbildern, Benutzern und Applikationen. Cloud PC versinnbildlicht einen Client, dessen Innenleben ziemlich nah am klassischen Desktop angelehnt ist.

Noch eine Spur näher an klassischen Desktoprechnern bewegen sich die in unserem Test genutzten Notebooks mit der Bezeichnung X00M. Auf den ersten Blick sind die Geräte nicht von klassischen Rechnern zu unterscheiden und lassen sich genauso wie diese nutzen, da im Inneren eine SSD verbaut wurde. Erst dadurch wird es möglich, die Notebooks autark und auch ohne Netzverbindung zu nutzen. Im Ge-

genzug bedeutet das allerdings auch, dass prinzipiell beliebige Notebooks als Cloud PCs eingesetzt werden könnten.

Der Einfachheit halber haben wir uns im Rahmen des Testprogramms für von Wyse gelieferte X00M-Systeme entschieden. Auf uns machten die 14-Zoll-Laptops einen ordentlichen, aber keinen herausragenden Eindruck. Das schlichte Plastikgehäuse ist zweckmäßig und bringt eine brauchbare Schnittstellenausstattung mit. Zu dieser gehören drei USB-Ports (davon zwei für USB 3.0), GBit-Ethernet, Audiobuchsen und Mediacard-Reader. Externe Bildschirme lassen sich per VGA oder Display-Port anbinden. WLAN ist integriert, ein UMTS-Modem nachrüstbar. Als CPU setzt Wyse auf einen Dual-Core AMD G-T56N mit 1,6 GHz sowie den AMD Radeon HD 6310-Grafikprozessor.

Die Verwindungssteifigkeit des Chassis und das Schreibgefühl des Keyboards sind in Ordnung, wenngleich die Tastatur auf Druck leicht nachgibt. Gefallen hat der weit über 180 Grad hinaus neigbare Bildschirm. Das Display löst mit 1.366 mal 768 Pixel auf und ist leider nur in verspiegelter Ausführung zu haben. Der ab Werk mitgelie-

ferte Akku bietet eine Kapazität von 5.200 mAh. Professionelle Anwender könnten Fingerabdruck-Scanner, Anschluss für eine Dockingstation oder – je nach Anwendung – etwas mehr Leistung vermissen.

Konzept und Infrastruktur

Obwohl der Name Cloud PC Assoziationen mit Googles Chromebook nahelegt, unterscheiden sich die Konzepte grundsätzlich. Während Google ein austauschbares Notebook liefert, mit dem Anwender fast ausschließlich online und mit Google-Diensten arbeiten können, liefert Wyse mit den mobilen Cloud PCs nahezu vollwertige Windows-Rechner mit eingebauter Ver-

Als Serverbetriebssystem schlägt WSM Windows XP Professional SP3 oder einen Windows Server ab 2000 vor. Auf Clientseite empfiehlt der Anbieter Windows ab XP Professional SP3, Vista Enterprise beziehungsweise Business Edition sowie Windows 7 Enterprise Edition oder Professional Edition. 64 Bit-Clients werden bislang noch nicht unterstützt. Wyse WSM unterstützt auch verteilte Serverumgebungen und kann Microsofts Active Directory einbinden. Für unseren Test haben wir uns jedoch auf eine Minimalconfiguration beschränkt.

Systemvoraussetzungen





Operating Systems
OS IMAGE DETAILS

This page allows you to edit the details associated with the OS Image.

[Back to Operating Systems](#)
[Add a New OS Image](#)
[Generate OS Image XML](#)

OS IMAGE DETAILS FOR DEMOOS FIXED:

Name: DemoOS Fixed
File Name: Betriebssystem
Description:
Image Header Version: 4
Version: 1.0.1
OS Class:
Device Class:
Enable Safe Boot: ☒
OS Image ID: a78eae67-433d-4343-9e66-72a7b3f10c15
First Partition Mode: No Cache (Private Mode)

[Reset](#) [Save Changes](#)
[Change Site Group Assignment](#)
[Deploy New OS Image Version For Site Group](#)

SITE GROUPS ASSIGNED OS IMAGE DEMOOS FIXED:

Site Group Name	Description	Version Deployed	Deployment Date
Default	Default Site Group	-	Schedule

[Change Site Assignment](#)

SITES ASSIGNED OS IMAGE DEMOOS FIXED:

Name	Description	Site Group Name	# Of OS Images
win-qhas01myb_site	win-qhas01myb_site	Default	6

[Change Server Group Assignments](#)
[Sync Server Group Assignments](#)

SERVER GROUPS HOSTING DEMOOS FIXED:

Name	Description	Site	# of Servers	# of Device Groups
ServerGruppe		win-qhas01myb_site	1	1

SERVERS STREAMING DEMOOS FIXED:

Name(Group)	IP Address	# of Hosted Images	Server Status	Version Deployed
win-qhas01myb (ServerGruppe)	192.168.2.99	6	Up	DemoOS Fixed

[Release Lock](#)

DEMOOS FIXED HIERARCHY:

Name	File name	Version	Status	Enabled
DemoOS Fixed	Betriebssystem	1.0.1	Active	No

IN PROGRESS CONTENT ENTRIES:

Name	To Machine	Type	Operation	Status	Progress	Schedule
------	------------	------	-----------	--------	----------	----------

Bild 1: In den tieferen Ebenen verliert die Web-GUI des Wyse WSM schnell an Übersichtlichkeit

waltung. Um die Infrastruktur müssen sich Unternehmen dabei selbst kümmern.

Zum portablen Cloud PC macht den X00M vor allem die im Hintergrund

agierende Streaming-Lösung Wyse WSM. Um ganz genau zu sein, handelt es sich dabei um den von der Technologie angebotenen Connection Type "Mobile Disconnected". Im Gegensatz zum Ver-

bindungsmodus "Network" ermöglicht dieser den bereits erwähnten, autarken Betrieb des Clients ohne eine stehende Netzverbindung.

Automatische Installation nur in Englisch

Für die Installation von Wyse WSM hatten wir uns ursprünglich für ein frisch aufgesetztes Microsoft Windows 2008 R2 Standard in der deutschen Version entschieden. Der Einfachheit halber wollten wir uns dabei auf einen einzelnen Serverstandort beschränken und verzichteten ebenso auf die Installation der Rollen für Active Directory und DNS-Dienste. Die Server-IP haben wir fest zugewiesen, Clients wurden per DHCP des LAN-Routers dynamisch mit IP-Adressen versorgt.

Für den Betrieb von WSM setzt Wyse einen laufenden SQL Server voraus, wobei die Express-Version ausreicht. Bereits bei der Installation sind allerdings einige Details zu beachten. So müssen Administratoren den "Mixed Mode" für die Authentifizierung auswählen und ein Passwort setzen. Im Nachgang gilt es noch die Protokolle "Named Pipes" und "TCP/IP" zu aktivieren. Die von Wyse gelieferte Installationsanleitung kann hier durchaus als gelungen bewertet werden, wenngleich sie sich am Procedere des angestaubten SQL Server 2005 orientiert und die angepassten Installationsprozesse des SQL Server 2008 ignoriert.

Weniger gelungen fanden wir hingegen die von Wyse gelieferte Datei *WSM_Pre-requisites.msi*. Die vom Anbieter als Installationshilfe angebotene Datei soll die händische Installation einer SQL-Datenbank komplett übernehmen. Auf unserem deutschen Windows Server 2008 R2 versagte das Tool allerdings mit irritierenden Fehlermeldungen seinen Dienst. So seien einzelne Komponenten nicht für 64 Bit-Betriebssysteme geeignet, bei anderen gäbe es wiederum bekannte Kompatibilitätsprobleme. Ernüchterndes Ergebnis: Die "SQL Server Database Services" sowie einige "Workstation Components" konnten nicht ordnungsgemäß installiert werden. Notgedrungen wichen wir nach diesem Erlebnis auf eine US-Version des Windows Server 2008 R2 Standard aus. Hier schufen



die Prerequisites dann schließlich doch eine ausreichende Grundlage zur Installation des eigentlichen WSM-Servers.

Doch auch dessen Installation scheiterte zunächst aufgrund einer nicht unterstützten Netzwerkverbindung. Aufmerksame Beobachter hätten den Fehler zwar beim Einrichten des Systems bemerken können, denn die von der Installationsroutine zur Wahl gestellten Netzwerkverbindungen blieben leer. Wer das Fenster allerdings leichtfertig wegklickt statt das Problem zu lösen, erhält eine unvollständige Installation – und das ohne weitere Fehlermeldung. Wegen fehlender Dateien versagen einige WSM-Dienste und entsprechend lässt sich dann auch die WSM Adminkonsole nicht starten.

Sind diese Klippen der Serverinstallation umschifft, empfiehlt Wyse noch das händische Aufspielen eines Provisioning Patches. Dann wäre zumindest der Server bereit: Per Link im Startmenü lässt sich die webbasierte WSM-Konfigurationskonsole aufrufen. Wahlweise funktioniert das per HTTP natürlich auch vom Browser eines anderen Rechners im gleichen Netzwerk.

Überarbeitungsbedürftige Management-Software

Wyse WSM liegt mittlerweile in Version 4.0 vor und der Anbieter selbst gibt eine gewisse Überfrachtung des Webinterfaces zu. Dabei macht die Oberfläche auf den ersten Blick einen gut sortierten Eindruck. Nach dem Login erhalten Administratoren einen "System Overview" mit den wichtigsten Daten und Warnungen zu möglichen Problemen. Eine horizontal an der Bildschirmoberseite angeordnete Tableiste erleichtert den Zugriff auf die Sites, Server, Devices oder User.

Bei der Arbeit mit dem Tool haben wir dann aber doch mitunter die Übersicht verloren. Das lag zum einen an den teils langen und nicht sonderlich klar strukturierten Seiten. Einige Inhalte werden zudem nur dynamisch eingeblendet und verwirren den ungeübten Administrator zusätzlich. Ebenfalls nicht wirklich gefallen konnten Fehlermeldungen, die keinen Link auf weiterführende Informationen ausgaben. Wyse verspricht jedoch Besse-

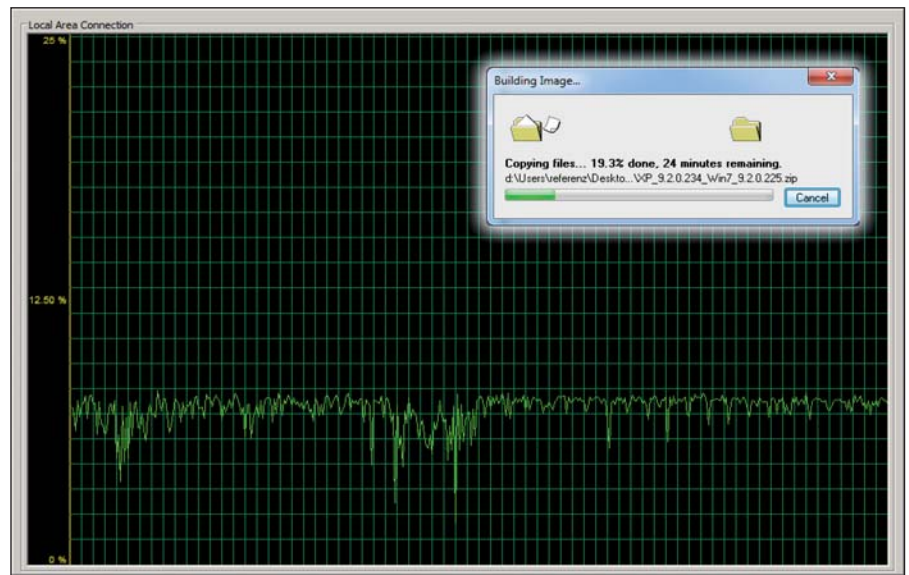


Bild 2: Der Fortschrittsbalken täuscht: Insgesamt dauerte das Erstellen eines OS-Images rund eine Stunde. Das kaum beanspruchte GBit-Ethernet war dabei nicht der Flaschenhals.

rung: In der kommenden Version soll das organisch gewachsene und stetig um Funktionen erweiterte Interface eine Frischeckur bekommen.

Auf die Berichtsfunktionen haben wir in unserem Test nur einen kurzen Blick geworfen. Offenbar können IT-Verantwortliche hier auch einen Überblick über die verwendeten Lizenzen erhalten. Wir haben zwar lediglich Betriebssysteme ausgeliefert, hätten aber auch hierfür gern eine Statistik erhalten. Leider liefert WSM keine solche.

Um Rechner zweifelsfrei zuzuordnen, greift Wyse WSM auf die MAC-Adresse zurück. Administratoren fügen Geräte über einen Assistenten im Web-GUI der Managementlösung hinzu und geben dabei auch die MAC-Adresse ein. Der erste hier eingebundene Client wird als Referenzgerät betrachtet – also das System, von dessen Installation sich das zu streamende Betriebssystemabbild ableitet. Dementsprechend sollte das Referenzsystem möglichst sauber gehalten werden. Per Wyse WSM vergeben Administratoren auch Namen für die jeweils eingebundenen Rechner – die Bezeichnungen werden dann später auch von den Clients als Computernamen übernommen. Typisch für Wyse WSM sind zusätzliche Klassifikationsmerkmale. Für eine bessere Übersicht in größeren Umgebungen können Administratoren Clients in bestimmte Geräteklassen einsortieren oder in Gruppen

zusammenfassen. Später lassen sich bestimmte Kriterien so auch herausfiltern.

Referenzgerät in zäher Handarbeit vorbereiten

Bevor es ans Provisionieren geht, muss noch ein Referenzgerät vorbereitet werden. Die Hardware dieses Systems sollte den später verwendeten Clients entsprechen. Die Installation des Clients gestaltete sich nach unserem Dafürhalten noch umständlicher als die des Servers. Zunächst installierten wir einen 32 Bit-Rechner unter Windows 7 Enterprise. Danach entpackten wir die wichtigsten Treiber für den X00M und installierten diese einzeln, begleitet von einigen Systemstarts. Wyse packt die Treiber für die eigenen Cloud PCs in ein knapp 1,4 GByte großes Paket; eine automatisierte Installationsroutine konnten wir darin nicht ausmachen.

Des Weiteren empfiehlt der Hersteller einen aktuellen Netzwerkkartentreiber direkt beim Chipsatzfertiger herunterzuladen und aufzuspielen. Das sei besonders wichtig, da der Treiber nach Installation der Wyse-Clientsoftware nicht mehr geändert werden könne. Für Windows 7 und Windows 7 SP1 muss vor der Installation der eigentlichen Wyse-Software zudem ein Hotfix für den Umgang mit PCIe-Karten installiert werden. Microsoft selbst liefert den Patch ausschließlich per E-Mail und empfiehlt, das Hotfix vor dem Einsatz in Produktivumgebungen ausgiebig zu

*Mit baramundi
in die Pole Positions.*



Start your Engines! Pole-Position für IT-Profis.

Von energieeffizienter IT-Verwaltung, über Mobile Device Management bis Datenschutz

Modernes IT-Lifecycle-Management geht weit über das reine Verteilen von Software hinaus. Sie sind herzlich eingeladen, das live zu erleben.

Finden Sie heraus, wie Sie Ihre IT noch effizienter und effektiver organisieren, wie Sie Routineaufgaben einfach automatisieren und sich für die Herausforderungen der Zukunft rüsten.

Mit am Start



Reibungslose automatisierte Migration zu Windows 7 – bald Windows 8



Mobile Endgeräte sicher ins IT-Management einbinden und administrieren



Stromverbrauch am PC-Arbeitsplatz senken und Kosten sparen



Tipps vom Rechtsanwalt: IT-Lifecycle-Management und die Einhaltung deutscher Datenschutzbestimmungen

Die Teilnahme ist kostenlos. Weitere Informationen und die detaillierte Agenda finden Sie online: www.baramundi.de/focustour

Die Plätze sind limitiert. Sichern Sie sich Ihr Eintrittsticket!

Renntage



08.05.2012 – Meilenwerk **Stuttgart**

22.05.2012 – Classic Remise **Düsseldorf**

23.05.2012 – Opel Forum **Rüsselsheim**



14.06.2012 – Classic Remise Meilenwerk **Berlin**

19.06.2012 – LENKWERK **Bielefeld**



20.06.2012 – AUTOMUSEUM PROTOTYP **Hamburg**

26.06.2012 – Da Capo Oldtimermuseum **Leipzig**

27.06.2012 – Museum für historische Maybach-



Fahrzeuge **Neumarkt i. d. Oberpfalz**

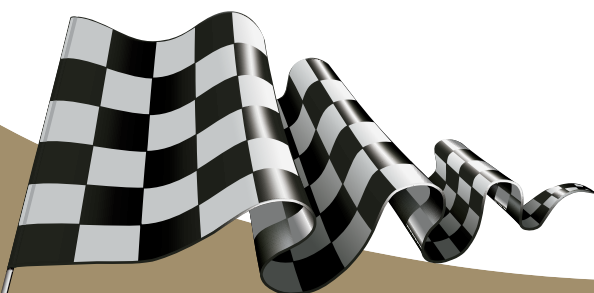
28.06.2012 – BMW Welt Event Forum **München**

Mit der besten Strategie gewinnen

Begleiten Sie uns in die faszinierende deutsche Automobilgeschichte – und erleben Sie High-tech für IT-Profis live. Gewinnen Sie neue Perspektiven für Ihr IT-Team und sichern Sie sich mit etwas Glück Ihre private Rennstrecke: eine digitale Carrera Rennbahn!

**Unverbindlich
Anmelden**

www.baramundi.de/focustour



*Mit baramundi
in die Pole Positions*

baramundi software AG
Beim Glaspalast 1
86153 Augsburg

IT einfach clever managen

Fon: +49 (821) 5 67 08 - 380
E-Mail: focustour@baramundi.de
Web: www.baramundi.de/focustour



testen. Nutzer der von Wyse angebotenen X00M-Notebooks haben freilich keine Wahl: Ohne diesen Hotfix schlägt der spätere Systemstart per Preboot Execution Environment (PXE) fehl. Erst nach all diesen Vorbereitungen sollte der WSM-Client selbst installiert werden. Im Anschluss daran rät der Hersteller auch hier wieder zum Aufspielen des Provisioning Patches, diesmal in der Client-Version. Erst damit wäre der Client dann also endgültig aufgesetzt.

Betriebssystemimage ziehen und ausliefern

Laufen Server und Client, können sich Administratoren an das Erstellen eines Betriebssystem-Images machen, das künftig auf die Clients verteilt werden soll. Zu diesem Zweck findet sich auf dem Referenzgerät ein eigenes Tool namens "WSM VDisk Image Creation Utility". Ein Link auf die Anwendung ist nicht zu finden; stattdessen müssen sich IT-Verantwortliche händisch zum entsprechenden Verzeichnis durchhangeln. Standardmäßig liegt das Tool unter dem Namen "OSMVDiskImage" im Pfad "C:\Programme\Wyse\WSM\os". Einmal gestartet, gibt sich das Werkzeug allerdings recht pflegeleicht. Als Pflichteingabe erwartet das Programm lediglich einen Namen für das zu erstellende Image; eine Beschreibung ist optional, ein Vorschlag für die Größe des virtuellen Festplattenabbildes bereits vorgegeben. Je nach Anforderung sind noch die Active Directory-Integration und erweiterte Optimierungen zu aktivieren. In unseren Tests dauerte das Erstellen eines zirka 23 GByte großen vir-

tuellen Images von einem nahezu frischen Windows 7 etwa eine Stunde. Das hierfür verwendete GBit-Ethernet wurde dabei kaum beansprucht.

Um das Betriebssystem an Clients auszuliefern, muss das OS-Image zunächst einmal im Wyse WSM eingefügt werden. Die Browseroberfläche stellt hierfür einen Schritt-für-Schritt-Assistenten bereit, ganz ohne händische Nacharbeit gelang uns das Verknüpfen der Images dennoch nicht. Bevor Geräte oder Gerätegruppen von dem Image booten können, müssen Administratoren das Betriebssystemabbild einer Servergruppe zuweisen. Zudem muss der Partition Mode vom Private Mode "No Cache" auf einen der Shared Modes "Persistent Cache" oder "Volatile Cache" geändert werden.

Cache-Modi und Verbindungstypen

Um zu verstehen, wie die mobilen Cloud PCs funktionieren, lohnt sich ein näherer Blick auf Verbindungstypen und Partition Modes. Per Verbindungstyp (Connection Type) legen Administratoren für einzelne Geräte oder Gerätegruppen fest, woher das Betriebssystem bezogen werden soll. Wird "Network" gewählt, lädt der Client sein Image bei jedem Bootvorgang per PXE direkt vom Server. Wird dagegen die Option "Mobile Disconnected" genutzt, kann der Client auch ohne Netz booten und arbeiten. In diesem Modus läuft lediglich der allererste Bootvorgang noch über das Netzwerk. Im Anschluss gelangt das Betriebssystem-Image dann aber auf

die lokale SSD des Clients. Darüber wird der Endanwender per Warnmeldung informiert und gebeten, das System während dieser Zeit nicht zu nutzen. In unseren Testläufen dauerte das Überspielen des Betriebssystems auf die Platte eine gute halbe Stunde. Danach kann das System auch im mobilen Modus genutzt werden.

Zu den Cache-Modi: Der erste, Private Mode genannte, Partition Mode dient im Wesentlichen zur Feinabstimmung des Images. Administratoren erhalten dabei den kompletten schreibenden Zugriff auf das System. Im Private Mode kann dementsprechend nur das Referenzgerät auf das Abbild zugreifen; normale Clients brechen den Bootvorgang ab und informieren Anwender per Fehlermeldung über aktuell durchgeführte Wartungsarbeiten.

In den beiden Shared Modi erhalten hingegen mehrere Rechner Zugriff auf die vom Server ausgelieferten Betriebssystemdateien. Die originalen Daten werden dabei nicht überschrieben. Anpassungen der einzelnen Nutzer werden in separat angelegten Caches abgelegt. Der Unterschied zwischen den beiden Modi: Während Änderungen beim Persistent Cache auch nach einem Reboot erhalten bleiben, wird der Volatile Cache bei jedem Systemstart zurückgesetzt. Damit eignet sich Letztgenannter beispielsweise für Kioskanwendungen.

Hakeliger Datenaustausch

Sollen Daten auf den Notebooks abgelegt werden, wäre ein Volatile Cache damit aber die denkbar schlechteste Einstellung, denn vom Nutzer erstellte Dokumente würden einen Systemstart nicht überleben. Doch auch der Persistent Cache scheint nur bedingt für solch ein Szenario geeignet zu sein. Spätestens mit dem Ausrollen eines neuen Betriebssystems sind nämlich auch hier die Daten in Gefahr – selbst dann, wenn Administratoren das Rollout nicht erzwingen, sondern dem Endanwender freie Wahl für den Zeitpunkt hierfür lassen.

Um Daten sicher zu speichern, könnte eine zusätzliche Partition dienen. Wahlweise können Anwender auch mit Netzwerkverzeichnissen arbeiten. Der mit der Bezeichnung Cloud PC einhergehende



Bild 3: Direkt aus der Tüte ans Netz: Wenn Wyse WSM die MAC-Adresse eines Clients kennt und der Administrator das System konfiguriert hat, lädt das Notebook beim ersten Start automatisch per PXE sein Betriebssystem

Nimbus erhält damit aus Endanwendersicht einige Kratzer. Die mobilen Rechner gleichen sich eben nicht automatisch mit einer Cloud ab und speichern Daten an einer zentralen Stelle, auf die Nutzer auch noch mit anderen Geräten zugreifen könnten. Stattdessen handelt es sich bei der Wyse-Lösung eher um eine Einbahnstraße zur Auslieferung eines gestreamten Betriebssystems.

Insbesondere beim "Mobile Connected Mode" haben wir unsere Clients hin und wieder "verloren", soll heißen: In unserer Rolle als Admin konnten wir keine Befehle an das Gerät senden, das Aktualisieren von OS-Images scheiterte häufig. Bei aller Selbstkritik suchen wir hierbei die Schuld insbesondere bei der überfrachteten und im Detail oft unübersichtlichen Managementlösung Wyse WSM. Trotz ausführlicher PDF-Dokumentation wurden wir mit dem Werkzeug nicht wirklich warm. Administratoren, die das Tool sicher und in Produktivumgebungen einsetzen möchten, prognostizieren wir einen nicht unerheblichen Lernaufwand.

Fazit

Mit dem wohlklingenden Namen Cloud PC weckt Wyse zahlreiche Assoziationen, die die Lösung nicht alle erfüllen kann. Was unter dem Namen Cloud PC verkauft wird, ist zunächst einmal eine von Thin Clients abgeleitete Managementlösung. Mit dieser können Administratoren Betriebssysteme und Applikationen in großer Zahl ausliefern, verwalten und pflegen. Mit X00M-Clients gibt es zusätzlich noch einen Mehrwert für mobile Mitarbeiter.

Für die Geräte spricht außerdem die PC-nahe Hardware: Anwender können mit einem Cloud PC nahezu das Gleiche anstellen wie mit einem "richtigen" PC; insbesondere fällt darunter auch der Anschluss zeitkritischer Peripherie wie Webcams. Definitiv nachbessern sollte Wyse bei der Implementierung und Bedienung der Lösung. Wir halten es für wenig gelungen, dass einzelne Installationsroutinen ausschließlich auf der US-Version eines Betriebssystems laufen und Anwender ihre Systeme händisch mit Patches und Hotfixes versorgen müssen, damit Wyse WSM überhaupt läuft.

Die "private Verwaltungswolke" ist schließlich nicht zu verwechseln mit einer Datencloud. Um die sichere Dateiablage kümmert sich die Lösung nämlich überhaupt nicht. Unüberlegt implementiert bringen Konzepte wie der "Volatile Cache" Daten des Endanwenders dagegen in Gefahr. Geeignet sind die portablen Cloud PCs daher vor allem für wechselnde Nutzergruppen, die stets auf ein frisches Betriebssystem zugreifen müssen – nicht umsonst adressiert Wyse auch den Bildungssektor. (dr)



Produkt

Portable Clients und Software zur Verwaltung und Pflege von Betriebssystem- sowie Applikations-Images.

Hersteller

Wyse
www.wyse.de

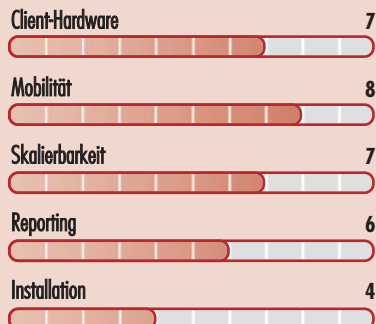
Preis

Eine WSM-Lizenz ist ab 140 Euro erhältlich. Der Wyse-Client X00C mit 160 GByte-Festplatte kostet 613 Euro. Das Modell X00M mit 128 GByte-SDD-Laufwerk gibt es für 859 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für große, wechselnde und mobil arbeitende Anwendergruppen, die auf PC-Anwendungen sowie nativ angebundene Peripherie angewiesen sind.

bedingt als Ersatz für reguläre Notebooks.

nicht für ausgelastete Netzwerkumgebungen oder reine WLANs sowie Szenarien, in denen Applikations-Streaming ohne OS-Streaming eingesetzt werden soll.

Mobile Cloud PCs und Wyse WSM 4.0

Portofrei im Web bestellen [D], [A]

VMware vSphere 5



NEU

- Installation, Konfiguration, Administration
- Sicherheit, Migration, Backup, Lizenzierung, Desktopvirtualisierung
- Storage-Design, Storage-Konfiguration u. v. m.

1.180 S., 2. Auflage 2012, 89,90 €
» www.galileocomputing.de/3000



Linux-Server



Bestseller!

- Linux-Server distributions-unabhängig einrichten und administrieren
- Backup, Sicherheit, Samba, LDAP, Webserver, Mail-server, Datenbanken
- Inklusive sofort einsetzbarer Praxislösungen

815 S., 2011, 49,90 €
» www.galileocomputing.de/2205



Microsoft SharePoint Server 2010 & SharePoint Foundation 2010



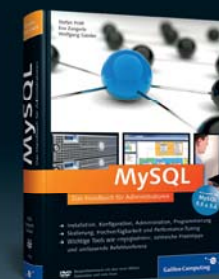
NEU

- Planen, Einrichten und Betreiben von SharePoint
- Business Intelligence, Collaboration, Portale, Informationskonsolidierung
- Entwickeln für SharePoint

1.269 S., 3. Auflage 2012, 59,90 €
» www.galileocomputing.de/2445



MySQL



- Installation, Konfiguration, Administration
- Skalierung, Hochverfügbarkeit und Performance-Tuning
- Wichtige Tools wie »mysqldadmin«, zahlreiche Praxistipps und umfassende Befehlsreferenz

750 S., 2011, mit DVD, 49,90 €
» www.galileocomputing.de/2533



www.GalileoComputing.de

booksonline

» facebook.com/GalileoPressVerlag

» twitter.com/Galileo_Press

» gplus.to/GalileoPress

**Im Test: KAMP Virtual-Core Customer Cloud**

Die ganz private Wolke

von Thomas Bär



Quelle: tele52 – 123RF

Rechenkapazität und Datenspeicher in die Cloud zu verlagern, ist ein Trend, den Administratoren zumindest ernst nehmen sollten. Denn auch wenn der technisch orientierte Nutzer vom IT-Outsourcing nicht begeistert ist – in vielen Szenarien ist Cloud Computing mit der Fähigkeit zur dynamischen Leistungszuordnung und zur Abrechnung nach tatsächlich erbrachter Leistung sehr nützlich. Wem die gängigen Modelle eine Nummer zu groß sind und wer auf die externe Speicherung von Unternehmensdaten lieber verzichtet, dem steht mit dem neuen Cloud-Ansatz von KAMP eine Alternative zur Verfügung. Durch die Trennung von Cloud-Ressourcen und Cloud-Steuerung verbleiben Daten und Hardware-Ressourcen im Unternehmen, während die Steuerung der Private Cloud über eine zentrale Managementplattform als Service erfolgt. IT-Administrator hat sich angesehen, was es mit diesem Modell auf sich hat und ob es im Alltag zu überzeugen weiß.

Geht es um Cloud Computing, so ist der auf Verfügbarkeit und Kontinuität getrimmte IT-Verantwortliche meist sehr vorsichtig. Die Kontrolle über die eigenen Serversysteme komplett aus der Hand zu geben, ist für die meisten Administratoren ein Graus. Als wäre dies nicht alles schon fremdartig und risikobehaftet genug, sollen auch noch die Unternehmensdaten auf irgendwelchen Storages bei dem externen Anbieter gespeichert werden. Spätestens wenn ein Dienstleister dann noch das Backup übernimmt, werden zudem die Datenschützer im Unternehmen hellhörig.

Ein über das Internet erreichbares zentrales Management für die eigenen Serversysteme, gekoppelt mit einer einfachen und gleichzeitig etablierten Virtualisierungsssoftware, die nicht gleich Unmengen an Lizenzkosten verursacht – das klingt für den IT-Profi schon besser und greifbarer. Genau diese Zusammenstellung an Service und Software haben die Entwickler und Produkt-Manager des deutschen Business Services Providers KAMP für eine Art

“Private-Cloud”-Variante umgesetzt. Der Anbieter adressiert mit seiner Lösung weniger große Unternehmen, sondern eher den kleineren Mittelständler und vor allem Dienstleister, die einen sicheren und flexiblen Zugriff auf die Serversysteme beim Kunden benötigen. Dabei kommt nicht die Infrastruktur eines Hosters zum Einsatz, sondern die eigene Hardware oder die Maschinen des Kunden, die von außen betreut werden sollen.

Zwei Ausprägungen von Virtual-Core

Zunächst vertrieb KAMP “Virtual Core” als Hosted Service im firmeneigenen Rechenzentrum. Mit der Neuvorstellung von Virtual-Core Customer Cloud beschreitet der Anbieter nun neue Wege. Der Betrieb der Management-Software erfolgt dabei zentral im Rechenzentrum von KAMP, anstelle der dortigen Hochleistungsserver nutzt der Administrator jedoch die eigene Hardware für die virtuellen Maschinen. Die von KAMP entwickelte Virtual-Core Basissoftware wird hierzu auf den Servern gestartet, diese

verbinden sich mit dem Service von KAMP und der Administrator steuert alle weiteren Schritte über das Internet.

Hinter der Umgebung für Virtual-Core steckt eine größere Anzahl aufeinander abgestimmter Konzepte. Virtual-Core basiert auf der Open Source-Virtualisierung KVM (Kernel-based Virtual Machine). KVM ist eine auf der Linux-Kernel-Infrastruktur aufsetzende Virtualisierung der x64/x86-Umgebung und nutzt hierzu die in der Umgebung integrierten Hardware-Virtualisierungstechniken von Intel (VT) oder AMD (AMD-V). Zwar basiert KAMP Virtual-Core auf KVM als Virtualisierungslösung, es handelt sich jedoch, so versichert der Hersteller auf Anfrage, um eine Eigenentwicklung ohne den Zukauf von Software-Teilen.

Aktuelle x64-Standard-Hardware mit lokalen Festplatten, mindestens 2 GByte RAM und Internetanbindung.

Systemvoraussetzungen



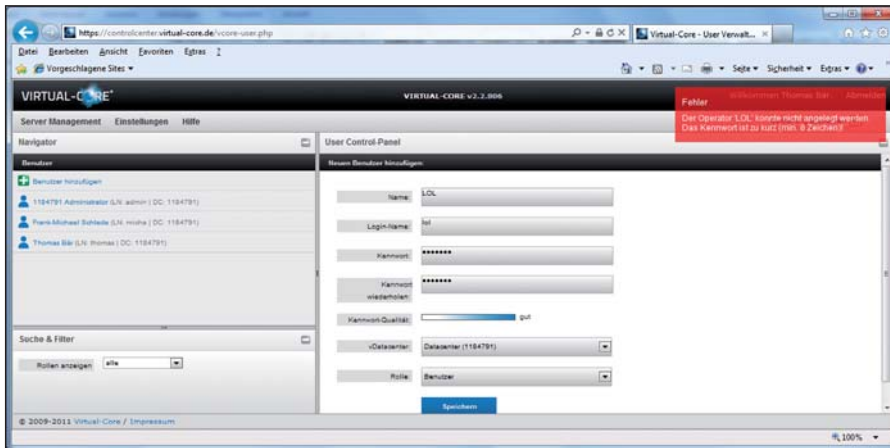


Bild 1: Der Systemverwalter steuert das virtuelle Datacenter und die virtuellen Maschinen mit dem Webinterface von KAMP über das Internet

Einfacher Einstieg

Für den Test nutzten wir den kostenlosen 6-Monats-Zugang, den KAMP für alle Interessenten von Virtual-Core Customer Cloud anbietet. Hierbei handelt es sich nicht um ein Abo oder ähnliches – Zahlungsinformationen muss der Interessent nicht hinterlegen. Endet der Zeitraum, so ist die Software nicht mehr nutzbar. Preislich beginnt das System aktuell bei knapp 13 Euro pro Monat (ein so genannter vRack, die Basis, kostet rund 10 Euro und ein vServer 3 Euro). Die Abrechnung erfolgt monatlich gemäß dem Motto “Pay what you need”. Dieses Modell koppelt den Preis beziehungsweise die Lizenz also nicht an bestimmte Hardware-Merkmale wie CPU oder RAM, sondern an die tatsächliche Nutzung.

Der Anmeldevorgang beginnt auf der KAMP-Webseite mit der Eingabe einiger persönlicher Stammdaten wie Name, Kontakt-Informationen oder Firmenname. Weiter benötigt der Anbieter für die Erstellung des Images für die so genannten Virtual-Core Host Server einige Details zur künftigen Netzwerkumgebung. Hier hat der Administrator die Auswahl zwischen “DHCP” oder “IP-Daten eintragen”. Wählt er die letztere Option, so muss er neben der Netzwerkmaske, dem Gateway und zwei DNS-Servern einen IP-Bereich eingeben. In diesem definierten Bereich sucht sich der spätere Hostserver selbstständig eine freie IP-Adresse. Eine solche Konfiguration ist äußerst praktisch, wenn in der Umgebung kein DHCP-Server eingesetzt werden kann. Die Festlegung einer komplett festen IP-Adresse ist zwar mög-

lich, jedoch wenig sinnvoll. Mit dem Image lassen sich mehrere Hostserver einrichten – da ist eine fixe IP-Adresse auf dem Image eher ein Hindernis denn eine Hilfe.

Gesicherter Zugang

Nach Bestätigung der ersten Web-Maske, gefolgt von der üblichen Kontaktdaten-Bestätigungs-E-Mail, erfolgt der Versand der Zugangsdaten für das virtuelle Datacenter an den Administrator. Der Zugriff auf das Datacenter darf mit Fug und Recht als sicher bezeichnet werden: Das Zufallskennwort ist komplex, zudem ist die Eingabe des Benutzernamens und die Datacenter-Bezeichnung erforderlich. Dass irgendjemand diese drei Daten errät, ist extrem unwahrscheinlich. Nach der ersten Anmeldung steht es dem IT-Profi natürlich frei, eigene Benutzernamen im Menübefehl “Benutzer-Management” anzulegen und mit individuellen Passwörtern zu versehen. Die Benutzeranlage erklärt sich dabei von allein, ein Blick in die Produktdokumentation, die als PDF-Datei zum Download bereitsteht, ist kaum nötig.

Für den eigenen Benutzer möchte der Administrator die maximalen Zugriffsrechte erhalten und wählt folgerichtig den “Datacenter Administrator” im Dropdown-Menü. Weitere Benutzer mit eingeschränkten Zugriffsrechten legten wir in der Teststellung ohne Probleme an. Einzelne User organisiert die Software in Benutzergruppen, denen wiederum Zugriffsrechte auf Server, Datacenter oder nur bestimmte Funktionen gegeben werden. Insgesamt ist die Virtual-Core Customer Cloud eine mandantenfähige Software, was bei der Zielgruppe

durchaus nützlich ist. Betreibt ein IT-Dienstleister das System für mehrere unterschiedliche Kunden, so kann er über die Benutzersteuerung sicherstellen, dass kein unberechtigter Querschnitt möglich ist.

Logbuch ohne Exportfunktion

Die Oberfläche ist insgesamt angenehm in der Bedienung. Dank der verwendeten Ajax-Technologie befindet sich das moderne Design auf der Höhe der Zeit. Während andere Programme oder ältere Systeme den Benutzer immer wieder durch modale Fehlerdialoge ablenken, arbeitet die KAMP-Oberfläche anders. Entsteht bei der Konfiguration ein Fehler, beispielsweise wenn das Passwort eines Benutzers kürzer als acht Zeichen ist, so erscheint der Fehler in einem knallroten Textrahmen am rechten Fensterrand. Weitere Informationen in Textrahmen stellt die Software unterhalb des vorherigen Eintrags dar. Ist das Fenster einmal voll, so verschwindet der jeweils älteste Eintrag. Entweder klickt der Benutzer auf die Meldungen, um diese auszublenden, oder er wartet einige Minuten. Dann verschwinden die Nachrichten ebenfalls.

Alle Hinweiseinträge bleiben zur späteren Betrachtung im Log-Buch erhalten. Dieses kann der Administrator auf der Hauptseite auf bis zu 1.000 Zeilen in der Ansicht vergrößern. Es enthält alle Einträge wie das Anlegen von Benutzern oder das Aufschalten per VNC-Sitzung. Eine Möglichkeit, diese Meldungen per E-Mail zu abonnieren oder in eine CSV-Datei zu exportieren, findet sich aktuell leider nicht. Auf Nachfrage versicherte uns der Hersteller aber, dass daran bereits gearbeitet wird.

Host-Server mittels ISO-Datei schnell erstellt

Mit dem Zugriff auf die Management-Webseite allein ist jedoch noch kein System nutzbar. Das Datacenter ist zwar angelegt, jedoch noch kein Hostserver. Ein Willkommensdialog zeigt die sieben Schritte, die für die Inbetriebnahme der eigenen Hostserver notwendig sind, beim Erststart an. Zunächst muss der Administrator das bereits erwähnte ISO-Image herunterladen. Dies geschieht entweder durch einen Mausklick auf das Symbol oder über den entsprechenden Menübefehl. Die Erzeugung des eigenen Boot-Images und der



Download der ISO-Datei gehen dank der zügigen Anbindung von KAMP an das Internet mit dem Maximaltempo der eigenen DSL-Anbindung vonstatten. Das Image hatte in der Teststellung einen Umfang von knapp 170 MByte.

Im zweiten Schritt gilt es nun, dieses Image entweder auf eine CD/DVD zu brennen oder auf einen bootfähigen USB-Stick zu übertragen. Ein Versuch, das ISO-Image als ESX-Container unter VMware Workstation zum Laufen zu bringen, scheiterte verständlicherweise. KVM benötigt nativen Zugriff auf die Virtualisierungstechnik, was die VMware-Workstation in dieser Form nicht bietet.

Moderate Systemanforderungen

Die Mindestvoraussetzungen für die Hardware erhält der Administrator per PDF-Datei zusammen mit einer Kurzerklärung. Neben der EULA und einigen Zusatzinformationen erhält der IT-Profi zudem die benötigten Einstellungen für die Konfiguration der Firewall, um auf die Management-Server bei KAMP zugreifen zu können. Für den Betrieb von Virtual-Core Customer Cloud wird mindestens eine x64-Maschine von Intel oder AMD mit CPU-seitigem Virtualisierungssupport, 2 GByte RAM, eine Netzwerkkarte und lokale Festplatten (IDE, SATA, SAS) benötigt. Von den mindestens 2 GByte Arbeitsspeicher nimmt sich die Virtual-Core vRack Software 1 GByte, der restliche Arbeitsspeicher steht den virtuellen Maschinen zur

Verfügung. Um Arbeitsspeicher im Bedarfsfall einsparen zu können, verfügt vCore über die Methodik der "Speicherdeduplizierung". Auf einer lokalen Festplatte, möglichst der schnellsten im System, wird hierzu eine virtuelle Festplatte wie ein "Swap"-Drive eingerichtet. Da nicht alle Maschinen dauerhaft unter Vollast laufen, erhöht sich so die Gesamtzahl der gleichzeitig zu betreibenden virtuellen Maschinen. Im Notfall, wenn alle virtuellen Maschinen gleichzeitig mehr Arbeitsspeicher anfordern sollten, ist das "Swapping" eine Art Lebensversicherung für das Gesamtsystem.

Wir nutzten für die Teststellung sowohl einen Standard-PC, der ganz genau den genannten Mindestvoraussetzungen entsprach, als auch einen leistungsfähigeren Server auf Basis einer Intel Sandy Bridge mit Intel Core i3-Prozessor und 8 GByte Hauptspeicher. Gestartet von der Boot-CD, war der Server innerhalb von drei Minuten über das Webinterface erreichbar. Kam anstelle einer Boot-CD ein bootfähiges USB-Device zum Einsatz, lief der Boot-Vorgang noch zügiger ab.

Reibungslose Storage-Anbindung

Ein Blick auf die lokale Konsole des Servers zeigt lediglich die Stamminformationen wie Maschinenlaufzeit, IP-Adresse, Versionsdaten und die Info darüber, ob der Admin-Link ins Rechenzentrum von KAMP aufgebaut ist. Die Konfiguration des Servers erfolgt ausschließlich über das Webinterface und muss daher auf der lokalen Konsole

auch nicht mehr angezeigt werden. Bis zu diesem Zeitpunkt wurde auf den Festplatten des Servers noch kein einziges Bit angelegt – die vCore-Software auf Basis von Ubuntu 10.04.3 LTS arbeitet ausschließlich als Live-System im Arbeitsspeicher.

Im nächsten Schritt, den der Assistent empfiehlt, sollte der Administrator die lokalen Festplatten oder iSCSI-Targets im Dialog "Storage-Devices" einbinden. Wer schon einmal Festplatten in ein System eingebunden hat, sollte bei dieser Aufgabenstellung kein Problem haben. Zunächst werden über diesen Schritt die Festplatten der Software lediglich bekannt gemacht. Erst bei der Definition von virtuellen Maschinen erfolgt die Zuweisung der "virtuellen Festplatten" als Festplatten-Container. Es ist also durchaus möglich, mehrere virtuelle Festplatten auf einer physikalischen Platte anzulegen. Neben den lokalen SATA-Platten im Server verknüpften wir im Test iSCSI-Targets einer FreeNAS-Installation.

Virtuelle Maschinen ohne große Extras

Offiziell unterstützt die Software die Betriebssysteme Windows XP SP3 oder 7 in 32 Bit, Windows Server 2003/2008 x86/x64, Ubuntu Desktop/Server in den Versionen LTS 8.04 32 Bit, 9.04 64 Bit, 9.10 64 Bit und LTS 10.04 64 Bit als virtuelle Betriebssysteme. Weiter stehen openSuse 11.2 64 Bit und 11.3 als 64 Bit- und 11.3 als 32 Bit-Variante auf der Liste. Suse Linux Enterprise 9/10 und OpenSolaris 2009/06 in den 64 Bit-Versionen und FreeBSD 8.1, OpenBSD 4.7 und Knoppix 6.2, jeweils in der 32 Bit-Ausprägung, stehen ebenfalls zur Verfügung. Andere Betriebssysteme können durch das Setzen der Option "Failsave" möglicherweise betrieben werden. Im Test richteten wir Ubuntu, Windows XP und Server 2003 ohne Probleme ein. Der administrative Zugriff auf die zu installierenden Server geschieht über einen integrierten VNC-Server.

Um eine virtuelle Maschine installieren zu können, muss das Installations-Medium zur Verfügung stehen. Hierzu gibt es bei der Customer-Cloud verschiedene Möglichkeiten. Entweder wird das Medium über das lokale CD/DVD-Laufwerk am physi-

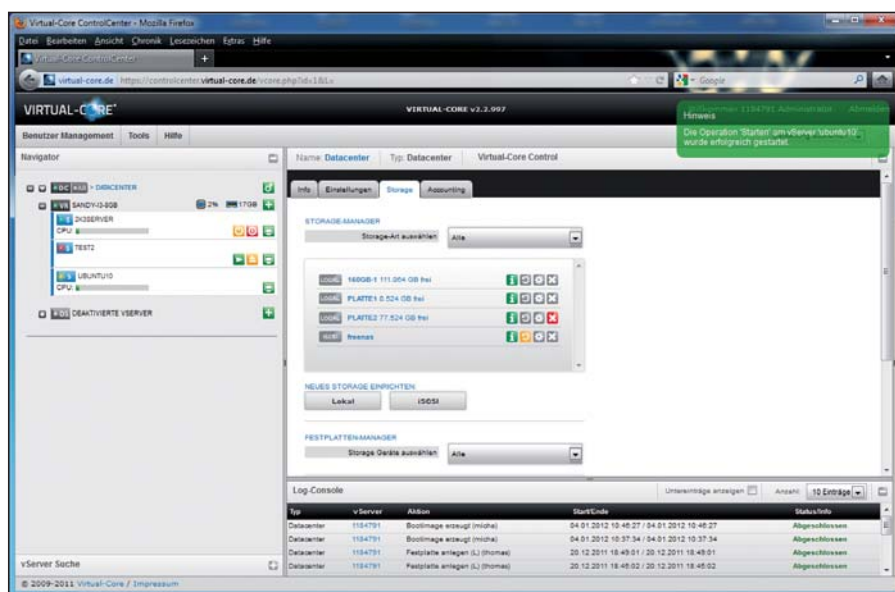


Bild 2: Neben lokalen Festplatten unterstützt die Virtual-Core Customer Cloud auch iSCSI-Targets

Your knowledge.
Your people.
Your future.



Optimiertes Load Balancing?



HOB RD Selector

Parametrisiert - Individuell - Effektiv

Entdecken Sie die neue, innovative Load Balancing Lösung von HOB!



Secure Business Connectivity

www.hob.de

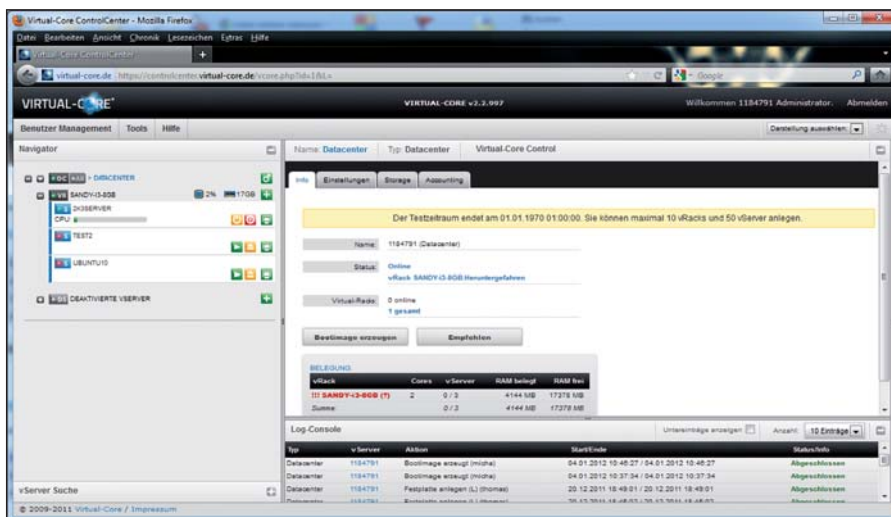


Bild 3: Virtuelle Maschinen in der Virtual-Core Customer Cloud lassen sich in ControlCenter verwalten

kalischen Server angesprochen, per NFS-Share aus dem lokalen Netzwerk zugegriffen oder über einen FTP-Zugriff auf den Server hochgeladen. Alternativ startet eine Installation aber auch bequem per PXE oder per Netboot. Die Boot-CD des vCore-Servers kann übrigens für eine Installation vom lokalen CD/DVD-Laufwerk problemlos entnommen werden.

