

iAdministrator

Das Magazin für professionelle System- und Netzwerkadministration

Im Test:
Citrix XenDesktop 4 12

Im Test:
RES PowerFuse 2010 24

Workshop:
**Red Hat Enterprise
Virtualisierung** 40

Workshopserie:
**Desktop-Pflege mit dem
Citrix Provisioning Server (1)** 45

Systeme:
Neues im SharePoint Server 2010 48

Desktop-Virtualisierung



VORSICHT: SCHLECHTER TONER ZIEHT IHNEN DAS GELD AUS DER TASCHЕ!



Undichte Tonerkartuschen, unbrauchbare Ausdrücke und häufige Ausfälle treiben Ihre Druckkosten unerwartet in die Höhe.

Original HP Toner sind optimal auf HP LaserJets abgestimmt und liefern hervorragende Qualität – Tag für Tag, Seite für Seite.



HIT PRINT
INTELLIGENTLY



Vermeiden Sie versteckte Druckkosten!
Entscheiden Sie sich für Original HP Toner!
Weitere Informationen finden Sie unter:

www.hp.com/de/toner

Von Säuen und Dörfern, Admins und Desktops

Liebe Leser,

heute schon virtualisiert? Vielleicht einen kleinen Server, einen Switch oder eine Handvoll Storage? Alles schon erledigt, rufen Sie mir entgegen – prima, dann können Sie sich ja daran machen, auch die Clients von der Last des physischen Daseins zu erlösen. Denn 2010, da scheint sich die IT-Industrie einig, steht voll im Licht der Desktop-Virtualisierung! Und Sie verschwenden noch Ihre Zeit damit, dieses Editorial zu lesen anstatt Ihrem Unternehmen gewaltige "Kostenreduktion", "Flexibilität" sowie "Endgerätesicherheit" zu sichern?



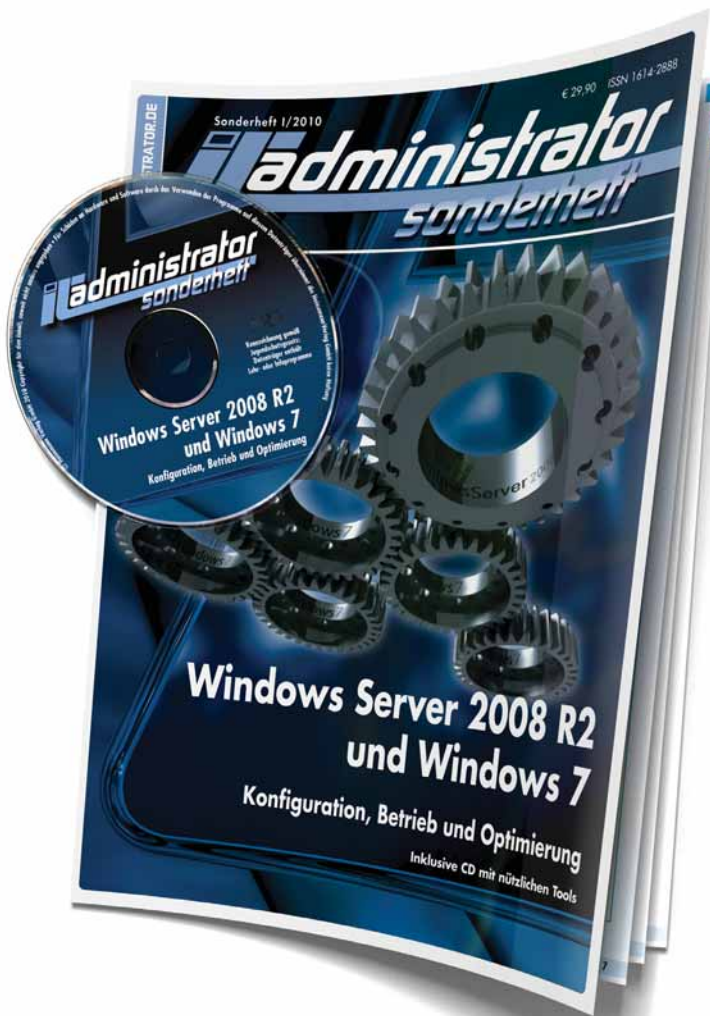
Ihre Entscheidung für Ersteres freut uns natürlich und bietet Ihnen zudem Gelegenheit, den Nutzen virtualisierter Desktops detailliert zu betrachten. Die folgenden knapp 70 Seiten zeigen Ihnen ausführlich auf, was aktuell dran ist am neuen IT-Wunderkind namens Desktop-Virtualisierung. Einerseits ist diese Technologie ohne Frage die Sau, die aktuell durchs Dorf getrieben wird: Obwohl die Virtualisierung im Serverraum keineswegs schon ausgereizt ist, verkünden die Hersteller lauthals unter Berufung auf die eingangs zitierten Vorteile, dass die Zeit reif sei für virtuelle Desktops. Verständlich insofern, als dass hier ein gewaltiger, komplett neu zu verteiler Markt winkt.

Andererseits sind Sie als Admin und IT-Verantwortlicher natürlich klug genug, die neue Sau nicht nach kurzer, oberflächlicher Betrachtung zu kaufen. Wer den Erwerb eines neuen Nutztiers plant, dem sei ans Herz gelegt, Martin Kuppingers Betrachtungen zu Sinn und Unsinn der Desktop-Virtualisierung ab Seite 31 zu lesen. Technologisch ist die Sache nämlich mittlerweile recht ausgereift, wie unsere Tests von XenDesktop 4 und VMware View 4 sowie der Workshop zur Red Hat-Virtualisierung zeigen. Aber ist eine ausgereifte Technik allein ein Grund zu einem Strategiewechsel, vor allem, wenn Sie Ihre Desktops nach jahrelangem Feinschliff und Investitionen in Clientmanagement-Suiten gut im Griff haben?

Zudem ist "ausgereift" dabei ein relativer Begriff, denn der nächste Technologiesprung steht unmittelbar bevor: als erster großer Anbieter stellte Citrix auf der CeBIT einen Bare Metal-Hypervisor für Clients vor, VMware will dieses Jahr noch nachziehen. Diese Gattung von Hypervisoren eröffnet mächtige neue Möglichkeiten bei Management und Virtualisierung von Clients. Hier bleiben wir für Sie am Ball, denn es wäre ja irgendwie schon blöd, wenn Sie die erste Sau kaufen, die zweite aber dann viel schöner ist.

Viel Vergnügen beim Lesen, Ihr


John Pardey
Chefredakteur



Bestellen Sie jetzt das IT-Administrator Sonderheft I/2010!

180 Seiten Praxis-Know-how

rund um das Thema

Windows Server 2008 R2 und Windows 7 + Tools-CD zum Abonnenten-Vorzugspreis* von

nur € 24,90!

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

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

Das Magazin für professionelle System- und Netzwerkadministration

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

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

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

Ich zahle per Bankeinzug

Firma: _____

Geldinstitut: _____

Name, Vorname: _____

Kto.: _____ BLZ: _____

Straße: _____

oder per Rechnung

Land, PLZ, Ort: _____

Datum: _____

Tel: _____

Unterschrift: _____

E-Mail: _____

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

So erreichen Sie unseren
Vertrieb, Abo- und
Leserservice:

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

leserservice@it-administrator.de

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



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

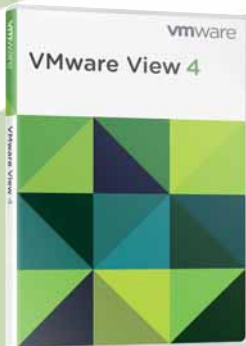
ITA 0410

INHALT

IT-Administrator – Ausgabe April 2010

Desktop-Virtualisierung

Im Test: VMware View 4



Auch im Desktop-Umfeld kommt die Virtualisierungs-Lawine nicht zum Halt: Mehr und mehr Unternehmen stellen dem Endanwender mittlerweile eine virtuelle Maschine als Desktop von zentraler Stelle aus zur Verfügung. Egal ob alter PC oder modernster Thin Client – die Oberfläche sieht immer gleich aus und wird von einem einzelnen oder einem Pool von Servern bereitgestellt. VMware schickt im Bereich Desktop-Virtualisierung VMware View ins Rennen. Wir haben uns in einem Test angesehen, wie sich Version 4 im Praxis-Einsatz schlägt.

Seite 19

DNS-Fehler finden und beheben (2)

Fehlermeldungen in Windows-Netzwerken und -Anwendungen haben ihre Ursache oft in Problemen bei der Namensauflösung. Vor allem bei verschachtelten Strukturen kann es schnell geschehen, dass einzelne Rechner keine korrekte Auflösung durchführen können. Im ersten Teil unserer Workshopserie haben wir Ihnen gezeigt, wie Sie Fehler in DNS-Einstellungen finden und beheben. Im zweiten Teil widmen wir uns spezifischen Fällen wie DHCP, Firewalls und dynamischen IP-Adressen, bei denen eine Namensauflösung per DNS nicht mehr ohne Weiteres funktioniert. Dabei erfahren, wo genau es hakt und wie Sie das Problem lösen.

Seite 52



Server- und Systemmanagement



Clientmanagement



Storage



Sicherheit



Messaging

Themenübersicht



Virtualisierung



Netzwerkmanagement



Job/Weiterbildung



Recht

AKTUELL

- 06 **News**
- 10 **ITANet aktuell:** IT-Administrator-Workshop "Virtualisierung mit Hyper-V R2" am 22. April 2010 in Köln – Nach Köln migrieren
- 11 **IT-Administrator vor Ort:** IT-Defense 2010, 3. bis 5. Februar, Brühl Gefühlte Sicherheit

PRODUKTE

- 12 **Im Test:** Citrix XenDesktop 4.0 Arbeitsplatz im Netz
- 19 **Im Test:** VMware View 4 Fernsicht für Clients
- 24 **Im Test:** RES PowerFuse 2010 Einheitlich individuell
- 30 **Im Kurzttest:** POPCon PRO 3.70 Von außen nach innen

PRAXIS

- 31 **Systeme:** Aspekte der Desktop-Virtualisierung Es ist nicht alles Gold, was glänzt
- 35 **Workshop:** Desktop-Virtualisierung mit dem Windows Server 2008 R2 Nah und doch fern
- 40 **Workshop:** Desktop-Verteilung mit Red Hat Enterprise Virtualisierung Der Pinguin wird virtuell
- 45 **Workshopserie:** Virtuelle Maschinen mit dem Citrix Provisioning Server warten (1) – Systeme am laufenden Band
- 48 **Systeme:** SharePoint Server 2010 Ansatz zur Punktlandung
- 52 **Workshopserie:** DNS-Probleme im Netzwerk beheben (2) Ohne Umwege ans Ziel
- 56 **Workshop:** Lotus Domino 8.5 Zentrales Passwort- und Zertifikatsmanagement
- 57 **Tipps, Tricks & Tools**

WISSEN

- 60 **Know-how:** Voraussetzungen für eine erfolgreiche Desktop-Virtualisierung – Chancen nutzen, Risiken vermeiden
- 63 **Buchbesprechung** "Clusterbau" und "Sichere Webanwendungen"
- 64 **Website & Fachartikel online**

RUBRIKEN

- 03 **Editorial**
- 05 **Inhalt**
- 33 **Stellenmarkt**
- 55 **Seminarmarkt**
- 65 **Das letzte Wort**
- 66 **Vorschau, Impressum, Inserentenverzeichnis**

Redundante Speicher für den Mittelstand

Netgear präsentiert zwei neue hochperformante **Netzwerkspeicherlösungen** der ReadyNAS-Produktfamilie. Mit dem Modell **ReadyNAS 3100** erhalten Anwender ein Rackmount-Gerät mit einer Höheneinheit (1U) und vier Festplatteneinschüben für eine Speicherkapazität von bis zu 8 TByte. Das Modell 4200 bietet zwei Höheneinheiten (2U) und zwölf Einschübe für bis zu 24 TByte Speicherkapazität. Die Storage-Server unterstützen dabei bis zu 500 Anwender und eignen sich laut Hersteller für den Einsatz als primäre Speicherlösung für mittlere Unternehmen oder als hochperformante Zweitlösungen für große Unternehmen. Bei-

de Speichersysteme, die auf dem Linux Betriebssystem "ReadyNAS RAIDiator" basieren, unterstützen zudem VMware, Microsoft Hyper-V sowie Citrix XenServer. Für Ausfallsicherheit sorgen hot-swappable SATA-Laufwerke sowie ein redundantes Kühlsystem, redundante Netzwerkanschlüsse, ECC (Error Correcting Code)-Speicher und redundante Stromversorgung. Die Variante ReadyNAS 4200 ist zudem das erste ReadyNAS-Gerät mit zwölf SATA-Einschüben, das eine 10-GBit-Netzwerkinfrastruktur unterstützt. Zu Redaktionsschluss standen die endgültigen Preise für die Geräte noch nicht fest. (dr)

Netgear: www.netgear.de



Speichern bis zu 24 TByte auf zwei Höheneinheiten: Die ReadyNAS-Appliances von Netgear

iSCSI-SAN für den Einstiegsbereich

Overland Storage stellt mit dem **SnapServer SAN S2000** eine neue, auf **iSCSI-basierende SAN-Plattform** vor. Das zwei Höheneinheiten messende System verfügt, je nachdem, ob es mit zwölf SATA II- oder SAS-Platten ausgestattet wird, über eine Brutto-Speicherkapazität zwischen 7,2 und 24 TByte. Mit Hilfe einer Erweiterungseinheit lässt sich die SAN-Komponente auf bis zu 120 TByte erweitern. Im Inneren des Gehäuses geben ein Intel Xeon E5504 Quad-Core-Prozessor und 2 GByte DDR3-RAM den Takt vor. Zum Funktionsumfang des Geräts zählen zur Steigerung der Anwendungsverfügbarkeit unter anderem Aktiv/Mirroring

und -Failover. Weiterhin ist der SnapServer SAN S2000 mit dem Windows Multi-Path I/O (MPIO) Framework kompatibel und unterstützt Microsoft Cluster Server. Bis zu 256 Snapshots, mehrere hunderttausende Replikationspunkte sowie die RAID-Level 0, 1, 5, 6, 10, 50 und 60 sollen für Datensicherheit sorgen. Um Überprovisionierung zu vermeiden, können Nutzer auf die automatische Kapazitätserweiterung zurückgreifen. Diese kontrolliert die Festplattenbelegung und stockt Volumes automatisch auf, wenn zuvor festgelegte Grenzwerte überschritten werden. Der Hersteller hat den Storage-Server für virtuelle Umgebungen unter VMware und Microsoft Hyper-V optimiert. So ist es möglich, den Speicher für ESX-Cluster bereitzustellen und mittels der Volume Shadow Copy Services Backups im laufenden Betrieb durchzuführen. Je nach Speicherkapazität ist der SnapServer SAN S200 ab 11.200 Euro erhältlich. (In)

Overland Storage: www.overlandstorage.com



Der "SnapServer SAN S2000" von Overland Storage fühlt sich auch in virtualisierten Umgebungen wohl

Acer macht auf Thin Client

Acer bringt seinen Nettop-Rechner **Veriton N260G** auch als **Thin Client-Variante** in den Verkauf. Das Gerät ist mit einem Intel Atom 280-Prozessor mit 1,66 GHz und 1 GByte DDR2-RAM sowie einem 8 GByte fassenden SSD-Speicher ausgestattet. Als Bildschirmauflösung sind über den integrierten Grafik-Chip Intel 4500M maximal 2.048 x 1.536 Pixel möglich. Anschluss an das Netzwerk findet der schlanke Rechner über eine GBit-Ethernet-Schnittstelle. Das mitgelieferte VESA Mount-Kit erlaubt eine platzsparende Montage des PCs an der Rückseite handelsüblicher Displays. Als Software kommt auf dem Thin Client der Universal Desktop Advanced von IGEL zum Einsatz. Das Betriebssystem bietet Zugriff auf die gängigen Server Based Computing- und Virtual Desktop-Umgebungen. Die Anbindung erfolgt hier unter anderem über RDP, ICA, X-Access, Citrix XenDesktop oder VMware View. Was Druckdienste betrifft, finden LPD, IPP und Thin Print Unterstützung. Wie alle IGEL-Produkte lassen sich auch die Acer-Modelle zentral über die Universal Management Suite verwalten. Die Thin Client-Version des Veriton N260G ist ab sofort für rund 340 Euro erhältlich. (In)

Acer: www.acer.com



Bei der Thin Client-Variante des "Acer Veriton N260G" kommt die Software von IGEL

Vielseitige Netzwerkknoten

SMC Networks stellt zwei neue **Managed Layer-3-Switches** der Reihe der **TigerStack II 1000** vor – die Modelle **SMC8926EM** und **SMC8950EM**. Die Switches arbeiten hochperformant, sind skalierbar und eignen sich laut Anbieter für den Einsatz in verteilten Netzwerkinfrastrukturen. Die Geräte verfügen über 24 beziehungsweise 48 10/100/1000 Base-T-Ports sowie vier kombinierte RJ-45/SFP-Ports, zwei Ports für das Stacking und zwei Slots für die XFP-Module für 10-GBit-Verbindungen. Die beiden Switches unterstützen zudem die Internet-Protokolle IPv4 sowie IPv6. Zum Funktions- und Protokollumfang gehören außerdem unter anderem statisches Routing, VLAN-

Unterstützung, das Routing Information Protocol RIP v1/2, das Virtual Router Redundancy Protocol, Open Shortest Path First und Spanning Tree. Die Geräte unterstützen zudem ACLs, den Standard 802.1x, RADIUS sowie TACACS+, statische Port-Sicherheit, DNS und das Link Layer Discovery Protocol LLDP. Über QoS lässt sich die Bandbreite an jedem Port verwalten. Administratoren können via Telnet und SSH, HTTP und HTTPS, SNMP sowie über den RS-232-Konsolen-Port auf die Geräte zugreifen. Für rund 1.700 beziehungsweise 2.600 Euro sind die beiden Switches verfügbar. (dr)

SMC Networks: www.smc.com



Die neuen TigerStack II-Switches von SMC verfügen über zahlreiche Netzwerk-Features

Suchmaschine für Server-Logs

Splunk bietet seine gleichnamige Software nun auch in Deutschland an. Die aktuelle **Version 4.1** indiziert im Unternehmensnetzwerk die **Logdaten** von Applikationen und stellt deren Inhalte in einer webbasierten Volltextsuche zur Verfügung. Damit können Administratoren quer durch alle Log- und Konfiguration-Files verschiedener Server – auch in virtuellen Umgebungen – nach Ereignissen und anderen Einträgen suchen und etwa Fehler, die auf unterschiedlichen Servern auftreten, miteinander in Verbindung bringen. Eine vorherige Anpassung (Parsing) der ausgewerteten Dateien ist für eine Nutzung mit Splunk nicht nötig. Auf Informationen, die nicht in zugänglichen Logdateien abgelegt wurden, greift die Software unter anderem

über Syslog und WMI zu. Die Suche in der Ajax-basierten Weboberfläche erinnert dabei stark an Internet-Suchmaschinen. Einmal angelegte Suchen lassen sich für eine spätere Nutzung abspeichern. Ferner besteht die Möglichkeit, bestimmte Ereignisse in Dashboards grafisch zusammenzufassen sowie E-Mail- oder SNMP-Alerts zu versenden. Ein Scheduler erlaubt zudem die regelmäßige und automatisierte Suche nach bestimmten Einträgen. An Betriebssystemen setzt Splunk entweder Unix oder Windows XP, Vista, Server 2003 oder Server 2008 voraus. Zudem läuft die Software unter Mac OS. Für bis zu 500 MByte an Logdaten pro Tag lässt sich die Suite kostenlos nutzen. (dr)

Splunk: www.splunk.com

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

Dem französischen Hersteller **Cocasse** ist es nach eigenen Angaben gelungen, ein leitfähiges **Glasfaserkabel** zu entwickeln, das parallel auch **Strom überträgt**. Hierfür kommt ein eigens patentiertes Material namens **Perfoflex** im Kabel zum Einsatz, das vergleichbare elektrische Eigenschaften wie Kupfer aufweisen und zudem Licht übertragen soll. Somit lassen sich laut Hersteller doppelte Verkabelungen für Fibre Channel und Ethernet beziehungsweise MPLS künftig vermeiden. Ein weiterer Vorteil soll die Dehnbarkeit des Materials sein, wodurch die Kabellängen beim Verlegen flexibel anpassbar würden. Am 1. April 2012 soll das Kabel auf den Markt kommen. (dr)

www.woxikon.de/tra/cocasse.php

azeti veröffentlicht mit dem **SONARMANAGER** eine Plattform für das **zentrale Management der Monitoring-Appliances** aus der Reihe SONARPLEX. Nach Filialen sortiert, erscheinen in der GUI die beteiligten Appliances, die Hosts und die eingerichteten Services. Mit dem integrierten Host-Scanner und fertigen Templates will der Hersteller zudem das Einrichten neuer Hosts vereinfachen. Das Werkzeug erkennt automatisch, welche IP-Adressen vergeben sind, so dass nur noch wenige manuelle Eingaben zum Anlegen neuer Hosts erforderlich sind. Weiterhin lässt der SONARMANAGER Backups der angeschlossenen Appliances zu. Im Preis einer Sonarplex-Appliance ist je eine Lizenz der Software enthalten. (In)

www.azeti.net

Mit dem Tool **ChangeBASE AOK** hilft **Matrix42** Unternehmen, die bei der Migration zu Windows 7 auf Probleme mit der **Kompatibilität von Altapplikationen** stoßen. Das Werkzeug erlaubt es, alle Anwendungen, die auf Basis eines MSI-Files installiert wurden, hinsichtlich ihrer Lauffähigkeit unter Windows 7 zu untersuchen. Ist die Software nicht kompatibel, so meldet sich das Programm entweder mit einer roten oder gelben Ampel. Ein gelbes Signal deutet darauf hin, dass das Tool die Software soweit anpassen kann, dass diese unter Windows 7 lauffähig wird. Die Lösung korrigiert bei der Konvertierung Einstellungen der Altsoftware auf der Basis von mehr als 200.000 Regeln, welche die Kompatibilität mit Windows 7 definieren.

Nach der sogenannten automatischen Bereinigung der Installationsdatei lässt sich diese auch nach der Migration zu Windows 7 weiter im Unternehmen betreiben. ChangeBase AOK von Matrix42 ist zu einem Preis von 175 Euro pro bearbeiteter Applikation erhältlich. (jp)

www.matrix42.de

ESET ersetzt mit **ESET Mail Security für Microsoft Exchange Server** die bisherige Version **ESET NOD32 für Microsoft Exchange Server**. Die neue Exchange-Lösung bietet einen proaktiven Antivirus-Schutz mit Anti-Rootkit-Technologie und HIPS-Funktion. Das integrierte Spam-Modul blockt zudem unerwünschte E-Mails, auch wenn sie das Unternehmensnetz TLS-verschlüsselt erreichen. Eine optimierte "ThreatSense Scan"-Engine unterstützt außerdem die gleichzeitige Verarbeitung mehrerer Threads im Hintergrund (Multithreading). Von Exchange-Version 5.5 bis 2010 lässt sich die Software einsetzen. Sie kostet beispielsweise für 20 zu schützende Mailboxen und zwei Jahre 384 Euro. (dr)

link:www.eset.de

Schneller Cache durch Solid State

FalconStor Software bringt in Kooperation mit Violin unter dem Namen **NSS SAN Accelerator** eine **SAN-Umgebung** auf den Markt, die mit Hilfe eines SSD-Cache für eine deutliche Beschleunigung beim Lesen und Schreiben von Daten sorgen soll. Das System ist eine Kombination des FalconStor Network Storage Server (NSS) mit einem Violin 1010 Flashspeicher. Als Cache-Plattform für alle Daten, die einen besonders schnellen I/O erfordern, kommt dabei ein Solid State-Speicher-Array zum Einsatz. Dieser beschleunigt die Lese- und Schreibvorgänge durch die Funktionen SafeCache und HotZone: SafeCache reserviert einen Bereich des SSD-Speicherarrays für das Schreiben der Anwendungen, so dass alle Schreibvorgänge mit geringer Latenzzeit empfangen und bestätigt werden können. Erst dann schreibt die Lösung die Daten in die Zielspeicher-Volumes



Als dem SAN vorgeschalteter Cache sorgt der "NSS SAN Accelerator" per SSDs für mehr Geschwindigkeit beim Datenzugriff

des SAN. HotZone hingegen beschleunigt den Lesevorgang, wie etwa kontinuierlich wiederkehrende Datenbankzugriffe, indem es die Zugriffsmuster auf dem Datenträger überwacht und häufig verwendete Daten für einen schnelleren Lesezugriff in einen Cache-Bereich im SSD-Speicherarray kopiert. Wenn die Daten weniger häufig in Nutzung sind,

werden diese wieder aus dem Cache gelöscht und auf ihren ursprünglichen Speicherort im SAN verwiesen. Der NSS SAN Accelerator ist ab Mai 2010 zu einem Preis von 25.600 Euro erhältlich. In diesem Preis ist bereits ein RAID-geschützter SSD-Speicherarray mit 500 GByte Kapazität enthalten. (In) FalconStor: www.falconstor.com

Switches mit Selbstschutz

D-Link baut mit den Serien **DES-1210** und **DGS-1210** das bestehende Portfolio an **Smart Managed Switches** weiter aus. Die neue Fast Ethernet-Reihe DES-1210 (24 oder 48 Port-Modelle) sowie die neue GBit-Reihe DGS-1210 (16, 24 oder 48 Port-Modelle) verfügen dabei über erweiterte Sicherheitsoptionen. So schaltet sich die "D-Link SafeGuard Engine" ein, wenn nach Virenbefall einzelner Netzwerkkomponenten große Daten-

mengen den Prozessor zu überlasten drohen. Darüber hinaus unterstützen die Geräte ACL (Access Control List). Diese legt fest, welcher Benutzer welche Dienste und Dateien nutzen darf, und authentifiziert diese Nutzer durch den IEEE 802.1X Standard. Für zusätzliche Sicherheit sorgt das DHCP Server Screening Feature (ab Firmware Release 2). Der Switch erkennt hierbei anhand der DHCP-Anfrage der

Clients und der entsprechenden Antwort des Servers dessen IP-Adresse und ordnet diese automatisch der dem Port zugehörigen MAC-Adresse zu. Außerdem hat der Hersteller die Switches mit nützlichen Layer 2 Funktionen ausgestattet, inklusive IGMP Snooping, Port Mirroring und dem LACP Trunking-Protokoll. Rapid Spanning Tree und Loopback Detection erkennen zudem redundante Schleifen und blockieren die doppelte Verbindung automatisch.

Die Cable Diagnostics-Funktion erlaubt Netzwerkadministratoren, den Status und eventuelle Fehlfunktionen der Kupferleitungen schnell zu ermitteln und zu beheben. Für 289 bis 945 Euro sind die Geräte ab sofort erhältlich. (dr)



D-Links Fast Ethernet Switch-Serie DES-1210 soll bis zu 20 Prozent weniger Energie als die Vorgänger verbrauchen

D-Link: www.dlink.de

Holen Sie sich das Netviewer-Buch
und testen Sie die Software
14 Tage gratis!

Erfolg kommt
online

Ein paar ziemlich gute Argumente
für eine Online-Meeting-Kultur

netviewer

So bekommt Ihr Online-Support Flügel!

Mit Netviewer Support sorgen Sie per Mausklick für einen besseren Kundenservice bei niedrigeren Kosten. Anfragen lösen Sie schnell und unkompliziert – und Ihre Kunden werden Sie für einen Engel halten.

Weitere überraschende Anregungen erhalten Sie im kostenlosen Netviewer-Buch. Gleich bestellen und Gratis-Testversion anfordern unter **0721 35 44 99 400** oder:

www.netviewer.com/engel

Online-Meeting-Kultur jetzt leben!


netviewer

IT-Administrator-Workshop "Virtualisierung mit Hyper-V R2" am 22. April 2010 in Köln

Nach Köln migrieren

von John Pardey



Dank der Live Migration in Hyper-V R2 kann der Administrator virtuelle Computer von einem Host auf einen anderen Host übertragen, ohne dass Benutzer ihre Daten verlieren oder von den Servern getrennt werden. Diese praktische Funktion betrachten wir in unserem April-Workshop in Köln im Detail.

Der große Unterschied zur Quick Migration in Hyper-V Version 1 ist, dass die Maschinen während der Übertragung aktiv bleiben und auch der Arbeitsspeicherinhalt zwischen den Servern übertragen wird. Basis der neuen Technik ist ein Cluster mit Windows Server 2008 R2, daher können nur die Enterprise Edition und Datacenter Edition von Windows Server 2008 R2 dazu verwendet werden.

Cluster Shared Volumes

Besonders wichtig für Live Migration sind die Cluster Shared Volumes, eine neue Funktion in Windows Server 2008 R2. Diese ermöglichen, dass mehrere Server in einem SAN gleichzeitig auf einen gemeinsamen Datenträger zugreifen können und damit dieselbe LUN verwenden können. Live Migration übernimmt dabei auch den Inhalt des Arbeitsspeichers auf den anderen Host, so dass Anwender weiterarbeiten können. Voraussetzung dafür ist, dass alle Knoten im Cluster vollkommen identisch sind. Der wichtigste Punkt bei der Live Migration ist die Echtzeitübertragung des Arbeitsspeicherinhalts zwischen den Clusterknoten, daher ist es auch extrem wichtig, dass es sich um die gleichen Prozessoren handelt, keine verschiedenen Typen. Durch die Live Migration können einzelne Clusterknoten effizient gewartet werden, da sich die VMs leicht und problemlos verschieben lassen. Dadurch lassen sich Erweiterungen, Softwareupdates und Hardwareaustausch sehr


schnell bewerkstelligen, ohne Anwender zu beeinträchtigen.

Ablauf einer Live Migration

Während des Vorgangs der Live Migration läuft die VM uneingeschränkt weiter. Beim Start einer solchen Migration baut der Quell-Server eine Verbindung zum Ziel-Server auf, der die virtuelle Maschine in Echtzeit erhalten soll. Anschließend überträgt der Quell-Server die Konfiguration der VM auf den Ziel-Server. Der Ziel-Server erstellt auf Basis dieser leeren Konfiguration eine neue VM, die der zu verschiebenden VM entspricht. Nun überträgt der Quell-Server die einzelnen Seiten des Arbeitsspeichers zur Ziel-VM in einer Standardgröße von etwa 4 KByte. In diesem Schritt zeigt sich die Geschwindigkeit des Netzwerks. Je schneller das Netzwerk, umso schneller wird der Inhalt des Arbeitsspeichers übertragen. Als Nächstes übernimmt der Ziel-Server die virtuellen Festplatten des Quell-Servers für die zu übertragende virtuelle Maschine. Anschließend setzt der Ziel-Server die virtuelle Maschine online. Nun wird der virtuelle Hyper-V-Switch informiert, dass der Netzwerkverkehr jetzt zur MAC-Adresse des Ziel-Servers gesendet werden soll.

Große Nachfrage

Um mehr über dieses und andere interessante Fähigkeiten des Hyper-V R2 zu erfahren, empfiehlt es sich, sich rasch einen Platz zu sichern, da wir bereits im März

sehr viele Anmeldungen zu verzeichnen hatten und das Platzkontingent begrenzt ist. Wir würden uns auf jeden Fall freuen, Sie in Köln begrüßen zu dürfen. 



Die Agenda des Workshops

13.00 Uhr: Begrüßung

13.15 Uhr: Hyper-V Server 2008 R2

- Leistungsfähigkeit von Hyper-V R2 unter der Lupe – Gegenüberstellung mit XEN/VMware
- Planung der Hyper-V-Installation (Storage-Planung und Kapazitätsplanung auf dem Host)
- Was alles unter der Haube steckt (Snapshots, Live-Migration, Backup)
- Management des Hyper-V mit SCVMM

*Dozenten: Thomas Wegener und Günther Schmitz
sepago GmbH, Köln*

17.30 Uhr: Ende des Workshops

Ort: sepago GmbH,
Dillenburger Straße 83,
51105 Köln

Teilnahmegebühren:

Für IT-Administrator Abonnenten kostenlos.

Anmeldung bis zum 16. April unter

www.it-administrator.de/workshops/

Workshop "Virtualisierung mit Hyper-V R2" am 22. April





IT-Defense 2010, 3. bis 5. Februar, Brühl

Gefühlte Sicherheit

von Daniel Richey

IT-Sicherheit geht weit über Antivirus, Firewalls und Intrusion Detection hinaus. Wie weit, das zeigte die IT-Defense 2010 in Brühl. Eine breite Palette an On- und Offline-Sicherheitsthemen gab den rund 200 Teilnehmern Denkanstöße und rüttelte so manchen IT-Administrator wach.

Gespant lauschten die rund 200 Teilnehmer der IT-Defense Anfang Februar Moxie Marlinspike, als er grundlegende Schwachstellen in SSL erläuterte. Diesmal ging es nicht um Angriffe auf die Algorithmen oder die zugehörige Software. Marlinspike vom Institute for Disruptive Studies verdeutlichte vielmehr, wie leicht sich Zertifikate von echten Zertifizierungsstellen – den sogenannten CAs – erschleichen lassen. Mit einem einfachen Trick bei der Beantragung der Zertifikate lassen sich Browser, Mailclient und Co. austricksen. So reicht es laut Marlinspike aus, in den Online-Antrag einen sogenannten Nullcharacter einzufügen, also etwa `www.bank.de\0.hackerdomain.com`. Die Zertifizierungsstelle erkennt den Antrag korrekterweise auf `hackerdomain.com` und stellt das Zertifikat entsprechend aus. Doch der Browser interpretiert den Nullcharacter anders und nimmt das Zertifikat für `www.bank.de` an. Opera hat als erster Hersteller hier versucht, den Fehler zu beheben – wenn auch nicht sonderlich erfolgreich. Doch sollen nach diversen Berichten inzwischen die Software-Hersteller diesen Fehler behoben haben.

Ein Bein im Knast

Auf ebenfalls sehr großes Interesse stieß der Vortrag von Prof. Thomas Hoeren, Richter am Oberlandesgericht Düsseldorf. Er verdeutlichte, wie schnell ein IT-Verantwortlicher durch das Bundesdatenschutzgesetz persönlich zur Kasse gebeten werden kann – auch wenn er


angestellt ist und auf Anweisung hin arbeitet. Welche abstrusen Urteile deutsche Gerichte dabei mitunter fällten, zeigte Hoeren an einigen Beispielen auf. Ein Mitarbeiter etwa klagte, weil der Administrator einen Spamfilter im Netzwerk einsetzte – und bekam vom OLG Karlsruhe Recht. So sei Spam in erster Linie Post und unterliege dem Briefgeheimnis. Nur bei einer gleichzeitigen Einwilligung von Empfänger und Absender dürfe das Spam gefiltert werden. Bei unerwünschten Werbemails kein leicht zu erfüllendes Kriterium. Dass diese Rechtsprechung nicht auf die leichte Schulter genommen werden darf, verdeutlicht das hierfür zuständige Strafrecht.

Auch Administratoren, die sich für ihre Unternehmenswebseite als Admin-C eintragen lassen, setzen sich besonderen Risiken aus. Denn ein Admin-C haftet laut Hoeren etwa bei Werberechts-, Urheberrechts-, Verbraucherschutzverstößen und ähnlichem mit dem Privatvermögen. Zudem entgeht der Admin-C nur dann der Denic-Verantwortung, wenn der Domaininhaber ihn daraus entlässt. Trägt sich ein Mitarbeiter als "Verantwortlicher im Sinne des Presserechts" (ViSdP) ein, haftet er sogar für alles, was auf dieser Website passiert. Dazu zählen auch Links – selbst wenn auf einen Haftungsausschluss hingewiesen wurde. Das so gerne zitierte Urteil des LG Hamburg vom 22. Mai 1998 hat es laut Hoerer dabei übrigens nie gegeben.

Neues in Snort

Da Administratoren natürlich im Rahmen ihrer Tätigkeit auch den Netzwerkverkehr überwachen müssen, stellte Martin Roesch als Vater des Traffic-Analyse-Systems Snort die neue Version 3.0 vor. So beinhaltet das Tool nun neben einer IPv6-Unterstützung auch Multiprotocol Label Switching und Generic Routing Encapsulation. Um die Datenanalyse dabei zu beschleunigen, soll Snort künftig auch über ein Multithread Execution Model verfügen und Datenpakchen gleichzeitig durch mehrere Engines laufen lassen können. Besonders legte Roesch Wert darauf, in der neuen Version 3 auch die Code-Basis bereinigt zu haben. So sei das Tool quasi von Grund auf neu entwickelt worden und alter Code beseitigt. Snort 3 besteht dabei aus zwei wesentlichen Komponenten.

Dies ist einerseits die SSP (Snort Security Platform), auf der die Analyse läuft und die die Applikationen kontrolliert. Die Engines sind daneben die Applikationen in Snort. Diese laufen auf SSP. Damit lassen sich praktische Anwendungen ausführen, etwa jede Traffic-basierte Applikation oder etwa Vulnerability-Scanner. Bei der Network Map andererseits lassen sich die Regeln anhand der im Netzwerk genutzten Geräte gruppieren und zuordnen. So muss eine Detection Logic nicht einen Windows-Server vor Linux-Exploits schützen und Snort kann darauf basierend die Regeln effizienter nutzen. Ein manuelles Einpflegen der Daten ist damit nicht mehr nötig und ein Angreifer verliert seinen Informationsvorsprung über die anzugreifenden Systeme.

Weitere Themen auf der IT-Defense 2010 waren unter anderem die Sicherheit des GSM-Mobilfunksystems, das McColo-Botnetz sowie das Social Engineering und Ausspähen von Daten ohne technische Hilfsmittel. Damit bot die Veranstaltung einen Einblick in das Thema Sicherheit, das weit über die üblichen Ansätze mit Firewall, UTM und Co. hinausgeht. 

**Im Test: Citrix XenDesktop 4.0**

Arbeitsplatz im Netz

von Christian Knermann

Seit im Februar 2007 der Citrix Desktop Server 1.0 veröffentlicht wurde und im Mai 2008 zum XenDesktop 2.0 avancierte, hat das Produkt eine rasante Entwicklung erfahren. Mit Version 4.0 bietet die inzwischen ausgereifte Lösung nun ein vollständig neues Lizenzmodell sowie angepasste Editionen.

IT-Administrator hat sich die derzeit aktuelle XenDesktop-Variante einmal genauer angeschaut.

Die gute Nachricht für Administratoren ist, dass sich mit dem Sprung auf die neue Version die Architektur gegenüber dem im letzten Jahr getesteten XenDesktop 3.0 [1] nicht gravierend geändert hat. Das erworbene Wissen bezüglich Installation und Administration bleibt also in weiten Teilen gültig. Nach wie vor funktioniert eine XenDesktop-Farm ähnlich der Terminalserver-Lösung XenApp.

An die Stelle der Terminalserver treten ein oder mehrere sogenannte Desktop Delivery Controller (DDC), die sich eine Datenbank für ihre Konfiguration teilen. Darin werden unter anderem Informationen darüber gespeichert, welche virtuellen Desktops verfügbar sind und welche Benutzer und Gruppen darauf zugreifen dürfen. Das Citrix Web Interface ruft diese Informationen vom XML-Dienst des DDC ab und liefert wahlweise eine interaktive Webseite oder eine Konfigurationsdatei für das Citrix Online-Plug-In an die Clients. Gleichmaßen lässt sich eine Terminalserver-Farm zusätzlich in das Web Interface integrieren, so dass unter einer Oberfläche eine integrierte Komplettlösung zur Anwendungsbereitstellung entsteht. Details zur Architektur liefert ein Citrix-Webinar, das als Aufzeichnung online verfügbar ist [2].