Wie bei den anderen Virtualisierungslösungen entscheidet der Administrator beim Anlegen der virtuellen Maschine, wie viele Cores, wie viel Arbeitsspeicher, Netzwerkkarten oder Festplatten dieser zur Verfügung gestellt werden sollen. Bezüglich der Performance überzeugt KVM als Virtualisierungs-Hypervisor – wir konnten keinen spürbaren Unterschied zu anderen Hypervisoren feststellen. Wie es um die Auslastung der Server steht, zeigen die noch rudimentären Auswertungen für CPU- und Netzwerkauslastung an. Wer hier die Detailtiefe von VMware ESX erwartet, wird enttäuscht sein – auf dieses Niveau kommen die Reports nicht.

Basierend auf den VMX/VMDK-Formaten von VMware besteht zudem die Möglichkeit, die virtuellen Maschinen als VMX- oder VMDK-Dateien zu importieren. Die VMX-Datei beschreibt die Konfiguration der "Virtual Appliance" wie beispielsweise Name, Anzahl der CPUs oder RAM. Die VMDK-Datei enthält die Daten der virtuellen Maschine. Die Virtual-Core Export-Funktion im Reiter "Funktionen" ist das entsprechende Gegenstück. Ein Export ist nur bei ausgeschaltetem vServer möglich

und die Dauer des Vorgangs vom Datenvolumen abhängig. Der Fortschritt des Exports wird in der Session-History und der Log-Console angezeigt. Nach abgeschlossenem Export ist ein neues Element im Reiter "Funktionen" sichtbar: "Download von generierten VMDK-Images".

Fazit

Im Vergleich zur großen Konkurrenz von Citrix, Microsoft oder VMware ist die Virtual-Core Customer Cloud noch nicht ganz so ausgereift. Eine größere Anzahl von Funktionen steht noch auf der diesjährigen Produkt-Roadmap. Einstellungsmöglichkeiten für SNMP oder automatischen E-Mailversand beim Ausfall von Systemen oder Verlassen von zuvor definierten Rahmenparametern sucht der Administrator noch vergeblich. Künftig wird es, zumindest im Zusammenspiel mit iSCSI-Storage, die Möglichkeit geben, zwischen zwei vServern virtuelle Maschinen in einem vRack zu verschieben, um beispielsweise eine Hardware für Wartungsarbeiten komplett freizubekommen. Bei Verwendung von lokalen Festplatten würde dieses Feature keinen Sinn machen – niemand möchte eine 50 GByte umfassende Maschine über einen 100 MBit-Switch von einem zum anderen Server verschieben müssen.

Ebenfalls schmerzhaft vermisst der von klassischen Hypervisoren kommende Administrator die Möglichkeit, Snapshots anzulegen. Technisch betrachtet ist dies für den Anbieter auch schwierig umzusetzen, da Virtual-Core Raw-Devices auf den Storage nutzt. Raw-Devices arbeiten direkt

auf der Hardware und sind entsprechend schnell im Einsatz, jedoch ist der Snapshot-Support somit von den Fähigkeiten des Storage-Systems abhängig.

Insgesamt ist die Software ein spannendes und zukunftsweisendes Angebot. Eine leistungsfähige, einfach zu bedienende Virtualisierungssoftware gepaart mit einer zentral über das Internet zu erreichenden Management-Oberfläche sind in Zeiten stabiler DSL-Verbindungen und mobiler Endgeräte mit Browsern ein äußerst nützliches Produkt. Besonders erfreut sein werden Administratoren und IT-Profis, die mehrere kleine Unternehmen zu betreuen haben. (In)

Produkt

Plattform zum externen Management von IT-Umgebungen mit Funktionen zur Server-Virtualisierung.

Hersteller

KAMP Netzwerkdienste
www.kamp.de

Preis

Ein V-Rack, die Grundbasis für Virtual-Core, ist für 9,99 Euro pro Monat verfügbar. Jeder V-Server, der in das V-Rack eingebunden wird, schlägt mit 2,99 Euro pro Monat zu Buche.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Virtualisierung	8
Erreichbarkeit	8
Speicherausnutzung	8
VM-Kompatibilität	7
Logging-Funktionen	5

Dieses Produkt eignet sich

optimal für Dienstleister, die für verschiedene Kunden an verschiedenen Standorten Serversysteme betreiben wollen.

bedingt Unternehmen, die ihr Know-how bereits in andere Virtualisierungstechniken investiert haben.

nicht für Unternehmen, die über keine stabile Internetanbindung verfügen.

KAMP Virtual-Core Customer Cloud



Im Test: NComputing L300 und vSpace

Das Büro in der Box

von Thomas Bär



Was auf den ersten Blick aussieht wie ein ganz gewöhnlicher, recht formschöner Thin Client, ist auf den zweiten Blick ein interessantes Zusammenspiel von Hard- und Software. Denn ohne die vSpace Desktop Virtualization Software, die jedem NComputing-Endgerät beiliegt, ist das Zugriffsgerät nutzlos. Gemeinsam aber sind sie eine äußerst interessante, leistungsfähige und gleichzeitig kostengünstige Mischung aus Computer, virtuellem Desktop und Terminalserver. In unserem Test haben wir sowohl das Zugriffsgerät als auch die Management-Software unter die Lupe genommen und dabei festgestellt, dass lizenzrechtliche Einschränkungen seitens Microsoft die Freude an der Mini-VDI etwas trüben.

Die Arbeitsumgebung eines Anwenders effektiv und kostengünstig bereitzustellen, ist nicht erst seit der "Erfindung" der Virtual Desktop Infrastructure (VDI) eine der wichtigsten Aufgaben der IT-Administration. Trotz vieler Vorteile bei der Verarbeitung auf dem eigenen PC kehrte sich der Trend nun wieder um. Besonders in größeren Unternehmen wird die Terminalservertechnik, bei der alle wichtigen Komponenten zentral im Serverraum durch die IT betrieben werden, sehr gern und erfolgreich eingesetzt. Gewöhnlich verwenden Firmen dazu Microsofts Terminalserver oder die entsprechenden Produkte von Citrix, um Windows-Desktops für die Anwender bereitzustellen. Allen Umsetzungen ist gemein, dass sie sich weniger gut für den Einsatz in kleineren Umgebungen eignen.

Perfekte Lösung für den Einsatz in kleinen Unternehmen

Dass es auch ganz anders geht, beweist das aus Kalifornien stammende Unternehmen NComputing. Mit der Software "vSpace Desktop Virtualization" wird selbst ein betagter Standard-PC mit Windows XP zum Terminalserver für bis zu zehn gleichzeitige Benutzer-Sitzungen. An denkbaren Einsatzszenarien neben dem Ersatz für den klassischen PC im Büro mangelt es einer solchen Lösung nicht – in Frage kommen etwa Schulungs- und

Trainingsräume oder Kiosk-, Anzeige- sowie Info-Terminals. NComputing liefert nicht nur die Software, sondern die dazu passenden Client-Zugriffsgeräte gleich mit. Dieses Zusammenspiel wird vom Hersteller passenderweise als "Office in a Box" bezeichnet.

Die speziellen Zugriffsgeräte, um sie nicht einfach Thin Clients zu nennen, verwenden nicht etwa die üblichen Protokolle wie HDX/ICA von Citrix oder RDP von Microsoft, sondern setzen auf dem UXP (User eXtension Protocol) von NComputing auf. UXP überträgt wie die anderen Remote Desktop Protokolle alle Bildschirm-, Sound- und Schnittstelleninformationen über das Netzwerk. Es gibt am Markt durchaus Hersteller, die ihre Geräte über das gewöhnliche Ethernet-Kabel verbinden, ohne jedoch Standard-Ethernet als Protokoll zu verwenden. Bei NComputing ist dies nicht der Fall – die Zugriffsgeräte werden wie gewöhnliche PCs am Hausnetz betrieben.

Zugriffsgeräte je nach Bedarf

Für das Zusammenspiel mit der vSpace-Desktop-Virtualisierungssoftware bietet der Hersteller drei unterschiedliche Ausbaustufen der nur einige Zentimeter großen Zugriffsgeräte in der so genannten L-Serie an. Der Monitor findet dabei stets über den analogen, traditionellen VGA-

Port mit den 15 Polen Anschluss. In den aus stabilen, schwarzen Kunststoff gearbeiteten Geräten befinden sich keinerlei bewegte Teile, sie sind somit komplett geräuschfrei. Die Stromversorgung übernimmt ein externes Netzteil mit angenehmem langem Anschlusskabel. Der Stromverbrauch liegt laut Herstellerangaben und unseren Messungen bei knapp 5 Watt pro Gerät, sofern keine externen USB-Geräte angeschlossen sind.

Die maximal unterstützte Farbtiefe ist beim kleinsten Gerät, dem L130, auf 16 Bit limitiert, die anderen Geräte arbeiten mit bis zu 24 Bit. Die Standard-Bildschirmauflösung liegt bei 1280x1024 Pixeln, das L300 erreicht maximal 1920x1080 Pixel. Während alle Geräte über den Standard 3,5mm Sound-Anschluss verfügen, sind nur die größeren Varianten mit einem Mikrofon-Anschluss ausgestattet. Die Geräte L130 und L230 verwenden PS/2-An-

Die Hardware-Anforderung für den Server variiert abhängig von der Anzahl gleichzeitiger Benutzer. Als Betriebssystem kommt Windows XP ab SP3 in Frage. Der Betrieb im Zusammenspiel mit Windows Vista/7 ist lizenzrechtlich nicht zulässig. Für das Bildungsumfeld empfiehlt sich die Kombination mit Windows MultiPoint Server 2011.

Systemvoraussetzungen



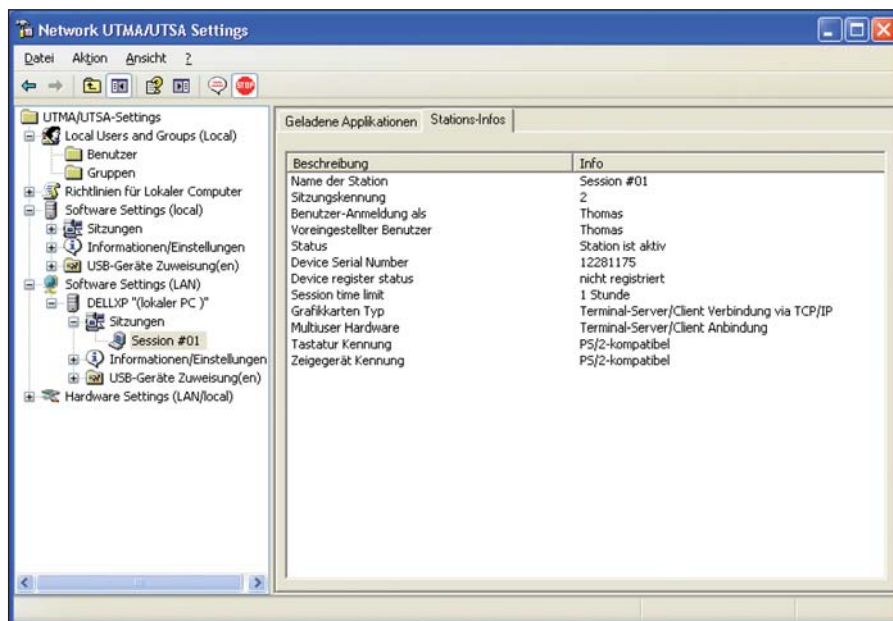


Bild 1: Die Management-Software für die NComputing-Lösung unterscheidet sich zwischen der XP/2003- und der 7/2008-Version

schlüsse für Maus und Tastatur, das größere Schwestermodell, Typ L300, verbindet die Eingabegeräte über USB 1.1. Lediglich mit einer USB-Apple-Tastatur wusste das Testgerät nichts anzufangen, mit anderen Keyboards kam das Zugriffsgerät gut klar.

Multimedia-Einsatz durch Streaming

Der Hauptvorteil des hier getesteten L300-Zugriffsystems liegt in der beschleunigten Darstellung von Multimedia-Inhalten, wie beispielsweise in Webseiten integrierte Videos oder bildschirmfüllende Filme. Diese Inhalte werden vom L300 fast so schnell dargestellt wie auf einem normalen PC. Für die ruckelfreie Darstellung sorgt bei NComputing ein spezieller Chip, der Numo system-on-chip (SOC). Das Geheimnis hinter dieser Beschleunigung ist an sich das Zusammenspiel der vSpace-Software auf dem Hostsystem und dem Chip im Zugriffsgerät. Videoinhalte, wie beispielsweise AVI- oder WMV-Dateien, transkodiert die vSpace-Engine und schickt diese als komprimierten Stream direkt an das Zugriffsgerät. Aus dem Protokoll entschlüsselt der Chip die komprimierten Daten und stellt diese in der vom Anwender oder der Applikation geforderten Größe dar.

Die Hardware-Voraussetzungen auf Seiten des Servers hängen sehr stark vom geplanten Einsatzfeld ab. Um zirka acht bis zehn L300-Zugriffssysteme mit Standard-Bü-

roprogrammen zu versorgen, empfiehlt der Hersteller die Leistungsklasse einer Core2-Maschine mit 3 GByte Hauptspeicher. Um jedoch Multimediainhalte auf derselben Anzahl von Clientsystemen darzustellen, steigt die Leistungsanforderung auf eine Core i7-Maschine.

NComputing vSpace funktioniert auch auf virtuellen Server- oder PC-Systemen,

sofern in der Virtualisierung die erforderliche Rechenleistung geboten wird. Wir haben die Software unter Windows XP Professional SP3 x86, Windows Server 2003 x86, Windows 7 Enterprise x64 und Windows Server 2008 R2 x64 getestet. Faktisch arbeitet vSpace mit allen gängigen Windows-Varianten und mit Ubuntu Linux 8.04 LTS/8.10 und höher zusammen.

Schnelle Installation

Der Aufbau unserer Testumgebung dauerte nicht einmal eine halbe Stunde. Auf einem Windows-Computer oder -Server installierten wir die vSpace Desktop Virtualization Software von der beigelegten CD und fügten die gewünschten Benutzer, seien es nun lokale Benutzer des Computers oder Benutzergruppen aus dem Active Directory, in die Gruppe der "Remotedesktopbenutzer" ein. Ein Neustart des Rechners nach der eigentlichen Installation ist zwingend erforderlich, da ansonsten keine Verbindung zustande kommt.

An das Zugriffsgerät schließt der Benutzer Maus-, Tastatur-, Netzwerk- und Monitor-Kabel an und schaltet das Gerät über den Kippschalter ein. Dank eines speziellen Anbaurahmens ist es möglich, das L300-Gerät auf die Monitorrückseite anzuschrau-

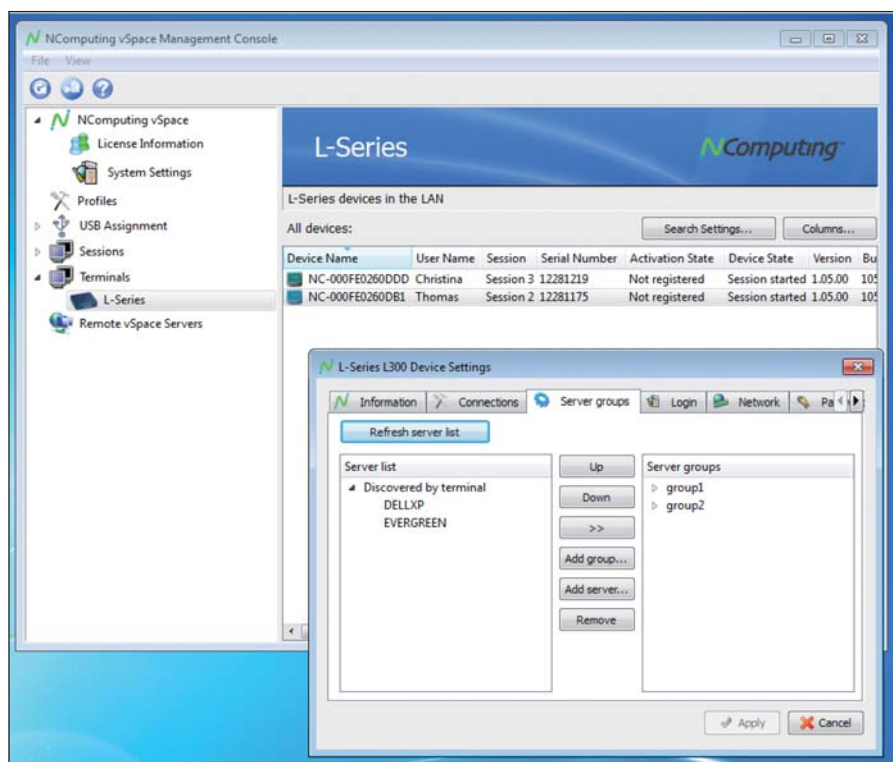


Bild 2: Welche Zugriffsgeräte welche Windows-Hosts nutzen dürfen, steuert der Administrator zentral über die Management-Software

CLEVER KOMBINIERT!

Premium Server + Symantec™ SSL -Zertifikat

Leistungsstark! Sicher! Günstig!

Jetzt 4 Wochen unverbindlich testen!

Inkl. Symantec™ Secure Site SSL-Zertifikat!



Nur bei InterNetX GRATIS!

VIRTUAL DEDICATED SERVER

- » 4 GB RAM
- » 100 GB Speicherplatz
- » Root-Zugriff
- » Parallels® Plesk
- » Hostingsystem von Dell®

Regulär: ~~49,-~~

39,-
EUR / Monat*

DEDICATED SERVER



- » Intel® Xeon® E3-1260L
- » 4 Cores mit je 2,4 GHz
- » 8 GB RAM
- » 2 x 600 GB SAS HDD
- » Dell® PowerEdge R210 II

Regulär: ~~129,-~~

79,-
EUR / Monat*

» Symantec™ SSL Secure Site

- » Malware Scan
- » Trust Seal
- » Seal-in-Search™
- » Bis 256-Bit-Verschlüsselung
- » Domain-, Server- & SSL - Management-Tools

Regulär: ~~299,-~~

Zu jedem Server
0,-
einmalig*

➤ Klickrate in Suchmaschinen maximieren



Durch Seal-in-Search™ wird in Suchmaschinen-Einträgen Trust Seal angezeigt.

➤ Mehr Bestellungen, mehr Kundenanfragen



Zeigen Sie Ihren Kunden, dass Ihr Unternehmen durch Trust Seal verifiziert ist.

➤ Security Scan Ihres Servers

Präventivschutz! Prüfen Sie Ihren Server mit Vulnerability Assessment* auf Schwachstellen.

➤ Vertrauenswürdige Webseite

Der Malware Scan garantiert Ihren Kunden eine sichere Website – frei von Schad-Software.

Jetzt informieren
und bestellen:

www.internetx.com
+49 (0) 941 / 59 559-483



InterNetX

*Alle Preise richten sich nur an Gewerbetreibende und verstehen sich zzgl. gesetzlicher MwSt. Bei allen Angeboten sind das Symantec™ Secure Site SSL-Zertifikat für 12 Monate gratis und 500 GB Traffic/Monat inklusive. Je nach Nutzung fallen weitere Traffic-Gebühren ab 0,29 €/GB an. Der Testzeitraum beträgt 28 Kalendertage nach Bereitstellung und ist begrenzt auf einen Test pro Kunden. Vulnerability Assessment ist erhältlich ab Symantec™ Secure Site Pro. **Virtual Dedicated Server:** 39,- €/Monat. Mindestvertragslaufzeit 12 Monate. Keine Einrichtungsgebühr. **Dedicated Server:** 79,- €/Monat. Mindestvertragslaufzeit 24 Monate. Einmalige Einrichtungsgebühr 79,- €. Nur solange der Vorrat reicht. Die Abbildung des Servers ist symbolisch.



ben, was dem ansonsten entstehenden Kabelsalat entgegenwirkt. Ist ein DHCP-Server aktiv, sind keine weiteren Konfigurationsschritte erforderlich. Das Modell L300 benötigt zirka eine Minute, bis es einsatzbereit ist, und findet die vSpace-Software im Netzwerk automatisch. Ein Doppelklick auf den Computernamen der vSpace-Installation, und schon ist der Anmeldebildschirm von Windows sichtbar und nutzbar. Welche Computer ihre Sessions einem Zugriffsgerät anbieten, kann der Administrator über die Konsolen-Software zu einem späteren Zeitpunkt exakt festlegen. Auch ein direktes Aufschalten ohne die zusätzliche Eingabe von Benutzerinformationen ist im Konzept von NComputing realisierbar.

Geringe Netzwerkbelastung

In allen Tests arbeiteten die L300-Geräte und die vSpace-Software problemlos und ohne besondere Vorkommnisse. Nach wenigen Minuten vergisst der IT-Profi bereits, dass es sich nicht um Standard-Terminalserver-Verbindungen handelt, sondern um mehrfach genutzte Windows-Desktops, selbst wenn darauf Client-Betriebssysteme laufen. Windows XP und 7 verhalten sich wie kleine Terminalserver und nur ein Blick in die Lizenzbestimmungen trübt diese Freude – mehr dazu weiter unten.

Die vom Hersteller versprochene zügige Darstellung von Multimedia-Inhalten mit dem L300-Zugriffsgerät wurde im Test in einem 100 MBit-Ethernet als beinahe ruckelfrei bestätigt. Lediglich bei der Verwendung der Pause-Funktion im Media-Player kommt es bei Darstellung von MPEG-Filmen zu einem oder zwei fehlerhaften Bildern. Das erweist sich jedoch nicht als störend. Die Netzwerkauslastung liegt bei der Darstellung eines Films bei gerade einmal zwei Prozent. Wird die Netzwerkanbindung bewusst auf die Geschwindigkeit 10 MBit/s reduziert, so kommt es zu sporadischen Aussetzern beim Abspielen des Videos. Typische Office-Anwendungen arbeiten jedoch auch bei 10 MBit/s im halben Duplex noch ausreichend schnell. Im Betrieb ermittelten wir ein seltsames Verhalten: Beim Test der Systemauslastung bei der Darstellung von Multimedia-Inhalten fiel uns die hohe Auslastung der AMD Opteron Prozessoren des Testrechners auf. Die CPU-Last von über 50% wurde jedoch

nicht vom Multimedia-Streaming produziert, sondern von der gleichzeitig geöffneten NComputing-Console.

Selbsterklärende Admin-Konsole

Die schnelle und unkomplizierte Bereitstellung ist natürlich beeindruckend, doch wie steht es um die administrativen Einstellungsmerkmale der Software? Je nachdem, ob das Programm auf einem Windows XP/2003 oder unter Windows 7/2008 installiert ist, so unterscheidet sich die Management-Darstellung voneinander. Auf modernen Windows-Systemen wird die "NComputing vSpace Management Console" installiert, auf den Vorgängern die MMC-Konsole "Network UTMA/UTSA". Unabhängig von der installierten Variante sind die Einstellungsmöglichkeiten äußerst umfangreich, ohne den Administrator dabei mit zu vielen Details zu erschlagen.

Das Menü der Konsole besteht aus wenigen Punkten, von denen einer auf die lokalen Windows/Benutzer-Einstellungen des Host-Systems verweist. Über die "Allgemeinen Einstellungen" legt der Administrator beispielsweise fest, ob das Hintergrundbild von Windows angezeigt wird, welche Standardkompression für JPEG in der Sitzung Verwendung findet oder wie viele gleichzeitige Sitzungen auf einem PC/Server zulässig sind. USB-Geräte können, sofern entsprechend aktiviert, über das Zugriffsgerät direkt in die Sitzung weitergeleitet werden – was insbesondere den Einsatz von Speichergeräten vereinfacht. Im Test wurden am L300 angesteckte USB-Devices problemlos in die Session des Benutzers gemappt. Am PC direkt angebrachte USB-Geräte finden Benutzer ebenfalls in ihren Sessions.

Im Menüpunkt "Sitzungen" zeigt die Software alle aktuellen Benutzersitzungen auf dem Server an. Wie von der Micro-soft-Terminalverwaltung bekannt, ist es dem IT-Support möglich, einem Benutzer über das "Spiegeln des Desktops" bei Problemen zu helfen und Kurzmeldungen in die Sitzungen zu senden. Besonders im Kiosk-Betrieb äußerst hilfreich ist die Funktion der automatischen Anmeldung. Schließt ein Benutzer die Sitzung über "Herunterfahren – Abmel-

den", so baut das Zugriffsgerät bei dieser Einstellung sofort eine neue Sitzung auf. Unterschiedliche Konfigurationen organisiert der Administrator mit der Software in Gruppen, denen Geräte und Hosts zugeordnet werden.

Für den Zugriff auf die Management-Oberfläche ist grundsätzlich ein administrativ berechtigter Nutzer erforderlich. Darüber hinaus erlaubt die Software dem Administrator das Festlegen eines zusätzlichen Konsolen-Kennworts. Ob ein Zugriff von einer Konsole auf eine andere Hardware möglich ist oder nicht und ob diese durch ein Passwort vor unerwünschten Zugriffen geschützt ist, legt der Administrator mit wenigen Mausklicks fest.

Produkt

Komplettpaket zum Aufbau einer Terminalserver-Infrastruktur für kleine Umgebungen.

Hersteller

NComputing
www.ncomputing.com

Preis

Der Marktpreis variiert je nach Gerätetyp. Aktuell liegt der Preis für ein L300-Zugriffsgerät inklusive vSpace-Software im Versandhandel bei rund 150 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Konfiguration	8
Administration	7
Bereitstellungstempo	9
Multimedia-Funktionalität	8
Lizenzanforderung	6

Dieses Produkt eignet sich

optimal für Schulungs- und Bildungseinrichtungen.

bedingt für Firmen, die eine Alternative zur Terminalservertechnik suchen.

nicht für Unternehmen, in denen moderne physikalische PCs bereits ausgelastet sind.

NComputing L300 und vSpace



Die MMC-Konsole für die XP/2003-Systeme bietet leider nicht den üblichen Befehl "mit anderem Server verbinden" im Menü "Aktion", um die Konfiguration eines anderen Hosts zu bearbeiten. Die Parametrierung der Zugriffsgeräte ist jedoch glücklicherweise von jeder Konsole zentral möglich, was die Verteilung beispielsweise von Firmware-Updates deutlich vereinfacht.

Hemmschwelle Lizenzierung

Die Desktop-Bereitstellung mit NComputings vSpace-Software ist ohne Frage beeindruckend und birgt die Chance, Kosten zu reduzieren und die Anforderungen an die technische Umgebung zu senken. Nicht nur in kleineren Szenarien, wie beispielsweise Schulungsräumen oder temporär genutzten Arbeitsplätzen, machen Soft- und Hardware ein gutes Bild. Haupteinsatzgebiet der Lösung ist jedoch nach Aussagen des Herstellers der Betrieb im Schul- und Ausbildungsumfeld.

Es stellt sich die Frage, welches Microsoft Betriebssystem für die Mehrbenut-

zer-Datenverarbeitung mit NComputing-Produkten zugelassen ist. Es versteht sich beinahe von selbst, dass es sich hierbei um die Server-Varianten von Microsoft Windows handelt. Um mit NComputing-Produkten arbeiten zu können, ist der Erwerb einer Lizenz für Windows Server 2003 R2 oder Server 2008 und höher erforderlich. Besonders gut eignet sich im Zusammenspiel der neue MultiPoint Server 2011.

Und wie sieht es mit Windows XP aus anstelle einer Server-Variante? Dies ist, laut Informationen von NComputing auf der Webseite, nur in einigen wenigen Fällen gestattet. Sofern der Kunde eine entsprechende Anzahl an Windows Server-Betriebssystemen lizenziert hat und über die dazugehörigen Client-Zugangslizenzen für den gleichzeitigen Zugriff mehrerer Benutzer auf die lizenzierten Computer verfügt, so kann er die Software auf einem separat lizenzierten Windows XP anstatt des Windows Server Betriebssystems installieren und ausführen.

Die gleichzeitige Benutzung der Server- und Client-Systeme ist nicht zulässig. Die beschränkt zulässige Nutzung wird jedoch nicht vom Microsoft-Support unterstützt. Bei Fragestellungen ist der Kunde auf NComputing angewiesen. Die moderneren Varianten des Client-Betriebssystems Windows, 7 oder Vista, sind für den Betrieb mit NComputing überhaupt nicht zugelassen. Funktioniert hat es im Test jedoch ohne Probleme. Offiziell und lizenzt wurde aber nur Windows Server von Microsoft für mehrere gleichzeitige Benutzer entwickelt und ist dementsprechend lizenzierbar.

Fazit

NComputing vSpace stellt in Verbindung mit dem Zugriffsgerät L300 eine praktische Variante einer Terminal-Services-Lösung mit einfach zu bedienender und gleichzeitig leistungsfähiger Software dar. Die Zugriffsgeräte machen einen überaus guten Eindruck. NComputing bietet die Geräte und Software für "Office In A Box" auch zur kostenlosen Leihstellung an. (In) 

Das Telefonbuch

Alles in einem

Wer hier mit seiner Werbung drin ist, ist besser dran.

Finden von A bis Z. Das Telefonbuch: Werben Sie dort, wo man Sie dreifach gut findet. Im Buch, online oder mobil.

Werbung rein,
Umsatz rauf!





Im Kurztest: *Personal Printing Essentials* *For your eyes only*

von Daniel Richey

Die "Personal Printing Essentials" von Cortado richten sich an Unternehmen, die für Sicherheit in Bezug auf Ausdrücke sorgen möchten. Druckt ein User ein Dokument aus, kann nur dieser mit seinem Smartphone oder einer Smartcard an einem Netzwerkdrucker im Unternehmen den Ausdruck starten. IT-Administrator hat sich die Lösung angeschaut.

Damit sich die Anwender an den Druckern authentifizieren können, bieten die Windows-basierten Personal Printing Essentials mehrere Alternativen an. Für Unternehmen, in denen Smartphones populär sind, eignen sich QR-Codes. Die Nutzer fotografieren diese mit einer speziellen App und erhalten nach einer Rückmeldung des Smartphones an den Printserver den Ausdruck am passenden Drucker. Ebenfalls möglich ist die Nutzung der noch relativ jungen Technik "Near Field Communication" (NFC) sowie der Einsatz von Smartcards.

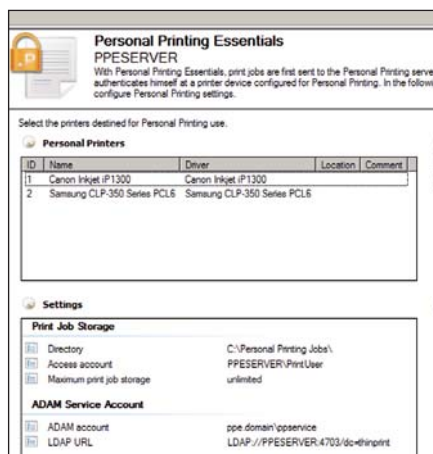
Einrichtung in wenigen Schritten

Die Personal Printing Essentials setzen für den Betrieb ein Active Directory voraus. So muss denn auch der Server, auf dem der Administrator die Software installiert, Mitglied einer Domäne sein. Die weitere Installation an sich geht dank Wizard schnell über die Bühne. Die einzige auf-

wändigere Interaktion für den Administrator besteht in der Eingabe des Lizenzschlüssels. Alternativ steht eine 30-Tage-Testvariante zur Auswahl. Für das weitere Setup und die anschließende Nutzung empfiehlt der Hersteller, zwei spezielle Konten für den Server selbst sowie die Druckaufträge anzulegen. Die User wählen fortan auf ihren Rechnern den "Personal Printer" zum Druck aus. Auf dem Printserver befinden sich dann die jeweiligen Treiber für die Netzwerkdrucker, wobei natürlich je Modell der Treiber nur einmal vorgehalten werden muss. Das Hinzufügen von Druckern auf dem Druckserver ist einfach: In einer Übersicht zeigt die Software die im Netzwerk vorhandenen Drucker an. Anschließend installiert der Administrator über die Funktion "Drucker hinzufügen" den entsprechenden Treiber.

Sicheres Drucken

Nutzerseitig muss der Administrator zunächst die gewünschten Authentifizierungsmethoden aktivieren, wobei sich auch mehrere parallel nutzen lassen. Diese Einstellungen gelten zunächst für alle Anwender. Auch lassen sich Einstellungen für einzelne User setzen – dazu gehört die Frage, ob die Funktion generell aktiviert ist sowie welche Authentifizierungsmethoden zum Einsatz kommen. Via Scripting lassen sich auch mehrere Benutzer gleichzeitig einrichten. Weshalb dies nicht auch über die grafische Oberfläche möglich ist, entzieht sich unserer Kenntnis.



Die eingerichteten Netzwerkdrucker lassen sich übersichtlich verwalten

Es folgt auf den Smartphones die Installation der Clientsoftware. Damit kön-

nen Nutzer dann den am Drucker aufgeklebten QR-Code abfotografieren und bestätigen, dass sie auf dem gewünschten Gerät ausdrucken möchten. Gegebenenfalls ist noch eine PIN einzugeben, falls dies vom IT-Verantwortlichen so eingerichtet wurde. Bei Nutzung der Chipkarten-basierten Authentifizierung schließt der Administrator zunächst die Authentifizierungsbox (Xtreme PC CXN 2321 von Chip PC) an und verbindet daran den eigentlichen Card Reader. Der Nutzer kann nun seine Karte in den Reader stecken und gibt bei Bedarf noch eine PIN am PIN-Pad ein.

Fazit

Mit den Personal Printing Essentials steht Administratoren eine einfach zu handhabende Suite zur Absicherung der Druckvorgänge zur Verfügung, die jedoch auch ihren Preis hat. Die Anwender dürften sich schnell mit dem Anmeldeprozedere zurechtfinden. Der Setup-Aufwand ist überschaubar – auch wenn ein komfortabler Weg zur Konfiguration mehrerer User über die GUI fehlt. Hier sind Scripting-Kenntnisse gefragt.



Produkt

Software zur Authentifizierung von Anwendern an Netzwerkdruckern.

Hersteller

Cortado
www.cortado.de

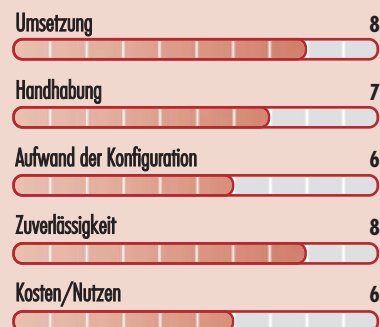
Preis

Für fünf Named User kostet die Lösung 3.050 Euro. Die Mietvariante kostet 21,30 Euro je Nutzer und Jahr.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Cortado Personal Printing Essentials

Netzwerkcapazitäten mit PRTG frühzeitig einplanen

Monitoring virtueller Umgebungen unterstützt Ressourcenmanagement

Der Virtualisierungstrend in Unternehmen und Rechenzentren setzt sich 2012 nahtlos fort. Mittels Servervirtualisierung können Administratoren Rechenleistung und Speicherplatz dynamisch zuordnen und so Ressourcen effizienter einsetzen. Verbrauchsspitzen einzelner Applikationen werden abgefangen. Doch kann nur ein schnelles und zuverlässiges Netzwerk in einer reibungslos funktionierenden virtuellen Umgebung diese Voraussetzungen erfüllen. Ein professionelles Netzwerk-Monitoring unterstützt schon vor dem Roll-Out der Virtualisierung bei der Planung – und überwacht später im laufenden Betrieb, ob die erforderliche Performance zur Verfügung steht.

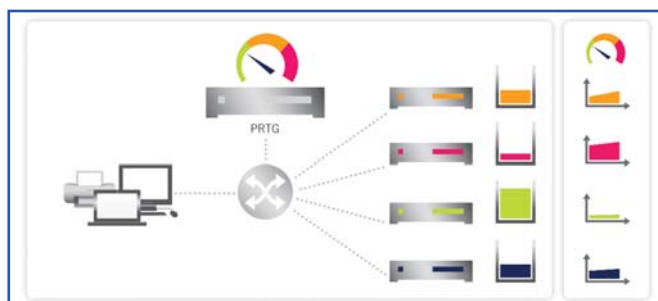
In nicht-virtualisierten Umgebungen ist Ressourcenplanung das A und O. Für jede Applikation müssen ausreichend Rechenkapazität, Arbeitsspeicher, Festplattenspeicher etc. vorhanden sein. Die jeweiligen Bedarfsspitzen und Leistungsunterschiede müssen rechtzeitig vorhergesagt werden. Der Knackpunkt liegt in den starken zyklischen Schwankungen hinsichtlich der Nutzung vieler Anwendungen. In einer nicht-virtualisierten Umgebung folgt daraus, dass die maximal benötigte Kapazität zur Verfügung gestellt werden muss. Dies wiederum hat oft zusätzliche Investitionen in Rechen- und Speicherleistung zur Folge, obwohl diese Leistung in der Praxis die meiste Zeit ungenutzt bleiben wird.

Virtuell = flexibler

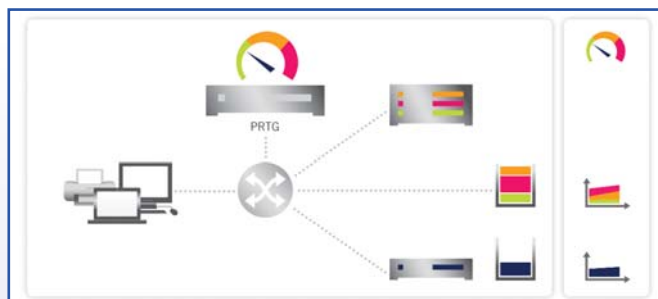
Server und Speichermedien in einer virtualisierten Umgebung können hinsichtlich der Ressourcenplanung quasi als ein großer Rechner behandelt werden. Denn virtuelle Infrastrukturen weisen Kapazitäten dynamisch einzelnen Applikationen zu. Anwendungen können so zusätzliche Ressourcen nutzen, die eigentlich für andere Applikationen vorgesehen sind, zu diesem Zeitpunkt aber ungenutzt zur Verfügung stehen. Eine Netzwerküberwachungslösung sammelt und analysiert die aktuellen Netzwerkdaten und bereitet diese anschaulich in Graphen auf, so dass der Verantwortliche alle Netzwerkaktivitäten inklusive dynamischer Leistungsspitzen permanent vor Augen hat.

Die Netzwerküberwachungs-Software PRTG Network Monitor gibt bereits in der Planungsphase der Einführung von Virtualisierung Aufschluss über die zu erwartenden Leistungsansprüche der einzelnen Applikationen und ermöglicht es dem Administrator, anhand von Langzeitanalysen Trends und Lastspitzen zu erfassen. Ressourcen können so von Beginn an bedarfsgerecht eingeplant werden, Engpässe in der Netzwerkperformance gehören der Vergangenheit an. Die aktuelle PRTG-Version enthält mehr als 120 verschiedene Sensortypen zur Überwachung der unterschiedlichen Aspekte eines

IT-Netzwerks. Allein 12 Sensortypen monitoren speziell virtuelle Systeme. IT-Administratoren, die z.B. VMware einsetzen, können mit PRTG ihre ESX-Hosts sowie über das Virtual Center einzelne virtuelle Maschinen überwachen. Zusätzlich hat die Software auch ein Auge auf virtuelle Maschinen, die in vApps laufen. So gewährleistet PRTG ein lückenloses Monitoring virtualisierter Umgebungen während des laufenden Betriebs. Bei Server-Beeinträchtigungen alarmiert das Programm den zuständigen Mitarbeiter. Detail-



Konventionelle Umgebung: Jede Applikation ist auf einem eigenen physischen Server mit angeschlossenem Speicher beheimatet.



Mittels Virtualisierung konsolidiert: Drei Anwendungen laufen in einer virtuellen Umgebung und teilen sich die Ressourcen des virtuellen Servers.

lierte Auswertungen der langfristig gesammelten Daten ermöglichen es den Netzwerkverantwortlichen, Schwachstellen frühzeitig aufzudecken und Ausfälle zu vermeiden.

Virtuelle PRTG-Sensoren im Überblick

- VMware Host Server (SOAP) Sensor
- VMware Virtual Machine (SOAP) Sensor
- VMware Host Hardware (WBEM)
- SSH VMware ESX(i) Disk Sensor
- Amazon CloudWatch Sensor
- Hyper-V Host Server Sensor
- Hyper-V Virtual Machine Sensor
- Hyper-V Virtual Storage Device Sensor
- Hyper-V Virtual Network Adapter Sensor
- Virtuozzo Container Disk Sensor
- Virtuozzo Container Network Sensor
- Xen Virtual Machine Sensor

Weitere Informationen stehen unter www.de.paessler.com/prtg zur Verfügung.



Paessler AG

Bucher Str. 79a

D-90419 Nürnberg

Tel.: +49 (911) 9 37 75 - 0

Fax: +49 (911) 9 37 75 - 409

E-Mail: info@paessler.com

URL: www.de.paessler.com

Ansprechpartner:

Dorte Winkler



Neuerungen in Hyper-V 3.0 unter Windows Server 8

Alles neu macht die 3

von Nils Kaczinski



Quelle: zenitix - 123RF

Microsofts Hyper-V hat einen respektablen Platz in der Riege professioneller Virtualisierungslösungen erobert. Obwohl Platzhirsch VMware mit vSphere technisch überlegen ist und es mit Citrix XenServer einen weiteren ernstzunehmenden Mitbewerber gibt, setzen viele Kunden auf den Hypervisor aus Redmond. Oft ist die niedrige Einstiegshürde der Grund, denn Hyper-V ist Teil des Betriebssystems, das den Administratoren vertraut ist. Mit der neuen Version Hyper-V 3.0 im kommenden Windows Server 8 versucht Microsoft den Sprung an die Spitze des Felds. IT-Administrator zeigt, welche Neuerungen auf Sie warten.

Seit Windows Server 2008 ist die Servervirtualisierung Hyper-V offiziell Teil des Betriebssystems. Zwar traf das zu Beginn noch gar nicht wirklich zu, denn im Lieferumfang war seinerzeit nur die Beta-Fassung enthalten. Erst ein halbes Jahr später konnten Kunden die produktive Version kostenlos nachladen. Trotzdem hat diese direkte Integration in das Server-Windows erheblich zur Verbreitung des Microsoft-Produkts beigetragen.

Die erste Version von Hyper-V legte den technischen Grundstein, hatte aber noch mit einigen Einschränkungen und dem Image ihres Vorgängers zu kämpfen – dem Virtual Server, den die Redmonder seit 2005 im Programm hatten. Dieser war eine Weiterentwicklung von Virtual PC, das Microsoft wiederum zwei Jahre vorher von Connectix übernommen hatte. Mit dieser Software ließen sich durchaus virtuelle Server betreiben, doch technisch war sie besonders dem Marktführer VMware weit unterlegen. Das lag vor allem daran, dass Virtual Server als Typ-2-Hypervisor ein Betriebssystem voraussetzte und dadurch weit weniger Performance zu bieten hatte als der Konkurrent ESX Server.

Diese Vorgeschichte ließ viele Kunden annehmen, dass Hyper-V nur eine neue Version des Virtual Server sei, die auf derselben Technik beruht. Tatsächlich aber war schon Hyper-V 1.0 eine völlig neue Software,

die je nach Anwendungsfall durchaus leistungsfähiger sein konnte als VMwares ESX. Gleichwohl ließ dieser Erstling einiges vermissen. So bot er noch keine „Live Migration“, Administratoren konnten virtuelle Maschinen also nicht im laufenden Betrieb von einem Hardware-Host auf einen anderen verschieben, sondern mussten immer eine Unterbrechung von mehreren Sekunden oder gar Minuten hinnehmen. Auch die Anbindung an SAN-Systeme oder andere professionelle Funktionen war noch nicht recht konkurrenzfähig.

Aufholjagd mit Version 2.0

Im Herbst 2009 änderte sich die Situation mit Hyper-V 2.0. Die noch immer aktu-

elle Fassung ist direkt in Windows Server 2008 R2 integriert und lässt sich ohne Download mit wenigen Mausklicks einrichten. Neben deutlich besserer Integration in Speicher-Netzwerke und zahlreichen Verbesserungen in Leistung und Administration ermöglicht diese Version vor allem die Live Migration, die den Mitbewerbern in nichts nachsteht: Für Wartungszwecke und zur Lastverteilung kann der Administrator die virtuellen Server von einem Host auf einen anderen schieben, ohne dass Anwender oder Applikationen eine Pause hinnehmen müssen.

Trotzdem bieten VMware und Citrix mit ihren Produkten eine Reihe technischer

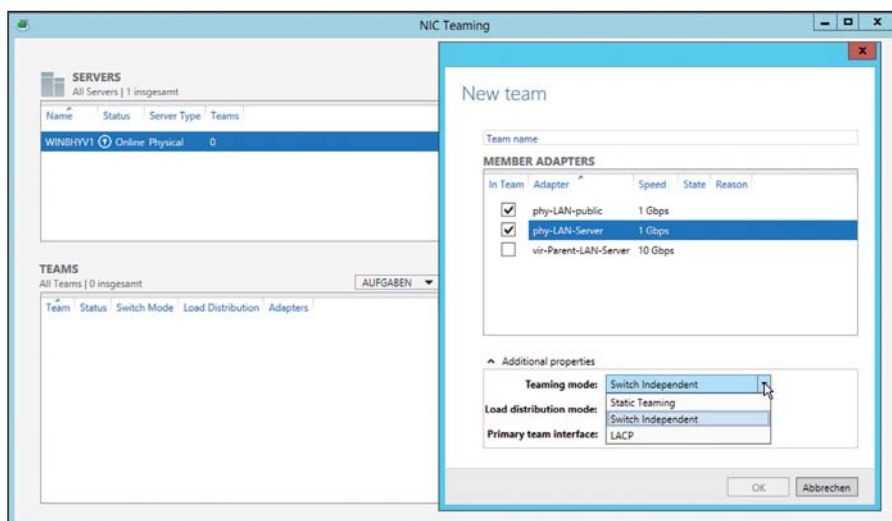


Bild 1: Netz im Team: Erstmals ermöglicht Windows Server 8 das Erzeugen von Netzwerkarten-Teams direkt aus dem Betriebssystem

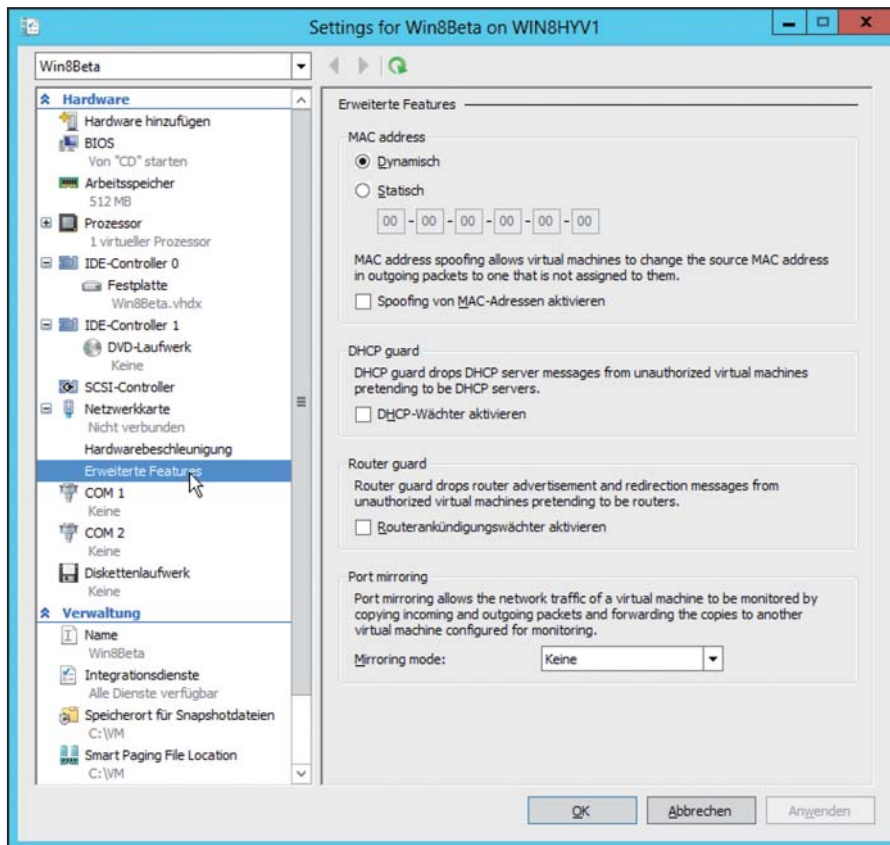


Bild 2: Die neuen Extensible Virtual Switches ermöglichen die Steuerung und Erweiterung virtueller Netzwerkfunktionen über eine zentrale Schnittstelle

Vorteile, für die Kunden oft bereit sind, beträchtliche Summen auszugeben. Dazu gehören zusätzliche Techniken, die die Verfügbarkeit virtueller Server erhöhen, aber auch anspruchsvolle Netzwerkfunktionen. Besonders VMware orientiert sich mit seinen hochwertigen, aber auch kostspieligeren Produkten am Bedarf großer Kunden, die sehr komplexe Rechenzentren virtuell betreiben wollen. Hier hat Hyper-V weniger zu bieten. Auch das Drumherum bietet VMware-Kunden Vorteile, denn sie finden eine große Zahl an Drittanbieter-Lösungen für die Nutzung virtueller Infrastrukturen.

Hyper-V 3.0: Doping für den Host

Grund genug für Microsoft, in der neuen Windows Server-Version besonders den Hypervisor weiterzuentwickeln. Die Vorabversionen, die MSDN-Abonnenten seit Herbst 2011 zur Verfügung stehen, zeigen schon einen Großteil dessen, was Hyper-V 3.0 mitbringen wird. Der Hersteller selbst, aber auch die Microsoft-nahe Community geben sich davon überzeugt, dass das neue Produkt zum Platzhirsch

aufschließen oder gar die Führung übernehmen wird.

Zunächst haben die Entwickler in Redmond vor allem die Leistungsgrenzen ihres Virtualisierers nach oben verschoben. Nicht nur Hyper-V-Hostserver werden deutlich mehr Prozessoren und RAM verwalten können, sondern auch die virtuellen Maschinen können auf wesentlich mehr Ressourcen zugreifen. Das ermög-

licht weit größere virtuelle Serverfarmen mit weniger Hardware als bisher. Gleichzeitig kommen sehr leistungshungrige Anwendungen für die Virtualisierung in Betracht. Eine Übersicht über die neuen Limits finden Sie in der Tabelle "Technische Grenzen für Hyper-V". Wichtig ist dabei auch eine neue Support-Aussage: Bislang gewährt Microsoft nur dann Unterstützung für eine virtuelle Serverwelt, wenn das Verhältnis von (logischer) Host-CPU zu virtuellen CPUs maximal 1:8 beträgt. Das bedeutet, dass ein Host mit zwei Quad-Core-Prozessoren und aktiviertem Hyper-Threading maximal 128 virtuelle CPUs an seine VMs verteilen kann. Nur für virtuelle Desktops liegt das Limit bei 1:12. Zwar sind diese Werte bereits sehr hoch, doch im neuen Produkt fällt diese Grenze ganz weg. Reizen Sie Ihre physischen CPUs also sehr hoch aus, wird Microsoft Ihnen im Zweifelsfall nicht die Unterstützung verweigern.

Daneben glänzt Hyper-V nun auch mit einer Client-Variante: Der Hypervisor ist nicht nur Teil des Server-Betriebssystems, auch Windows 8 für den PC wird in der Lage sein, virtuelle Maschinen auszuführen. Voraussichtlich ist dies zwar den Unternehmensversionen des Betriebssystems vorbehalten, doch attraktiv ist es nicht nur für Administratoren oder Software-Entwickler, die so einfacher Systeme testen können. Ein Hypervisor auf dem Anwender-PC dürfte auch für Unternehmen interessant sein, die auf einfache Weise ihren Mitarbeitern definierte und zentral gewartete Installationen bereitstellen oder je nach Si-

Technische Grenzen für Hyper-V

Komponente	Windows Server 2008 R2	Windows Server 8
Logische Prozessoren im Host	64	160
Arbeitsspeicher im Host	1 TByte	2 TByte
Server im Cluster	16	32
VMs im Cluster	1.000	4.000
Virtuelle Prozessoren pro VM	4	32
Arbeitsspeicher pro VM	64 GByte	512 GByte
Größe virtueller Festplatten	2 TByte	16 TByte
Speicheranbindung Host	SAN, lokale Platten	SAN, lokale Platten, Dateifreigaben
Speicheranbindung VM	VHD, iSCSI	VHD, VHDX, iSCSI, Fibre Channel

tuation unterschiedliche Setups einsetzen wollen. Virtuelle Computer als VHD-Dateien zu verteilen ist allemal einfacher als die Neuinstallation von PCs aus der Ferne.

Netzwerken leichtgemacht

Bislang bietet Hyper-V nur wenige Möglichkeiten, die Netzwerk-Anbindung virtueller Maschinen zu steuern. Als einzige Komponente stehen virtuelle Switches zur Verfügung, an die Sie die virtuellen Netzwerkkarten der VMs anknüpfen können. Abgesehen von VLAN-Tags, die Sie den virtuellen Ports zuweisen, besteht dort aber keinerlei Konfigurationsmöglichkeit. Zudem ist die Verwaltung der physischen Netzwerkkarten und der virtuellen Switches auf der Host-Ebene sehr unübersichtlich.

In Hyper-V 3.0 tut sich hier einiges. Schon die Ankündigung, dass Windows nun erstmals eine eingebaute Funktion für das Teaming von Netzwerkkarten bietet, lässt viele Anwender aufhorchen: Das Betriebssystem selbst kann Netzwerkports zur Lastverteilung und für das Failover zu einer Einheit bündeln, auch herstellerübergreifend und ohne Anpassung der physischen Switches. Bisher waren dafür stets Programme der Karten-Hersteller nötig. Microsoft selbst verweigerte jeden Support für Probleme, die eventuell daraus entstanden. Das ist vorbei, denn die Redmonder werden nun selbst Unterstützung gewähren.

Vor allem aber bietet der neue Hypervisor mit den "Extensible Virtual Switches" und den "Ressource Pools" erheblich mehr Flexibilität beim Aufbau virtueller Netzwerke. Erstmals bieten die virtuellen Switches eine einheitliche Schnittstelle, über die sich neue Funktionen als Add-ons integrieren lassen. In den Vorabversionen nutzt Microsoft dies selbst für einige Schutzfunktionen und zur Bandbreitensteuerung. Vor allem aber sollen hierüber Produkte von Drittanbietern zum Zuge kommen, die etwa Firewall-, Monitoring- oder Verwaltungsfunktionen bieten. So will Cisco zum Markstart des neuen Windows eine Komponente anbieten, die die virtuellen Switches gemeinsam mit den physischen im Netzwerk steuern kann.

Interessant an der Extensions-Schnittstelle ist, dass Sie mehrere Plug-Ins einbinden

können, die jeweils nur ihre eigenen Funktionen ausführen, aber nicht das gesamte Switching übernehmen müssen. Solche Funktionen lassen sich dann im laufenden Betrieb ein- oder ausschalten, was einfaches Troubleshooting ermöglicht. In einem Cluster sollten natürlich alle Hosts dieselben Plug-ins nutzen. Doch ist das einmal nicht der Fall, führt dies nicht automatisch zu einem Fehler beim Verschieben einer VM.

Schnell wieder auf den Beinen

Der zweite Neuheiten-Schwerpunkt in Hyper-V 3.0 bezieht sich auf die Verfügbarkeit virtueller Infrastrukturen. Neben Detailverbesserungen beim Clustering für anspruchsvolle Kunden wird Microsoft der erste Virtualisierungs-Anbieter sein, der seine Migrationsfunktionen nun auch ohne Cluster und sogar ohne gemeinsames Speichersystem bereitstellt. Sowohl die "Live Migration", also das Verschieben einer laufenden VM von einem Host-Server auf einen anderen, als auch die "Storage Live Migration" – das Übertragen der gesamten Datenbestände einer VM von einem Speicher auf einen anderen – werden ohne SAN und Cluster möglich sein. So migrieren Sie einen virtuellen

Server von der lokalen Platte eines Hosts auf die Platten eines anderen Hosts, ohne dass die Anwender etwas davon merken.

Für Furore hat die Ankündigung der "VM Replication" gesorgt, die so noch kein anderer Hersteller anbietet. Das Einsatzgebiet dieser neuen Technik sind virtuelle Systeme, die für ein Unternehmen sehr wichtig sind und nach einem Hardware-Ausfall an anderer Stelle wieder anlaufen sollen. Im Unterschied zu einem Host-Cluster wird die Replikation dafür keine erhöhten Anforderungen an die Umgebung stellen. Tatsächlich reicht es aus, zwei Hostserver zu betreiben, die über eine ausreichende Bandbreite miteinander kommunizieren können. Microsofts Ankündigung zufolge sollen hier auch übliche WAN-Verbindungen ausreichend sein, weil die Replikation im Normalbetrieb nur Differenzdaten überträgt, also keine übermäßige Last erzeugt.

Die Replikation lässt sich mit wenigen Mausklicks einrichten. Zunächst müssen Sie den Host und den Replikations-Empfänger miteinander bekannt machen. Das ist besonders einfach, wenn beide Server derselben Domäne angehören; eine Vo-

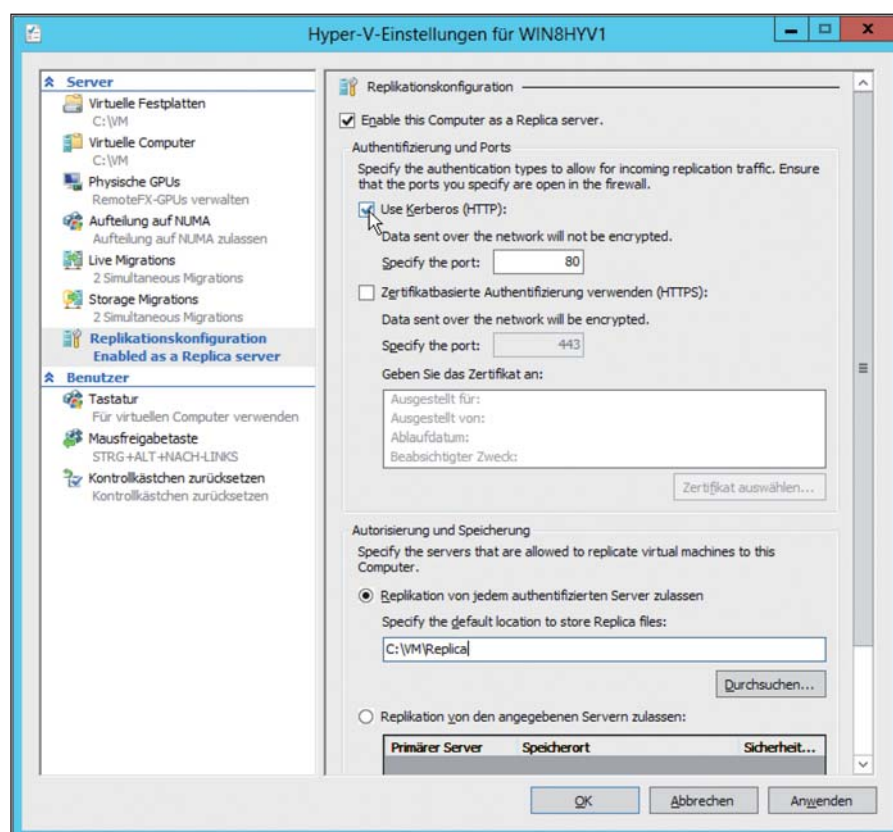


Bild 3: Jeder Hyper-V-Hostserver kann virtuelle Maschinen über den Replikationsserver replizieren oder Replikate empfangen. Die Einrichtung erfordert nur wenige Mausklicks.

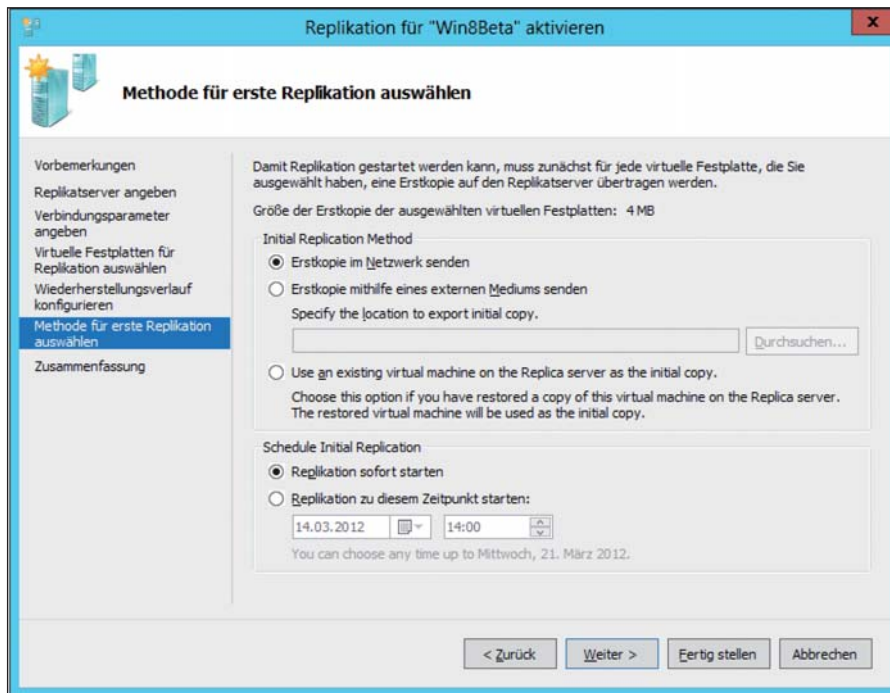


Bild 4: Für jede VM lässt sich festlegen, ob und wie Hyper-V sie replizieren soll. Die Konfiguration erfolgt bequem über einen Assistenten.

raussetzung ist das aber nicht. In diesem Schritt legen Sie auch fest, wo der Empfänger die replizierte VM speichern soll. Ist das erledigt, aktivieren Sie einzelne VMs zur Replikation. Je nach Bandbreite überträgt Hyper-V den Grundzustand der VM dann über das Netzwerk, Sie können hierfür aber auch einen Datenträger mit einem Backup nutzen. Die tatsächliche Replikation basiert dann auf Snapshots der VM, also den jeweiligen Unterschieden zum letzten Zustand. Nur diese Snapshots überträgt Hyper-V letztendlich an den Empfänger.

Daraus folgt, dass die "VM Replication" ein asynchrones Verfahren ist: Das Replikat einer VM ist nicht auf dem aktuellsten Stand, sondern weist immer eine gewisse Latenz auf. Das Verfahren kommt also nicht für jede Anwendung in Frage, kann aber sicher in vielen Szenarien dafür sorgen, ein Recovery an einem anderen Standort auch mit geringem Budget zu ermöglichen.

Unterbrechungsfreier Betrieb

Neben den erweiterten Kapazitätsgrenzen für Hyper-V-Cluster hat Microsoft auch die Speicheransprache über "Cluster Shared Volumes" (CSV) überarbeitet. Mit dieser Technik greifen seit Windows Server 2008 R2 alle Hosts in einem Cluster parallel auf dieselben SAN-Speicherbereiche zu. Erst

dadurch ist es möglich, virtuelle Maschinen live zwischen Hosts zu migrieren, denn hierfür ist ein nahtloser Zugriffswechsel auf die beteiligten Dateien im SAN nötig.

Die technische Basis der CSV tauscht Redmond komplett gegen ein neues Verfahren aus, behält die Schnittstellen zum Zugriff jedoch bei. Dadurch erreicht der Hersteller eine größere Skalierbarkeit und kann gleichzeitig die CSV-Technik, die bislang ausschließlich für Hyper-V zur Verfügung stand, auch für andere Applikationen einsetzen. Zusätzlich umgehen die neuen CSV nun bei der Datensicherung den "Redirected Mode", der bisher zu Performanceeinbußen beim Backup führte. Parallel haben die Windows-Entwickler die Dateidienste des Windows Server aufgebohrt und ermöglichen es in der kommenden Version, auch Serverapplikationen wie Hyper-V oder SQL Server an Dateiserver anzubinden statt wie bislang nur an blockbasierte SAN-Systeme. Das ermöglicht Cluster-Aufbauten zu geringeren Kosten als bisher, weil dadurch der gemeinsame Speicher unterhalb der Windows-Dateidienste mit günstigen Disk-Arrays ohne aufwändige SAN-Funktion abzubilden ist.

Neben diesen speicherbezogenen Erweiterungen erhalten Windows-Cluster neue Funktionen für Administration und Au-

tomatisierung. So wird es künftig möglich sein, Updates auf allen Servern eines Clusters automatisiert zu installieren. Hierbei kümmert sich der Cluster selbst darum, den jeweils betroffenen Serverknoten von allen Applikationen per Switchover beziehungsweise Live Migration zu befreien, und führt dort dann das Patching aus. Ist der Server nach dem Neustart wieder betriebsbereit, verschiebt Windows die Applikationen vom nächsten Server und fährt so fort, bis alle Hosts aktualisiert sind. Für unerwartete Ausfälle wird es im Cluster auch möglich sein, einzelnen virtuellen Maschinen und Applikationen Prioritäten für den automatisierten Neustart zuzuweisen. So lässt sich verhindern, dass etwa Exchange erfolglos startet, weil der Domänencontroller noch nicht läuft. Beim Clustering von Hyper-V sorgt ergänzend eine erweiterte Überwachungslogik dafür, dass das Failover nicht nur beim völligen Ausfall einer VM greift, sondern auch für Fehler aktiv wird, die innerhalb einer VM auf der Applikationsebene stattfinden. Das erfordert zusätzliche Konfiguration, ermöglicht aber noch größere Ausfallsicherheit als bisher.

Fazit

Der kommende Windows Server 8, dessen offizieller Name noch nicht feststeht, befindet sich derzeit in der Beta-Phase. Das fertige Betriebssystem ist für den Herbst 2012 zu erwarten. Was bislang davon zu sehen ist, verspricht ein Feuerwerk an Neuheiten, von denen ein großer Teil die Servervirtualisierung mit Hyper-V betrifft. Einige der neuen Funktionen bringen Microsoft die Technologieführerschaft, doch nüchtern betrachtet hat Marktführer VMware mit seiner vSphere-Technik insgesamt weiterhin die Nase vorn. Der Vorsprung allerdings, der noch vor kurzer Zeit uneinholbar erschien, wird mit Microsofts neuem Release deutlich geringer. Wer strategisch auf Virtualisierung setzt und eine Infrastruktur für anspruchsvolle Server-Umgebungen schaffen will, sollte sich Hyper-V 3.0 genau ansehen. Die Software verspricht zu vergleichsweise geringen Kosten ein hohes Maß an Leistung, Flexibilität und Zuverlässigkeit zu ermöglichen, von dem die Anwender im Netzwerk und damit der Geschäftserfolg des Unternehmens profitieren können. (dr)



Aufbau einer VDI-Umgebung mit VMware View 5

Schrumpfkur für Clients

von Christoph Harding



Quelle: Patinya Indrawoot – 123RF

Nach dem durchschlagenden Erfolg der Server-Virtualisierung verabschieden sich mehr und mehr Unternehmen auch im Desktop-Bereich vom einzelnen Rechner mit lokal installiertem Betriebssystem. Zur Verwirklichung einer Virtual Desktop Infrastructure bietet VMware mit View eine eigene Lösung an, die mit der Ende 2011 erschienenen Version 5.0 eine erneute Optimierung erfahren hat. In diesem Beitrag stellen wir die einzelnen Elemente des Produkts vor und gehen auf die wichtigsten Punkte ein, die im Rahmen einer (Teil-) Umstellung auf virtuelle Desktops zu beachten sind. Nicht zuletzt beleuchten wir das Zusammenspiel mit vSphere und den Einsatz von Thin Clients.

Desktop-Umgebungen stellen im IT-Bereich einen großen Kostenposten dar, der sich in seiner ganzen Dimension nur schwer kalkulieren und nachvollziehen lässt. Dabei geht es weniger um die Neuinvestition als vielmehr um Wartung und Betrieb der oftmals heterogenen Landschaften.

Dieses Szenario dürfte vielen Administratoren bekannt sein und hat vor einigen Jahren das Thema Desktop-Virtualisierung auf die Agenda in IT-Abteilungen gerufen. Der Endbenutzer sitzt dabei an einem entfernten Client, zum Beispiel einem Thin oder Zero Client, und greift über ein Remote Protokoll auf den virtuellen Desktop zu – er steuert das Betriebssystem fern. Dieser Aufbau verspricht großes Einsparungspotential bei den Betriebskosten der PC-Arbeitsplätze, bezogen auf Energieverbrauch, Softwareverteilung, Wartung und Support.

Eine virtuelle Desktop-Infrastruktur, kurz VDI genannt, ist aber viel mehr als nur die Installation und der Betrieb einer virtuellen Maschine (VM) auf einem Hypervisor. Sicher kann der Benutzer per RDP-Protokoll Zugriff auf den virtuellen Arbeitsplatz erhalten, aber dies ist eindeutig nicht genug. Es bedarf an dieser Stelle einer Komponente, die sich um den Single Sign-On, die Authentifizierung, die Nutzung von USB-Geräten oder auch

um die benutzergerechte Darstellung der Bildschirminhalte kümmert.

Überblick zu VMware View 5

Dass die Virtualisierung von Desktop-Arbeitsplätzen schon lange nicht mehr nur ein Hype ist, zeigt sich alleine schon dadurch, dass mit VMware View 5 eine mittlerweile sehr fortgeschrittene Version einer Desktop-Virtualisierungslösung vorliegt. Die Plattform, basierend auf dem vSphere Hypervisor, stellt eine VM bereit, in der das Windows Client-Betriebssystem ab Version Windows XP und aufwärts ausgeführt wird. Der Benutzer erhält Zugriff auf diese virtuelle Betriebssysteminstanz, indem er sich von einem Fat-, Thin- oder Zero-Client per Remote-Protokoll an dieser anmeldet und auf dem entfernten Computer im Rechenzentrum arbeitet. Zwischen seinem Endgerät und dem virtuellen Desktop werden nur Bildschirm-inhalte, Tastatur- und Maussignale ausgetauscht. Das bedeutet, dass alle Daten immer im Rechenzentrum liegen und der Benutzer die VM nur fernsteuert, was gerade unter Security-Gesichtspunkten positiv zu beurteilen ist.

Im beschriebenen Szenario fehlt aber noch die wichtigste Komponente: der Broker, oft auch VDI-Server oder Connection Server genannt. In einer VMware View-Um-

gebung nennt sich diese Komponente View Manager. Der View Manager spielt in einer VDI-Umgebung eine Schlüsselrolle, denn er kümmert sich neben der Authentifizierung des Anwenders um diverse Sicherheitsaspekte und ist verantwortlich für die Verwaltung der VMs und die Bereitstellung neuer Desktops. Im Folgenden geben wir einen Überblick zu den weiteren in einer VDI wichtigen Funktionen von VMware View.

Zugriff von verschiedensten Endgeräten

VMware View erlaubt den Zugriff auf den virtuellen Windows-Desktop von einer Vielzahl an unterschiedlichen Endgeräten und Betriebssystemen aus. Dazu gehören alle gängigen Betriebssysteme wie Microsoft Windows, Apple MacOS, Linux, iOS und Android. Thin- und Zero Client-Hersteller liefern den VMware View-Client, der für den Zugriff auf einen Desktop nötig ist, standardmäßig mit aus.

Offline Verfügbarkeit

Neben dem Fernzugriff auf die virtuellen Desktop-Arbeitsplätze bietet VMware View 5 zudem die Möglichkeit, die VMs lokal auf dem Client des Benutzers auszuführen, um so auch offline arbeiten zu können. Der VMware "Local Mode Desktop" wird auf einem Host-Betriebssystem ausgeführt,



genau wie bei VMware Workstation oder dem VMware Player. Unterstützung finden hier die Host-Betriebssysteme Windows XP, Vista und Windows 7. Die VM steht hierbei stets unter Kontrolle der IT-Administration. So lassen sich Local Mode-Desktops mit einem Ablaufdatum versehen – die VM muss sich spätestens zu diesem Zeitpunkt wieder beim Management-Server gemeldet haben, da sie ansonsten deaktiviert wird und erst nach einem erneuten Kontakt und der Authentifizierung des Benutzers wieder nutzbar ist.

Zudem ist die Remote-Deaktivierung des über AES verschlüsselten Desktops von zentraler Stelle aus möglich. Im Falle eines Diebstahls lässt sich so sicherstellen, dass die Daten nicht in unberechtigte Hände fallen. Die VMware View-Infrastruktur ist für die Nutzung des Local Modes nur geringfügig zu erweitern. Dazu ist die Installation eines weiteren View-Servers nötig, der sich um den Transfer der Daten zwischen Rechenzentrum und Client kümmert. Zusätzliche Optionen wie eine Datensicherung des Offline-Clients über das Netzwerk runden die Funktionalität ab. VMware hat einen auf Bandbreite und Geschwindigkeit optimierten Synchronisationsprozess integriert, der nur die veränderten Blöcke der virtuellen Festplatten und nicht den gesamten Datenträger überträgt.

Automatisierte Desktop-Bereitstellung

Immer wiederkehrende Tätigkeiten, die zur täglichen Routine gehören, stellen ein großes Potential für Fehleranfälligkeit dar, sofern die Aufgaben manuell zur Ausführung kommen – wie beispielsweise die Bereitstellung von Desktop-Arbeitsplätzen. Aufgrund der Anzahl von Arbeitsplätzen in einem Unternehmen werden die einzelnen Computer in den meisten Fällen nicht komplett neu installiert. Vielmehr kommen oft Cloning-Technologien zum Einsatz, die eine bestehende Betriebssysteminstallation anpassen und dem neuen Anwender zur Verfügung stellen. Dabei sind sehr viele Details zu beachten, wie etwa die ordnungsgemäße Integration in das Active Directory, Softwareinstallationen oder die Rechtevergabe für den Benutzer. Kleine Fehler können große Auswirkungen haben und die Fehleranalyse einen großen Zeitaufwand bedeuten.

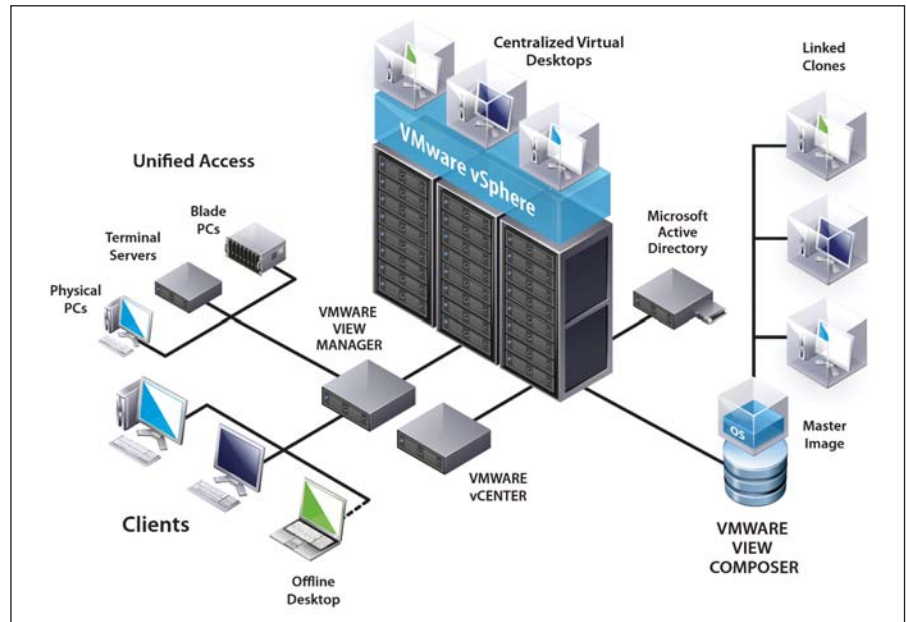


Bild 1: Eine VDI-Konstruktion mit VMware View besteht aus Komponenten wie dem View Manager und dem View Composer und lässt sich mit vSphere verzahnen

Um solche Fehlerquellen möglichst auszuschließen, gilt es, diese Tätigkeiten komplett zu automatisieren. VMware View bietet weitreichende Möglichkeiten, um Desktop-Arbeitsplätze in verschiedensten Konfigurationen und Mengen bereitzustellen. Desktops können als einzelne, individuelle Maschinen für einen Benutzer angeboten werden, aber auch in sogenannten Desktop-Pools, in denen Benutzergruppen sich eine vorgegebene Anzahl von Desktops teilen. Die Konfiguration der Arbeitsplätze erfolgt über den VMware View Administrator – eine Webseite, die auf dem VMware View Manager Server läuft. Dazu wird zunächst eine Vorlage (Template) für die VM erstellt, die das gewünschte Betriebssystem, zum Beispiel Windows 7, enthält. Der IT-Verantwortliche weist über den View Administrator dieses Template danach einem Pool zu und legt die Parameter für den Pool fest.

Zu diesen Konfigurationsparametern gehört beispielsweise die Größe des Desktop-Pools, also die Anzahl der sich darin befindenden Arbeitsplätze, die Namensgebung und viele weitere Einstellungen, wie auch das Verhalten bei Nichtbenutzung des Arbeitsplatzes. Die VM kann immer eingeschaltet bleiben, schlafen gelegt oder heruntergefahren werden. Nach dem Anlegen des neuen Desktop-Pools beginnt der View Manager Server mit der vollautomatisierten Generierung der VMs. Zum Schluss muss

der Administrator nur noch festlegen, welche Benutzer oder Benutzergruppen auf die neuen Arbeitsplätze zugreifen dürfen.

Integrierte Sicherheit

Die Sicherheit von IT Systemen, speziell die Datensicherheit bei Arbeitsplatzrechnern, ist eine große Herausforderung. Damit die virtuellen Computer bestmöglich vor ungewolltem Zugriff geschützt sind, läuft die gesamte Kommunikation zwischen Servern, Clients und virtuellen Desktops via SSL-Verschlüsselung ab. Das VMware-eigene PCoIP Remote-Protokoll kann entweder mit dem AES-Algorithmus oder mit Salsa-20 verschlüsselt werden. Neben der Datenverschlüsselung stehen verschiedene Optionen zur Authentifizierung der Anwender zur Verfügung, darunter die Authentifizierung am Verzeichnisdienst Active Directory mit oder ohne RSA Token-Schutz, die Nutzung von Smartcards oder die Zertifikat-basierende Authentifizierung.

PCoIP-Protokoll mit Verbesserungen

Durch die verbesserten Funktionen in Version 5 von VMware View hat der Hersteller die Anwendungsfälle für virtuelle Desktop-Umgebungen nochmals erweitert. So hat VMware eine neue Schnittstelle unter dem Namen "View Media Services for Integrated Unified Communications" geschaffen, die es VoIP-Herstellern ermöglicht, ihre Kommunikati-

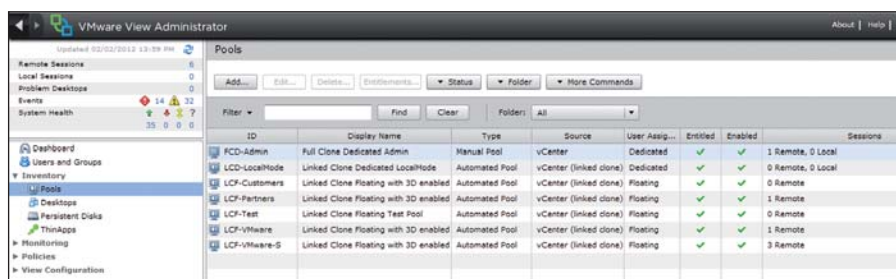


Bild 2: Der View Administrator verwaltet neben einzelnen virtuellen Desktops auch Pools, in denen sich Benutzergruppen eine vorgegebene Anzahl von Desktops teilen

onsprodukte einfach in die VDI-Lösung zu integrieren. Kompatible Produkte bieten beispielsweise Avaya, Cisco und Mitel. Dem Benutzer wird es so ermöglicht, ein Softphone in der VM zu betreiben oder sein Hardware-Telefon über die Software auf dem virtuellen Desktop zu steuern.

Auch das PCoIP-Protokoll selbst erfährt Verbesserungen: VMware bewirkt die Lösung mit einem bis zu 75 Prozent niedrigeren Bandbreitenverbrauch, der sich aus dem Zusammenspiel von verschiedenen Parametern ergibt. Neben dem optimierten Algorithmus des Remote-Protokolls wurden neue Funktionen wie das Client Side Caching und die Option zum No-Built-to-Lossless integriert. Client Side Caching speichert die Bildinhalte in vor-einstellbarer Größe auf dem Clientgerät zwischen, sodass diese nicht erneut über die Netzwerkverbindung übertragen werden müssen, sondern erst dann, wenn sich die Inhalte wirklich ändern sollten.

Die Option No-Built-to-Lossless gibt dem Administrator nun die Möglichkeit, die Komprimierung des Bildinhaltes zu beeinflussen. Wenn in der Vergangenheit jeder Pixel immer in höchster Qualität übertragen wurde, was eine höhere Bandbreitennutzung mit sich bringt, so lässt sich dies nun bei Bedarf, etwa bei niedrigen Bandbreiten der Netzwerkverbindung, auf Wunsch abschalten. Der Benutzer selbst wird den Unterschied an seinem Arbeitsplatz kaum oder gar nicht feststellen.

Vom physischen Desktop zum virtuellen Arbeitsplatz

Viele Unternehmen stellen sich heute die Frage, ob eine virtuelle Desktop-Umgebung Sinn macht oder nicht. Wie bereits zu Beginn erwähnt, sind die Kosten für den Desktop-Betrieb häufig der Treiber

für den Einsatz der neuen Technologien. Unternehmen identifizieren zunächst Anwendungsfälle, bei denen die Nutzung der virtuellen Desktops sinnvoll ist und in Verbindung mit Kosteneinsparungen steht. Die gesamte Migration aller Desktop-Computer eines Unternehmens stellt aber eher nicht den Regelfall dar. Am Beginn eines Projekts steht meist nur eine kleinere Umgebung, die dann aber sehr schnell wachsen kann. Es gibt aber auch Fälle, bei denen direkt mehrere tausend Desktops virtualisiert werden.

Die Planung einer VDI-Umgebung ist das A und O. Neben einem Assessment, bei dem eine genaue Untersuchung erfolgt, welche Hardware- und Software-Anforderungen die Anwender wirklich haben, sollten sich auch die Benutzer selbst von Anfang an mit in dem Projekt wiederfinden. Es ist stets darauf zu achten, dass die Anwender eine ordentliche User Experience erhalten, denn dies ist eines der Hauptkriterien für den Erfolg. Um dies zu erreichen, ist ein korrektes Hardware- und Storage-Sizing essenziell.

Dem produktiven Einsatz sollte immer ein Proof-of-Concept und eine Pilotphase mit echten Benutzern vorausgehen, in der die Kompatibilität von Anwendungen und die

User Experience eingehend getestet werden. Schon während der Planungsphase des Projekts, aber spätestens nach Abschluss, ist eine Berechnung zur Skalierung der Produktivumgebung durchzuführen. Zu den zu beachtenden Parametern gehören die gleichzeitige Benutzerzahl, Netzwerkbandbreiten und die Anwendungsfälle selbst, also Task-Worker oder Power User.

Nahtlose Integration in vSphere

Die Grundlage für eine auf VMware View basierende VDI-Umgebung ist die Virtualisierungsplattform vSphere, auf deren Hypervisor die virtuellen Arbeitsplätze betrieben werden. Der Hersteller liefert dazu das sogenannte VMware View Bundle, das in den Größen für zehn und 100 Benutzer verfügbar ist und die gesamte Plattform inklusive Hypervisor und dem Verwaltungstool vCenter enthält. Kunden, die bereits vSphere einsetzen, können auch Add-On-Lizenzen beziehen, die nur die VMware View-Komponenten hinzufügen.

Ist die Virtualisierungsplattform eingerichtet, sind die meisten Voraussetzungen für eine virtuelle Desktop-Umgebung bereits erfüllt. Alle Komponenten der VMware View Lösung lassen sich als VMs betreiben. Im minimalsten Szenario sind für den Betrieb einer VDI-Landschaft zwei vSphere-Hypervisoren, ein vCenter, ein VMware View Connection Server sowie die virtuellen Desktops nötig. Neben den VMware-eigenen Komponenten bedarf es aber weiterer Dienste für den Betrieb der VDI-Umgebung. Neben dem Active Directory sind dies DHCP und DNS für die Namensauflösung der virtuellen Arbeitsplätze.

Die Installation des VMware View Connection Servers erfolgt auf einem Windows

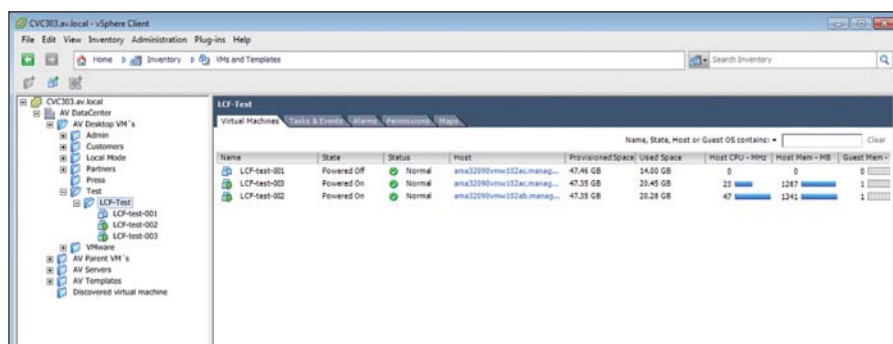


Bild 3: Sind die nötigen Voraussetzungen geschaffen, kann der View-Server auf die bestehenden virtuellen Maschinen und Vorlagen der vSphere-Umgebung zugreifen



Server 2008-Betriebssystem. Danach wird er mit dem zuständigen vCenter Server verbunden. Dazu verwendet der View Administrator das webbasierte Administrationstool. Nach der Etablierung der Verbindung kann der View-Server auf die bestehenden VMs und Vorlagen der VMware vSphere-Umgebung zugreifen. Dem View Manager werden nur VMs präsentiert, die eines der kompatiblen Desktop-Betriebssysteme enthalten.

Bevor diese nutzbar sind, ist auf den Desktops der View Agent zu installieren, der für die Kommunikation zwischen Server und Desktop zuständig ist. Der virtuelle Client meldet über diese Schnittstelle beispielsweise seinen aktuellen Status an den Server. Der View Server weiß so, ob ein Arbeitsplatz bereit für Verbindungen ist oder nicht. Über den gleichen Weg werden auch weitere Aufgaben aus Richtung des Servers erledigt. Dazu gehören die Übertragung neuer Konfigurationen durch den Server und Anweisungen zum Neustart oder Herunterfahren der Systeme. Grob gesehen sind das alle Voraussetzungen, die für einen Test gegeben sein müssen. Um in die Produktion zu gehen, sind aber weitere Konfigurationen, Optimierungen und Softwareinstallationen nötig.

Automatisierte Desktop-Verwaltung dank Schnittstellen

Die Verwaltung der VDI-Umgebung erfolgt maßgeblich über zwei Anwendungen: Zum einen über den vCenter Client,

über den sich die VMs erstellen lassen, zum anderen über den View Administrator, mit dem der Administrator die Desktops und Pools sowie die gesamten Konfigurationen verwaltet. Durch das rollenbasierte Konzept fällt es leicht, Verwaltungsaufgaben an verschiedene Abteilungen zu delegieren. Genau wie beim VMware vCenter sind verschiedene Profile möglich, über die der Zugriff auf die Verwaltungsoberfläche, den View Administrator, gesteuert wird. Während etwa die Administratoren Vollzugriff auf alle Funktionen haben, muss der Helpdesk lediglich mit lesendem Zugriff auskommen.

Der interessante Aspekt bei einer VDI-Installation ist, dass bereits getätigte Investitionen in Softwaredeployment-Lösungen, Monitoring- oder Administrations-Tools nicht umsonst waren, da sich diese oftmals sehr gut in die View-Umgebung integrieren lassen. Über diverse Schnittstellen ist der Import und Export von Daten sowie die nahezu komplette Automatisierung der Lösung möglich. Zu diesen Schnittstellen gehören Web Services, Powershell API und weitere Tools, die direkt auf die View-Komponenten zugreifen. Die Integration in den Microsoft System Center Operations Manager stellt über das beiliegende Kit auch kein Problem dar.

Auswahl geeigneter Clients

Unternehmen stehen im Rahmen eines VDI-Projektes vor der Frage, mit welcher Art von Client der Benutzer auf den vir-

tuellen Desktop zugreifen soll. Thin- oder Zero Clients etwa erweisen sich als kostensenkend, da sie zum einen weniger Energie verbrauchen als ein herkömmlicher Arbeitsplatz, zum anderen aber auch in der Anschaffung günstiger sind, einen längeren Lifecycle besitzen und kaum mit Software und Updates versorgt werden müssen. Die meisten Thin Client-Hersteller bieten den VMware View-Client für den Zugriff ab Werk an und haben neben diesem auch Zero Clients im Angebot, die speziell für den Zugriff auf VMware View Desktops per PCoIP-Protokoll konzipiert sind.

Für die Weiterverwendung bestehender Desktop-Arbeitsplätze lässt sich der View-Client direkt auf den entsprechenden Windows- oder Linux-Arbeitsplätzen installieren. Eine Alternative dazu ist eine Repurposing-Lösung. Dabei handelt es sich um einen von einem USB-Stick oder der lokalen Festplatte gestarteten, minimalen View-Client, der auf Linux basiert. Verschiedene Hersteller haben derartige Produkte im Angebot. (In) 

Übersicht zu VMware View 5 mit Download-Link
C5P71

TMV – Blog zu VMware View
C5P72

Myvirtualcloud.net – Blog zum Thema VDI und
Cloud-Computing
C5P73

Link-Codes



Virtualisierung und Cloud-Zugriff – mal einfach!



Bleiben Sie flexibel mit IGEL Thin Client Software und Hardware:

- ▶ Zugriff auf alle führenden VDI-Umgebungen
- ▶ Beste Performance und User-Experience
- ▶ Zahlreiche integrierte Software-Clients
- ▶ Einfache & schnelle Administration aller Geräte mit der remote Management Lösung UMS

Überzeugen Sie sich selbst! Fordern Sie jetzt eine KOSTENLOSE TESTSTELLUNG an:

www.igel.de/it-admin





Virtualisierung mit QEMU 1.0 Schneller Open Source-Vogel

von Dr. Holger Reibold

Beim Thema Desktop-Virtualisierung fallen den meisten Administratoren die Produkte von VMware oder das VirtualBox-Projekt ein. Doch es gibt interessante Alternativen. QEMU zum Beispiel wird für seine sehr gute Ausführungsgeschwindigkeit geschätzt. Wir zeigen Ihnen in diesem Workshop, wie Sie den freien Virtualisierer zum Laufen bringen und wie Sie damit virtuelle Maschinen zum Leben erwecken. Dabei gehen wir sowohl auf die Bedienung über die Kommandozeile als auch die grafische Benutzeroberfläche ein. Für Shell-Experten geben wir zudem Tipps zur Live Migration mit QEMU.

Neben den etablierten Virtualisierungslösungen existiert eine Fülle von weiteren bemerkenswerten Projekten, gerade aus dem Open Source-Umfeld. Zu den leistungsfähigsten Tools zählt zweifelsohne QEMU (Quick Emulator), das seit Dezember letzten Jahres in Version 1.0 verfügbar ist. Bemerkenswert ist hierbei der Umstand, dass verschiedene, weit bekanntere Virtualisierungslösungen wie beispielsweise VirtualBox und Xen Teile des Source-Codes von QEMU verwenden.

QEMU ist eine freie virtuelle Maschine (VM), die die Hardware eines vollständigen Computers emuliert und dank der dynamischen Übersetzung der Prozessor-Instruktionen des Gast-Prozessors in Instruktionen für den Host-Prozessor eine hohe Performance erzielt. Das Besondere ist die sehr gute Ausführungsgeschwindigkeit. Im Unterschied zu vielen anderen Emulatoren läuft QEMU auch auf anderen Prozessoren als x86 und kann x86-, x86-64- beziehungsweise AMD64-, PowerPC- und Sparc32/64-Hardware emulieren.

Ein weiterer Punkt macht QEMU interessant: Der Emulator läuft auf einer Vielzahl von Plattformen, angefangen bei Linux über Mac OS X bis hin zu Windows. QEMU unterstützt ferner die sogenannte Live Migration. Dabei können Sie den Status einer VM speichern und ohne die Maschine anzuhalten auf ein anderes Host-System übertragen. QEMU unterstützt unter Linux, BSD und Mac OS X zudem die Userspace-Emulation. Nicht zuletzt ist die Ausführung von Live-CDs und ISO-Images problemlos möglich.

Wenn Sie QEMU unter Windows einsetzen wollen, sind hierfür nicht einmal

Administratorrechte erforderlich. Eine weitere Besonderheit: Sie können QEMU auf einem USB-Stick als portable Software verwenden. Mancher Administrator wird QEMU schon deshalb mögen, weil sich das Programm überwiegend auf Konsolenebene steuern lässt. Wer lieber mit einer grafischen Benutzeroberfläche arbeitet, greift unter Windows zum QEMU Manager (siehe Kasten "QEMU unter Windows") und unter Linux zu AQEMU.

QEMU in Betrieb nehmen

Die Installation von QEMU ist in der Regel relativ einfach. Da Sie vermutlich mit einer recht aktuellen Linux-Distribution

```
monitor console
QEMU 0.12.5 monitor - type 'help' for more information
(qemu) info block
ide1-cd0: type=cdrom removable=1 locked=0 [not inserted]
floppy0: type=floppy removable=1 locked=0 [not inserted]
sd0: type=floppy removable=1 locked=0 [not inserted]
(qemu) 
```

Bild 1: Mit dem QEMU-Monitor steuern Sie die Virtualisierungssoftware



Tastaturkürzel in QEMU

Tastaturkürzel	Vorteile
"Strg" + "Alt" + "1"	Wechselt zur Anzeige des Gast-Betriebssystems
"Strg" + "Alt" + "2"	Wechselt zur Konsole 2 – QEMU-Monitor
"Strg" + "Alt" + "3"	Wechselt zur Konsole 3 – serielle Ausgabe
"Strg" + "Alt" + "4"	Wechselt zur Konsole 4 – parallele Ausgabe
"Strg" + "Alt" + "F"	Schaltet zwischen Vollbild- und Fenstermodus um
"Strg" + "Alt" + "+"	Vergrößert die Bildschirmausgabe
"Strg" + "Alt" + "-"	Verkleinert die Bildschirmausgabe

arbeiten, sollten Sie wissen, dass hier häufig QEMU und die Kernel-based Virtual Machine im Paket "qemu-kvm" zusammengefasst sind. Beachten Sie allerdings, dass das qemu-kvm nur x86-Gast-Systeme unterstützt. In diesem Fall ist auch die Installation des Pakets qemu-kvm-extras ratsam, da es die Emulatoren der anderen Architekturen beinhaltet.

Wenn Sie Debian und eine Ubuntu-Variante einsetzen, bietet sich die Installation mit dem Paketmanager an. Alternativ steht die Konsole zur Verfügung:

```
sudo apt-get install qemu-kvm
qemu-kvm-extras
```

Bei Fedora, Red Hat Enterprise Linux und CentOS kommt yum zum Einsatz. Hier lautet der entsprechende Installationsbefehl wie folgt:

```
yum install qemu-kvm qemu-kvm-extras
```

Wenn Sie OpenSUSE bevorzugen, greifen Sie zu YaST. Suchen Sie mit dem Tool die Pakete "qemu-kvm" und "qemu-kvm-extras" und installieren Sie diese.

Erste virtuelle Maschinen erstellen

Ist QEMU installiert, können Sie die ersten Gehversuche unternehmen und eine VM anlegen. Der Umgang mit VMs verläuft immer nach dem gleichen Schema:

1. Zunächst legen Sie eine virtuelle Festplatte, genauer eine Image-Datei, an.
2. Starten Sie mit QEMU diese virtuelle Festplatte und das Installationsmedium.
3. Schließlich installieren Sie das ge-

wünschte Gast-Betriebssystem. Hierbei müssen Sie insbesondere auf die Unterstützung der emulierten Hardware achten. Die Installation spezieller Treiber im Gast-System ist in der Regel nicht erforderlich.

QEMU verwendet unter allen Betriebssystemen die gleichen Startoptionen, es gibt also bei der Standardausführung keinerlei Unterschiede. Eine VM generieren Sie standardmäßig mit Shell-Kommandos. Der Vorteil: Die Kommandozeile gibt auch mögliche Fehlermeldungen aus. Für die Installation eines Gast-Betriebssystems greifen Sie auf ein Disk-Image zurück. Aus der Perspektive des Gast-Betriebssystems handelt es sich um eine Festplatte, auf der das Gastsystem sein eigenes Dateiensystem anlegen kann.

Das QEMU-Team stellt auf seiner Projekt-Site [1] verschiedene Gast-Systeme zum Download bereit. Wenn Sie zunächst ein wenig mit QEMU spielen wollen, laden Sie sich doch beispielsweise eine spezielle Linux-Distribution herunter, die gerade einmal 8 MByte klein ist und mit der Sie erste Erfahrungen sammeln können. Um das Image auszuführen, laden Sie es herunter, entpacken es gegebenenfalls und führen folgenden QEMU-Befehl aus:

```
qemu Name der Image-Datei.img
```

Ersetzen Sie die Image-Bezeichnung durch den Namen Ihres Gast-Image-Files. Besitzt das Gastsystem eine GUI und wollen Sie die Maus innerhalb des Systems verwenden, klicken Sie doppelt

in das Feld. QEMU vereinnahmt dann quasi die Maus. Um wieder zum Wirt zu wechseln, betätigen Sie die "Strg"- und "Alt"-Tasten. Weitere wichtige Tastenkombinationen fasst die Tabelle "Tastaturkürzel in QEMU" zusammen.

QEMU unterstützt verschiedene Image-Typen. Mit der aktuellen Version können Sie folgende Typen verwenden:

- raw : Standardformat
- cloop: Dieses Format kommt überwiegend für Live-CDs zum Einsatz
- cow: Wird lediglich aus historischen Gründen unterstützt
- qcow: Wird ebenfalls aus historischen Gründen unterstützt
- qcow2: Gilt als besonders flexibles Format mit einer Vielzahl interessanter Funktionen
- vmdk: VMware 3, 4 und 6 Image-Format
- vdi: Zu VirtualBox 1.1-kompatibles Image-Format

Die QEMU-Umgebung stellt mit dem QEMU-Monitor ein weiteres nützliches Werkzeug zur Verfügung. Damit können Sie VMs zur Laufzeit steuern. Die Steuerung erfolgt auf Konsolenebene und sieht neben den Standardfunktionen wie dem Wechseln oder Auswerfen von Wechselmedien oder dem Einfrieren und der erneuten Inbetriebnahme einer VM verschiedene erweiterte Funktionen vor. Sie können mit dem Monitor beispielsweise die verschiedenen Zustände der VM sichern und wiederherstellen. Auch das Inspizieren des Zustands einer VM oder das Verändern der Hardware und sogar das Injizieren von emulierten Hardwarefehlern ist mithilfe des QEMU-Monitors möglich.

Um in den QEMU-Monitor zu wechseln, führen Sie die Tastenkombination "Strg" + "Alt" + "2" aus. Das Kommando *info* gibt die Zustandsinformationen der aktuell ausgeführten Instanz aus. Um die Befehlszeilen-Historie auf den Bildschirm zu bringen, verwenden Sie den Befehl *info history*. Wenn Sie die Konfiguration eines Devices ändern wollen, nutzen Sie das folgende Kommando:

```
change device filename [format]
```

Die Ausführung einer Migration ist schon schwieriger. Mit dem folgenden Befehl übertragen Sie die VM von einem Host-System auf ein anderes Host-System:

```
migrate [-d] [-b] [-i] uri
```

Dabei bestimmt der Parameter "uri" die Ziel-URL.