Nur noch vier Editionen

Statt ehemals fünf umfasst das aktuelle Release nunmehr vier unterschiedliche Editionen. Die "Express Edition" ist weiter-

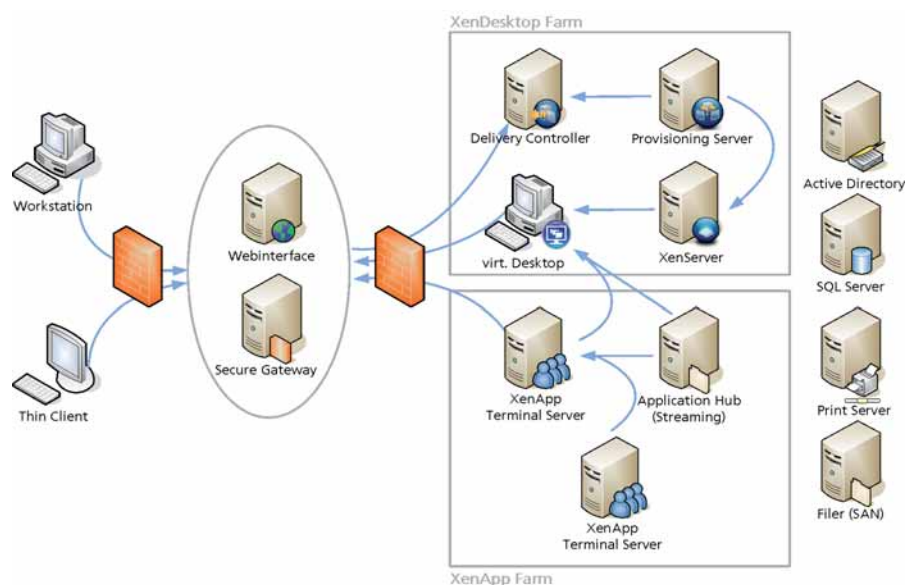


Bild 1: XenDesktop und XenApp vereinen sich zu einer umfassenden Lösung zur Applikationsbereitstellung

hin kostenfrei verfügbar und erlaubt es, Desktops an bis zu zehn gleichzeitige Benutzer, sogenannte Concurrent User (CCU), bereitzustellen. Dabei darf es sich allerdings ausschließlich um Desktops handeln, die als virtuelle Maschine auf einem Hypervisor laufen. Sollen auch Verbindungen zu physischen Maschinen, wie etwa dedizierte Desktop-Blades, vermittelt oder mehr als zehn CCU versorgt werden, so ist mindestens die neue "VDI Edition" erforderlich. Diese bietet zusätzlich die Möglichkeit, Desktop-Betriebssysteme an virtuelle Ziele zu streamen. Weiterhin ist Citrix StorageLink zur einfachen Verwaltung von SAN-Speicherplatz für die entsprechenden Desktop-Images an Bord.

Um die Roaming Profiles der Anwender kümmert sich der Citrix Profile Manager. Zur umfassenden Lösung zur Bereitstellung von Applikationen wird XenDesktop mit der "Enterprise Edition". Diese erlaubt es, nach Belieben virtuelle und physische Ziele mittels Provisioning Server zu starten. Hinter der zusätzlichen Funktion, "gehostete Shared Desktops" bereitzustellen, versteckt sich nichts anderes als die Terminalserver-Lösung XenApp, die mit zum Umfang der Enterprise Edition gehört. Diese eignet sich beispielsweise zur Bereitstellung von Anwendungen, die selten genutzt oder häufig aktualisiert werden müssen und daher nicht direkt in die Desktops integriert werden sollen.



Eine der Schlüsselfunktionen der Enterprise Edition wird sicherlich die Nutzung von "Offline Desktops" wer-

den. Damit soll es möglich werden, Desktop-Instanzen, die im Rechenzentrum laufen, beispielsweise auf ein

Notebook herunterzuladen, unabhängig vom Unternehmensnetz offline zu nutzen und Änderungen anschließend wieder mit der zentralen Desktop-Farm zu synchronisieren.

Zum Redaktionsschluss war diese Funktion noch nicht verfügbar, denn Voraussetzung ist ein Hypervisor auf dem Client, der analog zum XenServer im Rechenzentrum in der Lage ist, einen virtuellen Desktop auszuführen. Ein solcher Client-Hypervisor mit dem Namen Citrix XenClient befindet sich derzeit in der Entwicklung und soll in formellen Informationen zufolge im zweiten Quartal 2010 als finale Version erscheinen. Die "Platinum Edition" ergänzt XenDesktop schließlich um die nötigen Zugriffslizenzen zur Nutzung weiterer Citrix-Produkte, wie Monitoring mittels EdgeSight, sicherer Zugriff von außen via Access Gateway oder Beschleunigung von WAN-Sitzungen über den Citrix Repeater.

Die Versionen und ihre Funktionen					
Feature	Express	VDI	Enterpr.	Platinum	
Gehostete VM-basierte Desktops	✓	✓	✓	✓	
Gehostete Blade-PC-basierte Desktops	-	✓	✓	✓	
Gehostete Shared Desktops und Anwendungen	-	-	✓	✓	
Offline Desktops (ab Verfügbarkeit von XenClient)	-	-	✓	✓	
Provisioning virtueller Maschinen	-	✓	✓	✓	
Provisioning physischer und virtueller Maschinen	-	-	✓	✓	
Windows Profil-Management	-	✓	✓	✓	
Power Management	-	-	✓	✓	
StorageLink-Technologie	-	✓	✓	✓	
Performance Monitoring (Citrix EdgeSight)	-	-	-	✓	
Secure Remote Access (Citrix Access Gateway)	-	-	-	✓	
WAN-Optimierung (Citrix Repeater)	-	-	-	✓	
Single Sign-On (Citrix Password Manager)	-	-	-	✓	



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

180 Seiten Praxis-Know-how
rund um das Thema

Active Directory zum Abonnenten-Vorzugspreis* von

nur € 24,90!

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

Liefertermin:
Mitte Oktober 2010

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier 
www.it-administrator.de/kiosk/sonderhefte/



Neues Lizenzmodell

Eine Änderung hält bei der Art und Weise der Lizenzierung Einzug. Citrix wechselt hier erstmalig vom Prinzip des Concurrent Use hin zu Lizenzen pro namentlich benannten Benutzern (Named User) oder Endgeräten (Named Device). Was bedeutet dies für ein Unternehmen? Beginnen wir zunächst bei der VDI-Edition. Diese kann weiterhin wahlweise pro Concurrent Use oder pro User/Device lizenziert werden. Welche Variante wirtschaftlich sinnvoll ist, lässt sich nicht pauschal bestimmen. Da eine Lizenz pro User oder Device gegenüber CCU um mehr als die Hälfte günstiger ist, hängt die Entscheidung vom Nutzungsverhalten ab. Sind beispielsweise in einem Unternehmen 100 Benutzer beschäftigt, die nur selten und nicht zur gleichen Zeit einige Spezialanwendungen von virtuellen Desktops oder Terminalservern beziehen, empfiehlt sich das Concurrent Use-Modell. Sobald aber die Desktopvirtualisierung strategisch eingesetzt wird und mehr als 50 Prozent der Anwender gleichzeitig arbeiten, sollten die günstigeren Lizenzen pro natürliche Person oder pro physisches Endgerät zum Einsatz kommen. Letztere eignen sich für Szenarien, in denen sich mehrere Benutzer ein Arbeitsgerät teilen. Besitzt ein Anwender dagegen mit Notebook sowie Thin Client und Arbeitsplatz mehrere Geräte, empfiehlt sich stattdessen die Lizenzierung pro User.

Für die Editionen Enterprise und Platinum ist nunmehr ausschließlich die Named User-Lizenzierung verfügbar, was unter anderem in den erweiterten technischen Möglichkeiten begründet liegt. Sobald mit der Verfügbarkeit von XenClient virtuelle Desktops auch offline und unabhängig von der Unternehmensinfrastruktur genutzt werden können, ist zentral schlicht nicht mehr feststellbar, wie viele Anwender gleichzeitig arbeiten. XenDesktop 3.0 CCU-Lizenzen müssen bei einem Upgrade entsprechend in User- oder Device Lizenzen umgewandelt werden. Für Anwender von XenApp oder Presentation Server in den Editionen Enterprise oder Platinum stellt zudem das sogenannte "XenDesktop Trade-Up"-Pro-

gramm eine Option dar. Im Rahmen dieses Programms können noch bis zum 30.06.2010 bestehende CCU-Lizenzen im Verhältnis 1-zu-2 in XenDesktop 4.0 User- oder Device-Lizenzen umgewandelt werden. Nicht zu vergessen ist, dass in jedem Fall pro Gerät oder Benutzer zusätzlich eine Microsoft VECD-Lizenz nötig ist.

Installation und Betrieb

Für unseren Test nutzten wir unsere Umgebung, die wir im Rahmen des Provisioning Server Workshops (siehe Seite 45) bereits aufgebaut hatten. Damit konnten wir auf bereits bestehende Komponenten, wie Active Directory-Domäne, SQL Server, XenServer und Provisioning-Infrastruktur sowie das Citrix Licensing, zurückgreifen.

Wir erzeugten eine neue virtuelle Maschine unter Windows Server 2003 R2 und starteten die Installation des DDC, die weitestgehend analog zur Vorgängerversion XenDesktop 3.0 ablief. Neben dem eigentlichen DDC wurden in der Komponentenauswahl die Management-Konsolen und der Lizenzserver angeboten. Letzteren wählten wir ab. Eine Auswahl und Konfiguration von weiteren Teilkomponenten, wie etwa von XenApp bekannt, ist nicht erforderlich. Dies vereinfacht den Setup-Prozess, bedeutet im Umkehrschluss aber auch, dass das Citrix Web Interface auf einem DDC in jedem Fall mit installiert wird. Entsprechende Abhängigkeiten, wie IIS inklusive ASP.NET, .NET Framework 3.5 SP1, Visual J# 2.0 Redistributable Package und die SUN Java Runtime, werden im Laufe des Setups automatisch nachinstalliert. Der Citrix XML-Dienst teilt sich den TCP-Port 80 mit dem IIS.

Wir erzeugten eine neue Farm mit dem Namen "XenDesktop-Farm" unter Verwendung der Enterprise Edition. Anschließend wählten wir die Option, die bestehenden Datenbank- und Lizenz-Server zu verwenden. Aus dem Setup heraus startete dabei der ODBC-Dialog von Windows, wo wir eine Verbindung zu unserem SQL-Server definierten. Dort hatten wir zuvor bereits eine leere Datenbank mit dem Na-

men "XenDesktop" und einem gleichnamigen Benutzer mit DB-Owner-Rechten angelegt. Die Anmeldeinformationen dieses Benutzers konnten wir im nächsten Dialogschritt hinterlegen. Nach Eingabe unseres Lizenzservers blieb abschließend, eine Organisationseinheit im AD zu wählen. Diese siedelten wir innerhalb unserer Provisioning Server-Infrastruktur an.

Konfiguration der VDI-Infrastruktur

Bevor wir die Konfiguration der Farm fortsetzten, nahmen wir nun zunächst zwei virtuelle Maschinen unter Windows 7 in Betrieb und installierten darauf jeweils den "Virtual Desktop Agent (VDA)" aus dem aktuellen XenDesktop-Release. Dieser unterstützt nun auch 64-Bit Desktop-VMs. Standardmäßig belegte der VDA den TCP-Port 8080 zur Kommunikation mit dem Desktop Delivery Controller und konfigurierte die Windows Firewall entsprechend. Anschließend war die XenDesktop-Farm auszuwählen. Zurück auf dem DDC starteten wir die Delivery Services Console und riefen aus dem Kontextmenü des Ordners "Citrix Resources \ Desktop Delivery Controller \ {Farmname} \ Desktop Groups" die Aktion "Create desktop group" auf. Für eine Desktop-Gruppe stehen die Modi "Pooled" oder "Assigned" zur Wahl. In letzterem Fall wird eine 1:1-Relation zwischen einer VM und einem Benutzer hergestellt. Wir konfigurierten stattdessen einen Pool, in dem die VMs nach Sitzungsende wieder für andere Benutzer verfügbar werden. Neu ist in diesem Dialog die Checkbox "Use Desktop Group for VM Hosted Apps". Es handelt sich dabei um eine neue Funktion zur Integration von

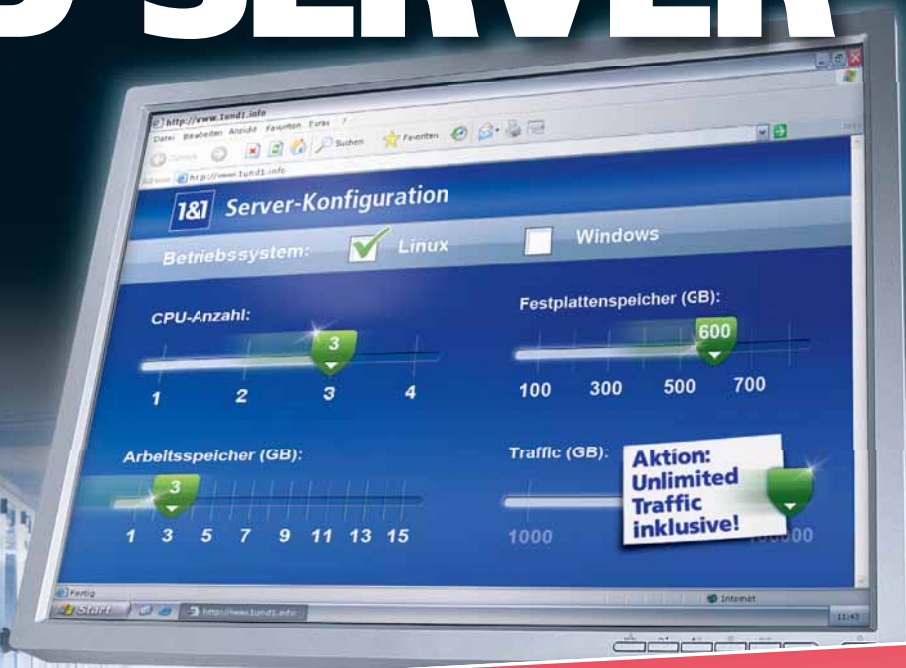
Wer nicht auf bestehende Komponenten aufbauen kann, findet innerhalb der Online-Dokumentation "Citrix eDocs" [3] unter "XenDesktop / XenDesktop 4 / Evaluating XenDesktop" hilfreiche Schritt-für-Schritt-Leitfäden, um mit einer eigenen Testumgebung zu starten. Der Integration von XenDesktop in eine bestehende XenApp Terminalserver-Farm widmet sich ein separates Whitepaper [4].

Tip



Günstig einsteigen – mehr Server-Leistung bei Bedarf:

DYNAMIC CLOUD SERVER



**6 MONATE 50% RABATT
NUR BIS 30.04.2010!***

Dynamic Cloud Server – Preis-/Leistungsbeispiel Basis-Paket:

- ✓ **1 Core von Quad-Core AMD Opteron™ Prozessor 2352 (auf 4 Cores erweiterbar)**
- ✓ **1 GB RAM**
- ✓ **100 GB Webspace**
- ✓ **Unlimited Traffic**

Weitere attraktive Server-Angebote finden Sie unter www.1und1.info

~~39,99~~
19,99 €/Monat*

Für 6 Monate, danach 39,99 €/Monat.*

* z. B.: 1&1 Dynamic-Cloud Server Basis-Paket jetzt zum Aktionspreis 6 Monate für 19,99 €/Monat, danach für 39,99 €/Monat. Einrichtungsgebühr 39,- € bei 12 Monaten Mindestvertragslaufzeit. Preise inkl. MwSt.

 **0180 5 / 001 535** 14 ct/Min. dt. Festnetz, Mobilfunk höchstens 42 ct/Min.

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

www.1und1.info



1&1



XenDesktop in XenApp, um einzelne Applikationen statt direkt vom Terminalserver von einem Desktop-Betriebssystem zu veröffentlichen. Dies zielt auf Applikationen ab, die inkompatibel oder zu ressourcenintensiv für den Terminalserver-Betrieb sind.

Im weiteren Verlauf wählten wir unsere Virtualisierungsinfrastruktur, nahmen die beiden Windows 7-VMs in die Gruppe auf und berechtigten die Gruppe der Domänen-Benutzer, darauf zuzugreifen. Verbindungen von Clients erfolgen auch unter XenDesktop 4.0 ausschließlich über das Citrix-Webinterface (WI). Dieses liefert wahlweise eine "XenApp Web-Site", an der sich Anwender interaktiv anmelden können, oder eine "XenApp Services-Site", welche die Konfigurationsdatei *config.xml* für das Citrix Online-Plug-In bereithält. Die aktuelle Version des WI im Lieferumfang von XenDesktop bringt eine neue, separate Konsole namens Citrix Webinterface-Verwaltung mit, anstatt sich in die Delivery Services Console zu integrieren. Im Webinterface-Management fanden wir sowohl eine "XenApp Web-Site" als auch eine "XenApp Services-Site" fertig konfiguriert vor. Somit konnten wir uns ohne weiteres Zutun direkt von einem unserer Client-Rechner mit installiertem Citrix Online Plug-In 11.2 an der Webseite <http://{{ddc-name}}/Citrix/DesktopWeb> anmelden und Verbindung zu einem unserer virtuellen Windows 7 Desktops aufnehmen.

Sicherlich ist das manuelle Verwalten der virtuellen Desktops bei größeren Zahlen zu versorgender Clients nicht der Weisheit letzter Schluss. Entsprechend bietet XenDesktop 4.0 die Möglichkeit zur nahtlosen Integration mit dem Citrix Provisioning Server. Natürlich lässt sich auch eine Desktop-VM mit installiertem Virtual Desktop Agent via Target Device in eine vDisk kopieren. Neben einer leeren vDisk wird vorbereitend in der Virtualisierungsinfrastruktur ein Template für weitere VMs benötigt. Da daraus erzeugte Maschinen vom Provisioning Server versorgt werden, genügt als Vorlage eine VM ohne eigene Festplatte, die per Netzwerk bootet.



Bild 2: Die Konfiguration des Plug-Ins wird als Flyout am oberen Bildschirmrand eingeblendet

Zur weiteren Vereinfachung findet sich im Umfang von XenDesktop der "XenDesktop Setup Wizard", der zusätzlich auf einem Provisioning Server zu installieren ist. Dieser Assistent verbindet sich mit der Virtualisierungsinfrastruktur, der Desktop-Farm sowie dem AD und erfragt aus welchem Template und welcher vDisk wie viele Desktops erzeugt werden sollen. Dabei werden automatisch entsprechende VMs mit passenden AD-Accounts in der gewünschten OU erstellt. Bei Bedarf erzeugt der Wizard auch gleich eine neue Desktop-Gruppe innerhalb der Farm. Werden darüber hinaus zusätzliche VMs benötigt, genügt es, den Wizard erneut zu durchlaufen, um weitere Desktops zu generieren.

Mehr Komfort für die Anwender

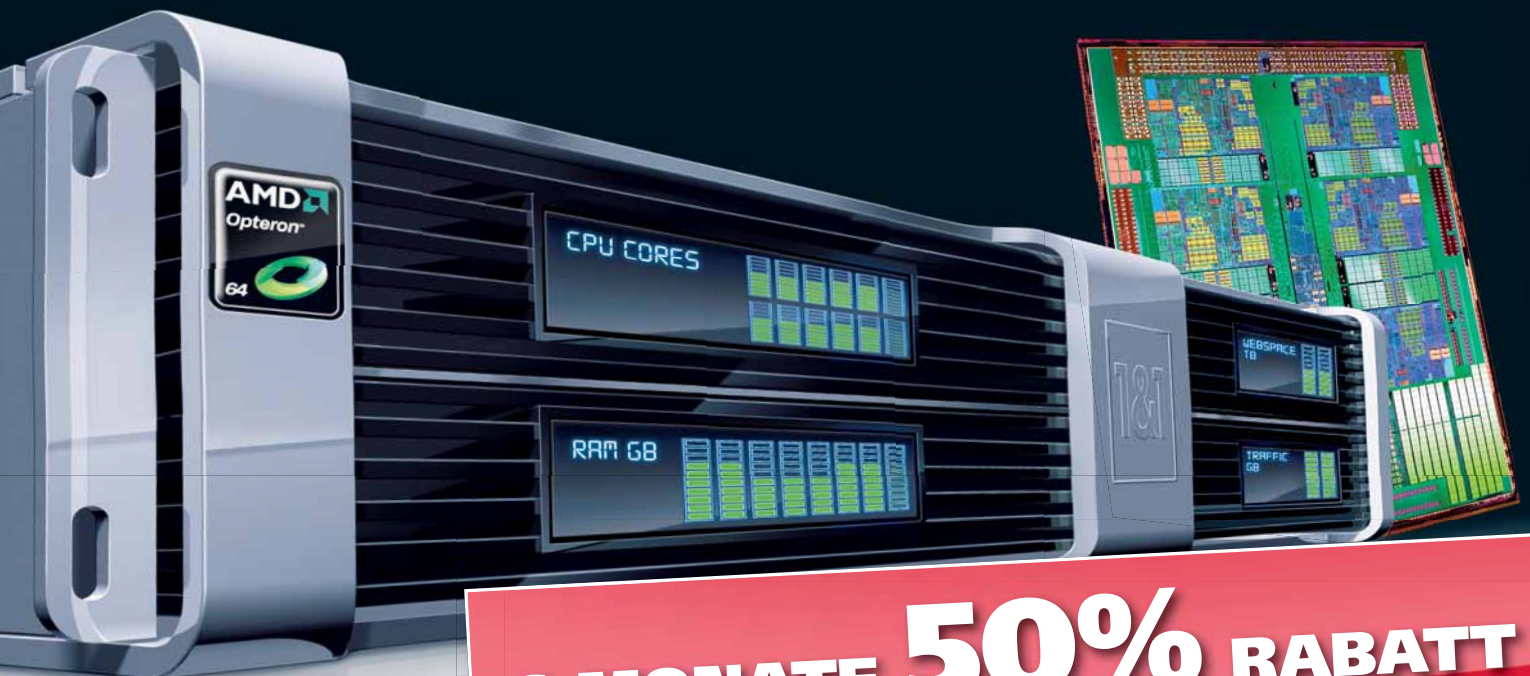
In den Bereichen Architektur und Management beschränken sich die Neuerungen der Version auf Modellpflege, was die Verwaltung vereinfacht und dennoch Administratoren des Vorgängers kein generelles Umdenken abverlangt. Die signifikanten Änderungen wirken weitestgehend im Verborgenen und betreffen Client-Unterstützung sowie User Experience. So hat das Remote Protokoll ICA deutliche Verbesserungen erfahren, die unter dem neuen Label "High Definition User Experience (HDX)" firmieren. Dies betrifft insbesondere den optimierten Zugriff auf grafiklastige Anwendungen und Multimedia.

Um insbesondere die Wiedergabe kontinuierlicher Medien zu beschleunigen, wird basierend auf verfügbarer Bandbreite, Rechenleistung des Clients und verfügbaren Codecs ermittelt, ob Inhalte Server- oder Client-seitig gerendert werden. Soll also beispielsweise in einer Remote-Sitzung ein DivX-Video in einem Fenster abgespielt werden, so wird die Grafikausgabe des umgebenden Desktops und aller Fenster weiter auf der entfernten Maschine erzeugt und als Bitmap an den Client übertragen. Das Video selbst wird dagegen zunächst direkt an den Client gestreamt, dort mit dem lokalen Codec dekodiert und nahtlos in die Bildschirmausgabe des Remote-Desktops integriert. Diese Technik namens HDX MediaStream unterstützt zahlreiche Audio- und Video-Formate, darunter AVI, MP4, DIVX, OGG, WMV, WAV, MP3, AAC, WMA und auch Flash.

Wir konnten uns von der Funktionalität in unserem Testaufbau an einem Windows-Client überzeugen, indem wir zunächst in einer Desktop-Sitzung einige AVI- und MP3-Dateien mit dem Windows Media Player abspielten. Weiterhin riefen wir einige Flash-lastige Webseiten auf. Dabei fragte der Client bei der ersten Verwendung an, ob HDX MediaStream für Flash aktiviert werden soll. Diese Einstellung lässt sich nachträglich auch über die Kopfleiste des Citrix Desktop Viewer konfigurieren und pauschal ein- oder ausschalten. Alle

1&1 Innovation – für maximale Server-Leistung:

HEXA-CORE TECHNOLOGIE



6 MONATE **50% RABATT**
NUR BIS 30.04.2010!*

1&1 Dedicated Hexa-Core Server XXL mit 12 Prozessorkernen:

- ✓ **2x Six-Core AMD Opteron™ Prozessor 2423HE**
- ✓ **Bis zu 32 GB Arbeitsspeicher – das gab's noch nie!**
- ✓ **Bis zu 2 TB nutzbarer Speicherplatz mit RAID 5!**
- ✓ **Stromsparend: High Efficiency!**

Weitere attraktive Server-Angebote finden Sie unter www.1und1.info


* z. B.: 1&1 Hexa-Core XXL jetzt 6 Monate für 149,99 €/Monat, danach für 299,99 €/Monat. Einrichtungsgebühr 99,- € bei 12 Monaten Mindestvertragslaufzeit. Preise inkl. MwSt.

~~299,99~~ €/Monat*

149,99 €/Monat*

Für 6 Monate, danach 299,99 €/Monat.*

 **0180 5 / 001 535** 14 ct/Min. dt. Festnetz, Festnetz, Mobilfunk höchstens 42 ct/Min.

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

www.1und1.info



1&1



von uns getesteten Inhalte einschließlich YouTube-Videos in HD-Auflösung ließen sich ohne Komplikationen wiedergeben. Dabei überzeugte der Client zum einen mit Audio-Wiedergabe in CD-Qualität, zum anderen mit ruckelfreier und schar-


fer Bildwiedergabe. Stockende Videos und verrauschte Tonspuren gehören mit HDX offensichtlich der Vergangenheit an.

Ein ähnliches Bild bot sich an einem Linux Thin Client vom Typ IGEL UD3-720 mit HDX-Unterstützung. Auch hier vermittelte die Remote-Sitzung weitestgehend das Gefühl, lokal an einem Windows 7-Desktop zu arbeiten. Einziger Minuspunkt ist dabei allerdings, dass der Citrix-Client für Linux zum Testzeitpunkt noch nicht die Optimierung von in Webseiten eingebetteten Flash-Inhalten unterstützt. Während in einem separaten Player aufgerufene Multimedia-Inhalte von der Beschleunigung profitieren, bereiten Flash-basierende Webseiten, insbesondere eingebettete Videos à la YouTube, also noch Probleme. Abhilfe schafft der neue Linux-Client 11.100, der im Februar erschienen ist und nun von den Thin Client-Herstellern in die Firmware integriert werden kann.

Weitere Verbesserungen betreffen den Multi-Monitor-Betrieb, der nicht mehr auf acht Monitore beschränkt ist. Der Client reicht dabei die tatsächliche Monitor-Anordnung eines Windows-Clients an eine Desktop-VM durch, welche die Ausgabe über native Windows-Kommandos ansteuern kann. Linux- und Mac-Clients setzen diese erweiterten Funktionen allerdings noch nicht um. Gleiches gilt für die Fortschritte beim USB-Support, die isochrone Verbindungen ermöglichen. Damit lassen sich nun im LAN Geräte wie Webcams, Headsets oder Scanner transparent in Remote-Sitzungen nutzen.

Fazit

Der Analyst Brian Madden entwickelte bereits 2008 die These, dass die erforderlichen Technologien zur Desktop-Virtualisierung bis Mitte 2010 soweit fortgeschritten sein werden, dass auch in komplexen Szenarien sämtliche Desktops im Unternehmensumfeld virtuell zu hosten sind [5]. Mit Blick auf die aktuellen Funktionen des XenDesktop könnte sich dies bewahrheiten. So ist es in Verbindung mit dem Provisioning Server bereits jetzt

möglich, mit einem Image viele Benutzer gleichzeitig zu versorgen. Durch die Integration mit XenApp und dem Anwendungsstreaming lassen sich die allermeisten Applikationen virtuell bereitstellen. Und mit den HDX-Erweiterungen lässt das ICA-Protokoll kaum mehr einen Unterschied zu einer lokalen Session erkennen. Lediglich der Umstand, dass derzeit die Aero-Oberfläche von Windows 7 und Vista in Remote-Sitzungen noch nicht nutzbar ist und Flash-Webseiten im Linux-Client nicht beschleunigt werden, verhindert hier die volle Punktzahl. Zur Bereitstellung von Anwendungen in allen Lebenslagen fehlt letztlich nur noch der Client-Hypervisor XenClient. Es steht zu vermuten, dass diese Lücke spätestens zur nächsten Citrix Synergy-Konferenz Anfang Mai geschlossen wird. (dr) 

Der Autor dieses Artikels, Dipl.-Inform. (FH) Christian Knermann, ist stellv. Leiter des IT-Managements am Fraunhofer Institut für Umwelt-, Sicherheits- und Energietechnik UMSICHT in Oberhausen. Zugleich leitet er das Projekt "Competence Center Application Service Providing" der Fraunhofer Gesellschaft.

Produkt

Infrastrukturlösung zur Virtualisierung von Desktops und Anwendungen.

Hersteller

Citrix Systems
www.citrix.de

Preis

Express Edition: frei für maximal 10 Concurrent User
VDI Edition pro User/Device: 95 US-Dollar
VDI Edition pro Concurrent User: 195 US-Dollar
Enterprise Edition pro User/Device: 225 US-Dollar
Platinum Edition pro User/Device: 350 US-Dollar
Alle Preise beinhalten ein Jahr Subscription Advantage, also die Möglichkeit, jeweils die neueste Version der Software einzusetzen.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Installation und Inbetriebnahme	8
Funktionsumfang	9
USB-Unterstützung	8
Grafik-Performance	9
Linux-Client-Support	7

Dieses Produkt eignet sich

optimal für Umgebungen, in denen standardisierte Windows-Arbeitsplätze zentral bereitgestellt werden sollen.

gut für mittlere und größere Unternehmen, insbesondere auch zur Anbindung von Außenstellen und Heimarbeitsplätzen.

bis zur Marktreife von XenClient **weniger** für Unternehmen mit überwiegend oder ausschließlich mobilen Benutzern, die noch dazu meistens offline arbeiten.

Citrix XenDesktop 4

- [1] "Virtuelle Arbeitsplätze - Im Test: Citrix XenDesktop 3.0" in IT-Administrator 9/2009, S. 28-34
- [2] Citrix-Webinar zur Architektur <https://www2.gotomeeting.com/register/443735643/> und http://www.citrix.de/events/webinararchiv/webinarslides/Webinar_XenDesktop_4.pdf
- [3] Online-Dokumentation "Citrix eDocs" <http://support.citrix.com/product/xd/v4.0/#tab-doc>
- [4] Whitepaper zur Integration von XenDesktop in eine bestehende XenApp-Terminalserver-Farm <http://support.citrix.com/article/CTX123614/>
- [5] Analyst zu den Virtualisierungsmöglichkeiten www.brianmadden.com/blogs/brianmadden/archive/2008/06/23/prediction-vdi-will-be-ready-for-wholesale-desktop-replacement-in-2010-here-s-how-we-ll-solve-the-problems-to-get-there.aspx

Links

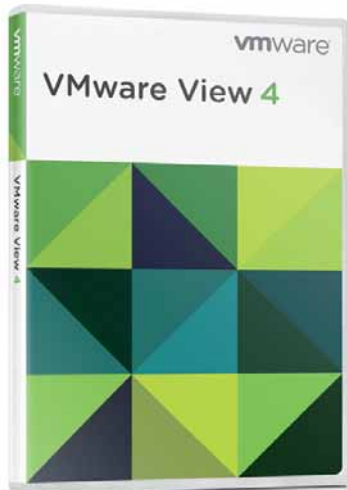




Im Test: VMware View 4

Fernsicht für Clients

von Dennis Zimmer



Auch im Desktop-Umfeld kommt die Virtualisierungs-Lawine nicht zum Halt: Mehr und mehr Unternehmen stellen dem Endanwender mittlerweile eine virtuelle Maschine als Desktop von zentraler Stelle aus zur Verfügung. Egal ob alter PC oder modernster Thin Client – die Oberfläche sieht immer gleich aus und wird von einem einzelnen oder einem Pool von Servern bereitgestellt. VMware schickt im Bereich Desktop-Virtualisierung VMware View ins Rennen. IT-Administrator hat sich angesehen, wie sich Version 4 im Praxis-Einsatz schlägt.

Das aktuelle Release von VMware View bringt neben der Unterstützung von vSphere vor allem eine verbesserte Leistungsfähigkeit für Multimedia-Anwendungen im Client mit. Zudem stellt der Hersteller die Zusatzsoftware zur Applikationsvirtualisierung, ThinApp, zur zentralen Verteilung von Applikationen bereit. Da das Microsoft-Protokoll RDP deutliche Limitierungen aufweist und die Konkurrenz mit dem ICA-Protokoll aufwartet, hat sich VMware mit dem Remote-Zugriff-Spezialisten Teradici zusammengetan und in einer Gemeinschaftsarbeit das Protokoll PCoIP (PC over IP) weiterentwickelt und in View 4 integriert.

Vier zentrale Komponenten

VMware View besteht aus vier Komponenten: View Server, View Agent, View Composer und View Client. Admins sollten den View Agent idealerweise bereits im Basis-Template zur Verteilung der VMs installieren, er lässt sich aber auch im Nachhinein manuell oder per Softwareverteilung in der virtuellen Maschine verankern. Der View Client stellt das Endgerät zum View Server dar. Er kann anstatt der Browservariante, die über ein ActiveX-Plug-In realisiert wird, zum Zugriff auf den View Server genutzt werden. Dabei ist

es möglich, einem Benutzer ein oder mehrere Desktops zur Verfügung zu stellen. Eine View Client-Erweiterung, die einen Offline-Desktop unterstützt, ist ebenfalls mit an Bord, befindet sich derzeit aber noch in einer experimentellen Phase.

Der View Composer schließlich ist eine Komponente, die direkt auf dem VMware vCenter Server arbeitet und unter anderem die Funktion "Linked Clones" anbietet. Dabei dient eine virtuelle Maschine (VM) als Master, auf deren Basis sich Dutzende weitere Klone erstellen lassen. Dabei wird nur so viel Plattenplatz verbraucht, wie sich die Klone gegenüber dem Master unterscheiden. Dies hat zum Ziel, Speicherplatz im zentralen Storage einzusparen. Diese Komponente ist nicht zwingend für die Nutzung von View notwendig. Wer trotzdem auf den Composer zurückgreifen will, muss wissen, dass dieser auch in der aktuellen Version 4 nicht mit 64-Bit-Systemen funktioniert. Kommt ein vCenter Server auf 64-Bit-Windows-Basis zum Einsatz, besteht derzeit keine Chance, den Composer zu nutzen. Mehr Informationen dazu bietet die Hardware-Kompatibilitäts-Liste [1] von VMware.

Den eigentlichen Kern des Produkts stellt allerdings der View Server dar, über den

Administratoren die virtuellen Desktops erstellen, verwalten und veröffentlichen. Der Server kann dabei mehrere Rollen annehmen: Connection Server, Replica Server oder Security Server. Der Connection Server ist der eigentliche VDI-Server und bildet die Schnittstelle zwischen Client-Agenten und VDI-VM. Soll die virtuelle Desktop Infrastruktur ausfallsicher betrieben werden, ist die Installation eines oder mehrerer Replica Server möglich, was neben der Ausfallsicherung zudem eine Lastverteilung zum Vorteil hat. Die replizierte Maschine ist im Endeffekt ebenfalls ein Connection Server, der allerdings seine Konfiguration vom ersten Connection Server erhält.

Schließlich ist der Security Server zu nennen, der normalerweise in der DMZ residiert, um externe Mitarbeiter mit einem Desktopzugriff zu versorgen. Dieser Sicherheits-Server muss im Gegensatz zum View Connection/Replica Server nicht zwingend Mitglied einer Active Directory-Domäne sein. Generell ist aber zu bedenken, dass nur das AD für die Authentifizierung in Frage kommt. Beim Betrieb des Security Servers in der DMZ müssen die vom Dienst benötigten Ports in der Firewall geöffnet werden, um die Verbindung zu ermöglichen. Leider ist der Se-



Bild 1: Während der Installationsroutine erfolgt die Auswahl der Serverrolle

curity Server in Version 4 nicht mit dem neuen PCoIP-Protokoll nutzbar.

Beim Installationsdialog des View Servers ist die wichtigste Entscheidung während der Installation zu treffen – welche Rolle der Server annehmen soll: View Connection Server, View Replica oder View Security Server. Die Installation läuft bei jeder der wählbaren Rollen äußerst intuitiv und einfach ab. View installiert neben der Webserver-Komponente zusätzlich eine ADAM-Datenbank, die eine lokale Active Directory-Instanz darstellt.

Unhandliche Zugriffsberechtigungen

Nach der Installation findet die eigentliche Administration komplett über die Web-Oberfläche statt, die sich über die IP-Adresse beziehungsweise den DNS-Namen des Servers ansteuern lässt. Hierbei ist zu beachten, dass View die Standardports 80 und 443 nutzt, die auf dem Installations-System offen sein müssen. Da View zur Authentifizierung zwingend einen AD-Zugriff voraussetzt, muss das System Mitglied der Domäne sein. Die Anmeldung als Benutzer oder Administrator findet daher mit den Windows-Benutzern beziehungsweise -Administratoren statt.

Leider unterscheidet View bezüglich der Zugriffsberechtigung nur zwischen Administratoren und Benutzern. Es sind keine

weiteren Einschränkungen oder Rollen verfügbar, was den Einsatz in sehr großen Umgebungen mit vielen Abteilungen und Zuständigkeiten erschwert. Während der Administrator lediglich für die Verwaltung des Servers und die Konfiguration der zu veröffentlichen Desktops berechtigt ist, kann der Benutzer mittels RDP- oder PCoIP-

Protokoll auf den ihm zugewiesenen Desktop zugreifen und gegebenenfalls den eigenen Arbeitsplatz zurücksetzen.

Wer zusätzlich die Linked Clones-Funktion mittels VMware Composer nutzen will, muss diesen auf dem vCenter Server installieren. In der Konfiguration von View wird im Administrator-Modus die Composer-Unterstützung automatisch erkannt.

Konfiguration auch als Proxy-Umgebung

Die wichtigsten Schritte im View Administrator sind die Eingabe der Lizenzschlüssel, die Verbindung zu den vCenter- und Security-Servern und weiteren Terminal-Servern, die Benutzerverwaltung und das Anlegen und Konfiguration der Virtual Desktop Pools. Außerdem bittet der View Connection Server um die Mitteilung, ob er ein Proxy- oder Non-Proxy-Server ist. Wird nicht der direkte Weg vom Client zum Agent über das LAN gewählt (Authentifizierung über View Server, RDP-Verbindung vom Client direkt zum VDI-Desktop), sondern soll der View Server als Proxy agieren (alle Kommunikation läuft durch den View Server, inklusive der Authentifizierung und dem Client-Zugriff), bedeutet dies eine Proxy-Umgebung.