Der QEMU-Monitor



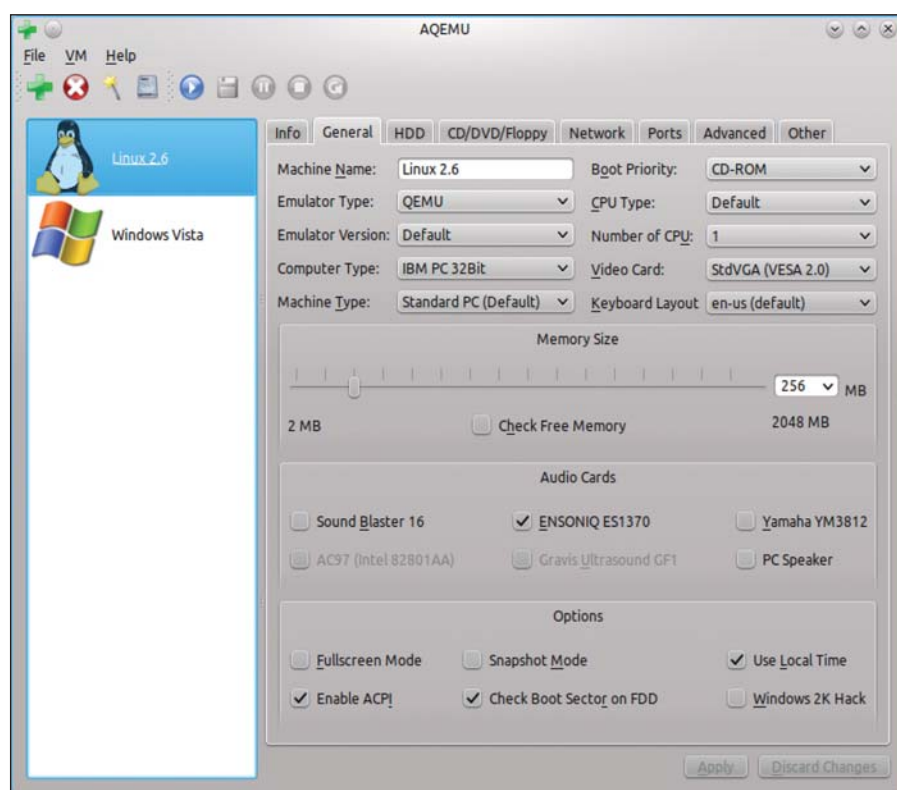


Bild 2: Wenn Sie QEMU unter Linux lieber über ein GUI steuern, sollten Sie zu AQEMU greifen

Um ein eigenes Image anzulegen, erzeugen Sie zunächst ein leeres Disk-Image. QEMU stellt Ihnen hierfür das Tool “qemu-img” zur Verfügung. Es dient dem Erstellen und Manipulieren von Disk-Images und unterstützt verschiedene Formate. Wenn Sie keinen Image-Typ vorgeben, erzeugt qemu-img RAW-Dateien. Das bevorzugte Format ist allerdings qcow2. Wenn Sie ein 10 GByte großes Image im qcow2-Format erzeugen wollen, auf dem Sie dann Windows 7 installieren möchten, verwenden Sie folgenden Befehl:

```
qemu-img create -f qcow2
win7p.img 10G
```

Der einfachste Weg, das Gast-Betriebssystem zu installieren: Sie erzeugen ein ISO-Image auf einer CD beziehungsweise DVD und lassen QEMU von dem Medium booten.

Der Umgang mit Speichermedien

Eine zentrale Anforderung an alle VM-Lösungen: Sie müssen auf unterschiedliche Speichermedien zugreifen können, damit die Verbindung mit Festplatten, CD-/DVD-Laufwerken oder USB-Sticks möglich ist. Die QEMU-basierten VMs verwenden anstelle von realen Festplatten

meist Image-Dateien, die im Dateisystem des Hosts angelegt sind. Der QEMU-Monitor gibt mit dem Befehl *info block* die Namen und die Zustände der verfügbaren Speichermedien aus. Wie die Ausgabe in der Praxis aussieht, ist natürlich von der aktuellen Systemkonfiguration abhängig. Eine typische Ausgabe sieht wie folgt aus:

```
(qemu) info block
ide0-hd0: type=hd removable=0
        file=os2w4.img ro=0 drv=qcow2
ide1-cd0: type=cdrom removable=1
        locked=0 file=p ro=0 drv=raw
```

Die tabellarische Übersicht führt in der ersten Spalte die Namen der Speichermedien auf. Die Ansprache der Medien erfolgt im QEMU-Monitor über die Medienbezeichnung. Mit “ide-hd” und “ide-cd” werden IDE- und DVD-/CD-Laufwerke emuliert. Der Zugriff auf (virtuelle) Festplatten erfolgt mithilfe der Optionen “-hda Image-Datei”, “-hdb Image-Datei”, “-hdc Image-Datei”, “-hdd Image-Datei” und “-drive Image-Datei”. Ersetzen Sie dabei Image-Datei durch die exakte Bezeichnung. Ein Beispiel:

```
qemu-system-x86_64 -hda fest-
platte1.img -hdb festplatte2.img
```

Wenn Sie lediglich auf eine virtuelle Festplatte zugreifen wollen, können Sie auf die Option “-hda” verzichten:

```
qemu-system-x86_64 Virtuelle_Fest-
platte.img
```

Eine weitere Besonderheit: Sie können eine Festplatte des Hosts auch dem Gast-System zur Verfügung stellen. Sie müssen dazu mit *file* den vollständigen Pfad angeben. Bei Unix-basierten Betriebssystemen wie Mac OS X und Linux finden Sie die Device-Dateien meist im Verzeichnis “/dev”.

QEMU kommt ohne eine grafische Benutzeroberfläche aus, doch gerade Windows-Nutzer vermissen diese meist sehr. Wenn Sie die Virtualisierungsumgebung unter Windows einsetzen, installieren Sie am besten den Qemu Manager [3]. Sie haben dann die Wahl zwischen beiden Varianten. Auch wenn es sich nicht um eine offizielle Komponente handelt, können Sie dieses Tool bedenkenlos einsetzen – es ist ausreichend stabil für den Einsatz in Produktivumgebungen. Um den Qemu Manager zu installieren, laden Sie sich die Installationsdatei *setupqemuk70.exe* herunter und führen den Einrichtungsassistenten mit einem Doppelklick aus.

Sie sollten die Option “Automatically check for new Qemu Manager Updates when Qemu Manager starts” aktivieren, um den Qemu Manager auf dem aktuellen Stand zu halten. Durch das Aktivieren der “Advanced Options” greifen Sie auf die erweiterten Einstellungen zurück, die dann relevant sind, wenn Sie die Windows-Variante nicht als portable Applikation auf einen USB-Stick installieren. Aktivieren Sie die Option “Install & Enable KQEMU accelerator support”, um die Ausführungsgeschwindigkeiten der VMs stark zu beschleunigen. Die Konfiguration schließen Sie mit einem Klick auf die Schaltfläche “Save & Finish” ab. Die weitere Vorgehensweise entspricht im Wesentlichen der Linux-Variante. Sie erzeugen mit einem Klick auf “Create new VM” eine neue VM-Konfiguration und weisen dieser eine Bezeichnung, einen Speicherplatz, eine Plattform und ein Betriebssystem zu. Anschließend können Sie über die Registerkarten “Hardware”, “Drives”, “Advanced”, “Console” und “Monitor” die Systemparameter definieren. Über das Icon “Add/Remove Hardware” können Sie weitere Netzwerkschnittstellen anlegen. Im Unterschied zu manch anderen VM-Lösungen erzeugt der Qemu Manager standardmäßig keinen TAP-Netzwerkadapter. Das können Sie über “Tools / Configure TAP Network Devices” nachholen. Um eine angelegte VM-Konfiguration zu starten, klicken Sie auf den Button “Launch selected VM” neben der Symbolleiste.

QEMU unter Windows



Die Boot-Reihenfolge bestimmen Sie mit der Option “-boot”. Wenn Sie mehrere Boot-Medien verwenden wollen, nutzen Sie den Parameter “order=Laufwerke”. In nachstehender Beispielkonfiguration wird zunächst versucht, von der Festplatte zu booten. Gelingt das nicht, startet der Boot-Vorgang von CD-ROM:

```
Host ~$ qemu-system-x86_64 -hda festplatte.img  
-cdrom cd.iso \  
-boot order=dc
```

Netzwerkconfiguration anpassen

Natürlich unterstützt QEMU auch Netzwerkverbindungen zwischen dem Gast- und dem Host-System. Wenn Sie mehrere VMs ausführen, können Sie quasi ein kleines Netzwerk auf einem Rechner simulieren beziehungsweise nachbilden. Um eine virtuelle Netzwerkkarte anzulegen, verwenden Sie die Option “-net nic”. In der Praxis geht das wie folgt:

```
qemu-system-x86_64 festplatte.img  
-net nic
```

Wenn Sie wissen wollen, welche virtuellen LANs QEMU zur Verfügung stehen, verwenden Sie den Befehl *info network*. Eine typische Ausgabe sieht wie folgt aus:

```
(qemu) info network  
VLAN 0 devices:  
user.0: net=10.0.2.0, restricted=n  
e1000.0: model=e1000,macaddr= 34:23:09:32:12:54
```

In diesem Beispiel ist die VM mit einem virtuellen Netzwerk (VLAN 0) verbunden. Der Instanz steht eine virtuelle Netzwerkkarte zur Verfügung.

Der Aufbau eines virtuellen Netzwerks ohne Administrator-Rechte im User Mode des Host-Rechners ist recht einfach zu realisieren. Wenn Sie QEMU ohne die Verwendung von Netzwerkooptionen beziehungsweise mit den Default-Optionen “-net nic -net user” aufrufen, erzeugt der Emulator ein virtuelles Netzwerk (10.0.2.0) mit Firewall und DHCP-Server (10.0.2.2).

Standardmäßig ordnet der DHCP-Server dem Gast-System automatisch eine IP-Adresse ab 10.0.2.15 zu. Für das Routing kommt der von QEMU bereitgestellte Gateway (10.0.2.2) zum Einsatz. In der Regel sind keinerlei Anpassungen der Netzwerkkonfiguration erforderlich und die Gast-Systeme können direkt auf das Netzwerk zugreifen. Besitzt das Host-System einen Internet-Zugang, so kann auch der Gast darauf zugreifen.

Um mehrere Netzwerkkarten mit einem Netzwerk zu verbinden, verwenden Sie den Parameter “-net nic,vlan=n”. Dazu ein Beispiel, das zwei Netzwerkkarten und zwei VLANs konfiguriert:

```
qemu-system-x86_64 festplatte.img  
-net nic,vlan=0 -net user,vlan=0 \  
-net nic,vlan=1 -net user,vlan=1
```

Login Virtual Session Indexer (Login VSI)

Tool zur Messung der Performance und Skalierbarkeit von zentralisierten Desktop-Infrastrukturen, wie Server Based Computing (SBC) und virtuellen Desktop-Infrastrukturen (VDI).



Login Solution4

Automatisierungs-Tool für das Management zentralisierter Windows-Umgebungen. Dazu zählen Software Updates sowie die Installation und Konfiguration der Anwendungen.



Log.in consultants

Specialists in desktop
deployment & virtualization

Independent • Innovative • Effective

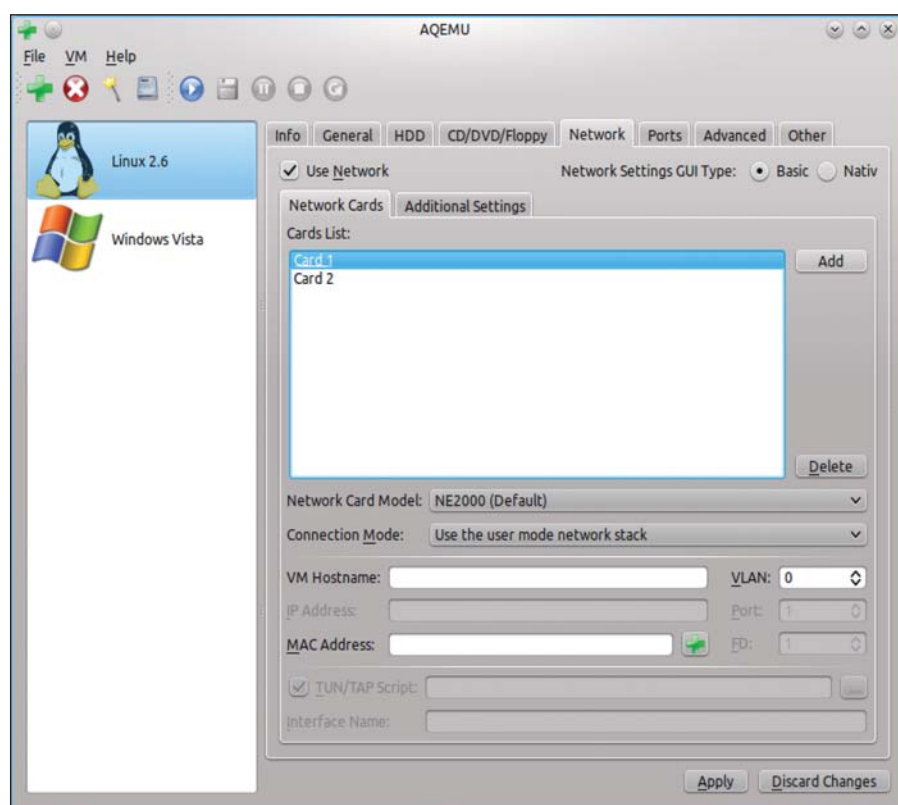


Bild 3: AQEMU vereinfacht die Verwaltung der virtuellen Maschinen und deren Netzwerkkonfigurationen

Um weitere VLANs hinzuzufügen, greifen Sie auf folgendes Kommando zurück:

```
host_net_add user vlan=1
```

Damit mehrere Gast-Systeme miteinander kommunizieren können, stellen Sie die Verbindung über einen TCP-Socket her. Dabei geben Sie die VM mit der Option “-net socket” an, wobei die Instanz auf eingehende Verbindungen auf dem angegebenen Port wartet. Der Verbindungsaufbau von der zweiten zur ersten Instanz erfolgt mit dem Befehl *connect*. Wenn zum Beispiel die zweite Instanz zur ersten eine Verbindung aufnimmt, könnte dies so aussehen:

```
qemu-system-x86_64 Platte-02.img -net
  nic,macaddr=12:32:09:32:30:22 \
-net socket,connect=127.0.0.1:port
```

Mehr Komfort dank AQEMU

Die Steuerung von QEMU auf Konsolebene ist nicht jedermanns Sache. Sie ist außerdem recht fehleranfällig. Doch es gibt Abhilfe: Mit AQEMU [2] steht Ihnen ein leistungsfähiges Frontend für Linux-Distributionen zur Verfügung. Die Paketmanager der gängigsten Linux-Va-

rianten stellen AQEMU zur einfachen Installation bereit. Das Programm bietet beim Handling von VMs und deren Konfiguration den Komfort, den Nutzer beispielsweise von Virtualbox kennen.

Um eine erste VM anzulegen, klicken Sie auf das Wizard-Zeichen. Es meldet sich der Einrichtungsassistent, in dem Sie die Eigenschaften der VM bestimmen. AQEMU stellt Ihnen mehrere Templates für Windows-, Linux- und BSD-Versionen zur Verfügung. In Folgeschritten bestimmen Sie die Festplattengröße und Netzwerkunterstützung. AQEMU besitzt eine zweigeteilte Benutzerschnittstelle: Links finden Sie die Spalte der angelegten VM-Instanzen, rechts die dazugehörigen Einstellungen. Für die Konfiguration der VM stehen Ihnen sieben Registerkarten zur Verfügung.

Die Registerkarte “Info” umfasst verschiedene allgemeine Informationen zu der ausgewählten VM, beispielsweise den Status, den CPU-Typ und die Größe des Arbeitsspeichers. Auf der Registerkarte “General” können Sie verschiedene dieser Einstellungen ändern, um beispielsweise eine andere Rechnerarchitektur

und eine andere RAM-Konfiguration zu verwenden.

Die Netzwerkkonfiguration können Sie mithilfe der Einstellungen der Registerkarte “Network” ändern. Die Netzwerkkonfiguration ist auf zwei Registerkarten verteilt: “Network Cards” und “Additional Settings”. Sie können unter Network Cards eine oder mehrere Netzwerkkarten konfigurieren und sogar den jeweiligen Kartentyp und die Verbindungsart anpassen. Auf dem Unterregister “Additional Settings” konfigurieren Sie die Port-Umleitung, ein TFTP-Präfix und ein Samba-Share.

Um eine VM-Konfiguration zu starten, klicken Sie einfach auf das Start-Symbol. Die Steuerung von QEMU wird so mithilfe von AQEMU zum Kinderspiel. Das Tool unterstützt alle wichtigen QEMU-Funktionen und vereinfacht den Umgang mit VMs ganz erheblich.

QEMU für Fortgeschrittene

Der Emulator bietet eine Fülle von erweiterten Anwendungsmöglichkeiten. Eine der interessantesten ist die bereits erwähnte Live-Migration, bei der VMs im laufenden Betrieb von einem Host-System auf ein anderes übertragen werden. Um eine reibungslose Migration sicherstellen zu können, sollten die Quell- und Ziel-Hosts über die gleiche Hardware-Architektur verfügen. Außerdem müssen beide das gleiche Netzwerksegment verwenden.

Um eine Live-Migration durchzuführen, sind drei Schritte notwendig. Zunächst muss eine Instanz auf dem Quell-Host

[1] QEMU Disk Images zum Testen
C5P31

[2] Grafische Oberfläche AQEMU
C5P32

[3] Qemu Manager
C5P33

Weiterführende Links:

Umfassende Dokumentation zu QEMU
C5P34

Link-Codes



betrieben werden. Dann starten Sie auf dem Ziel-Host eine Instanz mit den identischen Optionen, wie sie der Quell-Host aufweist. Dabei müssen Sie zusätzlich die Option “-incoming tcp:ip:port” verwenden. “ip” bestimmt die Ziel-IP-Adresse der Migration, “port” den Ziel-Port. Die Instanz auf dem Ziel-Host wartet quasi in eingefrorenem Zustand auf die zu migrierende Quell-Instanz.

Die eigentliche Migration starten Sie im QEMU-Monitor des Quell-Hosts mit folgendem Befehl:

```
migrate -d tcp: IP-Adresse:Port
```

Sind alle Rahmenbedingungen für eine erfolgreiche Migration gegeben, wird die Quell-Instanz eingefroren und Sie können auf dem Zielsystem mit der migrierten VM arbeiten. Auch die Umleitung des QEMU-Monitors ist möglich, um die Steuerkommandos auf einem Device Ihrer Wahl auszuführen. Standardmäßig wird der QEMU-Monitor auf der zweiten Konsole der VM-Instanz betrieben. Für das Umschalten verwenden Sie die Tastenkombination “Strg” + “Alt” + “2”.

Für die Umleitung des QEMU-Monitors verwenden Sie die Option “-monitor”, gefolgt von der Konfiguration des Ziel-Device. Wenn Sie die Ausgabe auf die Standardein- und -ausgabe des Host-Systems umleiten wollen, verwenden Sie die Option “stdio”. Konkret gestaltet sich dies folgendermaßen:

```
qemu-system-x86_64 festplatte.img  
-monitor stdio
```

Zudem ist das Umleiten des QEMU-Monitors auf einen Port des Host-Systems möglich. Sie können den Monitor beispielsweise auf dem Hostsystem verwenden. Der Zugriff erfolgt dabei über Telnet. Der entsprechende Befehl kann wie folgt aussehen:

```
qemu-system-x86_64 festplatte.img  
-monitor tcp::8000,server
```

QEMU unterstützt Tracing, also das Verfolgen von Programmausführungen. Dies setzt allerdings voraus, dass die Option “--trace-backend” beim Kompilieren verwendet wurde. Standardmäßig ist das nicht der Fall.

Um die Trace-Events auf die Standard-Fehlerausgabe auszugeben, verwenden Sie die Option “--trace-backend=stderr”. Sie können auch das dynamische Verfolgen mit “--trace-backend=dtrace” aktivieren.

Fazit

QEMU ist eine der interessantesten Virtualisierungslösungen der Open Source-Gemeinde. Sie ist dank der hervorragenden Performance manch kommerziellen Produkten überlegen. Gerade Administratoren werden die vielen Möglichkeiten schätzen, die sich über die konsolenbasierte Steuerung bieten. (In) 



EXPERTeatch



Cisco Zertifizierungen mit Termingarantie!



Associate Level

CCENT – Kurs ICND1

CCNA – Kurse ICND1 + ICND2

CCNA Voice – Kurse ICND1 + ICND2 + ICOMM

CCNA Security – Kurse ICND1 + ICND2 + IINS

CCNA Wireless – Kurse ICND1 + ICND2 + IUWNE

CCDA – Kurse ICND1 + ICND2 + DESGN



Professional Level

CCNP – Kurse ROUTE + SWITCH + TSHOOT

CCNP Voice – Kurse CVOICE + CIPT1 + CIPT2 + TVOICE + CAPPs

CCNP Security – Kurse SECURE + FIREWALL + IPSv7 + VPN

CCDP – Kurse ROUTE + SWITCH + ARCH

... und alles mit garantierten Kursterminen! 



Fordern Sie unseren
aktuellen Trainingskatalog an!
Tel. 06074 4868-0

Zentrale Datensicherung mit Bacula

Verlässlicher Datensauger

von Dr. Holger Reibold



Mit den Themen Datensicherheit und Sicherung wollen sich nach wie vor nur die wenigsten Mitarbeiter befassen – und zwar quer durch die gesamte Unternehmenshierarchie. Doch es gibt professionelle Lösungen wie Bacula, mit denen Sie als IT-Verantwortlicher dieses leidige Thema endlich ad acta legen können. Zu Unrecht fristet Bacula dabei ein Mauernblümchendasein, denn die Software ist eine ausgesprochen flexible und leistungsfähige Backup-Lösung, die keine Wünsche offenlässt.

Bacula basiert auf verschiedenen Komponenten, die miteinander interagieren. Die zentralen Komponenten der Umgebung sind

- Catalog-Datenbank, etwa PostgreSQL
- Director (bacula-dir)
- Storage-Daemon (bacula-sd)
- File-Daemon (bacula-fd)
- Konsole
- Monitor

Wie Sie in dem tabellarischen Vergleich von Bacula mit anderen überwiegend kommerziellen Produkten [1] sehen, steht das freie System kommerziellen Lösungen funktional in nichts nach. Das einzige Manko von Bacula: Bislang ist noch kein Mechanismus für die Sicherung von Oracle-Datenbanken integriert. Das ist momentan nur über von der Bacula-Community bereitgestellte Skripte möglich.

Bacula wurde für den Einsatz in komplexen, verteilten und heterogenen Umgebungen entwickelt. Aus diesem Grund besitzt Bacula eine flexible, modulare Architektur, bei der die verschiedenen Komponenten verteilt werden und nicht auf einem zentralen Server ausgeführt werden müssen. Das kommt Unternehmen entgegen, die mehrere Standorte besitzen, denn sie können die einzelnen Bacula-Komponenten unter den Gesichtspunkten der Performance und Redundanz auf diese Standorte verteilen. Die Kommunikation der einzelnen Komponenten erfolgt über TCP/IP.

Die Schaltzentrale von Bacula nennt sich Director, die von dem Dienst "bacula-dir" bereitgestellt wird. Er steuert alle Vorgänge, die die Sicherung, Wiederherstellung und Überprüfung der Daten betreffen. Der Director ist auch für die Ausführung zeitgesteuerter Aufträge verantwortlich. Eine weitere wichtige Aufgabe: Das Management von Medienpools und die Steuerung der einzelnen Datei- und Speicher-Daemons. Die Steuerung des Directors erfolgt über die Bacula Console, auch "bconsole" genannt.

Daemons am Werk

Im sogenannten Bacula-Katalog wird die gesamte Logik der Backup-Lösung dargestellt. Dabei handelt es sich um ein Datenbanksystem, das mehrere Aufgaben übernimmt. In der Datenbank werden der Dateiindex der gesicherten Dateien und die gesamten Sicherungs-Volumes verwaltet. Aktuell unterstützt Bacula folgende Datenbanken: MySQL, PostgreSQL und SQLite. Der Katalog übernimmt eine weitere wichtige Aufgabe: Er dient dem Auffinden und der Wiederherstellung einzelner Backup-Dateien. Für die eigentliche Sicherung der Daten sorgt der Storage-Daemon. Seine wichtigste Aufgabe ist das Schreiben und Lesen der Backup-Daten auf den Datenträgern. Bacula ist bezüglich der zu verwendenden Sicherungsmedien sehr flexibel. Sie können Ihre Daten auf Festplatte, CD- und DVD-Laufwerken, Bandlaufwerken und auch Tape-Bibliotheken speichern.

Im Bacula-System interagieren die verschiedenen Daemons miteinander. So auch der Storage- und der File-Daemon (bacula-fd). Der Storage-Daemon wird beispielsweise von dem File-Daemon mit den zu sichernden Dateien versorgt. Er muss überall dort installiert sein, wo Sie Daten sichern wollen. In der Praxis können Sie mehrere Storage-Server aussetzen und so die Sicherungslast auf verschiedene Schultern verteilen. Damit der Storage-Daemon mit den Informationen über zu sichernde Daten gefüttert werden kann, muss er die entsprechenden Informationen vom File-Daemon beziehen. Dieser wird auf allen Clients ausgeführt, deren Daten vom Bacula-System gesichert werden sollen. Das bedeutet natürlich, dass Sie auf jedem Netzwerk-Client, dessen Daten es zu sichern gilt, einen File-Daemon installieren müssen.

Bacula unterstützt in der aktuellen Version insbesondere alle relevanten Desktop-Betriebssysteme, neben Linux und diversen Unix-Derivaten (darunter FreeBSD, OpenBSD, NetBSD, BSDi, Solaris, Mac OS X, AIX, Tru64 sowie HP-UX) auch die verschiedenen Windows-Varianten. Dank der Unterstützung von Microsofts Volume Shadow Copy Service kann Bacula auch geöffnete Dateien und Datenbankdateien sichern. Das Sicherungsprinzip ist einfach: Der File-Daemon liest die Dateien von der Client-Festplatte und transferiert die zu sichernden Daten an den Storage-Daemon.



Schließlich benötigen Sie noch ein Tool, mit dem Sie den Bacula Director steuern. Das ist Aufgabe der Bacula Console. Wie anhand der Bezeichnung dieser Komponente unschwer zu erkennen ist, steht Ihnen hierfür eine typische Konsole zur Verfügung, mit der Bacula auf Terminalebene verwaltet wird. Als Administrator sind Sie allerdings keineswegs nur auf die konsolenbasierte Administration beschränkt, sondern Sie können auf verschiedene grafische Frontends zurückgreifen. Diese GUIs sind insbesondere für Linux und Windows verfügbar. Mit "bweb" steht Ihnen beispielsweise eine komfortable webbasierte Oberfläche zur Verfügung, über die Sie alle wichtigen Aktionen und Kommandos auslösen können. Auch das Monitoring der gesamten Bacula-Umgebung ist mit bweb möglich. Für Windows-Anwender gibt es mit dem Bacula Administration Tool (BAT) eine ausgesprochen komfortable Lösung, mit der Sie ebenfalls alle wichtigen Backup-Aufgaben erledigen können. Eine weitere sehr komfortable GUI ist Webacula.

Bacula in Betrieb nehmen

Bevor Sie sich an die Installation von Bacula machen, sind verschiedene Vorarbeiten zu leisten. Wenn Sie mit Debian arbeiten, führen Sie dazu folgenden Befehl aus:

```
# aptitude install build-essential
libpq-dev libncurses5-dev libssl-
dev psmisc
```

Bei alternativen Linux-Systemen verwenden Sie den Paketmanager für die Suche und Installation der entsprechenden Pakete.

Wie erwähnt, kann Bacula mit verschiedenen Datenbanksystemen zusammenspielen, genauer mit MySQL, PostgreSQL und SQLite. In diesen Datenbanken werden etwa alle Managementdaten verwaltet, die Bacula während eines Backup- beziehungsweise Wiederherstellungsvorgangs generiert. Besonders gut funktioniert das Zusammenspiel erfahrungsgemäß mit PostgreSQL. Also benötigen Sie noch eine PostgreSQL-Installation. Dazu führen Sie den Befehl `aptitude install postgresql` aus. Als Nächstes ist die Installation des Bacula-Servers dran. Der Einfachheit halber installieren Sie bei einer ersten Testinstallation alle Bacula-Komponenten auf einem

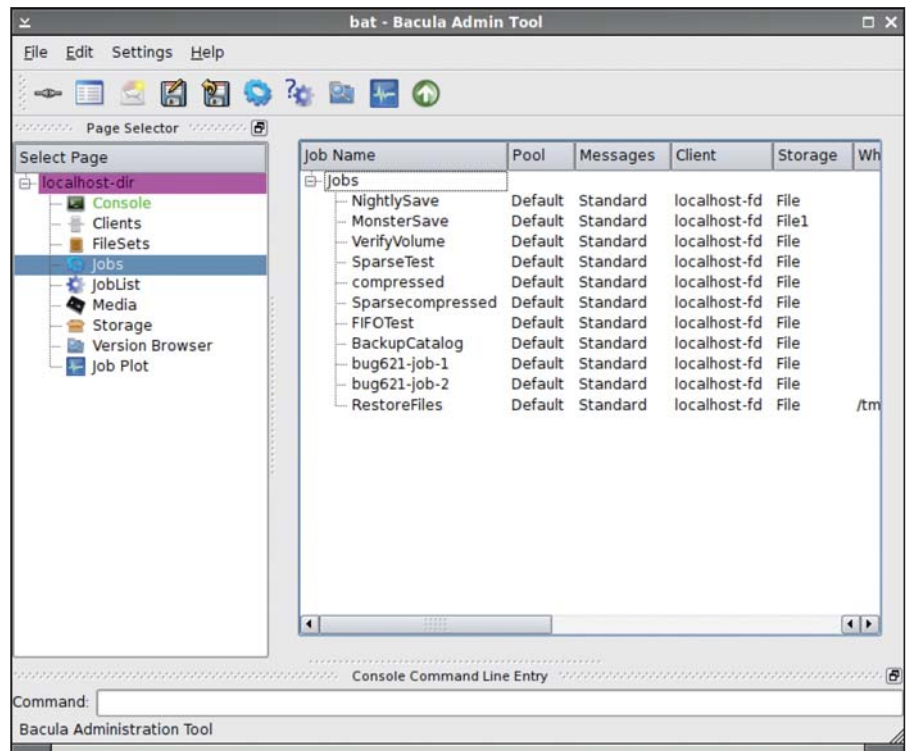


Bild 1: Mit dem Bacula Administration Tool gibt es eine komfortable GUI für Bacula, die etwa das Anlegen von Sicherungs-Jobs erlaubt

System, also den Director, den Storage-Daemon und den lokalen File-Daemon. Laden Sie sich zunächst das Installationspaket herunter:

```
# cd /usr/local/src
# wget http://sourceforge.net/
  projects/bacula/files/
  bacula-5.2.3/Bacula-5.2.3.tar.gz
# tar xzvf bacula-5.2.3.tar.gz
# rm bacula-5.2.3.tar.gz
```

Sie sollten lediglich darauf achten, dass Sie die aktuellste Version verwenden. Nach dem Download wechseln Sie in das Projektverzeichnis `/usr/local/src/bacula-5.2.3` und generieren die Makefiles:

```
# cd bacula-5.2.3
# ./configure --prefix=/usr --sbin-
  dir=/usr/sbin --sysconfdir=/etc/
  bacula --with-scriptdir=/etc/bacula
  --enable-smartalloc --enable-conio
  --with-postgresql --with-openssl
  --with-dir-user=bacula --with-dir-
  group=bacula --with-sd-user=bacula
  --with-sd-group=bacula --with-fd-
  user=root --with-fd-group=bacula
  --with-working-dir=/var/lib/bacula
  --with-pid-dir=/var/run --with-
  subsys-dir=/var/run/subsys
```

Wurde das Configure-Skript fehlerfrei ausgeführt, erfolgt die Ausgabe einer entsprechenden Statusmeldung. Für die eigentliche Installation des Bacula-Servers führen Sie den Befehl `make && make install` aus. Die nächsten Schritte dienen dem Erstellen der benötigten PostgreSQL-Datenbank. Die Bacula-Installation legt automatisch verschiedene Datenbank-Skripts an, die Sie für das Initialisieren der Datenbank verwenden:

```
# cd /etc/bacula
# chown postgres:postgres create_
  bacula_database create_post-
  gresql_database make_bacula_tables
  make_postgresql_tables grant_
  bacula_privileges grant_post-
  gresql_privileges drop_bacula_
  tables drop_postgresql_tables
  drop_bacula_database drop_post-
  gresql_database
# su postgres
$ ./create_bacula_database
```

Das Datenbanksystem gibt anschließend folgende Statusmeldung aus:

```
Creating PostgreSQL database
CREATE DATABASE
ALTER DATABASE
```



Creation of bacula database succeeded.

Die weitere Ausführung erfolgt mit den Befehlen

```
$ ./make_bacula_tables
```

Creation of Bacula PostgreSQL tables succeeded.

```
$ ./grant_bacula_privileges
```

Privileges for bacula granted on bacula.

Nach dem Abschluss der Initialisierung der PostgreSQL-Datenbank "bacula" legen Sie noch den Datenbankbenutzer "bacula" an mit `$ psql bacula`. In der PostgreSQL-Konsole weisen Sie diesem ein Passwort zu:

```
bacula=# alter user bacula with password Passwort;
```

Zwei weitere datenbankspezifische Aktionen sind noch erforderlich: die Anpassung der Zugriffs-Policy und ein Neustart des Datenbanksystems. Verlassen Sie dazu zunächst die PostgreSQL-Konsole mit `bacula=# \q`. Dann müssen Sie die Konfigurationsdatei `etc/postgresql/9.0/main/pg_hba.conf` anpassen, damit der Benutzer "bacula" beim Zugriff auf die Datenbank authentifiziert wird. Das geschieht mit folgendem Eintrag:

```
local bacula bacula md5
```

Um PostgreSQL neu zu starten, führen Sie den Befehl `/etc/init.d/postgresql-9.0 restart` aus.

Bacula flexibel konfigurieren

Bacula ist eine außergewöhnlich flexible und an nahezu jede Infrastruktur anpassbare Backup-Lösung. Der Preis für diese Flexibilität ist eine hohe Komplexität, die wiederum vom Administrator eine gewisse Einarbeitungszeit verlangt. Die Konfiguration des Bacula-Systems basiert auf der Anpassung der vier Komponenten, die jede über eine eigene Konfiguration verfügt:

- Konfigurationsdatei des Directors: `/etc/bacula/bacula-dir.conf`
- Konfigurationsdatei des Storage-Daemons: `/etc/bacula/bacula-sd.conf`

- Konfigurationsdatei des File Daemons: `/etc/bacula/bacula-fd.conf`
- Konfigurationsdatei der Console: `/etc/bacula/bconsole.conf`

Schauen wir uns zunächst die Konfiguration des Directors an. Er koordiniert alle Aktionen des Systems – also die Durchführung von Backups und Restores oder die Validierung der Backups. Aufgrund der vielfältigen Aufgaben des Directors fällt seine Konfiguration recht komplex aus. Um die Director-Konfiguration zu bearbeiten, editieren Sie die Konfigurationsdatei `/etc/bacula/bacula-dir.conf`. Im Kopfbereich erfolgt die Definition des Directors. Die sieht typischerweise wie folgt aus:

```
# Konfiguration des Directors
Director {
    Name = bacula.server.de
    Dirport = 9101
    QueryFile = "/etc/bacula/query.sql"
    WorkingDirectory = "/var/lib/bacula"
    PidDirectory = "/var/run"
    Maximum Concurrent Jobs = 1
    Password = "geheimes_passwort"
    Messages = Daemon
}
```

In der Konfigurationsdatei definieren Sie auch den Bacula-Katalog, in dem unter anderen die Metadaten der zu sichernden Dateien hinterlegt sind. Eine einfache Konfiguration könnte wie folgt aussehen:

```
# Catalog-Konfiguration
Catalog {
    Name = Meinsicherungskatalog
    dbname = "bacula"; dbuser = "bacula"; dbpassword = "Datenbank-Passwort"
}
```

Der nächste Schritt dient dem Anlegen eines Medien-Pools, der als Schnittstelle für den eigentlichen Schreib- und Lesezugriff auf die Backup-Medien dient. Das Anlegen eines solchen Pools in der Director-Konfigurationsdatei `/etc/bacula/bacula-dir.conf` ist einfach:

```
# Die Konfiguration des Medien-Pools
Pool {
```

```
    Name = MedienPool
    LabelFormat = "BackupVol"
    Pool Type = Backup
    Recycle = yes
    AutoPrune = yes
    Volume Retention = 365 days
}
```

Im nächsten Schritt müssen Sie das Storage-Device anlegen. Die Verbindungsaufnahme zu dem lokalen Storage-Daemon ist recht einfach zu realisieren, da Bacula auf einem System ausgeführt wird.

```
# Die Konfiguration des Storage-Daemons
Storage {
    Name = File
    Address = bacula.server.de
    SDPort = 9103
    Password = "GeheimesPasswort"
    Device = FileStorage
    Media Type = File
}
```

Als Nächstes steht die Konfiguration der Clients an. Wir beschränken uns hier auf einen Client, dessen Daten Bacula sichern soll. Eine simple Client-Konfiguration legen Sie wie folgt an:

```
# Einfache Client-Konfiguration
Client {
    Name = client
    Address = client.server.de
    FdPort = 9102
    Catalog = Meinsicherungskatalog
    Password = "GeheimesPasswort"
    File Retention = 30 days
    Job Retention = 6 months
    AutoPrune = yes
}
```

Der nun folgende Schritt dient dem Anlegen des sogenannten File-Sets. Damit bestimmen Sie, welche Client-Daten gesichert werden sollen. Wir legen lediglich eine Client-Konfiguration an, bei der das gesamte Root-Filesystem bis auf die beiden nicht benötigten Verzeichnisse `/tmp` und `/proc` gesichert wird. Die entsprechende Konfiguration könnte wie folgt aussehen:

```
# Dateiliste der zu sichernden Dateien
```



```
FileSet {
  Name = "Full Set"
  Include {
    Options {
      signature = MD5
    }
    File = /
  }
  Exclude {
    File = /tmp
    File = /proc
  }
}
```

Nun benötigt Ihre Sicherungskonfiguration natürlich noch einen Zeitplan, der die zeitliche Ausführung des Backups steuert. Eine wöchentliche Sicherung definieren Sie folgendermaßen:

```
# Backup-Zeitplan
Schedule {
  Name = "wöchentlich"
  Run = Full 1st sat at 0:00
  Run = Differential 2nd-5th sat at 0:00
  Run = Incremental mon-sat at 1:00
}
```

Professionelle Backup-Werkzeuge unterstützen verschiedene Backup-Arten, die Sie auch mit Bacula nutzen können:

- vollständig: Bei diesem Typ wird eine vollständige Sicherung erzeugt.
- differenziell: Bei dieser Variante werden lediglich die Dateien gesichert, die sich seit dem letzten vollständigen Backup verändert haben.
- inkrementell: Die dritte Variante sichert alle Dateien, die sich seit dem letzten Backup geändert haben, und zwar unabhängig von der Art des Backups.

In der Praxis hat sich folgendes Backup-Schema etabliert und dürfte die Anforderungen in den meisten Unternehmen und Infrastrukturen abdecken:

- Jeden ersten Samstag und/oder Sonntag im Monat wird eine Vollsicherung durchgeführt.
- Jeden zweiten, dritten und vierten Samstag und/oder Sonntag im Monat wird ein differenzielles Backup durchgeführt.
- Täglich außer Sonntag wird ein inkrementelles Backup gestartet.

Vollsicherungen führen in der Regel zu einer extrem hohen Netzwerklast. Da samstags und sonntags in den meisten Betrieben nicht gearbeitet wird, führen IT-Verantwortliche diese am Wochenende aus.

Das optimale Backup-Schema



Sind der Medien-Pool, der Storage-Daemon, der oder die Clients, das File-Set und die Zeitsteuerung angelegt, ist die Grundkonfiguration abgeschlossen und Sie können sich im nächsten Schritt dem eigentlichen Sicherungs-Job zuwenden. Für das Anlegen, Bearbeiten und Verwalten von Sicherungs-Jobs stellt Ihnen Bacula eine weitere interessante und zeitsparende Funktion zur Verfügung: Sie können Job-Charakteristika in Templates zusammenfassen.

Konfiguration eines Sicherungsjobs

Als Nächstes können Sie sich der Konfiguration des Storage-Daemons und der weiteren Daemons zuwenden. Um den Storage-Daemon zu konfigurieren, editieren Sie die Konfigurationsdatei `/etc/bacula/bacula-sd.conf`. Hier bestimmen Sie insbesondere das Zielverzeichnis, in dem die zu sichernden Dateien abgelegt werden. Nachstehende Konfiguration verwendet das Verzeichnis `/bacula_ordner`:

```
Storage {
  Name = client1.server.de
  SDPort = 9103
  WorkingDirectory = "/var/lib/bacula"
  Pid Directory = "/var/run"
  Maximum Concurrent Jobs = 20
}
```

```
Director {
  Name = bacula.server.de
  Password = "geheimesPasswort"
}
```

```
Device {
  Name = FileStorage
  Media Type = File
  Archive Device =
    /backup_ordner
  LabelMedia = yes;
  Random Access = yes;
  AutomaticMount = yes;
  RemovableMedia = no;
  AlwaysOpen = no;
}
```

```
Messages {
  Name = Standard
  director = bacula.server.de = all
}
```

Wichtig ist dabei, dass das verwendete Passwort dem der Storage-Definition in der Director-Konfigurationsdatei entspricht.

Die Konfiguration des File-Daemon erfolgt in der Konfigurationsdatei `/etc/bacula/bacula-fd.conf` auf den Clients, deren Daten Sie sichern wollen. Hier sind insbesondere die Informationen über den Director hinterlegt. Sie sollten den File-Daemon auch auf dem Sicherungs-server installieren, um die Katalogdatenbank des Backup-Servers zu sichern. In der Console-Konfigurationsdatei sind kaum Anpassungen erforderlich. Hier muss insbesondere der Director konfiguriert werden.

Damit ist das Bacula-Basissystem einsatzbereit und Sie müssen nun noch die Clients auf den zu sichernden Rechnern installieren. Bevor Sie erste Sicherungen durchführen, sollten Sie Ihre Installation auf die Funktionstüchtigkeit hin überprüfen. Auch hierfür stellt Ihnen Bacula das entsprechende Werkzeug zur Verfügung. Rufen Sie auf Konsolenebene die `bconsole` mit `bconsole` auf. Das Tool sollte ein Prompt ausgeben, der in etwa wie folgt aussieht:

```
Connecting to Director local-
host:9101
1000 OK: backup-dir version: 5.2.3
Enter a period to cancel a command.
*
```

Sie können Ihre Installation mit verschiedenen `bconsole`-Kommandos prüfen. Der Befehl `list clients` gibt beispielsweise alle in der Director-Konfiguration definierten Clients aus. Mit `status client` rufen Sie den Status der einzelnen Clients ab. Unter [3] finden Sie Informationen, wie Sie den Bacula-Status per E-Mail und SMTP-Authentifizierung abfragen. (dr)



- [1] Vergleich von Bacula mit anderen Produkten C4P71
- [2] Bacula Webseite C4P72
- [3] Bacula-Status per E-Mail abfragen C4P73

Link-Codes





Neuerungen in Citrix XenDesktop 5.5 und Provisioning Services 6.0

Desktops griffbereit

von Christian Knernmann

Mit Version 5.5 von XenDesktop setzt Citrix die Entwicklung der hauseigenen Infrastruktur-Lösung zur Bereitstellung virtueller Desktops fort. Brachte der Vorgänger 5.0 tiefgreifende Änderungen an der Architektur mit sich, konzentriert sich die neue Version primär auf die Optimierung des Bedienkomforts. Doch auch unter der Haube haben die Provisioning Services 6.0 Verbesserungen bei der Verwaltung der Desktop-Images im Gepäck. IT-Administrator stellt Ihnen die Neuerungen vor.

Die oberste Verwaltungseinheit einer XenDesktop-Infrastruktur ist die sogenannte Site. Eine Site fasst mehrere Virtualisierungshosts oder Pools von Hosts zusammen, die Desktop-VMs bereitstellen. Dabei kann es sich um Citrix XenServer, VMware vSphere oder Microsoft Hyper-V-Systeme handeln. Gleichartige Desktops werden zu Catalogs zusammengefasst, die wiederum mittels einer Desktop Group auf einzelne Benutzer oder Gruppen im Active Directory abgebildet werden.

Zentrales Element einer Site ist der Desktop Delivery Controller (DDC), der die virtuellen Desktops erzeugt, verwaltet und direkte Client-Verbindungen zu den VMs über das ICA-Protokoll vermittelt. Der DDC speichert die Konfiguration der Site in einer Datenbank, die im einfachsten Fall in Form eines Microsoft SQL Server Express lokal auf dem DDC residiert. Es ist möglich, mehrere DDC redundant zu installieren. In diesem Fall empfiehlt es sich, die Datenbank auf einen separaten SQL-Server auszulagern. Auf dem Datenbank-Server muss mindestens SQL Server 2008 SP2 zum Einsatz kommen [1]. Zur grundlegenden Verwaltung von Catalogs und Desktop Groups innerhalb

der Site dient das MMC-basierende Desktop Studio. Ferner existiert mit dem Desktop Director ein Webinterface, das zwar keine tiefgreifenden Veränderungen innerhalb der Site erlaubt; es verschafft dem IT-Support aber eine einfache Übersicht darüber, welche Benutzer mit welchen Desktops verbunden sind und welche Features des ICA-Protokolls die jeweilige Verbindung unterstützt.

XenDesktop in drei Editionen

XenDesktop ist in drei Editionen mit unterschiedlichem Funktionsumfang erhältlich. Mit der "VDI Edition" sind ausschließlich Verbindungen zu VM-basierten, gehosteten Desktops möglich. Die "Enterprise Edition" beinhaltet zahlreiche weitere Funktionen, darunter die Provisioning Services (PVS). Diese ermöglichen es, aus einem oder mehreren "Golden Images" Desktops sowohl auf physische als auch auf virtuelle Maschinen zu streamen, mehr dazu später. Zudem ist die Terminalserver-Infrastruktur XenApp enthalten. Somit ist es beispielsweise möglich, ein gemeinsames Basis-Image für alle Benutzer zu pflegen und Spezial-Anwendungen, die nur von wenigen Usern benötigt werden, im Backend über Ter-

minalservers bereitzustellen oder mittels Anwendungsvirtualisierung direkt an die Desktop-VMs zu streamen.

Hinzu kommt mit HDX 3D Pro eine Erweiterung für das ICA-Protokoll, mit der Hochleistungsgrafik auch auf virtuellen Desktops Einzug hält. Diese Funktion benötigt allerdings Hardware-Unterstützung in Form von Nvidia GPUs auf der Serverseite. Die Liste der von Citrix getesteten Chips und Komplettsysteme ist noch relativ kurz [2]. Es sind zwei Varianten möglich: Wahlweise installieren Sie ein Desktop-Betriebssystem direkt auf einem physischen Rechner, dessen GPU mitgenutzt wird. Alternativ verwenden Sie einen Virtualisierungshost mit einer oder mehreren Nvidia-GPUs. Dieser Ansatz setzt Citrix XenServer 6.0 als Hypervisor voraus, der die GPUs an einzelne Desktop-VMs durchreicht. HDX 3D Pro nutzt die GPU, um die Grafikinhalte serverseitig zu rendern, in einen H.264-Videostrom zu verpacken und diesen dann an den Client zu streamen. Neben dem Citrix Receiver ist auf dem Client somit lediglich ein H.264-Codec erforderlich, um in den Genuss hochperformanter Grafik zu kommen.



Schließlich beinhaltet die "Platinum Edition" weitere Komponenten wie Citrix EdgeSight für das Monitoring der Services bis hin zum Endgerät. Hinter dem Feature "HDX Smart Access" verbirgt sich der SSL-gesicherte Zugriff über das Citrix Access Gateway von extern. Über die ebenfalls enthaltene Branch Repeater VPX Virtual Appliance und den Branch Repeater Software-Client kann zudem der Zugriff über WAN-Verbindungen optimiert werden. Da jede dieser Erweiterungen jedoch den Rahmen dieses Artikels sprengen würde, konzentrieren wir uns im Folgenden auf die PVS, die ab der Enterprise Edition enthalten sind.

Installation vom ISO-Image

Als Workshop-Umgebung nutzen wir eine Active Directory-Domäne unter Windows Server 2008 R2 sowie einen XenServer-Pool. Darin installieren wir zunächst eine Windows Server 2008 R2-VM als Basis für unseren DDC. Die XenDesktop ISO-Images laden Sie von der Citrix-Download-Seite [3] herunter. Der komplette Umfang der Enterprise Edition steht dort als knapp 19 GByte großes Zip-Archiv bereit. Dieses enthält sämtliche Komponenten, darunter auch XenApp 5 for Windows Server 2003, den XenClient sowie den XenServer. Wir beschränken uns darauf, aus dem Bereich der "Custom Downloads" nur die Komponente zu wählen, die wir für unseren Workshop unmittelbar benötigten, nämlich das Zip-Archiv "Delivery Controller and Additional Components".

Das ISO-Image mit dem Setup des DDC weisen Sie nun Ihrer Server-VM zu, starten die Installationsroutine und wählen die Option "Install XenDesktop". Die Installation verläuft analog zum Setup von XenDesktop 5.0, dem wir uns bereits in einem Test gewidmet haben [4]. Nach dem Abnicken der Lizenzbestimmungen wählen Sie in einem ersten Schritt die gewünschten Komponenten aus. Hier sind standardmäßig sämtliche Punkte aktiviert. Wir belassen es bei dieser Auswahl und akzeptieren alle Komponenten mitsamt SQL Server Express. Der Assistent erstellt daraufhin die nötigen Regeln für die Windows Firewall, erfüllt automatisch die noch fehlenden Voraussetzungen und installiert schließlich die XenDesktop-Dienste. Daraufhin startet das

Desktop Studio, in dem Sie mit der Option "Desktop deployment" zunächst die Basis-konfiguration einer neuen Site vornehmen.

Für unseren Workshop konfigurieren wir eine Site namens "Oberhausen", die die "Default database" nutzen soll. Dies bedeutet, dass der DDC automatisch nach einer lokalen SQL-Instanz sucht und anbietet, die Datenbank neu zu erstellen, sofern er keine vorhandene findet. Im nächsten Dialogschritt geben Sie den Lizenzserver an. Wir verwenden hier einen bereits vorhandenen Lizenzdienst unserer Umgebung, auf dem wir Eval-Lizenzen für XenDesktop Enterprise bereits im Vorfeld eingerichtet haben. Abschließend ist die Hosting-Infrastruktur zu wählen. Zur Auswahl stehen hier "Citrix XenServer", "Microsoft virtualization", "VMware virtualization" oder "None". Wir entscheiden uns für die erste Option und konfigurieren die Adresse unseres Pool-Masters sowie die Anmeldeinformationen für die Hosting-Infrastruktur. Abschließend wählen wir die Option, neue virtuelle Maschinen manuell zu erzeugen und dies nicht dem DDC zu überlassen, da wir die nötigen Schritte auf den Hosts und den Provisioning Servern selbst durchführen möchten. Damit ist die initiale Konfiguration der Site abgeschlossen und wir können uns dem Punkt "Machine creation" zuwenden.

Passenden Desktop auswählen

Der erste Schritt auf dem Weg zu einem Desktop Catalog besteht in der Auswahl des gewünschten Typs. Zur Auswahl stehen hier die folgenden fünf Optionen:

- Pooled: In diesem Fall kümmern sich die Machine Creation Services (MCS) um die Verwaltung der virtuellen Desktops. Die Variante "Random" weist jedem Benutzer bei jeder Anmeldung wahlfrei eine beliebige VM aus dem Pool zu. Die Variante "Dedicated" ordnet dem Benutzer bei der ersten Anmeldung eine VM fest zu, mit der er zukünftig immer verbunden wird. In beiden Fällen wird die Maschine nach Abmeldung des Anwenders auf ihren ursprünglichen Zustand zurückgesetzt.
- Dedicated: Auch in diesem Fall werden die virtuellen Desktops durch die MCS erzeugt und verwaltet. Änderungen, die die Endanwender an der VM vornehmen, bleiben aber dauerhaft erhalten.

- Existing: Dieser Typ integriert bereits vorhandene VMs, die nicht von den MCS oder den Provisioning Services aus einem gemeinsamen Image erzeugt werden. Die VMs sind somit mit anderen Methoden einzeln zu pflegen. XenDesktop kann aber zumindest den jeweiligen Hypervisor veranlassen, die Maschinen je nach Bedarf zu booten oder herunterzufahren.
- Physical: Mit diesem Typ vermittelt XenDesktop ICA-Verbindungen zu beliebigen physischen Maschinen. XenDesktop kann diese darüber hinaus aber weder verwalten noch herauf- oder herunterfahren.
- Streamed: Dieser Typ integriert Desktops, die mittels der Citrix Provisioning Services (PVS) erzeugt und verwaltet werden.

Da XenDesktop mit MCS und PVS gleich zwei Wege anbietet, um mehrere Desktops aus einem gemeinsamen Golden Image zu erzeugen, erläutern wir zunächst die Unterschiede zwischen beiden Varianten, bevor wir uns der weiteren Konfiguration des Catalogs zuwenden.

Machine Creation Services mit Einschränkungen

Mit XenDesktop 5.0 hatte Citrix die MCS als zusätzliche Technik eingeführt, um gleichartige Desktops auf Basis einer Vorlage zu erstellen. Mit der technischen Umsetzung hatten wir uns bereits in unserem Test [4] beschäftigt, weshalb hier nur kurz die Funktionalität erläutert werden soll. Eine VM, die als Vorlage für Desktops dient, wird von den MCS in einen Snapshot überführt, der wiederum in einen separaten Storage-Bereich – bevorzugt auf eine NFS-Freigabe – kopiert wird.

Dort bildet die Kopie die Grundlage für beliebig viele Desktop-VMs. Alle Desktops verwenden somit das gleiche schreibgeschützte Golden Image und verfügen zusätzlich über zwei weitere virtuelle Festplatten: eine Diff Disk, in der sämtliche Abweichungen vom Golden Image gespeichert werden, und die Identity Disk, in der die Active Directory-Identität der jeweiligen Maschine abgelegt wird. Gegenüber den Desktops erscheinen das Golden Image und die Disks transparent als eine Festplatte.

Der Vorteil der MCS ist, dass diese direkt auf Ebene des Hypervisors arbeiten und somit keine weiteren Serverdienste wie TFTP oder PXE erfordern. Gegenüber den PVS ist diese Lösung somit weniger komplex und schneller in Betrieb zu nehmen. Der Nachteil auf der anderen Seite ist, dass die MCS ausschließlich für die Bereitstellung von Desktops in Form von virtuellen Maschinen geeignet sind.

Verbesserte Provisioning Services

Demgegenüber ist die Streaming-Technologie der PVS in der Lage, sowohl virtuelle als auch physische Ziele aus einem Golden Image zu bedienen. Hinzu kommt, dass die PVS nicht darauf beschränkt sind, virtuelle Desktops zu verwalten, sondern auch XenApp-Terminalserver und beliebige weitere Systeme bereitstellen können. Die größere Flexibilität geht allerdings auch mit einer komplexeren Infrastruktur einher. Die PVS nutzen ebenfalls den Citrix-Lizenzdienst und erfordern neben einer separaten Datenbank einen oder mehrere zusätzliche Server, die in einer eigenen Farm zusammengefasst werden. Eine Farm umfasst wiederum eine oder mehrere Sites, die die Farm nach logischen und geografischen Gesichtspunkten segmentieren. Wichtig ist an dieser Stelle, dass die Begriffe der Farm und Site vollkommen losgelöst von einer XenApp-Farm oder einer XenDesktop-Site zu verstehen sind. Es handelt sich hier um eine separate Struktur.

Neben den Provisioning Servern selbst gruppieren die Sites sogenannte vDisk Pools, Stores und Device Collections mit Target Devices:

- Hinter einer vDisk verbirgt sich das Golden Image, von dem mehrere physische oder virtuelle Ziele – die Target Devices – booten. Als Format für vDisks dient die Microsoft Virtual Hard Disk (VHD).
- vDisks werden pro Site in einer logischen Verwaltungseinheit – dem vDisk Pool – zusammengefasst.
- Der Pool wiederum kann mehrere als Store bezeichnete physische Speicherbereiche für vDisks umfassen.
- Zu guter Letzt werden gleichartige Target Devices in einer Device Collection gruppiert.

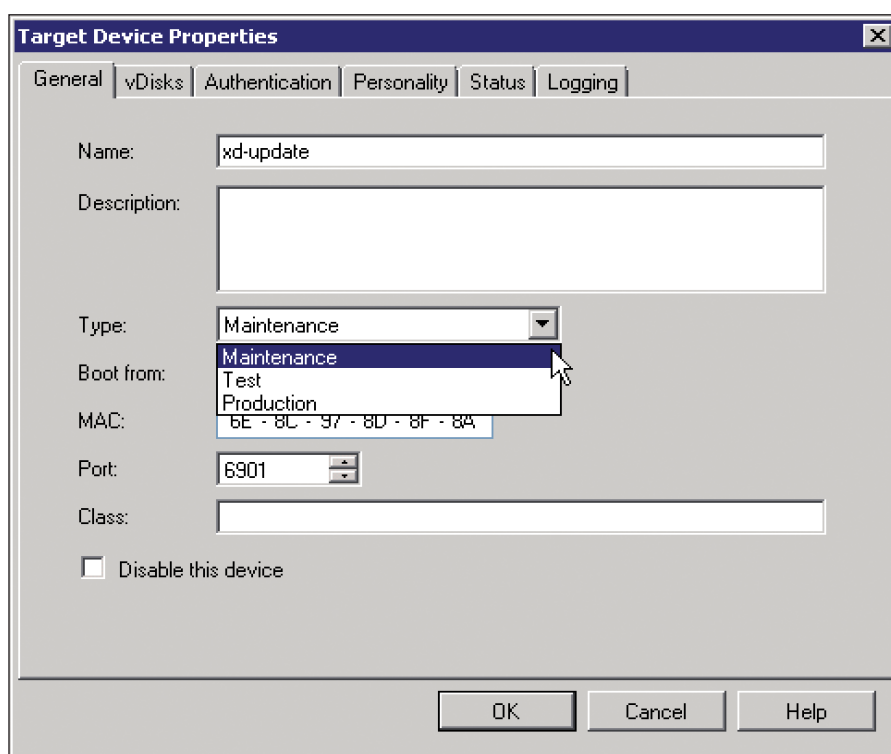


Bild 1: Das Type-Attribut regelt den Zugriff der Maschinen auf die entsprechenden Image-Versionen

Da die Targets in der Regel über keine eigene Festplatte mehr verfügen, sondern über das Netzwerk starten, sind zusätzlich DHCP, TFTP und PXE-Boot Dienste erforderlich. Die Dienste können Sie mit den PVS installieren oder anderweitig bereitstellen. Targets werden beim Start via DHCP mit einer IP-Adresse versorgt und laden per TFTP ein initiales Boot-Image, das das Target wiederum in die Lage versetzt, die PVS zu kontaktieren. Die Zuordnung von vDisks zu Target Devices erfolgt basierend auf der MAC-Adresse der Targets. Das Target bootet von der gewünschten vDisk über das Netzwerk. Dies ermöglicht ein Windows-Festplatten-Treiber, der über ein UDP-basiertes Protokoll mit den PVS kommuniziert und dem Target die vDisk als lokalen Datenträger anbietet. Dieses Protokoll arbeitet weitestgehend tolerant gegenüber Störungen im Netzwerk. Verliert ein Target die Verbindung zu den PVS, so stürzt es nicht ab, sondern bleibt lediglich stehen, bis die Konnektivität wiederhergestellt ist.

Mit der Installation und Konfiguration der PVS haben wir uns anhand der Version 5.1 bereits in allgemeiner Form [5,6] und für Terminalserver im Speziellen [7] beschäftigt. Da sich an dem grundlegenden Vorgehen in der Version 6.0 keine wesentlichen

Änderungen ergeben haben, soll der Fokus im Folgenden nur auf den Neuerungen, insbesondere dem wesentlich vereinfachten Update-Prozess, liegen. Die nötigen Vorarbeiten bestehen darin, Ihre PVS auf Version 6.0 zu aktualisieren. Anschließend bereiten Sie eine VM unter Windows 7 SP1 vor und installieren darauf neben einigen Applikationen den XenDesktop Virtual Desktop Agent (VDA). Hierzu wählen Sie die Methode "Advanced Install". Anschließend müssen Sie sich für ein Setup mit oder ohne HDX 3D Pro entscheiden. Mangels entsprechender Hardware in unseren Virtualisierungshosts entscheiden wir uns für das reguläre Setup des "Virtual Desktop Agent". Neben dem VDA bietet der Installer auch den Citrix Receiver für den Zugriff auf XenApp-Server an. Im folgenden Dialogschritt können Sie den FQDN Ihres DDC konfigurieren. Das Setup nimmt dann die notwendigen Anpassungen an der Windows Firewall vor, woraufhin die Installation erfolgt. Abschließend ist ein Neustart der Maschine erforderlich. Weiterhin installieren Sie den Target Device Treiber der PVS und konvertieren die VM mit dem Tool XenConvert in eine vDisk.

Gegenüber früheren Versionen der PVS fällt dabei positiv auf, dass dieser Prozess nun weitestgehend automatisiert abläuft. So kön-



Bestellen Sie jetzt das IT-Administrator Sonderheft I/2012!

180 Seiten Praxis-Know-how rund um das Thema

Exchange 2010 Migration, Betrieb und Troubleshooting

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

* IT-Administrator Abonnenten erhalten das Sonderheft I/2012 für € 24,90. Nichtabonnenten zahlen € 29,90.
Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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



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

☐ **Ja**, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft I/2012 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft I/2012 zum Preis von **€ 29,90** inkl. Versand und 7% MwSt.

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

Ich zahle ☐ per Bankeinzug

Geldinstitut:

Kto.:

BLZ:

oder ☐ per Rechnung

Datum:

Unterschrift:

Firma:

Name, Vorname:

Straße:

Land, PLZ, Ort:

Tel.:

E-Mail:

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

So erreichen Sie unseren
Vertrieb, Abo- und
Leserservice:

Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville
Tel: 06123/9238-251
Fax: 06123/9238-252

leserservice@it-administrator.de

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



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 0512

nen Sie sich mittels XenConvert direkt mit dem Provisioning Server verbinden und dort automatisch ein Target Device mit der MAC-Adresse der VM sowie eine passende vDisk erzeugen. Daraufhin fahren Sie die Maschine herunter und stellen die Boot-Reihenfolge auf "Network", so dass die VM beim nächsten Start den Provisioning Server kontaktiert. Dort ist das zugehörige Target zunächst darauf konfiguriert, von der lokalen Festplatte zu starten. Nach der Anmeldung über den Administrator-Account beginnt der Transfer der lokalen Installation in die vDisk automatisch. Anschließend fahren Sie die VM wieder herunter und entfernen die lokale Festplatte. Die VM konvertieren Sie daraufhin auf dem XenServer in ein Template und erzeugen daraus vier neue VMs sowie passende Targets auf dem Provisioning Server.

Als Boot-Medium dieser Targets wählen Sie "vDisk", weisen allen Targets Ihre zuvor erstellte Disk zu, ändern deren Modus auf den schreibgeschützten "Standard Mode" und aktivieren die Option "Enable Active Directory machine account password management". So gerüstet können Sie alle VMs von einem gemeinsamen Golden Image starten und diese auch in XenDesktop einbinden. Dies bringt uns zurück zum Assistenten für unseren ersten Catalog. Hier wählen Sie den Typ "Streamed" und geben die IP-Adresse Ihres ersten Provisioning Servers an. Daraufhin können Sie Ihre Device Collection auswählen und einen Namen für den Catalog vergeben. Damit ist die Basis-Konfiguration des Catalogs abgeschlossen.

Sie können nun eine neue Desktop Group erstellen, mit der Sie Ihren Domänen-Benutzern den Zugriff auf die Desktops erlauben. Mit den Power Management-Einstellungen legen Sie dabei etwa fest, dass tagsüber immer mindestens zwei bis drei und nachts noch eine virtuelle Maschine für neue Benutzersitzungen bereitstehen. Nachdem Sie diese Einstellungen gespeichert haben, sehen Sie, wie XenDesktop automatisch die gewünschte Anzahl an VMs auf den XenServern startet. Von einem Client mit installiertem Citrix Receiver können Sie sich daraufhin über <http://Servername/Citrix/DesktopWeb> mit dem Webinterface auf dem DDC verbinden. Nach Anmeldung eines Domänen-

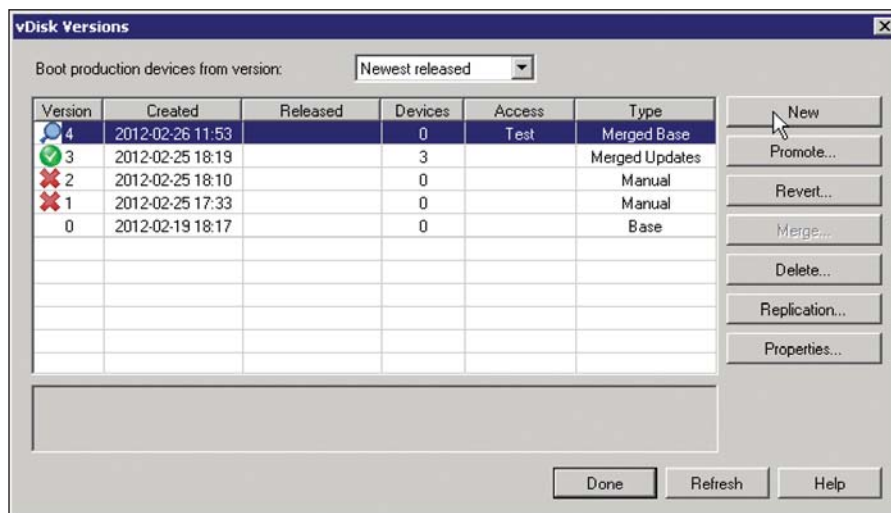


Bild 2: Mit dem vDisk Versions-Dialog werden die verschiedenen Entwicklungsstände eines Images verwaltet

Benutzers sehen Sie die Desktop Group und es öffnet sich automatisch eine Sitzung auf einem der freien Desktops.

vDisk-Updates einrichten

Sobald ein Image auf diese Weise produktiv in Betrieb ist, wird sich zeitnah der Bedarf für Updates ergeben – entweder durch die monatlichen Microsoft-Updates oder wenn Applikationen zu aktualisieren oder hinzuzufügen sind. Allein die Tatsache, dass sich durch die PVS nahezu beliebig viele Targets aus einem einzigen Image bedienen lassen, stellt hier schon eine signifikante Arbeitserleichterung gegenüber einzeln zu pflegenden VMs dar. Allerdings konnte bislang ein Image, das in Benutzung ist, nicht im laufenden Betrieb gewartet werden. Vielmehr galt es, eine vollständige Kopie der vDisk zu erzeugen, diese im "Private Mode" an eine separate VM anzuhängen und dann zu modifizieren. Sobald die neue vDisk wie gewünscht verändert war, ließen sich die produktiven VMs dazu veranlassen, von der neuen vDisk zu booten. Somit war der Update-Prozess der 5.x Versionen der PVS durchaus zeitintensiv und benötigte viel Platz im Storage, wenn je nach Größe der vDisk pro Update-Vorgang 15 bis 30 GByte zu kopieren waren.

Mit den PVS 6.0 hält nun optional ein neuer Update-Prozess Einzug, der auf inkrementellen vDisk-Updates basiert. Zu einer in Betrieb befindlichen vDisk vom Dateityp VHD können Sie zur Laufzeit mehrere Inkremente vom Dateityp AVHD anlegen, in denen sämtliche vom Basis-Image abweichenden Schreibzugriffe ge-

speichert werden. Das inkrementelle Update lässt sich anschließend testen und schließlich als produktiv markieren, sodass sämtliche Targets beim nächsten Neustart von der geänderten Version booten. Zu beachten ist bei diesem Vorgehen allerdings, dass Sie nicht beliebig viele inkrementelle Versionen erzeugen sollten, da lesende Zugriffe von Targets über alle Inkremente und das Basis-Image erfolgen. Zu viele Inkremente würden entsprechend den Zugriff verlangsamen und die Performance der Targets verschlechtern. Aus diesem Grund sieht der Update-Prozess Merge-Operationen vor, mit denen sich ein Basis-Image und mehrere Inkremente zu einer neuen Basis zusammenführen lassen. Die Warnschwelle, bei der die PVS automatisch einen Merge vorschlagen, lässt sich auf Site-Ebene konfigurieren und liegt per Default bei fünf Versionen.

[1] Supported Databases for Citrix Products

CSP61

[2] Tested Hardware for HDX 3D Pro

CSP62

[3] Citrix-Download-Seite

CSP63

[4] "Im Test: Citrix XenDesktop 5"

in IT-Administrator Nr. 5/2011

[5] "Virtuelle Maschinen mit dem Citrix Provisioning Server warten (1)" in IT-Administrator 04/2010

[6] "Virtuelle Maschinen mit dem Citrix Provisioning Server warten (2)" in IT-Administrator 05/2010

[7] "Virtuelle Maschinen mit dem Citrix Provisioning Server warten (3)" in IT-Administrator 06/2010

Link-Codes





Um das neue Update-Prozedere zu testen, erstellen Sie in Ihrer XenDesktop Device Collection zwei neue Targets mit den Namen "xd-update" und "xd-test" und ändern in deren Eigenschaften das neu eingeführte Type-Attribut (siehe Bild 1). Neue Targets erhalten automatisch den Typ "Production". Wie der Name vermuten lässt, steht dieser für produktiv betriebene Maschinen. Den Typ des Targets xd-update ändern Sie auf "Maintenance", für xd-test wählen wir naheliegend "Test". Den Gegenpart des Type-Attributs finden Sie im neuen Versionierungs-Assistenten der vDisks, den Sie im Kontextmenü der Disk über den Punkt "Versions..." erreichen. In dem darauffolgenden Dialog legen Sie über den Button "New" eine neue Version an, die automatisch den Zugriffs-Modus "Maintenance" erhält. Dieser Modus bedeutet, dass die Version zum einen für Schreibzugriffe geöffnet ist und zum anderen im Boot-Menü von Targets mit diesem Typ erscheint. Beim Start der VM xd-update wird Ihnen entsprechend neben dem weiterhin schreibgeschützten Basis-Image die neue Version angeboten. Starten Sie diese, installieren Sie zusätzliche Applikationen und fahren Sie die VM anschließend wieder herunter. Daraufhin können Sie auf den PVS über die Schaltfläche "Promote..." den Status der Version ändern. Dabei steht zur Wahl, ob der Status auf "Test" oder direkt auf "Production" geändert werden soll.

Wir entscheiden uns zunächst für "Test" und finden daraufhin die Version im Boot-Menü unserer VM xd-test wieder. Die Test-Version wurde dabei schreibgeschützt gestartet. Nachdem Sie die Änderungen ausprobiert und für gut befunden haben, können Sie die Version in der PVS-Konsole

wiederum mittels "Promote..." als produktiv markieren. Dabei ist zu entscheiden, ob die neue Version für neu startende Targets sofort oder erst ab einem geplanten Zeitpunkt verfügbar sein soll.

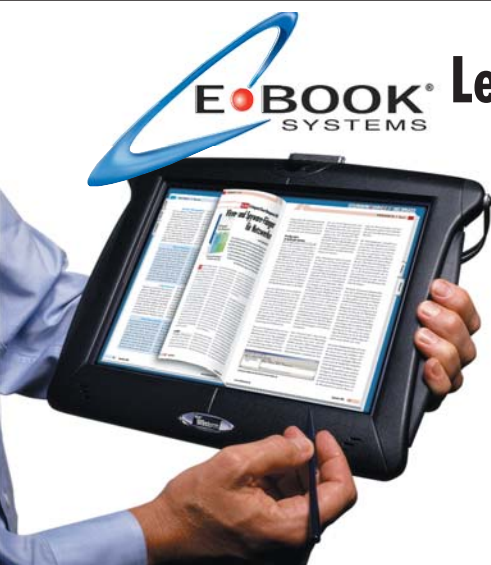
Dieser Ablauf lässt sich daraufhin nach Belieben wiederholen. So erzeugen, modifizieren, testen und betreiben Sie weitere Versionen. Im weiteren Verlauf machen wir dabei auch von der Merge-Operation Gebrauch. Zu beachten ist hierbei, dass die Schaltfläche "Merge..." nur verfügbar ist, wenn sich keine der Versionen im Modus "Maintenance" befindet. Sind nur Test- und Production-Versionen vorhanden, lassen sich mehrere Inkremente oder auch Inkremente und Basis-Images zu neuen Versionen zusammenführen – und das im laufenden Betrieb, ohne dass eine Downtime der Targets erforderlich wäre. Nicht mehr benötigte Zwischenstände können anschließend gelöscht werden. Über den Punkt "Show usage..." im Kontextmenü der vDisks ist es zudem möglich anzuzeigen, welches Target aktuell mit welcher Version verbunden ist.

Stellt die Versionierung somit bereits bei manueller Bedienung eine wesentliche Vereinfachung gegenüber früheren Versionen der PVS dar, bringt ein weiterer Punkt zusätzliche Flexibilität: das automatische vDisk Update Management. Zwar würde eine detaillierte Beschreibung dieser Funktionalität den Rahmen dieses Workshops sprengen, doch möchten wir die Möglichkeiten kurz beschreiben. So ist es mit dem vDisk Update Management denkbar, den Update-Prozess weitestgehend zu automatisieren, indem Sie einmalige, tägliche, wöchentliche oder monatliche Aufgaben de-

finieren. Beispielsweise wäre es möglich, eine monatliche Aufgabe zu definieren, die selbsttätig eine neue Version einer vDisk erstellt, diese startet und via WSUS die anstehenden Windows-Updates einspielt. Wenngleich das Testen weiterhin als manuelle Tätigkeit im Nachgang verbleibt, nehmen Ihnen die PVS 6.0 als Administrator auf diese Weise mehr und mehr lästige Aufgaben ab.

Fazit

XenDesktop bietet mit den MCS und den PVS zwei vielseitige Möglichkeiten für das Image-Management. Als besonders nützlich erweisen sich die PVS, da diese nicht nur XenDesktop VMs, sondern beliebige weitere Workloads bereitstellen können. Mit den vDisk Versionen wurde ein großer Schritt hin zu flexiblem Management der vDisks bei gleichzeitig unterbrechungsfreiem Betrieb getan. Und dies ist nur eine Momentaufnahme. Voraussichtlich noch im ersten Quartal 2012 wird XenDesktop 5.6 erscheinen und die Provisioning Services 6.1 mitbringen. Mit diesen steht die Integration von RingCube vDisk ins Haus, einer kürzlich von Citrix aufgekauften Technologie. Damit wird es möglich, zu einem schreibgeschützten Basis-Image pro Benutzer persönliche vDisks zu erstellen, die dem Endanwender gegenüber gemeinsam mit dem Basis-Image als ein Betriebssystem erscheinen. Es steht zu erwarten, dass der Pflegeaufwand für virtuelle Desktops nochmals deutlich reduziert werden kann, da es den Administratoren auf diese Weise ermöglicht wird, mit nur einem Golden Image unterschiedlichste Anforderungen seitens der User zu bedienen. Entsprechend bleibt es weiterhin spannend, die Entwicklung von XenDesktop zu beobachten. (dr)



Lesen Sie den IT-Administrator als E-Paper

Testen Sie kostenlos und unverbindlich die elektronische IT-Administrator Leseprobe auf 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



Administration von Windows Server 8 mit dem Server-Manager

Schaltstelle der Server-Macht

von Thomas Joos

Microsoft integriert in Windows 8 Server zahlreiche Neuerungen im Bereich Netzwerk, der Internetanbindung und der Cloud-Verwaltung. Der Nachfolger von Windows Server 2008 R2 SP1 ist im Netzwerk wesentlich leichter und effizienter zu verwalten. Das neue Betriebssystem erlaubt ohne Zusatztools, von einer zentralen Stelle aus mehrere Server zu verwalten. Den Server-Manager hat Microsoft komplett überarbeitet und zu einer Zentrale der Administration gemacht. Unser Beitrag geht der Frage nach, wie sich die Verwaltungs-Neuheiten in der Praxis schlagen.



Quelle: pixelfix.de

Der neue Server-Manager zeigt Server gruppiert nach Rollen an und bietet daher effizientere und übersichtlichere Verwaltungsmöglichkeiten als noch Windows Server 2008 R2. Nach der Vorabversion (Windows Server 8 Developer Preview) stellt Microsoft eine neue Beta-Version [1] zur Verfügung, die einen noch genaueren Blick zulässt. In dieser Version sind weitgehend alle Funktionen enthalten, die auch die finale Version bieten wird. Die Developer Preview war hier noch stark eingeschränkt.

Remote-Verwaltung mit dem Server-Manager

Das Erste, was nach der Installation von Windows Server 8 neben der neuen Metro-Oberfläche auffällt, ist die überarbeitete Version des Server-Managers. Dieser bietet aber nicht nur eine neue Oberfläche, sondern auch mehr Funktionen. So ist es in der neuen Version möglich, Serverrollen und -Features über das Netzwerk auf anderen Servern zu installieren. Die Server im Netzwerk lassen sich zentral im Server-Manager verwalten. Dazu gruppiert der Server-Manager die ver-

schiedenen Serverfunktionen zur besseren Verwaltung und zeigt installierte Serverrollen entsprechend an. Verwaltungswerkzeuge stellt der Server-Manager direkt über den Menüpunkt "Tools" dar. Hierüber lassen sich alle wichtigen Werkzeuge starten. So stört auch die sehr gewöhnungsbedürftige Metro-Oberfläche nicht, da alle Verwaltungsaufgaben zentral im Server-Manager stattfinden.

Um im Server-Manager weitere Server anzubinden, klicken Sie auf "Verwalten" und dann auf "Server hinzufügen". Im folgenden Fenster können Sie anschließend nach Servern suchen, um sie im lokalen Server-Manager zu verwalten. Auf diesem Weg erstellen Sie auch eigene Servergruppen, die Sie im Servermanager zusammenfassen. Von diesen Gruppen können Sie dann Ereignismeldungen anzeigen lassen.

Um auf Servern im Netzwerk über den Server-Manager remote Rollen oder Features zu installieren, ist allerdings keine vorherige Anbindung notwendig. Im Assistenten zum Hinzufügen von zusätzli-

chen Rollen erscheint ein neues Fenster, in dem Sie den Server auswählen können, auf dem Sie eine neue Rolle oder ein neues Feature installieren wollen. Hier fällt auch eine weitere Neuerung auf: In Windows Server 8 sind die Assistenten zum Hinzufügen von Rollen und Features zusammengefasst. Das heißt, Sie können über einen einzelnen Assistenten mehrere Serverrollen und Features gemeinsam und auf einmal installieren. Das erspart unnötige Neustarts und Installationen, da alles in einem Arbeitsschritt erfolgt. Im Assistenten lassen sich aber nicht nur physische Server im Netzwerk auswählen, um Serverrollen zu installieren, sondern auch virtuelle Festplatten auf Hyper-V-Hosts.

Einfache Übertragung der Serverkonfiguration

Bei der Installation von Rollen und Features können Sie zwischen der "Role-based or Feature-based"- und der "Scenario-based"-Installation auswählen. Die erste Option entspricht der herkömmlichen Installation von Rollen und Features wie bei Windows Server 2008 R2. Bei

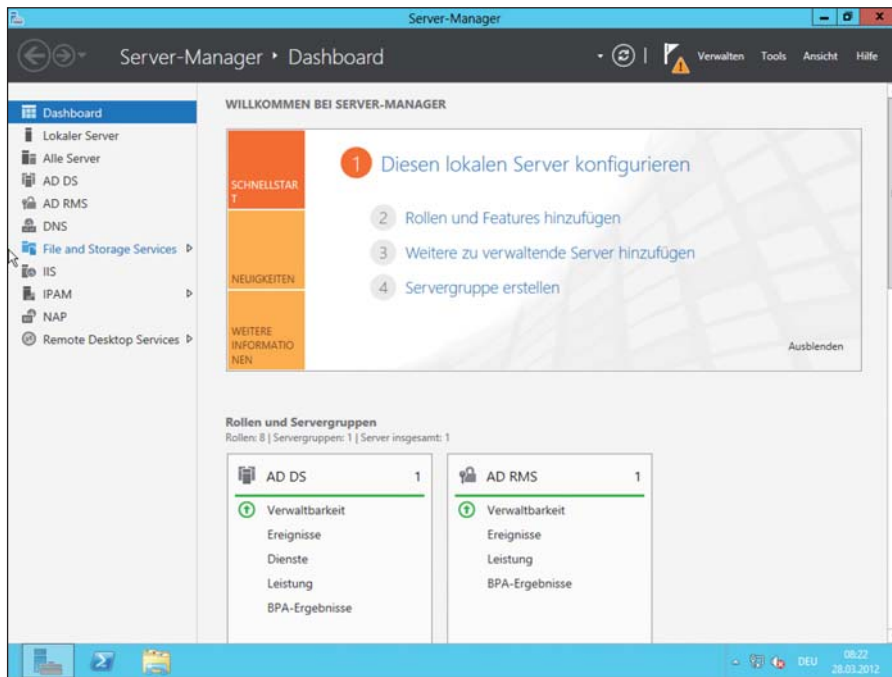


Bild 1: Über den neuen Server-Manager lassen sich nicht nur lokale Server managen, sondern auch Remote-Rechner

Scenario-based-Installationen können Sie die Remotedesktop-Dienste in einer Farm installieren, was vor allem für den Betrieb einer Virtual Desktop Infrastructure (VDI) sinnvoll ist. Unter Windows Server 8 arbeiten die Remotedesktop-Dienste sehr viel enger mit Hyper-V zusammen und ermöglichen auch die Virtualisierung von Anwendungen ohne Zusatzwerkzeuge. Beim Abschluss der Installation von Serverrollen und -Features erhalten Sie eine Zusammenfassung und die Möglichkeit, die Konfiguration in XML-Dateien zu exportieren. Mit diesen Dateien können Sie dann die gleichen Rollen oder Features auf einem anderen Server installieren. Zusätzlich haben Sie die Möglichkeit, einen alternativen Pfad zu den Installationsdateien von Windows Server 8 anzugeben. Hier sollten Sie auch die Option zum automatischen Neustart aktivieren. In diesem Fall starten die Server automatisch neu, wenn das notwendig ist. Vor allem wenn Sie Installationen von Serverrollen über das Netzwerk oder über eine RDP-Verbindung ausführen, ist das sinnvoll, da viele Rollen die Netzwerkverbindung kappen können, zum Beispiel die Installation von Hyper-V.

Überall im neuen Server-Manager lassen sich auf diesem Weg die anderen Server im Netzwerk schnell und einfach integrieren und verwalten. Über das Kontext-

menü von Servern lassen Sie Server über das Netzwerk neu starten, beginnen eine PowerShell-Sitzung auf dem Server oder öffnen eine RDP-Verbindung. Auch die Installation von Rollen und Features über das Netzwerk ist mit dem Kontextmenü möglich. Im Server-Manager sehen Administratoren am Wartungszentrumsymbol im oberen Bereich, ob Fehler auf einem angebundenen Server vorliegen oder Maßnahmen zur Verwaltung notwendig sind. Allerdings lassen sich auf diesem Weg nur Server mit Windows Server 8-Betriebssystem zentral verwalten. Windows Server 2008 R2 lässt sich nicht an den neuen Server-Manager anbinden. Ob sich das mit einem zukünftigen Service Pack oder einer Erweiterung ändern wird, lässt sich noch nicht sagen.

Core-Server ist keine Einbahnstraße mehr

Core-Server hat Microsoft mit Windows Server 2008 R2 eingeführt. Diese Server arbeiten ohne grafische Oberfläche und werden über die Befehlszeile, die PowerShell oder über das Netzwerk von anderen Servern aus verwaltet. Der Vorteil dabei ist die höhere Sicherheit und Stabilität, da ein großes Stück Angriffsfläche fehlt. Der Nachteil in Windows Server 2008 R2 ist, dass die Installation eine Einbahnstraße ist, da sich Core-Server nicht zu Servern mit grafischer Oberfläche aktua-

lisieren lassen. Umgekehrt lässt sich auch die grafische Oberfläche nach der Einrichtung nicht deinstallieren.

In Windows Server 8 ist die Installation als Core-Server der von Microsoft offiziell empfohlene Weg und auch standardmäßig ausgewählt. Im Gegensatz zu Windows Server 2008 R2 ist es aber möglich, eine Core-Installation zu einer Installation mit grafischer Oberfläche zu aktualisieren. Dazu müssen Sie lediglich das Verwaltungsprogramm "sconfig" auf dem Core-Server starten und den Menüpunkt "Wiederherstellen der grafischen Benutzeroberfläche" auswählen.

Anschließend installiert der Server seine grafische Benutzeroberfläche, die unter Windows Server 8 als Serverfeature verfügbar ist. Das bedeutet, dass auch eine Deinstallation möglich ist. Ab der Beta-Version des neuen Servers haben Sie die Möglichkeit, die grafische Oberfläche zu entfernen und diesen damit zu einem Core-Server umzuwandeln. Dazu rufen Sie im Server-Manager die Verwaltung der Rollen und Features auf und entfernen das Feature "Grafische Verwaltungstools und Infrastruktur" sowie "Grafische Servershell". So können Sie einen Server bequem über die grafische Oberfläche und den Server-Manager einrichten und danach die Oberfläche deinstallieren. Danach haben Sie einen sicheren und schnellen Core-Server.

Beim Wechsel zwischen Core-Server und Server mit GUI bleiben alle Einstellungen und Serverrollen oder -Features erhalten. Windows Server 8 entfernt nur Funktionen der grafischen Oberfläche. Ein Wechsel dauert nur wenige Sekunden bis Mi-

Windows Server 8 erlaubt, Netzwerkkarten als Team zu betreiben. Bisher war das nur mit speziellen Karten und entsprechenden Treibern möglich. Die Einstellungen nehmen Sie direkt im Server-Manager vor: Dazu klicken Sie in den Eigenschaften des Servers im Server-Manager auf die Option "Netzwerkadapter-Teamvorgang". Anschließend zeigt ein Assistent die verfügbaren Netzwerkkarten im Server an und Sie erstellen im Assistenten die gewünschten Teams.

Teaming von Netzwerkkarten



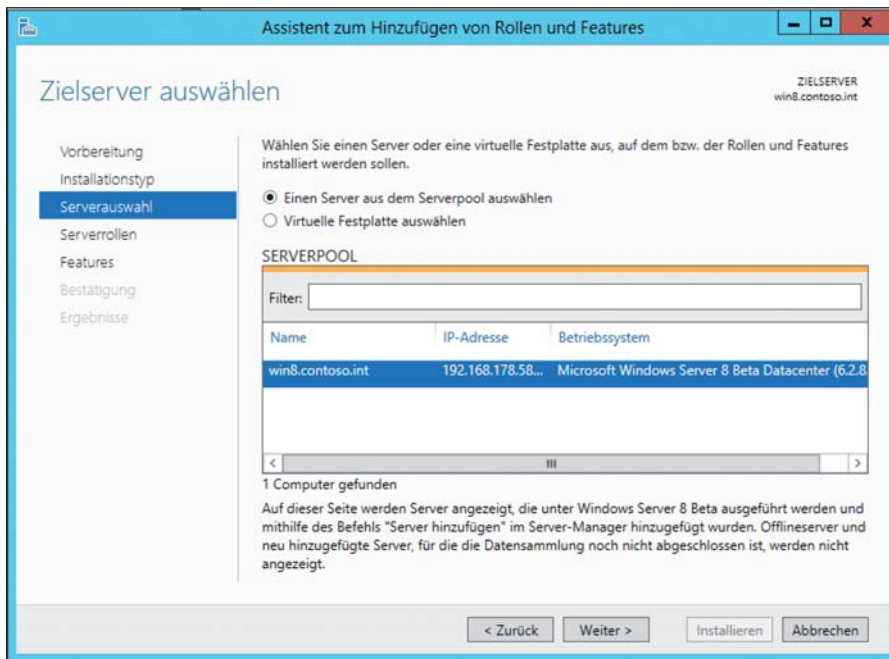


Bild 2: Windows Server 8 erlaubt es Administratoren, mehrere Serverrollen und -Features gleichzeitig zu installieren. Das spart vor allem Zeit dank weniger Neustarts.

nuten, abhängig von der Geschwindigkeit des Servers. Daten gehen dabei keine verloren. Das verbessert deutlich die Verwaltung. Einer der großen Vorteile dabei ist die Unterstützung von Core-Servern in SQL Server 2012. Da Datenbank-Server ohnehin jedes bisschen Leistung eines Servers benötigen, stört die grafische Oberfläche eher.

Verbesserungen im Active Directory

Nicht nur die generelle Installation von Serverrollen und die Überwachung von Servern hat Microsoft überarbeitet, sondern auch die Möglichkeit, Serverdienste mit verwalteten Dienstkonten zu konfigurieren. Diese Dienstkonten erhalten durch das Active Directory automatisch und regelmäßig neue Kennwörter. Netzwerkangriffe durch kompromittierte Serverdienste gehören daher der Vergangenheit an. Verwaltete Dienstkonten erlauben seit Windows Server 2008 R2 auch für Serverdienste regelmäßige Kennwortänderungen durchzuführen. In Windows Server 8 hebt Microsoft die Grenze der Konten für einzelne Server auf, sodass sich die verwalteten Dienstkonten netzwerkweit auch auf mehreren Servern nutzen lassen. In Windows Server 2008 R2 waren Dienstkonten noch auf einzelne Server gebunden, was die Verwaltung unnötig kompliziert hat.

Microsoft optimiert auch die Zusammenarbeit von Domänencontrollern (DC) und Hyper-V und die Wege, Domänencontroller schneller bereitzustellen. In Windows Server 8 lassen sich DCs problemlos virtualisieren, ohne bei der Erstellung von Snapshots Gefahr zu laufen, die AD-Datenbank zu zerstören. Um einen virtuellen Domänencontroller zu klonen, sind keine Spezialwerkzeuge notwendig, sondern Sie kopieren einfach die virtuelle Maschine und geben dem Klon einen neuen Namen im Netzwerk. Durch die neue GenID und deren Unterstützung in Hyper-

V 3.0 erkennt der neue Server das Active Directory und bindet sich ein. Administratoren können auf diesem Weg daher extrem einfach Domänencontroller im Netzwerk vervielfältigen und ohne Angst virtualisieren.

Auch den Installationsassistent für das Active Directory hat Microsoft überarbeitet. Dcpromo ist nicht mehr notwendig und in der bekannten Form nicht mehr verfügbar. Die Installation des Active Directory findet über die Installation der Serverrolle oder mit der PowerShell statt. Dazu hat Microsoft haufenweise neue Cmdlets integriert, um das Active Directory in der PowerShell zu verwalten und zu installieren. Diese Befehle sehen Sie, wenn Sie in der PowerShell 3.0 in Windows Server 8 zunächst das entsprechende Modul mit *Import-Module ADDS-Deployment* laden. Die Befehle lassen Sie sich zum Beispiel mit *get-command *adds** anzeigen. Mit dem Cmdlet "Install-ADDS-DomainController" installieren Sie in einer bestehenden Domäne zum Beispiel einen neuen Domänencontroller. Mit *Install-ADDSDomain* installieren Sie eine neue Domäne, mit *Install-ADDSForest* eine neue Gesamtstruktur. Um einen Domänencontroller herabzustufen, verwenden Sie das Kommando *Uninstall-ADSDomainController*. Die Cmdlets fragen alle notwendigen Optionen ab und starten den Server neu. Konfigurationen wie DNS-Server und globaler Katalog neh-

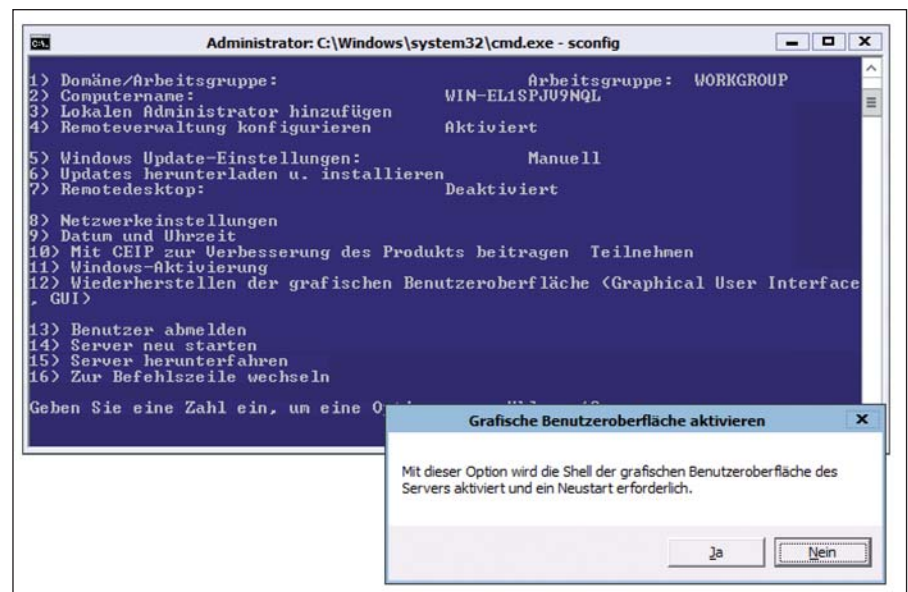
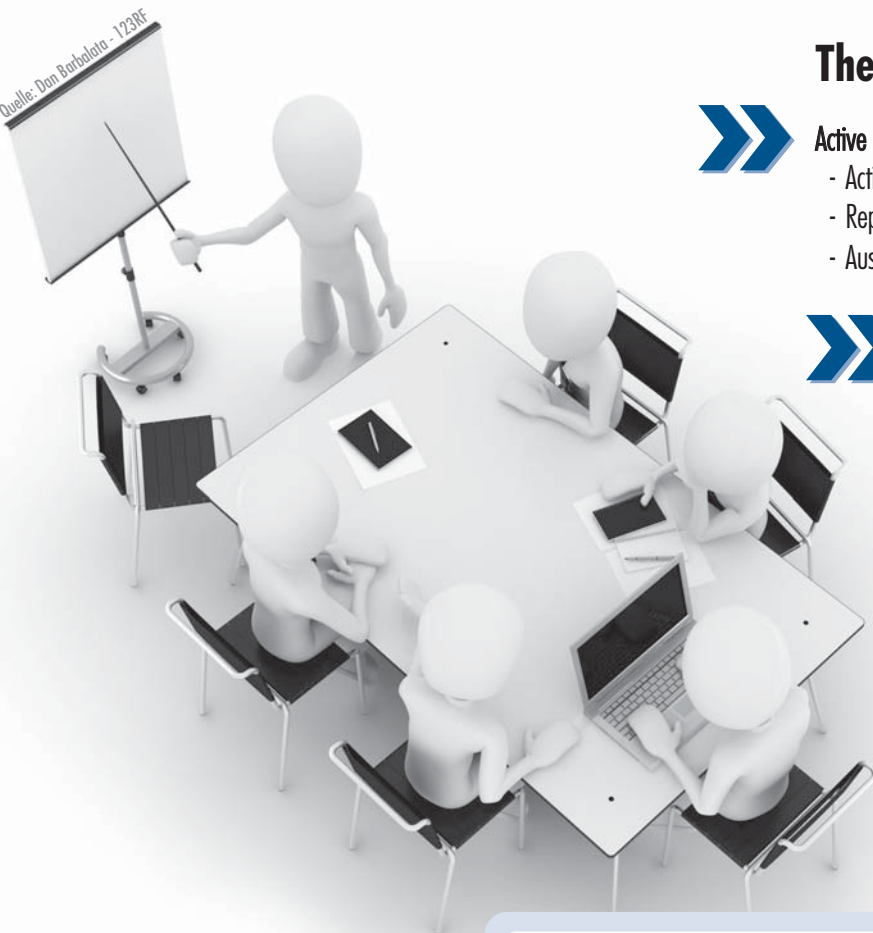


Bild 3: Das Leben als Core-Server ist unter Windows Server 8 keine endgültige Entscheidung mehr – jeder Core-Server lässt sich um eine grafische Oberfläche erweitern

Training Windows Server Best-Practice

Frankfurt/Dietzenbach, 19. Juni 2012



Themen des Trainings:



Active Directory: So läuft's rund. Praxis aus 12 Jahren

- Active Directory und DNS - Virtuelle DCs
- Replikation - Sicherheit - Lieblingsfehler
- Ausblick: Neuerungen im Active Directory unter Windows Server 8



Wiederbelebung: Disaster Recovery für das Active Directory

- Was kann denn kaputtgehen?
- Backup-Methoden: Was geht und was nicht?
- Restore ist mehr als Backup: Praxisdemos



Hyper-V sicher und sauber

- Warum virtualisieren wir eigentlich?
- Virtuelle Server, reale Gefahren
- Im Dutzend billiger: Sizing für Hyper-V
- Ausblick: Hyper-V 3.0 in Windows Server 8

Referent: Nils Kaczinski

Termin: 19. Juni 2012

Ort: ExperTeach Training Center Frankfurt/Dietzenbach – Waldstraße 94, 63128 Dietzenbach

Uhrzeit: 10.00 bis ca. 17.00 Uhr

Anmeldeschluss: 8. Juni 2012

Trainings-Partner:



EXPERTeach

Teilnahmegebühren:

Für IT-Administrator Abonnenten Euro 145,- (zzgl. 19% MwSt.), für Nicht-Abonnenten Euro 195,- (zzgl. 19% MwSt.).

Die Teilnehmerzahl ist auf 25 begrenzt.

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





men Sie anschließend vor. Diese Aufgaben müssen Sie nicht mehr im Assistenten zur Installation vorgeben.

Auch neue Cmdlets, um die Installation und den Betrieb von Active Directory zu testen, hat Microsoft integriert:

- Test-ADDSDomainController Installation
- Test-ADDSDomainController UnInstallation
- Test-ADDSDomainInstallation
- Test-ADDSEForestInstallation
- Test-ADDSEReadonlyDomain ControllerUnInstallation

Die Verwaltungskonsolle "Active Directory Administrative Center" (ADAC) bietet zudem mehr Möglichkeiten als die Vorgängerversion. So lässt sich in Windows 8 auf diesem Weg der AD-Papierkorb aktivieren und verwenden. In der neuen Konsole können Administratoren die einzelnen Einstellungen, die sie vornehmen, auch als PowerShell-Befehl anzeigen. Diese zeigt das ADAC in der Windows PowerShell History im unteren Bereich der Konsole an.

Migration zu Windows Server 8

Wollen Sie einen Domänencontroller zu Windows Server 8 aktualisieren, müssen Sie zunächst das Schema der Gesamtstruktur erweitern. Dazu führen Sie den Befehl `adprep /forestprep` auf einem Domänencontroller aus. Sie finden das Tool im Verzeichnis "support\adprep" auf der Windows Server 8-DVD. Damit Sie das Schema erweitern können, müssen Sie zuvor noch mit "c" die Erweiterung bestätigen. Diese Maßnahmen sollten Sie allerdings nicht in produktiven Umgebungen durchführen, da sich die Änderungen nicht mehr rückgängig machen lassen.