Der große Unterschied hierbei liegt hauptsächlich in der Tatsache, wie viele

Netzwerkverbindungen zum View Server dauerhaft gehalten werden. Daher muss ein View Server in einer Proxy-Umgebung über mehr Ressourcen (zum Beispiel zwei CPU-Kerne und 4 GByte RAM für bis zu 800 Desktops) verfügen als ein Non-Proxy-View Server, der bei gleicher Hardware 1.500 bis 1.700 Desktops schafft.

Der Proxy-Modus bietet dagegen Vorzüge im Bereich Sicherheit (Firewall-Konfiguration nur zum View Connection Server statt zu allen Desktops) und ist daher die Standardvariante. Besteht die Möglichkeit, eine RSA SecurID zu nutzen, lässt sich diese zur Authentifizierung ebenfalls mit View einrichten.

Unterschiede bei der Desktop-Zuweisung

Nach der Konfiguration des View Servers kann der Nutzer vier Arten von View Desktops anlegen: Der Modus "Individual" beschreibt eine einzigartige, vorinstallierte VM, während beim "Persistent Desktop Pool" jedem authentifizierten Benutzer ein Pool von Desktops zur Verfügung steht. Nach der ersten Anmeldung findet jedoch eine 1:1-Zuordnung von Client zu Desktop statt, welche in Zukunft bestehen bleibt. Beim "Non-Persistent Desktop Pool" entfällt diese Bindung, alle Desktops werden stets aufs Neue beliebig zugeordnet. Zu guter Letzt besteht außerdem die Möglichkeit, eine Verbindung zu einem bestehenden Microsoft Terminal Server herzustellen.

Abhängig von dieser Auswahl erfolgt danach eine Analyse der VMware-Infrastruktur und die Bearbeitung der Clients kann beginnen. Dies bedeutet in der Praxis die Auswahl von Resource-Pools, Templates und Customization Specification zur Anpassung des Clients während der Erstellung. Hier ist der Administrator allein für das Erstellen der Templates verantwortlich. Diese sollten in ihrer Installation neben sämtlicher benötigter Software zusätzlich natürlich auch noch den View Agenten aufweisen.

Um den Anwendern den Zugriff zu gestatten, muss der Administrator den Pool aktivieren und per AD-Berechtigung den entsprechenden Personengruppen zuordnen. Nach der Aktivierung findet je nach Konfiguration automatisch eine direkte Provisionierung der angegebenen Anzahl von Desktops statt. Es ist außerdem möglich, Provisionierungs-Regeln anzugeben, welche die Anzahl der Desktops im Pool bei Bedarf automatisch erhöhen. Um das Management der Clients möglichst einfach zu halten, sollten Administratoren die Einstellungen über Gruppenrichtlinien pflegen, die von VMware mitgeliefert werden und sich auf den Domänencontroller importieren lassen.

Mehr Multimedia und ThinPrint-Integration

VMware View 4 bringt weiterhin wesentliche Verbesserungen im Grafikbereich mit. Wem die Grafikfunktionalität des RDP-Protokolls bisher nicht ausreichte, der kann im aktuellen Release auf das bereits erwähnte PCoIP-Protokoll zurückgreifen, das jetzt die Unterstützung des Desktop-Agenten genießt. PCoIP bringt wesentliche Vorteile bei WAN-Zugriffen und bei der Nutzung von grafikintensiven Anwendungen wie Multimedia-Inhalten. Die Beschleunigung im Vergleich zu einer RDP-Sitzung ist markant. Außerdem spricht das Protokoll nun bis zu vier Monitore an. Allerdings traten während des Tests Probleme bei der automatischen Anpassung der Auflösung der View Client-Ansicht

auf, was beim Umschalten zwischen Vollbild und Fenstermodus zu einem schwarzen Rand führte. Eine Lösung für diese Problematik ist jedoch bereits bekannt und unter [2] im Web zu finden.

Zum effizienteren Druckverhalten hat VMware die Basisfunktion von ThinPrint als OEM lizenziert und direkt in View integriert. Wer Geräte über USB anschließen möchte, der profitiert von der mitgelieferten VMware View USB Redirection. Diese Funktionalität ermöglicht den unkomplizierten Anschluss von USB-Druckern, -Sticks oder -Headsets.

Offline-Desktop und Software-Virtualisierung

VMware View erlaubt es, eine virtuelle Maschine lokal auf einen Rechner oder ein Notebook herunterzuladen und nennt diese experimentelle Funktion "Offline Desktop". Dazu bedarf es eines speziellen VMware View Clients, der es erlaubt, die gesamte virtuelle Maschine lokal abzulegen und zu nutzen. Dieser Vorgang dauert erstmalig natürlich sehr lange und sollte daher mit LAN-Verbindung geschehen. Die folgenden Aktualisierungen betreffen nur noch die Änderungen (Deltas), was über WAN meist problemlos möglich ist. Der Client führt die VM dann lokal mit dem VMware Player aus. Hier wäre eine Integration mit VMware ACE (Assured Computer Environment) sinnvoll, um die Lebenszeit der VMs zu beschränken und die Systeme verschlüsseln zu können.



Bild 2: Über den VMware View Administrator erfolgt das Management der VDI-Umgebung

KAPAZITÄTSMANAGEMENT ZUR BEWERTUNG DER GESAMTBETRIEBSKOSTEN – GRUNDLAGE DER INVESTMENTSTRATEGIE FÜR IHR RECHENZENTRUM

ZÜRICH - 27 May 2010 - WTC Zurich

Die DatacenterDynamics Konferenz und Expo geht die Herausforderungen an, die sich Besitzer und Betreiber veralteter Gebäudestrukturen stellen, wenn die Nachrüstung oder ein Neubau anstehen. Was ist zu beachten um der komplexen Kombination aus exponentiellem Datenzuwachs, technischen Fortschritten, Energieeffizienz, Ausfallsicherheit und Sicherheit gerecht zu werden?

- **Sanierung** – Innerbetrieblicher Strukturwandel der bestehenden Ausstattung um den Anforderungen hinsichtlich Hochspannung, höherer Dichte und deren Nebenwirkungen im Datacenter-Design gerecht zu werden
- Bewertung der Konvergenz zwischen **physikalischen und logischen Management Tools**
- Gewinnen Sie einen Einblick in die Beweggründe des **Outsourcings** – Collocation, Managed Services oder Erhaltung der eigenen Infrastruktur und des Betriebes im Rechenzentrum
- **Freie Kühlung** – Die Wahl der geeigneten technischen Lösung, passend zu Ihrer Ausstattung

Zu den diesjährigen Referenten zählen:



Don Beaty
Präsident, DLB Associates
(und Internationaler Vorsitzender,
ASHRAE TC9.9)



Mark Eichenberger
Head Data Center Strategy, Technology
& Product Management, UBS



Adrian Altenburger
Partner und HLK Ingenieur
Amstein & Walther & ASHRAE Mitglied
TC 9.9 Mission Critical Facilities



Friedrich Bürki
Geschäftsführer
FRB DC Consulting

Partner



Platin Sponsor



Melden Sie sich jetzt an!

Zitieren Sie DCDZUR1 und sichern sich
10% Rabatt und kontaktieren Sie

Bettina Bermuth unter +44 (0) 20 7426 4814 oder per
Email: bettina@datacenterdynamics.com
Web: www.datacenterdynamics.com/zurich



DatacenterDynamics

ZÜRICH - MAY 27 2010





Wer die Premier Edition von View lizenziert hat, kann die Applikations-Virtualisierung durch ThinApp nutzen. Sie ermöglicht, Anwendungen zentral zu streamen, statt diese auf jeder VM installieren zu müssen. Dadurch lassen sich auch mehrere Versionen von Anwendungen gleichzeitig nutzen, ohne die üblichen DLL-Inkompatibilitäten bedenken zu müssen.

Administratoren können ThinApp recht komfortabel nutzen, indem sie ein Vor-

her/Nachher-Abbild einer "frischen" VM anfertigen. Die durch die Installation der Software erfolgten Änderungen im Betriebssystem lassen sich noch nachverfolgen und zur Weiterverteilung paketieren. Die Kombination aus VMware View zur Bereitstellung der Desktops und ThinApp zur Bereitstellung der Applikationen kann bei richtiger Anwendung deutliche Administrationsvorteile bringen, da die Desktops "stateless" sind, also über keine eigene Identität verfügen und sich somit beliebig austauschen lassen.

Fazit

Die Desktop-Virtualisierung steckt immer noch im Anfangsstadium ihrer Möglichkeiten. Allerdings reichen die Funktionen und Möglichkeiten von VMware View 4 vor allem für Durchschnittsumgebungen mit mehreren hundert bis wenigen tausend VMs zumeist aus und es sind nur wenige Anpassungen von Seiten des Administrators durchzuführen. Die Anpassungen beziehen sich zumeist auf die Verwaltung der VMware-Infrastruktur mit der PowerCLI oder eigenen Softwareprodukten und die Integration ins Active Directory, um den Anwendern den Zugriff automatisch zu ermöglichen.

Was fehlt sind integrierte Funktionen, um die Ist-Aufnahme bestehender physikalischer Infrastrukturen schnell und aussagekräftig durchzuführen, um die Virtualisierung möglichst gezielt anzugehen. Viele Möglichkeiten zur Provisionierung kommen von den Storage-Herstellern selbst. NetApp und EMC sind hier die beiden Unternehmen, welche die meisten VDI-Funktionen anbieten.

Insgesamt ist VMware View 4 für die meisten VDI-Umgebungen eine sehr gute Wahl und glänzt durch die einfache Installation und Bedienung sowie die stabile Basis in Form von vSphere 4. Weiterhin haben bereits sehr viele Dritthersteller Zusatzsoftware und Dokumentationen zum Thema View veröffentlicht. Das Produkt ist somit – das passende Einsatzszenario vorausgesetzt – rundum empfehlenswert. (In)

VMware View bietet bei der Erstellung die Möglichkeit, virtuelle Maschinen über mehrere Datastores zu verteilen. Dies ist bei einem SAN dringend zu empfehlen, da es bei einer erhöhten Anzahl von VMs auf einer LUN zu einer markanten Steigerung der SCSI-Reservierungen kommt und dies deutlich die Performance des Storage-Systems beeinträchtigen kann.

NFS-Speichersysteme sind von den SCSI-Reservierungen nicht betroffen und daher vor allem bei sehr großen View Umgebungen von Vorteil. IT-Verantwortliche sollten sich daher vorab mit den Best Practices des Storage-Herstellers im VDI-Umfeld auseinander setzen, da sich diese Anforderungen deutlich von den Anforderungen der Servervirtualisierung unterscheiden. An dieser Stelle variieren die Kompetenzen der Storage-Hersteller deutlich. NetApp beispielsweise liefert mit seiner Hardware ein Rapid Cloning Tool, das sich als Plug-In ins vCenter integrieren lässt, um per Fastclone Dutzende oder Hunderte Kopien eines Desktops in wenigen Minuten zu erstellen.

Außerdem sollte unbedingt das Lastverhalten der einzelnen VMs einer genauen Prüfung unterzogen werden, insbesondere bei Betriebssystemänderungen. Windows Vista etwa erzeugt ein Vielfaches an I/O-Last auf dem Storage-System als XP, was bei der Planung ein entscheidender Faktor ist. Windows 7 liegt von der I/O-Last ungefähr zwischen XP und Vista und ist somit besser zur Virtualisierung geeignet. Eine VDI-Planung steht daher immer in Abhängigkeit vom Gastbetriebssystem. Eine Veränderung macht in den meisten Fällen auch eine Anpassung der Ressourcen nötig.

Ein weiterer Übeltäter für Storage-Systeme sind Antivirenprodukte, welche mit Signatur-Updates oder gleichzeitigen Scanvorgängen eine enorme Last erzeugen können. In diesem Fall ist unbedingt darauf zu achten, die Updates und Scans zu unterschiedlichen Zeitpunkten zu starten, da 500 gleichzeitig nach Viren suchende VMs den Storage zum Glühen bringen.

Storage-Belastung im Auge behalten



[1] **Hardware-Kompatibilitäts-Liste von VMware**
www.vmware.com/go/hcl/

[2] **PCoIP-Probleme bei der Bildschirmausgabe beheben**
www.thatsmyview.net/2009/12/18/how-to-get-pcoip-with-view-4-to-work-every-time/

Links



Produkt

Software zur Bereitstellung virtueller Desktops über LAN oder WAN.

Hersteller

VMware
www.vmware.com/de/

Preis

VMware View ist in zwei Versionen verfügbar: Enterprise und Premier. View Enterprise ist ab 2.000 Euro erhältlich und beinhaltet die Lizenzen für zehn Desktop-VMs. View Premier schlägt mit rund 3.200 Euro zu Buche und enthält zusätzlich ThinApp, View Composer und Offline Desktop.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal zur Desktop Virtualisierung in kleinen und mittleren Umgebungen (bis 500 virtuelle Desktops).

gut für mittelgroße Umgebungen (500 bis 2.000 virtuelle Desktops).

weniger für große Umgebungen (mehr als 2.000 virtuelle Desktops), unter anderem wegen der rudimentären Verwaltung und der fehlenden Berechtigungsstruktur.

VMware View 4

Sind Sie Up-to-Tech?

Bleiben Sie Up-to-Tech: Kommen Sie zu den Microsoft® TechDays, besuchen Sie die TechNet Seminare, schauen Sie sich die TechNet Webcasts an, und informieren Sie sich über das TechNet Plus Abonnement.

⇒ Microsoft TechDays

Erfahren Sie IT-News zu aktuellen Themen aus erster Hand, und diskutieren Sie Fragen und Projektideen mit unseren Technical Evangelists. Hier erfahren Sie mehr: www.event-team.com/events/techday

⇒ TechNet Seminare

Unsere kostenlosen halb- oder ganztägigen Seminare für IT-Profis. Hier erfahren Sie mehr: www.microsoft.de/technet/seminare

⇒ TechNet Webcasts

Das Wesentliche von unseren Technologieberatern in einstündigen technischen Präsentationen, live und on Demand. Hier erfahren Sie mehr: www.microsoft.de/technet/webcasts

⇒ TechNet Plus

Ein Muss für IT-Experten – das TechNet Plus Abonnement, inklusive zeitlich unbegrenzten Zugriffs auf Software-Vollversionen. Hier erfahren Sie mehr: www.microsoft.de/technet/abo

© 2010 Microsoft Corporation. Alle Rechte vorbehalten.

JETZT WEBCAST DVD SICHERN!

Gegen Vorlage dieses Gutscheins erhalten Sie auf den Microsoft TechDays die aktuelle Webcast DVD kostenlos.



**Im Test: RES PowerFuse 2010**

Einheitlich individuell

von Jürgen Heyer

Mit der Einführung der Desktop-Virtualisierung und der zunehmenden Verwendung von Terminaldiensten zur Applikations- oder Desktop-Bereitstellung müssen sich viele Anwender ganz oder zumindest teilweise von einer personalisierten Arbeitsumgebung verabschieden. Darunter leidet vielfach die Akzeptanz dieser neuen Techniken. Abhilfe verspricht RES PowerFuse 2010 als zentraler Desktop-Designer, der jeden Anwender mit einer passenden Arbeitsumgebung versorgt, die dieser zusätzlich noch individuell gestalten kann. Ob dieses Versprechen eingelöst wird, zeigte sich im IT-Administrator-Test.

Die Bereitstellung der Arbeitsumgebungen über Terminaldienste und virtuelle Desktops erleichtert der IT-Abteilung das zentrale Management und reduziert die Fehlerhäufigkeit an den Arbeitsplätzen der Mitarbeiter. Allerdings führt dies meist auch zu einer sehr starken Vereinheitlichung, bei der die Anwender teilweise oder ganz auf ihre personalisierte Arbeitsumgebung verzichten müssen. Komplexer wird die Bereitstellung zudem dahingehend, dass sich alle Arbeitsumgebungen aus einer Vielzahl an Konfigurationen zusammensetzen (lokale Einstellungen, Roaming Profiles auf Servern, Policies im Active Directory, Profile im Citrix- beziehungsweise Terminal-Server sowie im virtuellen Desktop).

Genau hier wirkt RES PowerFuse 2010 (RPF) von RES Software entgegen, indem es eine "Zero-Profile-Philosophie" verfolgt und dazu die Anwender-Desktops konsequent von der Infrastruktur entkoppelt: Alle Einstellungen zur Beschreibung einer Arbeitsumgebung werden in einer zentralen Datenbank gespeichert und über eine Management-Konsole definiert. Unabhängig davon, wo im Unternehmen sich ein Anwender anmeldet, erhält er immer seinen Desktop, wobei sich dieser je nach Örtlichkeit auch noch verändern kann, wenn er beispielsweise aus dem Home Office eine bestimmte Applikation nicht starten können

soll. Weiterhin hat er die Möglichkeit, seinen Desktop individuell zu gestalten, wobei diese Einstellungen ebenfalls gesichert werden und auch mitwandern. Migrationen werden deutlich vereinfacht, da die Arbeitsumgebung weder an eine bestimmte Hardware noch an ein Betriebssystem gebunden ist. Zudem können die Applikationen mit wenig Aufwand je nach Örtlichkeit der Anmeldung von unterschiedlichen Quellen aus bereitgestellt werden.

Installation in mehreren Schritten

Voraussetzung für die Installation von RPF ist die Einrichtung eines Datenbankservers, wobei Microsoft SQL Server (2000 oder später), Oracle ab 9i, IBM DB2 ab 8.1 und MySQL ab Version 5.0 unterstützt werden. Im Test setzen wir auf MS SQL 2005 Express, wobei zu beachten ist, dass mit "Gemischter Authentifizierung" installiert wird. Zu kontrollieren ist außerdem, dass der SQL Server-Browser gestartet ist, und es sind die Optionen "TCP/IP" und "Named Pipes" zu aktivieren. Für kleinere Umgebungen ist eine Installation der Datenbanksoftware und RPF auf dem gleichen System möglich. Als Betriebssystem werden praktisch alle Windows-Versionen ab Windows 2000 Professional unterstützt. RPF selbst kommt als knapp 30 MByte großes MSI-Installationspaket, wobei wir dann noch ein 26 MByte großes Update, Auto-PowerPack genannt, einspielen mussten. Anschließend

ist die Verbindung zum Datenbank-Server herzustellen, wobei bei der ersten Verbindung eine Datenbank inklusive eines Datenbank-Benutzers angelegt wird. Ein Assistent unterstützt hier bei der Einrichtung.

Beim Einsatz von RPF ist auf allen Systemen das gleiche Paket zu verwenden, das heißt auch auf jedem Arbeitsplatz-PC wird die Management-Konsole mit installiert. Dafür, dass auf den meisten Clients nur die reine Agentenfunktion benötigt wird, ist also ein relativ großes Paket zu verteilen. Letztendlich ist dies aber vom Hersteller so beabsichtigt, damit ein innerhalb von RPF definierter Verwalter mit entsprechenden Rechten von jedem Arbeitsplatz aus die Möglichkeit hat, die Konsole zu öffnen. Für die übrigen Anwender ist über die Sicherheitseinstellungen von RPF festzulegen, dass diese die Konsole gar nicht öffnen können oder in dieser keine beziehungsweise nur stark eingeschränkte Rechte besitzen.

Ab Windows 2000 Professional für alle Workstation- und Server-Versionen. Hardwareanforderungen entsprechend des genutzten Betriebssystems. Für die zentrale Datenbank Microsoft SQL Server (2000 oder neuer, inklusive Microsoft SQL 2005 Express), Oracle (9i oder neuer, inklusive der Express Edition), IBM DB2 ab 8.1, MySQL ab 5.0

Systemvoraussetzungen



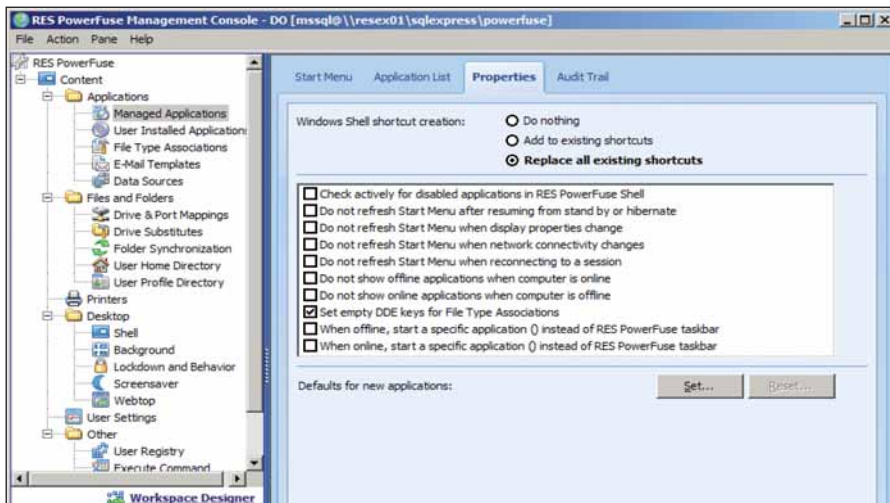


Bild 1: RPF stellt beeindruckend viele Einstellungen zur Verfügung, um einen Desktop individuell zu konfigurieren

Das Ausrollen von RPF auf viele Clients lässt sich über eine Softwareverteilung oder anderweitig skriptgesteuert automatisieren, wozu sich beim Paketaufruf alle zusätzlichen Angaben in der Kommandozeile mit vorgeben lassen. Eine Verteilroutine an sich ist aber in RPF nicht integriert. Nach der Installation ist ein Neustart erforderlich. Während sich der Agent nicht ohne Konsole installieren lässt, ist die Konsole auch ohne Agent verfügbar, dafür stellt RES Software ein eigenes Paket bereit. Damit auf einem Client statt des Windows-Desktops gleich eine RPF-Session gestartet wird, gibt es ein kleines Programm, mit dem sich zwischen den Einstellungen hin- und herschalten lässt.

Beim Verbinden weiterer Clients mit dem Datenbank-Server erkennt die Software, dass dort bereits eine RPF-Datenbank existiert und schlägt die Anbindung an diese vor. Ein großer Vorteil beim Konzept von RPF ist, dass sich die gesamte Kommunikation mit den Clients auf einen Port für die SQL-Kommunikation beschränkt und keinerlei weitere Freigaben oder sonstige gemeinsame Verzeichnisse benötigt werden, die auf das SMB-Protokoll aufsetzen. Der SQL-Port, beim MS SQL-Server standardmäßig 1433, lässt sich auf Wunsch auch ändern. Damit lässt sich RPF recht gut in Umgebungen implementieren, die durch Firewalls segmentiert sind, ohne dafür bekannt kritische Ports öffnen zu müssen. Al-

le Konfigurationseinstellungen werden nicht nur in der Datenbank gespeichert, sondern zusätzlich auf jedem Client lokal in ein Cache-Verzeichnis geschrieben. Dadurch ist sichergestellt, dass jeder Client auch dann die letzte Konfiguration laden kann, wenn die Datenbank einmal nicht erreichbar ist. Damit ist es nicht unbedingt erforderlich, die Datenbank zwingend ausfallsicher zu betreiben, es reicht prinzipiell, über eine entsprechende Datensicherung dafür zu sorgen, dass die Datenbank in akzeptabler Zeit wiederhergestellt werden kann.

Da zum Testzeitpunkt das hier vorgestellte RES PowerFuse 2010 noch nicht komplett freigegeben war, mussten wir mit einer englischsprachigen Version testen, ausgeliefert wird das Paket dann mit zusätzlichen Sprachpaketen, die sich vom Nutzer einspielen lassen.

Getestet haben wir mit der Enterprise-Version, die den vollen Funktionsumfang besitzt und unbegrenzt viele gleichzeitige Sitzungen unterstützt. Die kleinere Standard-Edition ist auf 500 gleichzeitige Sessions beschränkt und besitzt laut Hersteller ungefähr den halben Funktionsumfang der Enterprise Edition. Die kostenlose Express-Edition ist auf 100 Sessions beschränkt mit 20 Prozent des Enterprise-Funktionsumfangs. Die so genannte MyWorkspace-Edition ermöglicht es, personalisierte Desktops zu definieren, allerdings lassen sich hier keine Si-

cherheitseinstellungen festlegen. Für einen detaillierten Vergleich gibt es eine umfassende, mehrseitige Tabelle [1], welche die genauen funktionalen Unterschiede der vier Varianten beschreibt.

Übersichtliche Gruppierung sorgt für Durchblick

Beim ersten Aufruf und Durchklicken der verschiedenen Menüs erscheint die Vielzahl an Funktionen geradezu erschlagend, vor allem, weil die Fenster auch mehrfach in die Tiefe verschachtelt sind. Bei systematischer Betrachtung aber wird vieles verständlich und es zeigt sich eine sinnvolle Logik, die schon nach kurzer Zeit eine zügige, intuitive Bedienung erlaubt. Immerhin hat RES Software mit der vorliegenden Version RPF 2010 die Management-Konsole umfassend überarbeitet und die einzelnen Punkte jetzt übersichtlicher in fünf Bereiche (Context, Content, Sicherheit, Diagnose und Setup) zusammengefasst.

Clients gruppieren

Der Bereich "Context" beschäftigt sich mit der Filterung und Gruppierung der Clients sowie mit den Sicherheitsrollen. Hierzu lassen sich unter "Location and Devices" Zonen unter anderem anhand des Computernamens, einer OU-Mitgliedschaft, einer Umgebungsvariablen, der IP-Adresse, des Betriebssystems, aber auch anhand eines angeschlossenen USB-Gerätes definieren. Letzteres hat den Hintergrund, dass nun beispielsweise ein Administrator zur sicheren Authentisierung einen USB-Stick verwenden kann. Erkennt RPF bei der Anmeldung dieses USB-Gerät, wird der Client einer bestimmten Zone zugeordnet, aufgrund der der Administrator seinen Desktop erhält. So kann dieser sich überall anmelden, das Laden seines Desktop ist aber an den Besitz des Sticks gekoppelt, was die Sicherheit deutlich erhöht, da es für einen Unberechtigten nicht reicht, das Anmeldepasswort zu erraten.

Bezüglich der Verzeichnisdienste unterstützt RPF nicht nur das Microsoft AD, sondern auch noch das Windows-Domänenmodell sowie die Novell Directory



Services. So können Unternehmen zwischen den Verzeichnisdiensten migrieren, wobei die Mitarbeiter immer ihren Desktop erhalten und somit die Migration kaum spüren.

Der Menüpunkt "Workspace Containers" hilft ebenfalls bei der Gruppierung und fasst die Clients zusammen, wahlweise anhand einer dedizierten Auswahl oder aufgrund der Zugehörigkeit zu einer vorher unter "Location and Devices" definierten Zone. Die Sicherheitsrollen schließlich bestimmen die Rechte unterschiedlicher Gruppen innerhalb von RPF. Hier wird beispielsweise der Helpdesk definiert, der in RPF bestimmte Funktionen durchführen, andere nur lesen und manche gar nicht sehen darf. Für jeden Menüpunkt der Konsole lässt sich das Recht auf "Deny Access", "Read" oder "Modify" festlegen. Sicherheitsrollen in RPF lassen sich wiederum mit Benutzern, Gruppen und OUs im genutzten Verzeichnisdienst verknüpfen, was die automatische Pflege erleichtert. Es ist so auch kein Problem, in einem Unternehmen unterschiedliche Anwender nur auf bestimmte Workspace Container zu berechtigen, was eine verteilte Administration beispielsweise aufgrund von Außenstellen oder verschiedenen Örtlichkeiten erlaubt.

Im Bereich "Content" sind sämtliche Einstellungen zusammengefasst, die in irgendeiner Weise den Aufbau des Desktops beschreiben, wie die zugelassenen, gemagten Applikationen, benutzerseitig installierten Applikationen, Dateitypzuordnungen, Mail-Templates mit hinterlegten Servern und Adressen, Datenbankzugriffe, zugeordneten Laufwerke, Netzwerkdrucker, das Desktopdesign an sich (Hintergrund, Bildschirmschoner et cetera) und einige weitere benutzerspezifische Parameter. RPF unterstützt dabei die Definition sehr granularer Einstellungen. So lassen sich beispielsweise einer Applikation Laufwerkszuweisungen, Drucker, Registry-Einträge, Home- und Profilverzeichnisse sowie Kommandoaufrufe zuordnen. Dabei legt der Administrator auch den

Inhalt des Startmenüs fest, so dass jeder Anwender nur die Icons zu sehen bekommt, die er für seine Arbeit benötigt.

Für die Oberfläche an sich liefert RPF eine eigene PowerFuse-Shell mit, die statt des Explorers genutzt werden kann. Die PowerFuse Shell schränkt die Möglichkeiten des Anwenders weiter ein, da dann auch die Standardschaltflächen (Arbeitsplatz, Netzwerkumgebung, Systemsteuerung) des Explorers nicht angezeigt werden, außer sie werden explizit im Startmenü ergänzt.

Clients absichern

Hinter dem Bereich "Sicherheit" verbirgt sich unter anderem eine Application Firewall, die auf Wunsch den Programmzugriff steuert. RPF kontrolliert weiterhin den Zugriff auf Wechseldatenträger, Dateien und Ordner sowie Netzwerkressourcen aufgrund von IP-Adressen oder -Bereichen. Beispielsweise kann RPF den globalen Zugriff auf MP3-Dateien sperren, der Werbeabteilung aber erlauben. Für die verschiedenen Rubriken kann der Administrator die Überwachung aktivieren beziehungsweise deaktivieren sowie in den Lernmodus versetzen. Bei der Installation von RPF ist die Firewall auf diesen Lernmodus eingestellt, so dass sie nichts sperrt, aber sämtliche Programmaufrufe sowie Datei- und Ordnerzugriffe in einem Log notiert. Aus diesem heraus kann der Administrator nun einzelne ausführbare Dateien berechtigen und den Rest sperren. Im Test zeigte sich, dass das Aktivieren der Application Firewall mit großer Vorsicht geschehen sollte und anfangs auch nur auf einen kleinen Workspace Container beschränkt werden sollte, damit nicht plötzlich viele oder gar alle Anwender im Unternehmen nicht mehr



Bild 2: Der Administrator kann diverse Ereignisse wie ein Laufwerksmapping oder eine Druckerzuweisung mit einem Programmstart verknüpfen

arbeiten können. Auch muss sichergestellt sein, dass für den Betrieb wichtige Programme, wie beispielsweise ein Virenschutz-Update, starten können. Gut ist, dass der Administrator beim Design der Startmenüs für die Anwender die dort eingetragenen Applikationen so berechtigen kann, dass hier die Sperre durch die Application Firewall nicht greift. Übrigens verhindert die Application-Firewall auch, dass ein Anwender ein Programm, welches zwar lokal installiert, aber nicht im Startmenü enthalten ist, startet, indem er es über den Datei-Explorer aufruft.

Clients troubleshooten

Der Bereich "Diagnostics" erlaubt die Suche nach angelegten Workspaces mit Fehlern beziehungsweise Auffälligkeiten wie beispielsweise nach Benutzern mit Fehlern im Event-Log, nach gesperrten Anwendern oder solchen, die ihr Passwort nicht ändern können oder deren Passwort nicht ausläuft. Weiterhin lässt sich auslesen, welche Benutzer und welche Agenten aktuell aktiv sind. Für eine genaue Kontrolle aller Aktivitäten gibt es einen Modus, der alle Programmstarts sowie die aufgebauten Sitzungen und benutzten Ressourcen aufzeichnet. Auch alle aufgerufenen Webseiten lassen sich dokumentieren. Sinnvollerweise unterstützt RPF optional ein anonymes Logging, damit benutzerspezifische Informationen nicht aufgezeichnet werden.



Um die Stabilität der Umgebung sicherzustellen, gibt es letztendlich im Bereich "Setup" die Möglichkeit, die Anzahl der gleichzeitigen Logons auf einem Server zu beschränken, weiterhin die CPU-Nutzung durch einen Prozess des Desktops und die Speichernutzung pro Session. Zudem kann RPF verhindern, dass sich Anwender auf der gleichen Workstation mehrfach anmelden.

Bestehende Infrastruktur komfortabel übernehmen

Gerade bei der Einführung von RPF besteht die Hauptaufgabe darin, die vorhandenen Konfigurationen der Clients zu analysieren und nach gemeinsamen sowie individuellen Merkmalen zu sondieren. Hier bietet der Workspace Designer eine überaus wertvolle Hilfe. Zu dessen Nutzung ist RPF auf einem Client zu installieren. Im Programmverzeichnis von RPF findet sich dann ein zusätzliches kleines Paket, welches einen so genannten "Workspace Sampler" installiert. Dieser erzeugt beim Aufruf eine Datei mit allen Informationen zu den angeschlossenen Datenbanken, den Verzeichnisdiensten, den Laufwerks- und Port-Mappings, den Laufwerks-Substitutes sowie zu den eingerichteten Druckern. Da diese Einstellungen auch benutzerabhängig sein können, muss die Aufzeichnung auf einem Client gegebenenfalls mit mehreren Benutzern wiederholt werden.

Kopiert der Administrator nun diese Dateien in ein Verzeichnis und startet er den

Workspace Designer, so liest dieser alle Dateien ein, analysiert deren Inhalt und zeigt die gefundenen Einstellungen an. Nun muss der Administrator Ressource für Ressource durchgehen und prüfen, auf welchen beziehungsweise auf wie vielen Clients sie genutzt wird. Innerhalb des Assistenten kann er dann die Ressource mit entsprechenden Zonenzugehörigkeiten verknüpft als Workspace-Objekt übernehmen, so dass die Zuweisung zukünftig über RPF erfolgt. Letztendlich ist diese Analyse schon ein Stück Arbeit, der Aufwand ist aber weitaus geringer als bei einer rein manuellen Auswertung.

Zu beachten ist, dass Freigabe- sowie Verzeichnisrechte durch RPF nicht verändert beziehungsweise angepasst werden. Bekommt also ein Anwender eine Freigabe oder ein Mapping zugewiesen, für das ihm das Zugriffsrecht im Verzeichnisdienst fehlt, dann kann er nach wie vor nicht zugreifen. Bei einem Drucker wird ebenso vorausgesetzt, dass dieser am Client verfügbar ist, lokal oder auch im Netzwerk. Eine Treiberinstallation oder ähnliches führt RPF nicht durch. Gleiches gilt generell für Applikationen. Auch hier muss die Ressource auf dem vorgesehenen Weg verfügbar sein. Das bedeutet, dass RPF sehr wohl steuern kann, ob ein Programm lokal oder von einem Terminal-/Citrix-Server gestartet werden soll. RPF sorgt auch dafür, dass bei einem Anwender beispielsweise im Home Office die Applikationen lokal gestartet werden, bei der Anmeldung in der Firma dagegen von ei-

nem Terminalserver bereitgestellt werden. Das gewünschte Programm muss aber entsprechend lokal oder auf dem Terminalserver verfügbar sein. RPF betätigt sich also nicht als Softwareverteilung und installiert auch nichts neu. Allerdings bietet RES Software mit RES Wisdom ein entsprechendes Produkt an, welches eng mit RPF zusammenarbeitet.

Bei der Workspace-Bereitstellung unterstützt RPF alle verbreiteten Technologien wie Citrix XenApp und XenDesktop, MS Terminal Services sowie VMware

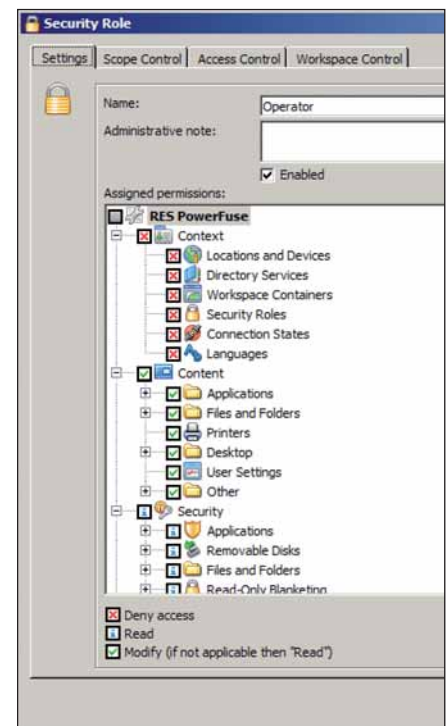


Bild 3: Für eine verteilte Administration erlaubt RPF die Anlage von Sicherheitsrollen mit unterschiedlichen Rechten

Bekommt fürs Putzen 400,- Euro von Ihnen.

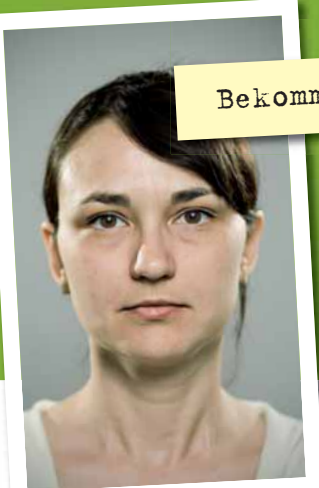
Plus 250,- von Ihrer Konkurrenz.

Mitarbeiter sind auch nur Menschen. Da kann es passieren, dass Daten unverschlüsselt in falsche Hände geraten. Oder gelöscht werden. Oder manipuliert. Oder mit Viren verseucht. Schützen Sie sich davor!

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

Informieren Sie sich jetzt!
www.deviceclock.de oder wählen Sie die Nummer sicher: +49.2102.89211-0

DeviceLock
 Proactive Endpoint Security





View. Nicht unerwähnt bleiben darf in diesem Zusammenhang der patentierte "Workspace Extender". Normalerweise muss ein Anwender zur Nutzung einer Applikation von einem Terminal- oder Citrix-Server sowie lokal zwischen den Desktops umschalten. Mit dem Workspace Extender wird nun eine lokal installierte Applikation wie beispielsweise eine Brennersoftware in den Terminal-Desktop mit eingeblendet und steht dort zur Verfügung. Damit entfällt für den Anwender das doch eher lästige Springen zwischen den Desktops.

Bezüglich der bereits eingangs erwähnten Möglichkeit, dass der Anwender bei einem vorgegebenen Desktop noch Änderungen vornehmen kann, kennt RPF zwei Möglichkeiten, die der Administrator erlauben kann. So ist es möglich, dass der Anwender individuelle Anpassungen bei einer zentral bereitgestellten Applikation vornehmen kann, wie die Vorgabe eines Speicherpfades, Favoriten, eine eigene Mailsignatur, die Ansicht bestimmter Symbolleisten und so weiter. Diese Anpassungen werden in der RPF-Datenbank gespeichert, so dass der Anwender jedes Mal seine Einstellungen wieder bekommt. Weiterhin unterstützt RPF teilweise gemanagte Workstations. In diesem Fall darf der Anwender zusätzlich eigene Applikationen installieren, die dann in den vorgegebenen Desktop mit integriert werden.

Übersichtliches Reporting


Auf praktisch allen Seiten der Management-Konsole hat der Administrator die Möglichkeit, einen so genannten "Instant Report" zu erzeugen. Beim Klick auf die entsprechende Schaltfläche werden alle Inhalte der Seite zu einem druckbaren Report aufbereitet, der sich auch als

PDF-Datei speichern lässt. Ebenso findet sich auf vielen Seiten eine kleine Schaltfläche namens "Audit Trail". Hier sind alle auf dieser Seite durchgeführten Aktionen mit Datum, Zeit, Benutzer und Computer aufgelistet. Das macht es sehr leicht, bereits durchgeführte Aktionen nachzuvollziehen.

Eine dritte, häufig vorhandene Schaltfläche namens "Building Blocks" dient dazu, einzelne Einstellungen in einer XML-Datei zu speichern. Auf diese Weise lassen sich Teile der Konfiguration vor Änderungen oder auch als Backup abspeichern. Ein Import erfolgt auf gleichem Wege. Insgesamt halten wir die gesamten Möglichkeiten für das Reporting, das Nachvollziehen von Aktionen sowie das Speichern von Einstellungen für sehr umfassend und gelungen. Vorteilhaft ist auch, dass die Funktionen nicht an einer zentralen Stelle zusammengefasst sind, sondern auf den jeweiligen Konfigurationsseiten direkt erreichbar sind. So ist die Nutzung stets nur einen Mausklick entfernt.

Fazit

Die Granularität der Einstellmöglichkeiten von RES PowerFuse 2010 eröffnet immense Möglichkeiten, ist aber zugleich eine Herausforderung für den Administrator, um diese dann auch in der Praxis effizient umzusetzen. Der Einsatz bietet sich vor allem dann an, wenn sich der Desktop des Anwenders aus Ressourcen unterschiedlicher Quellen (lokale Applikationen, Netzwerkfreigaben, virtuelle Desktops und Terminalsitzungen) zusammensetzt, die normalerweise an verschiedenen Stellen zu konfigurieren sind. Bei RPF übernimmt dies eine Management-Konsole, und die Desktops lassen sich einfach vereinheitlichen, ohne dem Anwender alle Möglichkeiten zur eigenen Gestaltung zu nehmen. Indem die auf dem Desktop veröffentlichten Objekte auf das notwendige Maß beschränkt werden, lässt sich die Bedienung vereinheitlichen. Durch die Trennung des Desktops von Hardware und Betriebssystem bekommt ein Anwender immer

seine gewohnte Umgebung, egal wo er sich anmeldet. Mit der verfolgten Zero-Profile-Philosophie, bei der alle Einstellungen in einer Datenbank gespeichert sind, lassen sich Roaming Desktops ebenso zuverlässig realisieren wie ein sicheres Arbeitsplatz-Sharing. (jip) 

Produkt

Programm für eine personalisierte Desktop-Bereitstellung.

Hersteller

RES Software
www.ressoftware.com

Preis

Die MyWorkspace-Edition ist ab 45 Euro pro Concurrent User erhältlich. Eine funktional beschränkte Express Edition für 100 Concurrent User kann kostenlos heruntergeladen werden. In der Enterprise-Version beträgt der Preis pro Concurrent User 180 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für den Einsatz in Netzwerken ab etwa 50 Windows-Clients in einer komplexen Umgebung mit virtuellen Desktops und zentraler Applikationsbereitstellung.

bedingt für kleinere Umgebungen, wenn spezielle Sicherheitsanforderungen verlangt werden, die genau definierte Desktops verlangen. Hier ist der im Vergleich hohe Administrationsaufwand zu berücksichtigen.

nicht für Umgebungen, die nicht auf Windows-Clients setzen.

RES PowerFuse 2010

[1] PowerFuse-Editionen im Vergleich

<http://www.ressoftware.com/download.aspx?id=115>

Links



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



Im Kurzttest: POPCon PRO 3.70

Von außen nach innen

von Sandro Lucifora

Mit POPcon für Exchange liefert die Servolutions GmbH ein schlankes und effektives Zusatzprogramm, das POP3-Konten – auch von verschiedenen Mailservern – gesammelt abrufen und die Nachrichten an einen SMTP-Server wie Exchange verteilt. Zusätzlich liefert die integrierte Spam- und Antivirus-Engine Schutz gegen ungebetene und gefährliche Nachrichten.

Konfiguration

Die einzige Aufgabe des Administrators ist die Grundkonfiguration von POPcon. Hierzu gehören das Eintragen des Exchange-Servers und das Setzen der Regeln, wie mit ungewollten E-Mails umgegangen werden soll. Zusätzlich lässt sich bestimmen, dass alle ein- und/oder ausgehenden E-Mails archiviert werden. Als nächster Schritt folgt die POP3- und IMAP-Konfiguration. Im Dauertest haben wir durchschnittlich 25 E-Mailkonten von verschiedenen Mail-Servern abgerufen. POPcon kommt dabei neben POP3 und POP3-SLL auch mit IMAP und IMAP-SLL-Accounts problemlos zurecht. Neben der Angabe des Mail-Servers, des Benutzernamens und des Kennworts haben wir zudem testweise die Portnummer verändert.

Im Anschluss ist anzugeben, ob es sich bei dem Konto um ein Sammelpostfach wie

“*@firma.de” oder ein Einzelpostfach handelt. Der Unterschied liegt darin, dass POPcon beim Sammelpostfach die Zustellung anhand der Empfänger-Adresse der abgeholten E-Mail auf dem Exchange-Server vornimmt. Somit muss die E-Mail-Adresse bei mindesten einem Exchange-Konto hinterlegt sein. Beim Einzelpostfach ist der E-Mail-Empfänger egal – die Zustellung erfolgt immer an das voreingestellte Postfach. Hinzu kommen noch Optionen, ob das Werkzeug die E-Mails auf dem Server belassen oder löschen soll.


Komfortables Scheduling

Ein Schmäckerl ist das Zeitmanagement des Programms: Zum einen lässt sich differenziert konfigurieren, mit welchem Zyklus ein Konto abgefragt wird. Zum anderen erlaubt die Zeitplanung sehr komplexe Einstellungen. Dabei lässt sich jeder Mailabruf sehr einfach definieren – zum Beispiel Montag und Dienstag von 7 bis 18 Uhr alle fünf Minuten, Mittwochs startet der Zyklus erst um 9 Uhr alle zehn Minuten und ab 13 Uhr alle fünf Minuten et cetera. Es lassen sich aber auch nicht zyklische Werte für jedes Abrufen eintragen.

Stellen wir ein, dass ein personenbezogenes Konto bei jedem ersten Zyklus abgerufen wird, können wir bei eher weniger relevanten Konten angeben, dass ein solches nur bei jedem vierten Zyklus Berücksichtigung findet. Damit ist ein ausgeklügeltes Management der E-Mail-Zustellung ohne Überlastung durch weniger wichtige Abrufe erlaubt. Die Möglichkeit, den Mailheader auszuwerten und Domainnamen zu ersetzen, ist hingegen etwas für sehr spezielle Manipulationen der empfangenen E-Mails vor deren Weiterleitung.

Die integrierte Spam-Engine bedient sich der bekannten DNS Open Relay- und Blacklist-Server, was im Zeitalter dynamischer IPs schnell False Positives verursacht. Eine Linderung verschafft die frei definierbare White- und Blacklist, wobei alles in allem bessere Spam-Filter für Exchange auf dem Markt sind. Die in der PRO-Version enthaltene Antivirus-Lizenz arbeitet zuverlässig, das Handling infizierter E-Mails ist aber eher einfach gehalten.

Fazit

POPcon hat in mehr als einem Jahr Dauer- und Praxistest bei rund 16.000 abgeholten E-Mails keinerlei Probleme bereitet. Andere, oft kostenlose Lösungen hatten nicht selten Schwierigkeiten mit nicht-konformen oder mit Zusatz-Attributen versehenen E-Mails – POPcon meisterte jede E-Mail problemlos. Nur die Spam- und Antivirus-Funktion ist weniger spektakulär. (In) 

Produkt

Programm zum POP3-Abruf von E-Mails und deren Weiterleitung an einen internen Groupware-Server.

Hersteller

Servolutions GmbH
www.servolutions.de

Preis

Der Preis der Standardversion beträgt 79 Euro. Die PRO-Version mit Antivirus-Updates für ein Jahr kostet 129 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



POPCon PRO 3.70

Exchange Server 5.5 bis 2007,
alle SBS-Versionen der oben genannten Software,
Lotus Domino/Notes,
Tobit David

Unterstützte Mailserver





Aspekte der Desktop-Virtualisierung

Es ist nicht alles Gold, was glänzt

von Martin Kuppinger

Desktop-Virtualisierung ist zweifelsohne eines der großen Hype-Themen der IT. Viele Unternehmen stürzen sich auf Grund der großen Versprechungen – insbesondere natürlich der Kostenreduktion – darauf. Und manche sind am Ende ernüchtert. Dieser Beitrag zeigt auf, ob die Desktop-Virtualisierung wirklich schon so weit ist, dass sie einen Mehrwert für die IT liefert. Und falls ja, in welchen Szenarien sie zum Tragen kommen sollte. Dazu betrachten wir bestehende Lösungen für den Desktopbetrieb vergleichend und analysieren, welche Faktoren IT-Verantwortliche vor der Einführung virtueller Desktops betrachten sollten.

samtinfrastruktur einschließlich der virtuellen Desktops.

Die Versprechen sind vielfältig. Dazu zählen flexible Desktop-Umgebungen, die sich auf unterschiedlichen Basissystemen, vom Thin Client über Windows- und Macintosh-Systeme bis hin zu Linux-Rechnern, nutzen lassen. Dazu zählen die Optimierung der Ressourcennutzung, die Reduktion von Kosten, ein effizienteres Management und eine auch aus Sicherheitsgründen gute Kontrolle über den Zustand der Desktops. Wie immer bei solchen Versprechen müssen IT-Verantwortliche aber sowohl hinterfragen, ob diese eingehalten werden, als auch, ob es nicht andere Lösungsansätze gibt, die das auch und vielleicht sogar besser liefern.

Aktuelle Desktop-Szenarien

VDIs arbeiten heute typischerweise so, dass auf einem oder mehreren Server-Systemen virtuelle Maschinen ausgeführt werden, auf die über Remote Desktop-



Oberflächlich betrachtet ist Desktop-Virtualisierung eine glänzende Alternative zu bekannten Clientmanagement-Methoden

Fragen nach dem Mehrwert der Desktop-Virtualisierung stellen sich sowohl, wenn IT-Verantwortliche einen nüchternen, distanzierten Blick auf den aktuellen Status der Technologie werfen, als auch bei der Betrachtung der wenig positiven Erfahrungen mancher Anwender. Das heißt nicht, soviel schon vorab, dass Desktop-Virtualisierung keinen Sinn macht. Sie bringt zum heutigen Entwicklungsstand aber sicher nicht in jedem Anwendungsfall die Vorteile, die versprochen werden. Das wird sich ändern, ein kritischer Blick ist aber dennoch, wie bei jeder Technologieentscheidung, ebenso anzuraten wie eine Strategie für die Virtualisierung, die nicht bei der Desktop-Virtualisierung endet.

Desktop-Virtualisierung und VDIs

Desktop-Virtualisierung bezeichnet Ansätze, die die klassische 1:1-Beziehung zwischen der physischen Maschine und dem lokalen Client-Betriebssystem auflösen. Der Desktop, über eben dieses lokale Client-Betriebssystem bereitgestellt, wird stattdessen als virtuelle Maschine (VM) geliefert. Damit lassen sich einfach verschiedene Desktop-Umgebungen auf einer physischen Maschine nutzen, ebenso wie ein virtueller Desktop auch von verschiedenen Systemen aus genutzt werden kann. VDIs sind Virtual Desktop Infrastructures und damit – je nach Marketing-Sicht des Herstellers – entweder nur die Backend-Systeme, die eine solche Infrastruktur bereitstellen, oder die Ge-



Protokolle wie RDP oder ICA zugegriffen wird. Dieser Ansatz des Zugriffs ist von grundsätzlicher Bedeutung, weil die virtuellen Desktops eben nicht auf der lokalen Maschine laufen. Dort läuft vielmehr eine Ausführungsumgebung für die virtuellen Maschinen, derzeit ebenso typisch noch innerhalb eines lokalen Desktop-Betriebssystems – wozu auch die “schlanken” Systeme auf Thin Clients zu zählen sind. Das ist ein wichtiger Punkt, weil er sowohl mit Blick auf das Management der Gesamtinfrastruktur als auch der Lizenzierung Probleme birgt.

Die lokale Bereitstellung der virtuellen Umgebungen ebenso wie die Ausführung von Hypervisor-Technologie “bare metal” auf der jeweiligen Hardware befindet sich bei den meisten Anbietern, wenn überhaupt, noch im Entwicklungsstadium. Eine Option, bei der die virtuellen Desktops lokal ausgeführt werden und damit einerseits die Einschränkungen von Remote Desktop-Protokollen umgangen und andererseits mobile Nutzungsszenarien mit Offline-Nutzung unterstützt werden, lässt für die produktive Nutzung noch auf sich warten.

Wenn wir uns bewusst machen, dass der typische Zugriffsweg heute die Remote Desktop-Protokolle sind, liegt auch eine Alternative zu den VDIs auf der Hand: Klassische Terminal-Dienste, bei denen auf den Server-Infrastrukturen eben nicht getrennte virtuelle Maschinen ausgeführt werden, sondern “nur” mehrere Instanzen innerhalb eines Terminal-Servers laufen. Auch hier wird die Infrastruktur zentral bereitgestellt und verwaltet. Und der Zugriffsweg ist der gleiche. Hinzu kommt, dass es für Terminal Service-Infrastrukturen viele erfahrene Experten, Hersteller und Add-On-Produkte beispielsweise für das System- und Lizenzmanagement gibt.

Nicht außer Acht lassen sollten Sie auch die Variante von lokalen Client-Systemen. Mit der Roaming-Unterstützung beispielsweise von Windows lassen sich

auch hier einheitliche Umgebungen auf unterschiedlichen Systemen nutzen, ebenso wie natürlich auch mehrere Benutzer mit individuellen Umgebungen auf dem gleichen System arbeiten können. Für solche Umgebungen gibt es vielfältige Lösungen für das Systemmanagement oder, wie es heute meist genannt wird, Client Lifecycle Management. Von der Installation über die Softwareverteilung bis hin zum Konfigurations-, Lizenz- und Asset-Management finden sich dort alle Funktionen. Dabei gibt es zwar Herausforderungen, aber eben auch viele Tools und viel Erfahrung. Insgesamt gilt aber auch hier, dass viele Firmen damit ihre Desktops gut im Griff haben. Und es lassen sich alle Anwendungsfälle, vom festen Arbeitsplatz im Unternehmen mit einem Benutzer pro PC über Notebooks bis hin zu Kiosk-Systemen abdecken – mit einer hohen Flexibilität der individuellen Systemkonfigurationen.

Die Frage, welcher Ansatz heute der richtige ist und welcher auf Dauer am besten geeignet scheint, muss daher zwingend gestellt werden, bevor Sie mit der Desktop-Virtualisierung beginnen. Das gilt natürlich vor allem dann, wenn Sie Ihre Infrastrukturen mit Client Lifecycle Management-Lösungen und Terminal Server-Systemen gut im Griff haben.

Desktop-Virtualisierung nicht isoliert betrachten

Klar ist auch, dass das Thema der Desktop-Virtualisierung nicht getrennt von anderen Virtualisierungsansätzen im Unternehmen betrachtet werden kann. Durch die Verlagerung der virtuellen Maschinen auf die Server entsteht dort, trotz der Optimierungsansätze für das Management und die Speicherung von Images, eine signifikante Last. Die Desktop-Virtualisierung müssen Sie daher immer im Zusammenhang mit der Server-Virtualisierung und der Storage-Virtualisierung betrachten. Eine Gesamtstrategie ist hier zwingend, um die Backend-Infrastruktur in effizienter Weise im Griff zu behalten.

Fast noch wichtiger ist aber der Blick auf die Anwendungsvirtualisierung. Mit dieser können Anwendungen bereitgestellt werden, die in einer “virtuellen Schicht” innerhalb des Desktops laufen. Damit lassen sich flexibel unterschiedliche Anwendungen für die virtuellen Desktops liefern – oder auch für klassische lokale Desktop-Systeme. Die Anwendungsvirtualisierung ist vor allem deshalb so wichtig, weil sich damit Anwendungen für eine überschaubare Zahl von vorgegebenen Images bereitstellen lassen und die Zahl der unterschiedlichen Images von VMs klein bleiben kann.

Desktop-Individualisierung und -Deployment

Beim Vergleich der Desktop-Virtualisierung mit anderen Ansätzen muss nach unterschiedlichen Anwendungsszenarien unterschieden werden: Das können Standard-Arbeitsumgebungen sein, die weitgehend einheitlich von vielen Benutzern an ihren Desktop-Systemen genutzt werden. Oder Umgebungen, auf die viele Benutzer beispielsweise in der Fertigung über gemeinsam genutzte Rechner gelegentlich zugreifen. Das sind aber auch die Notebooks von mobilen Benutzern, mal mit einer weitgehend einheitlichen Konfiguration, mal mit einer stärker individualisierten Einrichtung. Es gibt die Mitarbeiter, die stärker individualisierte Umgebungen mit spezialisierter Software brauchen. Es gibt die Entwickler und andere Gruppen, die einen noch größeren Freiheitsgrad bezüglich der verwendeten Software und der Konfiguration ihrer Systeme brauchen.

Die Erfahrung aus dem Client Lifecycle Management zeigt dabei klar, dass die Herausforderung nicht in erster Linie die vielen einheitlichen Systeme sind, sondern die Systeme, bei denen Sie spezifische Änderungen benötigen. Einheitliche Systemumgebungen für viele Benutzer lassen sich auch mit gängigen Client Lifecycle Management-Lösungen effizient ausrollen und verwalten. Und bei der Einschränkung der Freiheitsgra-



de der Benutzer für Anpassungen unterscheiden sich die lokalen Systeme nicht von virtuellen Maschinen, wenn die gleichen Betriebssysteme verwendet werden. Die derzeit noch in den Kinderschuhen steckende Unterstützung eines Deployments der virtuellen Maschinen auf lokale Systeme und einer anschließenden Synchronisation von Änderungen bei VDIs machen dabei bereits deutlich, dass sich mit der Desktop-Virtualisierung nicht alle Anwendungsfälle abdecken lassen.

Hinzu kommt, dass sich die Lösungen heute vor allem auf das Management von Images fokussieren, also eine effiziente Bereitstellung einmal definierter Images. Was innerhalb der Images geschieht, ist aber oft viel interessanter. In den Anwendungsfällen, in denen standardisierte Clients von sehr vielen Benutzern verwendet werden, reicht das auf den ersten Blick aus. Aber auch dort müssen Sie gezielt steuern, zum Beispiel die Konfigurationseinstellungen. Mit anderen Worten: Wer aufgrund seiner Anforderungen etwas mehr Flexibilität benötigt, kommt ganz sicher nicht an ergänzenden Werkzeugen für das Client Lifecycle-Management vorbei. Nur die meist als "OS Deployment" bezeichnete Funktion ist redundant. Das gilt umso mehr, als es ja nicht nur um die Konfiguration und die

Bereitstellung von Software geht, sondern auch um das Management von Lizenzen und anderen Assets. Die Integration mit dem Lizenz-, Asset- und Contract-Management ist natürlich in Umgebungen mit virtuellen Desktops genauso zwingend wie sie es in "klassischen" Umgebungen mit lokal installierten Client-Betriebssystemen ist.

Am Markt ist zu beobachten, dass immer mehr Anbieter von Client Lifecycle Management-Lösungen ihr Portfolio auch auf die Unterstützung von VDIs erweitern. Hier müssen Sie zwar genau hinschauen, was für bestimmte VDIs schon verfügbar ist und was nicht – aber es gibt zunehmend mehr Lösungsansätze. Nur: Sie sollten sich auch darüber bewusst sein, dass die Desktop-Virtualisierung zwar Veränderungen für das Client Lifecycle-Management mit sich bringt, dass dieses aber keineswegs überflüssig wird.

Management und Komplexität im Backend

Wie schon im Zusammenhang mit der Server- und Storage-Virtualisierung angedeutet, müssen Sie sich auch darüber im Klaren sein, dass jede Entlastung beim Client eine Verschiebung von Funktionen und administrativen Aufwänden in Richtung Server bedeutet. Die meisten

VDIs im Markt sind darauf ausgerichtet, große Zahlen an Clients in einer zuverlässigen und hoch skalierenden Infrastruktur zu unterstützen. Es gibt einzelne schlankere Ansätze. Im Grundsatz gilt aber: Sie erhalten – wie in Terminal Server-Infrastrukturen – eine komplexe Backend-Landschaft.

Dabei ist allerdings zu Recht anzumerken, dass auch das lokale Deployment über Client Lifecycle Management-Infrastrukturen gerade beim Imaging und OS-Deployment einiges an Komplexität im Backend schafft. Dieser Preis ist zu zahlen, wenn Sie Funktionen vom Client auf den Server verlagern. Und die Anbieter von VDIs sind auch dabei, hier für Optimierung zu sorgen – durch schonendere Ressourcennutzung beim Speichern von VM-Images, durch bessere und stärker integrierte Administrationschnittstellen. Genauso klar ist aber, dass es hier noch Optimierungsbedarf gibt. Viele der VDIs sind über verschiedene, durchaus komplexe und nicht optimal integrierte Tools zu verwalten – von einer engen Integration des Client Lifecycle Managements ganz abgesehen. Und auch die in der Kombination durchaus sinnvolle Nutzung der Anwendungsvirtualisierung erfordert typischerweise noch einmal getrennte Tools mit anderen Verwaltungsschnittstellen.

STELLENMARKT

Stellenausschreibung



In der Universitäts- und Hansestadt Greifswald ist im Haupt- und Personalamt zum nächstmöglichen Termin die Planstelle

eines/r Abteilungsleiters/in Organisation und EDV

in der Entgeltgruppe 13 TVöD zu besetzen.

Das Stellenangebot ist unter www.greifswald.de/verwaltung.html veröffentlicht.



Log-into success – join the Team!

Für unser junges motiviertes Team suchen wir weitere

Junior Consultants/Consultants

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

Interessiert?

Dann freuen wir uns auf Ihre Bewerbung unter job@loginconsultants.de.

www.loginconsultants.de



Desktop-Deployment im Vergleich				
	Management	Deployment	Laufzeitumgebung	Desktopzugriff
Desktop-Virtualisierung (Remote Desktop)	Server-seitig	Server-seitig	Server	Remote Desktop-Protokoll (RDP, ICA)
Desktop Virtualisierung (Lokales Deployment)	Server-seitig	Lokal (entweder einzeln oder synchronisiert)	Lokal	Lokal
Terminal Services	Server-seitig (oft über Client Lifecycle Management-Software)	Server-seitig	Server	Remote Desktop-Protokoll (RDP, ICA)
Lokales Deployment	Lokal oder Server-seitig (Client Lifecycle Management-Software)	Lokal	Lokal	Lokal

Technologische Entwicklungen

Nun müssen wir den Anbietern von VDIs allerdings auch zu Gute halten, dass es sich um einen relativ neuen Markt handelt und dass die Hersteller sehr viele der genannten Punkte erkannt haben und an Lösungen dafür arbeiten. Bei den Remote Desktop-Protokollen und bei der effizienten Speicherung von Images hat sich schon viel getan. Dennoch gilt: Der Zugriff über ein Remote Desktop-Protokoll ist nicht mit dem lokalen Zugriff auf eine Umgebung gleichzusetzen.

Im Moment ist einer der Entwicklungsschwerpunkte die Unterstützung von mobilen Geräten, auf die VMs lokal installiert und dann synchronisiert werden. Hier dürfte es in absehbarer Zeit auch erste finale Versionen geben, die sich im Produktivbetrieb nutzen lassen. Auch beim Management von Backends, der Integration mit der Anwendungsvirtualisierung, bei Schnittstellen zu Client Lifecycle Management-Lösungen und Funktionen für das License-, Asset- und Contract-Management ist viel Bewegung im Markt.

Noch interessanter werden in Zukunft aber "Bare Metal"-Hypervisoren werden. An solchen Ansätzen arbeiten sowohl Virtualisierungsanbieter als auch Betriebssystemhersteller. Damit lassen sich die virtuellen Systeme ohne darunter liegendes lokales Betriebssystem ausführen, womit sich auch manche offene Frage bezüglich der Betriebssystemlizenzierung er-

übrigt. Mittelfristig wird das dazu führen, dass auf einem lokalen Hypervisor mehrere VMs laufen, wobei eine den Standard-Desktop bereitstellt. Und es spricht viel dafür, dass beispielsweise eBanking-Lösungen zukünftig mit spezialisierten Betriebssystemen in VMs geliefert werden.


Schneller als diese grundlegende Entwicklung, die auch den Betriebssystem-Markt verändern wird, wird es mit Cloud-Angeboten für virtuelle Desktops vorangehen. Der Remote-Zugriff auf von Service Providern betriebene VDIs oder das lokale Deployment von virtuellen Desktops aus solchen Umgebungen ist gerade für kleine Unternehmen eine hochinteressante Option – idealerweise verbunden mit der Branchensoftware als Teil solcher Desktops. Und die Lieferung von virtualisierten Anwendungen aus der Cloud ist ein ebenso naheliegender Ansatz. Hier liegt eines der interessantesten Potenziale der Desktop-Virtualisierung – und hier ist sie jedem alternativen Ansatz klar überlegen.

Fazit

Auch wenn wir heute noch kritisch auf das Thema Desktop-Virtualisierung blicken, ist doch klar, dass dieses ein großes Potenzial hat. Allerdings gilt es gerade bei kurzfristigen Entscheidungen zu überlegen, ob die Anwendungsfälle zu dem heutigen technischen Stand der Desktop-Virtualisierung passen oder ob Unternehmen abwarten oder, zumindest

für den Übergang, auf andere Technologien ausweichen. Wichtig ist auch, dass Sie sich immer darüber bewusst sind, dass die Desktop-Virtualisierung auch ergänzende Funktionen benötigt – sowohl bei der Server-Virtualisierung und dem Storage-Management/-Virtualisierung als auch für das Management dessen, was innerhalb der Images geschieht.

Bei einer mittelfristigen Betrachtung geht es vor allem darum, dass Sie eine Gesamtsicht auf die Virtualisierungsansätze entwickeln. Anwendungs- und Desktop-Virtualisierung hängen ebenso zusammen wie die Desktop-Virtualisierung mit der Server- und Storage-Virtualisierung. Das ist wiederum nur Teil der Strategie für ein effizientes Management, Deployment und Procurement für IT-Infrastrukturen. Und bei Letzterem gilt es, den Blick auf das zu werfen, was sich an Angeboten aus der Cloud entwickelt und entwickeln wird.

Heute gilt dagegen die Empfehlung, das Hype-Thema Desktop-Virtualisierung nüchtern zu bewerten. Ob Sie es dann für einzelne Benutzergruppen, in der Fläche oder vorerst noch nicht verwenden, muss der Einzelfall entscheiden. Sie sollten sich aber nicht nur der Chancen, sondern auch der Herausforderungen bewusst sein – und darüber, dass es ein spannendes Thema mit vielen Aspekten ist, diese vielen Entwicklungen aber auch zeigen, dass es ein noch vergleichsweise neues Themenfeld ist. (j/p) 



Desktop-Virtualisierung mit dem Windows Server 2008 R2

Nah und doch fern

von Christian Knerrmann

Mit der Zunahme an virtuellen Desktops wachsen klassische Terminaldienste und neue Technologien zur Bereitstellung und Verwaltung von virtuellen Desktops kontinuierlich zusammen. Mit dem "Host für Remote-Desktopvirtualisierung" hat Microsoft einen neuen Rollendienst zur Bereitstellung virtueller Desktops in den Windows Server integriert. IT-Administrator stellt Ihnen in diesem Beitrag die neuen Funktionen vor.

Nach und nach wachsen die klassischen Terminaldienste und die neuen Technologien zur Bereitstellung und Verwaltung von virtuellen Desktops kontinuierlich zusammen. Wartete der Windows Server 2008 bereits mit drei neuen Rollendiensten (Terminaldienste-Sitzungsbroker, Terminaldienstegateway und Terminaldienste-Webzugriff) auf, fällt bei der neuen Version R2 zunächst vor allem die konsequente Umbenennung sämtlicher Dienste auf. So heißen die "Terminaldienste" nun "Remotedesktopdienste" und der "Terminalserver" wird zum "Remote Desktop Session Host". Mit dem "Host für Remotedesktopvirtualisierung" findet sich zusätzlich eine neue Rolle im Server Manager, die es erlaubt, neben klassischen Terminalservern nun auch virtuelle Desktops zu realisieren. Als Host kann dazu allerdings aktuell nur der hauseigene Hypervisor Hyper-V zum Einsatz kommen, der automatisch mit installiert wird. Die Verwaltung des Hosts erfolgt anschließend über die MMC "Hyper-V-

Manager", die sich im Server-Manager unter "Rollen\Hyper-V" integriert. Der Hyper-V-Manager ist die zentrale Anlaufstelle zum Erzeugen und Verwalten der virtuellen Desktops.

Hyper-V aufsetzen

Wir nehmen entsprechend einen Hyper-V-Server in unserer Testumgebung in Betrieb und erzeugen zwei virtuelle Maschinen, die wir mit Windows 7 in der 32-Bit-Variante installieren und in unsere Domäne aufnehmen. Um die VMs als virtuelle Desktops verwenden zu können, sind anschließend einige weitere Anpassungen nötig. Diese werden jedoch von keinem Assistenten unterstützt, sondern müssen manuell erfolgen. So aktivieren Sie über den Punkt "Remoteeinstellungen" in den Eigenschaften der Computer den Remotedesktop. Weiterhin autorisieren Sie die Gruppe der Domänen-Benutzer für den Zugriff und aktivieren anschließend gemäß Microsoft-Leitfaden RPC für die Remotedesktopdienste durch

Sie doppelt auf den Wert "AllowRemoteRPC" und weisen diesem eine "1" zu. Anschließend müssen Sie noch das "Remote Service Management" in der Windows-Firewall zulassen. Nun weisen Sie dem Host per WMI-Kommandozeile die nötigen Berechtigungen auf der RDP-Verbindung der VM zu. Nach einem Neustart sind die VM für die Verwendung als virtueller Desktop konfiguriert.

Verbessertes RDP

Betrachten wir zunächst die Clientseite, wo mit Version 6.1.7600 der Remote-Desktopverbindung die Unterstützung für das Remote Desktop Protocol 7 Einzug hält. Der Client ist in Windows 7 und Server 2008 R2 ab Werk integriert und zudem als Update für Vista und XP SP3 verfügbar [2]. Ein Beitrag im Microsoft-Blog liefert eine detaillierte Übersicht dazu, welche Kombination von RDP-Client und Betriebssystem welche Features unterstützt [3]. Windows 7 bietet exklusiv eine Option, wie sie bislang nur von Drittanbietern bekannt war: Verbindungen zu Terminalservern und ihren RemoteApps sowie zu virtuellen Desktops lassen sich nun deutlich einfacher in das Startmenü integrieren.

Serverseitig ist dazu der neue "Remote Desktop Web Access" erforderlich. Neben dem interaktiven Logon an einer Webseite stellt der Web Access Informationen über verfügbare Applikationen und Desktops unter der URL `https://{Servername}/RDWeb/`



Bild 1: Die Desktop-Virtualisierung ist Teil der Rolle "Remotedesktopdienste"

Setzen des entsprechenden Registrierungsschlüssels [1]. Öffnen Sie hierfür den Registry-Editor und gehen Sie zu "HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Control \ TerminalServer". Dort klicken



Feed/webfeed.aspx automatisch auch als RSS-Feed bereit. Dazu wird bei der Einrichtung des Rollendienstes automatisch ein selbst-signiertes Server-Zertifikat erzeugt, das im produktiven Betrieb gegen ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle ausgetauscht werden sollte, zu Testzwecken aber zunächst ausreicht. Rufen Sie die URL `https://{Servername}/RDWeb` zunächst im Browser auf und importieren Sie das Zertifikat in den Speicher "Vertrauenswürdige Stammzertifizierungsstellen", um später Fehlermeldungen zu vermeiden. Anschließend lässt sich über das Systemsteuerungs-Applet "RemoteApp- und Desktopverbindungen" die Integration in das Startmenü konfigurieren. Dazu ist als Option lediglich die URL zum Webinterface anzugeben. Der Feed wird anschließend eingelesen, integriert RemoteApps und Desktops ins Startmenü und hält die Liste aktuell. Diese Art des Zugriffs stellt eine deutliche Verbesserung gegenüber Windows Server 2008 dar, da damit die Notwendigkeit entfällt, die Informationen über einzelne RDP-Verbindungen zu paketieren und mittels Gruppenrichtlinien oder anderweitiger Verteilungsarten zum Client zu transportieren.

Web Access und Verbindungsbroker einrichten

Damit das Ganze funktioniert, sind natürlich zuvor Web Access und Remotedesktop-Verbindungsbroker entsprechend zu konfigurieren. Letzteren haben wir uns unter Windows Server 2008 bereits im Detail angesehen [4]. Wahlweise per lokaler Konfiguration oder mittels Gruppenrichtlinie werden mehrere Terminalserver unter einem gemeinsamen Farm-Namen zusammengefasst, der als zusätzlicher Host-Record für die IP-Adressen der teilnehmenden Server im DNS einzutragen ist. Statt gezielt mit einem Terminalserver Kontakt aufzunehmen, kann nun der Farm-Name in der Remotedesktopverbindung eingegeben werden. Da in den Eigenschaften des DNS-Servers auch unter Windows Server 2008 R2 Round-Robin aktiv ist, werden die Anwender reihum zu den Servern geleitet. Diese nehmen die

Anfrage aber nicht sofort an, sondern kontaktieren ihrerseits den Verbindungsbroker. Sofern eine getrennte Sitzung für den anfragenden Benutzer existiert, wird dieser wiederverbunden. Andernfalls bestimmt der Broker den am wenigsten belasteten Server, zu dem der Anwender dann umgeleitet wird. Der Server wird dabei allerdings weiterhin allein nach der Anzahl der Sessions bestimmt. Erweiterte Metriken, die etwa die Auslastung von Prozessor oder Hauptspeicher berücksichtigen, bietet auch der Windows Server 2008 R2 nicht.

Dennoch hat sich der Broker gegenüber seinem Vorgänger weiterentwickelt und integriert nun auch virtuelle Desktops. Die Änderungen werden insbesondere in Verbindung mit dem Web Access deutlich. Die Oberfläche des "Web Access für Remotedesktop" präsentiert sich unter Windows Server 2008 R2 in neuem Design und ist flexibler beim Zugriff auf mehrere Remotedesktop-Sitzungshosts. War es in der Vorgängerversion nur möglich, einen Terminalserver oder eine Farm als Ziel einzutragen, lassen sich nun auch mehrere Server oder Farmen als RemoteApp-Quellen in einer Liste angeben.

Interessanter noch, als mehrere Terminalserver oder Farm-Namen zu hinterlegen, ist aber die Option, den Broker direkt als Quelle zu verwenden. Dieser ruft dann seinerseits die verfügbaren RemoteApps von den Servern der Farm ab und macht sie dem Web Access bekannt. Damit dies funktioniert, muss das Computerkonto des Web Access-Servers auf dem Broker-Server Mitglied in der lokalen Sicherheitsgruppe "Terminaldienste-Webzugriff-computer" sein. Das Computerkonto des Servers, der den Broker ausführt, muss wiederum auf allen teilnehmenden Terminalservern Mitglied in eben dieser lokalen Gruppe sein. Weiterhin ist der DNS-Name der Farm auf dem Verbindungsbroker im Server-Manager zu konfigurieren. Dies bewerkstelligen Sie mit der Aktion "RemoteApp-Quelle hinzufügen..." per Rechtsklick auf den Knoten "Rollen / Remotedesktopdienste / Remotedesk-

topverbindungs-Manager / RemoteApp-Quellen". Indem der Verbindungsbroker auf diese Weise zwischen Web Access und Terminalserver-Farm positioniert wird, ermöglicht er, via RD Sitzungshost bereitgestellte RemoteApps und via Hyper-V betriebene komplette Desktop-Instanzen unter einer Oberfläche zu vereinen.

Aus Sicht eines Clientrechners stellt sich dies so dar, dass die Remotedesktopverbindung *mstsc.exe* per HTTP(S) Verbindung zum Web Access aufnimmt. Web Access wiederum nimmt die Anmeldeinformationen des Benutzers entgegen und ruft beim Broker eine Liste aller für den Benutzer verfügbaren RemoteApps und Desktops ab. Bevor der Broker zur Bereitstellung der virtuellen Desktops konfiguriert werden kann, ist aber ein weiterer Rollendienst notwendig, ein separater Remotedesktop-Sitzungshost. Installieren Sie diesen Rollendienst zusätzlich auf dem Server, der auch als Broker dient. Dies ist das von Microsoft empfohlene Vorgehen, wenngleich es ebenso unterstützt wird, den Sitzungshost auf einem anderen Server zu betreiben. Es ist somit auch möglich, einen bereits bestehenden Terminalserver zu verwenden. Allerdings müssen Sie dabei beachten, dass der Server fortan ausschließlich als Vermittler von Verbindungen zu den Desktop-VMs dient und damit nicht mehr als regulärer Terminalserver zur Verfügung steht. Die entsprechende Einstellung findet sich in den Eigenschaften des Remotedesktop-Sitzungshosts, wo der Server auf der Registerkarte "Remotedesktop-Verbindungsbroker" für die "Umleitung virtueller Computer" zu konfigurieren ist. Dies lässt sich über die Schaltfläche "Einstellungen ändern..." bewerkstelligen.

Diese Konfiguration führt somit einen weiteren Dienst in das Betriebskonzept ein. Was auf den ersten Blick als zusätzliche Komplikation wirkt, bringt jedoch unmittelbaren Nutzen mit sich, nämlich die Abwärtskompatibilität bis hin zu RDP 5.2-Clients. Der Ablauf beim Verbinden mit einem virtuellen Desktop weist große Ähnlichkeit mit dem Konzept der Terminalserver-

ver-Farm auf. Die RDP-Datei, welche beim Klick auf ein Icon im Web Access an den Client ausgeliefert wird, weist lediglich in diesem Fall nicht auf den DNS-Namen einer Farm, sondern direkt auf den Umleitungs-Server. Dieser fragt wiederum beim Broker an, welche VM dem anfragenden Benutzer zugeordnet ist und startet diese gegebenenfalls. Anschließend kommt eine direkte Verbindung zwischen Client und VM zu Stande.

Letzteres ist insbesondere von Bedeutung für Verfügbarkeit und Skalierbarkeit. Sobald eine Verbindung hergestellt ist, sind Verbindungsbroker und Umleitungs-Server nicht mehr involviert. Eine eventuelle Störung dieser Rollendienste beeinträchtigt bestehende Verbindungen also nicht. Entsprechend sind laut Microsoft keine besonderen Anforderungen an die Leistung der Systeme zu stellen. Broker und Umleitungs-Server sollen bis zu 200 neue Verbindungen pro Minute verarbeiten können [5]. Damit dies aber funktioniert, ist zu guter Letzt noch der Broker entsprechend zu konfigurieren. Dies erledigen Sie im Server-Manager unter "Rollen / Remotedesktopdienste / Remotedesktopverbindungs-Manager / Remotedesktop-Virtualisierungshostserver / Persönliche virtuelle Desktops". Über den Link "Konfigurieren" startet ein Assistent, der durch sämtliche Schritte führt. Auf diese Weise geben Sie dem Broker den Virtualisierungshost, den Web Access Server sowie den Umleitungs-Server bekannt. Im abschließenden Dialog ist die Option "Persönlichen virtuellen Desktop zuweisen" standardmäßig aktiv. Diese startet automatisch einen weiteren Assistenten, der es ermöglicht, virtuelle Desktops und Benutzeraccounts in einer 1:1-Beziehung zu verknüpfen. Der Anwender findet anschließend im Web Access und im Startmenü des Windows 7-Clients sowohl die für ihn freigegebenen Applikationen als auch den Desktop vor. Auf Seiten der Administration existiert dabei im Management des Brokers keine Ansicht, aus der hervorgeht, welche Desktops welchen Benutzern zugeordnet sind. Die Hilfe verweist hier lediglich auf die Möglichkeit, ei-

ne entsprechende Liste mittels PowerShell-Befehlen manuell zu generieren. Ansonsten bleibt über die GUI nur die Möglichkeit, eine Maschine über den Assistenten neu zuzuordnen. Erst wenn Sie dies versuchen, erscheint ein Warnhinweis, falls die VM bereits zugeordnet ist.