Nach der Aktualisierung des Schemas aktualisieren Sie mit `adprep /domainprep` noch die einzelnen Domänen. Installieren Sie neue DCs, lassen sich diese problemlos in das Active Directory aufnehmen. Auch Mitgliedsserver mit Windows Server 8 können Sie in bestehende Domänen aufnehmen, wenn Domänencontroller mit Windows Server 2003, 2003 R2, 2008 oder 2008 R2 vorhanden sind. Bei Migrationen können Sie Betriebsmasterrollen

von Vorgängerversionen auf die neuen Domänencontroller übernehmen. Die Vorgänge dazu sind identisch mit der Übernahme in Windows Server 2008 R2.

Verbessertes und sicheres DNS-System

Durch die engere Verzahnung der Server miteinander ist auch eine Verbesserung des DNS-Systems notwendig, vor allem im Bereich der Sicherheit. Bereits mit Windows Server 2008 R2 hat Microsoft DNSSEC eingeführt, um Zonen und Einträge abzusichern. Die Verwaltung von DNS-Servern ist im Server-Manager von Windows Server 8 durch die Gruppierung wesentlich effizienter. So lassen sich Zonen online digital signieren und DNSSEC integriert sich in der neuen Version komplett in das Active Directory. Das umfasst auch die Möglichkeit, dynamische Updates für geschützte Zonen zu aktivieren.

Windows Server 8 unterstützt weiterhin offizielle Standards wie NSEC3 und RSA/SHA-2. Neu ist auch die Unterstützung von DNSSEC auf schreibgeschützten Domänencontrollern (RODC). Findet ein RODC mit Windows Server 8 eine signierte DNS-Zone, legt er automatisch eine sekundäre Kopie der Zone an und überträgt die Daten der DNSEC-geschützten Zone. Das hat den Vorteil, dass auch Niederlassungen mit RODCs gesicherte Daten auflösen können, aber die Signatur und Daten der Zone nicht in Gefahr sind. DNSSEC lässt sich über das Kontextmenü von Zonen erstellen. Eine komplizierte Konfiguration in der Befehlszeile ist nicht mehr notwendig. Auch das Offline-Setzen von Zonen ist nicht mehr notwendig.

Die Signierung der Zone erfolgt über einen Assistenten. Mit diesem schützen Sie recht einfach DNS-Zonen vor Manipulationen. Der Assistent erlaubt die manuelle Signierung, eine Aktualisierung der Signierung und eine Signierung auf Basis automatischer Einstellungen. Windows Server 8 ist auch dazu in der Lage, signierte Zonen auf andere DNS-Server im Netzwerk zu replizieren. Eine weitere Neuerung ist der IP-Adressverwaltungsserver (IPAM). Dieser Serverdienst überwacht und steuert zentral DHCP- und

DNS-Server. Die Installation erfolgt als Serverrolle. Der Dienst kann Änderungen überwachen und die Serverdienste zentral überwachen.

Bessere Remotedesktop-Server mit Windows 8 Server

Betreiben Sie Windows Server 8 in einer Remotedesktop-Farm mit Windows Server 2008 R2, profitieren die veröffentlichten Anwendungen in der Farm von den neuen Funktionen in RemoteFX. In der neuen Version bietet RemoteFX eine Reduzierung des Netzwerkverkehrs und verbesserte Darstellung des Desktops in Virtual Desktop-Infrastrukturen, vor allem beim Einsatz von Clients mit Windows 8.

Die neue RemoteFX-Version kann automatisch zwischen TCP und UDP umschalten, abhängig davon, welche Paketart am besten für die aktuelle Geschwindigkeit geeignet ist. Entsprechende Firewall-Einstellungen nimmt Windows Server 8 automatisch vor. So ist zum Beispiel automatisch der UDP-Port 3389 auf Windows Server 8-RDP-Servern freigeschaltet und RemoteFX erkennt automatisch die Geschwindigkeit des Netzwerkes, um optimale Einstellungen zu finden. RemoteFX unterstützt 3D-Darstellungen und Aero mit einer Software GPU. Außerdem bieten Remotedesktop-Server durchgehend USB-Unterstützung für Clients, auch für normale Sitzungen auf Remotedesktop-Servern.

Fazit

Windows 8 Server bietet im Vergleich zu Windows Server 2008 R2 zahlreiche Neuerungen. Die zentrale Verwaltung ist jetzt auch ohne Zusatzwerkzeuge möglich und der Server-Manager ist deutlich übersichtlicher und flexibler zu bedienen. Durch die serverübergreifende Installation von Rollen und Diensten sowie die Gruppierung von Servern lassen sich Netzwerke leichter verwalten. (jp)



[1] Download Windows Server 8 Beta
C5P81

Link-Codes





Aufbau einer Testumgebung mit VMware Workstation

Admin-Spielplatz

von Sandro Lucifora

Die Neuinstallation von Software oder das Durchführen von Updates im Netzwerk ist oft genug ein kleines Glücksspiel. Nicht selten arbeitet nach der Installation einer Software eine andere nicht mehr – sei es durch das Update eines Datenbankservers oder die Aktualisierung einer globalen Library. Wie sich solche Überraschungen durch eine praxisnahe virtuelle Testumgebung auf Basis von VMware Workstation vermeiden lassen, beschreiben wir in diesem Workshop.



Quelle: scusi - 123RF

Das Ziel dieses Workshops ist es, eine unabhängige, virtuelle Testumgebung mit Servern und Clients zur Verfügung zu stellen, die individuell skalierbar und einfach zu verwalten ist. Damit lassen sich dann die Auswirkungen von Installationen und Updates im Netzwerk testen, bevor diese im Live-Betrieb vorgenommen werden.

Anforderungen an die Testumgebung

Als Grundlage für unseren Workshop setzen wir VMware Workstation 8.0.2 unter Windows 7 in 64 Bit ein. Alternativ kann in unserem Workshop auch mit der Linux-Version gearbeitet werden. Wer die 32 Bit-Version nutzt, kann keine 64 Bit Betriebssysteme in virtuellen Umgebungen installieren und starten. Die Installation der Voll- als auch der Testversion laufen gleichermaßen ab. Nach dem Start erhalten wir den zweigeteilten Bildschirm – links die Liste der virtuellen Maschinen (VM) und rechts das Aktionsfenster.

Bevor wir uns mit der Installation befassen, widmen wir uns einigen grundlegenden Überlegungen hinsichtlich der Struktur und des Umfangs der Umgebung: VMware erlaubt es, Klone von VMs zu erstellen. Ein solcher Klon ist eine auf Basis einer VM erstellte Kopie, die als eigenständiges System arbeiten kann. Um sowohl Speicherplatz als auch administrativen Aufwand zu sparen, lassen sich Klone verlinken. Diese greifen auf eine bestehende VM zu, nutzen den vorhandenen Zustand, und können ab dem Installationszeitpunkt (dem Erstellen des Klons), autark und als eigenes System erweitert werden. Diese Funktion machen wir uns zu Nutzen, um mehrere virtuelle Maschinen, die auf Basis einer VM erstellt werden, aufzusetzen.

Zunächst ist es wichtig festzustellen, welche Betriebssysteme in der Testumgebung laufen sollen. Neben Windows werden auch verschiedene Linux-Derivate, Sun

Solaris sowie Novell NetWare unterstützt. Apple Macintosh wird nicht offiziell unterstützt, was sicher an der Politik von Apple liegt. Zwar gibt es im Internet die eine oder andere fertig installierte VM mit Max

VMware Workstation 8 bietet mehr als der reine VMware Player. Mit der Software werden virtuelle Maschinen erstellt und abgespielt. Weitere Funktionen sind die Anfertigung von Snapshots, das Erstellen von Screenshots und eine Mitfilmfunktion. Über die grafische Benutzeroberfläche erstellt der Administrator virtuelle Maschinen, kann diese editieren und eine Verbindung zu entfernten Servern herstellen. Die VMs sind in einer anderen virtualisierten Umgebung von VMware lauffähig: in einer Workstation 8-Instanz, in vSphere oder vCenter. Mehreren Personen ist die gemeinsame Verwaltung einer VM gestattet. VMware Workstation hat eine 3D-Beschleunigung, unterstützt HD-Audio mit 7.1-Surround-Sound, USB 3, Bluetooth-Geräte, Virtualisierung symmetrischer Multiprozessoren (SMP), 3D-Grafik und 64 GByte RAM in einer VM. Die Vollversion kostet etwa 160 Euro.

VMware Workstation 8 in der Übersicht



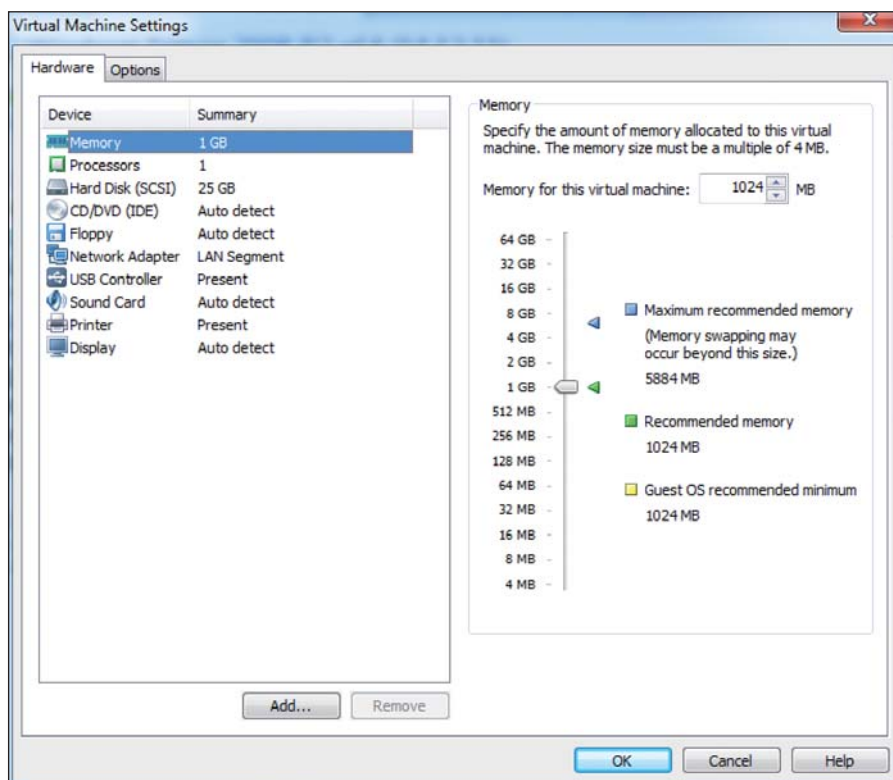


Bild 1: In den Hardwareeinstellungen der virtuellen Maschine sollte auf einen sparsamen Umgang mit dem Arbeitsspeicher geachtet werden

OS X, doch ist uns bisher von keiner Installation ohne Einschränkungen bekannt. Zudem erlaubt es die Lizenzvereinbarung von Apple nicht, Mac OS X auf einer anderen Plattform als auf Apple-Hardware zu installieren.

Die Lizenzen sind auch der nächste Vorbereitungspunkt. Grundsätzlich dürfen Microsoft Client-Betriebssysteme nur einmal – egal ob auf einer physikalischen oder virtuellen Maschine – installiert sein. Andere Hersteller von Betriebssystemen sind hier mittlerweile großzügiger und erlauben teilweise eine Backup-Installation in einer VM (virtuellen Maschine). Microsoft bietet hierzu die Software Assurance an. Unter dieser Lizenzform darf flexibler installiert werden.

Alternativ zu gekauften Lizenzen und abhängig von der Einsatzdauer der virtuellen Testumgebung lassen sich seit Windows 7 und Windows 2008 Server die Systeme auch als Testversion, mit einer Laufzeit von 60 beziehungsweise 120 Tagen, installieren. Im Kasten “Erweiterung des Evaluierungszeitraums” finden Sie einen Link zu Internetseiten, auf denen die Installationsdaten legal angeboten werden.

Virtuelle Maschinen erstellen

In diesem Workshop installieren wir einen Windows Server 2008 R2, einen Ubuntu-Server sowie eine beliebige Anzahl Windows 7- und Windows XP-Clients. Die Clients gruppieren wir anhand der darauf installierten Software zu einer Master-VM. Das heißt, wir überlegen uns, welche gemeinsame Basis die verschiedenen VMs später haben können und erstellen dafür eine VM als Vorlage. Dazu stellen wir sicher, dass alle benötigten Installationsmedien als ISO-Datei vorliegen. Bis auf Windows XP lassen sich diese legal aus dem Internet herunterladen. Für Windows XP haben wir uns mit der Freewarelösung ISO Builder eine ISO-Datei von der Installations-CD erstellt. Zwar lässt sich eine VM auch ganz normal von CD installieren, doch erfolgen spätere Nachinstallationen und der gesamte Installationsablauf schneller, wenn wir ISO-Dateien nutzen.

Als Erstes richten wir den Windows Server 2008 ein und starten dazu über das Menü “File / New Virtual Maschine” – oder mit der Tastenkombination Strg+N – den Installations-Assistenten. In unserem Fall fahren wir im nächsten Schritt mit

der “Typical Installation” fort. Als Installationsquelle wählen wir jetzt nicht das Diskimage im ISO-Format an, denn der Wizard würde bei der Prüfung das zu installierende Betriebssystem erkennen und uns durch Easy Install führen. Dabei handelt es sich um einen Installations-Prozess, der am Anfang Product-Key, Name und Logindaten benötigt. Die Installation erfolgt dann ohne Benutzereingriff.

Da wir in unserem Workshop von der Testversion ohne Lizenzschlüssel ausgehen, klicken wir auf “I will install the operating system later”. Das nächste Fenster fragt uns nach dem zu installierenden OS. Hier wählen wir Microsoft Windows 2008 R2 x64. Nun geben wir den Namen der VM und den Speicherort an, den wir unterhalb des unter “Eigene Dateien / Virtual Machines” erstellten Ordners “Master VM” festlegen. Weiter geben wir die Festplattengröße der neuen VM an. Diese muss gut gewählt sein, da bei einer späteren Änderung – die in einer VM problemlos möglich ist – die verlinkten Klone nicht mehr lauffähig sind. Für den Server wählen wir 50 GByte und die Option “Split virtual disk into multiple files”. Im nächsten Fenster gehen wir über den Button “Customize Hardware” zu den Hardwareeinstellungen.

Als Speicher legen wir 4 GByte fest. Beachten Sie, dass die Summe des Speichers aller zu einem Zeitpunkt laufenden VMs die Summe des Hauptspeichers Ihres Computers nicht übersteigen sollte. Daher gehen wir sparsam damit um, da es sich nur um eine Testumgebung handelt. Dasselbe gilt für die Anzahl der Prozessoren. Hier reicht uns einer.

Das CD/DVD-Laufwerk verbinden wir mit der ISO-Datei des zu installierenden Betriebssystems. Bei der Floppy stellen wir “Connect at power on” aus. Das lässt

Die kostenlose Testversion von Windows Server 2008 als auch Small Business Server ist auf 60 beziehungsweise 120 Tage begrenzt. Auf legalem Wege lässt sich dieser Zeitraum drei beziehungsweise zwei Mal auf bis zu 240 Tage verlängern [2].

**Erweiterung
des Evaluierungszeitraums**



Kompetentes Schnupperabo sucht neugierige Administratoren

Sie wissen, wie man Systeme
und Netzwerke am Laufen hält.
Und das Magazin IT-Administrator weiß,
wie es Sie dabei perfekt unterstützt:

mit praxisnahen Workshops, aktuellen
Produkttests und nützlichen Tipps und Tricks
für den beruflichen Alltag.

Damit Sie sich Zeit,
Nerven und Kosten sparen.

**Teamwork in Bestform.
Überzeugen Sie sich selbst!**



6

**Monate
lesen**

3

**Monate
bezahlen**

www.it-administrator.de



Heinemann Verlag
Im Dialog mit Spezialisten.

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München

Tel: 0049-89-4445408-0
Fax: 0049-89-4445408-99
info@heinemann-verlag.de

Vertrieb, Abo- und Leserservice IT-Administrator

vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville

Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de



sich im laufenden Betrieb immer ändern. Den Netzwerkadapter stellen wir auf "LAN Segment" – dies ist eine in sich geschlossene Netzwerkumgebung entsprechend einem autark arbeitendem Switch oder einem VLAN. Steht noch kein LAN Segment zur Auswahl, legen wir dieses einmalig über den gleichnamigen Button an. Wir nennen unser Segment "Master-VM". Hierüber richten wir später verschiedene Netzwerkumgebungen ein.

Beim USB-Controller schalten wir "Automatically connect new USB devices" und "Share Bluetooth devices with the virtual machine" aus. Auch diese Funktionen werden später, für jede VM separat, wieder eingeschaltet. Bei "Sound Card" und "Printer" wählen wir ebenfalls "Connect at power on" ab.

Je nach Testumgebung beziehungsweise Master-VM-Vorlage kann jetzt noch Hardware fehlen – wie weitere Netzwerkkarten oder ein SCSI-Gerät. Benötigen Sie diese schon in Ihrer Master-VM, so fügen Sie die weiteren Geräte über den Button "Add" hinzu. Nachdem VMware die VM erstellt hat, verschieben wir noch den neuen Eintrag in den Unterordner "MasterVM".

Für die Windows-Installation wählen wir die neu erstellte VM aus. Die Einzelheiten zeigt der rechte Fensterbereich. Über "Power on this virtual machine" starten wir die VM. Da wir zuvor die ISO-Installationsdatei von Windows auf das CD-Laufwerk gemappt haben, startet diese automatisch die Windows-Installation. Wenn Sie – vor allem für die Clients – später ein Netzwerk-Boot benötigen, richten Sie dies über das virtuelle BIOS wie auf jedem "normalen Computer" ein. Hierzu müssen Sie beim Start der VM direkt ins Aktionsfenster klicken und dann F2 drücken – damit rufen Sie das virtuelle BIOS auf. Oder Sie drücken F12 für den Network Boot.

VMware Tools bringen Treiber

Der Ablauf der Installation des OS entspricht jetzt dem einer üblichen Neuinstallation und konfiguriert das Betriebssystem entsprechend Ihrer Anforderungen. Da VMware für das eingesetzte Betriebssysteme eine Hardware-Plattform wie jede andere darstellt, benötigt das OS entspre-

chende Treiber. Diese sind in den VMware Tools gesammelt und werden durch die VMware Workstation installiert. Nach der Windows-Installation und dem Neustart der VM starten wir die Einrichtung der Tools über das Menü "VM / Install VMware Tools". Innerhalb der VM startet die Installation automatisch.

Weitere Server und Arbeitsplätze einrichten

Wie gerade für den Windows Server 2008 beschrieben, erstellen wir auch die virtuellen Maschinen mit Ubuntu 11 und Windows 7/XP. Der Unterschied ist hier lediglich, dass wir als Festplattengröße lediglich 10 GByte angeben und als Hauptspeicher – abhängig von den später auszuführenden Applikationen – wahlweise 512 MByte für den Ubuntu-Server und 1 oder 2 GByte für die Windows-Arbeitsplätze festlegen.

Da Windows XP eine Vollversion ist und wir einen Product-Key haben, wählen wir im Schritt "Install from" direkt die ISO-Datei aus. Jetzt haben wir unterhalb des Ordners "Master-VM" in der Workstation-Umgebung eine VM mit Windows Server 2008, je eine mit Windows 7 und Windows XP als auch eine mit Ubuntu. Alle VMs sind zudem mit dem LAN Segment "Master-VM" verbunden.

Linked Clones nutzen

Wie erwähnt, erstellen wir aus unseren Master-VMs verlinkte Klone und schaffen

Auf Basis der einzusetzenden Betriebssysteme und um später den geringsten Aufwand und die größte Flexibilität zu haben, haben wir uns ein Schema erstellt, über das wir gleichartige virtuelle Computer zu einem Master zusammenfassen. Die Master sind – wie schon beschrieben – der Ausgangspunkt für unsere verlinkten Klone. Sie sind wie eine Vorlage zu verstehen, von der aus die VM der Testumgebung erstellt wird. Während der Installation legt VMware im lokalen Verzeichnis "Eigene Dateien" einen Unterordner "Virtual Machines" an. Unterhalb dieses Ordners platzieren wir einen Ordner namens "Master VM", ebenso in der VMware-Umgebung. Somit haben wir für die VMware-Umgebung als auch auf der Festplatte jeweils einen eigenen Speicherplatz für unsere Master-VMs eingerichtet.

Schema zur Erstellung der Testumgebung



uns so unsere bedarfsgerechte Testumgebung. Hierzu erstellen wir in der VMware Workstation einen Ordner "Testumgebung". Einen weiteren Ordner erstellen wir unterhalb "Eigene Dateien / Virtual Machines" mit demselben Namen "Testumgebung". Hier werden die Daten der verlinkten Klone abgespeichert.

Um einen Klon zu erstellen, klicken wir auf die zu klonende VM mit der rechten Maustaste, gehen auf "Manage" und klicken dann auf "Clone". Im Assistenten klicken wir zwei Mal auf "Weiter". Bei der Frage nach dem "Clone Type" stellen wir sicher, dass der erste Radiobutton "Create a linked clone" ausgewählt ist, und wählen erneut "Weiter". Der Name kann frei gewählt werden und als Speicherort geben wir den zuvor neu angelegten Pfad an.

Kurz danach steht uns die verlinkte Kopie der Master-VM als Klon zur Verfügung. Diesen Vorgang wiederholen wir jetzt so oft mit den Master-VMs, bis wir unsere virtuelle Testumgebung zusammengestellt haben. In unserem Workshop nehmen wir einen Windows Server 2008, zwei Windows 7, zwei Windows XP und einen Ubuntu-Server.

Virtuelles Netzwerk und der Datenaustausch mit dem Host

Alle VMs unserer Testumgebung müssen jetzt in einem eigenen LAN Segment verbunden werden. Dazu klicken wir mit der rechten Maustaste auf die erste VM und dann auf "Setting". Der Dialog der Hardware-Einstellungen öffnet sich. Wir klicken auf "Networkadapter" und ändern unter "LAN Segment" über die Auswahlbox die Verbindung. Bei der ersten VM erstellen wir ein neues LAN Segment mit dem Namen "Testumgebung". So haben wir alle VMs der neuen Testumgebung in das neue, geschlossene LAN-Segment eingebunden.

Um die geschlossene Testumgebung individuell unseren Bedürfnissen anzupassen, benötigen wir zusätzliche Dateien und Programme, die uns der Host-Rechner – auf dem VMware Workstation läuft – liefert. Dazu müssen wir einen sogenannten "Shared Folder" einrichten, auf den sowohl die VMs als auch der Host Zugriff haben – ein Austauschverzeichnis. Auch dies neh-



men wir in den Settings vor. Bei der VM, die Zugriff auf die Daten haben soll – in unserem Fall ist es nur der Server –, klicken wir auf den Reiter “Options” und wählen den Eintrag “Shared Folders”. Wir aktivieren “Always enabled” und “Map as a network drive in Windows guests”. Unter “Add” fügen wir den Verzeichnispfad hinzu, auf den die VM später Zugriff haben soll. Hier lassen sich beliebig viele Pfade als verschiedene Netzwerkpfade einrichten.

Zweite virtuelle NIC erstellen

In einigen Fällen reicht der Datenaustausch über den Hostrechner nicht aus und eine oder alle VMs müssen Daten aus dem lokalen Netzwerk oder dem Internet erhalten. Wir richten dazu mit Hilfe einer zweiten, virtuellen Netzwerkkarte über den Windows Server ein Gateway ein.

Über die bekannten Virtual Machine Settings und den Reiter “Hardware” fügen wir über den Button “Add” einen weiteren Netzwerkadapter hinzu. In dem sich öffnenden Hardware Wizard stellen wir die “Network Connection” dieses Mal auf “Bridged”. Mit dieser Einstellung wird die zweite virtuelle Netzwerkkarte einfach über den Netzwerkport des Hostrechners in das angebundene Netzwerk durchgeschleift. Die virtuelle Netzwerkkarte wird

vom “externen” Netzwerk behandelt wie jedes andere Netzwerkgerät und bekommt eine eigene IP-Adresse. Alternativ können Sie auch auf NAT stellen, womit die virtuelle LAN-Karte nach außen dieselbe IP-Adresse nutzt wie der Host.

Start der Testumgebung

Als Erstes starten wir in der Testumgebung den Windows-Server, geben den LAN-Karten eine feste IP-Adresse und richten hier eine Domäne beziehungsweise das Active Directory und den DHCP-Server ein. Als Gateway tragen wir die zweite virtuelle Karte ein. Je nach Testaufgabe richten wir auf dem Server noch User und weitere Serverdienste ein.

Nun können wir jeden einzelnen Arbeitsplatz nacheinander starten und diese der virtuell erstellten Domäne hinzufügen. Damit haben wir eine betriebsbereite Testumgebung, auf der wir jegliche Installationen und Tests durchführen können. Um nicht bei jedem neuen Test die Testumgebung neu einrichten zu müssen, bedienen wir uns der Funktion der Snapshots. Ist die Umgebung so eingerichtet, wie wir sie benötigen, erstellen wir – vor dem Testbeginn – von jeder VM einen Snapshot. Wir klicken wieder mit der rechten Maustaste auf die VM und wählen den Eintrag “Snapshot

/Take Snapshot”. Wir geben eine Bezeichnung und eine Kurzbeschreibung ein, etwa den aktuellen Zustand der Installation. Sind alle Snapshots getätigt, starten wir die Rechner der Testumgebung und führen unsere Tests – zum Beispiel ein Update oder eine Neuinstallation – durch.

Stellen wir fest, dass das Update fehlerhaft verlief, und wollen es erneut durchführen, stellen wir den “Vorherzustand” auf dem zuvor erstellten Snapshot wieder her. Dazu klicken wir ins Kontextmenü der VM wieder auf “Snapshot” und dann auf “Snapshot Manager”. Übersichtlich sehen wir alle zuvor erstellten Snapshots. Um nun den Zustand wiederherzustellen, klicken wir einen Snapshot an – meist den letzten – und dann auf “Go To”. Die VM wird zurückgesetzt und der Test kann aufs Neue erfolgen. Ist der Test erfolgreich verlaufen, erstellen wir vom neuen Zustand einen Snapshot und können von hier später weiter testen. (jp) 

[1] VMware Workstation 8
als kostenlose 30-Tage-Testversion
CEP21

[2] Erweitern des Windows
Server 2008-Evaluierungszeitraums
CEP22

Download-Quellen der Betriebssysteme

Testversion Microsoft Windows 7
CEP23

Testversion Microsoft Windows Server 2008 R2 SP1
CEP24

Testversion Microsoft SQL Server 2008 R2
CEP25

Testversion Microsoft Exchange Server 2010 SP1
CEP26

Testversion Microsoft
Small Business Server 2008 Premium
CEP27

Testversion Microsoft
Small Business Server 2011 Essential
CEP28

Testversion Microsoft
Small Business Server 2011 Standard
CEP29

Microsoft Windows 8 Consumer Preview
CEP20

Vollversion Ubuntu Linux 10.04 und 11.1
CEP2A

Vollversion openSUSE 11.4 und 12.1
CEP2B

Link-Codes

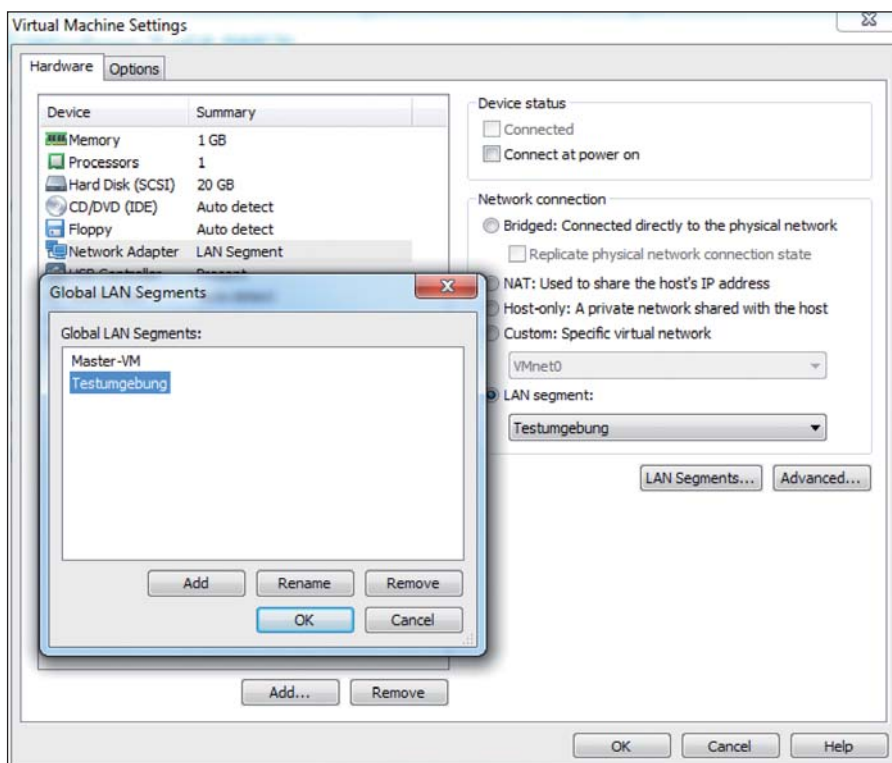


Bild 2: Über “LAN Segment” verbinden wir die VMs zu einer Testumgebung

Fortgeschrittene Methoden des IT-Projektmanagements (2)

Aber der da hat angefangen!

von Dr. Markus Blaschka



Wo gehobelt wird, fallen Späne: Dieses Sprichwort beschreibt die Realität in Projektteams bisweilen recht treffend. Kommen Menschen mit unterschiedlicher Kompetenz und Persönlichkeit zusammen, um gemeinsam auf eine Sache hinarbeiten, sind nicht selten soziale Konflikte programmiert. Damit diese Ihr Projekt nicht lahmlegen und Sie als Projektleiter künftig souverän mit zwischenmenschlichen Problemen umgehen können, geben wir Ihnen passende Konfliktmanagementwerkzeuge an die Hand.

Streit, Meinungsverschiedenheiten, Rollenkonflikte oder Konkurrenzkämpfe im Team können in jedem noch so gut geplanten Projekt vorkommen und bieten den Beteiligten die Chance, daran zu wachsen. Konfliktlösung ist ein Lernprozess, durch den jeder Projektleiter einmal marschiert sein sollte – im Interesse jedes weiteren Projekts, das er zu führen hat. Dieser Beitrag soll verdeutlichen, wie Konflikte entstehen, wie Sie Konfliktpotential im neuen Team schnell erkennen und bereits schwelenden Konflikten beikommen. Ein wenig psychologisches Hintergrundwissen kann dabei keinem Projektleiter schaden.

Zunächst einmal die Frage: Was ist ein Konflikt? Jeder von uns hat dazu seine subjektive Meinung; für den einen ist es schon tragisch, wenn ein Kollege sich bei Meetings immer in den Vordergrund spielt. Andere würden vielleicht sagen, dass man über so ein Verhalten hinwegsehen kann, solange der Projektleiter auch die Meinung der anderen für gleich wichtig erachtet. Ein ernsthafter Konflikt kann daraus im Team entstehen, wenn der aufdringliche Kollege sich im Recht wähnt, überall mitzureden, und der Rest des Teams ihn am liebsten rauskicken würde. Der Konflikt kann aber auch frühzeitig im Keim erstickt werden. Dabei kommt

es, wie wir später noch sehen werden, auch darauf an, dass jemand auf unbefriedigende Verhältnisse aufmerksam macht – im Idealfall merkt der Projektleiter als Erster, dass etwas nicht stimmt, bevor das Team ins Straucheln gerät.

Im Lexikon-Stil definiert halten wir also fest: Konflikte sind Spannungssituationen, in denen zwei oder mehrere Parteien, die voneinander abhängig sind, mit Nachdruck versuchen, scheinbar oder tatsächlich unvereinbare Handlungspläne zu verwirklichen, und sich dabei der Gegnerschaft bewusst sind.

Kein Konflikt kommt umsonst

Wie erkennen Sie nun einen Konflikt und machen ihn dingfest? Diese beiden Schritte gehören zusammen – auch wenn so mancher Projektleiter den unangenehmen zweiten gerne auslassen würde. Nehmen wir das Beispiel des vorlauten Teamkollegen: Bei jedem Gespräch, auch wenn es ihn nicht betrifft, muss er dabeistehen. Kein Meeting ohne seine nicht immer gefragten Kommentare. Kurzum: Da ist einer, der immer seine Meinung sagt, sich überall in den Vordergrund spielt und den Kollegen damit gehörig auf die Nerven geht. Noch hat keiner sich direkt bei Ihnen beschwert, aber Ihnen ist der Kollege auch schon unangenehm aufgefallen und

Sie ahnen: Das geht nicht mehr lange gut. Eindeutig geht es hier darum, das aus seiner Rolle gefallene Teammitglied wieder zu integrieren und die gestörte Kommunikation im Team zu kitten.

In den meisten Fällen geht es bei solchen Konflikten nicht um die Kompetenz des Störenfrieds, sondern um Charaktereigenschaften, die in der Gruppenarbeit hinderlich sind. Das Thema des Konflikts ist also nicht ein fachliches – auch mag der Betreffende gut in seiner Aufgabe sein –, sondern es betrifft das Verhalten des Teammitglieds und seine Art, zu kommunizieren.

Den Stein des Anstoßes zu erkennen ist die Voraussetzung, den Konflikt zu lösen: Der Seitenhieb "Müller, halten Sie sich doch bitte etwas mehr zurück!" kann, auch hundert Mal gesagt, das Problem nicht an der Wurzel packen: Warum muss Müller immer seinen Senf dazugeben? Hat er Angst, sonst nicht ernst genommen zu werden? Oder sollte man sogar öfter seinen Rat suchen, der vielleicht manchmal gar nicht so verkehrt ist? Könnte das nicht auch sein Ziel sein – in der Gruppe mehr (berechtigtes) Gehör zu finden oder herausfordernde Aufgaben zu bekommen, die ihn mehr befriedigen? Es mag befremdlich klingen, dass auch Konflikte ihre Qualität haben. Und doch ist es ein



Unterschied für einen Projektleiter, ob er einen latent vor sich hin schwelenden Konflikt zu bereinigen hat oder bei einem offen ausgetragenen vehement einschreiten muss. Ein kurzer, klärender Schlagabtausch kann befreiend und klärend wirken. Ein subtil ausgetragener Machtkampf unter den Kollegen kann das Team und das Projekt kaputt machen – das Thema Mobbing wird uns noch an anderer Stelle beschäftigen. Mit dem Thema Gewalt muss sich ein Projektleiter also zwangsläufig auseinandersetzen. „Aber, aber, meine Herren, wir sind doch alle erwachsen“ – nicht selten geht in solchen Situationen dem (unerfahrenen) Projektleiter der Allerwerteste auf Grundeis, wenn er nicht schon vorher das Handtuch geworfen hat.

Zugegeben, das wäre der „worst case“. Doch wir wollen hier ja keine Untergangsszenarien aufzeigen, sondern wie Sie dem Ganzen den Wind aus den Segeln nehmen. Konfliktauslöser können zu jedem Zeitpunkt des Projekts zum Ausbruch kommen. Klassische Beispiele wie eine gestörte Kommunikation gibt es viele: Beschuldigungen und Missverständnisse, Sympathien und Antipathien, kurz: Die ganze Bandbreite menschlicher Gefühle und Befindlichkeiten kann vorkommen und die Menschenkenntnis des Projektleiters herausfordern. Dazu kommen noch mögliche innere Konflikte der Teammitglieder, die zu einem störenden Verhalten beitragen. Einen solchen inneren Konflikt können wir etwa bei unserem vermeintlichen Großmaul ausmachen, der sich vom Team nicht respektiert und genug beachtet fühlt. Vielleicht wurde ihm schon in der Kindheit, später im Studium und dann in der Abteilung nie richtig zugehört.

Aber wo fängt Ihre Verantwortung als Konfliktlöser im Projektteam an, wo hört sie auf? Sicher sollten Sie im klärenden Gespräch mit dem Kollegen ein offenes Ohr für seine persönlichen Probleme haben, die eben in der Teamarbeit zum Tragen kommen („in meiner Ehe konnten wir auch nie reden, und jetzt hat mich meine Frau verlassen“). Aber bleiben Sie fokussiert auf das Projekt; schließlich lassen sich tiefgreifende, in der Person verwurzelte Konflikte nicht von heute auf morgen beseitigen. Aber vielleicht kann der Kollege so auf-

gebaut werden, dass er für die Laufzeit des Projekts teamfähiger wird. Projektleiter sind auch nur Menschen. Auf Konflikte reagieren sie mit ihrer eigenen Strategie:

- Der eine vermeidet von vornherein jeden Konflikt.
- Der andere lässt Konflikte zu, handelt aber nicht.
- Für manchen ist ein Konflikt ein willkommener Wettkampf, den es zu gewinnen gilt.
- Der eine lässt Konflikte zu, will sie aber nicht lösen.
- Der andere wünscht sich eine gemeinsame Lösung.

Wir müssen reden!

Miteinander reden fällt vielen Menschen überraschend schwer. Erwachsene Menschen in verantwortungsvollen Positionen sollten doch nicht gerade damit Probleme haben. Die Wahrheit ist, dass Projektarbeit kein Kaffeekränzchen ist. Zeit für persönliche Gespräche muss mühsam freigeschaufelt werden – besser, sie wird fest eingeplant, zum Beispiel regelmäßig in einer 20-Minuten-Runde am Jour fixe. Jeder darf frei formulieren, was ihn stört oder freut, ohne verurteilt zu werden. Bei kleinen Teams geht das noch; andernfalls ließe sich noch eine Pinnwand als „Klagemauer“ benutzen, an der jeder anonym seine Kommentare hinterlassen darf.

Mit dem Kommunikations-Guru Friedemann Schulz von Thun wollen wir uns noch einmal auf die empirische Ebene von sozialen Konflikten begeben: Kommunikation hat viele Gesichter, und eine Äußerung kommt bei mehreren Zuhörern unterschiedlich an. Sie kann sachlich daherkommen, als Selbstkundgabe, als Appell gar oder als Beziehungsbotschaft, wie Schulz von Thun es formuliert.

Als Projektleiter haben Sie also vier Kommunikations-Möglichkeiten, auf den umtriebigen Kollegen zuzugehen und ihn auf sein auffälliges Verhalten anzusprechen. Natürlich gehen Sie nicht zu ihm und sagen ihm ins Gesicht: „So, wie Sie ständig Ihren Senf dazugeben, vergraulen Sie mir noch das ganze Team!“. Welche Herangehensweise würden Sie spontan wählen?

a) „Sie sind omnipräsent und geben überall Ihre Kommentare ab.“ (sachlich)

- b) „Mich stört, dass Sie sich ständig einmischen.“ (Selbstkundgabe)
 c) „Mischen Sie sich nicht permanent ein!“ (Appell)
 d) „Wenn Sie alles besser wissen, bin ich wohl überflüssig.“ (Beziehungsbotschaft)

Wir können uns alle in der „Du-“ oder der „Ich“-Form äußern. Der Unterschied besteht darin, dass die jeweilige Botschaft vom Gegenüber unterschiedlich aufgenommen wird, auch wenn im Kern dasselbe Problem angesprochen wird: Was wird den anderen eher zum Nachdenken bringen – der Satz „Ich habe das Gefühl, Sie sind mit Ihrer Aufgabe unterfordert und würden gern noch andere Bereiche übernehmen.“ oder vielleicht „Sie sollten sich überlegen, ob Sie wirklich ins Projektteam passen?“? Zu jedem Konflikt gehören (mindestens) zwei, und so ist es nicht verwunderlich, wenn „Du“-Botschaften oft lehrerhaft und wenig subtil daher kommen: „Sie mischen sich zu viel ein, Sie untergraben ja die Kompetenz Ihrer Kollegen.“ Solche Aussagen zwingen den anderen in eine Verteidigungshaltung und werden als Schuldzuweisung aufgefasst. Mehr Bereitschaft zur Klärung können Sie erwarten, wenn Sie formulieren, was Sie persönlich empfinden. Bleiben Sie bei Ihrer Linie, auch wenn Ihr Gegenüber erst einmal abweisend reagiert („Sagen Sie mir doch bitte gleich, dass man mich im Team nicht braucht!“). Mit der nächsten „Ich“-Botschaft knacken Sie den Kollegen vielleicht: „Ich wünsche mir eben, dass Sie Ihre Arbeit im Team gerne machen, Sie sind ja dafür ausgewählt worden. Aber ich habe den Eindruck, Sie sind mehr an der technischen Umsetzung unserer Aufgabe interessiert als an den Tests, wie die Verkaufsabteilung mit der neuen Software klarkommt.“

Wer hat das Problem?

Im Beispiel hat die Gruppe ein Problem mit dem Kollegen, der sich einfach nicht richtig mit seiner Rolle identifizieren kann. Er selbst sieht das vermutlich gar nicht so. Um ein offenes Gespräch werden alle Beteiligten also nicht herumkommen. Gibt es aber ein Teammitglied, das zum Beispiel mit seinen Aufgaben im Gegensatz zu den anderen so gar nicht zu Recht zu kommen scheint, mit seinen Ergebnis-



sen hinterherhinkt, gestresst wirkt: Dann ist es Ihre Aufgabe als Projektleiter, Ihr Teammitglied zu beobachten und irgendwann zum Gespräch zu bitten.

Egal, ob es ein Problem gibt, das die ganze Gruppe betrifft oder einen Einzelnen, Konflikte lassen sich nur mit dem Instrument Kommunikation lösen. "Aktives Zuhören" ist dann Ihr Part als, wenn Sie so wollen, Mediator Ihres Projektteams (in seltenen Fällen muss tatsächlich ein echter Mediator oder Projektcoach von außen hinzugezogen werden). Aktiv zuhören bedeutet:

- Die eigenen Interessen (zunächst) zurückstellen, unparteiisch bleiben.
- Das Gehörte in eigenen Worten wiederholen – zum besseren Verständnis.
- Emotionen heraushören und ansprechen.
- Erst verstehen, dann verstanden werden.
- Wertschätzung und ehrliches Interesse am Gegenüber zeigen.
- Sich in den anderen hineinversetzen.

Wenn es nicht weiter geht

Verhärtete Fronten können Sie oft nicht mit nur einem klärenden Gespräch oder einem informellen Treffen beseitigen. Gerade, wenn mehrere Personen betroffen sind, ist anfangs unklar, wo der Auslöser des Konflikts zu suchen ist. Unzufriedenheit und Unsicherheiten äußern sich oft subtil – die Grenzen zum Mobbing sind hier fließend. So genannte Teufelskreise durchbrechen Sie nur sehr langsam – für die meisten Menschen gehören sie sogar derart zum (Berufs-)Alltag, dass vieles fraglos hingenommen wird.

Wir kennen das alle: Kollegin Schmid gibt sich "mal wieder zickig", lässt sich nichts sagen. Als ihr Vorgesetzter weisen Sie sie leicht genervt zurecht ("Frau Schmid, wir werden ja alle sehen, was am Ende dabei herauskommt."), wohl wissend, dass diese halbherzige Intervention nicht wirklich etwas bringen wird. Und wie sollte es anders sein: Die Kollegin reagiert erst recht schnippisch und blockt jegliche weitere Kommunikationsversuche ab – weiter geht es wie bisher. Dabei ist sie insgeheim der Meinung, selbstbewusst und durchsetzungsstark zu sein – als einzige Frau im Projektteam hat sie es eben manchmal nicht leicht und will in ihrer Kompetenz genauso anerkannt werden wie ihre

männlichen Kollegen. Die haben eigentlich gar kein Problem mit Schmid und finden ihr Fachwissen sogar recht beeindruckend. Nur offen ausgesprochen wurde ein Lob eben auch noch nie: Kein Wunder, dass Schmid sich eine Ellbogenmentalität angeeignet hat. Und der Chef? Sein Kommentar wird allenfalls als arrogant empfunden, sicher nicht als hilfreich.

Konfliktmuster durchbrechen

Bevor ein Konflikt eskaliert und Ihr Projektteam lahmlegt, schreiten Sie zur Tat. Bei all der Relevanz, die wir dem Menschlichen, dem Persönlichkeitsfaktor im Projektteam beimessen, dürfen Sie auch die ökonomische Komponente nicht vergessen. Schließlich haben Sie noch einen Auftraggeber im Nacken, der nicht begeistert sein wird, sollte er von Unstimmigkeiten im Team erfahren – als Geldgeber hat er ein berechtigtes Interesse am reibungslosen Vorankommen des Projekts. Brauchen Sie also den letzten Anstoß, eine komplizierte Situation zu klären, denken Sie an Ihr nächstes Meeting mit dem Lenkungskreis.

Eigentlich haben Sie für das Gespräch mit Ihrem Kollegen oder Ihrer Kollegin das nötige Handwerkszeug schon parat:

- Benennen Sie den Konflikt mit einer "Ich-Botschaft".
- Hören Sie aktiv zu.
- Sprechen Sie aus Ihrer Perspektive, vermeiden Sie Schuldzuweisungen.
- "Beziehungs-Botschaften" vermeiden ("Ja, also, wir alle sind der Ansicht, dass Sie...").
- Offene Fragen stellen, Diskussion anregen und fördern.
- Teufelskreise ansprechen.
- Interesse zeigen, keine faulen Kompromisse eingehen.
- Den anderen/seine Werte respektieren.

Zur Konfliktlösung tragen auch folgende Anregungen bei (in Anlehnung an die "Harvard-Methode"): Das Sachthema vom Menschen trennen. Wichtig sind nur Interessen, keine Positionen. Es ist besser, mehrere Lösungsalternativen zu erarbeiten, als nur einen Kompromiss zu entwickeln. Das Ergebnis des Konfliktgesprächs sollte von den Betroffenen noch einmal gemeinsam betrachtet werden. Wenn die Balance zwischen eigenen Bedürfnissen und denen

der anderen Teammitglieder wieder stimmt, haben beide Seiten gewonnen – setzt sich nur einer durch, haben Sie schon bald wieder die alte Situation. Konfliktgespräche zu führen, ist zugegebenermaßen nicht die Lieblingsaufgabe von Projektleitern, aber es gehört nun mal dazu.

Zur Orientierung stellen Sie sich die Lösung eines Konflikts im Team als fünfstufigen Prozess vor. Dieser umfasst auch ein klar definiertes "Ende" – damit auch alle wieder mit sortierten Gefühlen zur Tagesordnung übergehen können:

1. Vorbereitung: Klären Sie für sich Ihre Gefühle, Bedürfnisse und die Ziele, die Sie mit der Bereinigung des Konflikts verfolgen (es soll wieder Ruhe ins Team einkehren, alle wieder zu der Leistung zurückfinden, zu der sie ohne Störung eigentlich fähig sind). Gestalten Sie den Rahmen für das Ganze – zum Beispiel, indem Sie einen passenden Zeitpunkt und einen Ort für das Gespräch wählen. Versetzen Sie sich in den Konfliktpartner hinein, sammeln Sie Sachthemen. Überdenken Sie Ihre Botschaften.
2. Einstieg: Auch wenn Sie sich kennen – brechen Sie das Eis, nennen Sie Anlass und Ziel des Gesprächs. Stimmen Sie vorher gegebenenfalls mit Teamkollegen oder eigenen Vorgesetzten das Vorgehen ab, holen Sie sich eventuell von Dritten Anmerkungen ein.
3. Klärung: Sprechen Sie den Konflikt konstruktiv an, gehen Sie auf den Konfliktpartner ein. Planen Sie für das Gespräch mehr Zeit ein als für sonstige Unterhaltungen; der "verlangsamte Dialog" dient jetzt dazu, die Situation ein für alle Mal zu klären. Sonst übersehen Sie Missverständnisse, die ausgeräumt werden könnten. Wünsche und Bedürfnisse dürfen ausdrücklich genannt werden.
4. Lösungen: Sammeln Sie gemeinsam Ideen, wie der Konflikt gelöst, ein Streit beigelegt werden könnte. Treffen Sie Vereinbarungen und halten Sie sie fest; vergessen Sie nicht, nochmals Bedürfnisse zu klären ("Was halten Sie davon, beim nächsten Meeting als Erste Ihre Ergebnisse zu präsentieren, damit Sie nicht wieder die letzten unruhigen Minuten für Ihre Präsentation haben?")
5. Abschluss: Wenn sich die Parteien einig sind, dass alles besprochen wurde, fassen

Sie das Gesagte zusammen. Es muss Zeit sein, alles nochmals gemeinsam zu reflektieren. Was nehmen Sie alle mit aus der Situation (Lessons learned)? Finden Sie einen positiven Abschluss.

Alles im Lot

Es ist nicht immer leicht, andere voll und ganz in ihrer Persönlichkeit anzuerkennen – gerade am Arbeitsplatz und besonders im Projektteam, eine für kurze Zeit zusammengestellte Gruppe ohne sonstigem gemeinsamen Bezugspunkt, gehört dazu viel Toleranz und Menschenkenntnis. Können Sie das immer von allen erwarten? Zumindest Sie als Projektleiter sollten mit gutem Beispiel vorangehen. Arbeiten Sie in diesem Punkt an sich selbst: Wie es in den Wald hineinruft, so schallt es bekanntlich heraus. Hilfreich ist in diesem Kontext das Werte- und Entwicklungsquadrat, ursprünglich konzipiert vom Münchner Psychologen Paul Helwig, das der Kommunikations-Experte Friedemann Schulz von Thun in Bezug auf zwischenmenschliche Kommunikation weiterbearbeitet hat.