Unklarer Desktoppool

Unter der Prämisse, dass viele Benutzer mit möglichst identischen Desktops versorgt werden sollen, erscheint es im Sinne vereinfachten Managements lohnenswert, mehrere VMs zu einem Pool zusammenzufassen. Dies lässt sich per Rechtsklick auf den Knoten "Remotedesktop-Virtualisierungshostserver" über die Aufgabe "Virtuellen Desktoppool erstellen..." erledigen. Auch diese Aufgabe wird durch einen Assistenten unterstützt, der die auf dem Host vorhandenen VMs zur Auswahl anbietet.

Der Assistent weist darauf hin, dass die VMs keinem Benutzer als persönlicher Desktop zugewiesen sein dürfen. Dennoch wird aus dem Dialog nicht ersichtlich, ob diese Voraussetzung erfüllt ist. Ist eine Maschine bereits zugewiesen, wird dieser Umstand nicht erkannt und der Dialog lässt sich trotzdem fortsetzen. Die Überprüfung bleibt also Ihnen selbst überlassen, obwohl Sie wie zuvor erläutert keine einfache Handhabe haben, um festzustellen, ob die Maschinen zugewiesen sind. Weiterhin ist weder über den Assistenten noch über die

MMC eine Option auffindbar, den Zugriff auf bestimmte Benutzer oder Gruppen einzuschränken. Der Assistent informiert zudem, dass alle VMs im Pool identisch konfiguriert sein müssen, was sich aber im gegenwärtigen Entwicklungsstand ebenfalls nicht ohne Weiteres automatisieren lässt. Mehrere Desktops aus einer Vorlage zu erzeugen, ließe sich nur mit dem Microsoft System Center Virtual Machine Manager (SCVMM) oder einer Drittanbieter-Lösung zusätzlich realisieren.

Natürlich ist es unter Verwendung des Sysprep-Tools möglich, mehrere VM aus einer Vorlage zu erzeugen. Diese müssen Sie dann allerdings ab diesem Zeitpunkt jeweils einzeln weiterpflegen. Immerhin gibt es eine Option, um zu verhindern, dass sich die VMs verselbständigen. Legen Sie einen Snapshot einer VM an und benennen diesen um, so dass der Name den String "RDV_Rollback" enthält, wird die VM nach Abmeldung eines Benutzers automatisch auf den Stand des Snapshots zurückgesetzt. Auf diese Weise ist zumindest eine rudimentäre Möglichkeit geboten, mehrere Benutzer mit einheitlichen virtuellen Desktops zu versorgen. Dabei ist es aber nicht möglich, diese Desktops aus einem Master-Image zu provisionieren, so dass die kontinuierliche Pflege inklusive Patch- und Software-Management wieder manuell oder mittels weiterer Produkte erfolgen muss.

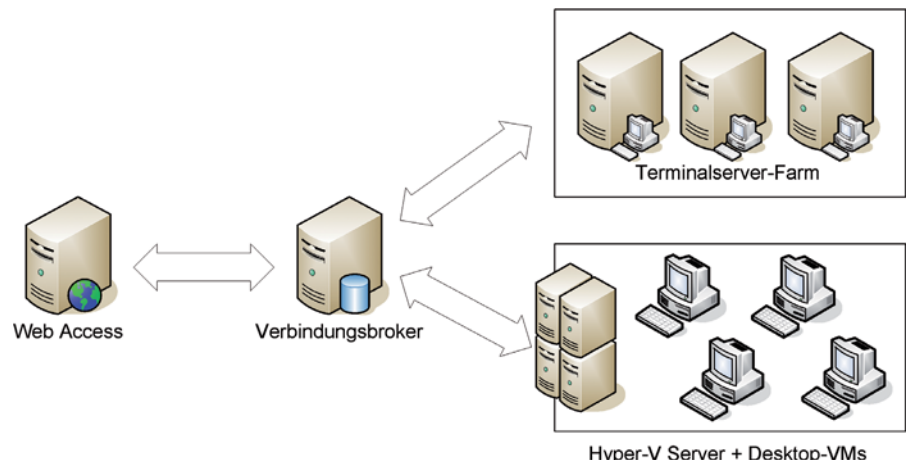


Bild 2: Der Verbindungsbroker vermittelt Sitzungen zu Terminalservern und virtuellen Desktops



Die passende Lizenz

Eines der am häufigsten unklaren Themen bleibt weiterhin die Frage nach der richtigen Lizenzierung. Grundsätzlich stellt das R2-Release gegenüber dem Vorgänger Windows Server 2008 ein eigenständiges Betriebssystem dar. Update oder Neuinstallation eines Servers sind also entsprechend neu zu lizenzieren. Bestehende Client Access Licenses (CAL) zum Zugriff auf die Basisdienste der Windows Server können aber weiter verwendet werden. Auch die bisherigen Terminalservices Client Access Licences (TS-CAL) behalten weiterhin ihre Gültigkeit und sind äquivalent zu den neuen Remote Desktop Services Client Access Licenses (RDS-CAL). Dies spiegelt sich auch in der technischen Verankerung wieder. Die neue Remotedesktoplizenzierung fasst beide Lizenzen zu einem Punkt zusammen. Umgekehrt kann ein R2-Server ebenso Lizenzen von der Terminaldienstlizenzierung unter Windows Server 2008 beziehen. Wer also bereits einen Lizenzserver unter 2008 besitzt, muss nun nicht sofort einen neuen installieren. TS-CAL und RDS-CAL wurden zudem auch inhaltlich erweitert und beinhalten nun das Recht, die Lösung zur Applikationsvirtualisierung Microsoft App-V auf Terminalservern beziehungsweise Remotedesktop-Sitzungshosts zu nutzen [6].

Möchten Sie statt Terminalservern virtuelle Desktops einsetzen, benötigen Sie natürlich keine TS-CAL. Stattdessen war bislang eine Virtual Enterprise Centralized Desktop (VECD)-Lizenz erforderlich.

Sobald Sie die Umleitung konfiguriert haben, ist es nicht mehr ohne Weiteres möglich, sich per RDP direkt mit dem Server zu verbinden. Möchten Sie zu Wartungszwecken darauf zugreifen, müssen Sie dazu die Remotedesktopverbindung mit dem Admin-Schalter aufrufen:

```
mstsc.exe /admin /v:{servername}
```

Der Schalter "/console" älterer Clients funktioniert ebenfalls.

Umleitungen umgehen



Diese war pro Endgerät zu beschaffen und wurde unabhängig von der zur Bereitstellung der Desktops verwendeten Infrastruktur (Citrix Xen-Desktop, Microsoft VDI, VMware View, et cetera) benötigt. Ab dem 01.07.2010 ist das Recht, auf virtuelle Desktops zuzugreifen, für alle Kunden mit Software Assurance inklusive und die VECD-Lizenz entfällt [7]. Soll die Bereitstellung virtueller Desktops, wie im Artikel beschrieben, allein mit Produkten von Microsoft realisiert werden, so bietet der Hersteller hierzu zusätzlich Lizenzen für die "Microsoft Virtual Desktop Infrastructure (VDI) Standard Suite" und die "Microsoft VDI Premium Suite" an [8]. Diese beinhalten Nutzungsrechte für sämtliche Produkte, die im Rechenzentrum zur Bereitstellung virtueller Desktops benötigt werden.

Fazit

Mit dem neuen Windows Server 2008 R2 hat es Microsoft wiederum verstanden, die Funktionalität der Terminaldienste zu erweitern und damit zu bisherigen Alleinstellungsmerkmalen von Drittanbietern aufzuschließen. Die Performance von RDP 7 öffnet im Hinblick auf multimediale Inhalte den Terminalserver für weitere Anwendungsfälle. Web Access vereint dabei Terminalserver und virtuelle Desktops unter einer Oberfläche. Schade ist allerdings, dass viele Funktionen wie die beschleunigte Multimedia-Übertragung oder die Startmenü-Integration aktuell nur für Windows 7-Clients verfügbar sind. Für alternative Plattformen wie Linux-Derivate oder Mac OS X ist zwar die Abwärtskompatibilität gewährleistet, allerdings nur mit dem Funktionsumfang von RDP 5.2. Über den Verbindungsbroker ist es zwar grundsätzlich allen Clients möglich, auf virtuelle Desktops zuzugreifen. Bei den neueren Funktionen bleiben diese Clients – und damit auch die meisten Thin Clients – aber außen vor.

So bedient der Windows Server 2008 R2 mit seinen Bordmitteln primär homogene Windows-Umgebungen von überschaubarer Größe und geringer Komplexität. Der

Host für Remotedesktopvirtualisierung erscheint im gegenwärtigen Entwicklungsstand mit der Festlegung auf Hyper-V sowie Einschränkungen bei der einheitlichen Bereitstellung von VM eher für kleinere Arbeitsgruppen geeignet. Zwar ist in der Microsoft VDI-Lizenz der SCVMM bereits enthalten. Dieser hilft beispielsweise, die Bereitstellung virtueller Desktops durch Klonen zu automatisieren. Bei der Zuordnung von Benutzern zu VM und der Verwaltung laufender Sessions fehlt es aber noch an zentralen Management-Tools und differenzierter Rechte-Vergabe. (dr) 

[1] Installieren und Einrichten der VM

[http://technet.microsoft.com/en-us/library/dd883257\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd883257(WS.10).aspx)

[2] Client-Update für Vista und XP SP3

<http://support.microsoft.com/kb/969084/en-us/>

[3] Übersicht zu möglichen Kombinationen von RDP-Client und Betriebssystem

<http://blogs.msdn.com/rds/archive/2009/08/21/remote-desktop-connection-7-for-windows-7-windows-xp-windows-vista.aspx>

[4] IT-Administrator-Beitrag zum Windows Server 2008

"Unsere kleine Farm - Terminaldienste unter Windows Server 2008 (2)"
in IT-Administrator 10/2008 S. 45-50

[5] TechNET Webcast zum Broker und Umleitungs-Server

www.microsoft.com/germany/technet/events/eventdetail.aspx?EventID=1032422451

[6] Unterschiede zwischen RDS-CAL und TS-CAL

<http://blogs.msdn.com/rds/archive/2009/09/04/what-s-the-difference-between-rds-cal-and-ts-cal.aspx>

[7] Virtual Enterprise Centralized Desktop (VECD)-Lizenz

www.microsoft.com/Presspass/press/2010/mar10/03-18DesktopVirtPR.msp

[8] Lizenzen für die "Microsoft Virtual Desktop Infrastructure (VDI) Standard Suite" und die "Microsoft VDI Premium Suite"

http://blogs.technet.com/virtualization/archive/2009/07/13/Microsoft_1920_s-new-VDIlicensing_3A00_-VDI-Suites.aspx

Links



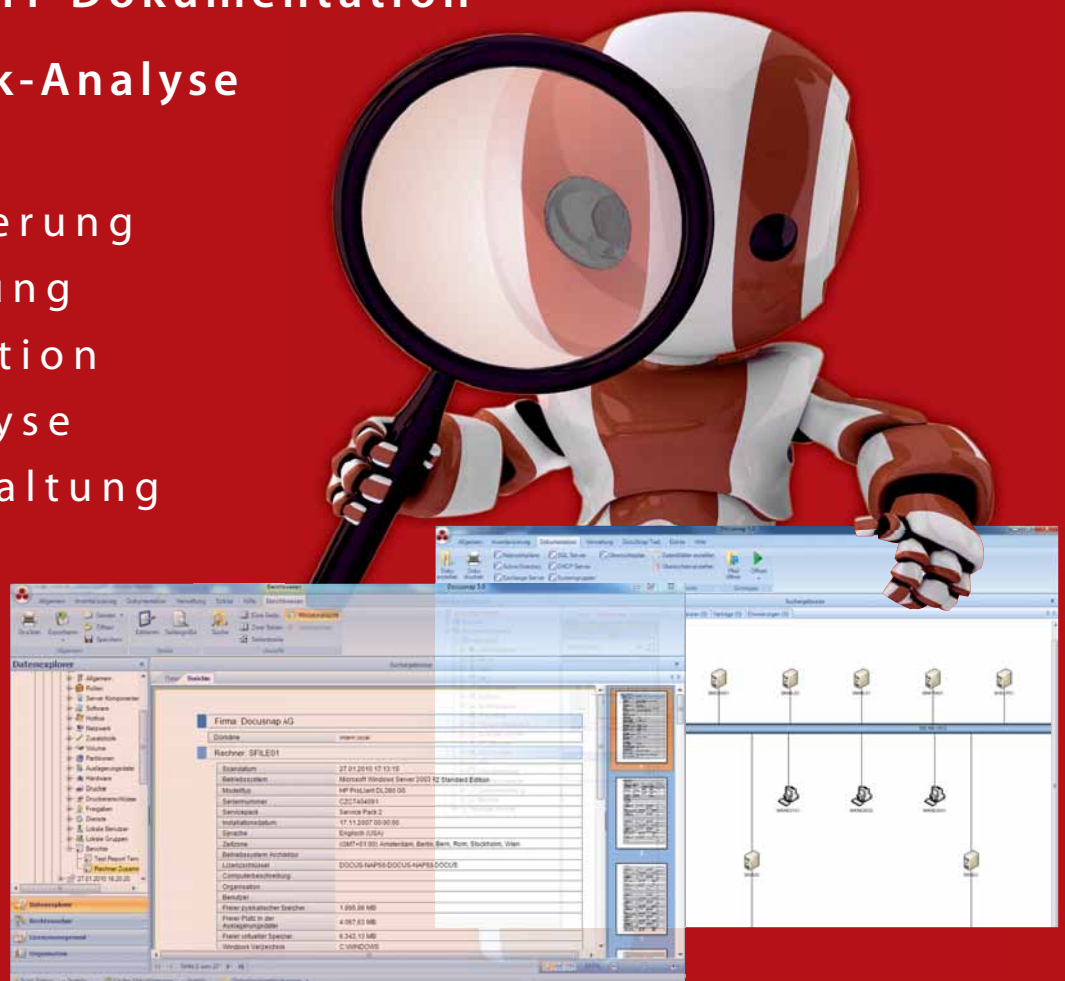


DocuSnap®

Schluss mit dem IT-Chaos!

Software für IT-Dokumentation und Netzwerk-Analyse

- Inventarisierung
- Visualisierung
- Dokumentation
- Rechteanalyse
- Lizenzverwaltung



www.docusnap.de

Desktop-Verteilung mit Red Hat Enterprise Virtualisierung Der Pinguin wird virtuell

von Thorsten Scherf

Nach den Servern erscheint aktuell immer häufiger der Endbenutzer-Desktop auf dem Radar der Virtualisierungsanbieter. Eine neue Lösung aus dem Hause Red Hat tritt an, um den Platzhirschen VMware, Citrix und Microsoft Marktanteile streitig zu machen. Red Hat Enterprise Virtualisierung (RHEV) kam Ende 2009 für Server-Systeme auf den Markt, Mitte dieses Jahres wird die finale Version zur Desktop-Virtualisierung erwartet, die sich gerade in der Beta-Phase befindet. Höchste Zeit also, sich den neuen Stern am Virtualisierungshimmel etwas genauer anzusehen.

RHEV [1] unterstützt aktuell die Gast-Betriebssysteme Red Hat Enterprise Linux 3/4/5, Windows XP, Windows Server 2003 und 2008. Auf den physischen Host-Systemen gibt Red Hat einen Support von bis zu 96 CPU-Cores und 1 TByte RAM an, auf den virtuellen Systemen bis zu 16 vCPUs mit 64 GByte RAM. Das Host-System muss dabei über eine x86_64 CPU verfügen.

Die Komponenten von RHEV

Beim RHEV-Framework arbeiten mehrere Komponenten zusammen: Zum einen bildet der Virtualization Manager (RHEV-M) die eigentliche Core-Komponente der Software. Hierbei handelt es sich um eine Management-Plattform zur Installation, Konfiguration und Verwaltung von Hypervisor-Systemen, virtuellen Server- und Desktop-Instanzen. Der eigentliche Hypervisor ist Teil der RHEV-H Komponente. Hierbei kommt ein minimales Red Hat Enterprise Linux 5.4-System mit einem KVM-Hypervisor [2] zum Einsatz. Das ganze System ist so klein, dass es bequem auf einen USB-Stick passt. Die Installation der Software erfolgt dann auf der lokalen Festplatte.

Natürlich können auch reguläre Red Hat Enterprise Systeme ab der Version 5.4 als Host-Systeme für die virtuellen System-Instanzen zum Einsatz kommen. Dies ist jedoch auch aus ökonomischer Sicht nicht anzuraten, wenn dieses System le-

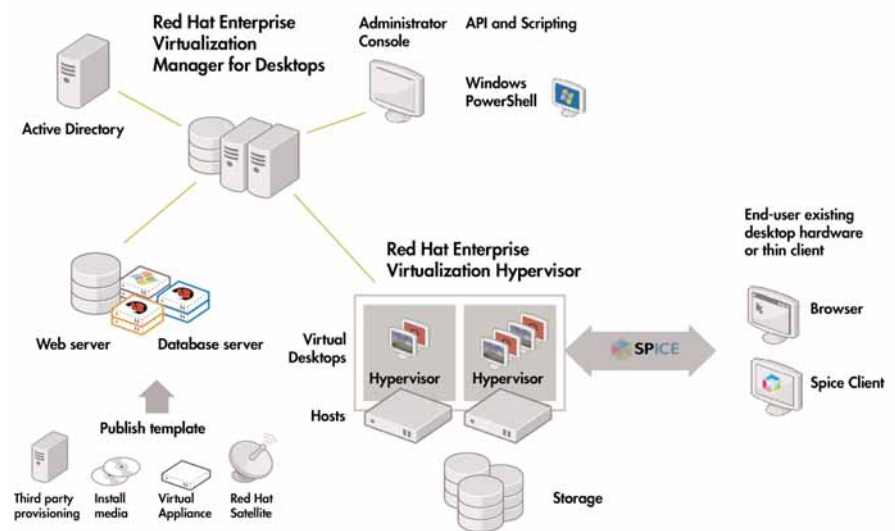


Bild 1: Das RHEV-Framework besteht aus einer Vielzahl einzelner Komponenten

diglich als Host für virtuelle Maschinen dienen soll, hierfür eignet sich ein entsprechend konfiguriertes RHEV-H-System besser. Sowohl RHEV-H als auch reguläre RHEL-Nodes sind vor der eigentlichen Konfiguration am Management-System (RHEV-M) anzumelden und zu registrieren. Dank des neuen Remote-Rendering-Protokolls SPICE [3] ist auch der Einsatz von Desktop-Systemen innerhalb einer virtuellen Maschine kein Problem mehr. Die Performance ist mit nativen Installationen vergleichbar. SPICE ist dabei in der Lage, auf CPU- und GPU-Ressourcen der Client-Maschine zuzugreifen. Hierdurch verringert sich die Last auf den Hypervisor-Systemen entsprechend.

Aufbau und Verwaltung der Infrastruktur mit RHEV-M

Das Management-Framework RHEV-M basiert dabei auf der von Qumranet entwickelten SolidICE-Plattform. Hierbei handelt es sich um eine ASP.NET-Webapplikation, die einen Microsoft Windows Server 2003 R2 sowie einige zusätzliche Komponenten wie .NET, WPF und Microsoft SQL Server voraussetzt.

Das derzeit verfügbare Installationsprogramm *rhev-m-2.1.exe* benötigt eine Active Directory-Umgebung. Benutzer, die sich beim RHEV-M anmelden, müssen in der AD-Umgebung über ein entsprechendes Konto verfügen. Nach der Installation der Management-Oberfläche

lassen sich sämtliche administrativen Aufgaben bequem über ein Webinterface durchführen. Hierfür rufen Sie im Webbrowser einfach die Adresse `http://localhost/RHEVManager` auf. Der RHEV-M verwaltet sämtliche logischen und physikalischen Ressourcen in einem "Data-Center". Standardmäßig ist nach der Installation lediglich ein einzelnes Data-Center vorhanden, bei Bedarf können Sie natürlich weitere hinzufügen. Zu den RHEV-M-Ressourcen zählen neben den Hypervisor- und RHEL-Hosts auch Cluster-, Speicher-Pools und Speicher-Domänen, Netzwerke und natürlich die eigentlichen virtuellen Server- und Desktop-Instanzen.

Bei den Host-Systemen handelt es sich entweder um dedizierte Hypervisor-Hosts (RHEV-H) oder um reguläre x86_64-Systeme auf Basis von Red Hat Enterprise Linux 5.4 (RHEL) oder höher. Auf beiden kommt als Hypervisor das Linux-Kernel-Modul KVM zum Einsatz. Aus diesen Host-Systemen ist dann ein Cluster-Verbund zu bilden. Hierbei handelt es sich um eine Gruppierung von physikalischen Hosts, die sich die gleichen Ressourcen teilen und zur gleichen Migrations-Domäne gehören. Alle bereits oben genannten Ressourcen (Hosts, Storage, Netzwerk), eine Scheduling Policy für virtuelle Maschinen sowie CPU- und Memory-Ressourcen sind dann diesem Cluster zuzuordnen und stehen allen Instanzen der virtuellen Maschinen zur Verfügung. Eine Migration der virtuellen Maschinen ist dabei nur innerhalb der gleichen Migrations-Domäne möglich. Beim Anlegen der Speicher-Domänen ist grundsätzlich zwischen sogenannten Data- und ISO-Domänen zu unterscheiden. Erstere halten die eigentlichen Images der virtuellen Maschinen vor (virtuelle Festplatten-Abbilder oder Volume Snapshots), letztere enthalten ISO-Dateien zur Installation neuer virtueller Systeme. Als Backend für eine solche Speicher-Domäne kommt entweder iSCSI, Fiber-Channel (FC) oder NFS zum Einsatz. Bei der Verwendung von iSCSI oder FC

kümmert sich der Device-Mapper LVM um die Verwaltung der Festplatten. Wichtig dabei ist, dass lediglich ein physikalischer Host die Kontrolle über die Speicher-Metadaten besitzt. Bei diesem Host handelt es sich um den sogenannten "Storage Pool Manager" (SPM). Dieser läuft üblicherweise auf dem ersten Host-System eines Data-Center-Clusters. Fällt dieses System aus, sorgt der Virtualization Manager für eine Migration des Dienstes auf einen anderen Host des gleichen Clusters. Bevor also nicht mindestens ein Host auf dem RHEV-M registriert wurde, ist keine weitere Konfiguration der Umgebung möglich.

Beim Anlegen von logischen Netzwerken ist der Einsatz von Bonding- und VLAN-Geräten möglich. Standardmäßig existiert nach der Installation des Virtualization Managers nur ein einzelnes Netzwerk (rhev). Um den auftretenden Netzwerkverkehr entsprechend zu trennen, sollten Sie unbedingt weitere Netzwerke einrichten. Somit erhalten Sie dedizierte Umgebungen für den Speicher, Management-, Display- und Failover-Daten-Verkehr. Es ist darauf zu achten, dass sämtliche Hosts eines Clusters eine identische Netzwerkkonfiguration aufweisen, ansonsten kann es bei der Migration von virtuellen Maschinen eventuell zu Fehlern kommen. Bei der Auswahl des Bonding-Modes ist außerdem zu bedenken, dass einige Modi eine spezielle Konfiguration der Netzwerk-Switche erfordern [5].

KVM als Hypervisor

Neben dem Management-Framework bilden die physikalischen Host-Systeme das Herzstück von RHEV. Wie bereits erwähnt, kommen hierfür entweder reguläre RHEL-5.4 Systeme oder dedizierte RHEV-H-Hosts zum Einsatz. Bei Letzteren handelt es sich um Thin Clients, die ein ungefähr 100 MByte großes LiveOS-Image booten. Dieses Image hat einen Memory-Footprint von circa 512 MByte, bei der Installation sind knapp 700 MByte Festplatten-Speicher notwendig.

Unabhängig davon, welches System als Host für die virtuellen Maschinen dient, kommt auf beiden der KVM-Hypervisor zum Einsatz. Bei KVM handelt es sich um ein Kernel-Modul, welches auf den Virtualisierungssupport der eingesetzten CPU angewiesen ist. Diese kennt zwei unterschiedliche Modi zur Ausführung von Befehlsanweisungen. Zum einen den sogenannten Root-Mode und zum anderen den Non-Root-Mode. Führt eine virtuelle Maschine im Non-Root-Mode eine privilegierte Aktion aus, so fängt der Prozessor diese Anweisung ab und schickt sie an den KVM-Hypervisor.

Dieser führt nun im Root-Mode den Befehl stellvertretend für das Gastsystem aus und wechselt danach wieder in den Non-Root-Mode, bevor er wieder die Kontrolle über die CPU an das Gastsystem zurückgibt. Somit muss der Hypervisor nicht ständig jede Aktion der Gastmaschinen aktiv überprüfen, um eventuell auftretende privilegierte Aktionen abfangen zu können. Aktuelle Intel-VT- und AMD-V-Prozessoren verfügen über die benötigte Erweiterung. Um den erweiterten Befehlssatz des jeweiligen Prozessors benutzen zu können, benötigt der KVM-Hypervisor jeweils ein eigenes Kernel-Modul (kvm-intel beziehungsweise kvm-amd). Die virtuellen Maschinen laufen dann als reguläre Prozesse im User-Space und sind über die Geräte-Datei `/dev/kvm` ansprechbar.

Als Emulator für I/O-Hardware kommt ein modifiziertes qemu zum Einsatz. Für einen performanten Zugriff auf die einzelnen IO-Subsysteme existieren jedoch spezielle Treiber, die den Hypervisor direkt ansprechen (virtio). KVM unterstützt auch aktuelle Kernelfeatures wie beispielsweise Kernel Samepage Merging (KSM) [6]. Hiermit ist eine Zuweisung von identischen Speicherbereichen an mehrere virtuelle Maschinen gleichzeitig möglich. Mit Hilfe dieser neuen Technologie lässt sich der zur Verfügung stehende Speicher des Host-Systems "überbuchen".



Installation und Konfiguration von RHEL-Hosts

Um einen bestehenden RHEL 5.4-Host im REHV-Manager zu registrieren, sind im Vorfeld einige Arbeiten durchzuführen. Als Erstes stellen Sie bitte sicher, dass Ihre x86_64-CPU wirklich über die notwendige Virtualisierungsfunktion verfügt. Dies erfolgt am einfachsten über den folgenden Aufruf:

```
# grep -color -e svm -e vmx  
/proc/cpuinfo
```

Achten Sie auch darauf, dass die Funktion nicht im BIOS deaktiviert ist. Für eine unkomplizierte Installation der Software-Pakete sollte das System im Red Hat Network registriert sein. Natürlich ist es aber auch möglich, die notwendigen Pakete lokal abzulegen und zu installieren. Mit Hilfe des RPM-Frontends "yum" gelangen die Pakete schnell auf das eigene System:

```
# yum install vdsmd vdsmd-reg vdsmd-  
cli fence-agents kvm-qemu-img kvm-  
tools bridge-utils openssh-server
```

Zur Kommunikation zwischen dem RHEV-M und dem lokalen Host kommt das vdsmd-Protokoll zum Einsatz. Das Paket "vdsmd-reg" kümmert sich um die Registrierung auf dem Virtualization-Manager und mit Hilfe von *vdsmd-cli* kontrollieren Sie Ihr Host-System auf der Kommandozeile. Hiermit ist es dann nicht notwendig, auf das grafische Webinterface zurückzugreifen, um einzelne virtuelle Maschinen zu administrieren. Dabei ist *vdsmd-cli* vergleichbar mit dem *virsh*-Tool aus dem *libvirt*-Paket. Da RHEV in der aktuellen Version jedoch nicht *libvirt*-kompatibel ist, kommt dieses Protokoll momentan nicht zum Einsatz. Der Support hierfür ist jedoch für ein späteres RHEV-Release geplant. Aktuell benutzt RHEV das angesprochene *vdsmd*-Protokoll zur Kommunikation zwischen dem Manager und den Host-Systemen.

Das Paket "fence-agents" ist optional und nur dann notwendig, wenn Sie die HA-

Funktionalität von RHEV nutzen wollen. Hierbei kümmert sich ein Fence-Agent darum, einen ausgefallenen Host zu rebooten, falls dieser nicht mehr auf Anfragen reagiert. Das ist notwendig, damit nicht mehrere Hosts versehentlich gleichzeitig auf die Ressourcen einer virtuellen Maschine zurückgreifen. Gerade bei Dateisystemen könnte dies schwerwiegende Folgen haben.

Nach der Installation der Pakete stellen Sie sicher, dass sowohl der *vdsmd*- wie auch der *vdsmd-reg*- und *ssh*-Dienst aktiv sind. Der *ssh*-Dienst wird zum initialen Registrieren der Hosts auf dem RHEV-M benötigt. Kommt eine Firewall zwischen den Systemen zum Einsatz, so sind hier die eingehenden TCP-Ports 22, 16509, 54321, 5634 bis 6166 und 49152 bis 49216 freizuschalten. Zur Registrierung der Maschine rufen Sie dann das Management-Webinterface über <https://rhev-host/RHEVManager> auf. Über den Menüpunkt "Hosts / New" nehmen Sie dann den gewünschten RHEL-5.4-Host als neues System auf. Damit der Virtualization-Manager auf den Host zugreifen kann, sind neben der IP-Adresse auch das root-Passwort und der Port des *vdsmd*-Dienstes anzugeben (default: 54321). Abschließend ordnen Sie den Host einem RHEV-Cluster zu. Sämtliche Ressourcen dieses Clusters stehen dem Host somit zur Verfügung. Ein abschließendes "OK" beginnt den Registrierungsprozess auf dem Manager. Hierbei lädt der Host die in Python geschriebene Bootstrap-Datei *vds_bootstrap* vom Managementsystem herunter und führt die Anweisung aus dieser Datei aus. Hat alles funktioniert, so taucht das System schließlich auf dem Management-System in der Host-Liste auf und ist ab diesem Zeitpunkt in der Lage, als Wirtssystem für virtuelle Maschinen zu dienen.

Thin Clients als RHEV-H-Hosts

Anstatt ein reguläres RHEL-System als Hypervisor-Host zu verwenden, können Sie natürlich auch einen Thin Client mit dediziertem Hypervisor einsetzen. Dieser ist bereits im RHEV-Paket enthalten und speziell für den Einsatz unter RHEV aus-

gelegt. Im Vergleich zu einem regulären RHEL-Host bieten sich hier nicht nur Vorteile bezüglich der System-Lizenzierung, sondern auch im Bereich Sicherheit. Hierzu zählt beispielsweise ein spezielles SELinux-Regelwerk. Hiermit ist ein fein granulierter Zugriff der virtuellen Maschinen auf die vorhandenen Ressourcen auf Basis der Mandatory-Access-Control (MAC) möglich.

Zur Installation der RHEV-H-Software können Sie die 100 MByte große ISO-Datei entweder auf eine CD, einen USB-Stick oder einen TFTP/PXE-Server kopieren. Für diese Aufgabe bietet sich der Einsatz der LiveCD-Tools an. Wollen Sie den Hypervisor-Host mit einer CD installieren, so rufen Sie hierfür den folgenden Befehl auf:

```
# cdrecord -v -dev=/dev/cdrw  
/usr/share/rhev-hypervisor/  
rhev-hypervisor.iso
```

Das Kopieren der Software auf einen USB-Stick gelingt über:

```
# livecd-iso-to-disk -format  
rhev-hypervisor.iso /dev/usbstick
```

Haben Sie im Netzwerk einen TFTP/PXE-Server im Einsatz, so extrahieren Sie den Kernel und die *initrd* wie folgt aus der ISO-Datei:

```
# live-iso-to-pxeboot rhev-  
hypervisor.iso
```

Anschließend kopieren Sie die beiden Dateien auf Ihren TFTP-Server und passen die Konfigurationsdateien entsprechend an. Anschließend booten Sie das System entweder mit der soeben erzeugten CD, dem USB-Stick oder über das Netzwerk mit Hilfe von PXE.

Um die RHEV-H-Software auf dem Host zu installieren, können Sie zum einen alle notwendigen Informationen direkt am boot-Prompt des Setup-Programms übergeben oder aber Sie gehen

Schritt für Schritt durch alle Menü-Optionen und führen die Installation manuell aus. Hierbei ist neben diversen anderen Aufgaben auch das Dateisystem und das Netzwerk des Hosts entsprechend einzurichten. Damit der Host weiß, wie sein Management-System lautet, ist natürlich auch diese Information mit zu übergeben. Für alle Punkte schlägt das Setup-Programm entsprechende Default-Einstellungen vor. Schließlich führen Sie mittels "Install locally and Reboot" die eigentliche Installation auf der lokalen Festplatte des Systems aus. Nach dem Reboot erscheint auch dieses System in der Host-Liste des Management-Systems und wartet auf seinen Einsatz.

Virtuelle Server und Desktops

Sind die Vorarbeiten erfolgreich ausgeführt, so sollte zu diesem Zeitpunkt ein Windows Management-System mit mindestens einem RHEL 5.4-Hypervisor-Host vorhanden sein. Der Host liegt dabei entweder als dedizierter Hypervisor oder als reguläres RHEL 5.4-System vor. Ihr Management-System verfügt über ein Data-Center mit mindestens einem Cluster und allen notwendigen Ressourcen, wie beispielsweise einer Speicher-Domäne und einem logischen Netzwerk.

Zum Einrichten eines virtuellen Server- oder Desktop-Systems stehen nun sämtliche Ressourcen dieses Clusters zur Verfügung. Über den Menüpunkt "Virtual Machines / New" stoßen Sie das Setup eines neuen Systems an. Damit Sie bei der Installation einer neuen Maschine nicht immer wieder die gleichen Aufgaben durchführen müssen, stehen Ihnen sogenannte Templates zur Verfügung. Diese enthalten die Konfiguration für virtuelle CPUs, Memory, Speicher-Domäne und Netzwerk. Mit Hilfe solcher Templates erzeugen Sie eine große Anzahl von Systemen in sehr kurzer Zeit.

Nach dem Setup der Maschine können Sie diese dann über den Menüpunkt "Run once" starten. Zur Installation des eigentlichen Betriebssystems kommt dann beispielsweise eine ISO-Datei aus der entsprechenden Speicher-Domäne zum Einsatz. Diese wählen Sie über den Menü-Punkt "Attach CD" aus. Beim Hochfahren der soeben erstellten virtuellen Maschine bootet diese dann in das Installationsprogramm des ISO-Images. Alternativ ist auch eine PXE-basierte Installation über den Red Hat Network Satellite Server (RHNS) mit integriertem Cobbler Management-System möglich [7]. Dies ist eine sehr elegante Möglichkeit, da bereits sämtliche Installationsressourcen auf dem RHN-Server liegen. Hierzu zählen neben den eigentlichen Installationspaketen auch eine Kickstartdatei, die eine Antwort-Datei zur automatischen Installation von Linux-Systemen darstellt. Diese ist vergleichbar mit einer *unattended.txt*, welche zur automatisierten Installation von Windows-Systemen dient.

Auf der anderen Seite bietet auch der Einsatz von virtuellen Maschinen-Templates gewisse Vorteile. Ist eine große Anzahl von

Kostenlos für
IT-Administrator-Abonnenten

iläNet

Workshop in Köln

Virtualisierung mit Hyper-V R2 am 22. April 2010

Die Agenda:

- 13.00 Uhr: Begrüßung
- 13.15 Uhr: Hyper-V Server 2008 R2
 - > Leistungsfähigkeit von Hyper-V R2 unter der Lupe – Gegenüberstellung mit XEN/VMware
 - > Planung der Hyper-V-Installation (Storage-Planung und Kapazitätsplanung auf dem Host)
 - > Was alles unter der Haube steckt (Snapshots, Live-Migration, Backup)
 - > Management des Hyper-V mit SCVMM

Referenten: *sepago GmbH, Köln*



17.30 Uhr: Ende des Workshops

Termin: 22. April 2010

Ort: sepago GmbH,
Dillenburger Straße 83, 51105 Köln

Uhrzeit: 13.00 bis 17.30 Uhr

Teilnahmegebühren:

Für IT-Administrator Abonnenten kostenlos.

Anmeldeschluss: 16.04.2010

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

virtuellen Systemen mit identischen Parametern zu installieren, beispielsweise Arbeitsplatz- oder Cluster-Systeme, so eignet sich hierfür ein Template zum Clonen einer Basis-Installation besser. Im Vergleich zur Kickstart-basierten Methode ist dieser Vorgang um einiges schneller und die virtuellen Systeme stehen schneller zur Verfügung. System-spezifische Details wie IP-Adresse, Krypto-Keys und Maschinen-SID sind bei Linux-Systemen dann mit Hilfe von Makros im ursprünglichen Template zu ersetzen, für Windows-Systeme lässt sich dieses Problem mit Hilfe des Tools Sysprep lösen [8]. War die Installation der virtuellen Maschine erfolgreich, so taucht diese anschließend im Management-Interface unter dem Tab "Virtual Machines" auf. Sie können die Maschine nun über den Menüpunkt "Run" zum Leben erwecken.

Grafische Desktops mit Würze

Für den Zugriff auf grafische Desktops, unabhängig davon, ob diese unter Windows oder Linux laufen, stehen drei unter-

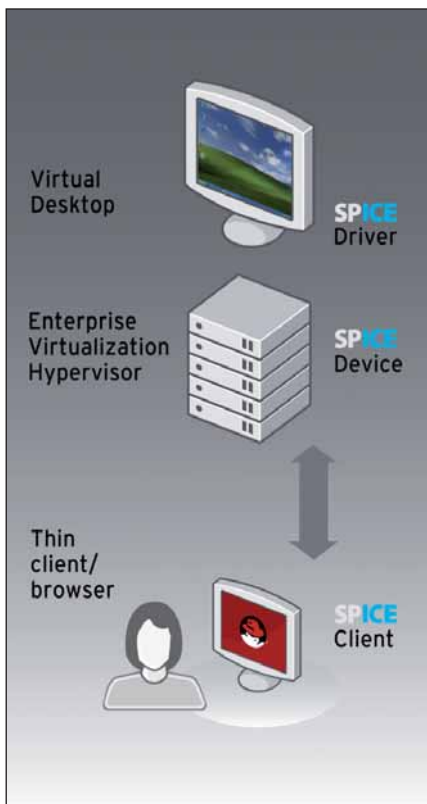


Bild 2: Das SPICE-Framework besteht aus mehreren Komponenten. Der Treiber steht dabei sowohl für Linux- als auch Windows-Systeme zur Verfügung.

schiedliche Protokolle zur Verfügung. Zum einen enthält RHEV das plattformunabhängige VNC-Protokoll sowie das aus der Windows-Welt bekannte RDP-Protokoll. Beide Protokolle haben den Nachteil, dass Sie ursprünglich nicht für den Einsatz in heutigen Multimedia-Landschaften entwickelt wurden. So ist beispielsweise die Übertragung von Media-Streams ein großes Problem, auch bidirektionale Protokolle, wie sie unter anderem bei Voice-over-IP-Anwendungen zum Einsatz kommen, sind problematisch. Nahezu unmöglich ist der Anschluss externer Hardware an den lokalen Rechner, beispielsweise PDAs oder USB-Sticks, so dass diese dann im virtuellen Desktop zur Verfügung steht.