Demnach hat jeder (positive) Wert einen (positiven) Gegenwert; beide nehmen eine bestimmte negative Entwicklung, wenn die Balance nicht stimmt. So kann ein Mensch sparsam sein, aber auch großzügig, wenn es darauf ankommt. Wenn er nicht aufpasst, beide Werte in Balance zu halten, sieht ihn seine Umwelt jedoch schnell als Geizkragen; umgekehrt kann auch die Großzügigkeit in Verschwendungssucht umschlagen. Die als zickig empfundene, selbstbewusste Kollegin ist, sobald man mal zusammen am Kaffeeautomaten steht, offen und zugewandt. Beschränkt sie sich allerdings aus lauter Ehrgeiz nur noch aufs Berufliche und lässt auch in der Kantine nicht ein wenig Privatperson durchblicken, stemeln die Kollegen sie wahrscheinlich bald als abgehoben-karrieregeil ab. Umgekehrt könnte ihr zu viel Nähe auch den Ruf als "Projekt-Mama" einbringen, die sich um alles und jeden kümmert und am Ende nicht mehr für ihre Arbeit respektiert wird.

Eigenschaften, die wir am anderen gering-schätzen, können auch ein Hinweis darauf sein, dass wir eben jene insgeheim an uns vermissen. Genauer gesagt, ist diese Eigen-

schaft als "Schatten" in uns verborgen und kann aus bestimmten Gründen, die oft weit in der Kindheit wurzeln, nicht ausgelebt werden. Entsprechend lehnen wir sie als etwas, was nicht sein darf, auch bei anderen ab. Vielleicht wurden wir als Kinder ermahnt, anderen nicht zu viel von zu Hause zu erzählen und zogen uns zurück hinter eine perfekte Fassade, die keine näheren Einblicke duldet. Oder man brachte uns bei, nur etwas wert zu sein, wenn wir uns um andere kümmern, nett und angepasst sind. Die Kollegin, die sich also morgens nach den Kindern erkundigt oder fragt, ob wir unseren Kaffee mit Zucker trinken, behandeln wir unwirsch – obwohl wir uns eigentlich freuen, dass sie das lustige Kinderbild überm Schreibtisch entdeckt hat.

Niemand kann sich auf Dauer ausschließlich repräsentativ und sozialverträglich verhalten, ohne irgendwann über verdrängte innere Eigenschaften zu stolpern – sie begegnen einem früher oder später in Form eines anderen Menschen wieder. Er ist unser "Anti-Typ", und wenn wir ihn ablehnen, führen wir im Grunde einen kleinen Krieg gegen uns selbst.

Fazit

Es wäre wünschenswert, auch und vor allem in der Arbeit mit Projektteams, sich um diese gegenseitige Akzeptanz zu bemühen. So manche Konflikte könnten vermieden werden, viel Zeit und Geld gespart werden – und die Nerven des Projektleiters geschont –, wenn man sich hin und wieder mit derjenigen Person näher beschäftigt, mit der man am wenigsten gut zusammenarbeiten kann oder mag. Auch der Projektleiter muss oft mit einem Team vorliebnehmen, das er gern anders zusammengestellt hätte. Doch gerade dann, wenn die unterschiedlichsten Menschen zusammen auf ein Ziel hinarbeiten müssen, haben sie das größte Entwicklungspotential. (jp) 

Dr. Markus Blaschka ist geschäftsführender Gesellschafter der 2006 gegründeten Dr. Blaschka Consulting GmbH (www.drblaschka-consulting.eu) mit Sitz in Raubling. Der Fokus des Unternehmensberaters, Trainers und Coach liegt auf Menschen, Persönlichkeiten und Projekten, was ihn vor allem in der IT- und Automotive-Branche zum Experten in Sachen Projektmanagement gemacht hat.

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



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.



Wir nutzen in unserem Unternehmen zur Virtualisierung Hyper-V. Beim **Einrichten des System Center Virtual Machine Manager** per Bare Metal Deployment mit Hilfe des Cmdlets **New-SCVMMHost** sahen wir uns nun schon mehrfach dem Problem gegenübergestellt, dass der Prozess stets mit der gleichen Meldung fehlschlug: "Error (21117). Cannot find an OS present in the VHD which support native VHD boot. Recommended Action: Verify the vhd file". Wir sind uns jedoch ziemlich sicher, dass die VHD-Dateien in Ordnung sind – zumal bei unterschiedlichen VHD-Files immer die gleiche Fehlermeldung erscheint. Kann es denn andere Gründe für die geschilderte Problematik geben?

Sie haben Recht in der Annahme, dass Ihr VHD-Image in bester Ordnung ist. Die von Ihnen beschriebene Fehlermeldung kann sich nämlich auch bemerkbar machen, wenn das Windows Automated Installation Kit (WAIK) in einer anderen Sprache als Englisch installiert wurde. In einem derartigen Fall hilft ein kleiner Workaround: Stellen Sie zunächst die WAIK-Ressource (CD, ISO) bereit und wechseln Sie in das Verzeichnis "x:\WinPE_LangPacks \ amd64". Kopieren Sie von dort den Ordner "en-us" in das Host-Verzeichnis "C:\Program Files \ Windows AIK \ Tools \ PETools \ amd64 \ WinPE_FPs". In diesem Directory existieren nun zwei Ordner, der eben hineinkopierte "en-us" und der ursprüngliche, zum Bei-

spiel "de-de". Nachdem Sie auch Englisch auf das System gebracht haben, müssen Sie die Spracheinstellungen noch in SCVMM respektive in WDS (Windows Deployment Services) bereitstellen. Dazu führen Sie ein Update des WinPE-Image aus. Mit der Konsole funktioniert dies über "Fabric / PXE Server / Update WinPE Image". Alternativ klappt dies mit dem Kommando **Publish-SCWindowsPE -UseWindowsAIK** auch über die Shell. Führen Sie dann den Vorgang zum Bare Metal Deployment erneut aus. Haben Sie die oben beschriebenen Schritte ausgeführt, bevor der PXE-Server zum VMM hinzugefügt wird, verwendet das System von Beginn an das korrekte WinPE-Image. (Michel Lüscher/ln)



Weitere Informationen zu Server 2008 R2 und Hyper-V finden Sie im Internet auf www.server-talk.eu

Immer wieder mal kommt es in unserer Umgebung vor, dass ein Client aus der Domäne fällt, weil er kein gültiges Passwort mehr besitzt, mit dem er sich im Active Directory anmelden kann. Nicht immer sind die Gründe für ein plötzlich ungültiges Passwort auf den ersten Blick ersichtlich. Bei der Analyse würde uns schon helfen, wenn wir sehen könnten, wann das Kennwort im Active Directory und wann es auf dem Client selbst geändert wurde. Gibt es hierzu eine einfache Möglichkeit?

Mit dem folgenden Vorgehen können Sie vergleichen, wann der Netlogon-Dienst zuletzt das lokale Passwort geändert hat und wann es im Active Directory (AD) zuletzt zu einem Neusetzen des Kenn-

worts kam. Um dieses Datum für den lokalen Computer zu bestimmen, laden Sie zunächst unter [Link-Code C5PE4] das Sysinternals-Tool *PsExec.exe* herunter. Dies ist deshalb ratsam, da Netlogon den lokalen Passwort-Hash in der Registry unter "HKEY_LOCAL_MACHINE \ SECURITY \ Policy \ Secrets \ \$MACHINE.ACC" ändert. Der Registry-Hive "SECURITY" ist jedoch per Default selbst dem lokalen Administrator nicht zugänglich. Damit Sie die Permissions nicht modifizieren müssen, greifen Sie auf das Werkzeug von Sysinternals zurück und führen *regedit.exe* mit dem Kommando **psexec.exe -s -i regedit.exe** im Systemkontext interaktiv aus. Im Registry-Editor navigieren Sie dann zum Eintrag "HKEY_LOCAL_MACHINE \ SECURITY \ Policy \ Secrets \ \$MACHINE.ACC \ CurrVal". Über das Kontextmenü exportieren Sie nun diesen Key mit der rechten Maustaste über "Export Registry File" als TXT-Datei. Ist dies erfolgt, können Sie in der ausgegebenen Datei *sec_currval.txt* in der Zeile "Last Write Time" den Zeitpunkt der letzten Änderung des Passworts einsehen. In einem zweiten Schritt sehen Sie sich die Änderung des Computer-Kennworts im AD an. Dazu benötigen Sie jedoch – sofern nicht schon bekannt – die Kennung des Domänencontrollers (Trusted DC Name) und den Distinguished Name (DN) des entsprechenden Clients. Das Kommando **NLTEST /SC_QUERY:Domäne** führt zu einer Ausgabe der DC-Kennung in einer wie folgt aussehenden Zeile: **Trusted DC Name \\MyDC01.contoso.com**

Den Distinguished Name (DN) des Clients geben Sie über das Kommando `SETSPN /L Computername` oder mittels PowerShell und `get-adcomputer Computername` aus, wenn das AD-Modul für die PowerShell installiert ist. Der DN des Rechners ist nach der Zeile "Registered ServicePrincipalNames for:" zu lesen und lautet etwa `CN=MyClient01,OU=workstations,OU=Machines,DC=contoso,DC=com`

Diese beiden Informationen kombinieren Sie nun in einem `repadmin`-Kommando mit der Syntax

```
repadmin / showobjmeta Trusted DC
Name DN des Clients
```

Gemäß den obigen Ausgaben lautet der vollständige Befehl in unserem Fall also `repadmin /showobjmeta MyDC01`

```
"CN=MyClient01,OU=workstations,
OU=Machines,DC=contoso,DC=com"
```

In der nun ausgegebenen Tabelle verrät Ihnen der Eintrag "pwdLastSet", wann im AD eine Änderung des Computer-Passworts erfolgte. Bei Fehlersituationen unterscheiden sich die Daten der Änderung am Computer und im AD. Wenn das lokale Computer-Kennwort neuer ist als das im AD, kann es sich um einen "Replication Delay" handeln oder generell um Replikationsprobleme. Wenn das AD konsistent eine ältere Änderung anzeigt, wurde der AD-Stand eventuell durch einen AD-Restore zurückgesetzt. Möglich ist ferner, dass der Client das neue Passwort zwar lokal setzt, dann aber keinen DC erreichen kann, um es im AD abzugleichen. Nicht zuletzt kann es vorkommen, dass der Client einen RODC kontaktiert, aber in der Password Replication Policy nicht eingetragen ist. Wenn das lokale Computer Passwort älter ist als das im AD, mag ein Problem darin liegen, dass der Computer selbst durch einen Restore

zurückgesetzt wurde und damit auch der Registry Hive "SECURITY". Dies kann etwa durch eine automatische System-Wiederherstellung passieren, zum Beispiel wenn das System abstürzt. In einer derartigen Situation muss der Client-PC dann der Domäne neu beitreten. (ln)

Group Policy Objects (GPOs) sind auch in unserem Unternehmen ein weit verbreitetes und beliebtes Instrument, um Clients im Active Directory zu verwalten. Wenn wir nun die Einstellung der Windows-Firewall über GPOs konfigurieren, kommt es bisweilen vor, dass die gerade gemachten Settings nicht gespeichert und somit nicht wirksam werden. Im Event Log findet sich kein Hinweis auf eine diesbezügliche Fehlfunktion. Wo liegt hier das Problem?

Das von Ihnen beobachtete Phänomen ist bekannt und entspricht dem Design der Windows-Firewall GPO Extension: Die Konfiguration wird über ein API vorgenommen, und zwar von vielen unterschiedlichen Anwendungen heraus (netsh, mmc, directaccess, powershell et cetera). Das ist auch der Grund, warum Sie die hier vorgenommenen Änderungen sofort anwenden müssen – gehen Sie nach Änderungen an der Konfiguration der Windows Firewall auf eine beliebige andere Einstellung einer (in `registry.pol` abgespeicherten) Komponente und ändern diese, kommen die ursprünglichen Modifikationen an der Firewall nicht zur Ausführung. Intern erzeugt das System beim Bearbeiten einer Policy einen temporären GUID und einen Registry Key, wo es die Änderungen der GPedit-Session speichert. Diese GUID / Registry Key-Kombination wird auch von allen anderen Komponenten genutzt – außer von der Windows Firewall. Diese legt eine eigene temporäre Kombination an. Aus diesem Sachverhalt ergibt sich die sinnvollste Lösung, um die beschriebene Problematik zu umgehen: Nehmen Sie Firewall-Konfigurationen am besten in einer eigenen GPO vor. (ln)



Wir haben kürzlich **Citrix VDI-in-a-Box 5.0** eingeführt. Gelegentlich werden einzelne Anwender dort sofort **automatisch vom System abgemeldet**, nachdem sie sich mit ei-

nem virtuellen Desktop verbunden haben. Woran könnte dies liegen?

Das sofortige Abmelden eines Nutzers kann mehrere Gründe haben. Sie sollten zunächst darauf achten, dass beim Einloggen über die Konsole von VDI-in-a-Box der gleiche Benutzername Verwendung findet wie unter Windows. Bei Abweichungen lässt sich die Verbindung möglicherweise nicht ordnungsgemäß aufbauen. Sie sollten die Anwender also darauf hinweisen, zu jeder Zeit die identischen Login-Daten zu verwenden. Für die automatische Abmeldung eines VDI-Nutzers kann allerdings auch der erzwungene Reboot des zugrunde liegenden Desktops verantwortlich sein. Deaktivieren Sie dort daher möglichst alle Dienste, die für einen ungewollten Neustart sorgen könnten. (Citrix/ln)



Google Chrome

Für den ein oder anderen Support-Fall nutzen meine Kollegen und ich unterschiedliche Werkzeuge zum Remote-Zugriff. Nun hat mir ein Bekannter erzählt, dass ein derartiger Fernzugriff – einmal abgesehen von Microsofts Remotedesktopverbindung – auch mit Bordmitteln möglich ist. Voraussetzung sei jedoch, dass der Browser Google Chrome auf beiden Systemen installiert ist. Stimmt dies und wenn ja, wie kann ich eine derartige Verbindung einrichten und starten?

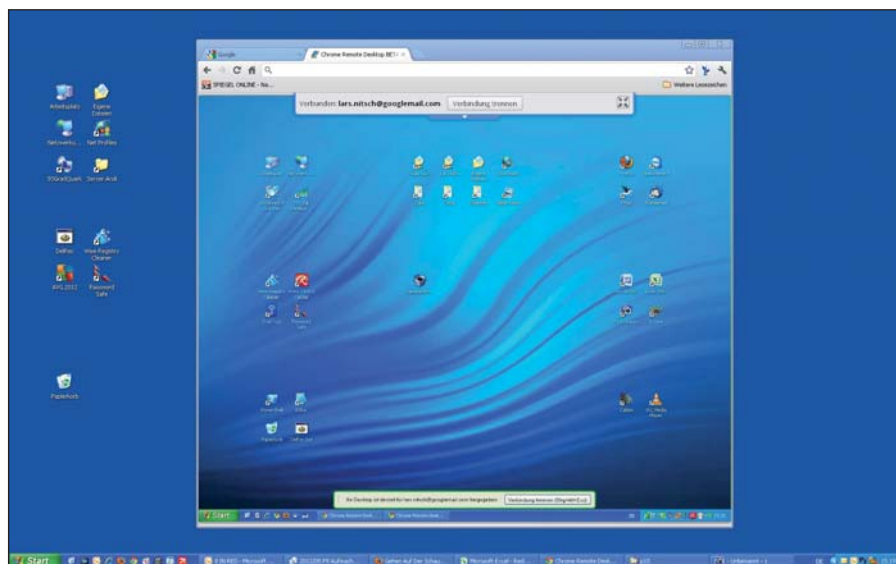
Dass Sie den Zugriff auf einen entfernten Computer mit Google Chrome und Bordmitteln durchführen, ist nicht zu 100 Prozent korrekt. Vielmehr bedarf es dazu der Installation der Chrome-App "Chrome Remote Desktop", die Sie unter [Link-Code C5PE5] im Chrome Web Store herunterladen können. Beachten Sie, dass es sich bei dem Add-on um eine Beta-Version handelt und dass Sie über ein Google-Konto verfügen müssen, um die App zu verwenden. Sind Sie mit beiden Prämissen einverstanden, haben Sie jedoch eine äußerst praktische Möglichkeit für die Fernwartung zur Hand. Nach der Installation der App und der Anmeldung über Ihr Google-Konto klicken Sie zunächst auf die Schaltfläche "Neuer Tab". Sie haben dann die Möglichkeit, über das entsprechende Icon eine Verbindung aufzubauen. Beachten Sie, dass eventuelle Tab-Erweiterungen für

Viele weitere Tipps & Tricks sowie konkrete Hilfe bei akuten Problemen bekommen Sie auch im Internet bei unserem exklusiven Foren-Partner 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 praxisnahe Fachmagazin für Administratoren ist administrator.de die Internetplattform für alle System- und Netzwerkadministratoren.

www.administrator.de



ADMINISTRATOR | IT-FORUM



Mit dem Chrome Remote Desktop gelingt es beinahe mit Bordmitteln, problemlos von einem Rechner auf einen entfernten PC zuzugreifen

Chrome die Standardseite verändern können, die beim Drücken des Buttons "Neuer Tab" erscheint. Deaktivieren Sie in diesem Fall (temporär) die entsprechende Erweiterung. Die Funktionsweise des Chrome Remote Desktops ist ganz einfach: Wollen Sie Ihren PC für einen Zugriff freigeben, klicken Sie auf "Jetzt freigeben" bei "Diesen Computer für einen anderen Nutzer zur Ansicht und Steuerung freigeben". Dann erhalten Sie einen zwölfstelligen Zugriffscode, den Ihr Gegenüber in seinem Browser eingeben muss, nachdem er auf "Jetzt zugreifen" bei "Freigegebenen Computer sehen und steuern" geklickt hat. Die gesamte Kommunikation zwischen den beiden Rechnern läuft verschlüsselt. Besonders praktisch: Googles Lösung arbeitet plattformunabhängig, so dass Sie die Software überall dort einsetzen können, wo Chrome läuft – dies schließt Windows, Linux, Mac OS X und Chromebooks ein. (ln)



Linux

Auf meiner aktuellen Fedora-Distribution kann ich meine System-Services nicht mehr wie gewohnt über ein SystemV-Skript und das Service-Kommando starten. In früheren Versionen war dies problemlos möglich. Was hat sich hier verändert?

Die Entwickler haben beim aktuellen Fedora das in die Jahre gekommene Init-System durch den moderneren System- und Service-Dienst "Systemd" ersetzt.

Das in C geschriebene Programm soll die Abhängigkeit zwischen den einzelnen Diensten besser berücksichtigen und die Performance durch Parallelisierung steigern. Systemd kümmert sich dabei nicht mehr nur um Prozesse, sondern beispielsweise auch um Sockets und Dateisysteme. Er ist deshalb wesentlich leistungsfähiger als das alte Init-System. Die einzelnen Objekte bezeichnet Systemd als Units. Eine Liste aller Service-Units gibt der folgende Befehl aus:

```
# systemctl list-units -type service
```

Um nun beispielsweise den SSH-Server zu starten und sich im Anschluss daran den Status des Dienstes ausgeben zu lassen, sind die beiden folgenden Kommandos einzugeben:

```
# systemctl start sshd.service
# systemctl status sshd.service
```

Um einen Dienst dauerhaft zu starten, so dass dieser auch nach einem Reboot des Systems zur Verfügung steht, ist folgender Befehl notwendig:

```
# systemctl enable sshd.service
```

Dies entspricht in etwa dem alten Befehl `chkconfig` auf SysV-basierten Systemen. (Thorsten Scherf/ln)



Tools

Heutzutage gibt es für IT-Verantwortliche eigentlich kaum Gründe, auf eine automatisierte **Inventarisierung** zu verzichten. Ganz im Gegenteil drängen Sicherheits- und auch Gesetzesfragen die IT-Abteilungen nachdrücklich zur **Etablierung eines solchen Datenbestandes**. Erschwerend kommt für die Inventarisierungs-Verweigerer hinzu, dass Programme, die eine professionelle Inventarisierung ermöglichen, mittlerweile kostenlos zu haben sind. Und wenn noch eine Softwareverteilung an Bord ist und das Netzwerk geschont wird, sollten wir unverzüglich alle zu Ja-Sagern werden.

All dies bietet nämlich das kostenlose **OCS Inventory NG**: Inventarisierung von Hard- und Software kombiniert mit einer Funktion zur Verteilung von Betriebssystemen und Anwendungen. Und dabei wickelt OCS Inventory seine Aufgaben über HTTP ab und schont so die verfügbare Bandbreite Ihres Netzwerks. Das Werkzeug arbeitet zur **Inventari-**

Tag Type	Last inventory	Computer	User	Operating system	RAM (MB)	CPU (MHz)	Delete
PORTABLE	2011-03-16 19:25:10	BZO	Ouilaume	Microsoft Windows XP Professional	2000	2393	X
SERVEUR	2011-03-16 07:36:03	hufu	root	Debian GNU/Linux 6.0 (squeeze)	757	2171	X
SMARTPHONE	2011-03-15 20:07:35	KS-20		Windows CE	209		X
PC FINE	2011-02-26 21:52:27	GUILAUME	goula	Microsoft Windows XP Professional	2048	2671	X
SERVEUR	2011-02-22 13:47:01	W16753500P2	Administrateur	Microsoft Windows(R) Server 2003, Enterprise Edition	512	2682	X
SERVEUR	2011-02-22 13:43:50	LABO-AV-2K-04	Administrateur	Microsoft Windows(R) Server 2003, Standard Edition	1280	995	X
SERVEUR	2011-01-05 18:48:11	thelid	root	OpenBSD AMD Athlon(TM) 64 Processor 3500+	2048	0	X
PC FINE	2011-01-05 18:47:44	SNOOPY-DIDIER	didier	Microsoft Windows 7 Edition Intégrale	2048	2200	X
VM OPENBSD	2011-01-05 18:47:00	ocs-server	luser	OpenBSD Intel(R) Pentium(R) 4 CPU 2.80GHz (Celeron/Intel® 686-class)	2039	0	X
SERVEUR	2011-01-05 18:46:15	ocs-openuse	root	openUSE 11.3 (598)	499	1919	X

Das kostenlose OCS Inventory bietet eine Kombination aus Inventarisierung und Softwareverteilung

sierung mit einem Agenten, der sowohl auf Clients als auch auf Servern zum Einsatz kommt und die gesammelten Daten an den Management Server weitergibt. Dabei ermitteln die Agenten ein umfassendes Set an Daten zu jedem Rechner. Enthalten sind detaillierte Daten zum Betriebssystem, der installierten Software, den verwendeten Laufwerken und weiterer Peripherie. Und auf Basis dieser Daten erlaubt OCS Inventory das **Erstellen und Verteilen von Softwarepaketen** für die Clients. Diese stößt der Administrator am Management Server an, der die Verteilung über HTTP anstößt und gleichzeitig den IT-Verantwortlichen mit laufenden Berichten zum Fortschritt der Verteilung auf dem Laufenden hält. Der Administrator steuert OCS – genauer gesagt den Management Server – über die integrierte **Web-Administrations-Konsole**. Diese ermöglicht neben der Übersicht aller laufenden Vorgänge umfangreiche Zugriffsmöglichkeiten auf alle Funktionen. Systemvoraussetzungen sind die Betriebssysteme Microsoft 2000 und höher. Die Anwendung ist jedoch auch unter Linux lauffähig und unterstützt zudem die Verteilung von Linux/Unix. (jp)

Link-Code: C5PE1

Nach wie vor zählt das Dateiformat **PDF** zu den gefährlichsten **Transportmechanismen für Schadsoftware** in das Unternehmen. Dies begründet sich zum einen auf die große Beliebtheit und Verwendungshäufigkeit von PDF, zum anderen auf eine scheinbar nicht abreißen wollende Liste an gefährlichen Sicherheitslöchern. So sind denn auch viele Szenarien vorstellbar, in denen es wichtig und nützlich zu wissen ist, was sich in einem verseuchten PDF genau versteckt.

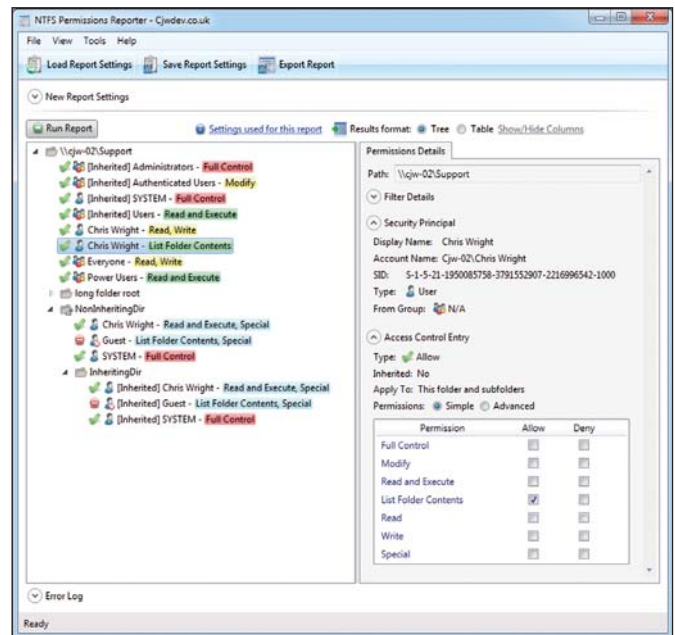
Zum Zweck einer solchen PDF-Analyse stellt Sicherheitsexperte und -Blogger Didier Stevens **zwei kostenlose Werkzeuge zur PDF-Forensik** bereit. Die Tools pdf-parser und pdfid.py arbeiten dabei zusammen bei der **Analyse des im PDF enthaltenen Schadcodes**. Die Details der Funktionsweise der beiden Werkzeuge, eine umfangreiche Anleitung und Video-Tutorials von Stevens finden Sie, wenn Sie unserem Link-Code folgen. Wir werden darauf nicht im Detail

eingehen, denn der Leser sei gewarnt: Dies sind Werkzeuge für echte Sicherheitsspezialisten, die "normale" Administratoren unter Umständen überfordern und so mehr schaden als nutzen. Auch ersetzen sie in keinem Fall eine moderne Security-Infrastruktur gegen das Eindringen von Schadsoftware ins Unternehmen. Für Sicherheitsexperten oder zum Einsatz auf einem Testsystem sind die beiden Werkzeuge aber absolut empfehlenswert und können sehr wertvolle Informationen liefern. (jp)

Link-Code: C5PE2

Administratoren, die viel mit Systemdateien arbeiten beziehungsweise diese modifizieren und ändern, müssen dazu oftmals die Besitzrechte, Sicherheitseinstellungen und Zugriffsrechte für eine solche Datei ändern. Der übliche Weg dazu führt über einen Rechtsklick auf eine Datei oder einen Ordner, die Auswahl der Eigenschaften und ein Klick auf den Reiter "Sicherheit". Hier erhält der IT-Verantwortliche für jede Datei und jeden Ordner angezeigt, wem die Besitzrechte zugesprochen sind und welche Zugriffsrechte bestimmte User und Gruppen haben. Doch schon diese Beschreibung lässt erahnen, dass dieser Prozess bei vielen Dateien und vielen Rechten darauf leicht unüberschaubar wird.

Das freie Werkzeug **NTFS Permissions Reporter** schafft hier Abhilfe. Es erlaubt Administratoren, sich schnell einen **Überblick über die Zugriffsrechte und die Sicherheitseinstellungen** zu verschaffen. Ebenfalls reportet das Werkzeug die **Besitzrechte von Dateien und Ordnern**. Das Programm listet die gewünschten Daten nach Auswahl der Partitionen, Ordner und Dateien detailliert auf. Ändern lassen sich diese Einstellungen aus dem NTFS Permissions Reporter jedoch nicht. Nach der Instal-



Mit dem NTFS Permissions Reporter kommt Licht ins Dickicht der Dateiberechtigungen

lation und dem Start des Programms legt der Administrator zunächst den zu scannenden Bereich fest. Dies erfolgt auf Basis der durch das Programm angezeigten vorhandenen Partitionen. Der Scanbereich lässt sich individuell anpassen, etwa indem ein einzelner Ordner außerhalb der festgelegten Partition zusätzlich ausgewählt wird. Als Ergebnis der Recherchierung erhält der Administrator eine Übersicht der einzelnen Ordner und der darin enthaltenen Dateien mit ihren Sicherheitseigenschaften. Der NTFS Permissions Reporter liegt neben der freien auch als Kaufversion vor, doch erfreulicherweise bietet die freie Version dem IT-Verantwortlichen einen Funktionsumfang, der in vielen Fällen ausreicht. (jp)

Link-Code: C5PE3

Auf der Homepage des IT-Administrator-Magazins stellen wir jede Woche für Sie ein praktisches Tool zum Download bereit. Neben einer Kurzbeschreibung finden Sie Systemvoraussetzungen und alle weiteren wichtigen Informationen auf einen Blick. Und können so gezielt Werkzeuge für Ihren täglichen Administrationsbedarf herunterladen.

www.it-administrator.de/downloads/software/

Download der Woche

WAN-Optimierung vs. RDP-Beschleunigung

Turbo für die Virtualisierung

von Alexander Vierschrodt



Quelle: mareandmare – 123RF

Virtuelle IT-Umgebungen liegen auch im Desktop-Bereich im Trend. Die Vorteile wie Konsolidierung, niedrige Ausfallzeiten und mehr Flexibilität für die Mitarbeiter liegen aus Unternehmenssicht auf der Hand. Die Anwender hingegen kämpfen nicht selten mit langsamem Bildaufbau, verzögerten Anwendungsstarts oder eingefrorenen Systemen. Abhilfe versprechen WAN-Optimierer und RDP-Beschleuniger. Dieser Artikel zeigt die Vor- und Nachteile beider Techniken auf und soll bei der Kaufentscheidung helfen.

Immmer mehr Unternehmen setzen auf virtualisierte IT-Landschaften. Die Server-Virtualisierung hat sich über Jahre bewährt, sodass der Schritt hin zur Virtualisierung von Desktops und Anwendungen auf den ersten Blick logisch erscheint. Die Umsetzung gestaltet sich bei vielen Unternehmen jedoch nicht so einfach wie im Server-Bereich. Egal, ob virtuelle Desktops und Anwendungen oder Terminalserver-Strukturen – die Mitarbeiter erleben die Virtualisierung nicht immer als den Heilsbringer der IT-Zukunft. Der Grund dafür ist oftmals in überlasteten Unternehmensnetzwerken oder in langsamen WAN- und Mobilfunkstrecken zu finden. Gerade Außenstellen und mobile Mitarbeiter sind besonders häufig unzufrieden mit der Leistungsfähigkeit der virtuellen Umgebungen.

User werden ausgebremst

Allen Virtualisierungstechnologien gemein ist die Notwendigkeit eines Protokolls zur Übertragung der Bildschirmhalte an das Endgerät. Als De-Facto-Standard hat sich das von Microsoft entwickelte Remote Desktop Protocol (RDP) durchgesetzt. Trotz der enormen Weiterentwicklung des RDP-Protokolls seit seiner Entstehung um die Jahrtausendwende gibt es auch heute noch Optimierungsbedarf, insbesondere wenn es um die Übertragung von

Multimedia-Inhalten oder die Nutzung schmalbandiger WAN-Verbindungen geht. Denn in diesen Fällen müssen die Anwender oft lange Wartezeiten und einen insgesamt nicht zufrieden stellenden Arbeitskomfort hinnehmen. Bemängelt werden in erster Linie langsam reagierende Anwendungen, unzureichende Darstellung von Multimedia-Dateien und eingefrorene Bildschirmhalte.

Besonders häufig treten diese Probleme bei der Nutzung virtualisierter Anwendungen und Desktops außerhalb des Firmen-LANs auf – also über WAN- oder mobile Datenleitungen. Zur Lösung der Probleme weichen manche Unternehmen auf alternative Protokolle aus oder investieren in teure Maßnahmen zur Netzwerk-Optimierung. Viele Organisationen verzichten aus diesen Gründen sogar ganz auf moderne Virtualisierungstechnologien und deren Vorteile. Dabei gibt es durchaus praktikable und bezahlbare Lösungen, die auch in virtuellen Umgebungen den Nutzerkomfort ermöglichen, den die Anwender von klassischen EDV-Systemen gewohnt sind.

Den Transport oder das Protokoll beschleunigen

Um die Leistungsfähigkeit virtualisierter IT-Infrastrukturen zu steigern, gibt es

grundsätzlich zwei Ansatzpunkte: das Transportmedium, sprich das Netzwerk, und das Protokoll – in den allermeisten Fällen ist dabei RDP der Ausgangspunkt. Bei der Netzwerkoptimierung geht es in erster Linie darum, Bandbreite und Latenzzeit zu optimieren, da diese Parameter den größten Einfluss auf die Übertragung der Bildschirmhalte haben. Das gilt für LAN, WAN und Mobilfunk gleichermaßen. Da sich die beiden Faktoren auch gegenseitig beeinflussen, bringt es nichts, nur an einer Schraube zu drehen. Viele Unternehmen mit virtualisierten Systemen haben bereits große Summen in die Erhöhung ihrer Netzwerkbandbreiten investiert und dennoch keine Verbesserungen in Sachen User-Experience verzeichnen können – etwa weil die Latenzzeit außer Acht gelassen oder andere komplexere Ursachen für mangelnde Netzwerk-Performance nicht aufgedeckt wurden.

Beim zweiten Ansatzpunkt geht es nicht darum, das Netzwerk zu optimieren, sondern um die Beschleunigung des Übertragungsprotokolls. Microsoft selbst hat RDP über die Jahre in Sachen Performance und Features stark verbessert. Die aktuelle Version 7 ist den Vorgängerversionen im Umgang mit eingeschränkter Netzwerk-Performance deutlich überle-

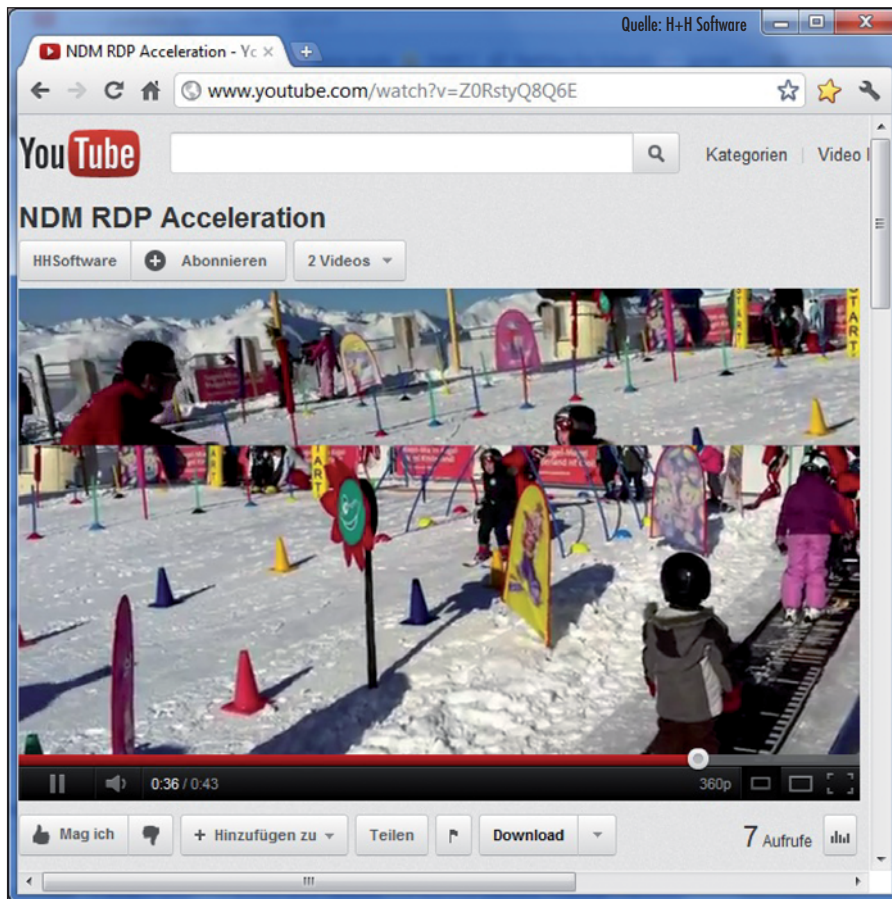


Bild 1: Gerade bei eher schmalbandigen RDP-Verbindungen kann es bei Multimedia-Inhalten zu Aussetzern kommen

gen. Dennoch zeigt das Protokoll gerade bei WAN-Verbindungen mit gleichzeitig geringer Bandbreite und hoher Latenz Schwächen. Das gilt ebenso für überlastete LANs und insbesondere für Verbindungen über das Mobilfunknetz. Am häufigsten treten Schwierigkeiten auf, wenn mobile oder Home Office-Mitarbeiter auf grafiklastige Anwendungen und Daten wie etwa PDF-Dokumente, Powerpoint-Präsentationen, Videos und Flash-Animationen zugreifen.

RDP und seine Schwächen

Bei grafiklastigen Anwendungen kommt RDP schnell an seine Grenzen. Und dabei nimmt der Anteil an Animationen, Effekten und eingebetteten Videos stetig zu. Hinzu kommt, dass der Bildaufbau ursprünglich auf sehr langsame Wählverbindungen hin optimiert war. Dabei erfolgt die Datenübertragung idealerweise in kleinen Paketen. Hierdurch erscheint RDP leistungsfähiger, da Bilder schrittweise aufgebaut werden und erst nach und nach an Detailtiefe gewinnen. In Netzwerken mit hoher Bandbreite hin-

gegen ist diese Methode des Bildaufbaus nicht sinnvoll, da sie in langsamerer und schlechterer Bilddarstellung resultiert. Eine weitere Schwachstelle von RDP ist die Kompression der zu übertragenden Daten. Diese betrifft in erster Linie Bilder und erfolgt verlustfrei. Damit ist sichergestellt, dass die Darstellungsqualität der Bilder stets einwandfrei ist.

Das Manko der verlustfreien Kompression liegt in der vergleichsweise geringen Kompressionsrate. Mit RDP 7 hat Microsoft erstmals einen verlustbehafteten Kompressions-Algorithmus eingeführt. Die Kompressionsrate ist jedoch eher gering und führt nur zu einer geringen Steigerung der Effizienz. Ebenfalls neu ist die Umleitungs-Funktion für Multimedia-Inhalte. Mithilfe der so genannten Multimedia Redirection verlagert RDP 7 die für die Darstellung von Multimedia-Inhalten erforderliche Rechenarbeit vom Server zum Client. Dieses Vorgehen reduziert die zu übertragende Datenmenge signifikant. In früheren Versionen von RDP wurden etwa Filme

zuerst auf dem Server gerendert und dann als speicherintensive Bitmaps an die Clients übertragen.

Um in den Genuss der neuen Funktionen und verbesserten Performance zu kommen, ist jedoch als Host der Einsatz von Windows Server 2008 R2 zwingend erforderlich. Ältere Serversysteme lassen sich nur mit dem deutlich leistungsschwächeren RDP 6.x nutzen. Weitere neue Funktionen in RDP 7 sind die vollständige Unterstützung der Aero-Oberfläche, Multimonitor-Support sowie verbesserte Multimedia- und Druckfunktionen. Je nach Anwendungsgebiet ist RDP 7 den vorherigen Versionen deutlich überlegen.

WAN-Beschleuniger müssen mitdenken

Da Verzögerungen bei der Übertragung der Datenströme und dem Bildaufbau in den meisten Fällen auf mangelnde Leistungsfähigkeit des Transportmediums zurückzuführen sind, bietet sich eine Optimierung der genutzten Infrastrukturen an. Dabei sind die Möglichkeiten, die sich im lokalen Netzwerk bieten, recht einfach handzuhaben und in den meisten Unternehmen weitgehend umgesetzt. Die Rede ist von modernen, managbaren Netzwerkkomponenten, ausreichend dimensionierter Bandbreite und der Anbindung der Endgeräte über schnelle Kupfer- oder Lichtwellenstrecken. Hinzu kommt, dass die Übertragung virtueller Desktops oder Terminalservices im LAN die geringsten Schwierigkeiten bereitet.

Optimierungsbedarf besteht in erster Linie für Datenleitungen, die externe Standorte oder mobile Mitarbeiter mit dem Rechenzentrum des Unternehmens verbinden sollen – also entweder über WAN- oder Mobilfunkstrecken. Bei Letzteren sind den Unternehmen allerdings in Sachen Beschleunigung die Hände gebunden, außer dass sie sich für den in der entsprechenden Region stärksten Mobilfunkanbieter entscheiden können. An der meist sehr hohen Latenzzeit selbst von breitbandigen HSDPA-Verbindungen ist nichts zu ändern. Für WAN-Datenleitungen hält der Markt hingegen zahlreiche Beschleuniger-Produkte bereit. Dabei handelt es sich für gewöhnlich um Ap-



pliances, die für eine Priorisierung von Datenströmen sorgen, die deutlich über das klassische Quality-of-Service-Verfahren hinausgeht. Obendrein arbeiten WAN-Optimizer mit einer starken Kompression des Datenstroms, die protokoll- und anwendungsspezifisch genutzt werden kann. Ziele der WAN-Optimierung sind schnellere Antwortzeiten von Anwendungen, eine bessere Ausnutzung der bereitgestellten Bandbreite und eine Reduzierung der Netzwerk-Latenz.

Appliances eignen sich nicht für jedes Einsatzgebiet

Die Verfolgung dieser Ziele gelingt den WAN-Beschleunigern jedoch auf unterschiedliche Weise. So arbeiten manche Appliances recht pragmatisch, indem sie einfach alle Daten möglichst stark komprimieren, um Bandbreite zu sparen. Das ist grundsätzlich ein guter Ansatz, führt aber nicht zu einer optimalen Beschleunigung von Remote-Desktop-Anwendungen, da auf diese Weise auch Applikationen von der Bandbreitenoptimierung profitieren, die nicht unternehmenskritisch sind. Ob Mails oder der normale HTTP-Verkehr etwas mehr Zeit beanspruchen, wird einem Unternehmen nicht wirklich schaden, und der Nutzerkomfort leidet nicht übermäßig darunter. Moderne, innovative WAN-Optimizer hingegen analysieren die einzelnen Anwendungen dahingehend, ob sie einer Priorisierung bedürfen und inwiefern eine Kompression der Datenströme sinnvoll ist. Auf diese Weise lassen sich durchaus Beschleunigungen um den Faktor 25 und mehr erreichen.

Hardware-Lösungen zur Beschleunigung von WAN-Verbindungen setzen jedoch sowohl auf Server- als auch meist auf Client-Seite die Implementierung spezieller Komponenten voraus. Die Kosten für solche Lösungen übersteigen mit etwa 80 bis 400 Euro pro Nutzer die Investition in ein reines Software-Produkt meist deutlich. Gerade wenn es um die Anbindung kleiner Zweigstellen geht, sind die Kosten pro User schnell meist unverhältnismäßig hoch. Für die Anbindung mobiler Clients eignen sich Hardware-Beschleuniger gar nicht, da die Implementierung von Hardware beim Nutzer in diesem Fall nicht möglich ist.

Weitere mögliche Stolpersteine beim Einsatz von WAN-Beschleunigern sind die Kompression und Verschlüsselung der Daten durch das RDP-Protokoll. Dies führt dazu, dass die Accelerator-Hardware die Datenströme nicht cachen kann. Eine Abschaltung von Kompression und Verschlüsselung schafft nur bedingt Abhilfe, birgt aber Sicherheitsrisiken. Selbst wenn WAN-Beschleuniger eine positive Auswirkung auf die Leistungsfähigkeit des Netzwerks und damit auf den Nutzerkomfort bei Remote-Desktop-Anwendungen haben, steht der hohe Kostenaufwand in keinem sinnvollen Verhältnis zum Ergebnis. Hinzu kommt, dass WAN-Beschleuniger bei der Skalierbarkeit nicht mit virtuellen Umgebungen mithalten können und damit einen der größten Vorteile der Virtualisierung quasi kannibalisieren.

RDP-Beschleunigung: Das Problem an der Wurzel packen

Die aufgeführten Schwächen des RDP-Protokolls führen oft dazu, dass sich Unternehmen nach alternativen, teils proprietären Protokollen umsehen, oder die Entscheidung für Virtualisierung wird gänzlich infrage gestellt. Da sich RDP aber über die Jahre als das dominierende Protokoll für virtualisierte Infrastrukturen durchgesetzt hat, ist eine Optimierung des Protokolls naheliegend. Hierbei stehen kurze Antwortzeiten und ein schneller Bildaufbau im Vordergrund. Moderne

Lösungen wie H+H NetMan Desktop Manager 5 erreichen eine Beschleunigung um bis zu Faktor 10. Dazu trägt hauptsächlich die anpassbare Kompression von grafiklastigen Inhalten und Anwendungen wie Bildern, Videos, PDF-Dokumenten bei.

Weitere Maßnahmen zur RDP-Beschleunigung sind Packet Shaping, das zu einer deutlich effizienteren und damit schnelleren Übertragung des RDP-Datenstroms führt, und ein intelligenter Bildaufbau. Natives RDP transportiert Bildschirmseiten als einzelne Pakete geringer Größe und setzt diese erst am Client wieder zum Gesamtbild zusammen. Bei langsamen Verbindungen – typischerweise bei Nutzung von WAN- und Mobilfunkleitungen – baut sich der Bildschirminhalt bei dieser Vorgehensweise nur schrittweise auf. In der Folge sind die Mitarbeiter unzufrieden, weil ein flüssiges Arbeiten nicht möglich ist. Manche RDP-Beschleuniger setzen daher auf die Übertragung ganzer Bildschirmseiten. Dies führt zwar nicht zu einer Beschleunigung von RDP an sich, trägt aber zu einer besseren User Experience bei. Vorteile gegenüber Hardware-Lösungen bietet eine Software-seitige RDP-Beschleunigung zudem beim Kostenkapitel. Denn entsprechende Produkte sind nur für die Arbeitsplätze zu kaufen beziehungsweise zu lizenzieren, an denen sie auch tatsächlich benötigt werden.

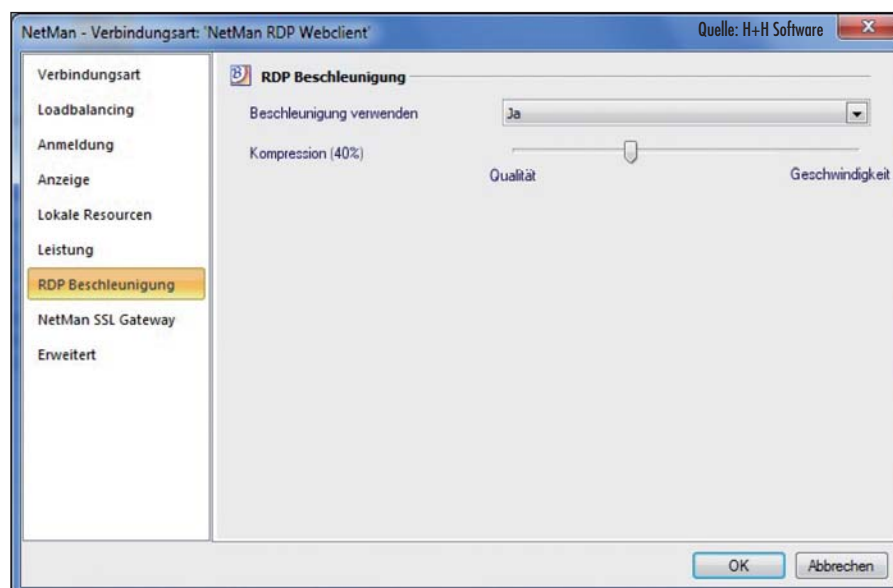


Bild 2: Bei einer Software-basierten RDP-Beschleunigung lässt sich im Idealfall je nach Anwendungsfall die Kompressionsrate festlegen



RemoteFX – nur fürs LAN konzipiert

Mit dem Service-Pack 1 (SP1) für Windows Server 2008 R2 führte Microsoft eine Erweiterung des RDP-Protokolls namens RemoteFX ein. RemoteFX verbessert die Multimedia-Performance von virtualisierten Umgebungen, sodass RDP-Clients Windows Aero, Silverlight nutzen, Flash und Videos abspielen und 3D-Anwendungen ausführen können. Der Einsatz von RemoteFX unterliegt aber gewissen Restriktionen. Zum einen sieht Microsoft die Nutzung nur innerhalb eines LANs vor. Zum anderen erfordert das Codieren und Decodieren von Multimedia-Inhalten entsprechend leistungsfähige Grafik-Chips auf Serverseite, die in den allerseltensten Fällen vorhanden sind. Eine weitere Einschränkung betrifft den Einsatz eines Hypervisors für VDI-Umgebungen. RemoteFX funktioniert derzeit nur zusammen mit Hyper-V und kann somit nicht mit VDI-Lösungen genutzt werden, die einen anderen Hypervisor voraussetzen wie etwa VMware View oder Citrix XenServer. Auch ist die Auswahl an Thin Clients, die eine RemoteFX-Unterstützung bieten, noch gering.

Alternative Protokolle

RDP hat sich zwar zum Quasi-Standard entwickelt, das einzige Protokoll im Remote Desktop-Bereich ist es dennoch nicht. Hersteller wie Citrix und VMware investieren viel Zeit und Geld in die Entwicklung eigener Protokolle, die insbesondere hinsichtlich der Übertragung von Multimedia-Inhalten optimiert sind. Citrix beispielsweise setzt mit seinem Protokoll HDX – soweit möglich – auf Client-seitiges Rendering, um den Datenstrom möglichst gering zu halten und eine bestmögliche Anzeigequalität am Endgerät zu erreichen.

VMware verwendet mit dem von Teradici entwickelten PC-over-IP-Protokoll (PCoIP) eine ursprünglich Chip-integrierte Lösung, die sowohl auf Server- als auch auf Client-Seite spezielle Hardware-Komponenten erfordert. Diese Chips komprimieren Bildschirmsignale und USB-Daten von Peripheriegeräten und wandeln sie in einen IP-Stream um,

der am Endgerät wiederum entschlüsselt wird. Mittlerweile ist PCoIP rein auf Software-Basis realisierbar. Wie bei allen Alternativ-Protokollen sind Unternehmen hierbei allerdings an einen Anbieter gebunden, statt mit Hersteller-unabhängigen Standards zu arbeiten. Außerdem fällt die Kostenbilanz einer solchen Lösung in den meisten Fällen schlechter aus als beim Einsatz von RDP.