All diese Probleme verspricht das relativ neue SPICE-Protokoll (Simple Protocol for Independent Computing Environments) zu lösen. Bei SPICE handelt es sich ebenfalls um ein plattformunabhängiges Protokoll, welches ursprünglich von Qumranet entwickelt wurde. Im September 2008 übernahm Red Hat die Firma und stellte im Dezember 2009 das Protokoll unter eine Open Source-Lizenz [9]. SPICE besitzt eine mehrschichtige Architektur, bestehend aus einem Treiber, Server und einem Client. Der Treiber ist dabei innerhalb des virtuellen Desktops zu installieren. Hierbei kann es sich um einen Red Hat Enterprise Linux-Desktop oder Windows XP handeln. Beim Server handelt es sich um ein Virtual Desktop Infrastructure (VDI)-Gerät im Hostsystem. Genau genommen wird hierbei ein QXL PCI-Gerät emuliert. Der Endbenutzer kann dann mit Hilfe einer Clientanwendung eine Verbindung zum RHEV-M aufbauen. Für den Zugriff steht eine dedizierte Client-Anwendung sowie ein Plug-In für Mozilla-basierte Browser zur Verfügung.

Innerhalb des RHEV-M existiert ein sogenannter "Connection Broker". Dieser regelt den Zugriff auf die einzelnen Desktop-Systeme. Meldet sich ein Benutzer am Virtualization-Manager an, so erfragt der Connection Broker für diesen Benutzer ein Security-Token aus dem Active Di-

rectory. Anhand der darin enthaltenen Informationen entscheidet der Connection Broker, ob der Benutzer Zugriff auf einen dedizierten Desktop oder einen Desktop-Pool bekommt. Bei Letzterem teilen sich mehrere Benutzer die gleiche virtuelle Maschinen-Instanz. Die Entscheidung darüber, welcher Benutzer Zugriff auf welche Art von Desktop bekommt, fällt beim Einrichten der virtuellen Maschine. Hierbei ist als zusätzliche Eigenschaft für dieses System festzulegen, welcher Benutzer oder Gruppe von Benutzern auf diesen Desktop zugreifen darf.

Fazit

RHEV stellt eine umfangreiche Umgebung zur Virtualisierung von Linux- und Windows-Systemen bereit. Dank SPICE existiert erstmals eine vielversprechende Lösung auch zur Virtualisierung von Multimedia Desktop-Systemen. Auch was die Konfiguration, Verwaltung und den Zugriff auf die Desktop-Systeme anbelangt, bietet RHEV einen bisher im Linux-Umfeld nicht gewohnten Komfort. (jip)

- [1] Red Hat Enterprise Virtualization
www.redhat.com/virtualization/rhev/
- [2] Kernel-based Virtual Machine
www.linux-kvm.org/page/Main_Page/
- [3] SPICE-Protokoll
www.redhat.com/virtualization/rhev/desktop/spice/
- [4] JBoss Enterprise Middleware
www.redhat.com/jboss/
- [5] Bonding-Dokumentation im System
[/usr/share/doc/kernel-doc-version/Documentation/networking/bonding.txt](http://usr/share/doc/kernel-doc-version/Documentation/networking/bonding.txt)
- [6] Kernel Samepage Merging
www.linux-kvm.com/content/using-kvm-kernel-samepage-merging-kvm/
- [7] Red Hat Network System Management
www.redhat.com/red_hat_network/
- [8] Microsoft Knowledge Base Artikel zu Sysprep
<http://support.microsoft.com/kb/302577/de/>
- [9] SPICE-Projektseite
www.spice-space.org

Links





Virtuelle Maschinen mit dem Citrix Provisioning Server warten (1) Systeme am laufenden Band

von Christian Knermann

Mit zunehmendem Standardisierungsgrad und steigenden Benutzerzahlen stellt sich Administratoren von Terminalservern wie auch von virtuellen Desktops gleichermaßen eine zentrale Herausforderung: Eine große Anzahl physischer oder auch virtueller Maschinen ist konsistent zu pflegen. Neben klassischer Softwareverteilung empfiehlt sich der Citrix Provisioning Server, diese Aufgaben zu lösen. In dieser Workshopserie zeigen wir Ihnen anhand der Bereitstellung mehrerer Windows-Server von einem Image die Funktionsweise des Werkzeugs.



Quelle: Phoenixpix - Fotolia.com

Die grundlegende Funktionalität des Citrix Provisioning Server (CPS) basiert auf einer als "Disk Streaming" bezeichneten Technik. Beim Streaming booten physische und virtuelle Maschinen nicht von einer lokalen Festplatte, sondern von einem zentral bereitgestellten Image. Welches Image eine Maschine bootet, wird anhand der MAC-Adresse auf dem CPS festgelegt. Bevor wir detaillierter auf die Funktionalität eingehen, machen wir uns zunächst mit einigen Begriffen im Zusammenhang mit dem CPS vertraut (Bild 1).

Bestandteile des Provisioning Server

Die Farm bildet die höchste Ebene der Verwaltung für ein oder mehrere Provisioning Server. Es handelt sich bei dieser Farm um eine separate Verwaltungseinheit, nicht zu verwechseln mit dem Begriff der Farm im Zusammenhang mit XenApp oder XenDesktop. Eine Farm benötigt eine Datenbank und einen Lizenzserver. Im Lieferumfang ist der Microsoft SQL Server Express enthalten. Natürlich lässt sich stattdessen auch eine Datenbank auf einem separaten SQL Ser-

ver nutzen. Der Provisioning Server kann sich dabei den Datenbank-Server mit XenApp- und XenDesktop-Farmen teilen, benötigt aber in jedem Fall eine eigene Datenbank auf diesem Server. Auch der Lizenzserver kann gleichermaßen CPS sowie XenApp und XenDesktop versorgen. Hier setzen alle Produkte inzwischen auf das Citrix Licensing auf.

Innerhalb einer Farm finden sich ein oder mehrere Sites. Diese gruppieren wiederum einzelne Provisioning Server, vDisk Pools, Device Collections mit Target Devices und Views. Die Gruppierung kann dabei nach Standort oder logisch nach Anwendungszweck erfolgen. Bei einem Store handelt es sich um einen logischen Bezeichner für den physischen Ablageort von vDisks. Dieser lässt sich der kompletten Farm oder einer Site zuordnen. Neben der lokalen Festplatte eines CPS kommen CIFS-Freigaben oder auch anderweitige NAS-/SAN-Lösungen in Betracht.

Bei einem Target Device handelt es sich um eine physische oder virtuelle Maschine, die über den CPS von einem Image bootet. Views können auf Farm-Ebene oder pro Site definiert werden. Sie erlauben die logische Gruppierung von Target Devices, welche mehreren Views zugeordnet werden können, da es sich letztlich nur um eine Ansicht zur vereinfachten Verwaltung handelt. Gleichartige

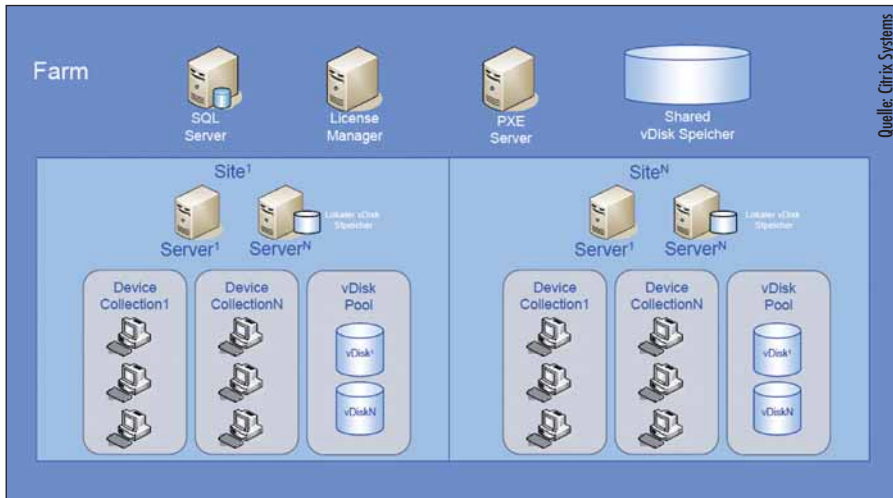


Bild 1: Organisationsstruktur einer Provisioning Server Farm

Target Devices werden in einer Device Collection zusammengefasst. Ein Target Device kann im Gegensatz zu den Views nur einer Collection zugeordnet werden.

Das Boot-Image für ein oder mehrere Target Devices wird als vDisk im Store bereitgestellt. Hierbei kommt das Microsoft Virtual Hard Disk (VHD)-Format zum Einsatz. Somit ist es möglich, die vDisk beispielsweise mit Tools wie "VHD Mount" aus dem Lieferumfang des Microsoft Virtual Servers oder "VHD Resizer" [1] zu bearbeiten. Beim Anlegen einer vDisk kann deren Größe als "Fixed" oder "Dynamic" konfiguriert werden. Im ersten Fall wird sofort der komplette angegebene Speicherplatz belegt, die zweite Option lässt die vDisk dynamisch bis zur maximalen Größe anwachsen. Dies spart Speicherplatz, muss aber auch mit Bedacht eingesetzt werden, da damit das Überbuchen des tatsächlich verfügbaren Platzes möglich ist. Die vDisks werden jeweils in einem vDisk-Pool pro Site zusammengefasst. Ein Pool kann dabei auf mehrere Speicherorte verweisen.

Zusammenspiel der Komponenten

Neben den zuvor beschriebenen Elementen wird in der Regel ein DHCP-Server benötigt, denn die Target Devices booten nicht von einem lokalen Medium, sondern über das Netzwerk und la-

den das Boot-Programm, das via TFTP bereitgestellt wird. Dabei kann wahlweise ein separater TFTP-Server oder der entsprechende Dienst des Provisioning Servers zum Einsatz kommen. Die Adresse des TFTP-Dienstes kann den Target Devices auf verschiedene Weise bekannt gegeben werden, im einfachsten Fall durch Verwendung der DHCP-Optionen 66 und 67 im entsprechenden Adress-Bereich (die Option 66 enthält IP-Adresse oder Hostnamen des TFTP-Servers, Option 67 den Dateinamen des Boot-Programms. Im Fall des Provisioning Servers lautet dieser *ARDBP32.BIN* [2]). Ein Nachteil dieser Konfiguration ist allerdings, dass die Option 66 nur auf einen TFTP-Server verweisen kann. Soll durchgängige Redundanz der Infrastruktur gewährleistet werden, müssten entsprechend zwei TFTP-Server geclustert werden. Als Alternative bietet der Provisioning Server den heute weniger gebräuchlichen BOOTP-Dienst oder PXE Boot. Letzteres beherrschen in der Regel alle aktuellen Netzwerkkarten inklusive der virtuellen Adapter der gängigen Virtualisierungslösungen.

Der Boot-Code wird vom Target Device geladen und veranlasst dieses wiederum, Kontakt mit dem Provisioning Server aufzunehmen. Dieser identifiziert das Target an Hand seiner MAC-Adresse und weist

ihm die gewünschte vDisk zu. Das Target bootet anschließend von der vDisk über das Netzwerk. Anders als der Begriff "Streaming" vielleicht impliziert, wird die vDisk also nicht auf das Target Device heruntergeladen – entsprechend ist keine lokale Festplatte erforderlich. Möglich macht dies ein spezieller Festplatten-Treiber, der dem Betriebssystem die über das Netz verbundene vDisk als lokales Medium präsentiert. Im Hintergrund kommuniziert der Treiber mit dem CPS über ein proprietäres Protokoll auf Basis von UDP. Diese Technik arbeitet also ähnlich iSCSI, allerdings mit dem signifikanten Unterschied, dass nicht ein bereits bestehendes Protokoll in eine IP-Verbindung verpackt wird, sondern das Protokoll von vornherein für den Netzwerkeinsatz entwickelt wurde. Entsprechend arbeitet der Provisioning Server effizienter mit geringerem Protokoll-Overhead bezogen auf die Nutzlast.

Ein weiterer Vorteil besteht darin, dass das Protokoll des Provisioning Servers sich tolerant gegenüber Netzwerkstörungen und -ausfällen verhält. Geht während eines Boot-Vorgangs oder im laufenden Betrieb die Verbindung verloren, so führt dies nicht zu einem Absturz der Target Devices. Diese bleiben stattdessen stehen und laufen weiter, sobald die Verbindung wiederhergestellt ist. Für den produktiven Einsatz im Unternehmen würde dies natürlich nichtsdestotrotz eine Betriebsunterbrechung bedeuten, denn die Targets sind auf eine kontinuierliche Verbindung zum CPS angewiesen. Dieser stellt somit einen "Single Point of Failure" dar, kann aber redundant ausgelegt werden, wie wir im Folgenden sehen werden.

Workshop-Szenario

Im Rahmen dieses Workshops möchten wir mehrere Windows Server 2003 R2 mittels CPS von einem gemeinsamen Image starten. Dabei bauen wir auf eine bestehende Windows Domäne mit folgenden Serverrollen auf:

- Zwei Windows Server 2008, eingesetzt als Active Directory Domain Controller.

- Zwei Windows Server 2003 R2, eingesetzt als SQL Server 2005 Cluster.
- Ein Fileserver mit der Möglichkeit, Speicherplatz als CIFS-Freigabe oder via iSCSI bereitzustellen.
- Drei Virtualisierungshosts, installiert mit dem Citrix XenServer 5.5 und den Citrix Essentials for XenServer in der Enterprise Edition. Die Hosts bilden einen Pool, beziehen ihr Storage Repository für die virtuellen Maschinen via iSCSI, die ISO-Images der Installationsmedien werden per CIFS-Freigabe verbunden.
- Eine virtuelle Maschine als DHCP-Server unter Windows Server 2003 R2, abgesichert über den HA-Modus der XenServer.

Auf einem der DC installieren wir zusätzlich das Citrix Licensing 11.6.1. Anschließend fügen wir eine Lizenz der Essentials pro XenServer hinzu. Letztere erlauben in der Enterprise Edition, auf jedem entsprechend lizenzierten XenServer beliebig viele Target Devices per Provisioning Server zu versorgen. Legen Sie im AD zunächst den neuen Domänenbenutzer "ctx_provisioning" an. Auf dem Datenbank-Server erzeugen Sie unter "Datenbanken" die neue Datenbank "Citrix-Provisioning" und unter "Sicherheit / Anmeldungen" eine neue Anmeldung für den zuvor erstellten Benutzer. Dem Benutzer wird die neue Datenbank als Standard zugewiesen. Unter "Datenbanken / Citrix-Provisioning / Sicherheit / Benutzer" le-

gen Sie auf der Datenbank den Benutzer "ctx_provisioning" an, welcher der gleichnamigen Anmeldung zugeordnet ist und die Datenbankrolle "db_owner" erhält.

Installation


Auf den XenServern nehmen Sie nun zwei virtuelle Maschinen namens PVS01 und PVS02 mit jeweils zwei virtuellen CPUs, 2 GByte RAM und 15 GByte großer virtueller Disk in Betrieb. Diese installieren Sie mit dem Windows Server 2003 R2 inklusive Service Pack 2 und allen aktuellen Updates. Anschließend nehmen Sie Ihren Domänen-Benutzer "ctx_provisioning" in die lokale Gruppe der Administratoren auf, entpacken das ZIP-Archiv der Citrix Provisioning Services 5.1 SP2 und starten die Installation der Server-Dienste für die 32-Bit-Plattform. Die Installation selbst ist denkbar schnell erledigt. So akzeptieren Sie die Lizenzbedingungen sowie den Standard-Pfad und entscheiden sich mit der Option "Complete" für alle Komponenten.

Nach erfolgreicher Installation startet automatisch ein Wizard zur Konfiguration. Diesen durchlaufen Sie zunächst auf dem Host PVS01. Die erste Frage gilt den DHCP-Diensten und Sie wählen "The service that runs on another computer". Im folgenden Dialog zum PXE-Boot entscheiden Sie sich für die Option "The service that runs on this computer (Provisioning Services PXE Service)". Da es sich um unseren ersten Provisioning Server handelt, aktivieren Sie im nächsten Dialogschritt den Punkt "Create farm" und wählen daraufhin aus der Dropdown-Box unseren SQL Server-Cluster. Anschließend wählen Sie Ihre Datenbank "CitrixProvisioning" aus und geben als Farm Namen "PVS-Farm" an. Im gleichen Dialog bietet sich die Mög-

lichkeit, eine erste Site und Device Collection zu erzeugen, in unserem Fall "Oberhausen" und "Test-Server".

Bei der Frage nach dem Lizenzierungsdienst können Sie auf Ihren DC verweisen. Sie definieren weiterhin Ihren Domänen-Benutzer "ctx_provisioning" als Konto für den Stream Service. Die Verwendung eines Domänen-Benutzers an dieser Stelle ermöglicht zum einen, eine CIFS-Freigabe als Speicherort für die vDisks zu verwenden, sofern der entsprechende Account Vollzugriff auf diese Freigabe hat. Zum anderen ist der Account nötig zur Windows-Authentifizierung am SQL Server. Entsprechend aktivieren Sie auch die Option "Configure the database for the account".

Da die VM in unserem Beispiel nur über einen virtuellen Netzwerkadapter verfügt, bleibt im nächsten Dialog zur weiteren Konfiguration der Stream Services nichts zu tun. Akzeptieren Sie entsprechend die Standardvorgaben. Auch im folgenden Schritt belassen Sie es beim Standard – "Use the Provisioning Services TFTP service". Zu guter Letzt bleibt nur, die Liste der möglichen Boot-Server zu füllen. Neben Ihrem frisch installierten Provisioning Server fügen Sie hier zusätzlich die IP-Adresse Ihres zweiten Systems PVS02 hinzu. Anschließend führen Sie auch auf dem Server PVS02 den Wizard zu Ende, wählen dort aber "Join Existing Farm". So gerüstet können Sie mit der Konfiguration erster vDisks und Target Devices beginnen.

Im nächsten Teil unserer Workshopserie beschäftigen wir uns mit Konfiguration und Betrieb des CPS sowie seiner Integration ins Active Directory. (jp) 

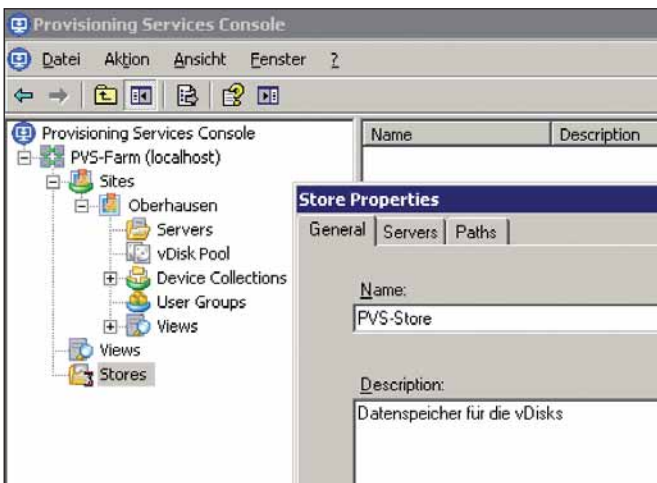


Bild 2: Die Konfiguration erfolgt über die Provisioning Services Console

- [1] VHD Resizer
<http://vmtoolkit.com/files/folders/converters/entry87.aspx>
- [2] How to Add DHCP PXE Options to Microsoft DHCP Server
<http://support.citrix.com/article/CTX115094/>

Links 



Ansatz zur Punktlandung

von Thomas Bär

Die SharePoint-Technologie gilt innerhalb des Microsoft-Konzerns nach Office und Windows als das dritterfolgreichste Produkt im Portfolio. Einst war der Start des zentralen Intranet-Servers von Microsoft eher holperig. Nun, kurz vor dem Veröffentlichungstermin von SharePoint 2010, liegen uns erstmals handfeste Informationen aus einem Test der Beta-Version vor. IT Administrator fasst für diesen Beitrag die wichtigsten Ergebnisse zusammen. Die Quintessenz: An der aktuellen Version holpert höchstens noch die Hardware.

In der Vergangenheit hat Microsoft SharePoint mehrfach unbenannt. Nach einigen Entwicklungszyklen blieben zwei Namen bestehen: Microsoft SharePoint Server und Microsoft SharePoint Services. Die SharePoint Services, aktuell in Version 3.0 mit SP2, sind eine kostenfreie Erweiterung für Windows Server ab der Version 2003. Das primäre Augenmerk der SharePoint Services liegt darin, innerhalb des Unternehmensnetzwerks Intranet-Seiten zu betreiben, die in Microsoft Office integriertes Teamworking ermöglichen. Die SharePoint Services bieten dazu verschiedene Hilfsmittel wie Online-Diskussionen, Team-Webseiten, Wikis, eine gemeinsame Dateiablage mit Revisionen, Adressverzeichnisse und eine Ablaufsteuerung auf Basis der Microsoft Workflow Foundation.

Der Microsoft SharePoint Server, künftig in der Version 2010 (SPS 2010), ist eine Erweiterung der SharePoint Services zur Abbildung von Business-Anforderungen auch für externe Einsatzgebiete. Die Oberflächen und Funktionalitäten der SharePoint Services und des großen Bruders, des SharePoint Servers, überschneiden sich in vielen Dingen und bilden eine einheitliche Infrastruktur mit hohem Wiedererkennungsfaktor: Interaktion, Kommunikation und gleichzeitiges Arbeiten mit Kollegen und Partnern über das Web mit den Schwerpunkten



Sites, Communities, Content und Suchen. Modernere Funktionalitäten wie Insights – der Kreuzanalyse von Suchdaten und Composites – und die Möglichkeit, mit SharePoint ohne die Eingabe von Quellcode Collaboration-Lösungen zu entwickeln, sind Neuerungen mit der aktuellen Server-Version.

Hohe Systemanforderungen

Wer bis dato eher nebenbei auf einem Server für verschiedene Teamfunktionen die SharePoint Services hat mitlaufen lassen, der wird sich über die Hard- und Softwareanforderungen des SPS 2010 wahrlich wundern, denn nebenbei macht eine solche Maschine überhaupt nichts mehr. Ein Windows Server 2008 mit Service Pack

2 oder Windows Server 2008 R2 in der Standard- oder Enterprise-Ausprägung steht ganz oben auf der Soll-Liste. Windows 7 ist für Evaluationen ebenfalls ausreichend, jedoch ist in diesem Fall der Installationshelfer für die Softwareanforderungen nicht in der Lage, die benötigten Updates automatisch zu installieren.

Dass es sich dabei ausschließlich um x64-Maschinen handeln darf, versteht sich beinahe von selbst. Während einige Webseiten noch von einem Dual-Core-Prozessor mit mindestens 3 GHz Taktfrequenz berichten, erhöht sich die Forderung auf aktuellen Microsoft-Seiten auf mindestens vier Prozessorkerne. Außerdem sollte die Maschine in Test- und Entwicklungsze-



narien über 4 GByte Arbeitsspeicher verfügen. Produktiv-Servern verlangen die Entwickler aus Redmond eine Ausstattung von 8 GByte RAM oder höher ab. Datenbank-seitig ist der SPS 2010 in der Lage, mit einem aktualisierten Microsoft SQL 2005 oder Microsoft SQL 2008 zusammenzuarbeiten. Für Test- und Entwicklungsumgebungen ist ein SQL-Server in der Express Edition ausreichend. Eine Partition mit rund 80 GByte Kapazität stellt für die Installation und die ersten Anwenderdaten die Einstiegsgröße dar. Je nach verwendeter Datenbank ist nach oben hin so schnell kein Limit zu erreichen.

Wie seine Vorgänger bietet auch die aktuellste Version die Möglichkeit, als einzelstehendes System mit eigener Datenbank zu agieren oder in einem Verbund von Servern, die durch verschiedene Webserver entlastet werden. Im Testlabor haben wir einen Windows Server 2008 SP2 unter Windows 7 mithilfe VMware Workstation 7 virtualisiert und mit vier virtuellen Prozessorkernen ausgestattet. Zunächst stellten wir dem System versuchsweise lediglich 1 GByte zur Verfügung, da uns die 4 GByte-Anforderung als unrealistisch hoch erschienen. Kommen allerdings weniger als

3 GByte Arbeitsspeicher zum Einsatz, dann starten diverse Dienste nicht rechtzeitig und es hagelt Fehlermeldungen. Ein Blick auf den Task-Manager spricht eine deutliche Sprache: Besonders direkt nach der Installation sind offenbar zahlreiche Optimierungs-Prozesse aktiv. Erst nach wenigen Minuten kommt die Software zu Ruhe und erzeugt eine verträgliche Grundlast von rund drei Prozent der Prozessorleistungen.

Ein halber Tag für Installation und Konfiguration

Für die Installation des Servers mit allen Service Packs und allen Systemvoraussetzungen sind mindestens zwei Stunden nötig. Wer dann noch die ersten Konfigurationsschritte wie ein automatisiertes Backup oder die Einbindung an den Mailserver vornehmen will, kann gleich einen halben Arbeitstag für die Vorbereitungen einplanen. Die Installation selbst ist kein Hexenwerk. Es gilt nur, die aktuelle Beta mit rund 550 MByte Umfang aus dem Internet zu laden, sich nicht über den Namen "Office Server" zu wundern und die Datei mit einem Doppelklick zu starten. Steht ein Windows Server 2008 (R2) für die Installation bereit, so lädt die Setup-Routine alle erforderlichen zu-

sätzlichen Komponenten automatisch herunter und installiert diese. Diese lassen sich aber auch einzeln herunterladen. Sind alle Voraussetzungen erfüllt, beginnt die eigentliche Installation mit Hilfe eines Assistenten. Der Vorgang ähnelt sehr stark dem des Vorgängers. Am Ende des Installationsvorgangs und einen Neustart später öffnet sich die Hauptseite. Diese ist bei der Beta-Version bereits mit einigen Demodaten der imaginären Firma "Adventure Works" gefüllt. Der Link zur Zentraladministration auf dem Server findet sich nun nicht mehr im Menü "Verwaltung", sondern in einem eigenen Zweig namens "Microsoft SharePoint 2010 Products". Hieraus lässt sich zudem die Verwaltungskonsole aufrufen, hinter der sich die aktuelle PowerShell 2 verbirgt. Alle Anwendungseinstellungen, Sicherungs- und Wiederherstellungsaufträge, Upgrade- und Migrationsvorhaben oder Anpassungen der Systemeinstellungen nimmt der Nutzer wie gewohnt über die Webseite der Zentraladministration vor, die insgesamt aufgeräumter wirkt. Ein Konfigurations-Assistent, symbolisiert durch einen mit Sternen umgebenen Zauberstab, unterstützt beim Aufbau einer SharePoint Server-Farm.

Die Neuerungen: Ribbons und Multimedia

Die augenscheinlichste Änderung, die dem wiederkehrenden Benutzer ins Auge sticht, ist die überarbeitete Benutzeroberfläche. Die mit Microsoft Office 2007 eingeführte und von vielen Umsteigern zunächst nicht sonderlich geschätzte Ribbon-Technik hält nun auch bei SPS 2010 Einzug. Durchgängig auf allen Webseiten, von der Zentraladministration bis hin zu den Anwendungen – allorten zeigt sich SharePoint im neuen Gewand. Auf Wunsch der Anwender lassen sich die Ribbons anpassen, mit eigenen Funktionen erweitern oder komplett ausschalten.

Die Anpassung von Oberfläche und Ribbons wurde in der aktuellen Version noch einmal deutlich vereinfacht. Der An-

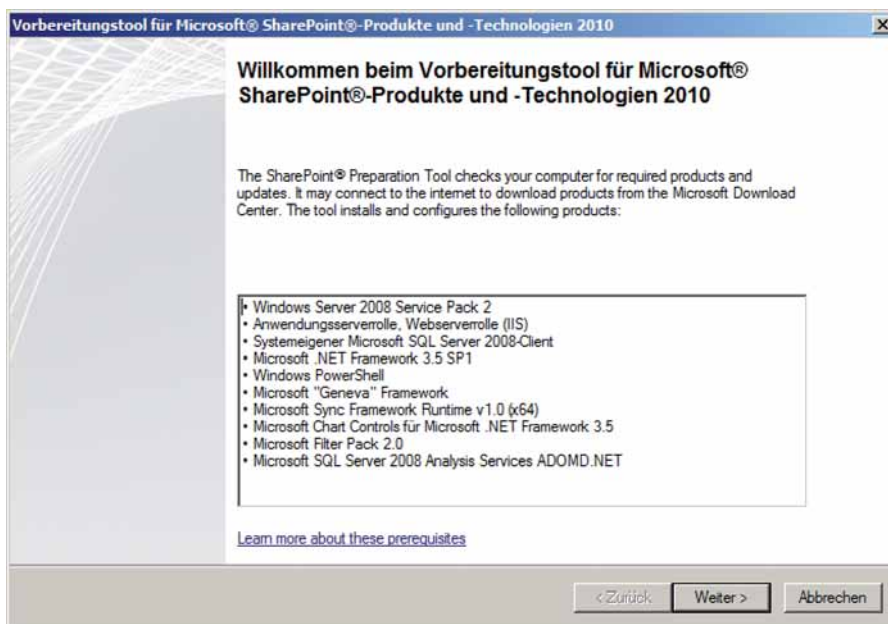


Bild 1: Der aktuelle SharePoint Server verlangt in der Beta-Version nach diversen Technologien, die auf vielen Installationen kaum vorhanden sein dürften. Glücklicherweise unterstützt ein Installationsassistent den Administrator.

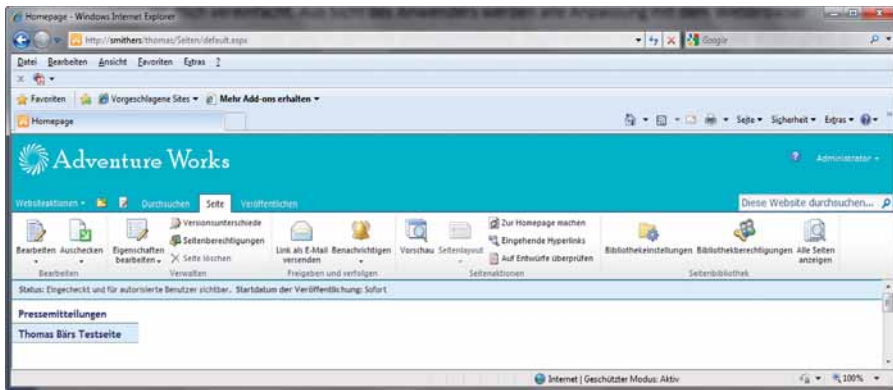


Bild 2: Alle Änderungen an Seiten oder Inhalten werden über benutzerspezifisch anpassbare Ribbons vorgenommen

wender nimmt alle Modifikationen mit dem Webbrowser vor, fast alle Funktionen sind selbsterklärend. Trotzdem sollten Nutzer den Inhalt einer Webseite erst einmal aufmerksam durchlesen, ehe hastig irgendwohin zu klicken. Glücklicherweise ist der Wiedererkennungswert hoch: Wer schon einmal mit einer Vorgängerversion gearbeitet hat, der wird sich zügig zurechtfinden. Zumindest für Anwender ist eine separate Schulungsmaßnahme kaum erforderlich.

Silber- und Mondlicht sind Pflicht

Sobald mehr als eine Auflistung auf einer Website dargestellt werden soll, beispielsweise ein Video-Clip, macht SPS 2010 höflich, aber bestimmt darauf aufmerksam, dass nun der Zeitpunkt gekommen ist, den eigenen PC mit "Silverlight" auszustatten. Die kostenlose Erweiterung des Webbrowser, eine direkte Konkurrenz zu Adobe Flash, bietet Microsoft derzeit für Windows und Mac OS an. Für Linux wird, von Novell und von Microsoft unterstützt, "Moonlight" angeboten. Es ist empfehlenswert, bereits im Vorfeld Client-Computer und Terminalserver mit der aktuellen Version Silverlight 3 auszustatten, um den vollen Funktionsumfang von SharePoint nutzen zu können.

Demo-Firma veranschaulicht Funktionalität

Bei der Installation der Beta-Version des SPS 2010 finden automatisch die Demodaten von "Adventure Works" den Weg auf die Festplatte. Öffnet der An-

wender die Hauptseite, so gelangt er automatisch auf diese Webseite. Die Demodaten der imaginären Firma sind nicht nur für den ersten Blick auf die generellen Funktionalitäten des SharePoint's interessant, viele Funktionen lassen sich direkt über die Inhalte anpassen. So heißt der erste Punkt auf der Homepage beispielsweise "Anonymen Zugriff aktivieren". Dass der anonyme Zugriff auf die aktuelle Website-Sammlung zunächst durch einen Administrator aktiviert werden muss, ergibt sich aus dem Folgetext – mit einem Klick auf den Link ist der administrativ berechtigte Benutzer sofort in der Lage, diese Funktion zu aktivieren. Ähnlich geht es bei anderen Aufgaben weiter, beispielsweise dem Ändern von Navigationslinks, dem Anpassen des Designs über den Gestaltungsvorlagenkatalog, dem Einrichten des Supports für mehrere Sprachen, Änderungen am Seitenlayout oder der Struktur- und Inhalts-Verwaltung.

Schnellere Anpassungen bei Inhalt und Design

Mit den Ribbons hat Microsoft das sogenannte "Web Edit" integriert. Hiermit lassen sich Inhalte wie Texte, Bilder

oder Webparts auf einer SharePoint-Webseite mit wenigen Mausklicks modifizieren. Anpassungen in den Unternehmens-Wikis in Bezug auf Aussehen, Größe und Position von Grafiken sollen im Vergleich zum Vorgänger so deutlich einfacher gestaltet werden. Für Webdesigner wurde die Erstellung von Design-Vorlagen, die sogenannte Theming-Technologie, komplett überarbeitet. Themes zeigt SPS 2010 in einer Vorschau "live" an und kann sie darüber hinaus aus dem kommenden PowerPoint 2010 importieren.

Das Zusammenspiel des kostenlos als optionale Software zu installierenden SharePoint Designers 2010 und dem SharePoint Server soll laut Microsoft auch im Bereich der Workflow-Erstellung, der Applikationsdefinition und der Administration eine deutliche Aufwertung erfahren haben. Die aktuell verfügbare Version des SharePoint Designers reagiert beim Versuch, eine SharePoint-Seite direkt zu bearbeiten, mit einem Fehlerdialog. Neben der angenehmen Aktualisierung des Designs, welches nun wie aus einem Guss zu anderen Microsoft-Programmen passt, fällt eine Veränderung im Seitenaufbau auf: Während die Vorgängerversionen stets die komplette Seite geladen haben, so ist der Aufbau der Oberfläche nun asynchron.

Office wandert weiter ins Web

Die Möglichkeit, Programme aus dem Microsoft Office-Umfeld innerhalb eines Web-Browsers laufen zu lassen, ist ein wesentlicher Bestandteil der Web 2.0-Komponenten von SPS 2010. Die Arbeitsumgebungen auf IT-Basis verlagern sich zunehmend ins Internet. Der SharePoint Server ist für diesen Trend die

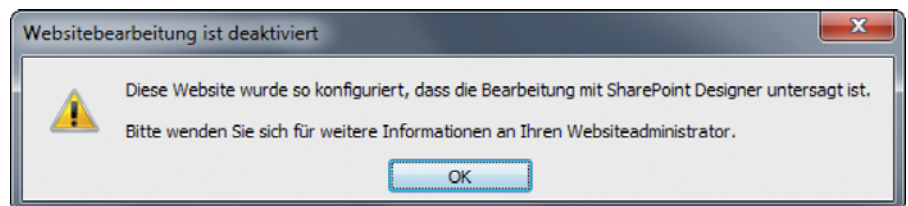


Bild 3: Die Zusammenarbeit mit dem derzeit verfügbaren SharePoint Designer 2007 funktioniert auf Anhieb nicht

unternehmensbezogene Antwort von Microsoft. Word, Access und Excel ließen sich bereits schon in der 2007er-Version des SharePoint Servers als Webseite nutzen. Die neuen Microsoft Visio Services bieten ein Echtzeit-Rendering von Visio Daten direkt im Webbrowser und die Option, Daten aus verschiedenen Systemen grafisch aufzubereiten.


Microsoft positionierte SharePoint stets als Lösung, um Line-of-Business-Anwendungen (LOB) zu integrieren oder Business-Workflows direkt mit dem System abzubilden. Einerseits haben die Redmonder den einstigen "Business Data Catalog" in die "Business Connectivity Services" umbenannt. Andererseits haben Sie den SharePoint Designer 2010 und Microsoft Visual Studio 2010 für die Integration von Backend-Systemen vorbereitet. Externe LOB-Anwendungen lassen sich so wie einfache Listen in SharePoint-Seiten einbinden und bearbeiten. Die Hauptanwendung, die im Gespann mit SharePoint 2010 am meisten profitiert, heißt wie bisher Microsoft Office. Schon bei den Vorgängerversionen war es stets so, dass das aktuellste Office-Paket von Microsoft am besten mit dem neuesten SharePoint zusammenarbeitet.

Neuerungen für Administratoren

Was die Bereitstellung angeht, so hat Microsoft zu Gunsten der Administratoren schon einiges unternommen, wie der an sich einfache Installationsvorgang zeigt. Die Zentraladministration erscheint subjektiv betrachtet übersichtlicher und die Fenster unterscheiden sich etwas deutlicher in ihrer Gestalt. Hilfetexte und kontextbasierte Funktionen erleichtern die Arbeit mit dem neuen SharePoint. Upgrade-Wilige können sich über ein neues Feature, den so genannten "Visual Upgrade", freuen. Wer einen SharePoint Portal Server 2003 nach SharePoint 2010 aktualisiert, hat die Möglichkeit, das Look and Feel der Ursprungsversion zu übernehmen. Das macht Nutzern den Umstieg deutlich leichter.

Eigentlich soll der SharePoint die Notwendigkeit des Einsatzes von Entwicklern reduzieren und Endanwendern die Möglichkeit geben, viele Abläufe einfach selbst zu erstellen. Während Microsoft die Administratoren stets mit den notwendigen Funktionen bedacht hat, so hatten es Entwickler mit den früheren Versionen nicht gerade leicht. Neben der insgesamt einfacheren Anpassung an die eigenen Bedürfnisse wurden deshalb in Visual Studio 2010 einige Projektvorlagen für den SharePoint inklusive Workflows, visuelle Webparts und Assistenten integriert.

Fazit

Das Fazit ist kurz und knackig: Er sieht gut aus, der neue SharePoint Server 2010. Sowohl für den Anwender als auch für Administratoren und Entwickler hat Microsoft viel getan, um Bedienung und Verwaltung zu erleichtern und noch besser an Web-2.0-Erfordernisse anzupassen. Preisinformationen lassen allerdings aktuell noch auf sich warten. Wie genau die SharePoint Foundation als Nachfolger der Services aussehen wird, darüber halten wir Sie auf dem Laufenden. (In) 

[1] Größte deutschsprachige SharePoint-Community mit Blogs, User Groups und News
<http://sharepointcommunity.de>

[2] SharePoint 2010 verwalten I:
"Professional Sharepoint 2010 Administration"
von Todd Klindt, Shane Young und Steve Caravajal,
960 Seiten, ISBN-10: 0470533331

[3] SharePoint 2010 verwalten II:
"Microsoft SharePoint Server 2010
für Administratoren - Das Handbuch"
von Wojciech Micka, 900 Seiten,
ISBN-10: 3866451369

[4] 100-seitiges PDF/XPS-Dokument für Entwickler
www.microsoft.com/downloads/details.aspx?FamilyID=cffb14e8-88a9-43bd-87aa-4792ab60d320&DisplayLang=de

Links und Ressourcen



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

DNS-Probleme im Netzwerk beheben (2)

Ohne Umwege ans Ziel

von Thomas Joos



Quelle: Pixel - Fotolia.com

Fehlermeldungen in Windows-Netzwerken und -Anwendungen haben ihre Ursache oft in Problemen bei der Namensauflösung. Vor allem bei verschachtelten Strukturen kann es schnell geschehen, dass einzelne Rechner keine korrekte Auflösung durchführen können. Im ersten Teil unserer Workshopserie haben wir Ihnen gezeigt, wie Sie Fehler in DNS-Einstellungen finden und beheben. Im zweiten Teil widmen wir uns spezifischen Fällen wie DHCP, Firewalls und dynamischen IP-Adressen, bei denen eine Namensauflösung per DNS nicht mehr ohne Weiteres funktioniert. Dabei erfahren Sie, wo genau es oftmals hakt und wie Sie das Problem lösen.

Geben Clients oder Server die Meldung aus, dass sie den Domänencontroller nicht erreichen können, sollten Sie auf den beteiligten Computern zunächst per Ping testen, ob ein Aufruf der IP-Adresse des Servers funktioniert. Ist dies möglich, stellen Sie sicher, dass in den Netzwerkeinstellungen der Server die IP-Adresse eines DNS-Servers eingetragen ist, welcher den Domänencontroller auflösen kann. Auch auf den Domänencontrollern selbst müssen in den Netzwerkeinstellungen die DNS-Server so gesetzt sein, dass die Auflösung funktioniert.

So machen Sie den Domänencontroller ausfindig

Achten Sie in den erweiterten Netzwerkeinstellungen darauf, ob spezielle DNS-Suffixe gesetzt sind. Auch der Test mit `nslookup` zur Namensauflösung ist wichtig. Verwenden Sie den vollständigen DNS-Namen des aufzulösenden Servers (FQDN), stellen Sie sicher, dass das DNS-Suffix des Clients korrekt ist oder in den erweiterten DNS-Einstellungen der Netzwerkverbindung eingetragen ist. Haben

Sie diese Grundlagentests durchgeführt, aber die Auflösung funktioniert noch immer nicht, fehlen unter Umständen DNS-Einträge der Domänencontroller in den DNS-Zonen. Diese Einstellungen finden Sie unter “_msdcs” auf den DNS-Servern. Auf den Domänencontrollern kommen Sie solchen Fehlern am schnellsten auf die Schliche, wenn Sie `dcdiag` in der Befehlszeile eingeben. Überprüfen Sie zudem mit `nltest /dsgetsite`, ob der Domänencontroller dem richtigen Active Directory-Standort zugewiesen ist. Mit

```
nltest /dclist:{NetBios-Name der Domäne}
```

lassen Sie sich eine Liste aller Domänencontroller der entsprechenden Domäne ausgeben. Die Einträge sollten als FQDN aufgelistet sein. Daneben listet der Befehl

```
nltest /dsgetdc:{NetBios-Name der Domäne}
```

Name, IP-Adresse, GUID, FQDN des Active Directory und weitere Informa-

tionen auf. Alle Informationen sollten ohne Fehler angezeigt werden.

Bei Windows Server 2003 oder Windows 2000 Server können Sie DNS-Probleme mit `netdiag /fix` in der Befehlszeile beheben. Dabei verwendet das Tool den Inhalt der DNS-Daten aus der Datei `\windows\system32\config\netlogon.dns` und trägt diese wieder in das Active Directory ein. Bei Windows Server 2008 und R2 ist das Tool nicht nutzbar, da es kein Bestandteil des Betriebssystems mehr ist. Mit `dcdiag /fix` können Sie einige, aber längst nicht alle Probleme beheben. Netdiag lässt sich unter Windows Server 2008 zwar installieren, das Werkzeug startet aber nicht. Setzen Sie Windows Server 2008 R2 ein, können Sie im Server-Manager mit dem Best Practice Analyzer das Active Directory scannen und sich den Fehler mit Lösungsmöglichkeiten präsentieren lassen. Der gleiche Assistent existiert für die DNS-Rolle. Führen Sie für beide Rollen die Überprüfung aus.

Leider gibt es für Windows Server 2008 keine ähnlichen Werkzeuge. Starten Sie



```

Administrator: C:\Windows\system32\cmd.exe
Anfangssetup wird ausgeführt:
Der Homeseverer wird gesucht...
Homeseverer = WIN-RC04ST5TQ2T
* Identifizierte AD-Gesamtstruktur.
Sammeln der Ausgangsinformationen abgeschlossen.

Erforderliche Anfangstests werden ausgeführt.

Server wird getestet: Default-First-Site-Name\WIN-RC04ST5TQ2T
Starting test: Connectivity
Der Host 34df588f-a299-41ef-b5d4-a324eb1fe8ce._msdcs.contoso.com
konnte nicht zu einer IP-Adresse aufgelöst werden. Überprüfen Sie
DNS-Server, DHCP, Servername, usw.
Fehler beim Überprüfen der LDAP- und RPC-Konnektivität. Überprüfen Sie
die Firewall-Einstellungen.
..... WIN-RC04ST5TQ2T hat den Test Connectivity
nicht bestanden.

Primärtests werden ausgeführt.

Server wird getestet: Default-First-Site-Name\WIN-RC04ST5TQ2T
Alle Tests werden übersprungen, da der Server WIN-RC04ST5TQ2T nicht auf
Anforderungen des Verzeichnisdienstes reagiert.
  
```

Bild 1: Fehler in den DNS-Einstellungen des Active Directory finden
Sie am schnellsten per `dcdiag` auf den Domänencontrollern

mit `net stop netlogon` und dann `net start netlogon` den Anmeldedienst auf dem Domänencontroller neu. Beim Starten versucht der Dienst, die Angaben der Datei `netlogon.dns` erneut im DNS zu registrieren. Gibt es hierbei Probleme, finden Sie im Ereignisprotokoll unter "System" einen Eintrag des Dienstes, der bei der Problemlösung weiterhilft. Auch der Befehl `nltest /dsregdns` hilft oft bei Problemen in der DNS-Registrierung. Funktioniert die erneute Registrierung durch Neustart des Anmeldedienstes nicht, dann löschen Sie die DNS-Zone "_msdcs" und die erstellte Delegation ebenfalls. Starten Sie dann den Anmeldedienst neu, liest dieser die Daten von `netlogon.dns` ein, erstellt die Zone "_msdcs" neu und schreibt die Einträge wieder in diese Zone. Testen Sie anschließend erneut mit `dcdiag`, ob die Probleme behoben sind. Einen ausführlichen Test führen Sie mit `dcdiag /v` durch.

So klappt die Namensauflösung von Mitgliedsservern

Stellen Sie Probleme bei der Namensauflösung von Mitgliedsservern fest, lassen sich diese recht einfach beheben. Die Server müssen die richtigen DNS-Server in den Netzwerkeinstellungen eingetragen haben, außerdem muss ein Host A-Eintrag in der entsprechenden Zone gesetzt sein. Arbeiten Sie mit dynamischer DNS-Registrierung, achten Sie darauf, dass dynamische Aktualisierungen für die Zone in den Eigenschaften von DNS erlaubt sind. Vor allem wenn es sich um Server handelt, die nicht Mitglied einer Domäne sind, aber von Active Directory-DNS-Servern aufgelöst werden sollen, müssen Sie darauf achten, die entsprechenden Namenseinträge manuell zu setzen oder auch unsichere Aktualisierungen für die Zone in den Eigenschaften der Zone zu ermöglichen. Im laufenden Betrieb starten Sie mit dem Befehl `ipconfig`

`/registerdns` die dynamische Aktualisierung auf dem Mitgliedsserver. Starten Sie mit `net stop netlogon` und `net start netlogon` den Anmeldedienst neu, um sicherzugehen, dass die Aktualisierung funktioniert hat.

Integration von WINS in DNS

Seit Windows Server 2003 SP1 sind Erweiterungen in das Betriebssystem integriert, welche die Namensauflösung zur Replikation des Active Directory über WINS abwickeln können, falls DNS Probleme hat. Diese Verbesserungen sind in Windows Server 2008 R2 übernommen worden. Um WINS in DNS zu integrieren, müssen Sie die Eigenschaften der einzelnen Zonen im DNS öffnen. Dort können Sie auf der Registerkarte "WINS" die Option "WINS-Forward-Lookup" auswählen und die IP-Adresse eines WINS-Servers angeben. Richtet ein Client eine Anfrage an den DNS-Server, versucht dieser zunächst diese Anfrage über die lokalen Informationen in der DNS-Datenbank zu beantworten. Gelingt ihm das nicht, sendet er den Hostnamen an den WINS-Server. Dieser versucht, die Anfrage zu beantworten, und liefert gegebenenfalls das Ergebnis an den DNS-Server zurück.

Sie können in den einzelnen DNS-Zonen alle WINS-Server einrichten, um auch an dieser Stelle eine Ausfallsicherheit zu erreichen. Die Einstellungen tragen Sie für jede Zone auf den Servern ein. DNS speichert außerdem die WINS-Antwort in seinem Cache. Über die Schaltfläche "Erweitert" definieren Sie unter "Cachezeitlimit", wie lange ein Eintrag, der von einem WINS-

EBOOK
SYSTEMS

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



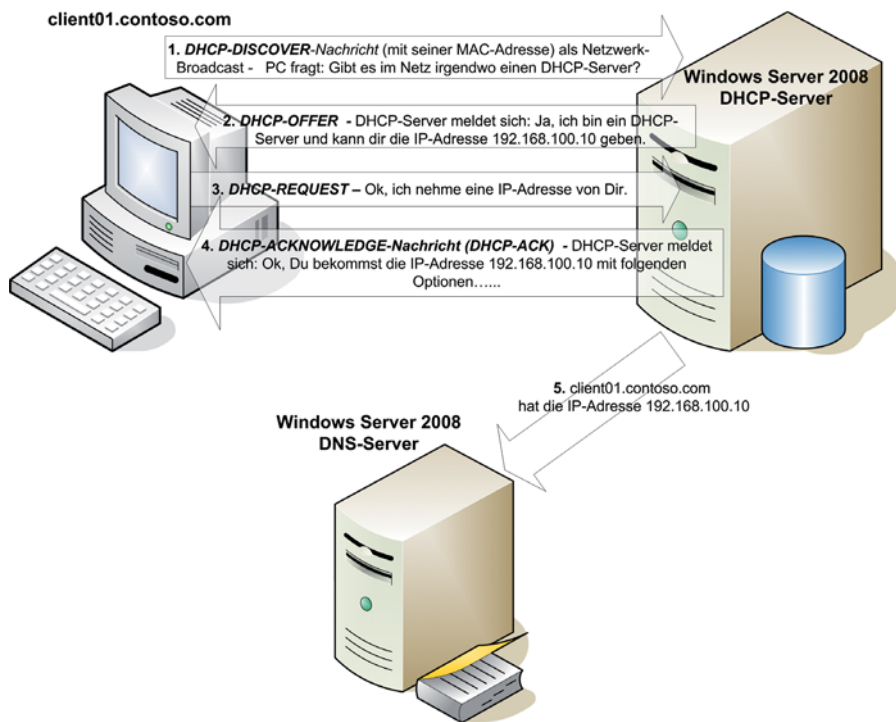


Bild 2: DHCP-Verbindungsablauf zusammen mit dynamischem DNS

Server geliefert wurde, im DNS-Cache verbleibt (Standard 15 Minuten) und wie lange der DNS-Server auf die Antwort eines WINS-Servers wartet, bevor er zum nächsten Server in der Liste übergeht (Standard 2 Sekunden). In der Standardeinstellung wird nach der Aktivierung des WINS-Lookup ein DNS-Eintrag generiert, über den sekundäre DNS-Server erfahren, dass ein WINS-Server zur erweiterten Abfrage bereitsteht. Durch diese Koppelung von WINS und DNS verbessert sich die Stabilität der Namensauflösung in einem Active Directory erheblich.

Stammhinweise setzen und Firewalls modifizieren

Findet der Server keinen DNS-Eintrag zu einem Client, leitet der Server die Anfrage an denjenigen Server weiter, der als Weiterleitungsserver für die Domäne hinterlegt ist. Sind keine Weiterleitungsserver konfiguriert, verwenden DNS-Server die DNS-Server, die auf der Registerkarte "Stammhinweise" in den Eigenschaften des DNS-Servers hinterlegt sind. Haben Sie auf dem Server allerdings eine Punkt-Zone "." angelegt, leitet der Server keinerlei Anfragen

an Stammhinweise weiter, die er nicht selbst auflösen kann. Haben Sie das Active Directory und die DNS-Infrastruktur zum Beispiel mit einem Assistenten installiert, legt dieser automatisch die Punkt-Zone an. Können Ihre DNS-Server keine Weiterleitungen durchführen, dann löschen Sie diese Punktezone und stellen sicher, dass Sie entweder Weiterleitungen konfiguriert haben oder die Server auf der Registerkarte "Stammhinweise" erreichbar sind.

Ein weiteres Problem kann darin liegen, dass der DNS-Server nicht bei allen eingebauten Netzwerkkarten und -Verbindungen auf Anfragen wartet. In den Eigenschaften des DNS-Servers finden Sie auf der Registerkarte "Schnittstelle" eine Auflistung aller IP-Adressen, bei denen der Server auf DNS-Anfragen wartet. Wollen Sie im Unternehmen sekundäre DNS-Zonen einsetzen, die nicht zwangsweise unter Windows installiert sein müssen, können Sie auf diesen Servern nur dann die Zonen übertragen, wenn Sie in den Eigenschaften der Zone auf dem primären DNS-Server auf der Registerkarte "Zonenübertragungen" diese Übertragung zu-

lassen. Standardmäßig verweigern Windows-DNS-Server eine solche Übertragung.

Ist zwischen verschiedenen DNS-Servern oder DNS-Server und Client eine Firewall positioniert, blockiert diese unter Umständen DNS-Abfragen. DNS-Server verwenden den TCP/UDP-Port 53, den Sie für DNS-Abfragen freischalten sollten. Gelingt der Verbindungsaufbau immer noch nicht, schalten Sie alle UDP-Ports oberhalb von 1023 in Zusammenhang mit dem DNS-Server frei. Ein häufiges Problem ist die Namensauflösung der eigenen Internetdomäne über interne DNS-Server, vor allem dann, wenn die Active Directory-Domäne die gleiche Bezeichnung hat. Dieses Problem lösen Sie sehr einfach dadurch, indem Sie manuell entweder nur einen Host A-Eintrag mit der Bezeichnung "www" und der externen IP-Adresse der Internetseite erstellen, oder für jeden Servernamen, den Sie extern auflösen lassen wollen, einen eigenen Eintrag setzen. In diesem Fall lösen die internen DNS-Server den Eintrag der WWW-Seite korrekt nach der externen IP-Adresse auf.

DHCP und die DNS-Namensauflösung

Ändern Sie die IP-Adresse eines Servers, wird nicht unbedingt gleich der entsprechende DNS-Eintrag des Servers geändert. Funktioniert nach einer IP-Änderung die Namensauflösung selbst nach dem Ausführen von `ipconfig /registerdns` nicht, löschen Sie den Host A-Eintrag auf dem Server und versuchen Sie die dynamische Registrierung erneut. Ist auf dem Client der korrekte DNS-Server eingetragen und auf dem DNS-Server die dynamische Aktualisierung aktiv, sollte sich der Server neu registrieren. Arbeiten Sie mit DHCP, müssen Sie noch weitere Bereiche beachten.

Damit der DHCP-Server für die Clients eine automatische DNS-Registrierung auf den DNS-Servern durchführen kann, müssen Sie ihn erst dafür konfigurieren. Wenn Sie die Eigenschaften von IPv4 oder IPv6 des DHCP-Servers aufrufen, können Sie auf der Registerkarte "DNS" konfigurieren



ren, welche Einträge der DHCP-Server auf den DNS-Servern erstellen soll.

Setzen Sie noch Clients ein, die kein dynamisches DNS unterstützen, sollten Sie in den Eigenschaften des DHCP-Servers auf der Registerkarte "DNS" die Option "DNS-A- und -PTR-Einträge für DHCP-Clients, die keine Aktualisierungen anfordern..." sowie zusätzlich die Option "DNS-A- und -PTR-Einträge immer dynamisch aktualisieren" aktivieren. Ein Computer, dessen Lease-Dauer für die IP-Adresse abgelaufen ist, muss seine Adresse abgeben. Daher löscht der DHCP-Server in der Standardeinstellung auch die zugehörigen DNS-Einträge. Falls Sie die Einträge trotzdem behalten wollen, deaktivieren Sie das Kontrollkästchen "DNS-A- und PTR-Einträge beim Löschen der Lease verwerfen".

Über die Schaltfläche "Konfigurieren" auf der Registerkarte "DNS" in den Eigenschaften des DHCP-Servers können Sie noch den Namensschutz aktivieren, der bereits existierende Einträge im DNS vor Änderungen schützt. In der Windows-Gruppe "DnsUpdateProxy" befinden sich Computer, die als Proxy für die dynamische Aktualisierung von DNS-Einträgen fungieren können. DHCP-Server werden in diese Gruppen nicht automatisch aufgenommen. Sie sollten die Computerkonten der DHCP-Server in die Gruppe "DnsUpdateProxy" aufnehmen, wenn

die DNS-Aktualisierung nicht funktioniert. Alternativ können Sie auf der Registerkarte "Erweitert" in den Eigenschaften für IPv4 oder IPv6 Anmeldedaten hinterlegen, die eine Aktualisierung ermöglichen. Ändern Sie die IP-Adresse des DNS-Servers selbst, stellen Sie sicher, dass in den Eigenschaften der Zonen, die dieser Server verwaltet, auf der Registerkarte "Namensserver" der korrekte Name und die richtige IP-Adresse hinterlegt ist.


Dynamisches DNS im Internet nutzen

Damit die Benutzer und Server Verbindung ins Internet aufbauen können, müssen Sie dafür sorgen, dass die Server die Namen im Internet auflösen können. Setzen Sie noch einen ISA-Server oder das neue Forefront Threat Management Gateway (TMG) ein, müssen Sie auf dem Server Regeln für den DNS-Zugriff erstellen. Die DNS-Server des Active Directory können nicht nur die internen Zonen auflösen, sondern auch als Weiterleitungsserver die DNS-Server Ihres Providers verwenden oder die Root-DNS-Server, die bereits standardmäßig hinterlegt sind. Die interne Netzwerkkarte des ISA-Servers nutzt als DNS-Server den lokalen DNS-Dienst der Active Directory-DNS-Server. Der DNS-Dienst kennt die IP-Adressen der DNS-Server im Internet, die auf der Registerkarte "Stammhinweise" in den Eigenschaften des Servers in der DNS-Verwaltung zu finden sind. Sobald

ein interner DNS-Server eine Abfrage erhält, die er nicht selbst auflösen kann, schickt er diese zu der IP-Adresse, die als Weiterleitungsserver oder bei "Stammhinweise" eingetragen ist.

Damit der Zugriff auf das Internet für die Namensauflösung funktioniert, müssen folgende Voraussetzungen geschaffen sein:

1. Die interne Netzwerkverbindung des ISA-Servers hat eine IP-Adresse im internen Netzwerk und verwendet als DNS-Server die internen DNS-Server.
2. Die interne LAN-Verbindung hat in den IP-Einstellungen kein Standardgateway eingetragen.
3. Die externe Schnittstelle des ISA-Servers ist mit der internen Schnittstelle einer Hardware-Firewall verbunden.
4. Die Hardware-Firewall ist erfolgreich mit dem Internet verbunden.
5. Die externe Schnittstelle des ISA-Servers verwendet als Standardgateway die interne IP-Adresse der Hardware-Firewall und als DNS-Server die internen DNS-Server.

Geben Sie in der Befehlszeile auf dem Server `nslookup` ein und lassen Sie den Namen einer Internetseite auflösen, zum Beispiel "www.it-administrator.de". Der Name muss aufgelöst werden, da der interne DNS-Server die Abfrage an die Stammhinweise oder seine Weiterleitungsserver übermittelt. (In) 

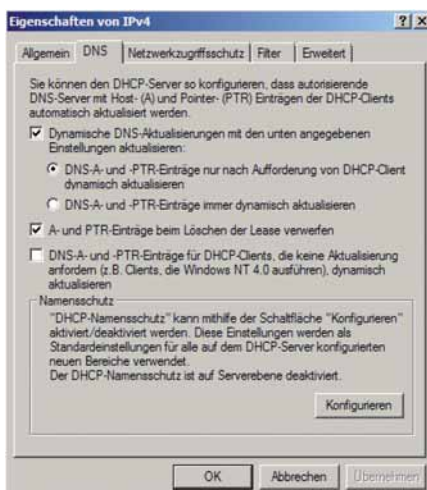


Bild 3: DNS-Anbindung eines DHCP-Servers

SEMINARMARKT

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

www.it-administrator.de/seminarmarkt

**Log.in
consultants**

**Von Profis entwickelte
High-Level-Trainings!**

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

Jetzt buchen!

www.loginconsultants.de



Lotus Domino 8.5

Zentrales Passwort- und Zertifikatsmanagement

von Roland Joeriskes

Die Verwaltung von Benutzerzertifikaten und deren Kennwörtern gestaltet sich bislang äußerst kompliziert und zeitaufwendig. Langwierige Wiederherstellungen von IDs und Passwörtern gehören zum Alltag eines jeden Supporters. Mit dem in der Version 8.5 eingeführten Lotus Domino ID-Vault werden diese Aufgaben deutlich vereinfacht und sogar ein "Passwort Self Service" lässt sich nun implementieren. Dabei handelt es sich um eine serverbasierte Datenbank, die geschützte Kopien der Benutzer-ID-Dateien enthält. Damit vereinfacht sich das gesamte ID- und Zertifikatsmanagement in einer Lotus Domino-Infrastruktur. So können Kennwörter durch autorisierte Benutzer geändert oder zurückgesetzt und beschädigte oder verlorengegangene ID-Dateien wiederhergestellt werden. Verwendet ein Lotus Notes-Nutzer mehrere ID-Dateien, werden die Kennwörter über den Zertifikatspeicher synchronisiert.

Das erstmalige Hochladen der ID-Datei kann dabei auf verschiedene Arten erfolgen. Erkennt der Lotus Notes-Client die Zuweisung des Benutzers zu einem Vaultspeicher, wird die ID-Datei in die zugehörige Datenbank hochgeladen. Alternativ wird bei der Benutzerregistrierung bereits eine Kopie der ID im Vault abgelegt. Werden nun Änderungen an den ID-Dateien – ob im Vault oder auf dem Lotus Notes Client – vorgenommen, müssen diese synchronisiert werden. Ändert ein Benutzer seine ID-Datei, indem er etwa eine Kennwortänderung durchführt, versucht der Client eine sofortige Synchronisation mit dem ID-Vault.

Andernfalls wird der Abgleich mit dem Vault periodisch nach definierten Regeln durchgeführt, sofern eine Verbindung zum Server besteht. Hat ein Benutzer seine ID-Datei gelöscht, wird diese automatisch durch den Notes-Client heruntergeladen.


Zertifikatspeicher einrichten

Die Einrichtung der Vault-Speicher erfolgt gänzlich über den Domino-Administrationsclient. Für eine Domino-Domäne lassen sich mehrere Repositories definieren. Dieses kann beispielsweise bei der Arbeit mit verteilten Administrationsteams sinnvoll sein oder wenn ausgewählten Benutzergruppen aus Sicherheitsgründen ein separater Vault zur Verfügung gestellt werden soll. Jedem ID-Vault können Sie Berechtigung zur Verwaltung und zur Rücksetzung der Kennwörter hinterlegen. Für Lastverteilung und Failover kann der Vault auf unterschiedliche Replikserver verteilt werden. Die Verwendung des zentralen Zertifikatspeichers wird über Richtlinien im Domino-Verzeichnis gesteuert. Dabei legen Sie über die Sicherheitseinstellung fest, welchen Speicher der Benutzer verwendet und ob die Anzahl der Downloads aus diesem beschränkt werden soll.

Der ID-Vault besteht sowohl aus einer Client- als auch aus einer Serverkomponente. Daher müssen die beteiligten Bestandteile wie Lotus Notes-Client, Homeserver, Administrationsserver und ID-Vaultserver mindestens auf Version 8.5 betrieben werden, damit sich das ID-Repository verwenden lässt.

Neue Funktionen in der Version 8.5.1

Ab der Version 8.5.1 stehen die Vault-Funktionen auch anderen Programmen zur Verfügung, die die Lotus Notes-API verwenden. So bedienen sich die Software Lotus iNotes oder auch der Push-Dienst für mobile Endgeräte, Lotus Traveler, für die Entschlüsselung von Nachrichten bereits dem ID-Vault. Aber auch Drittanbieter binden den Vault bereits in Ihre Sicherheitsmechanismen ein. So unterstützt der kanadische BlackBerry-Hersteller RIM mit der Version 5.0.1 seines BlackBerry Enterprise Servers bereits den Vault für die Ver- und Entschlüsselung von E-Mails.

Mit der Veröffentlichung der Version 8.5 hat Lotus Software eine neue Funktion implementiert, die das Zertifikatsmanagement im Unternehmen deutlich vereinfacht und den Userhelpdesk entlastet. Für viele Unternehmen dürfte dieses Feature ein weiterer Grund sein, ein Update auf Version 8.5 auch auf den Workstations in Betracht zu ziehen. (jp) 

Roland Joeriskes ist Geschäftsbereichsleiter Solutions bei der acon GmbH in Bielefeld.

[1] **Einrichtung und Verwendung der ID-Vault**
www-10.lotus.com/ldd/dominowiki.nsf/xpViewTags.xsp?categoryFilter=Notes%20ID%20Vault

Links



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



Tipps & Tricks ohne Gewähr



Das **WMI (Windows Management Instrumentation)** ist ein Windows-Standard, der entwickelt wurde als mächtiges Tool zur (Fern-) Administration in Windows-Netzwerken und zum einfachen Hardware-Monitoring. Wir möchten WMI gerne nutzen, doch scheint dies mit **Windows Vista** und **Server 2008** nicht gut zu funktionieren. Woran liegt das?

Wer auf das "falsche" Betriebssystem setzt, kann WMI in der Tat nur mit angezogener Handbremse nutzen. Eigentlich ist WMI seit Windows 95 ein "alter Hut", in der Praxis haben sich hier jedoch ausgerechnet die Windows-Versionen Vista und 2008 R1 als tückisch erwiesen. In einem Test-Setup überwachten wir verschiedene Systeme mittels WMI. Die Informationen (etwa Prozessorlast, Speicherverbrauch, Festplattenkapazität, laufende Dienste und Prozesse einzelner Rechner) flossen dabei vor allem in sehr großen Netzwerken unter Windows XP und 2003 bis zu 70 Mal schneller. Die beste Plattform für WMI-Monitoring bietet dabei Windows 2003 R2, dicht gefolgt von XP und Windows 7. Auf Vista und Windows 2008 R1 sollten Sie dagegen verzichten. Sind Sie dennoch zwingend auf diese Systeme angewiesen, kön-

nen Sie zur Überwachung eine virtuelle Maschine mit Windows XP verwenden. Selbst diese Lösung war im Test noch leistungsfähiger. Als Alternative: SNMP mag nicht so komfortabel sein, verbraucht jedoch nur ein Zehntel der Ressourcen im Vergleich zu WMI. Mehr zum WMI-Test finden Sie unter www.paessler.com/blog/2009/06/03/. (Paessler/jp)

In unserer Kundenkommunikation kommt es immer wieder vor, dass Anhänge mit **EML-Dateien** im Posteingang landen. Dieses E-Mailformat, unter anderem von **Outlook Express** verwendet, kann unter **Windows 7** nicht mehr ohne Weiteres geöffnet werden, denn der Express-Nachfolger **Windows Mail** ist nicht mehr direkter Bestandteil des Betriebssystems. Wie können wir auf diese Dateien dennoch zugreifen?

Mit Outlook 2007 lassen sich diese Dateien mit einem versteckten Schalter direkt öffnen. Um nur den Inhalt einer MIME-kodierten EML-Datei anzuzeigen, genügt es meist, die Dateiendung auf MHT zu ändern. Ein Doppelklick öffnet sie dann lesbar im Internet Explorer. Um auch enthaltene Anhänge zu sehen, klicken Sie auf "Start / Ausführen..." und geben Sie ein:

```
outlook /eml C:\Pfad\mail.eml
```

Outlook öffnet dann die Mail mit allen Anhängen. Die Verknüpfung mit dem Doppelklick können Sie unter Windows

7 jedoch nicht mehr so einfach wie unter XP in den Explorer-Ordneroptionen einstellen. Abhilfe kann hier eine CMD-Datei schaffen, die Sie mit der EML-Endung verknüpfen (Rechtsklick auf die EML-Datei: "Öffnen mit"). Für Outlook 2007 hat diese Datei folgenden Inhalt:

```
"C:\Program Files (x86)\Microsoft
office\office12\OUTLOOK.EXE"
/EML %1
```

Bei einem Doppelklick wird dann zukünftig die CMD-Datei aufgerufen, die Outlook mit dem /EML-Parameter startet und dabei den Dateinamen samt Pfad übergibt. Übrigens: Damit auch Outlook 2003 EML-Dateien öffnet, benötigen Sie eventuell den Microsoft-Hotfix unter <http://support.microsoft.com/kb/965495/>. (Paessler/jp)

Anwender, die **Windows 7 Ultimate** oder **Enterprise** einsetzen, oder Unternehmen mit **Windows Server 2008 R2** können **USB-Sticks mit Bordmitteln verschlüsseln**. Dazu steht **BitLocker-To-Go** zur Verfügung. Verbinden Sie den USB-Stick mit dem Rechner und wählen Sie über das Kontextmenü die Option "BitLocker aktivieren" aus.

Wählen Sie für die Verschlüsselung die Kennwort-Methode aus und geben Sie das Kennwort ein. Sie können statt einem Kennwort auch eine Smartcard verwenden. Speichern Sie das Kennwort oder

drucken Sie es auf der nächsten Seite aus. Windows 7 oder Windows Server 2008 R2 verschlüsselt jetzt den USB-Stick und zeigt die Verschlüsselung mit einem Schloss an. Über das Kontextmenü machen Sie die Eingaben wieder rückgängig, wenn Sie den USB-Key entschlüsseln wollen. Hier können Sie auch ein neues Kennwort eingeben oder das Kennwort erneut ausdrucken, wenn Sie über entsprechende Rechte verfügen. Wollen Sie auf den USB-Stick zugreifen, auch von anderen Computern, erscheint ein Fenster, über das Sie das hinterlegte Kennwort eingeben. (jp)

Wir planen, den neuen Windows Server 2008 R2 in unserem Netzwerk einzusetzen und würden das Betriebssystem gerne über einen USB-Stick installieren. Wie können wir das tun?

Wollen Sie Windows Server 2008 R2 oder Windows 7 über einen USB-Stick installieren, können Sie zum Beispiel auch die Antwortdatei hinterlegen. Diese wendet der Installationsassistent dann automatisch an. Sinnvoll kann das für Server sein, die über kein DVD-Laufwerk verfügen, oder für Netbooks. Gehen Sie zur Installation folgendermaßen vor:

1. Verbinden Sie den USB-Stick mit einem Windows Server 2008 R2-Computer. Sie benötigen für den Betrieb das Befehlszeilen-Tool Diskpart. Die Versionen in Windows Server 2003 und Windows Server 2008 unterstützen keine Bearbeitung von USB-Sticks in der Art, wie Sie der Bootvorgang benötigt.
2. Starten Sie eine Befehlszeile über das Kontextmenü im Administratormodus.
3. Starten Sie die Festplattenverwaltung in der Befehlszeile mit Diskpart.
4. Geben Sie *list disk* ein.
5. Geben Sie den Befehl *select disk {Nummer des USB-Sticks aus list disk}* ein.
6. Geben Sie *clean* ein.
7. Geben Sie *create partition primary* ein.

8. Geben Sie *active* ein, um die Partition zu aktivieren. Dies wird für den Bootvorgang benötigt.
9. Formatieren Sie den Datenträger mit *format fs=fat32 quick*.
10. Geben Sie den Befehl *assign* ein.
11. Beenden Sie Diskpart mit *exit*.
12. Wechseln Sie in der Befehlszeile in das Verzeichnis `\boot` der Windows Server 2008 R2-DVD.
13. Geben Sie optional den Befehl *bootsect /nt60 {Laufwerksbuchstabe des USB-Sticks}* ein. Unbedingt notwendig ist das nicht in jedem Fall.
14. Kopieren Sie den Inhalt der Windows Server 2008 R2-DVD in das Stammverzeichnis des USB-Sticks.
15. Verbinden Sie den USB-Stick mit dem Zielgerät und stellen Sie im Bios oder dem Bootmenü die Option ein, dass der Rechner von USB bootet.
16. Starten Sie den Rechner und stellen Sie sicher, dass der Bootvorgang über USB startet. Arbeiten Sie mit einer Antwortdatei, kopieren Sie diese ebenfalls in das Verzeichnis. (jp)



Apple

Ich arbeite mit einem Mac OS X-Rechner und nutze dabei auch den Finder, um Dateien zu suchen. Manchmal wäre es dabei hilfreich, wenn in den Suchergebnissen auch Kalendereinträge oder E-Mails angezeigt würden, da ich diese für meine Arbeit sehr intensiv nutze. Wie lässt sich das einrichten?

Sie können sich E-Mails und Kalendereinträge aus iCal relativ einfach anzeigen lassen. Hierfür geben Sie Ihren gewünschten Suchbegriff ein und klicken in den Fundstelle auf "Alle einblenden". Im anschließend offenen Finder-Fenster sehen Sie nun auch Nachrichten und Kalendereinträge, die zu Ihrer Suche passen. Alternativ dazu geben Sie Ihren Suchbegriff im Finder ein, klicken auf das kleine "Plus" neben dem Punkt "Sichern" und gehen auf den Menüpunkt "Art / Andere". Danach öffnet sich ein neues Fenster, in dem Sie zum Punkt "Spotlight-Objekte" gehen und dort

den Eintrag "Im Menü" mit einem Häkchen aktivieren. Im Menü "Art" stellen Sie anschließend "Spotlight-Objekte" ein und klicken im dazugehörigen Untermenü auf "Enthält". Leider ist diese Einstellung nicht von Dauer und bei der nächsten Suche müssen Sie wieder im Menü "Art" die "Spotlight-Objekte" wählen. Insofern dürfte der erste Weg der einfachere sein. (dr)



Für den Citrix XenServer existiert eine Vielzahl von Vorlagen, die zur Erstellung neuer virtueller Maschinen genutzt werden können. Neben denen, die bereits der Installationsdatenträger mitbringt, sind weitere für Linux-Systeme auf dem Datenträger mit dem "Linux Support Pack" enthalten. Dieser Datenträger kann während der initialen Installation des XenServer eingelegt und mit installiert werden. Doch was ist, wenn dieser Schritt während der Installation vergessen oder bewusst übersprungen wurde?

Die Tools können über das Command Line Interface (CLI) des XenServer nachinstalliert werden. Hierzu können Sie sich per WinSCP auf den XenServer verbinden und das Linux-Support-ISO in ein Verzeichnis auf dem Server kopieren – hierzu empfiehlt es sich, ein neues Verzeichnis zu erstellen, um Verwechslungen mit vorhandenen Verzeichnissen oder Inhalten zu vermeiden. Anschließend können Sie sich mit einem SSH/Telnet-Client wie etwa Putty auf

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

den Server verbinden und die Installation durchführen. Hierfür wechseln Sie in das Verzeichnis mit dem ISO-Image und geben nacheinander die Befehle

```
mkdir -p /mnt/iso
mount -o loop XS-linuxcd.iso /mnt/iso
cd /mnt/iso
```

ein. Über `./install.sh` können Sie nun das Paket installieren. Anschließend stehen Ihnen alle Funktionen des Linux Support Packs zur Verfügung. (jp)



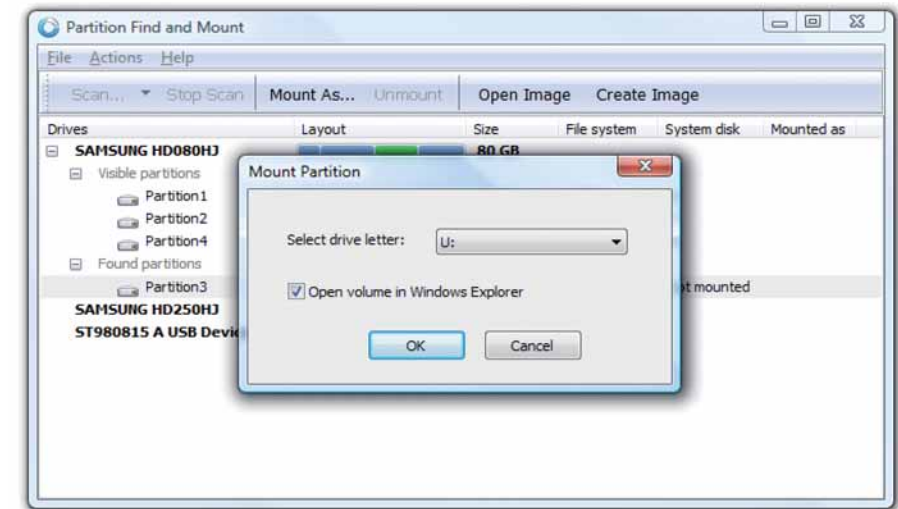
Tools

Ist eine **Partition der Festplatte verschwunden**, kann die Ursache, neben dem offensichtlichen

Löschen, auch in Schäden der Partition oder der Partitionstabelle zu finden sein. Nur hat die Partition in diesen Fällen einen erheblichen Nachteil, sie ist praktisch unsichtbar geworden. Da solche Fälle im Support einen kniffligen Fehlerfall darstellen, ist – wenn sich auf der Partition wichtige Daten befinden und somit eine Neubetankung des Clients keine Option darstellt – ein kleines Werkzeug, das die verschwundenen Daten aufspürt, ein wertvoller Helfer.

Die Freeware **Partition Find and Mount** durchsucht die Festplatte nach gelöschten oder durch Fehler an der Partitionstabelle beschädigten Partitionen. Die Software unterstützt dabei FAT- und NTFS-Dateisysteme und kennt drei verschiedene Scanmethoden, um verlorene Partitionen zu finden. Findet das Werkzeug solche nicht sichtbaren Partitionen, zeigt es anschließend eine Liste mit allen physikalischen Laufwerken und bereits sichtbaren sowie den neu entdeckten Partitionen an. Die mit Partition Find and Mount gefundenen Partitionen lassen sich mit eigenem Laufwerksbuchstaben in den Windows Explorer einbinden. Alternativ exportiert das Programm neue Partitionen in Form von Image-Dateien. Die für den Privatgebrauch kostenlose Version ist jedoch auf eine Datentransfer-Rate von 512 KBytes/s beschränkt. (jp)

Quelle: <http://findandmount.com/download/>



Partition Find and Mount erlaubt es, verschwundenen Partitionen einen Laufwerksbuchstaben zuzuordnen und so die Daten zu retten

Die **Konfiguration von Switchen** und anderen Netzwerkgeräten ist in den meisten Fällen eine Sache der Kommandozeile. Dies trifft auch auf Arbeiten wie das Ändern von Interface-Bezeichnungen, Einstellungen der Port-Security oder die Konfiguration von VLANs zu. Neben der möglichen Fehleranfälligkeit ist bei dieser Tätigkeit vor allem die Wiederholung auf zwei, drei oder 40 Switchen ebenso zeitwie nervraubend. Hier prescht wieder einmal SolarWinds in die Bresche und stellt ein kostenloses Werkzeug für derlei Arbeiten zur Verfügung.