Fazit

Der Nutzerkomfort ist beim Einsatz von Remote Desktop und Terminalserver-Lösungen eines der wichtigsten Kriterien. Nur wenn die User Experience auf dem Niveau klassischer PCs liegt, können kritische Geschäftsprozesse schnell und effi-

zient bearbeitet werden. Zudem steigt die Produktivität der Mitarbeiter, wenn sie sich im Umgang mit ihrem Endgerät wohl fühlen. Als Quasi-Standard für die Übertragung von Bildschirmhalten in virtualisierten Umgebungen zeigt RDP leider spezifische Schwächen, die den Nutzerkomfort nachhaltig beeinträchtigen können. Unternehmen sollten aber deswegen nicht auf den Einsatz modernster Technologien wie VDI oder Terminal Services verzichten, sondern vielmehr in eine leistungsfähige Optimierung von RDP investieren, um den Anwendern den maximalen Arbeitskomfort zu ermöglichen. (ln) 

Alexander Vierschrodt ist Leiter Marketing und Produktmanager bei H+H Software.



Fast Lane, die Spezialisten für:

Training & Consulting rund um Virtualisierung, Cloud- & Data Center-Technologien



Cloud Computing, Data Center & Virtualisierungs-Trainings, z.B.:

- FlexPod for Account Managers (FPAM)
- FlexPod for VMware Essentials (FPVE)
- FlexPod for VMware Administration (FPVA)
- FlexPod for VMware Design & Implementation (FPVI)
- Implementing Enhanced Secure Multi-Tenancy Solutions (IESMT)
- Cisco Virtualization Experience Infrastructure (VXI) Curriculum
- Virtualisierung: Konzepte, Potenziale & Risiken (VIRT)
- Cloud Computing Overview (CLOUD)
- Implementing Vblock (VBLOCK-TECH)
- Data Center Unified Computing Implementation (DCUCI)
- Implementing Cisco Data Center Unified Fabric (DCUFI)
- Implementing Cisco Storage Networking Solutions (ICSNS)
- VMware vSphere 5: Install, Configure, Manage (VICM)
- VMware vCloud: Architecting the VMware Cloud (AVC)
- VMware View: Install, Configure, Manage (VIEW)
- Data ONTAP 8.0 7-Mode Administration (D7ADM)
- VMware vSphere on NetApp (VVNA)
- Symantec Backup Exec Administration (BE2010)
- Symantec NetBackup Administration (NBUW7)

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

Cisco European Learning Partner
of the Year 2009, 2010 & 2011

NetApp Partner Award 2011

VMware EMEA Training (VATC)
Partner of the Year 2012





Die acht Gebote des Datenschutzes: Eingabekontrolle (4)

Auf die Finger geschaut

von Christian Regnery

In den ersten drei Teilen unserer Serie haben wir uns mit der Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle und der Weitergabekontrolle befasst. Der vierte Teil behandelt die Eingabekontrolle. Hierbei ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Wie Sie dies rechtskonform sicherstellen, lesen Sie in diesem Beitrag.

In der Anlage zu § 9 BDSG stellt das Bundesdatenschutzgesetz acht Anforderungen an die innerbetriebliche Organisation der Datenverarbeitung auf. Auch wenn die IT-Abteilung den Zugriff und Zugang zu IT-Systemen umfassend geregelt hat – Lücken finden sich immer und kein System ist absolut sicher. Berechtigungen können etwa fehlerhaft vergeben oder nachträglich weggefallen sein, Passwörter missbraucht werden. Daher ist es wichtig nachträglich feststellen zu können, wer welche Daten wie in das System eingegeben oder verändert hat.

Revisions- und Beweisfunktion

Bei der Eingabekontrolle geht es weniger um die Verhinderung unberechtigten Zugriffs als vielmehr darum, nachträglich erkennen zu können, ob und wie es zu Fehlern gekommen ist und dies auch nachweisen zu können. Da die Daten letztlich zu Revisions- und Beweis Zwecken verwendet werden, müssen die Daten vollständig sein, dürfen nur den berechtigten Personen zugänglich sein und nicht nachträglich verändert werden können.

Diese Kontrollpflicht bezieht sich allerdings nur auf personenbezogene Daten. Rein sachliche Protokolldaten werden hiervon nicht erfasst. Zudem betrifft die

Protokollierung nur Programme und Verfahren, die auch personenbezogene Daten verarbeiten.

Zu erfassende Daten

Im Unternehmen werden in den verschiedensten Systemen und Programmen personenbezogene Daten erhoben und verarbeitet: von Personalsoftware und CRM-Systemen, ERP und individuellen Datenbanken bis hin zur Zeiterfassung, Zutrittskontrolle und Videoüberwachung. Obwohl das Gesetz bei der Eingabekontrolle keine Unterscheidung nach Art und Umfang der Daten macht, ist es kaum praktikabel, sämtliche Ereignisse zu erfassen.

Hier hilft das Gesetz weiter: Da nach § 9 BDSG nur die technischen und organisatorischen Maßnahmen getroffen werden müssen, die angesichts der Bedeutung der Daten angemessen sind, kann man auch bei den Maßnahmen zur Kontrolle der Eingabe nach der Sensibilität der Daten unterscheiden:

1. Freizugängliche Daten: Etwa konzernweite Adressbücher, Ansprechpartner im CRM-System.
2. Unmittelbare Personaldaten: private Adressen, Familienverhältnisse, Einkommen, Unterhaltspflichten.

3. Besonders sensible Daten: Krankheit, Vorstrafen, Abmahnungen, Lohnpfändung, Kontodaten, Auswertungslisten.

Umfang der Protokollierung

Bei freizugänglichen Daten ist regelmäßig keine Protokollierung erforderlich. In allen anderen Fällen sind zu protokollieren:

- Log-In / Log-Out
- Änderung von Passwörtern
- Änderung der Zugriffsrechte
- Schreibende Zugriffe auf Dateien und Datenbanken
- Identität des Eingebenden
- Datum der Eingabe
- Ordnungsnummer des Datensatzes und Software

Bei Änderung von Datensätzen sollte grundsätzlich auch der Inhalt des geänderten Datensatzes protokolliert werden. Anders bei besonders sensiblen Daten: Hier sollten Sie nur die Feldbezeichnung erfassen. Zudem gilt bei dieser Datenkategorie, dass immer auch der Nur-Lese-Zugriff zu protokollieren ist.

Differenzieren zwischen Admin und Nutzer

Es ist zu unterscheiden zwischen fachlichen und administrativen Zugriffen auf ein Informations- und Kommuni-

kationssystem. Während der gewöhnliche Nutzer aufgrund des Berechtigungskonzepts ohnehin nur Zugriff auf die jeweils erforderlichen Daten haben darf, sind die Zugriffsrechte der IT-Administration naturgemäß nahezu unbegrenzt. Zu den genannten Basis-Daten sind daher nach einem Vorschlag des Landesdatenschutzbeauftragten Hessen bei der Administrationstätigkeit zusätzlich zu protokollieren:

- Installation / Deinstallation von Anwendungssoftware,
- Änderungen und Modifikation der Anwendungskonfiguration (Customizing, Festlegen von Migrationsregeln, Residenzzeiten, Löschfristen, Login-Parameter, Anzeigeparameter et cetera),
- Zugriffe im Rahmen einer etwaigen Mandantenverwaltung, die Anlage, Änderung und Löschung von Rollen, die Vergabe, Änderung und Löschung von Berechtigungen, die Administration von Benutzern (Anlage, Sperre, Löschung, Rollenzuweisung), die Einrichtung / Änderung standardmäßig vorgegebener Auswertungsmöglichkeiten (Reports), der Import / Export von Datenbeständen,
- Datenübermittlungen, Prozesse zur Aggregation, Pseudonymisierung / Anonymisierung von Datenbeständen (Data Warehouse), Archivierungen / Datensicherungen.

Wichtig: Bei den gesammelten Protokolldaten handelt es sich selbst um personenbezogene Daten. Im gesamten Erhebungs- und Auswertungsverfahren sind daher die allgemeinen datenschutzrechtlichen Prinzipien zu beachten. Die Daten sind insbesondere nur soweit zu erheben, wie es wirklich erforderlich ist. Gerade für die Protokollierung ist dies ausdrücklich gesetzlich bestimmt: Gemäß § 31 BDSG (Besondere Zweckbindung) dürfen personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, nur für diese Zwecke verwendet werden. Eine Protokollierung sämtlicher Aktivitäten oder Auswertung von Protokolldaten zur allgemeinen Mitarbeiterüberwachung ist unzulässig.

Betriebsrat beteiligen, Zugriffe beschränken

Da personenbezogene Daten ausgewertet werden und damit eine Leistungs- und Verhaltenskontrolle der Arbeitnehmer möglich ist, besteht ein Mitbestimmungsrecht des Betriebsrats nach § 87 I Nr. 6 BetrVG. Allerdings hat dieser im Ergebnis kein Verhinderungsrecht, da die Protokollierung eine gesetzliche Pflicht darstellt und der Arbeitgeber ein Recht darauf hat, sein IT-System vor Missbrauch zu schützen, zu kontrollieren und die Ergebnisse zu protokollieren. Hier sollte ein datenschutzfreundliches Verfahren implementiert werden. Bei entdeckten Auffälligkeiten – nach technischer Sicherung des Systems vor weiterem Missbrauch – sollte unter Beteiligung des Betriebsrats und des Datenschutzbeauftragten zunächst versucht werden, intern den Grund der Auffälligkeit mit dem betroffenen Mitarbeiter zu klären.

Da es sich bei den Protokolldaten selbst um personenbezogene Daten handelt, ist der Kreis der Zugriffsberechtigten auf die unbedingt Erforderlichen zu begrenzen.



+++ Neu: Root Camp Berlin +++
 +++ Security-Day +++ Hacking Contest by SOPHOS +++
 +++ Academy-Day: Weiterbildung und potentielle Arbeitgeber +++
 +++ kostenlose Beta-Prüfung: LPI +++
 +++ Workshop: Richtig bewerben +++
 +++ umfangreiches Vortragsprogramm +++ LinuxNacht +++

Der LinuxTag wird volljährig!
Feier mit uns! Komm zum LinuxTag!

Jetzt Tickets sichern!



Zum
Ticketshop



Zum
Programm

Mach dich schlau. Tausch dich aus.
Finde deinen Job von Morgen.



23.-26. Mai 2012 in Berlin
**EUROPE'S LEADING
 OPEN SOURCE EVENT**
www.linuxtag.org

Hauptmedienpartner:



Partner:



Bronze Partner:



Content Partner:



Hacking Contest by



Dies sind:

- IT Administrator
- IT-Sicherheitsbeauftragter
- Datenschutzbeauftragter
- Revisor
- Betriebsrat/Personalrat

Zum Zweck der Revisionssicherheit und Beweiskraft ist der Zugriff stets nur lesend zu gestatten. Sind besonders sensible Daten oder die IT-Administrator-Protokolle betroffen, ist nach dem Vier-Augen-Prinzip zu verfahren. Es darf nicht möglich sein, die laufenden Protokollierungsdaten zu löschen oder inhaltlich abzuändern. Der Beweiswert lässt sich durch eine digitale Signatur der einzelnen Ereignisse erhöhen. Allerdings erfordert dies in der Praxis oft einen unverhältnismäßig hohen Aufwand.

Organisatorische Maßnahmen

Das Verfahren der Protokollierung (Zugriffsberechtigung, Umfang und Inhalt der Protokollierung, Auswertungsverfahren) und die Konsequenzen bei einem Verstoß sollten durch eine Dienstanweisung geregelt sein. Das steigert nicht nur die Akzeptanz bei den Beschäftigten und dem Betriebsrat. Es verdeutlicht den IT-Verantwortlichen auch nochmals die Bedeutung der Eingabekontrolle. Denn oft wird vieles einfach so nebenher protokolliert oder eine Protokollierung ist programmtechnisch vorgegeben, ohne dass eine korrekte Auswertung vorgenommen wird.

Datenschutzfreundliche Protokollierung

Ist der Zugriff derart auf die unmittelbar erforderlichen Personen beschränkt und eine Beteiligung des Betriebsrats oder Datenschutzbeauftragten bei der Auswertung garantiert, ist einem Missbrauch der Protokolldaten hinreichend vorgebeugt. Dennoch wird vereinzelt empfohlen, zusätzlich zu den beschriebenen Maßnahmen noch eine Pseudonymisierung der Protokolle vorzunehmen, soweit sie personenbezogene Daten betreffen.

Hierzu dienen etwa komplexe kryptografische Verfahren oder einzelne Log-File-Anonymisierer, die personenbezogene Anteile der Log-Files datenschutzfreundlich verschlüsseln. Einer gesonderten Pseudonymisierung bedarf es vom Gebot der Datensparsamkeit her aber in der Regel nicht. Der einzelne Nutzer ist regelmäßig ohnehin nur über eine spezielle ID-Nummer identifizierbar und der Zugriff auf die Daten durch das abgestufte Berechtigungskonzept begrenzt.

Eine Protokollierung macht zudem nur Sinn, wenn sie zeitnah erfolgt. Je schneller kontrolliert und ausgewertet wird, desto schneller können Verfahren abgeschlossen und die erhobenen Daten gelöscht werden. Die Logdaten sollten zudem möglichst getrennt von anderen Daten aufbewahrt und zusätzlich an sicherer Stelle gespiegelt werden. Mittels Checksummenprüfung kann der Versuch eines Angreifers, einen Angriff

durch Manipulation der Logdateien zu verschleiern, dann leicht aufgedeckt werden. Eine hilfreiche Checkliste hierzu finden Sie in der Tabelle "Checkliste für eine Eingabekontrolle". Diese stammt von der Landesdatenschutzbehörde Niedersachsen [1].

Aus den Archivierungsfristen ergibt sich für den Anwender jedoch ein Dilemma: Einerseits soll er die Daten zum Nachweis eines etwaigen Missbrauchs speichern, andererseits gilt der Grundsatz, dass nicht mehr benötigte Daten zu löschen sind. Ob und wann die Protokolldaten benötigt werden, ist im Voraus nicht klar. Allgemeingültige Archivierungsfristen gibt es ebenfalls nicht. Sofern keine besonderen gesetzlichen Archivierungsfristen bestehen, werden gewöhnlich Aufbewahrungsfristen zwischen einem halben und einem Jahr vorgeschlagen. Unabhängig davon sollte der Anwender selbst entscheiden, in welchem Zeitraum unberechtigte Zugriffe und Fehler anhand der Protokolle überhaupt noch aufgedeckt werden können und daran die Speicherfrist bemessen.

Tools zur Protokollauswertung

Je größer die protokollierte Datenmenge ist, desto schwieriger gestaltet sich die Auswertung und Kontrolle der Daten. Daher bieten sich in der Praxis automatisierte Auswertungstools an, mit denen gezielt nach Auffälligkeiten und Abweichungen von vorgegebenen Sicherheitsrichtlinien gesucht werden kann. Auch wenn für proprietäre Werkzeuge teils erhebliche Kosten anfallen können, liegt der Vorteil auf der Hand: Lücken, Missbrauch und externe Angriffe werden schneller erkannt, Datenverlust und Imageschäden wird vorgebeugt und die IT/Revision wird entlastet. (dr) 

Rechtsanwalt Christian Regnery, LL.M., ist Fachanwalt für IT-Recht, Gewerblicher Rechtsschutz und Urheber- und Medienrecht, Consultant Datenschutz und IT-Compliance bei der intersoft consulting services AG, Hamburg/Berlin

Checkliste für eine Eingabekontrolle			
Zu prüfende Aspekte	Ja	Nein	Anmerkung
Besteht Dienstanweisung über Art, Inhalt, Umfang der Protokollierung?			
Zugriffsberechtigung auf die Protokolldaten auf die erforderlichen Stellen beschränkt und schriftlich geregelt / 4-Augen-Prinzip gewahrt?			
Sind Protokolldaten zugriffssicher gespeichert?			
Sind Protokolldaten vor nachträglichen Veränderungen gesichert?			
Sind Löschfristen für Protokolldaten bestimmt?			
Wird Einhaltung der Dienstanweisung kontrolliert?			
Betriebsrat / Personalrat beteiligt?			

[1] Checkliste der Landesdatenschutzbehörde Niedersachsen
C5W21

Link-Codes





Liefertermin:
Ende Oktober 2012

Bestellen Sie jetzt das IT-Administrator Sonderheft II/2012!

180 Seiten Praxis-Know-how rund um das Thema

Virtualisierung

Betrieb und Management
virtualisierter Infrastrukturen

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

* IT-Administrator Abonnenten erhalten das Sonderheft II/2012 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/



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

☐ **Ja**, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft II/2012 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft II/2012 zum Preis von **€ 29,90** inkl. Versand und 7% MwSt.

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____

BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

So erreichen Sie unseren
Vertrieb, Abo- und
Leserservice:

Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville

Tel: 06123/9238-251

Fax: 06123/9238-252

leserservice@it-administrator.de

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



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 0512



Als Opa Admin war: HP-85 Taschenrechner 2.0

von John Pardey

Als EDV-Geräte, die im weitesten Sinne dem entsprachen, was heute als "Clients" geläufig ist, begannen, die Schreibtische der Welt zu erobern, herrschte noch das monolithische Mainframe-Konzept. Die einzige Alternative, die individuelle Rechenkraft am Arbeitsplatz bot, war schlicht und ergreifend der Taschenrechner. Einer der Marktführer in diesem Segment war Ende der 70er Jahre Hewlett Packard. Programmierbare und mathematisch äußerst leistungsfähige Taschenrechner waren damals durchaus schon Standard. Doch mit dem HP-85, den wir Ihnen heute vorstellen wollen, gelang dem Hersteller der Übergang vom Tischtaschenrechner zum modernen Client-PC.

Alles inklusive

HP kündigte sein Modell 85 Ende 1979 an und im Januar 1980 begann die Auslieferung, die gleichzeitig HPs Ära der Tischtaschenrechner beendete. Zwar bot der HP-85 auch alle gewohnten Funktionen des Taschenrechners, war jedoch durch seine Erweiterung um einen relativ leistungsstarken Monitor, einen eingebauten Drucker und den Massenspeicher genau das richtige Gerät zu einer Zeit, in der sich PCs anschickten, die Desktops zu erobern. Und so war dem HP-85 denn auch ein großer kommerzieller Erfolg beschieden.

Integriert in das große, aber vergleichsweise leichte Gehäuse war der kleine Monitor mit einer Auflösung von 320 x 200 Punkten, ein Bandlaufwerk für DC100-Bänder mit jeweils 210 KByte Kapazität und ein Thermodrucker. Dieser war ebenso wie der Bildschirm grafikfähig und erzeugte auf Tastendruck eine Hardcopy des Bildschirminhalts. Das eingebaute Bandlaufwerk verfügte über ein echtes Filesystem und war in der Lage, nach dem Einschalten des Rechners ein Programm automatisch zu starten.

Auf der Rückseite des HP-85 befinden sich vier Steckplätze für Erweiterungsmodule. Hier ließ sich der Arbeitsspeicher erweitern, Peripherieschnittstellen einbauen oder ein ROM-Modul einstecken. Letzteres enthielt Fächer für mehrere EPROMs, die den Basic-Befehlsschatz erweiterten oder Betriebssystemfunktionen zur Ansteuerung zusätzlicher Peripheriegeräte wie etwa Diskettenlaufwerke enthielten.

Der Apfel fällt nicht weit vom Stamm

Auch wenn viele Anwender den HP-85 für sein gelungenes Design und seine Ro-

bustheit lobten, war seine Rechengeschwindigkeit oft eher bescheiden. Die Ausnahme dabei bildeten lediglich rein mathematische Funktionen, die der Rechner – sicher zum Stolz seiner "Vorfahren" – mit enormer Geschwindigkeit erledigte.

Dies lag nicht zuletzt am Prozessor des HP-85: Dieser war speziell für die 80er-Baureihe entwickelt worden und zeichnete sich durch einige Fähigkeiten aus, die für 8 Bit-Prozessoren außergewöhnlich waren. So enthielt er sehr viele Register (64), die für manche Operationen auch zusammengeschaltet werden konnten.

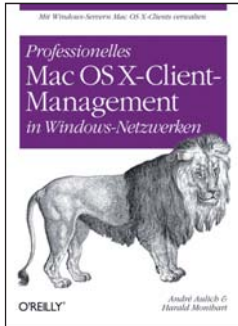
Aus dem Kuriositätenkabinett

Der HP-85 stand unseren heutigen Rechnern technisch zweifellos näher als einige andere Geräte, die wir in dieser Rubrik schon vorgestellt haben. Daher fallen auch die technischen Kuriositäten nicht so haarsträubend aus wie bei den EDV-Dinosauriern der 50er- und 60er-Jahre, doch einige der Eigenheiten des HP-85 wollen wir Ihnen nicht vorenthalten. Positiv ist dabei eine Fähigkeit zu nennen, die die Funktionalität von USB vorwegnahm: alle Interfaces und der Speicher ließen sich zusammenschalten, ohne das Gehäuse öffnen zu müssen. Das war damals nicht üblich und steht uns heutzutage in der Regel wie erwähnt nur per USB zur Verfügung. Auch seine Historie als Taschenrechner konnte das Gerät nicht verbergen. So war der Anwender jederzeit und völlig unabhängig von der aktuellen Aufgabe des HP-85 in der Lage, über eine spezielle Taste direkt etwas auszurechnen. Das Ergebnis wurde unmittelbar angezeigt und der Anwender arbeitete anschließend einfach weiter. Schon anstrengender dürfte es für den Nutzer gewesen sein, dass sich sein Bildschirm immer schwarz schaltete, wenn er etwas druckte oder Daten aus dem Bandlaufwerk lud.



"Nein Papi, ich will nicht wie Du Taschenrechner werden!" – der HP-85 ist eine Weiterentwicklung der Ende der 1970er-Jahre weit verbreiteten Taschenrechner

Professionelles Mac OS X-Client- Management



Mit Mac OS X hat sich ein Außenseiter unter den Betriebssystemen auf den Vormarsch in die Unternehmen gemacht. Kenntnisse für eine erfolgreiche Integration mussten bisher eher mühsam im Internet

zusammengetragen oder via Trial-and-Error erprobt werden. Die erfahrenen Autoren beschreiben zwei Vorgehensweisen, mit denen die Integration gemeistert werden soll: In der ersten Variante wird zusätzlich zur Windows Server-Architektur eine Apple Server-Infrastruktur aufgebaut, aber das MAC-Umfeld in das Active Directory integriert. Die zweite Variante ver-

folgt dasselbe Ziel, vermeidet aber den Aufbau einer zusätzlichen Apple-Server-Umgebung, indem der Administrator die Windows-Umgebung an die Apple-Erfordernisse anpasst.

Der Inhalt des Buchs orientiert sich am Lebenszyklus eines Mac-Rechners im Unternehmen, sodass der Administrator praxisnah an die Hand genommen wird. Nach Anschaffung eines Macs (das Buch behandelt primär 10.6- und 10.7-Clients) wird dieser mit der Unternehmens-Software bespielt. In diesen Abschnitten erfährt der Leser Relevantes zu den Themen Netzwerk-konfiguration und Benutzerverwaltung. Hinzu kommen die Mac OS-Management-Lösungen MCX und Login-Hooks, die die Autoren auf Basis von Windows Server 2008 R2 beschreiben. Demnach funktionieren diese Lösungen aber auch mit Windows Server 2003. Beschrieben wird die Einbindung in das Active Directory und die AD-Schema-Erweiterung, um die MCX-Techniken zentralisiert bereitstellen zu können. Nachfolgend gehen die

Autoren ausführlich auf mögliche Deployment-Strategien ein, die die Installation des OS sowie von Programmen beinhalten, was den Anforderungen an eine zentralisierte Clientverwaltung entspricht.

Fazit

Ziel dieser Publikation sind nicht die Spielzeug-Macs der Chefs, sondern Clientlandschaften, die sich der Herausforderung einer zentralen Verwaltung stellen wollen. Dafür werden sowohl betriebsinterne wie auch Open Source-Tools und kommerzielle Lösungen vorgestellt. In Zukunft führt wohl kein Weg vorbei an Mac OS im Netzwerk, ebenso wenig wie an dieser Lektüre, die ein hilfreicher Begleiter ist.

Frank Große

Autoren	André Aulich, Harald Monihart
Verlag	O'Reilly
Preis	39,90 Euro
ISBN	978-3868991314

Bewertung (max. 10 Punkte) **10**

OS X Lion und UNIX, 6. Auflage



Kai Surendorf ist ein anerkannter Experte für die Kombination Mac OS X und UNIX, sodass es nicht verwundert, dass sein Administrator-Guide zu dieser Thematik bereits in der 6. Auflage erscheint. "Darwin", der UNIX-Kern als Grundlage für iOS sowie OS X 10.7, bildet den Fokus des Buches und der administrativen Arbeit auf

derartigen Systemen. Der Leser wird zu Beginn mit den wichtigsten Methoden der Terminal-Arbeit vertraut gemacht und erfährt eine knappe Beschreibung der UNIX-Dokumentationen. Im zweiten Teil wird die Arbeit am Terminal praktiziert: Dateien und Verzeichnisse editieren und manipulieren, Arbeit mit Prozessen, Zugriffsrechte und Benutzerverwaltung, Dateisysteme, das Drucksystem CUPS, Suchen und Finden mit Spotlight, der Su-

per-Daemon "launchd" und Methoden zur produktiven, effizienten Arbeit mit dem Terminal sind die Inhalte.

Nachfolgend beschreibt der Autor die Möglichkeiten der Arbeit im Netzwerk, wobei sich Surendorf sowohl auf die Konfiguration der Netzwerke als auch auf die Arbeit mit Diensten wie SSH oder SNMP konzentriert. Das Thema Firewalls wird hingegen nur angerissen, ebenso die Beschreibungen der Serverdienste Apache, Postfix, NFS, MySQL und FTP. Auf die Automatisierung von Wartungsarbeiten und den damit verbundenen Einsatz von Shellskripten konzentriert sich der vierte Teil, der durchaus Verbesserungspotenzial besitzt. Auch wenn das Buch keinen Anspruch auf Vollständigkeit erhebt, so eignet sich dieser Part für Anwender, die zum ersten Mal mit Shellskripten arbeiten, nur bedingt, da die Knappheit der Beschreibung zum Teil doch Fragen offenlässt. Erfahrene Skriptnutzer können diesen Teil ohnehin überspringen. Auch einige der Code-Beispiele scheinen fehlerhaft zu sein. Die Schnittstelle zur Welt der Open Source-Software beschreibt das Abschlusskapitel.

Fazit

Die Arbeit mit dem gereiften UNIX-Kernel ist das Hauptanliegen des Autors. Dabei versucht er den Spagat zwischen Einführung, Effizienz und fortgeschrittener Fummelei zu absolvieren – was nicht immer perfekt gelingt. Insgesamt handelt es sich dennoch um eine solide Publikation zum zukunftssträchtigen Thema Mac OS, die ihre größten Schwachstellen im Bereich der Shell-Programmierung vorweist. Die Neuauflage hat den strukturierten Aufbau der Vorgängerversionen beibehalten. Die Ergänzungen und neuen Inhalte beziehen sich primär auf OS X 10.7. Damit erspart der Autor dem Leser mühsames Zusammensuchen aus den unterschiedlichen Quellen des Internets.

Frank Große

Autor	Kai Surendorf
Verlag	Galileo Design
Preis	44,90 Euro
ISBN	978-3836217927

Bewertung (max. 10 Punkte) **7**

www.vireference.de

Virtuelle Referenz

Die Virtualisierung entwickelt sich zusehends zum Dauerthema in der Unternehmens-IT. Egal ob Server, Desktop oder Applikationen – angesichts zahlreicher Vorteile wie Kosteneinsparungen, flexiblere Applikationsnutzung und größere IT-Sicherheit schießen virtuelle Umgebungen aus dem Boden wie Pilze. Doch fällt es dem ungeübten Virtualisierungseinsteiger nicht ganz leicht, sich im Dschungel der unterschiedlichen Produkte, Protokolle und Verfahren zurechtzufinden. Welche Lösung basiert auf welcher Technologie und was bedeutet dies für das eigene Projekt? Bei solchen grundlegenden Fragen hilft ein übersichtliches Nachschlagewerk wie vireference.de weiter. Die deutschsprachige Webseite vermittelt einen Einstieg in die Welt der Virtualisierung – angefangen bei den unterschiedlichen Methoden zur Betriebssystemvirtualisierung über die Systemvirtualisierung hin zur Netzwerkvirtualisierung. Damit kann sich der Besucher schon einmal grob orientieren.

Im Navigationsmenü auf der rechten Seite nimmt die Desktop-Virtualisierung den bei weitem größten Platz ein. Hier bildet eine Marktübersicht den Einstieg. Neben bekannten Namen wie VMware, Microsoft oder Kaviza tauchen auch weniger be-

kannte Anbieter auf wie Pano oder NxTop. Damit geht die Site sowohl auf Software- als auch Hardware-Lösungen im Bereich der Desktop-Virtualisierung ein. Zahlreiche Screenshots und Videos veranschaulichen die Technologien und Produkte. Doch wer glaubt, auf der Webseite nur grundlegende Informationen zu finden, irrt. An technischen Details Interessierten bietet vireference.de beispielsweise eine detaillierte Übersicht an Thin Clients. Ebenfalls ausführlich kommt der Vergleich zwischen den Protokollen Citrix HDX 3D und PCoIP daher – wenn auch die Übersichtlichkeit aufgrund der etwas aus den Fugen geratenen Webseiten-Formatierung leidet. Deutlich besser aufbereitet findet sich ein Vergleich zwischen RDP, Provision EOP, RGS, TCX, Teradici PCoIP und Pano Logic.

Natürlich dürfen die beiden anderen wesentlichen Aspekte der Virtualisierung nicht fehlen: Die Server- und die Desktop-Virtualisierung. Auch hier stehen Übersichtstabellen mit den Produkten der jeweiligen Anbieter zur Verfügung. Allerdings sind diese – wie auch im Bereich Desktop-Virtualisierung – nicht unbedingt die aktuellsten. Auch leidet die optische Darstellung so manches Mal an unschönen Formatierungen. Dennoch bietet die Seite einen hilfreichen Überblick. Damit können sich Einsteiger einen ersten Eindruck sowohl von der Technik als auch verfügbaren Lösungen verschaffen. (dr) 



MAIN MENU

- Home
- Neuigkeiten ganz kurz
- Add On Produkte zur Virtualisierung
- Die TOP 10 Reihe
- Impressum

DESKTOP VIRTUALISIERUNG

- Marktübersicht VDI-Systeme
- Client Geräte für die Desktop Virtualisierung
- Tabelle mit Produkten von Wyse und Pano Logic
- Der Thin Client
- Aktueller Vergleich von Thin Client Arbeitsplatzgeräten
- Protokolle der Desktop Virtualisierung
- FAQ zur Client-Virtualisierung
- Teradici (PC-over-IP)
- Connection Broker im Vergleich
- drei großen Techniken aus dem Rechenzentrum
- Aktueller Vergleich von VMware View 3.0 Thin Clients
- Desktop-Virtualisierung unter Windows: fünf Techniken und ihre Vorteile
- Multimedia in der Desktop Virtualisierung
- Vergleich von VDI Produkten
- Client Technologie im Vergleich
- Desktop-Virtualisierung mit Notebook, Laptop
- Alte Desktop PCs als Thin Clients nutzen

Virtualisierung und Produkte im Vergleich - Thin Client - Desktop Virtualisierung - Zero Client

Softwarevirtualisierung
Die Softwarevirtualisierung kann für mehrere Zwecke eingesetzt werden. z. B. zum Simulieren eines Betriebssystems oder nur einer Anwendung.

Erzeugung virtueller Betriebsumgebungen
Einordnung von Virtualisierungsansätzen zur Schaffung virtueller Betriebsumgebungen im Gesamtkontext der Virtualisierung.
Kategorisierung von Virtualisierungstechniken zur Schaffung virtueller Betriebsumgebungen.

1. Betriebssystemvirtualisierung mittels OS-Container
Ansatz von "OS-Containern" zur Schaffung virtueller Betriebsumgebungen. Bei Virtualisierung auf Betriebssystemebene wird anderen Computerprogrammen eine komplette Laufzeitumgebung virtuell innerhalb eines geschlossenen Containers oder "jails" zur Verfügung gestellt, es wird kein zusätzliches Betriebssystem gestartet. Die OS-Container stellen eine Teilmenge des Wirtbetriebssystems dar. Vorteil dieses Konzepts liegt in der guten Integration der Container in das

Die Seite vireference.de bietet ausführliche Informationen zu Desktop-, Server- und Applikations-Virtualisierung

Fachartikel
Netzwerk-Monitoring
Basissystemfunktionen

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

Der richtige Browser für IT-Administratoren

Zum Alltagsgeschäft eines Administrators gehört die Versorgung der Anwender mit einem funktionsfähigen Internet-Browser. Die Anforderungen an diese Software steigen jedoch ständig und der IT-Profi muss Aspekte wie Sicherheit, Performance, Rollout und Patch-Deployment berücksichtigen. Unser Online-Beitrag zeigt, wie sich die Admin-Arbeit bei der Browser-Verwaltung vereinfachen lässt, warum sich jedes Unternehmen eine Browser-Strategie zurechtlegen sollte und ob der Einsatz mehrerer Browser sinnvoll ist.

Link-Code: C5W51

Anwenderbericht: Endgeräte-Sicherheit an der Universität Wuppertal

Die Bergische Universität Wuppertal bietet Lebens- und Arbeitsraum für über 18.500 Studenten und Mitarbeiter. Unlängst stand der IT-Dienstleister der Bildungseinrichtung vor der Herausforderung, für die Anbindung von Endgeräten eine neue Sicherheitslösung zu finden. Diese sollte flexibel skalierbar sein und das stets steigende Datenvolumen problemlos bewältigen. Unser Anwenderbericht legt dar, welche Kriterien während des Auswahlprozesses besonders wichtig waren und ob die Implementierung des neuen Systems reibungslos verlief.

Link-Code: C5W52

Die vernachlässigte Gefahr: Silent Data Corruption

Gegen schleichende Datenkorruption scheint kein Kraut gewachsen zu sein. Keines der proprietären Dateisysteme großer Hersteller bietet vollkommenen Schutz gegen den Verlust von Informationen. Anders sieht es bei auf ZFS basierendem Open Storage aus: Mittels End-to-End Prüfsummen, transaktionellen Schreiboperationen und dem Copy-on-write-Verfahren sorgt ZFS dafür, dass wichtige Informationen sicher gespeichert sind. Unser Fachartikel im Web zeigt, dass Datenkorruption zwar real, aber vermeidbar ist.

Link-Code: C5W53

Anwenderbericht: Desktop-Virtualisierung senkt IT-Kosten der Stadt Bergheim

Die Stadt Bergheim setzte früh auf Terminalserver und hatte schon 2006 drei Citrix-Server in Betrieb. Um zusätzlich Betriebskosten zu senken, führte die Kommune dort vermehrt Thin Clients ein. Nach dem Vorbild einer Studie des Fraunhofer-Instituts UMSICHT ermittelte die Behörde 2011 die realen Kosten ihrer IT-Landschaft. Das Fazit unseres Anwenderberichts: Die durchschnittlichen Desktop-Kosten der Thin Client-Umgebung lagen um fast 45 Prozent niedriger als bei der dezentralen Anwendungsbereitstellung in einer PC-Umgebung.

Link-Code: C4W54

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

Link-Codes eingeben auf www.it-administrator.de

»Desktop-Virtualisierung kostet erst einmal Geld«

Alexander Gaber (35) und sein Team sind für die komplette IT-Infrastruktur am Standort Heidelberg der Firmengruppe ProMinent sowie für alle IT-Infrastrukturfragen weltweit verantwortlich. Seit mehr als 50 Jahren ist das Unternehmen als Hersteller von Komponenten und Systemen im gesamten Umfeld der Fluid-Dosiertechnik tätig. Neben dem Hauptsitz der Unternehmensgruppe in Heidelberg verfügt ProMinent über 56 Vertriebs- und Servicegesellschaften.

Warum sind Sie IT-Administrator geworden?

Als IT-Administrator bin ich immer an der vordersten Front, was die neuesten Technologien angeht. Dies faszinierte mich schon immer.

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

Administratoren sind schon lange nicht mehr nur "Kistenschrauber". Vielmehr wird ihnen eine extrem hohe Sozialkompetenz und Flexibilität abverlangt. Wenn jemand die Herausforderung zwischen komplexer Technik und Vertriebstalent mit ein klein wenig kaufmännischem Grundwissen sucht, dann ist der Job als Admin genau das richtige und wird ihm oder ihr sicherlich Spaß machen.

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

Mir gefällt es, neue Projekte zu planen und zu realisieren. Nur wenn wir in der IT Ideen und Businessanforderungen verwirklichen, können wir auch den wachsenden Unternehmensanforderungen gerecht werden. Keinen Spaß machen unnötige Grundsatzdiskussionen.

Virtualisieren Sie Applikationen?

Ja, wir arbeiten mit virtualisierten Applikationen. Naturgemäß haben wir im Produktionsumfeld einige Spezialapplikationen, die beispielsweise nur unter Windows XP funktionieren. Hier nutzen wir den XP-Modus von Windows 7.

Denken Sie über Virtualisierung als Teil der Desktop-Strategie nach?

Da wir die Server-Virtualisierung erfolgreich abgeschlossen haben, wäre die Desktop-Virtualisierung nun der nächste Schritt. Dabei sind natürlich die Kosten zu bedenken. Bei der Client-Virtualisierung fallen neben Lizenzgebühren für das Betriebssystem auch noch die Kosten für eine VDA-Lizenz an. Wenn sich die

Lizenzpolitik ändern würde, beispielsweise wie bei den DataCenter-Lizenzen bei Servern, wäre dies sicherlich der Durchbruch für eine Desktop-Virtualisierung im großen Stil.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Auf der Agenda stehen der Ausbau des Konzernrechenzentrums, die globale Active Directory-Integration und gerade in den Schwellenländern das Erhöhen der Sicherheitsstandards.

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

Da fällt mir eigentlich keines ein. Stattdessen möchte ich hier einmal die Herausforderung im internationalen Management von IT-Projekten erwähnen, besonders in der Region Asien.

Nehmen Sie Ihre Arbeit auch in den Urlaub oder ins Wochenende mit?

Das bleibt gelegentlich nicht aus, denn gerade in etwas "ruhigeren" Zeiten habe ich immer wieder Ideen, wie wir Prozesse optimieren könnten. Leider gibt es manchmal aber auch konkrete Probleme, die gelöst werden müssen und somit bin ich in Notfällen erreichbar.

Wie finden Sie den nötigen Ausgleich zu Ihrer Arbeit?

Eine harmonische Familie ist als Ausgleich zum anstrengenden Berufsleben ganz wichtig.

Sind Sie auch in Ihrem Freundes- und Bekanntenkreis als IT-Supporter gefragt?

Ja und ich habe kein Problem damit, eine kurze Frage zu beantworten. Was ich allerdings nicht mache, ist im großen Stil PCs zu installieren oder ein großes Troubleshooting durchzuführen.

Wie denken Sie, arbeitet ein Administrator in 10 Jahren?

Der IT-Administrator wird noch mehr zum Dienstleister werden. Er muss noch flexibler, "always on" und online arbeiten. Getrieben wird diese Entwicklung meiner



Geburstag: 13.07.1976
Admin seit: 16 Jahren
Hobbys: Handball, Windsurfen

Alexander Gaber, IT-Administrator

Ausbildung und Tätigkeit

- Kaufmännische Ausbildung zum Bürokaufmann.
- Zwei Jahre Ausbildung in der Abendschule zum MCSE Win NT4.0.
- Anschließend zwei Jahre IT-Support bei einem IT-Dienstleister.
- Danach Einstieg als IT-Administrator.
- Heute Leiter der globalen IT-Infrastruktur im Konzern ProMinent.

Betreute Umgebung

- 100 Server und 700 Client-PCs am Standort in Heidelberg mit dem Team.
- Zudem TK- und Videokonferenzanlage, Videoüberwachung, das Netzwerk, die Firewalls sowie die WAN-Strecken.
- International Betreuung und Unterstützung von rund zehn Standorten weltweit, Tendenz steigend.
- Darüber hinaus zwei Rechenzentren am Firmensitz in Heidelberg.

Einschätzung nach durch das Cloud Computing sowie den Trend zu "Bring your own device".

Das Interview führte Petra Adamik.

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

Was haben Sie zu sagen?

Die Ausgabe 6/12 erscheint am 29. Mai 2012

Schwerpunktthema:

SAN-Management

Im Test: StarWind Native SAN for Hyper-V

Im Test: Quest Software Secure Copy 6.0

Workshop: Große und verteilte Datenmengen mit Hadoop verarbeiten

Workshop: Plattformunabhängige RAID-Konfiguration durch Booten vom Netz

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

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

Der Schwerpunkt unserer Ausgabe im Juli befasst sich mit dem Thema **Endpoint & mobile Security**. In unseren Tests müssen unter anderem die Security-Suite Ubitexx Multiplatform Management und LogMeln Hamachi VPN ihr Können unter Beweis stellen. In der Praxisrubrik lesen Sie außerdem, wie Sie System Center Endpoint Protection 2012 implementieren und Applocker unter Windows Server 2008 R2 optimal einsetzen.

Als Schwerpunkt im August geht es dann um **Infrastruktur & Inventarisierung**.

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, Dr. Markus Blaschka,
Frank Große, Christoph Harding, Thomas Joas,
Nils Kaczinski, Christian Knermann, Sandra Lucifora,
Christian Regnery, Dr. Holger Reibold, Dirk Srocke,
Alexander Vierschrodt

Anzeigen

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

Es gilt die Anzeigenpreisliste
Nr. 9 vom 01.01.2012

LAC/2011



Produktion / Anzeigendisposition

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

Druck

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

Vertrieb

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

Abo- und Leserservice

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

Vertriebsbetreuung

SI special interest Pressevertrieb GmbH,
www.specialinterest.com

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

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 en-
thalten 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 zur Verwertung
angeboten worden sein, so ist dies anzugeben.
Die Redaktion behält sich vor, die Manuskripte
nach eigenem Ermessen zu bearbeiten. Honorare
nach Vereinbarung.

So erreichen Sie den Leserservice

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

Bankverbindung für Abonnenten

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

So erreichen Sie die Redaktion

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

So erreichen Sie die Anzeigenabteilung

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

Baramundi
Das Telefonbuch
ExperTeach
Fast Lane
Galileo

S. 13
S. 25
S. 41
S. 73
S. 15

HOB
IBM
IGEL Technology
InterNetX
LinuxTag

S. 19
S. 84
S. 35
S. 23
S. 75

Login Consultants
Microsoft
Paessler

S. 39
S. 02
S. 27

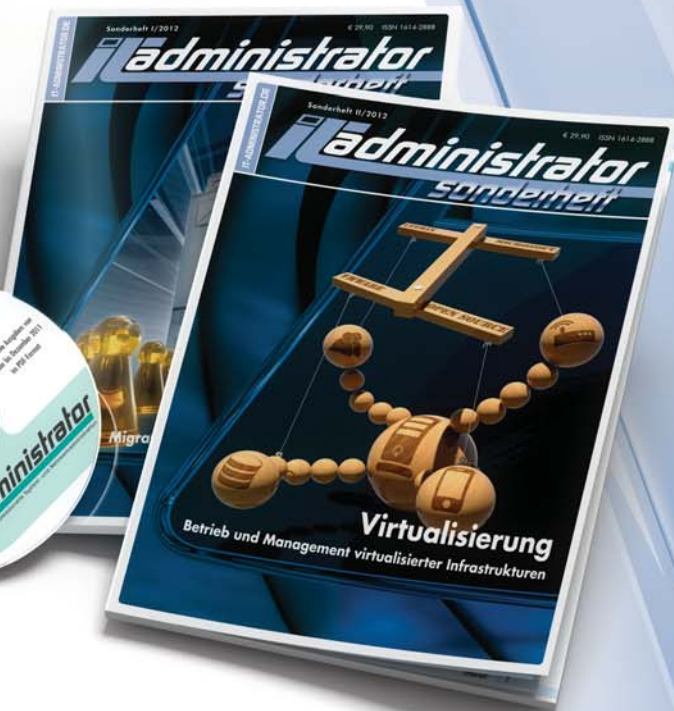
INSERTENTENVERZEICHNIS

Das IT-Administrator Komplettprogramm!!!

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

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

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



Als bestehender Jahresabonnent
können Sie hier upgraden:

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

Oder Sie sind Neukunde? Hier können Sie bestellen:

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

www.it-administrator.de



Heinemann Verlag
Im Dialog mit Spezialisten.

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München

Tel: 0049-89-4445408-0
Fax: 0049-89-4445408-99
info@heinemann-verlag.de

Vertrieb, Abo- und Leserservice IT-Administrator

vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville

Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de

Komplexität war gestern. System x ist heute.



Mit dem Unternehmen wachsen auch die Ansprüche. Der IBM System x® 3650 M3 Express Server mit den neuesten Intel® Xeon® Prozessoren der 5600er Serie wurde speziell für wachsende Unternehmen entwickelt: Vereinfachen Sie Ihre IT-Infrastruktur und profitieren Sie von schneller Einsatzbereitschaft, vereinfachter Verwaltung und verbesserter Wartungsfreundlichkeit – egal ob virtuell oder physisch, vor Ort oder am anderen Ende der Welt. Außerdem hilft Ihnen Ihr IBM Geschäftspartner, eine IT-Umgebung zu entwickeln, die mit dem Wachstum Ihres Unternehmens Schritt hält.

Die Nr. 1 bei der Kundenzufriedenheit im Bereich Server.¹

IBM System x3650 M3 Express

2.154,- € (inkl. MwSt.)*

monatl. IBM Leasingrate: 59,45 € (inkl. MwSt.)**

Best.-Nr.: 7945KNG

Intel® Xeon® Prozessor E5645

1x 4 GB RDIMM-Hauptspeicher

Open Bay, 2,5" HS SAS/SATA, ServeRAID Controller M5014

1x 460 W HS Power Supply, Multiburner

1 Jahr Gewährleistung, 3 Jahre freiwilliger Herstellerservice



IBM BladeCenter® HS22 Express

1.690,- € (inkl. MwSt.)*

monatl. IBM Leasingrate:

46,46 € (inkl. MwSt.)**

Best.-Nr.: 7870K4G

Intel® Xeon® Prozessor E5620

2x 2 GB Hauptspeicher

Open Bay, 2,5" SAS

Passend für alle IBM BladeCenter Chassis

1 Jahr Gewährleistung, 3 Jahre freiwilliger Herstellerservice



IBM System Storage® DS3524 Express

7.020,- € (inkl. MwSt.)*

monatl. IBM Leasingrate:

186,73 € (inkl. MwSt.)**

Best.-Nr.: 1746A4D, 49Y1836

6-Gbps-SAS-Schnittstellen, optional 8-GB-FC-Anschluss

Dual Controller fasst bis zu 24 Festplatten

1 Jahr Gewährleistung, 3 Jahre freiwilliger Herstellerservice

Plus: 8x 300 GB Hot-Swap-fähige 2,5" SAS-Festplatten



Trade-In-Programm für IBM Express Seller:

Neuen Server kaufen – Altgerät in Zahlung geben.

Bei welchen Geschäftspartnern Sie die IBM Express Seller Produkte direkt bestellen können, erfahren Sie unter

ibm.com/systems/de/express1



¹TBR Studie Q3 2011 bei x86-basierten Servern: Corporate IT Buying Behavior & Customer Satisfaction, Nov. 2011.

*Alle Preise sind Einzelhandelsverkaufspreise von IBM, gültig ab 1. Januar 2012. Die Preise können je nach Konfiguration schwanken. Die Einzelhändler legen ihre eigenen Preise fest, daher können die Wiederverkaufspreise an die Endverbraucher schwanken. Produkte unterliegen der Verfügbarkeit. Die Preise können ohne vorherige Mitteilung geändert werden. Es kann sein, dass im Einstiegspreis Festplatte, Betriebssystem oder andere Elemente nicht enthalten sind. Wenn Sie am aktuellen Preis in Ihrem geografischen Gebiet interessiert sind, setzen Sie sich bitte mit Ihrem IBM Ansprechpartner oder Ihrem IBM Geschäftspartner in Verbindung. *Monatliche IBM Leasingrate inkl. MwSt., bei 36 Monaten Laufzeit und einem Vertragsvolumen von mind. 4.000 Euro. Die Finanzierungsangebote sind freibleibend, gelten vorbehaltlich einer positiven Bonitätsprüfung durch IBM und richten sich ausschließlich an Geschäftskunden. IBM Gewährleistungsregelung zu den aufgeführten IBM System x Produkten: 1 Jahr Gewährleistung, 3 Jahre freiwilliger Herstellerservice. Die Bedingungen dieses freiwilligen Herstellerservice liegen der Lieferung bei bzw. sind unter ibm.com/servers/support/machine_warranties abrufbar. Die Gewährleistung gemäß den Geschäftsbedingungen von IBM, insbesondere die Gewährleistungsfrist von zwölf Monaten, bleibt davon unberührt. IBM, das IBM Logo, ibm.com, IBM System x, IBM BladeCenter und IBM System Storage sind Marken oder eingetragene Marken der International Business Machines Corporation in den Vereinigten Staaten und/oder anderen Ländern. Die komplette Liste der IBM Marken siehe unter: <http://www.ibm.com/legal/us/en/copytrade.shtml>. Intel, das Intel Logo, Intel Inside, das Intel Inside Logo, Xeon und Xeon Inside sind Marken oder eingetragene Marken der Intel Corporation oder ihrer Tochtergesellschaften in den Vereinigten Staaten und/oder anderen Ländern.

© 2012 IBM Corporation.