Der **Network Config Generator** erlaubt es Administratoren, VLANs und andere komplizierte Netzdienste einfach zu konfigurieren. Das Programm von SolarWinds ermöglicht den Umgang mit komplexen Switch-Features wie VLAN und NetFlow über eine grafische Oberfläche. Das Programm erlaubt Anwendern so den Zugriff und die Konfiguration von zahlreichen Features, die normalerweise nur über die Kommandozeile des Switch erreichbar sind. Unterstützt werden in erster Linie Switches von Cisco mit dem IOS-Betriebssystem. Das wahrscheinlich interessanteste Feature ist das Anlegen von Templates, die alle Einstellungen für einen Switch enthalten. Durch die Anwendung des Templates lassen sich mehrere Switches ohne Aufwand iden-

tisch konfigurieren. Der Network Config Generator erstellt passende Skripte (die erwähnten Templates) aus einer Serie von CLI-Befehlen. Das Tool läuft unter Windows XP (ab SP2), Windows Vista Business/Ultimate, Windows 7, Windows Server 2003 (ab SP1) und Windows Server 2008. Außerdem muss auf dem Rechner das Dot-Net-Framework 3.5 oder höher installiert sein. Wie immer bei SolarWinds muss sich der interessierte Administrator vor dem Download registrieren und leider sind einige der Features nur in Verbindung mit kostenpflichtigen Produkten des Herstellers voll nutzbar. (jp)

Quelle: www.solarwinds.com/products/free-tools/network_config_generator/

Software-Downloads

openQRM ★★★★★

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



Voraussetzungen für eine erfolgreiche Desktop-Virtualisierung

Chancen nutzen, Risiken vermeiden

von **Andreas Kohne**

Noch steckt die Desktop-Virtualisierung in den Kinderschuhen. Für standardisierte oder mobile Arbeitsplätze eignet sie sich beispielsweise sehr gut. Die Einführung virtueller Desktops will gut geplant sein, damit die Systemadministration sie erfolgreich implementieren und administrieren kann.

Auch künftig werden voraussichtlich physische PCs im Einsatz sein. Deshalb ist das Management heterogener Desktop-Landschaften ein entscheidender Erfolgsfaktor.

In absehbarer Zeit steht voraussichtlich in vielen Unternehmen der Wechsel auf Windows 7 an. Dies kann ein guter Anlass dafür sein, die aktuelle PC-Landschaft auf eine Virtual Desktop Infrastructure (VDI) zu migrieren. Bei einer parallelen Migration der aktuellen PC-Umgebung auf eine VDI können Administratoren alle Möglichkeiten der Virtualisierung nutzen – beispielsweise auch die Applikations-Virtualisierung. Das ermöglicht eine Migration auf Windows 7 mit wenigen Mausklicks, bei der IT-Verantwortliche einfach zwischen den Betriebssystemen umschalten können. Der Grund: Im Rahmen der Desktop-Virtualisierung werden Applikationen, Nutzerdaten und das Betriebssystem voneinander getrennt. Das vereinfacht die Migration und macht sie weniger komplex, da die einzelnen Bereiche unabhängiger voneinander sind als in einem klassischen Client-Konzept.

Da alle Bereiche durch die Virtualisierungsschicht klar voneinander getrennt sind, ist es auch möglich, diese schrittweise auf eine Migration vorzubereiten, ohne die jeweils anderen Bereiche einzubeziehen. Somit kann der Administrator beispielsweise ein neues Basis-Image mit dem neuen Betriebssystem vorbereiten,

die Applikationen in der neusten Version für das Streamen anpassen und die Benutzerprofile nahtlos in die Umgebung einpassen. Die Migration lässt sich also soweit vorbereiten, dass die Anwender am Tag der Migration Schritt für Schritt neue Desktops erhalten – seien es Thin Clients oder Notebooks. Da die eigentliche Migration nur im Rechenzentrum stattfindet und in der Vorbereitung nicht den Benutzer mit seinem lokalen Desktop betrifft, können in einem Übergangszeitraum auch beide Welten parallel laufen. Dies hat den Vorteil, dass der Benutzer zwar noch seinen lokalen Rechner besitzt, aber bereits mit dem neuen virtuellen Desktop arbeiten kann. Dies kann dazu führen, dass sich Berührungsängste aus der Welt schaffen lassen, die schon aus dem Terminal-Server-Bereich bekannt sind.

Der Weg zur virtuellen Desktop-Landschaft

Beim Aufbau einer VDI sind einige Parameter zu berücksichtigen: Die IT-Verantwortlichen müssen insbesondere die Nutzungsprofile der Anwender bestimmen und genau betrachten. Denn ob sich der Umstieg auf virtuelle Desktops lohnt, hängt auch davon ab, welche Benutzergruppen damit arbeiten sollen und welche Aufgaben die Mitarbeiter erledigen.

Handelt es sich beispielsweise um Standard-Arbeitsplätze mit den üblichen Office-Anwendungen oder müssen auch spezielle Fachanwendungen und Multimedia-Applikationen geladen oder gar Videos gestreamed werden? Es gilt also, Schlüsselgruppen mit bestimmten Anwendungsprofilen zu identifizieren und auf eine möglichst kleine Zahl an Basis-Images zu konsolidieren. Die Schnittmenge an Einstellungen sowie genutzten Applikationen und Ressourcen, wie Bandbreite, CPU und RAM, sollte in einer Schlüsselgruppe möglichst groß sein. Aus der Definition von Schlüsselgruppen können IT-Verantwortliche verlässliche Informationen für das Sizing der virtuellen Infrastruktur gewinnen: Beispielsweise die zu erwartenden Netzlasten durch den Betrieb von virtuellen Desktops, notwendige Bandbreiten und Zugriffs-Protokolle. Weiteres Ziel einer solchen Analyse ist es, die Infrastruktur für eine bessere Automatisierung weitestgehend zu standardisieren.

Anforderungen an eine virtuelle Infrastruktur

Die Netzwerklast stellt ein entscheidendes Kriterium für das Sizing der virtuellen Infrastruktur dar. Müssen beispielsweise grafikintensive Anwendungen über

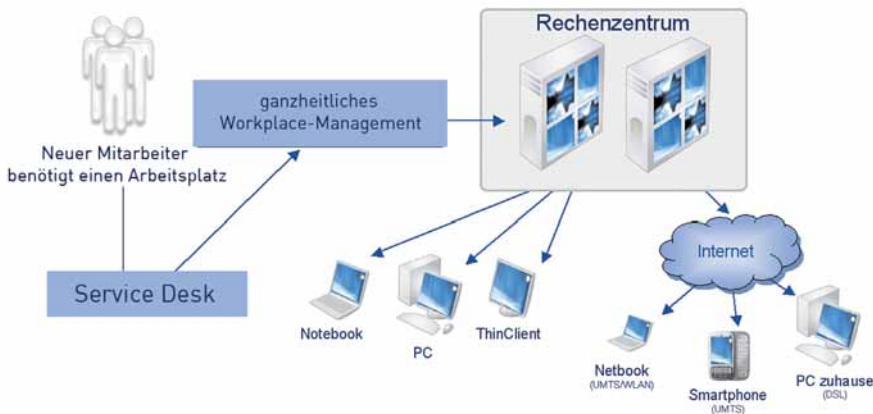


Bild 1: Bei der Desktop-Virtualisierung wird anstelle einer einzelnen Komponente oder Anwendung der komplette Desktop-PC im Rechenzentrum virtualisiert und zentral für die Auslieferung auf ein nahezu beliebiges Endgerät bereitgestellt

schmalbandige Verbindungen geschickt oder ein zentraler virtueller Desktop an einen lokalen Drucker angebunden werden, steigt die Netzwerklast stark an. Außerdem sollten IT-Verantwortliche die Wege analysieren, über die auf das Netz zugegriffen werden kann – beispielsweise über ein Virtual Private Network (VPN). Zu prüfen ist, ob Richtlinien für den sicheren Zugriff auf virtuelle Desktops zu erweitern sind. Erhöhte Sicherheitsrichtlinien sind sehr wichtig, da potenzielle Angreifer über einen ungeschützten virtuellen Desktop direkt auf die gesamte zentrale Infrastruktur zugreifen können. Hier droht deutlich mehr Schaden, als dies beispielsweise im Vergleich mit einer bereitgestellten Applikation möglich wäre. Die zu erwartende Netzwerklast und Zugriffswege bilden die Basis für die Leistungsanforderungen an eine virtualisierte Umgebung. Im nächsten Schritt sollten IT-Verantwortliche aus dem bisherigen Verbrauch unter anderem ableiten, welche Ressourcen die Anwender künftig auf ihren virtuellen Desktops benötigen. Hier spielt unter anderem auch die Nutzung von Druckern im Netz eine wesentliche Rolle. Werden diese Punkte berücksichtigt, lassen sich optimale Netzwerkverbindungen einrichten: Die Latenzen sind dann gering und die Anwender zufrieden.

Anhand dieser Informationen können die Verantwortlichen auch entscheiden, wel-

che Protokolle für den Zugriff zu verwenden sind. Die Protokollwahl wird vor allem beeinflusst von der Bandbreite, dem Einsatz im LAN oder WAN beziehungsweise Internet sowie der Nutzung von Multimedia-, VoIP- und CAD-Anwendungen. Die großen Hersteller der Virtualisierungslösungen haben ihre Protokolle inzwischen weiterentwickelt, um die Desktop-Performance auch tatsächlich zum Endbenutzer zu bringen. Zur Auswahl stehen etwa das einfache RDP-, das optimierte HDX-Protokoll von Citrix, das von VMware neu in Software eingeführte PCoIP-Protokoll sowie offene Protokolle wie SPICE oder NX. Welche Protokollarchitektur gewählt wird, richtet sich danach, ob die Anwender beispielsweise im LAN, mobil oder hochdynamisch arbeiten. Im LAN genügt beispielsweise das einfache RDP-Protokoll. Das WAN erfordert Protokolle wie ICA oder PCoIP. Für die Bereitstellung von CAD- und Multimedia-Anwendungen empfiehlt sich die Nutzung von ICA mit HDX oder auch PCoIP.

Schließlich gilt es, die passenden Endgeräte auszuwählen. Werden beispielsweise hoch performante Anwendungen etwa für 3D benötigt, sind normale Thin Clients hierfür nicht leistungsstark genug. Solche Endgeräte benötigen eine gute Grafikkarte und eine leistungsstarke CPU, um Daten lokal zu verarbeiten. Das kann sonst dazu führen, dass zwar die Sessions

aus dem Rechenzentrum übertragen werden, der PC aber weiterhin am Arbeitsplatz steht. Dies liegt daran, dass die Grafik-Protokolle auf der virtuellen Maschine den Multimedia-Grafikstrom komplett aus dem Bild herausrechnen und speziell komprimiert an den Client übertragen. Das übertragene Bild beinhaltet dann an der Stelle der Animation oder des Films einen leeren Kasten. Der Client muss dann den Multimedia-Datenstrom lokal dekomprimieren und an der entsprechenden Stelle über das Desktop-Bild blenden. Dieses benötigt beispielsweise bei Citrix HDX eine lokal installierte Nvidia Grafikkarte, die in der Lage ist, über das Compute Unified Device Architecture (CUDA)-Framework Video-Decodierung auf der Grafik-Hardware durchzuführen.

Speicherbedarf ermitteln

Ein entscheidender Aspekt im Rahmen der Desktop-Virtualisierung ist auch der von den Anwendern benötigte Speicherplatz. Stellt der Administrator jedem virtuellen Arbeitsplatz denselben exklusiven Plattenplatz zur Verfügung, den er auch mit einem Desktop-PC hätte, wäre das zentrale Storage-Management mit einer geeigneten Datensicherung sehr umfassend und teuer. Thin Provisioning lautet hier die Alternative – die kostensparende Bereitstellung von Speicherkapazität in virtualisierten Speicherumgebungen verspricht, diese Probleme zu lösen.

Allerdings gibt es hier bisher mit dem Storage-Wachstumsverhalten während des produktiven Betriebs mit Windows Client-Betriebssystemen kaum Erfahrungswerte aus der Praxis. Somit muss auch bei einer VDI-Realisierung mit Thin-Provisioning-Systemen eine Lösung für die dauerhafte Sicherung individueller Änderungen bei den virtuellen Desktops gefunden werden. Entscheidend ist also für eine akzeptable und wirtschaftliche Lösung, dass die erforderlichen Arbeitsplatzkategorien zahlenmäßig erfasst werden und ein auf die Anwenderbedürfnisse passendes Storage-Konzept erstellt wird. Hierzu empfiehlt sich der Einsatz erfahrener Berater.

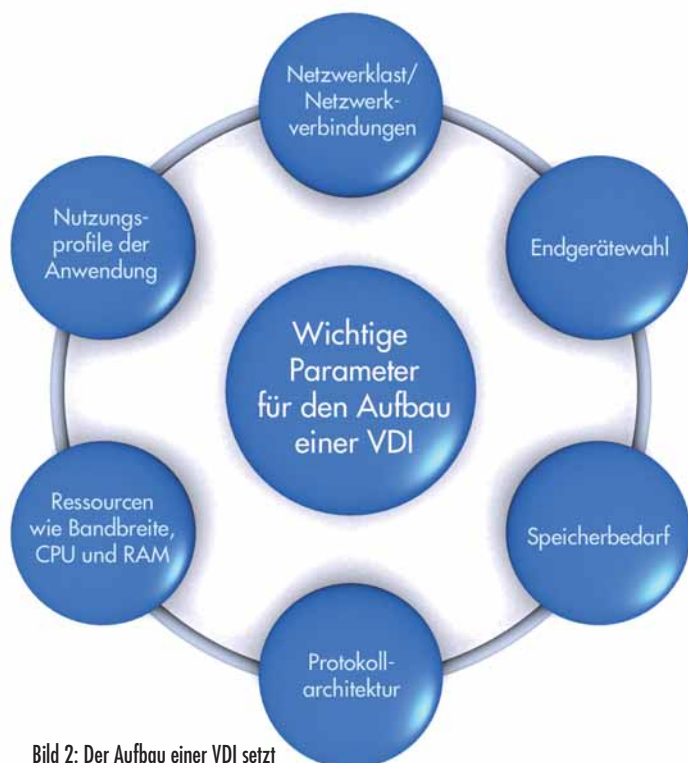


Bild 2: Der Aufbau einer VDI setzt eine Reihe wichtiger Parameter voraus

Bei den ersten Versionen der Virtualisierungslösungen wurden die Systeme zunächst noch 1:1 im Storage abgebildet, was umständlich und kostenintensiv war. Die Betriebssysteme wurden dabei als vollständige virtuelle Maschine im Storage abgelegt. Bei einer Umgebung von beispielsweise 100 Desktops mit einer durchschnittlichen Desktop-Größe von 10 GByte führt dies zu einer zusätzlichen Belastung von einem TByte im hochverfügbaren Storage. Mittlerweile haben die Hersteller ihre Produkte nachgerüstet, so dass dies nicht mehr erforderlich ist.

VMware setzt beispielsweise seine Linked Clone-Technologie ein, um den benötigten Speicherplatz zu reduzieren. Dabei machen Basis-Images, die so genannten Golden Images, die Grundapplikationen verfügbar. Zunächst wird von den Golden Images ein Clone erstellt. Die Anwender arbeiten auf Snapshots des Clones. So müssen lediglich die Deltas zu den Golden Images vorgehalten werden. Deshalb erhalten nicht alle Anwender eine vollwertige virtuelle Maschine und der benötigte Speicherplatz fällt deutlich geringer aus. Auch Citrix hat mit dem Provisioning Ser-

ver eine ähnliche Komponente in seine XenDesktop Suite integriert. Der Provisioning-Server ermöglicht das Streaming von Betriebssystem und Festplatten. Es wird daher nur noch eine geringe Anzahl an Basis-Images im Storage vorgehalten. Diese werden dann nach Bedarf in die Maschinen-Sessions übertragen. Anschließend lädt das System aus dem Golden Image nur noch die Ressourcen nach, die der Anwender tatsächlich benötigt. Ein

solches Vorgehen sorgt für geringen Bandbreitenbedarf. Außerdem kann ein Provisioning-Server mehrere Hundert virtuelle Maschinen gleichzeitig versorgen. Damit schließt sich der Kreis für die Desktop-Virtualisierung: Die Analyse der Benutzeranforderungen liefert auf allen Ebenen wichtige Informationen für das Sizing.

Virtuelle und physische Desktops in einem Management

Der Anteil physischer Hardware überwiegt heute noch. Doch ist davon auszugehen, dass sich dieses Verhältnis in den kommenden Jahren zugunsten der virtuellen Desktops verschieben wird. Das stellt Unternehmen vor die Herausforderung, dass sie sich mit zwei Welten auseinandersetzen müssen. Damit IT-Leiter mit den neuen Technologien keine weiteren Insellösungen aufbauen, sollten beide Welten unter einer einheitlichen Management-Plattform administriert werden. Es gilt, die virtuelle Welt von Anfang an in das IT-Service-Management, in die Automatisierung und das Client-Management zu integrieren. Damit zählt ein einheitliches Management zu einem der größten Fallstricke bei der Virtualisierung. Hier kom-

men Lösungen wie DX-Union mit der Variante "Desktop-as-a-Service" von Materna ins Spiel. Diese administrieren virtuelle und physische Desktops unter einer einheitlichen Management-Oberfläche und stellen darüber hinaus virtuelle Desktops vollautomatisiert bereit.

Beim Konzept Desktop-as-a-Service erfolgen sämtliche administrativen Tätigkeiten für die virtuellen und physikalischen Desktops aus einer Management-Oberfläche. Der große Vorteil ist, dass alle Objekte gleich aussehen. Für den Administrator macht es beim Handling der Objekte keinen Unterschied, ob er mit physikalischen oder virtuellen Maschinen arbeitet. IT-Verantwortliche können auf diese Weise reale PCs und virtuelle Desktops verwalten, ohne dass sie sich in die unterschiedlichen Management-Tools der Hersteller vertiefen müssen. Desktop-as-a-Service erleichtert auch eine Migration zu einer VDI. Denn durch die Virtualisierung der Desktops kommen viele weitere herstellereigenspezifische Administrationskonsolen hinzu. Der Administrator muss weitere Virtualisierungs-Hosts managen, die Applikations-Virtualisierung verwalten und er muss den Connection Broker zu jeder Zeit überwachen und aktuell halten.

Passende Schutzmaßnahmen

Vor allem die Sicherheit spielt bei der einheitlichen Verwaltung von virtuellen und physikalischen Desktops eine besondere Rolle. Vorhandene Sicherheitsstandards müssen beinahe noch strikter auf virtuelle Desktops angewendet werden. Verschlüsselung, Firewalls, Authentifizierung und Autorisierung sind entscheidende Aspekte, was die Sicherheit von virtuellen Desktops betrifft. Hier ist ein User Rights Management hilfreich: Es regelt, wer wann was darf. Zudem sind stärkere Logging-Strukturen als bisher erforderlich, um sämtliche Zugriffe nachvollziehen zu können. (dr)

Andreas Kohne ist Consultant im Team Virtualisierung bei Materna.

Clusterbau



Zunächst scheint es sich um eine Neuauflage zu handeln, denn schon 2008 kam der Titel "Clusterbau mit Linux-HA" heraus. Doch zu den Möglichkeiten, die Linux-HA, mittlerweile auch als "pacemaker"

bekannt, bietet, haben sich weitere Komponenten gesellt, mit denen die Verfügbarkeit von IT-Systemen erhöht werden kann. Manches ist gleich geblieben, doch viele Abschnitte sind durchaus neu hinzugekommen oder erweitert worden. Für Einsteiger in das Thema ist die Hochverfügbarkeitstheorie im ersten Abschnitt erhellend. Was im Tagesgeschäft gern durcheinander geworfen wird, nämlich Hochverfügbarkeit und Ausfallsicherheit,

Sichere Webanwendungen



Das Buch "Sichere Webanwendungen" eines Autorenteam handelt praktisch alle Webtechnologien ab, mit denen heute am meisten Schindluder getrieben wird. SQL Injection gehört ebenso dazu wie Cross Site Scripting und Directory

Traversal. Nachdem der Autor in den Kapiteln großen Wert auf Nachvollziehbarkeit legt, beschreibt er die Schwachstellen sehr oft detailliert und versieht sie mit Anleitungen zum Nachmachen. Es gibt natürlich einen Einführungsteil, der den so genannten "Hackerparagrafen" 202c er-

klärt der Autor hier sauber und mit ein paar theoretischen Grundlagen unterfüttert. In diesem Einstiegsbereich erfährt der Leser auch die Historie von pacemaker und OpenAIS. Weil sich recht viel in den Distributionen geändert hat und zum Teil deutlich mehr nachinstalliert werden muss, ist der Teil mit den distributionsspezifischen Anleitungen umfangreicher geworden. Gegen Ende richtet der Autor zusammen mit dem Leser noch einen rudimentären Mini-Cluster ein, damit die Hands-On-Fraktion auch etwas zu tun hat.

Das bleibt auch für die nächste Zeit das einzige Praktische, denn die Konfiguration der Ressourcen per XML ist eine recht trockene Angelegenheit. Schwartzkopff macht aus dem hohen Theorieanteil keinen Hehl, schon im Vorwort legt er den potenziellen Lesern umfangreiche Linux- und Netzwerkkenntnisse ans Herz. Gut, dass nun eine übersichtliche GUI, deren Anwendung der Autor auch empfiehlt, den eigentlichen Umgang mit der Software erleichtert. Auch das Kapitel über Planung, Aufbau und Betrieb erleichtert

läutert, den (fast) aktuellen Stand der Rechtsprechung dazu dokumentiert und vor Nachahmung warnt. Jeder Leser muss aber selbst Sorge dafür tragen, dass er die Beispiele aus dem Buch nicht in der freien Wildbahn, sondern in seinem eigenen Netz anwendet und nirgendwo sonst.

Auch wenn immer wieder Codeschnipsel und Tabellen den Fluss unterbrechen, findet sich der interessierte Laie gut in den beschriebenen Techniken zurecht. Am Ende der Kapitel ermöglichen umfangreiche Linkverweise die weitere Recherche nach Tools und tiefer gehenden Anleitungen. Besonders lobenswert: Die Autoren beschreiben nicht nur den Angriff und überlassen es dem Admin, die Erkenntnisse selbst sozusagen "rückwärts" zur Verteidigung anzuwenden. Der Großteil des Buchs beschäftigt sich explizit mit dem Bauen sicherer Webanwendungen. Das fängt ganz weit unten bei Besonderheiten des HTTP-Protokolls an, geht mit der String-Konver-

durch seinen relativ hohen Praxisbezug das Verständnis. Mehr Praxis wäre auch bei den Beispielen schön gewesen. Der Autor hat nach wie vor nur etwa 30 Seiten dafür vorgesehen und beschreibt vier Einsatzszenarien. Dabei ist die Qualität der Beschreibung sehr unterschiedlich. Eine hochverfügbare virtuelle Maschine mit iSCSI als Massenspeicher wird sehr detailliert erläutert, eine hochverfügbare Firewall – eigentlich das komplexere Projekt – ungleich kürzer.

Fazit: Ein Buch für Anwender, die genau wissen, dass sie mit pacemaker einen Cluster bauen und betreiben wollen. Es sind sehr solide Linux- und Netzwerkkenntnisse für die Anwendung der beschriebenen Einsatzmöglichkeiten notwendig. Fachlich ist das Buch makellos. *Elmar Török*

Autor:	Michael Schwartzkopff
Verlag:	O'Reilly
Preis:	39,90 Euro
ISBN:	978-3-89721-919-9
Bewertung:	★★★★☆

tionierung und Unicode weiter und hört mit der Validierung auf. Alles ist so laiengerecht aufbereitet, dass auch ein Nichtprogrammierer ganz gut mit den meisten Konzepten und deren Anwendung klarkommt. Also optimal für den Admin, der die Sicherheit seiner Webanwendungen nicht nur dem Dienstleister überlassen will.

Fazit: Das Buch führt hervorragend und vor allem sehr praxisorientiert in das Thema Applikationssicherheit ein. Selbst ohne oder mit geringen Programmierkenntnissen lassen sich sinnvolle Checks auf die Anfälligkeit der eigenen Webanwendungen durchführen. *Elmar Török*

Autoren:	Mario Heiderich, Christian Matthies, Johannes Dahse, fukami
Verlag:	Galileo Computing
Preis:	39,90 Euro
ISBN:	978-3-8362-1194-9
Bewertung:	★★★★★


<http://msexchangeteam.com>

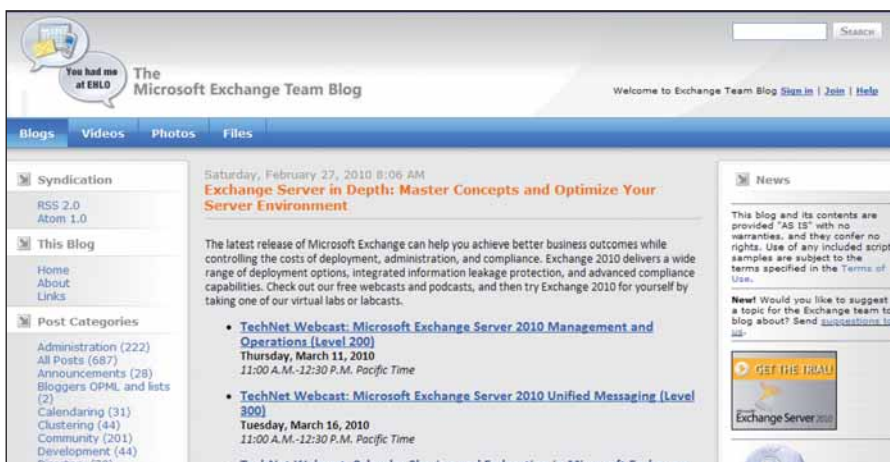
Auf Du und Du mit Exchange

Er ist das Arbeitstier in Unternehmen, wenn es um die Kommunikation mit der Außenwelt geht: Der Microsoft Exchange Server. Längst hat die E-Mail das Telefon, Fax oder gar den Brief als Kommunikationsmedium der Wahl abgelöst. Umso schlimmer, fällt der Mailserver einmal aus und stürzt die Mitarbeiter ins digitale Chaos. Dabei ist die Konfiguration einer komplexen Mailumgebung nicht unbedingt einfach. Sicher soll der Server sein, vor Spam und Viren schützen, sich nahtlos ins Active Directory integrieren und natürlich stabil laufen. Und mit Exchange Server 2010 steht nun auch noch eine neue Version ins Haus, die zahlreiche Änderungen mit sich bringt. Das sind durchaus viele Aspekte auf einmal für einen Admin, der den Server in kleineren Umgebungen oft nur nebenher betreut.

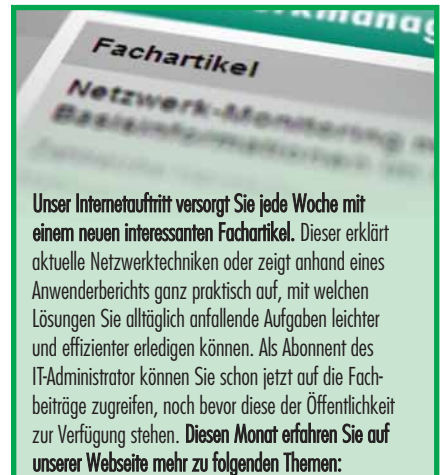
Was bietet sich da mehr an, als sich die nötigen Infos direkt von den Exchange-Machern selbst zu holen? Unter "msexchangeteam.com" bloggt das Exchange-Team von Microsoft seit 2004 in Englisch über aktuelle Entwicklungen und gibt Tipps rund um die Administration des Mailservers. Früher unter "blogs.msdn.com/exchange" und "blogs.technet.com/

exchange" zu finden, erfreut sich die Seite nach wie vor großer Beliebtheit und listet inzwischen an die 4.000 Einträge in über 40 Kategorien auf – angefangen bei der Administration über Clustering hin zu Storage und Troubleshooting. Dass die Blogger dabei durchaus etwas zu sagen haben, beweisen die zahllosen Bloggrafien eindrucklich. Mit teilweise jahrzehntelanger Erfahrung bei Microsoft kennen die Engineers, Technology Architects und Program Manager ihr Produkt in- und auswendig.

Wie tief die Blogger technisch in Exchange Server stecken, beweisen natürlich auch ihre Beiträge. Praxisorientierte Schritt-für-Schritt-Anleitungen führen die Besucher durch Themen wie die ISA 2006 SP1-Konfiguration mit Exchange 2010 oder das Veröffentlichen von S/MIME-Zertifikaten externer Kontakte im Active Directory. Anhand von Screenshots können Admins dabei nachvollziehen, ob sie sich auch wirklich auf dem gleichen Klickpfad befinden wie die Autoren. Weiterführende Links am Ende der Beiträge runden das Angebot ab. Zudem stehen zahlreiche Links zu anderen Webseiten rund um Exchange bereit – unter anderem auch in Deutsch. Und für Geschichtsliebhaber stehen nach wie vor alle Beiträge seit dem Start 2004 online. Eine Volltextsuche hilft dabei, die innerhalb der Kategorien teils unsortierten Artikel zielsicher zu durchforsten. (dr) 



Bietet Infos rund um Exchange von den Machern selbst: Das Microsoft Exchange Team-Blog



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

Reibungslose Migration auf Windows 7

Marktforscher gehen davon aus, dass innerhalb der nächsten drei Jahre fast zwei Drittel aller gewerblich genutzten Desktop-PCs mit Windows 7 ausgestattet sein werden. Die Migration auf den jüngsten Betriebssystem-Spross lässt sich mit den entsprechenden Tools – etwa dem Microsoft Deployment Toolkit 2010 – im Normalfall recht problemlos bewerkstelligen. Unser Online-Artikel verrät Ihnen, welche Werkzeuge besonders hilfreich sind und was Sie schon bei der Planung unbedingt bedenken sollten.

www.it-administrator.de/themen/server_client/fachartikel/75055.html

Sicherheit beim Cloud Computing

Kostenreduktion und erhöhte Flexibilität sind zwei der Hauptargumente, die für Cloud Computing sprechen. Diesen Vorteilen stehen aber neue Herausforderungen bezüglich der Sicherheit entgegen: Die eingeschränkte Möglichkeit zur Lokalisierung der Daten oder der illegale Handel mit Ressourcen sind nur zwei Alpträume eines IT-Verantwortlichen. Wir zeigen Ihnen in unserem Online-Beitrag, wie Sie mögliche Risiken besser einschätzen und auch in der Wolke für mehr Sicherheit sorgen.

www.it-administrator.de/themen/sicherheit/fachartikel/75056.html

Anwenderbericht: Hochverfügbare Virtualisierung beim Stader Tageblatt

Der Produktionsprozess bei Zeitungen hat sich in den letzten Jahren stark verändert. Auch beim Stader Tageblatt mit einer Auflage von 32.000 Exemplaren wurden Layout und Druck auf IT-Systeme umgestellt. Ebenso verläuft die Kommunikation nach außen bevorzugt digital, wobei dem Austausch von Anzeigen mit den Kunden sowie der redaktionellen Recherche besondere Bedeutung zukommt. In unserem Online-Anwenderbericht erläutern wir, mit welcher Lösung die IT-Verantwortlichen den Exchange Server virtualisiert und gleichzeitig hochverfügbar gemacht haben.

www.it-administrator.de/themen/virtualisierung/fachartikel/75057.html

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

»Virtuelle Maschinen treiben Green IT voran«

Harald Löscher (34) verantwortet bei der Napiag Kunststoffverarbeitung im österreichischen Zeltweg, einem Unternehmen des Mondi-Konzerns, das gesamte Netzwerk- und Systemmanagement. In Zeltweg werden mit rund 140 Mitarbeitern Kunststofffolien für unterschiedliche Anwendungsbereiche gefertigt. Die IT ist dabei eine wesentliche Säule der betrieblichen Infrastruktur.

Welche Ausbildung haben Sie gemacht?

2002 habe ich an der Fachakademie für angewandte Informatik in Graz die zweieinhalbjährige Ausbildung zum Fachwirt der Informatik erfolgreich abgeschlossen. Im Selbststudium erwarb ich seither weitere Zertifikate wie MCP, MCTS und MCSA. Das Lernen auf die Upgrade-Zertifizierung MCITP verschlingt derzeit einen großen Teil meiner Freizeit. Ich hoffe aber, dass ich diese in den nächsten Monaten abschließen kann.

Warum sind Sie IT-Administrator geworden?

Mich kann man getrost als totalen Quereinsteiger in die IT bezeichnen. Der Umstieg vom gelernten Zimmerer erforderte anfangs sehr viel Selbstdisziplin, da ich schnellstmöglich im neuen Berufsfeld Fuß fassen wollte.

Welche IT-Umgebung betreuen Sie?

In unserem Unternehmen bin ich verantwortlich für das komplette Netzwerk- und Systemmanagement und den EDV-Einkauf. Dabei betreue ich unter anderem eine VMware ESX 4.0-Infrastruktur, die im Clusterverbund aufgebaut und an eine MSA SAS-Storage-Lösung angebunden ist. Zur Umgebung zählen neben Servern 2008 R2 noch DNS-, DHCP-, File-, Print-, WDS- und WSUS-Server. Im Clientbereich administrierte ich 50 PCs und 35 Laptops, die unter Windows XP, Vista und 7 laufen.

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

Um eine stabile IT-Infrastruktur zu gewährleisten, ist in gewissen Abständen das Einspielen von Firmware- und Treiber-Updates auf den Servern und aktiven Netzwerkkomponenten sowie das manuelle Einspielen der Betriebssystem-Updates unumgänglich. Das Erstellen von Dokumentationen, Bereitstellen neuer Clients und Testen neuer Soft- und Hard-



Geburtstag: 21.10.1975
Familienstand: verheiratet
Hobbys: IT, Lesen, Mountainbike Freeride und Downhill, Tennis

Harald Löscher, IT-Administrator

ware in unserer Testumgebung ist ebenso Teil meiner täglichen Arbeit.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

In den nächsten Wochen steht die Einführung unseres Managementsystems auf Basis von SharePoint an. Für das Jahr 2010 ist auch das Update aller Clients von Windows XP auf Windows 7 sowie nach Erscheinen des neuen Office 2010 die Erneuerung des Office-Pakets geplant.

Was macht Ihnen an Ihrem Job am meisten Spaß?

Das Arbeiten an fordernden Projekten. Mein Arbeitgeber schenkt mir im IT-Bereich sehr viel Vertrauen und das ist sehr hilfreich beim Umsetzen der Projekte und der täglichen Aufgaben.

Was tun Sie für Ihre Fort- und Weiterbildung?

Themenspezifische Schulungen, Diskutieren in Foren und das Lesen von IT-Zeitschriften sind ein großer Bestandteil meiner Fortbildung.

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

Ich habe beim Konfigurieren sämtlicher neuer und unterschiedlicher Hardware jeweils von allen Maschinentypen Images erstellt und auf eine externe Festplatte gesichert. Beim Partitionieren der Festplatte eines neuen Gerätes war diese externe Festplatte noch angeschlossen und ich löschte aus Versehen die Partitionen, auf denen alle Images gespeichert waren.


Was war Ihr größter Erfolg als IT-Administrator?

Auf die reibungslose Umstellung unserer Infrastruktur von Windows NT auf Server 2003, Citrix MF und den Wechsel von PCs zu Thin Clients bin ich sehr stolz.

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

Ein unerfahrener Benutzer behauptete, dass seine Maus nicht funktionieren würde. Nach Kontrolle vor Ort sagte ich, er sollte die Maus mal am Bildschirm bewegen. Er nahm tatsächlich die Maus in die Hand und fuhr mit dieser am Bildschirm hin und her.

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

Das Schlagwort "Green IT" werden IT-Verantwortliche in Ihren Entscheidungen in den nächsten Jahren vermehrt berücksichtigen müssen. Virtuelle Maschinen beziehungsweise Komponenten, SSD-Festplatten und die MAID-Technologie bei Disk-Arrays werden diesbezüglich einen großen Beitrag leisten. 

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 5/10 erscheint am 4. Mai 2010

Schwerpunktthema:

Remote-Access, VPN und Gateway-Schutz

Im Test: HOB RD VPN 1.3

Workshop: VPN-Remotenzugriff mit SSTP

Workshop: Windows 2008 R2 BrancheCache

Workshop: Forefront Unified Access Gateway

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

Unsere Ausgabe im Juni steht unter dem Schwerpunkt **Server-based Computing**. In der Test-Rubrik schauen wir uns den Thinstuff XP/VS Terminal Server sowie den ProPalms TSE 6.0 genauer an. In einem unserer Workshops lesen Sie außerdem, wie Sie die Virtualisierungslösung NoMaschine nutzen.

Als Schwerpunkt im Juli folgt dann das Thema **SAN- und Datenmanagement**.

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

Redaktion

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

Daniel Richey (di), *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, Jürgen Heyer,
 Roland Joeriskes, Thomas Joos, Christian Kriemann,
 Andreas Kohne, Martin Kuppinger, Sandra Lucifora,
 Nico Lüdemann, Thorsten Scherf, Eknar Török,
 Dennis Zimmer

Anzeigen

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

Es gilt die Anzeigenpreisliste
 Nr. 7 vom 01.11.2009



Produktion / Anzeigendisposition

Lightrays: Andreas Skrzypnik
 dispa@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

Ab- und Leserservice

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

Erscheinungsweise

monatlich

Bezugspreise

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

Studentenabonnement Ausland: € 75,-
 Jahresabonnement Inland mit Jahres-CD: € 144,84
 Studentenabonnement Inland mit Jahres-CD: € 77,34
 Jahresabonnement Ausland mit Jahres-CD: € 159,84
 Studentenabonnement Ausland mit Jahres-CD: € 84,84
 E-Paper-Einzelheftpreis: € 9,45
 E-Paper-Jahresabonnement: € 99,-
 E-Paper-Studentenabonnement: € 49,50
 Jahresabonnement-Kombi mit E-Paper: € 168,-
 (Studentenabonnements nur gegen Vorlage
 einer gültigen Immatrikulationsbescheinigung)

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

Internet

www.it-administrator.de

Verlag / Herausgeber

Heinemann Verlag GmbH
 Leopoldstraße 85
 80802 München

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

(zugleich Anschrift aller Verantwortlichen)

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

Eingetragen im Handelsregister des
 Amtsgerichts München unter
 HRB 151585.

Geschäftsführung / Anteilsverhältnisse

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

ISSN

1614-2888

Urheberrecht

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

Haftung

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

Manuskriptensendungen

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

Tundl	S.15, S.17	Hewlett Packard	S.02	Log.in Consultants	S.33, S.55
Datacenter Dynamics	S.21	itelio / Docusap	S.39	Microsoft	S.23
DeviceLock	S.27	LANCOM	S.68	Netviewer	S.09

INSERENTENVERZEICHNIS

Die Ausgabe enthält
 einen Beihefter der Firma IAIT
 (Institut zur Analyse von IT-Komponenten)
 zwischen Seite 34 und 35

Das IT-Administrator Komplettprogramm!!!

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

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

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



Als bestehender Jahresabonnent können Sie hier upgraden:

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

Oder Sie sind Neukunde? Hier können Sie bestellen:

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

www.it-administrator.de

 **Heinemann Verlag**
Im Dialog mit Spezialisten.

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

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

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

LANCOM



... connecting your business

Das beste WLAN aller Zeiten!

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

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

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



LANCOM OAP-310agn



LANCOM
Systems

www.lancom.de